Information Gathering

Steps in **hacking**

- Information Gathering
- Exploitation
- Maintaining Access
- Clearing tracks

Steps in **pentesting**

- Information Gathering
- Exploitation
- ~~Maintaining Access~~
- ~~Clearing tracks~~
- Documentation
- Report writing

Why we need to know the target?

- Speed up the process of finding vulnerabilities
- Increase the chance of a successful exploitation

What do we want to know?

- Address of our target
- OS type
- Running services
- What type of service software
- Any info on the target

What do we want to know?

- **Address of our target**
- OS type
- Running services
- What type of service software
- Any info on the target

URL vs Internet address

- URL – Uniform Resource Locater
  - For human
  - Translated to Internet Address through DNS
  - E.g. www.google.com
- Internet Address
  - For machines (and human)
  - The address being used for internet communication
  - E.g. 66.249.89.104

Internet address

- IP address
  - Internet protocol address
- Two versions
  - IPv4 = 66.249.89.104 (decimal)
    = 255.255.255.255
  - IPv6 = 2001:4860:0:1001::68 (hexadecimal)
    = ffff: ffff: ffff: ffff: ffff: ffff: ffff: ffff

IPv4

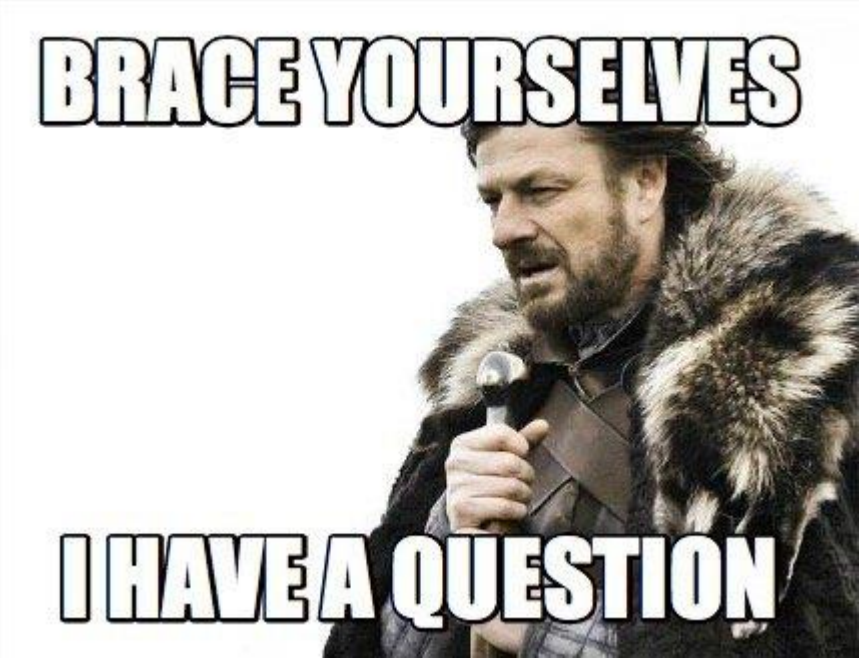
- Many forms of IPv4
  - Decimal

    66.249.89.104
  - Hexadecimal

    0x42F95968

Question

- What tool can we use to get the IP address of a host?



Favourite answer

PING

ping

- **`ping`** is a utility that sends an ICMP echo packet to usually used to check for the availability of a host
- Usage: ping <host>
- Example:

```
ping www.google.com
```

ping in action

C:\Windows\system32\cmd.exe

```
C:\Users\Owner>ping www.google.com

Pinging www.l.google.com [66.249.89.104] with 32 bytes of data:
Reply from 66.249.89.104: bytes=32 time=94ms TTL=51
Reply from 66.249.89.104: bytes=32 time=87ms TTL=51
Reply from 66.249.89.104: bytes=32 time=88ms TTL=51
Reply from 66.249.89.104: bytes=32 time=88ms TTL=51

Ping statistics for 66.249.89.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 87ms, Maximum = 94ms, Average = 89ms

C:\Users\Owner>
```

ping pros & cons

- Pros:
  - Easy to use
  - Available on all platforms (built-in tool)
- Cons:
  - Cannot change default nameserver (within the tool)
  - Some server might block ICMP echo packets
  - Might only get partial result

Tools to check IP address

- nslookup
- host
- dig

nslookup

- Usage: nslookup <host> [dns-server]
- Examples:

```
nslookup www.google.com
nslookup www.google.com 8.8.8.8
```

nslookup in action

C:\Windows\system32\cmd.exe

```
C:\Users\Owner>nslookup www.google.com
Server:  ns2.utm.my
Address:  161.139.16.2

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:    www.l.google.com
Addresses:  66.249.89.99
          66.249.89.104
Aliases:  www.google.com


C:\Users\Owner>_
```

nslookup in action (cont.)

C:\Windows\system32\cmd.exe

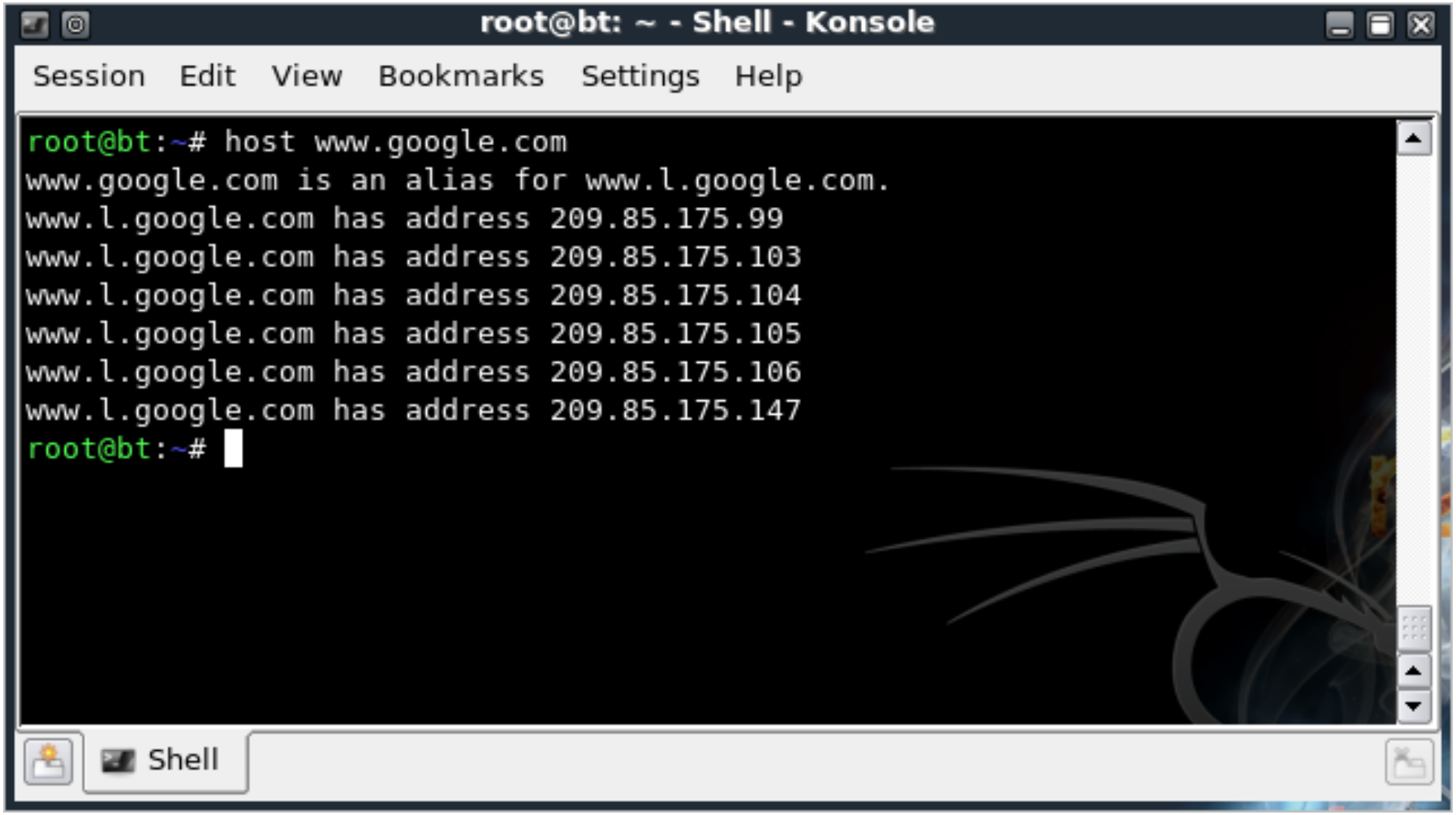
```
C:\Users\Owner>nslookup www.google.com 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.l.google.com
Addresses:  209.85.175.147
          209.85.175.99
          209.85.175.104
          209.85.175.106
          209.85.175.103
          209.85.175.105
Aliases:  www.google.com


C:\Users\Owner>_
```

