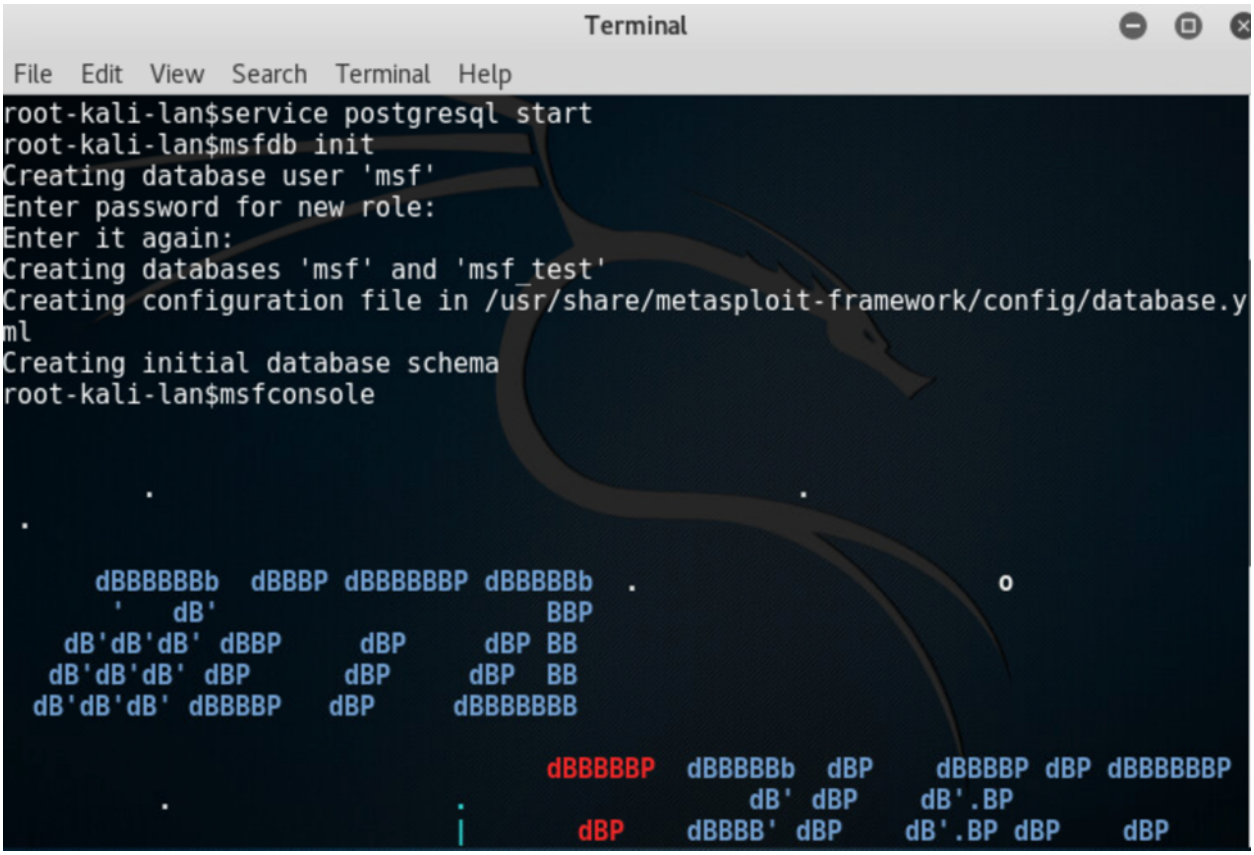
Pen-testing & Network Exploitation: LAN Exploitation Capstone V2

