Hacking Exposed 7
Network Security Secrets & Solutions

Chapter 3 Enumeration

Enumeration

- Service fingerprinting
- Vulnerability scanners
- Basic banner grabbing
- Enumerating common network services

Prelude

- Scanning vs. enumeration
  - Level of intrusiveness
  - Enumeration: active connections to systems and directed queries
    - Generic : banner grabbing
    - Platform-specific: dependent on port scans and OS detection
- Enumerated info
  - User account names
    - E.g. subsequent password-guessing attacks
  - Misconfigured shared files
  - Older software versions with known vulnerabilities
    - E.g. web-servers with remote buffer overflows
- Common services with fruitful enumerated info
  - ftp (21), telnet (23), smtp (25), etc.
- Binding from ports, services, protocols, to software

3

Service Fingerprinting

- Revision/patch level with service ports
- Manual vs. automatic
  - Stealth vs. efficiency
- Nmap version scanning
  - nmap-services (mapping ports to services) vs. nmap-service-probe (known service responses → known protocol and version)
    - -sV in nmap
    - Hidden services: e.g. OpenSSH disguised as Timbuktu service (on TCP port 1417)
- Amap version scanning
  - Second opinion to Nmap
  - Another service pattern-matching technique

4

```
[root$] nmap -sS target.com p 1417
Starting Nmap 4.68 (http://nmap.org) at 2011-10-25 19:29 PDI
Interesting ports on localhost (127.0.0.1) :
PORT            STATE   SERVICE
1417/tcp        open    timbuktu-srvl
Nmap done: 1 IP address (1 host up) scanned in 0.135 seconds"


[root$] nmap -sV target.com -p 1417
Starting Nmap 4.68 (http://nmap.org) at 2011-10-25 19:25 PDT
Interesting ports on localhost (127.0.0.1):
PORT            STATE           SERVICE         VERSION
1417/tcp        open            ssh             OpenSSH 3.7
Service detection performed. Please report any incorrect
results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.981 seconds
```

Vulnerability Scanners

- Database of known vulnerability signatures
- Free scanners (Nessus, OpenVAS - Open Vulnerability Assessment System) vs. commercial ones from McAfee, Qualys, Rapid7, nCircule, Tenable
- Nessus by Tenable
  - Exhaustive scanning
  - Custom plug-ins using Nessus Attack Scripting Language (NASL)
  - Free and open source till version 3 (proprietary closed source)
- Nessus scanning countermeasures
  - Audit yourself regularly. Effective patch and configuration management
  - IDS/IPS: alert on Nessus behaviors, slow scans down to redirect hackers to softer targets
- Nmap vs. Nessus
  - Wider (not as powerful in vulnerability scanning) vs. focused
  - Nmap Scripting Engine (NSE): uses Lua interpreted programming
  - A library of NSE scripts
    - Network discovery, version detection, backdoor detection, exploitation of vulnerabilities

Basic Banner Grabbing

- Banners in the responses to requests
- Manual
  - telnet www.example.com 80
  - Generic to work on many common applications on standard ports, e.g. HTTP (80), SMTP (25), FTP (21)

```
C:\>telnet www.example.com 80

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Tue, 15 Jul 2008 21:33:04 GMT
Content-Type: text/html
Content-Length: 87

<html><head>ctitlexErrorc/title>
</head><body>The parameter is incorrect. </body>
</html>
```

Basic Banner Grabbing

- Banners in the responses to requests
- Manual
  - telnet www.example.com 80
  - Generic to work on many common applications on standard ports, e.g. HTTP (80), SMTP (25), FTP (21)
- Automatic
  - netcat or nc
  - Redirect an input file of requests to nc
    - To grab more outputs in responses
- Vendor and version of software → known vulnerabilities

```
"[root$]nc -nvv -o banners.txt 10.219.100.1 80 < nudge.txt
(unknown) [10.219.100.1] 80 (http) open

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 16 Jul 2008 01:00:32 GMT
X-Powered-By: ASP.NET
Connection: Keep-Alive
Content-Length: 8601
Content-Type: text/html
Set-Cookie: ASPSESSIONIDCCRRABCR=BEFOAIJDCHMLJENPIPJGJACM; path=/
Cache-control: private

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
http://www.w3.org/TR/xhtml1/DTD/xhtm
11-transitional.dtd">
<HTML>
<HEAD>
<META NAME="keywords" CONTENT"= Example, Technology ">
<META NAME="description" CONTENT="Welcome to Example's Web site. "
<TITLE>Example Corporate Home Page</TITLE>
</HEAD>
</HTML>
```

Basic Banner Grabbing

- Banners in the responses to requests
- Manual
  - telnet www.example.com 80
  - Generic to work on many common applications on standard ports, e.g. HTTP (80), SMTP (25), FTP (21)
- Automatic
  - netcat or nc
  - Redirect an input file of requests to nc
    - To grab more outputs in responses
- Vendor and version of software → known vulnerabilities
- Banner grabbing countermeasures
  - Shut down unnecessary services
  - Access control lists
  - Audit yourself regularly. Try to disable the presentation of vendor and version in the banners.

Enumerating Common Network Services

- FTP, TCP 21
- Telnet, TCP 23
- SMTP, TCP 25
- DNS, TCP/UDP 53
- TFTP, TCP/UDP 69
- Finger, TCP/UDP 79
- HTTP, TCP 80

FTP Enumeration, TCP 21

- Still popular for Web Content Uploading.