host

- Usage: host <host> [dns-server]
- Examples:

```
host www.google.com
host www.google.com 8.8.8.8
```

host in action



dig

- Usage: dig [host] [@dns-server]
- Examples:

```
dig www.google.com
dig www.google.com @8.8.8.8
```

dig in action

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# dig www.google.com

; <<>> DiG 9.5.0-P2.1 <<>> www.google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35709
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         5       IN      CNAME   www.l.google.com.
www.l.google.com.       5       IN      A       209.85.175.105
www.l.google.com.       5       IN      A       209.85.175.106
www.l.google.com.       5       IN      A       209.85.175.147
www.l.google.com.       5       IN      A       209.85.175.99
www.l.google.com.       5       IN      A       209.85.175.103
www.l.google.com.       5       IN      A       209.85.175.104

;; Query time: 5 msec
;; SERVER: 192.168.118.2#53(192.168.118.2)
;; WHEN: Mon Apr 25 03:12:26 2011
;; MSG SIZE  rcvd: 148

root@bt:~#
```

Shell

Which tool to use?

- Depends on availability and personal preference
- Suggestion:
  - **`ping`** NOT RECOMMENDED !
  - Go for **`nslookup`** / **`host`** / **`dig`**

What do we want to know?

- **Address of our target**
- **OS type**
- Running services
- Exact version of software
- Any info on the target

Operating Systems

- OS – Software that runs/manages the computer and its services
- Different OS uses different sets of command and may do things differently
- Example:
  - Show list of files:
    - **`ls`** = linux/unix
    - **`dir`** = windows

ls vs dir

root@bt: / - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:/# ls
bin    dev   initrd.img  media  pentest  sbin  tmp  vmlinuz
boot   etc   lib         mnt    proc     srv   usr
cdrom  home  lost+found  opt    root     sys   var
root@bt:/#
```

Shell

C:\Windows\system32\cmd.exe

```
C:\>dir
 Volume in drive C is System
 Volume Serial Number is 9002-5611

 Directory of C:\

08/03/2011  10:47 PM             1,024 .rnd
11/06/2009  05:42 AM                24 autoexec.bat
11/06/2009  05:42 AM                10 config.sys
15/04/2011  04:06 PM    <DIR>          Downloads
14/07/2009  10:37 AM    <DIR>          PerfLogs
21/04/2011  02:45 PM    <DIR>          Program Files
04/03/2011  04:26 PM    <DIR>          Users
08/03/2011  10:49 PM    <DIR>          VMware
08/03/2011  11:42 PM    <DIR>          WinDDK
26/04/2011  10:02 AM    <DIR>          Windows
               3 File(s)          1,058 bytes
               7 Dir(s)   6,293,090,304 bytes free
```

Why we need to know the OS?

- Lets say that we found a vulnerability in a system that allows us to execute commands on the remote OS
- We send the command:

```
net user hacker 123456 /add
```

- However, we scratch our head wondering why the command didn’t work
- Hint: The target is a linux machine

Tools to OS fingerprinting

- **`nmap`**
- **`xprobe2`**

nmap

- **`nmap`** - **n**etwork **map**per
- a multipurpose tool for OS detection, port scanning, & service software detection
- Option -O (capital ‘O’) is for OS detection
- Usage: nmap [options] <host>
- Example:

```
nmap -O www.google.com
```

nmap in action

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# nmap -O www.google.com

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-04-25 21:36 EDT
Nmap scan report for www.google.com (209.85.149.103)
Host is up (0.0075s latency).
Other addresses for www.google.com (not scanned): 209.85.149.104 209.85.149.
105 209.85.149.106 209.85.149.147 209.85.149.99
rDNS record for 209.85.149.103: ber01s02-in-f103.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least
 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING) : Apple Mac OS X 10.5.X (98%), BlueArc embedded (93%
)
Aggressive OS guesses: Apple Mac OS X 10.5.5 (Leopard) (98%), BlueArc Titan
2100 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.74 seconds
root@bt:~#
```

Shell

xprobe2

- **`xprobe2`** is an OS fingerprinting tool
- uses multiple approaches for OS detection
- Usage: xprobe2 <host>
- Example:

```
xprobe2 www.google.com
```

xprobe2 in action

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# xprobe2 www.google.com

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com,
meder@o0o.nu

[+] Target is www.google.com
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting mo
dule
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting
module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinti
ng module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
```

Shell

xprobe2 in action (cont.)