Homework Assignment 19

Part 1: Lan Segment



- launch msf console and Metasploit database

```
root-kali-lan$ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.50  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe01:8000  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:01:80:00  txqueuelen 1000  (Ethernet)
        RX packets 3563  bytes 316450 (309.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 578  bytes 36152 (35.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.2  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::215:5dff:fe01:8001  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:01:80:01  txqueuelen 1000  (Ethernet)
        RX packets 5402  bytes 1316595 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1326  bytes 166303 (162.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 185689  bytes 30923841 (29.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 185689  bytes 30923841 (29.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

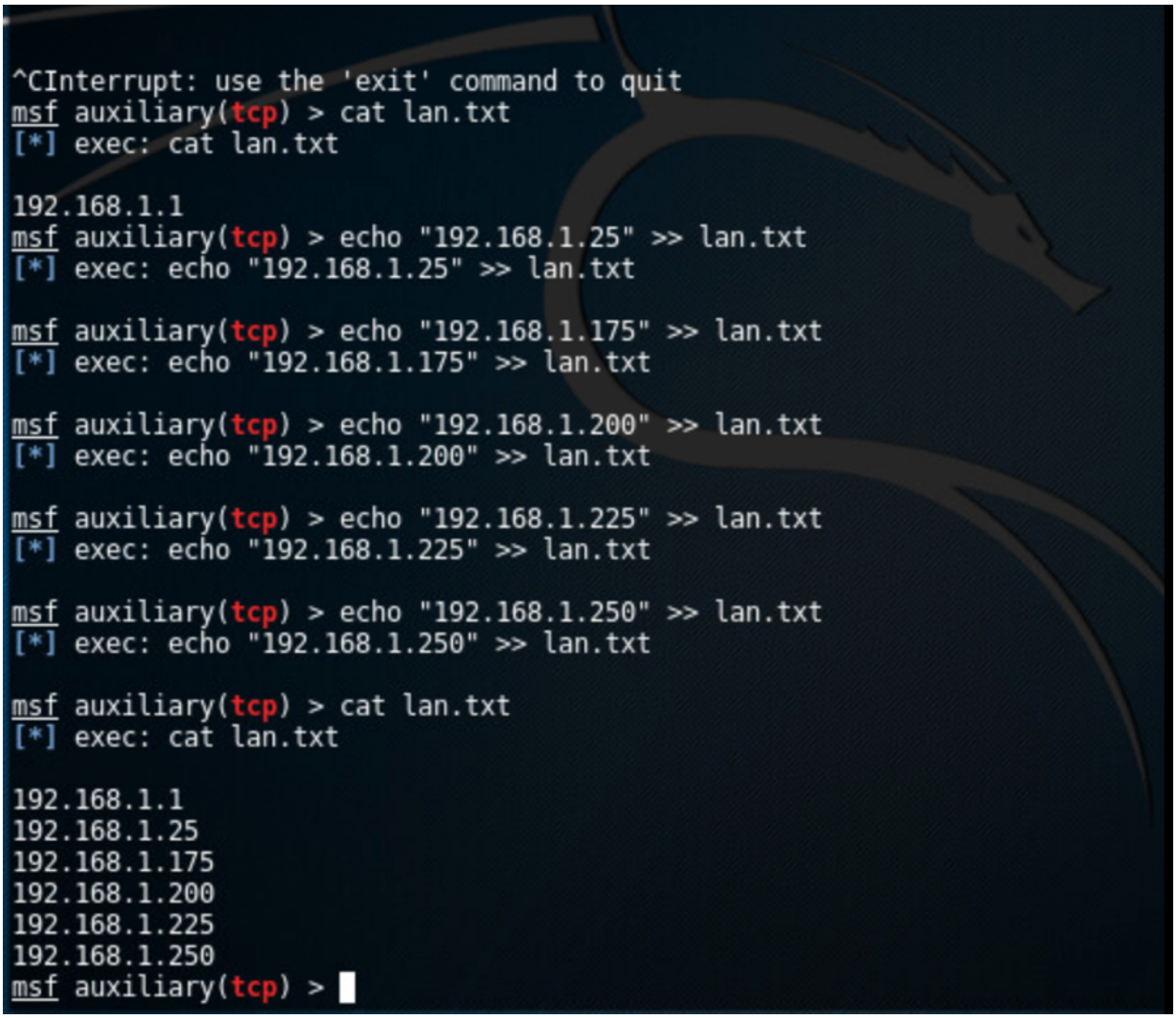
- On a separate terminal use ifconfig to discover your systems IP address
- Here we see 192.160.1.50 is the ip

```
[*] Nmap: MAC Address: 00:0C:29:5E:E6:65 (VMware)
[*] Nmap: Nmap scan report for kali-lan (192.168.1.50)
[*] Nmap: Host is up (0.0000060s latency).
[*] Nmap: All 1000 scanned ports on kali-lan (192.168.1.50) are closed
[*] Nmap: Nmap done: 256 IP addresses (7 hosts up) scanned in 16.27 seconds
msf > hosts