- FTP passwords are sent in the clear
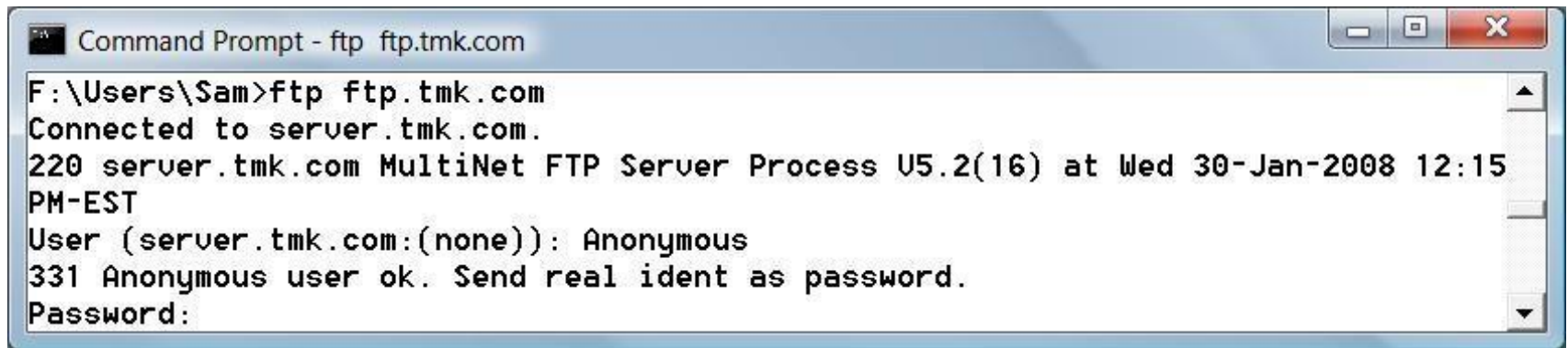
- List anonymous FTP-sites:
- e.g. ftp-sites.org

Googling for FTP Servers

- Search for
  - intitle:"Index of ftp://"
- Here's an overly informative HTTP banner

FTP Banner

- Here's the corresponding overly informative FTP banner


```
Command Prompt - ftp ftp.tmk.com

F:\Users\Sam>ftp ftp.tmk.com
Connected to server.tmk.com.
220 server.tmk.com MultiNet FTP Server Process V5.2(16) at Wed 30-Jan-2008 12:15
PM-EST
User (server.tmk.com:(none)): Anonymous
331 Anonymous user ok. Send real ident as password.
Password:
```

FTP enumeration countermeasures

- Plaintext password transmission!

- Alternatives:
    - SFTP (over SSH)
    - FTPS (over SSL)

- Public content should be served over HTTP, not FTP

- Watch out anonymous FTP, disallow unrestricted uploading

Enumerating Telnet, TCP 23

- Telnet has banners, and allows bruteforce username enumeration
  - **System enumeration**: display a system banner prior to login: host's OS and version, or vendor, explicitly or implicitly
  - **Account enumeration**: attempt login with a particular user and observe error messages
    - Valid/invalid username & invalid password $\rightarrow$ a list of valid accounts
- It sends passwords+data in cleartext

Telnet enumeration countermeasures

• Telnet should be eliminated if possible

Use SSH instead

If you must use Telnet, restrict it to proper source IP addresses

Or run it through a VPN

• Modify banner info

• Reconnect between failed login attempts

Enumerating SMTP, TCP 25

- SMTP can be enumerated with Telnet, using these commands
  - VRFY confirms names of valid users
  - EXPN reveals the actual delivery addresses of aliases and mailing lists

- automatic tool vrfy.pl specify SMTP server and username to test

SMTP Enumeration Countermeasures

- Disable the EXPN and VRFY commands, or restrict them to authenticated users

- Sendmail and Exchange both allow that in modern versions

```
[root$] telnet 192.168.202.34 25
Trying 192.168.202.34...
Connected to 192.168.202.34.
Escape character is '^]'.
220 mail.bigcorp.com ESMTP Sendmail 8.8.7/8.8.7; 11 Apr 2002
vrfy root
250 root <root@bigcorp.com>
expn adm
250 adm <adm@bigcorp.com>
quit
221 mail.bigcorp.com closing connection
```

DNS Zone Transfers, TCP 53

- Zone transfers dump the entire contents of a given domain's zone files

- Restricted to authorized machines on most DNS servers

```
F:\Users\Sam>nslookup
Default Server:  buffalo.setup
Address:    192.168.11.1:53

> ls -d certifiedhacker.com
[buffalo.setup]
*** Can't list domain certifiedhacker.com: Unspecified error
The DNS server refused to transfer the zone certifiedhacker.com to your computer
. If this
is incorrect, check the zone transfer security settings for certifiedhacker.com
on the DNS
server at IP address 192.168.11.1.
```

DNS on TCP/UDP 53

– Normally on UDP 53; TCP 53 for zone transfer

– DNS enumeration by zone transfer on misconfigured DNS servers: dump entire zone files (A and HINFO records)

- nslookup, ls –d <domainname>; or dig

– BIND (Berkley Internet Name Domain server) enumeration: dig to get version.bind

`~ $ dig @10.219.100.1 version.bind txt chaos`

DNS Cache Snooping

- +norecurse, examines only the local DNS data (note ANSWER: 0)

```
sam@Sam-Bownes-MacBook-Air:~$ dig @192.168.11.1 kittenwar.com +norecurse

; <<>> DiG 9.7.3-P3 <<>> @192.168.11.1 kittenwar.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 13152
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kittenwar.com.                     IN      A

;; Query time: 954 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Wed Sep  5 14:07:11 2012
;; MSG SIZE  rcvd: 31
```

Recursive DNS

```
sam@Sam-Bownes-MacBook-Air:~$ dig @192.168.11.1 kittenwar.com

; <<>> DiG 9.7.3-P3 <<>> @192.168.11.1 kittenwar.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60160
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kittenwar.com.                  IN      A

;; ANSWER SECTION:
kittenwar.com.          2062    IN      A       205.196.209.62

;; Query time: 111 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Wed Sep  5 14:07:17 2012
;; MSG SIZE  rcvd: 47
```