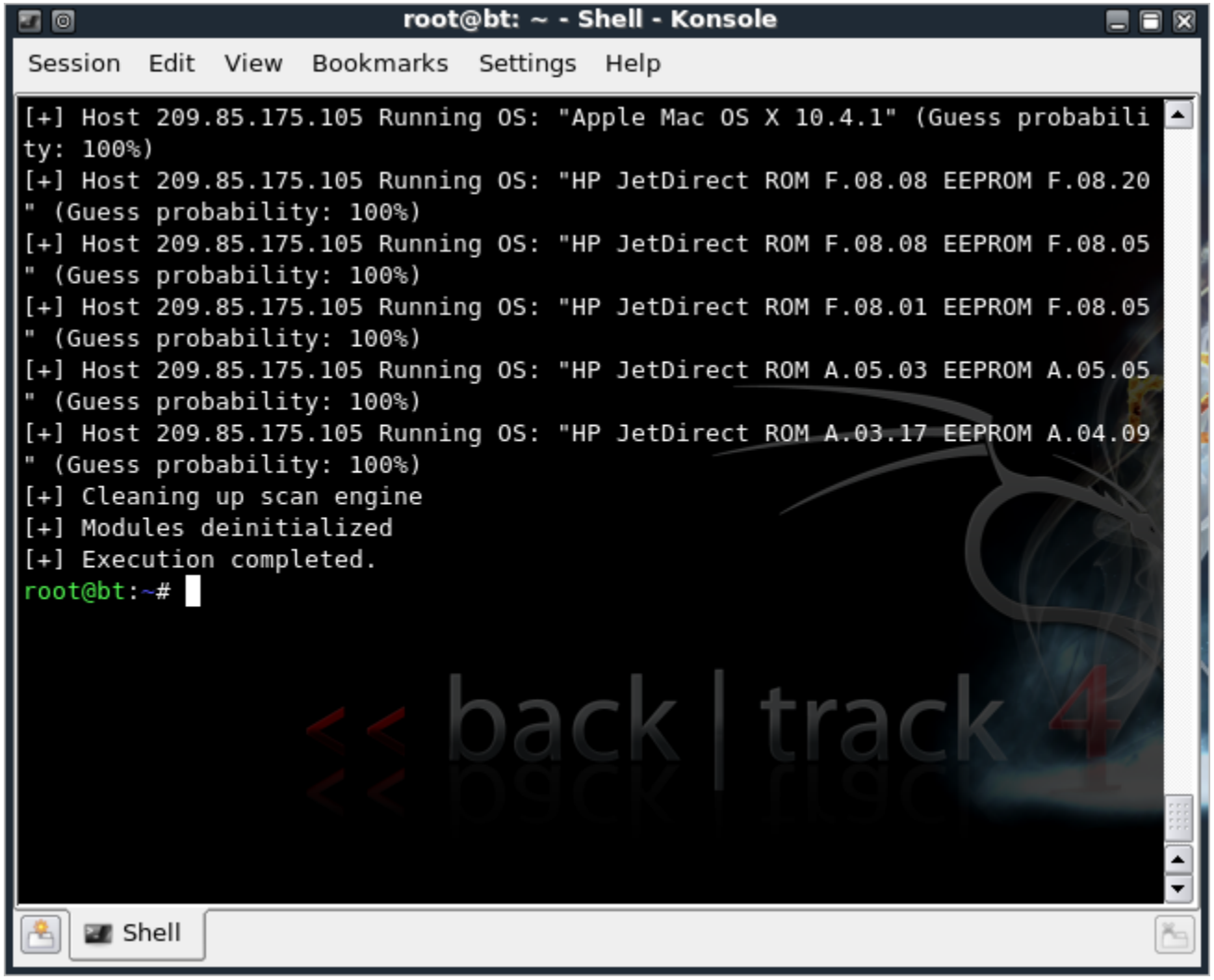
root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 209.85.175.105.
Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 209.85.175.105.
Module test failed
[-] No distance calculation. 209.85.175.105 appears to be dead or no ports k
nown
[+] Host: 209.85.175.105 is up (Guess probability: 50%)
[+] Target: 209.85.175.105 is alive. Round-Trip Time: 0.01273 sec
[+] Selected safe Round-Trip Time value is: 0.02547 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known
)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 209.85.175.105 Running OS: "Apple Mac OS X 10.3.7" (Guess probabili
ty: 100%)
[+] Other guesses:
[+] Host 209.85.175.105 Running OS: "Apple Mac OS X 10.3.8" (Guess probabili
ty: 100%)
[+] Host 209.85.175.105 Running OS: "Apple Mac OS X 10.3.9" (Guess probabili
ty: 100%)
[+] Host 209.85.175.105 Running OS: "Apple Mac OS X 10.4.0" (Guess probabili
ty: 100%)
```

Shell

xprobe2 in action (cont.)



nmap vs xprobe2

- **`nmap`** output is a lot cleaner, less info
- **`xprobe2`** spills out tons of info, most of it about it's configuration
- Suggestion:
  - Go for **`nmap`**

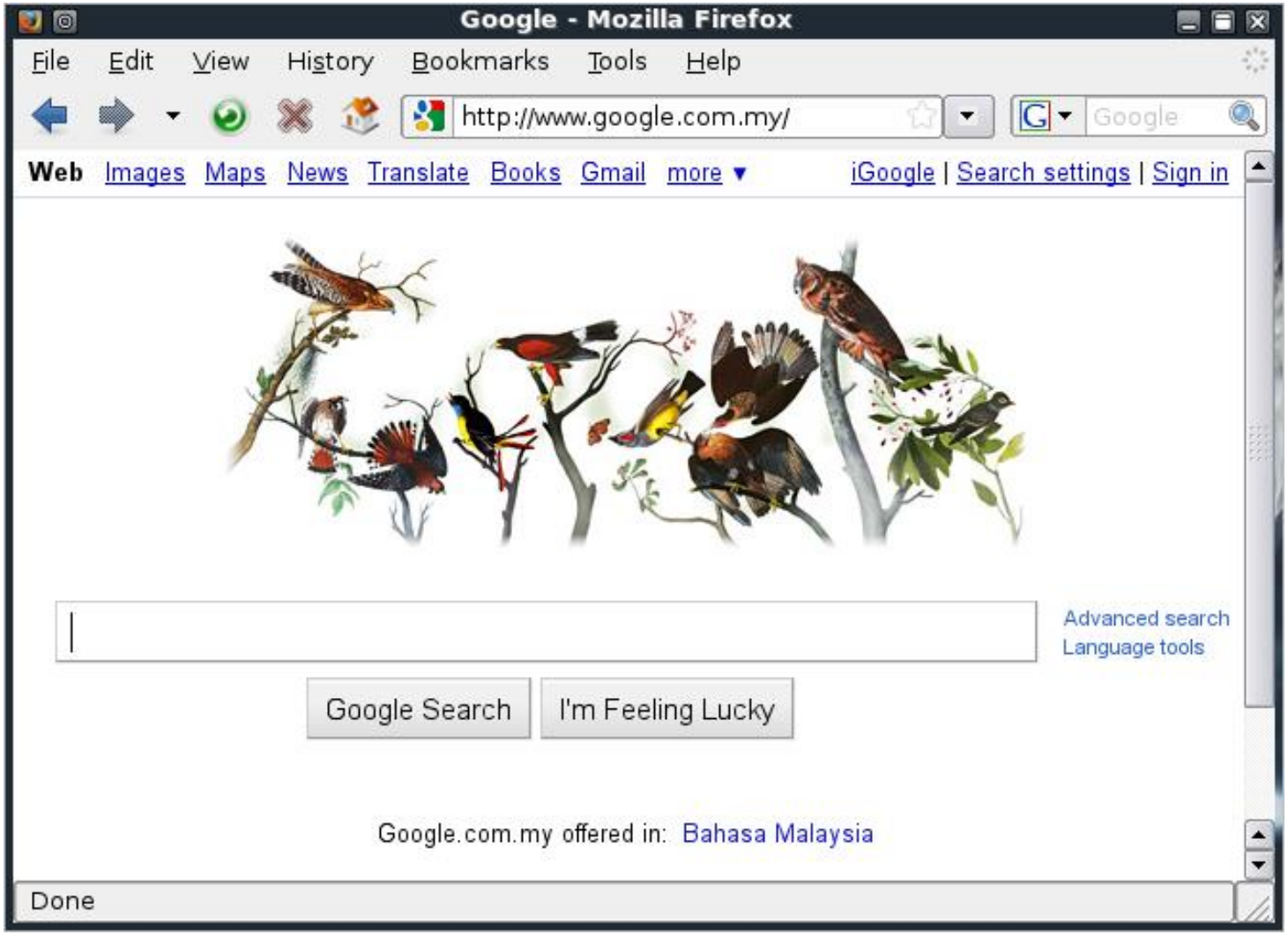
What do we want to know?

- **Address of our target**
- **OS type**
- **Running services**
- Exact version of software
- Any info on the target

What are services ?

- Services as the name implies – what the computer can do for you
- Runs at a particular port address (number)
- Example:
  - http : 80
  - https : 443
  - ftp : 20 & 21 (for active mode)
  - MySQL : 3306

Normal access to http service



View source

Source of: http://www.google.com.my/ - Mozilla Firefox

File Edit View Help

```
<!doctype html><html><head><meta http-equiv="content-type" content="text/html;
charset=UTF-8"><title>Google</title><script>window.google={kEI:"0C-
2TZXrK82rrAeQh42KAg",kEXPI:"17259,23756,24878,27400,27495,29050,29106,29432,29680,29685,
{e:"17259,23756,24878,27400,27495,29050,29106,29432,29680,29685,29822,29876,29881",ei:"0
2TZXrK82rrAeQh42KAg",expi:"17259,23756,24878,27400,27495,29050,29106,29432,29680,29685,2
{},pageState:"#",kHL:"en",time:function(){return(new Date).getTime()},
log:function(c,d,b){var a=new Image,e=google,g=e.lc,f=e.li;a.onerror=(a.onload=
(a.onabort=function(){delete g[f]}));g[f]=a;b=b||"/gen_204?atyp=i&ct="+c+"&cad="+d+"&
zx="+google.time();a.src=b;e.li=f+1},lc:[],li:0,j:{en:1,l:function()
{google.fl=true},e:function(){google.fl=true},b:location.hash&&
location.hash!="#",bv:11,pl:[],mc:0,sc:0.5,u:"c9c918f0"},
Toolbelt:{}};(function(){var c=google.j;window.onpopstate=function(){c.psc=1};for(var
d=0,b;b=["ad","bc","is","p","pa","ac","pc","pah","ph","sa","slp","spf","xx","zc","zz"]
[d++];)(function(a){c[a]=function(){c.pl.push([a,arguments])}})(b)})();