Hosts
=====

address        mac                name                os_name  os_flavor  os_sp  purpo
se  info  comments
-------        ---                ----                -------  ---------  -----  -----
--  ----  --------
192.168.1.1    00:0c:29:ea:80:9f  pfSense.localdomain  Unknown                    devic
e
192.168.1.25   00:0c:29:30:01:c7                      Unknown                    devic
e
192.168.1.175  00:0c:29:4f:a3:49                      Unknown                    devic
e
192.168.1.200  00:15:5d:01:80:03                      Unknown                    devic
e
192.168.1.225  00:0c:29:49:e7:9e                      Unknown                    devic
e
192.168.1.250  00:0C:29:5E:E6:65                      Unknown                    devic
e

msf >
```

```
-------         ---                   ----                  -------  ---------  -----  -----
--  ----  --------
192.168.1.1    00:0c:29:ea:80:9f  pfSense.localdomain  Unknown                    devic
e
192.168.1.25   00:0c:29:30:01:c7                       Unknown                    devic
e
192.168.1.175  00:0c:29:4f:a3:49                       Unknown                    devic
e
192.168.1.200  00:15:5d:01:80:03                       Unknown                    devic
e
192.168.1.225  00:0c:29:49:e7:9e                       Unknown                    devic
e
192.168.1.250  00:0C:29:5E:E6:65                       Unknown                    devic
e

msf > ls
[*] exec: ls

Desktop
Documents
Downloads
lan.txt
Music
Pictures
Public
Templates
Videos
msf >
```

- After creating an “internal” workspace; navigate to that workspace and perform nmap scan and host discovery
- Create new file lan.txt to store host information

```
msf > hosts -o lan.txt
[*] Wrote hosts to lan.txt
msf > cat lan.txt
[*] exec: cat lan.txt

address,mac,name,os_name,os_flavor,os_sp,purpose,info,comments
"192.168.1.1","00:0c:29:ea:80:9f","pfSense.localdomain","Unknown","","","device","",""
"192.168.1.25","00:0c:29:30:01:c7","","Unknown","","","device","",""
"192.168.1.175","00:0c:29:4f:a3:49","","Unknown","","","device","",""
"192.168.1.200","00:15:5d:01:80:03","","Unknown","","","device","",""
"192.168.1.225","00:0c:29:49:e7:9e","","Unknown","","","device","",""
"192.168.1.250","00:0C:29:5E:E6:65","","Unknown","","","device","",""
msf > hosts -c address

Hosts
=====

address
-------
192.168.1.1
192.168.1.25
192.168.1.175
192.168.1.200
192.168.1.225
192.168.1.250

msf >
```

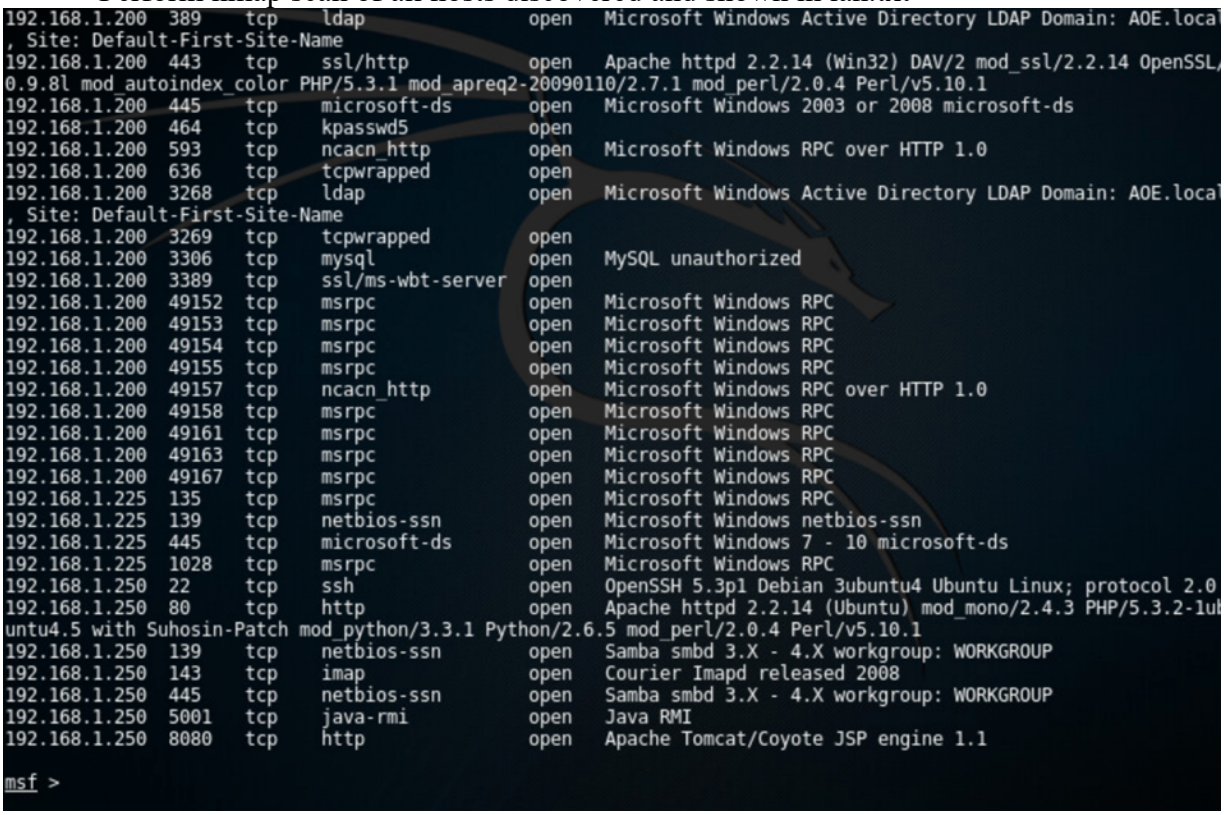


- This had to be done manually with the echo command; but an alternative would be using hosts -o lan.txt