Now It's in the Cache

```
sam@Sam-Bownes-MacBook-Air:~$ dig @192.168.11.1 kittenwar.com +norecurse

; <<>> DiG 9.7.3-P3 <<>> @192.168.11.1 kittenwar.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31042
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kittenwar.com.                    IN      A

;; ANSWER SECTION:
kittenwar.com.            2059    IN      A       205.196.209.62

;; Query time: 12 msec
;; SERVER: 192.168.11.1#53(192.168.11.1)
;; WHEN: Wed Sep  5 14:07:21 2012
;; MSG SIZE  rcvd: 47
```

DNS Enumeration Tools

- dnsenum
  - Google scraping for additional subdomains
  - Brute forcing subdomains
  - List domain network ranges
  - Perform WHOIS on the ranges identified
  - Information Correlation

- Web resources

C | 🔒 Sicuro | https://centralops.net/co/

CentralOps.net *Advanced online Internet utilities*

Free online network tools

user: ar
balance: 4
lo

Tools

Domain Dossier

Investigate domains and IP addresses. Get registrant information, DNS records, and more—all in one report.

enter a domain or IP address

[   ] [go]

or learn about yourself

Domain Check

See if a domain is available for registration.

Email Dossier

Validate and troubleshoot email addresses.

Browser Mirror

See what your browser reveals about you.

Ping

See if a host is reachable.

Traceroute

Trace the network path from this server to another.

NsLookup

Look up various domain resource records with this version of the classic NsLookup utility.

How this

The tools at
interactive
on the left ar

As an anony
every 24 ho
cost in servi
balance runs
the 24-hour
for 99% of o
automated
available.

Fierce.pl tool

```
root@bt:/pentest/enumeration/dns/fierce# perl fierce.pl -dns samsclass.info -threads 5 -file
sam-fierce
Now logging to sam-fierce
DNS Servers for samsclass.info:
        coco.ns.cloudflare.com
        tom.ns.cloudflare.com

Trying zone transfer first...
        Testing coco.ns.cloudflare.com
                Request timed out or transfer not allowed.
        Testing tom.ns.cloudflare.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 1895 test(s)...
108.162.198.183 games.samsclass.info
108.162.198.83  games.samsclass.info
108.162.198.183 www.samsclass.info
108.162.198.83  www.samsclass.info

Subnets found (may want to probe here using nmap or unicornscan):
        108.162.198.0-255 : 4 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 4 entries.
```

DNS Enumeration Countermeasures

- Use separate internal and external DNS servers (do not expose internal targets)

- Block or restrict DNS zone transfers

- Restrict DNS queries to limit cache snooping

Enumerating TFTP, TCP/UDP 69

```
[root$]tftp 192.168.202.34
 tftp> connect 192.168.202.34
 tftp> get /etc/passwd /tmp/passwd.cracklater
 tftp> quit
```

- TFTP is inherently insecure
  - Runs in cleartext
  - Have to know the file name. No authentication at all
  - Anyone can grab any file (even /etc/passwd in the worst cases)
  - Used in routers and VoIP Telephones to update firmware. Look for config files

TFTP Enumeration Countermeasures

- Wrap it to restrict access
  - Using a tool such as TCP Wrappers
  - TCP Wrappers is like a software firewall, only allowing certain clients to access a service
- Limit access to the /tftpboot directory
- Make sure it's blocked at the border firewall

Finger, TCP/UDP 79

```
$ finger
Login          Name              TTY Idle      When
sbowne     Sam Bowne             *0         Wed 10:37
zzeng01    zelong zeng           *1      51 Wed 09:41
root               ???           *tf  019: Sun 16:27
amarko01   adam markosian        *2         Wed 10:10
jcompt01   joshua francis compt  *3         Wed 10:41
sfreit01   stephen earl freitag  *4    2:15 Wed 08:25
cmetzler   Charlie Metzler       *5       2 Wed 10:29
jcater01   joseph p catera       *6         Wed 10:41
$ finger @sol
[sol.ccsf.cc.ca.us]
No one logged on
```

- Shows users on local or remote systems, if enabled
  - Useful for social engineering
- Countermeasure: block remote access to finger

Enumerating HTTP, TCP 80

- Grab banners with telnet or netcat (nc)
- For SSL-enabled website. Redirect to SSL proxy (sslproxy) or use SSL client (openssl)