window.google.sn="webhp";var i=window.google.timers=
{};window.google.startTick=function(a,b){i[a]={t:{start:(new Date).getTime()},bfr:!
(!b)}};window.google.tick=function(a,b,c){if(!i[a])google.startTick(a);
i[a].t[b]=c||(new
Date).getTime()};google.startTick("load",true);try{window.google.pt=window.gtbExternal&&
window.gtbExternal.pageT();
}catch(v){}
</script><style id=gstyle>body{margin:0}#gog{padding:3px 8px 0}td{line-
height:.8em}.gac_m td{line-height:17px}form{margin-bottom:20px}body,td,a,p,.h{font-
family:arial,sans-serif}.h{color:#36c}.q{color:#00c}.ts td{padding:0}.ts{border-
collapse:collapse}em{font-weight:bold;font-
style:normal}.lst{height:25px;width:496px}.ds{border-bottom:solid 1px #e7e7e7;border-
```

Manual access to http service

root@bt: / - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:/# nc www.google.com.my 80
GET / HTTP/1.0
Host: www.google.com.my

HTTP/1.0 200 OK
Date: Tue, 26 Apr 2011 02:35:50 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie: PREF=ID=16c488badd0ac7ed:FF=0:TM=1303785350:LM=1303785350:S=RzSAHYyeEFR
DRwt1; expires=Thu, 25-Apr-2013 02:35:50 GMT; path=/; domain=.google.com.my
Set-Cookie: NID=46=F7MnMo1NbBEyOhSWq9OdE-Kk1De31JLlHmRsqKxQE5BNZrLdOqtHLZr-8NTzYnGu
8jjHrRzSGPmXVoWGMADRz2fSiVn_uk0F73-BLjm_NFLoOTMFWUvzifw1vMXHKX4o; expires=Wed, 26-O
ct-2011 02:35:50 GMT; path=/; domain=.google.com.my; HttpOnly
Server: gws
X-XSS-Protection: 1; mode=block

<!doctype html><html><head><meta http-equiv="content-type" content="text/html; char
set=ISO-8859-1"><title>Google</title><script>window.google={kEI:"hi-2TZ2BCsSxtAam-6
jvCw",kEXPI:"29050,29106,29685,29859,29876,29881",kCSI:{e:"29050,29106,29685,29859,
29876,29881",ei:"hi-2TZ2BCsSxtAam-6jvCw",expi:"29050,29106,29685,29859,29876,29881"
},authuser:0,ml:function(){},kHL:"en",time:function(){return(new Date).getTime()},
log:function(c,d,b){var a=new Image,e=google,g=e.lc,f=e.li;a.onerror=(a.onload=(a.o
nabort=function(){delete g[f]}));g[f]=a;b=b||"/gen_204?atyp=i&ct="+c+"&cad="+d+"&zx
="+google.time();a.src=b;e.li=f+1},lc:[],li:0,
```

Shell

Tools to scan for services

- **`nmap`**
  - Scans for open ports
- **`amap`**
  - Scans services on nonstandard ports

nmap scan options

- Soooo many scan options:
  - TCP
    - TCP Connect Scan (-sT)
    - SYN scan (-sS)
    - FIN scan (-sF)
    - XMAS scan (-sX)
    - NULL scan (-sN)

    Unreliable
  - UDP
    - UDP Scan (-sU)

nmap: which one to choose?

- TCP port scanning
  - Fast scan (but noisy): **TCP connect**
  - Stealthy (but very slow) : **SYN scan**

- UDP port scanning
  - **UDP scan** (no other options)

nmap usage

- Usage: nmap [options] <host>
- Example:
  - TCP Connect scan

```
nmap -sT www.google.com
```

  - SYN scan

```
nmap -sS www.google.com
```

  - UDP scan

```
nmap -sU www.google.com
```

nmap TCP connect scan

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# nmap -sT webs.cs.utm.my

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-04-26 03:41 EDT
Nmap scan report for webs.cs.utm.my (161.139.68.212)
Host is up (0.0034s latency).
rDNS record for 161.139.68.212: webs.fsksm.utm.my
Not shown: 990 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
2179/tcp  open  unknown
3306/tcp  open  mysql
3389/tcp  open  ms-term-serv
49152/tcp open  unknown
49154/tcp open  unknown
49157/tcp open  unknown
49161/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.81 seconds
```

Shell | Shell No. 2

nmap SYN scan

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# nmap -sS webs.cs.utm.my

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-04-26 03:51 EDT
Warning: 161.139.68.212 giving up on port because retransmission cap hit (10).
Nmap scan report for webs.cs.utm.my (161.139.68.212)
Host is up (0.89s latency).
rDNS record for 161.139.68.212: webs.computer-science.utm.my
Not shown: 971 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
514/tcp   filtered shell
666/tcp   filtered doom
1234/tcp  filtered hotline
1900/tcp  filtered upnp
2002/tcp  filtered globe
2179/tcp  open     unknown
3071/tcp  open     unknown
```

Shell | Shell No. 2

nmap SYN scan (cont.)

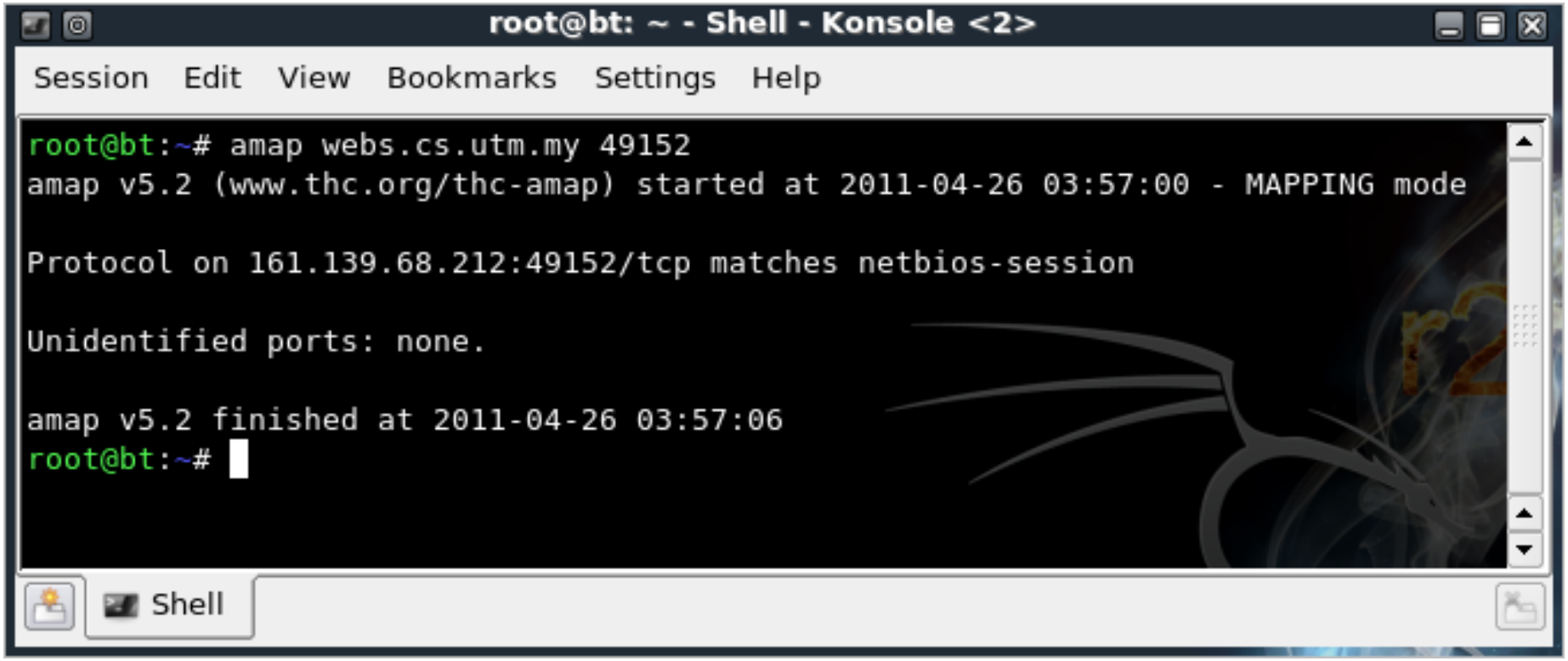
```
3128/tcp  filtered squid-http
3306/tcp  open     mysql
3389/tcp  open     ms-term-serv
6667/tcp  filtered irc
8873/tcp  filtered unknown
8888/tcp  filtered sun-answerbook
9898/tcp  filtered unknown
12345/tcp filtered netbus
31337/tcp filtered Elite
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49155/tcp open     unknown
49157/tcp open     unknown
49161/tcp open     unknown
65000/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 4054.27 seconds
root@bt:~#
```