```
[*] Nmap: Device type: general purpose|specialized|phone
[*] Nmap: Running: Microsoft Windows 2008|8.1|7|Phone|Vista
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_
7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsof
t:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
[*] Nmap: OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windo
ws 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or
SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Nmap scan report for 192.168.1.250
[*] Nmap: Host is up (0.00014s latency).
[*] Nmap: Not shown: 993 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suho
sin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1)
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 143/tcp  open  imap        Courier Imapd (released 2008)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 5001/tcp open  java-rmi    Java RMI
[*] Nmap: 8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the foll
owing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port5001-TCP:V=7.25BETA1%I=7%D=3/10%Time=5E6840B9%P=x86_64-pc-linux-gnu
[*] Nmap: SF:%r(NULL,4,"\xac\xed\0\x05");
[*] Nmap: MAC Address: 00:0C:29:5E:E6:65 (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.17 - 2.6.36
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 6 IP addresses (6 hosts up) scanned in 189.37 seconds
msf >
```

```
192.168.1.250  8080   tcp    http              open   Apache Tomcat/Coyote JSP engine 1.1

msf > db_nmap -sV 192.168.1.250
[*] Nmap: Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2020-03-10 21:49 EDT
[*] Nmap: Debugging Increased to 1.
[*] Nmap: NSE: Script scanning 192.168.1.250.
[*] Nmap: NSE: Starting runlevel 1 (of 2) scan.
[*] Nmap: NSE: Starting http-server-header against 192.168.1.250:8080.
[*] Nmap: NSE: Starting http-server-header against 192.168.1.250:80.
[*] Nmap: NSE: Finished http-server-header against 192.168.1.250:80.
[*] Nmap: NSE: Finished http-server-header against 192.168.1.250:8080.
[*] Nmap: NSE: Starting runlevel 2 (of 2) scan.
[*] Nmap: Nmap scan report for 192.168.1.250
[*] Nmap: Host is up (0.000053s latency).
[*] Nmap: Scanned at 2020-03-10 21:49:14 EDT for 60s
[*] Nmap: Not shown: 993 closed ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suho
sin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1)
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 143/tcp  open  imap        Courier Imapd (released 2008)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 5001/tcp open  java-rmi    Java RMI
[*] Nmap: 8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 1 service unrecognized despite returning data. If you know the service/version, please submit the foll
owing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF-Port5001-TCP:V=7.25BETA1%I=7%D=3/10%Time=5E6843A1%P=x86_64-pc-linux-gnu
[*] Nmap: SF:%r(NULL,4,"\xac\xed\0\x05");
[*] Nmap: MAC Address: 00:0C:29:5E:E6:65 (VMware)
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Final times for host: srtt: 53 rttvar: 14  to: 100000
[*] Nmap: Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-payloads nmap-service-probes nmap-services.
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 59.94 seconds
msf >
```

- Run default nmap scripts against 192.168.1.250
- Perform nmap scan of all hosts discovered and shown in lan.txt