- Crawl Web sites with Sam Spade utility
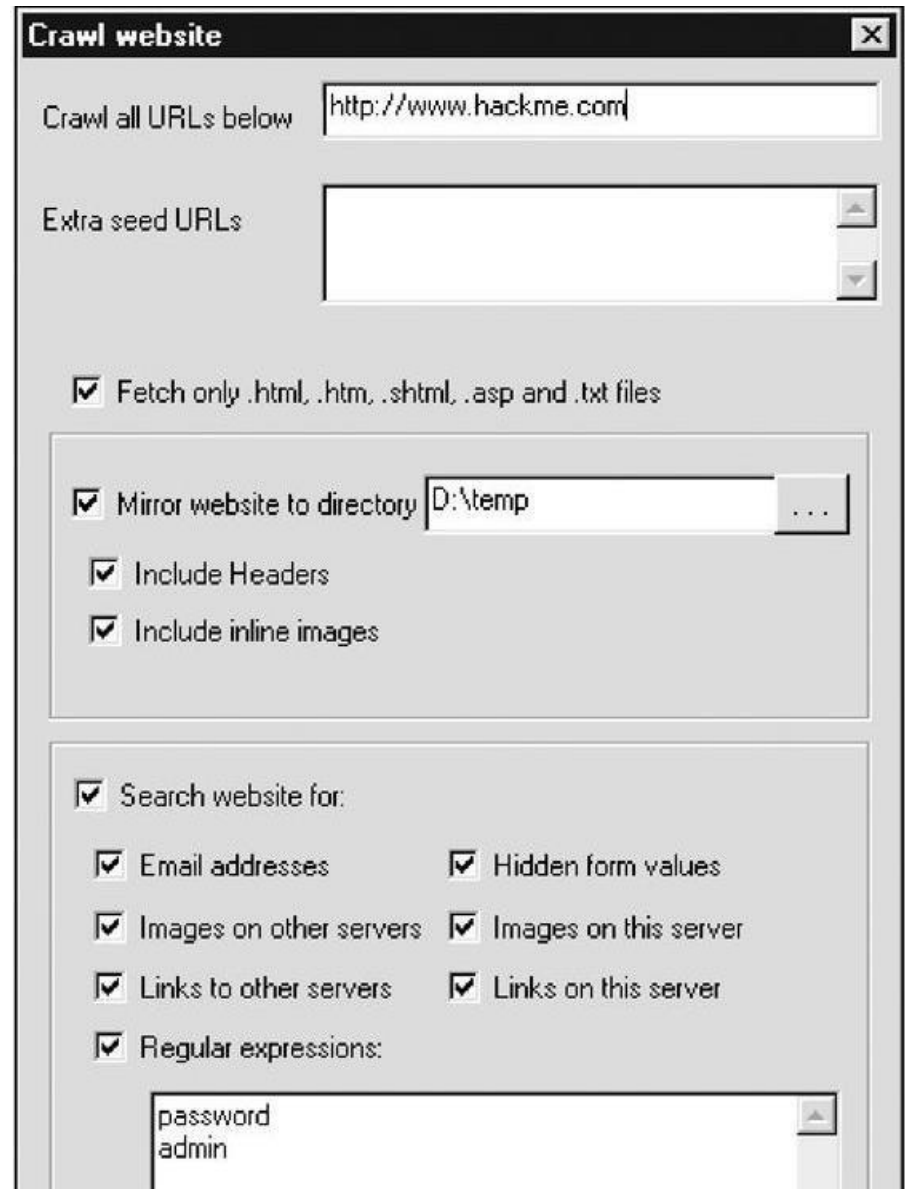
Sam Spade for Windows is free

SANS

SANS Institute
Information Security Reading Room

Using Sam Spade

Terry Pasley

Automatic tool Grendel-Scan

- Crawls sites and reports on vulnerabilities
- Look for comments, **robots.txt file**, directories, etc.

- Very slow

Status | Transactions | Manual Request | Proxy settings | Interception settings | Fuzzer

Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomssydvp.cgi
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomssydvp.cgi
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Nikto cgi dir search is requesting GET http://games.samsclass.info:80/cgi-sys/
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomtoxsdh.wsdl
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomtoxsdh.wsdl
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Module 11 is requesting GET http://games.samsclass.info:80/IWSCCJGW.exe
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randommmpjqs.nsf
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randommmpjqs.nsf
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Nikto cgi dir search is requesting GET http://games.samsclass.info:80/scripts/
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomzjrzab.axd
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomzjrzab.axd
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Module 11 is requesting GET http://games.samsclass.info:80/IWSCCJGW.hta
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomctxygi.aspx
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomctxygi.aspx
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Nikto cgi dir search is requesting GET http://games.samsclass.info:80/cgi-home/
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomveyesn.sh
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomveyesn.sh
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Module 11 is requesting GET http://games.samsclass.info:80/IWSCCJGW.htm
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomytxztw.jsp
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomytxztw.jsp
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Nikto cgi dir search is requesting GET http://games.samsclass.info:80/cgi-local/
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomlxsyga.pl
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomlxsyga.pl
Not sure why this happened at HttpTransaction.execute: org.apache.http.ProtocolException: The server failed to respond with a valid HTTP resp
Module 11 is requesting GET http://games.samsclass.info:80/IWSCCJGW.html
Testing for logical 404 responses: http://games.samsclass.info:80/cdn-cgi/cache-err/randomecfhux.dll
Response code overrides is requesting GET http://games.samsclass.info:80/cdn-cgi/cache-err/randomecfhux.dll

Queue Sizes

Tester: `3`   Categorizer: `0`   Requester: `0`

Help | Terminate Scan | Pause Scan

HTTP Enumeration Countermeasures

- Change the banner on your web servers (may fool automated malware)

    - Download MS URLScan for IIS v 4 and later
        - Use filters and allows custom banners

    - Microsoft Internet Information Services has many exploits ready for use.

Microsoft RPC Endpoint Mapper (MSRPC), TCP 135

- Remote Procedure Call (RPC) endpoint mapper (or portmapper) service on TCP 135
- Querying this service can yield information about applications and services available on the target machine

epdump

- From Microsoft's Windows Resource Kit
- Shows services bound to IP addresses
- It takes some research to interpret the results

Microsoft: epdump

Example 9-1. Using epdump to enumerate RPC interfaces

```
C:\> epdump 192.168.189.1

binding is 'ncacn_ip_tcp:192.168.189.1'

int 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc v1.0

  binding 00000000-000000000000@ncadg_ip_udp:192.168.0.1[1028]

  annot 'Messenger Service'

int 1ff70682-0a51-30e8-076d-740be8cee98b v1.0

  binding 00000000-000000000000@ncalrpc:[LRPC00000284.00000001]

  annot ''
```

Linux: rpcdump.py

- In Backtrack, similar results

Example 9-2. Using rpcdump to enumerate RPC interfaces

```
D:\rpctools> rpcdump 192.168.189.1

IfId: 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc version 1.0

Annotation: Messenger Service

UUID: 00000000-0000-0000-0000-000000000000

Binding: ncadg_ip_udp:192.168.189.1[1028]


IfId: 1ff70682-0a51-30e8-076d-740be8cee98b version 1.0

Annotation:

UUID: 00000000-0000-0000-0000-000000000000

Binding: ncalrpc:[LRPC00000290.00000001]
```