amap

- **`nmap`** scans sometimes resulted in a number of unknown ports
- These ports can be examined further by using **`amap`**
- Usage: amap <host> <port>
- Example:

```
amap webs.cs.utm.my 49152
```

amap scan


root@bt: ~ - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
root@bt:~# amap webs.cs.utm.my 49152
amap v5.2 (www.thc.org/thc-amap) started at 2011-04-26 03:57:00 - MAPPING mode
Protocol on 161.139.68.212:49152/tcp matches netbios-session
Unidentified ports: none.
amap v5.2 finished at 2011-04-26 03:57:06
root@bt:~#
Shell

What do we want to know?

- **Address of our target**
- **OS type**
- **Running services**
- **Exact version of software**
- Any info on the target

But why?

- Enables faster identification of known or 0-day vulnerabilities

CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search View CVE

.og In Register

Vulnerability Feeds & WidgetsNew www

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores

Apache » Http Server : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **193** Page : 1 (This Page) 2 3 4

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ
1	CVE-2016-5387	284			2016-07-18	2016-11-02	5.1	None	Remote	High	Not required	Partial	Parti

The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the prese untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outb traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

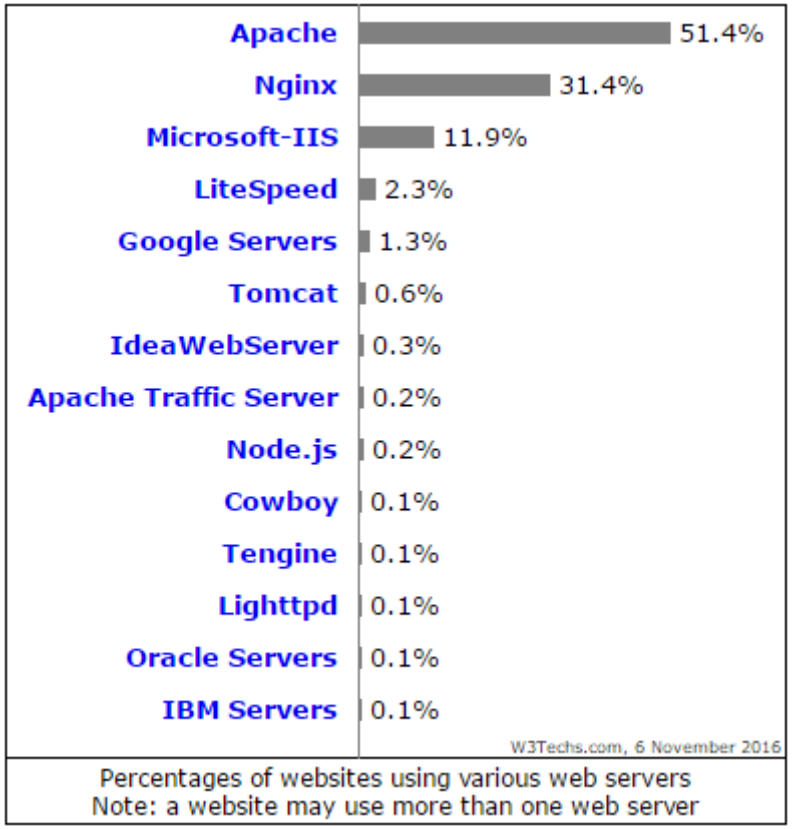
2	CVE-2016-4979	284		Bypass	2016-07-06	2016-10-26	5.0	None	Remote	Low	Not required	None	Parti

The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVe require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leverag ability to send multiple requests over a single connection and aborting a renegotiation.

Service and Software

Service	Software
HTTP	Apache IIS nginx lighttpd
FTP	FileZilla ProFTPD Wu-ftpd

Usage share of webserver



Server (software)

- Different server (software) does things differently
- Some are cross platform (e.g. Apache), some are not (e.g. IIS)
- It is important to identify it because we can understand :
  - how it works
  - **how to exploit it !**

Service software detection tool

- Automated:
  - **`nmap`** (scan option: -sV)
- Manual:
  - **`nc`** / **`telnet`** (text based services)
  - **`openssl`** (text based services + SSL)

Using nmap for service detection

- Command: nmap –sV <host>
- Example:

```
nmap -sV www.google.com
```

nmap service detection

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# nmap -sV webs.cs.utm.my

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-04-26 21:58 EDT
Warning: 161.139.68.212 giving up on port because retransmission cap hit (10).
Nmap scan report for webs.cs.utm.my (161.139.68.212)
Host is up (0.69s latency).
rDNS record for 161.139.68.212: webs.computer-science.utm.my
Not shown: 972 closed ports
PORT      STATE    SERVICE            VERSION
21/tcp    open     ftp                FileZilla ftpd 0.9.31 beta
80/tcp    open     http               Apache httpd 2.2.11 ((Win32) DAV/2 mod_ssl
/2.2.11 OpenSSL/0.9.8i PHP/5.2.9 mod_aspdotnet/2.2)
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     ssl/http           Apache httpd 2.2.11 ((Win32) DAV/2 mod_ssl
/2.2.11 OpenSSL/0.9.8i PHP/5.2.9 mod_aspdotnet/2.2)
445/tcp   filtered microsoft-ds
514/tcp   filtered shell
666/tcp   filtered doom
1234/tcp  filtered hotline
1900/tcp  filtered upnp
2002/tcp  filtered globe
2179/tcp  open     unknown
3071/tcp  open     ssl/unknown
```

Shell

nmap service detection (cont.)

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
3128/tcp  filtered squid-http
3306/tcp  open     mysql                MySQL 5.1.33-community
3389/tcp  open     microsoft-rdp        Microsoft Terminal Service
6667/tcp  filtered irc
8888/tcp  filtered sun-answerbook
9898/tcp  filtered unknown
12345/tcp filtered netbus
31337/tcp filtered Elite
49152/tcp open     msrpc                Microsoft Windows RPC
49153/tcp open     msrpc                Microsoft Windows RPC
49154/tcp open     msrpc                Microsoft Windows RPC
49155/tcp open     ssl/megaraid-monitor MegaRaid Monitoring Agent
49157/tcp open     msrpc                Microsoft Windows RPC
49161/tcp open     msrpc                Microsoft Windows RPC
65000/tcp filtered unknown
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.o
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3894.12 seconds
root@bt:~#
```