```
192.168.1.200  389    tcp    ldap              open   Microsoft Windows Active Directory LDAP Domain: AOE.local
, Site: Default-First-Site-Name
192.168.1.200  443    tcp    ssl/http          open   Apache httpd 2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/
0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
192.168.1.200  445    tcp    microsoft-ds      open   Microsoft Windows 2003 or 2008 microsoft-ds
192.168.1.200  464    tcp    kpasswd5          open
192.168.1.200  593    tcp    ncacn_http        open   Microsoft Windows RPC over HTTP 1.0
192.168.1.200  636    tcp    tcpwrapped        open
192.168.1.200  3268   tcp    ldap              open   Microsoft Windows Active Directory LDAP Domain: AOE.local
, Site: Default-First-Site-Name
192.168.1.200  3269   tcp    tcpwrapped        open
192.168.1.200  3306   tcp    mysql             open   MySQL unauthorized
192.168.1.200  3389   tcp    ssl/ms-wbt-server open
192.168.1.200  49152  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.200  49153  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.200  49154  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.200  49155  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.200  49157  tcp    ncacn_http        open   Microsoft Windows RPC over HTTP 1.0
192.168.1.200  49158  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.200  49161  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.200  49163  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.200  49167  tcp    msrpc             open   Microsoft Windows RPC
192.168.1.225  135    tcp    msrpc             open   Microsoft Windows RPC
192.168.1.225  139    tcp    netbios-ssn       open   Microsoft Windows netbios-ssn
192.168.1.225  445    tcp    microsoft-ds      open   Microsoft Windows 7 - 10 microsoft-ds
192.168.1.225  1028   tcp    msrpc             open   Microsoft Windows RPC
192.168.1.250  22     tcp    ssh               open   OpenSSH 5.3p1 Debian 3ubuntu4 Ubuntu Linux; protocol 2.0
192.168.1.250  80     tcp    http              open   Apache httpd 2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ub
untu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
192.168.1.250  139    tcp    netbios-ssn       open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.250  143    tcp    imap              open   Courier Imapd released 2008
192.168.1.250  445    tcp    netbios-ssn       open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.1.250  5001   tcp    java-rmi          open   Java RMI
192.168.1.250  8080   tcp    http              open   Apache Tomcat/Coyote JSP engine 1.1

msf >
```

- In the scan of 192.168.1.250; We notice that IMAP appears to be open on port 80
- Further investigation into “WORKGROUP” and port 5001,8080 could be necessary

Part 2:Verify Scan Data

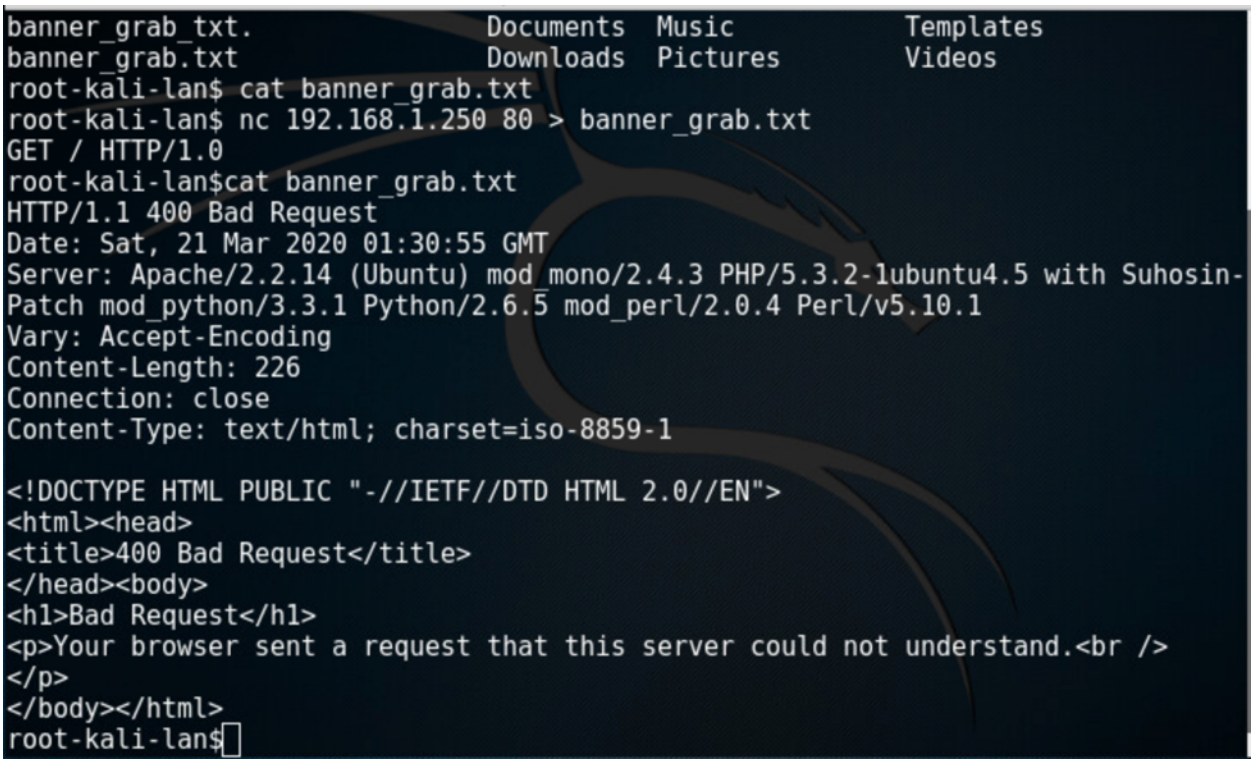
```
msf > sudo telnet 192.168.1.250 143
[*] exec: sudo telnet 192.168.1.250 143