MSRPC Enumeration Countermeasures

- Block port 135 at the firewall, if you can
  - But some Microsoft Exchange Server configurations require access to the endpoint mapper by remote user
  - You can avoid that by using Virtual Private Networks to internal network, or
  - Outlook Web Access (OWA) which works over HTTPS
  - Exchange 2003 and later implements RPC over HTTP

NetBIOS Name Service, **UDP 137**

- NetBIOS Name Service (NBNS) is Microsoft's name service, DNS-like

- What is Name Resolution?
  - Suppose you issue a command that refers to a computer by name, such as PING

```
F:\Users\Sam>PING SAMP4

Pinging SAMP4 [192.168.11.3] with 32 bytes of data:

Reply from 192.168.11.3: bytes=32 time=1ms TTL=128
Reply from 192.168.11.3: bytes=32 time<1ms TTL=128
```

Name Resolution

- Windows needs to change a computer name to an IP address to send data packets

- Windows uses two naming systems:

  – DNS (the preferred method)

  – NetBIOS Name Resolution (still used by all versions of Windows)

    – Available only on IPv4

Standard Name Resolution Methods

Resolution Method	Description
Local host name	The configured host name for the computer as displayed in the output of the Hostname tool. This name is compared to the destination host name.
Hosts file	A local text file in the same format as the 4.3 Berkeley Software Distribution (BSD) UNIX \etc\hosts file. This file maps host names to IP addresses. For TCP/IP for Windows XP and Windows Server 2003, the contents of the Hosts file are loaded into the DNS client resolver cache. For more information, see "The DNS Client Resolver Cache" in this chapter.
DNS server	A server that maintains a database of IP address-to-host name mappings and has the ability to query other DNS servers for mappings that it does not contain.

Additional Name Resolution Methods

Resolution Method	Description
DNS client resolver cache	A random access memory (RAM)-based table of the entries listed in the local Hosts file and the names that were attempted for resolution by using a DNS server.
NetBIOS name cache	A RAM-based table of recently resolved NetBIOS names and their associated IPv4 addresses.
NetBIOS name server (NBNS)	A server that resolves NetBIOS names to IPv4 addresses, as specified by Requests for Comments (RFCs) 1001 and 1002. The Microsoft implementation of an NBNS is a Windows Internet Name Service (WINS) server.
Local broadcast	Up to three NetBIOS Name Query Request messages are broadcast on the local subnet to resolve the IPv4 address of a specified NetBIOS name.
Lmhosts file	A local text file that maps NetBIOS names to IPv4 addresses for NetBIOS processes running on computers located on remote subnets.

NET VIEW

- NET VIEW can list the domains, or the computers in each domain

```
F:\Users\Sam>net view /domain
Domain

-------------------------------------------------
WORKGROUP
The command completed successfully.


F:\Users\Sam>net view /domain:workgroup
Server Name            Remark

-------------------------------------------------
\\S214-00
\\SAM2G
\\SAMP4
The command completed successfully.
```

NBNS over TCP/IP

- Normally NBNS only works on the local network segment
- It is possible to route NBNS over TCP/IP, allowing enumeration from a remote system

Other Tools to Enumerate NBNS

- NLTEST and NETDOM can find domain controllers
- NETVIEWX finds specific services
- NBTSTAT collects information from a single system
- NBTSCAN scans a whole range of addresses, and dumps the whole NetBIOS name table
- NMBscan in **Kali Linux**

NBTSCAN

```
F:\Users\Sam\Desktop>nbtscan-1.0.33.exe -f 192.168.11.0/24
192.168.11.2        WORKGROUP\SAM2G                        SHARING
  SAM2G             <00> UNIQUE Workstation Service
  WORKGROUP         <00> GROUP  Domain Name
  SAM2G             <20> UNIQUE File Server Service
  WORKGROUP         <1e> GROUP  Browser Service Elections
  00:30:48:82:11:bc  ETHER   Sam2G.astound.net

192.168.11.3        WORKGROUP\SAMP4                        SHARING
  SAMP4             <00> UNIQUE Workstation Service
  WORKGROUP         <00> GROUP  Domain Name
  SAMP4             <20> UNIQUE File Server Service
  WORKGROUP         <1e> GROUP  Browser Service Elections
  WORKGROUP         <1d> UNIQUE Master Browser
  .._MSBROWSE__.<01> GROUP  Master Browser
  00:10:b5:0e:5c:8a  ETHER   SAMP4

192.168.11.28       WORKGROUP\S214-00                      SHARING
  S214-00           <00> UNIQUE Workstation Service
  S214-00           <20> UNIQUE File Server Service
  WORKGROUP         <00> GROUP  Domain Name
  WORKGROUP         <1e> GROUP  Browser Service Elections
  00:0c:29:28:f6:71  ETHER   S214-00

*timeout (normal end of scan)
```

Stopping NetBIOS Name Services Enumeration

- All the preceding techniques operate over the NetBIOS Naming Service, UDP 137

- Block UDP 137 at the firewall, or restrict it to only certain hosts

- To prevent user data from appearing in NetBIOS name table dumps, disable the Alerter and Messenger services on individual hosts

- Blocking UDP 137 will disable NBNS name authentication, and stop some applications

NetBIOS Session, TCP 139

- These are the notorious Null Sessions
- The Windows Server Message Block (SMB) protocol hands out a wealth of information freely
- Null Sessions are turned off by default in Win XP and later versions, but open in Win 2000 and NT
  - They are NOT available in Win 95, 98, or Me

Null Session Against Win 2000

```
F:\Users\Sam\Desktop>net view \\192.168.11.29
System error 5 has occurred.

Access is denied.


F:\Users\Sam\Desktop>net use \\192.168.11.29\IPC$ "" /user:""
The command completed successfully.


F:\Users\Sam\Desktop>net view \\192.168.11.29
Shared resources at \\192.168.11.29



Share name      Type   Used as   Comment

-------------------------------------------------------------------
My Documents    Disk
The command completed successfully.
```