Shell

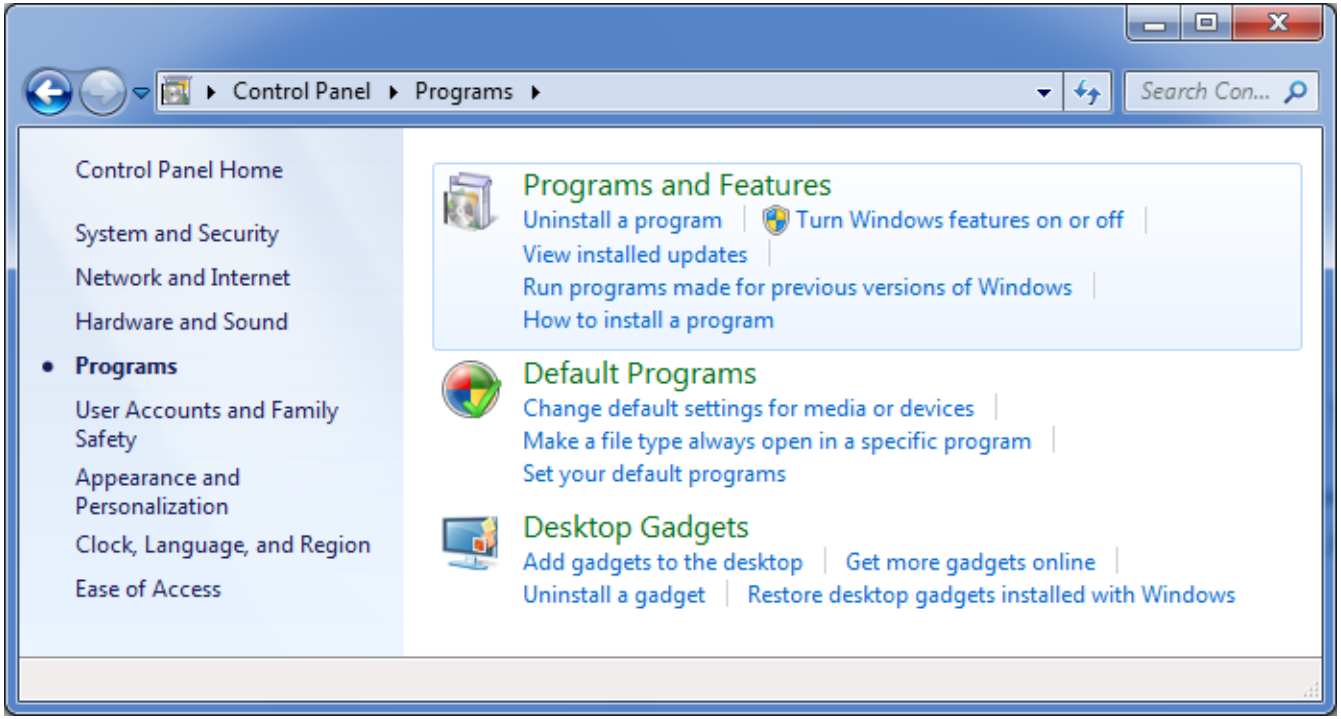
nc

- **`nc`** (netcat) is available by default in popular linux distributions
- netcat command: nc <host> <port>
- Example:

```
nc www.google.com 80
```

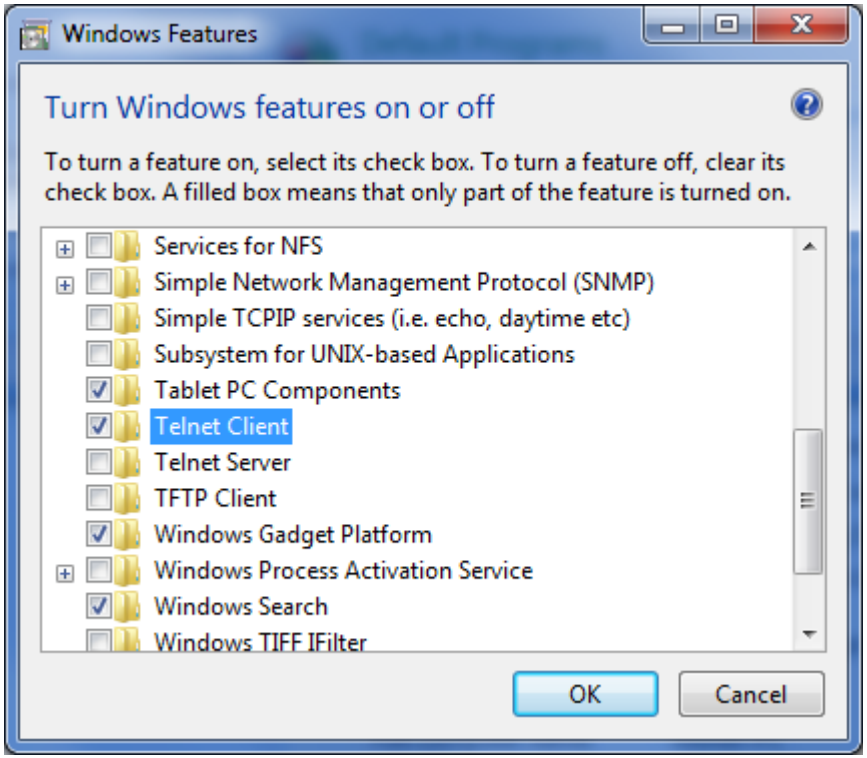
telnet

- telnet is not available by default in Windows Vista, Windows 2008 and Windows 7
- To enable it, go to Control Panel -> Programs



telnet (cont.)

- Click on ‘Turn Windows features on or off’
- Check on ‘Telnet Client’ and click ‘OK’ and restart your PC.



telnet (cont.)

- telnet usage: telnet <host> <port>
- Example:

```
telnet www.google.com 80
```

nc or telnet

- **`nc`** has a lot more features than **`telnet`**
- Both will do for **banner grabbing**

Banner grabbing

- Banner grabbing – grabbing a service software greeting info (banner)
- Service software usually greets newly connected clients by displaying a banner with **useful information** (for hackers of course !)
- Service software banner is **normally not shown** in client application

Banner grabbing

- Banner info may include:
  - OS type
  - Service Software name
  - Service Software version
  - Local time information

HTTP banner grabbing

- Example:

```
nc www.google.com 80↵
HEAD / HTTP/1.0↵
Host: www.google.com↵
↵
```

or

```
telnet www.google.com 80↵
HEAD / HTTP/1.0↵
Host: www.google.com↵
↵
```

↵ = Enter

HTTP banner grabbing (cont.)

```
root@bt:~# nc www.utm.my 80
HEAD / HTTP/1.0
Host: www.utm.my

HTTP/1.1 200 OK
Date: Wed, 27 Apr 2011 03:01:16 GMT
Server: Apache/2.2.6 (Unix) PHP/5.2.4 mod_ssl/2.2.6 OpenSSL/0.9.7d
X-Powered-By: PHP/5.2.4
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

HTTPS banner grabbing using nc?

- HTTPS is different from HTTP
  - Uses SSL for encrypted communication
  - Runs on port 443
- **`nc`** cannot be used since it only supports plain text communication (no SSL support)
- Time for a new tool **`openssl`**

OpenSSL for banner grabbing

- Usage:

  openssl s_client –connect <host>:<port>

- Example:

```
openssl s_client -connect www.google.com:443
```

HTTPS banner grabbing

- Example:

```
openssl s_client -connect www.google.com:443⏎
HEAD / HTTP/1.0⏎
Host: www.google.com⏎
⏎
```

HTTPS banner grabbing (cont.)

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
root@bt:~# openssl s_client -connect www.google.com:443
CONNECTED(00000003)
depth=1 /C=ZA/O=Thawte Consulting (Pty) Ltd./CN=Thawte SGC CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
   i:/C=ZA/O=Thawte Consulting (Pty) Ltd./CN=Thawte SGC CA
 1 s:/C=ZA/O=Thawte Consulting (Pty) Ltd./CN=Thawte SGC CA
   i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIQL9+89q6RUm0PmqPfQDQ+mjANBgkqhkiG9w0BAQUFADBM
MQswCQYDVQQGEwJaQTElMCMGA1UEChMcVGhhd3RlIENvbnN1bHRpbmcgKFB0eSkg
THRkLjEWMBQGA1UEAxMNVGhhd3RlIFNHQyBDQTAeFw0wOTEyMTgwMDAwMDBaFw0x
MTEyMTgyMzU5NTlaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRYwFAYDVQQHFA1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKFApHb29nbGUgSW5jMRcw
FQYDVQQDFA53d3cuZ29vZ2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEA6PmGD5D6htffvXImttdEAoN4c9kCKO+IRTn7EOh8rqk41XXGOOsKFQebg+jN
gtXj9xVoRaELGYW84u+E593y17iYwqG7tcFR39SDAqc9BkJb4SLD3muFXxzW2k6L
05vuuWciKh0R73mkszeK9P4Y/bz5RiNQl/Os/CRGK1w7t0UCAwEAAaOB5zCB5DAM
BgNVHRMBAf8EAjAAMDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly9jcmwudGhhd3Rl
LmNvbS9UaGF3dGVTR0NDQS5jcmwwKAYDVR0lBCEwHwYIKwYBBQUHAwEGCCsGAQUF
```