Information Available

- Null sessions on Win 2000 and NT provide information about:
  - Shares
  - User accounts
  - Password policies

DumpSec – free tool

- Enumerate file permission, services, ecc.
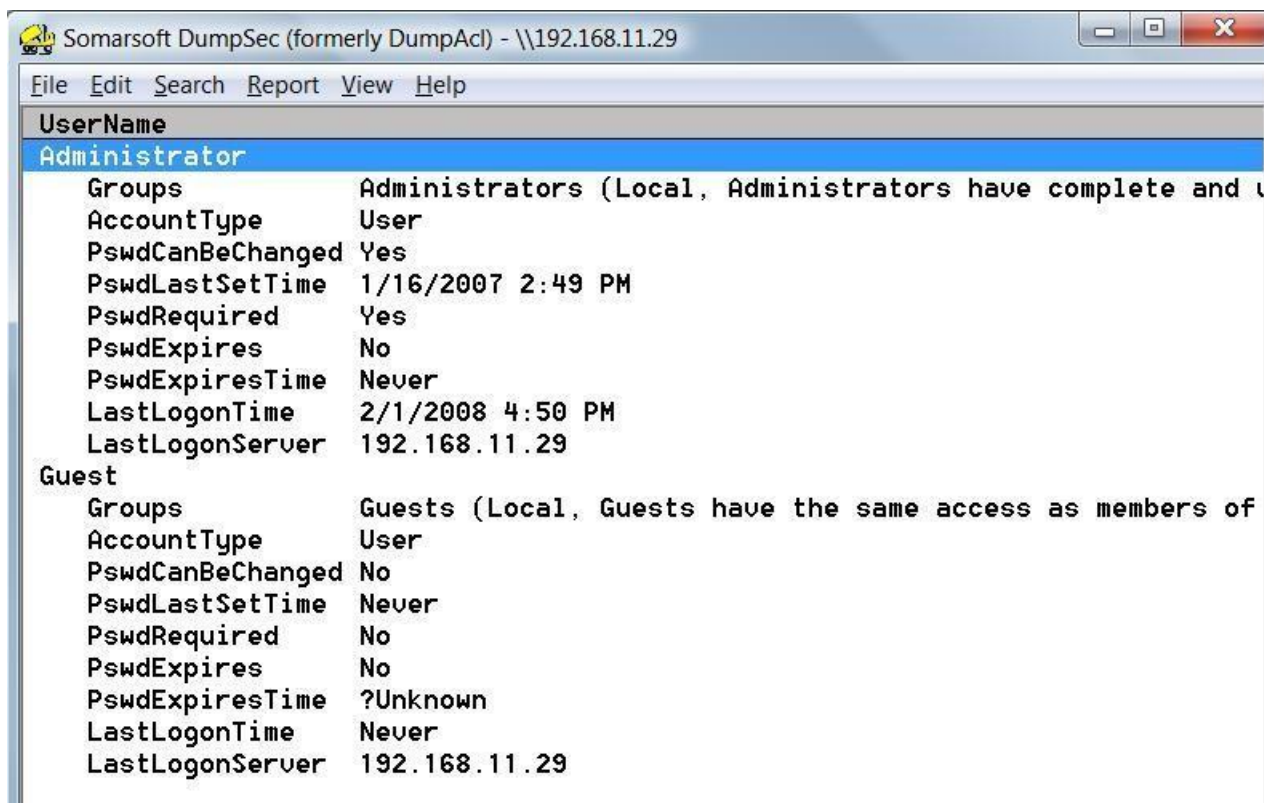
Registry Enumeration

- The Registry can be viewed remotely with reg (MS built-in) or DumpSec

- Requires Administrator privileges by default on Windows servers
  - You can NOT do it with null sessions

- Gary McKinnon used remote registry access to hack into the Pentagon

https://www.youtube.com/watch?v=Stz7ZMQ3p7I&ab_channel=ZeitzumAufwachen

Security Identifier (SID)

- **SID** is a unique, immutable identifier of security principal: a user, user group,…
- S-1-5-21-1180699209-877415012-3182924384-1004
- Relative Identifier (RID)

Username	RID
Administrator	500
Guest	501
Account created	1000, 1001, 1002,…

- Changing the last 3 numbers of another account's SID to 500 for Admin.
- Or script for user enumeration

User Enum - user2sid/sid2user

- These utilities can get user account names and **SID** remotely, even if blocking anonymous connections (the registry key RestrictAnonymous is set to 1)
- They can find the Administrator's account name, even if it's renamed
- Works against NT family OS, but not Win XP SP2

```
C:\>user2sid \\192.168.202.33 "domain users"

S-1-5-21-8915387-1645822062-1819828000-513
Number of subauthorities is 5
Domain is ACME
Length of SID in memory is 28 bytes
Type of SID is SidTypeGroup




C:\>sid2user \\192.168.2.33 5 21 8915387 1645822062 18198280005 500

Name is godzilla
Domain is ACME
Type of SID is SidIypeUser
```

All-in-One Null Session Enumeration Tools

- ## Winfingerprint

  - Through Active Directory and WMI

- ## Winfo

- ## NBTEnum 3.3

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\SamLimited\Desktop>wir

Winfo 2.0 - copyright (c) 1999-2003, Arne Uidst:
         - http://www.ntsecurity.nu/toolbox/wir

Trying to establish null session...

Null session established.

SYSTEM INFORMATION:

 - OS version: 5.0

DOMAIN INFORMATION:

 - Primary domain (legacy): WORKGROUP
 - Account domain: S214-17-SAM2
 - Primary domain: WORKGROUP
 - DNS name for primary domain:
 - Forest DNS name for primary domain:

PASSWORD POLICY:

 - Time between end of logon time and forced log
 - Maximum password age: 42 days
 - Minimum password age: 0 days
 - Password history length: 0 passwords
 - Minimum password length: 0 characters

LOCOUT POLICY:

 - Lockout duration: 30 minutes
 - Reset lockout counter after 30 minutes
 - Lockout threshold: 0

SESSIONS:

 - Computer: 192.168.2.222
 - User:

LOGGED IN USERS:

 * Administrator
```

SMB Null Session Countermeasures

- Block TCP 139 and 445 at the network perimeter
- Set the **RestrictAnonymous** registry key to 1 (or 2 on Win 2000 and later)

  Use regedt32

  - HKLM\SYSTEM\CurrentControlSet\Control\LSA
  - Can be bypassed by querying NetUserGetInfo API call at Level 3
    - NBTEnum and Userinfo bypass it
- Anonymous Access settings do not apply to remote Registry access. Ensure the Registry is Locked Down
  - http://support.microsoft.com/kb/153183
- Audit yourself with dumpsec

SNMP, UDP 161

- Simple Network Management Protocol (Security Not My Problem). SNMP is intended for network management and monitoring It provides inside information on net devices, software and systems.

  – Administrators use SNMP to remotely manage routers and other network devices

Community Strings

- SNMP has a minimal security system called *SNMP Community Strings*
- Community strings act like passwords
- There are three kinds of SNMP Community strings: *Read-Only*, *Read-Write*, and *Trap* (Trap is rarely used)
  - But the community strings are often left at obvious defaults like "public" and "private"
  - Attackers often use wireshark to obtain the communisty string by packet inspection

Management Information Bases (MIBs)

- The MIB contains a SNMP device's data in a tree-structured form, like the Windows Registry

- Vendors add data to the MIB

- Microsoft stores Windows user account names in the MIB

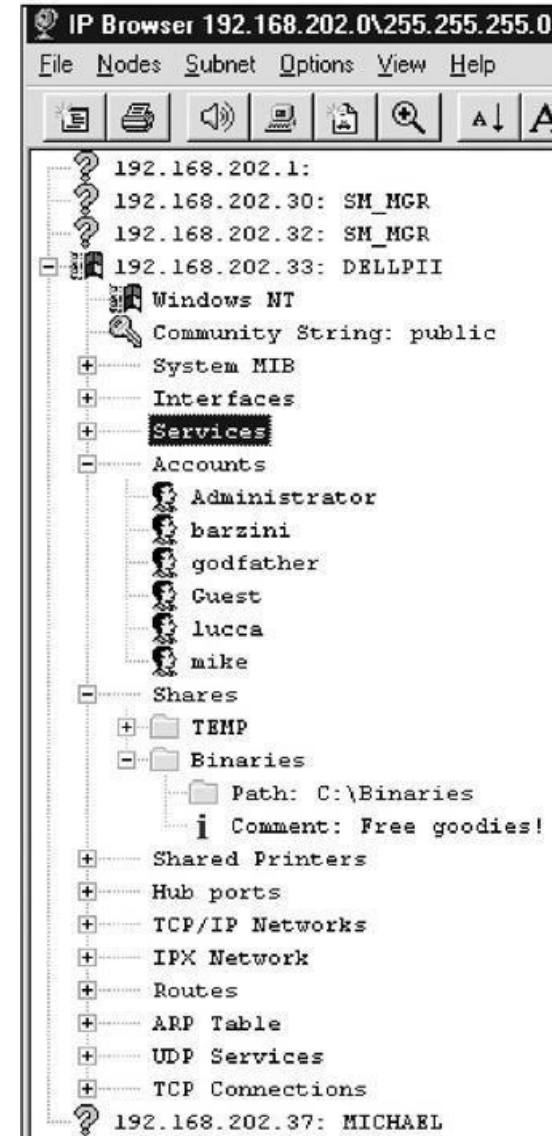

FIGURE 1:
The basic idea of the MIB tree
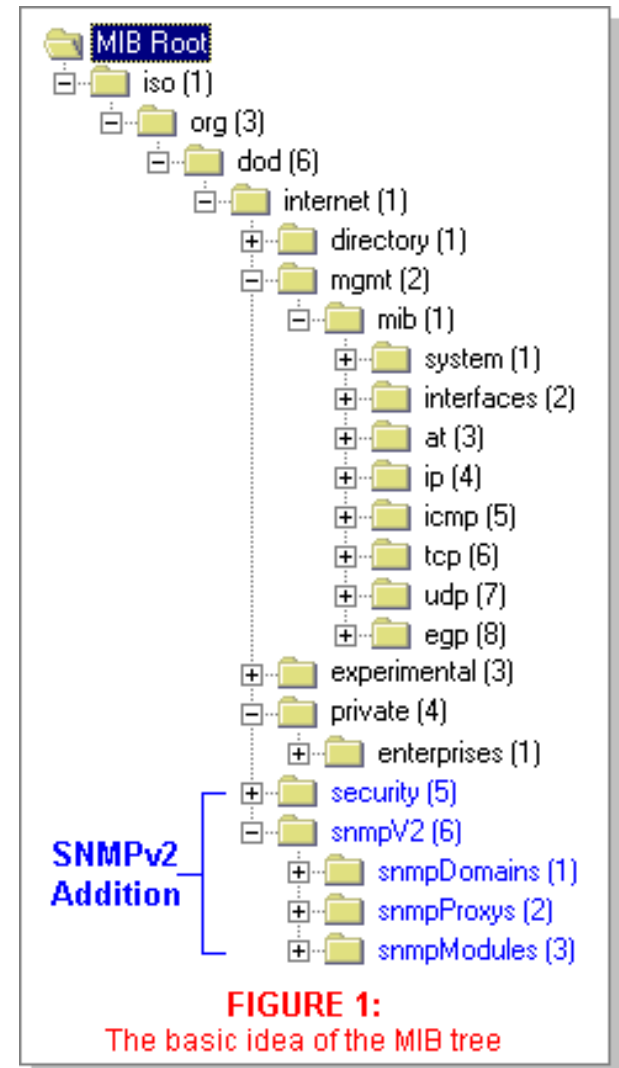
Data Available Via SNMP Enumeration

- Running services
- Share names
- Share paths
- Comments on shares
- Usernames
- Domain name

SNMP Enumeration Tools

- **snmputil** from the Windows NT Resource Kit

- **snmpget** or **snmpwalk** for Linux (netsnmp suite)

- **IP Network Browser** graphical tool by Solarwinds