Shell

HTTPS banner grabbing (cont.)

root@bt: ~ - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
BwMCBglghkgBhvhCBAEwcgYIKwYBBQUHAQEEZjBkMCIGCCsGAQUFBzABhhZodHRw
Oi8vb2NzcC50aGF3dGUuY29tMD4GCCsGAQUFBzAChjJodHRwOi8vd3d3LnRoYXd0
ZS5jb20vcmVwb3NpdG9yeS9UaGF3dGVfU0dDX0NBLmNydDANBgkqhkiG9w0BAQUF
AAOBgQCfQ89bxFApsb/isJr/aiEdLRLDLE5a+RLizrmCUi3nHX4adpaQedEkUjh5
u2ONgJd8IyAPkU0Wueru9G2Jysa9zCRo1kNbzipYvzwY4OA8Ys+WAi0oR1A04Se6
z5nRUP8pJcA2NhUzUnC+MY+f6H/nEQyNv4SgQhqAibAxWEEHXw==
-----END CERTIFICATE-----
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=www.google.com
issuer=/C=ZA/O=Thawte Consulting (Pty) Ltd./CN=Thawte SGC CA
---
No client certificate CA names sent
---
SSL handshake has read 1765 bytes and written 304 bytes
---
New, TLSv1/SSLv3, Cipher is RC4-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : RC4-SHA
    Session-ID: F30A26C1EBE802A315EAC55A7245346676387B709B6974FBFF5C74C0F9D9D50F
    Session-ID-ctx:
    Master-Key: 44D0C16FB8DE3BDFCF0DA44505CD7EDBE853995C10440312F832AD14A5F9BD3E
02B1787945E2F6C385BB830A6149C6
```

Shell

HTTPS banner grabbing (cont.)

```
    Key-Arg   : None
    Start Time: 1303874962
    Timeout   : 300 (sec)
    Verify return code: 20 (unable to get local issuer certificate)
---
HEAD / HTTP/1.0
Host: www.google.com

HTTP/1.0 302 Found
Location: https://encrypted.google.com/
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Set-Cookie: PREF=ID=00fd5583020adf35:FF=0:TM=1303874977:LM=1303874977:S=TQcnoVqK
6P_cGQ; expires=Fri, 26-Apr-2013 03:29:37 GMT; path=/; domain=.google.com
Date: Wed, 27 Apr 2011 03:29:37 GMT
Server: gws
Content-Length: 226
X-XSS-Protection: 1; mode=block

read:errno=0
root@bt:~#
```

nmap vs nc/telnet/openssl

- **`nmap`**
  - Easier to use
  - Very noisy (not stealthy)
  - Could be very slooow
- **`nc` / `telnet`**
  - Need to understand target protocol
  - Could be stealthy (if we faking a particular client)
  - Superfast !

What do we want to know?

- **Address of our target**
- **OS type**
- **Running services**
- Exact version of software
- **Any info on the target**

More info?

- We already know
  - Server IP address
  - OS type
  - Running service
  - Service Software

- Isn’t that enough already ? **NO**

More info = better chance

- Additional ways to get information
  - Google
  - Error messages
  - Directory brute force

Google for hacking ?

- **Google hacking** - the art of explicit google searching using advanced keywords (dork)

- Useful advanced search keywords:
  - **`site:`** = search within this website
  - **`ext:`** = file extension to search for
  - **`inurl:`** = word is in the URL
  - **`intitle:`** = word is in the title page

Google hacking

- Scenario: searching **website.com** for an excel file (**XLS**) that contains **password**

- Example:

```
site:website.com ext:xls password
```

Google hacking example

site:u[redacted].my ext:xls password - Google Search - Mozilla Firefox

http://www.google.com/search?num=100&hl=en&safe=active&

site:u[redacted].my ext:xls password - G...

Web Images Videos Maps News Shopping Gmail more Sign in

Google

site:u[redacted].my ext:xls password Search

SafeSearch strict

2 results (0.19 seconds) Advanced search

Everything
Images
Videos
News
Shopping
Blogs
More

All results
Wonder wheel
Related searches

[XLS]
Downlo[redacted]search Management Centre
File Format: Microsoft Excel - View as HTML
31 Dec 2010 ... The **password** is apc2010.[redacted]
Name of Nominee, : 50, Faculty/Institute, : 51. 52, Award Category. 53, Science and Technology ...
www.r[redacted].my/.../2.
[redacted]2010.xls

Free Password !

[XLS]
Downlo[redacted]search Management Centre
File Format: Microsoft Excel - View as HTML
The **password** is apc2009. 46. 47. 48, Name of Nominee, : 49, Faculty/Institute, : 50. 51, Award Category. 52, Science and Technology ...

Done Proxy: None

More dorks

- Searching for login page

  `site:website.com inurl:login.php`

- Searching for certain pattern (e.g. &controller)

  `site:website.com inurl:&controller`

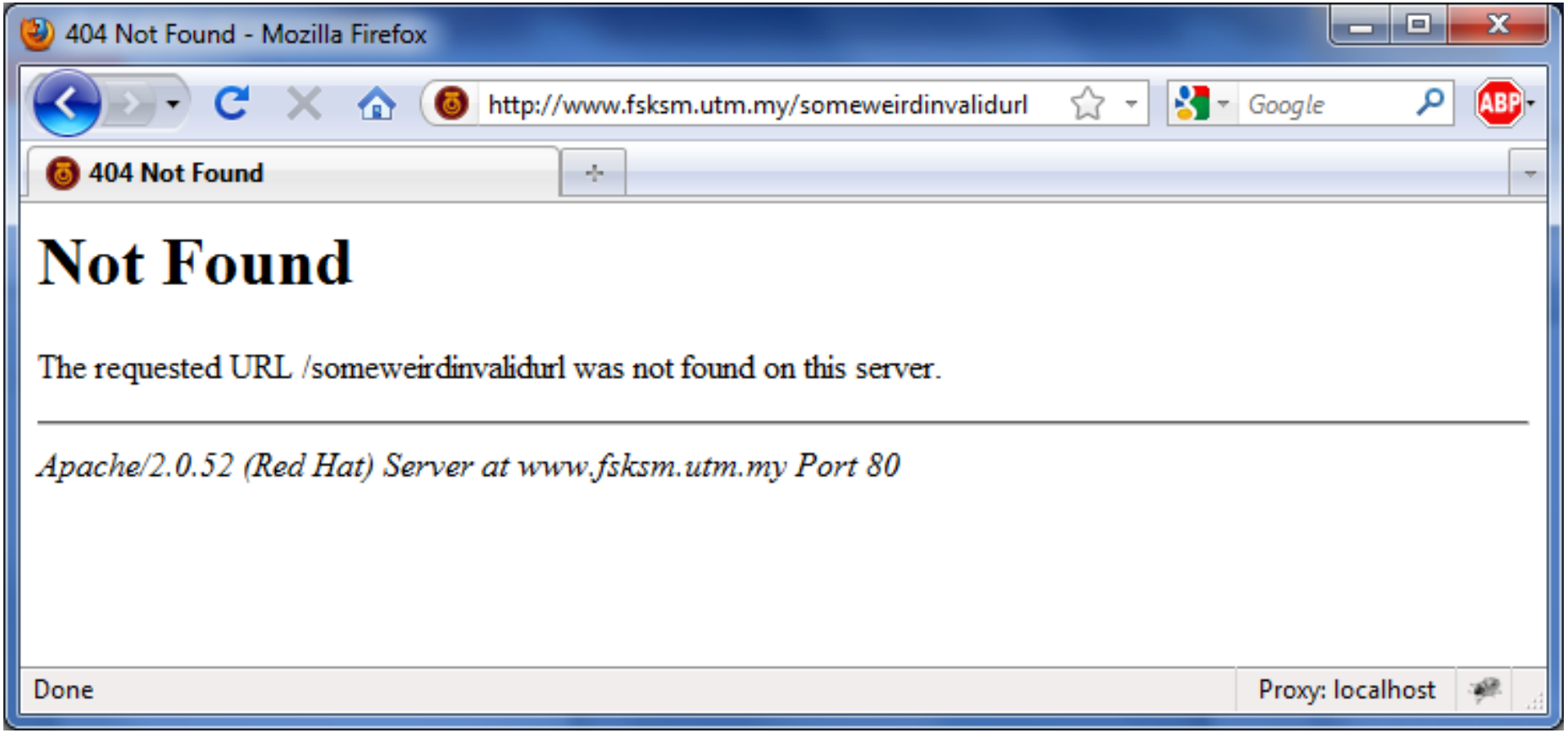
Error message ?

- Error message is a hacker's best friend
- Common methods to cause an error in web applications:
  - Invoking invalid URLs
  - Modifying GET/POST parameter
  - Modifying cookie values

Will be covered in later chapters Insya-Allah

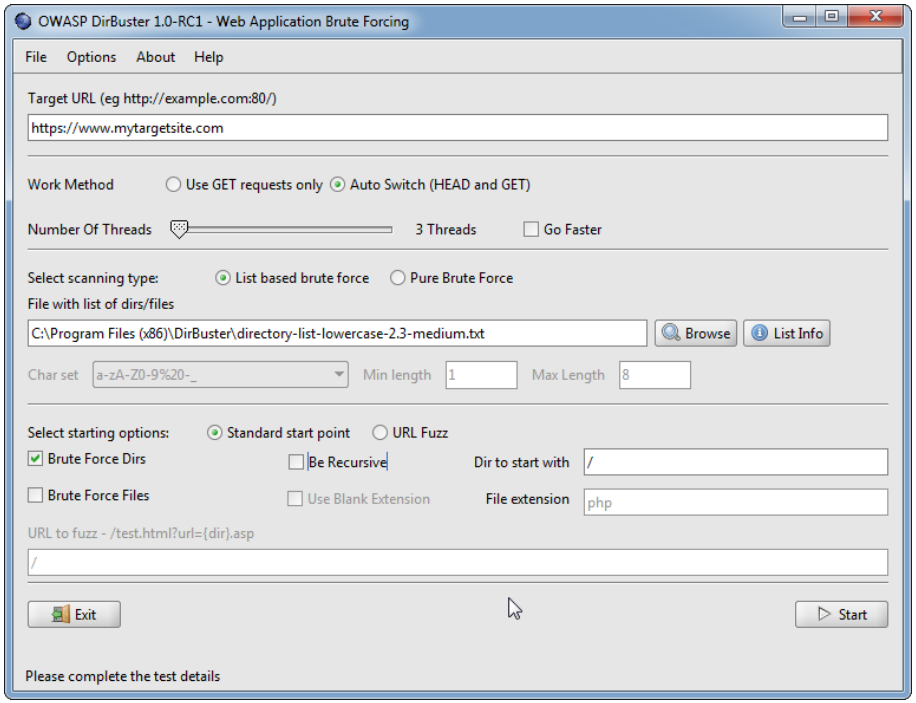
Invoking invalid URLs

- Example: http://abc.com/<type anything>



Directory brute forcing

- Find directories which are not referred to by any web page links
- Tool example: DirBuster



DirBuster sample output

OWASP DirBuster 0.12 - Web Application Brute Forcing

File Options About Help

http://192.168.56.101:80/

List View | Tree View

Type	Found	Response	Size	Include	Status
Dir	/docs/	200	1117	✓	Waiting
Dir	/icons/	200	178	✓	Waiting
Dir	/web/	200	200	✓	Waiting
Dir	/doc/	403	480	✓	Waiting
File	/docs/DVWA-Documentation.pdf	200	498801		
Dir	/external/	200	1095	✓	Waiting
Dir	/logout/	302	352	✓	Waiting
Dir	/external/phpids/	200	1112	✓	Waiting
Dir	/config/	200	1106	✓	Waiting
Dir	/external/phpids/0.6/	200	1912	✓	Waiting
Dir	/setup/	200	3863	✓	Waiting
File	/config/config.inc.php	200	191		
Dir	/logs/	200	191	✓	Waiting
Dir	/vulnerabilities/	200	3303	✓	Waiting

Current speed: 210 requests/sec

(Select and right click for more options)

Average speed: (T) 247, (C) 234 requests/sec

Parse Queue Size: 126

Total Requests: 5439/76429657

Current number of running threads: 10

Change

Time To Finish: 3 Days

Back Pause Stop Report

DirBuster Stopped

/Intro/

Done ?

- Information gathering is an art
- Techniques for information gathering evolve with technology
- Hackers will always try to find clever ways to gather enough information for an attack
- Never stop learning !

Thank you !

Appendix A

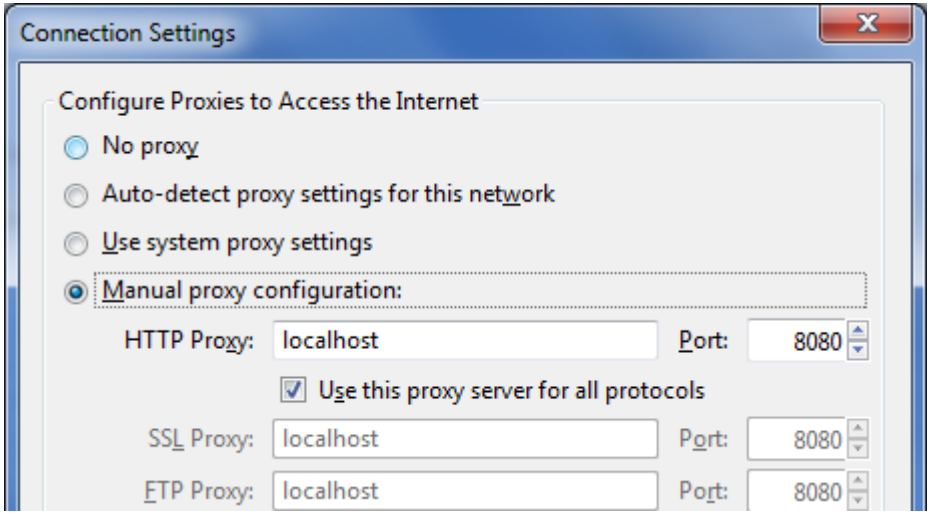
- Proxy

Paros

- Paros is a web proxy
- By default, listens (run) at localhost (127.0.0.1) at port 8080
- How to use:
  1. Configure browser to use proxy
     (HTTP Proxy: localhost) (Port: 8080)
  2. Browse target website using the browser

Browser proxy configuration

- Firefox
  - (On Windows) Tools -> Options -> Advanced -> Network -> Settings
  - (On Linux) Edit -> Preferences -> Advanced -> Network -> Settings



Paros in operation

Untitled Session - Paros

File Edit View Analyse Report Tools Help

Sites

- Sites
  - http://a323.yahoofs.com
  - http://api.bit.ly
  - http://api.connect.facebook.com
  - http://bit.ly
  - http://cdn.slidesharecdn.com
  - http://clients1.google.com
  - http://code.google.com
  - http://connect.facebook.net
  - http://control.units.it
  - http://counter.zaigadgets.com
  - http://csc.fsksm.utm.my

Request | Response | Trap

```
GET http://csc.fsksm.utm.my/ HTTP/1.1
Host: csc.fsksm.utm.my
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.15) Gecko/20
110303 Firefox/3.6.15 Paros/3.2.13
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```

Raw Vie...

URI found during crawl:

```
http://csc.fsksm.utm.my/v1/about.html
http://csc.fsksm.utm.my/v1/research.html
http://csc.fsksm.utm.my/v1/taught-course.html
```

URI found but out of crawl scope:

```
http://web.utm.my/skpost/
http://utmonline.utm.my/
```

History | Spider | Alerts | Output