```
C: >snmputil walk 192.168.202.33 public .1.3.6.1.4.1.77.1.2.25

Variable=.iso.org.dod.internet.private.enterprises.lanmanager.
lanmgr-2.server.svUserTable.svUserEntry.
svUserName. 5. 71.117.101.115.116
Value    = OCTET STRING - Guest
Variable =.iso.org.dod.internet.private.enterprises.lanmanager.
lanmgr-2.server. svUserTable.svUserEntry.
svUserName. 13. 65.100.109.105.110.105.115.116.114.97.116.111.114
Value     = OCTET STRING - Administrator
End of MIB subtree.
```

- **.1.3.6.1.4.1.77.1.2.25 object identifier (OUI)**

SNMP MIB (Append this to .iso.org.dod.internet.private .enterprises.lanmanager.lanmgr2)	Enumerated Information
.server.svSvcTable.svSvcEntry.svSvcName	Running services
.server.svShareTable.svShareEntry.svShareName	Share names
.server.svShareTable.svShareEntry.svSharePath	Share paths
.server.svShareTable.svShareEntry.svShareComment	Comments on shares
.server.svUserTable.svUserEntry.svUserName	Usernames
.domain.domPrimaryDomain	Domain name

Worse than Enumeration

- Attackers who guess the SNMP community string may be able to remotely control your network devices

- E.g. write community string = private
  - That can be used for DoS attacks, or …
  - In CISCO networks you can copy their configuration to a TFTP server (copy-router-config.pl tool).
    - Decode passwords

SNMP Enumeration Countermeasures

- Remove or disable unneeded SNMP agents
- Change the community strings to non-default values
- Block access to TCP and UDP ports 161 (SNMP GET/SET) at the net perimeter devices
- Restrict access to SNMP agents to the appropriate management console IP address

SNMP Enumeration Countermeasures

- Use SNMP V3—much more secure than V1 or 2

  – Provides enhanced encryption and authentication mechanisms

- Adjust Win NT registry keys to make SNMP less dangerous

BGP, TCP 179

- Border Gateway Protocol (BGP) is the de facto routing protocol among Autonomous Systems
- Organizations with more uplinks use BGP
- Use AS-Number to guide packets to their destinations.
- ASN: unique IP-like for a large organization
- BGP can be used to enumerate all the networks of a particular corporation (AS-Number)
  - That may give more targets to attack
- No countermeasure, BGP cannot be blocked

Windows Active Directory LDAP TCP/UDP 389 and 3268

- **Active Directory** contains all user accounts, groups, and other information on Windows domain controllers

- If the domain is made compatible with earlier versions of Windows, such as Win NT4 Server, any domain member can enumerate Active Directory

- MS tool ldp.exe

Active Directory Enumeration Countermeasures

- Filter access to ports 389 and 3268 at the net perimeter devices

- Legacy-compatible mode vs. Native Win 2000

- If possible use "Native" domains - do NOT allow Win NT4 Domain Controllers

Enumerating Common Network Services

- Other services
  - Microsoft RPC endpoint mapper on TCP 135: epdump, rpcdump.py
  - NetBIOS name service on UDP 137: net view, nltest, nbtstat, nbtscan, nmbscan
  - NetBIOS session on TCP 139/445: net use, net view
  - SNMP on UDP 161: snmputil, snmpget, snmpwalk
  - BGP on TCP 179: telnet
  - LDAP on TCP/UDP 389/3268: Active Directory Administration Tool
  - UNIX RPC on TCP/UDP 111/32771: rpcinfo
  - rwho and rusers
  - SQL resolution service on UDP 1434: SQLPing
  - Oracle TNS (Transparent Network Substrate) on TCP 1521/2483
  - NFS on TCP/UDP 2049
  - IPsec/IKE on UDP 500

Summary

- Enumeration → seal the lips of your software
- Software → reduce the info leaks
  - Fundamental OS architectures
    - Lock down by disabling or restricting access
  - SNMP
    - Default community string "public" give out data to unauthorized users
  - Leaky OS services
    - Services such as finger and rpcbind give too much info
  - Custom applications
    - Web-application → more info given out
  - Firewalls
    - Patching holes in software vs. screening by firewall
- AUDIT yourself: nmap, Nessus,…

Homework #2 Ch2 & Ch3 (total: 180)

(format: problem, solution with explanation, screen dumps)

1. (50 points) Select a target domain and use Nmap for the following tasks.
   a) host discovery on the selected domain,
   b) port scanning on a selected host,
   c) active stack fingerprinting on the selected host,
   d) version scanning on a selected port,
   e) vulnerability scanning on the selected port.
2. (20 points) List and compare nmap-os-fingerprints used in Nmap and osprints.conf used in Siphon. Discuss how and why they differ.
3. (20 points) List and compare nmap-services and nmap-service-probe. Discuss how and why they differ.
4. (10 points) On a UNIX/Linux host, list /etc/inetd.conf. Discuss what services are being offered.
5. (30 points) Select a target domain, run metaexploit with Nmap scans and import Nmap results into the database. Show found hosts and available ports.
6. (30 points) Select a website to do banner grabbing with telnet, netcat, and grendel-scan, respectively. Show and compare their results.
7. (20 points) Select a target domain to do automatic DNS enumeration by dnsenum to find subdomains, servers, and their IP addresses.