Trying 192.168.1.250...
Connected to 192.168.1.250.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT T
HREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION] Courier-IMAP ready. Copyrigh
t 1998-2008 Double Precision, Inc.  See COPYING for distribution information.
Connection closed by foreign host.
```

- Use telnet to check to see if imap running on port 143 is actually open
- Interesting; after a couple of seconds the “connection is closed by a foreign host”

```
msf > echo "" | nc -v -n -w1 192.168.1.250 80
[*] exec: echo "" | nc -v -n -w1 192.168.1.250 80

(UNKNOWN) [192.168.1.250] 80 (http) open
msf >
```

- Use netcat to grab the banner from this system and export the results to 192_168_1_250_Banner_Grab.txt

```
msf > cat 192_168_1_250_Banner_Grab.txt
[*] exec: cat 192_168_1_250_Banner_Grab.txt

(UNKNOWN) [192.168.1.250] 80 (http) open
msf >
```



- Use netcat to grab the banner from this system and export the results to
  nc 192.168.1.250 80 > banner_grab.txt

- To pull more information from the webserver:
  Use GET/HTTP/1.0

3. Target Host Enumeration

```
Hosts
=====

address        mac                name                os_name  os_flavor  os_sp  purpose  info  comments
-------        ---                ----                -------  ---------  -----  -------  ----  --------
192.168.1.1    00:0C:29:8E:FD:5C  pfSense.localdomain  Unknown                    device
192.168.1.25   00:0C:29:EC:B4:A9                       Unknown                    device
192.168.1.175  00:0C:29:A9:DC:D5                       Unknown                    device
192.168.1.200  00:15:5D:01:80:03                       Unknown                    device
192.168.1.225  00:0C:29:6A:B0:12                       Unknown                    device
192.168.1.250  00:0C:29:5C:DE:56                       Linux                      server

msf > nmap -O 192.168.1.250
[*] exec: nmap -O 192.168.1.250


Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2020-03-19 23:02 EDT
Nmap scan report for 192.168.1.250
Host is up (0.000089s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
MAC Address: 00:0C:29:5C:DE:56 (VMware)
Device type: general purpose
Running: Linux 2.6.X
```

- Return to internal workspace
- Show hosts for target enumeration
- Use nmap -O <IP address> to further investigate service devices

```
msf > nmap -O 192.168.1.1
[*] exec: nmap -O 192.168.1.1


Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2020-03-19 23:07 EDT
Nmap scan report for pfSense.localdomain (192.168.1.1)
Host is up (0.00013s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:8E:FD:5C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), OpenBSD 4.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: Comau C4G robot control unit (92%), OpenBSD 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.35 seconds
```

```
msf > nmap -O 192.168.1.25
[*] exec: nmap -O 192.168.1.25


Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2020-03-19 23:11 EDT
Nmap scan report for 192.168.1.25
Host is up (0.00013s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1028/tcp open  unknown
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:EC:B4:A9 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.41 seconds
```

- It was discovered that Windows XP is running multiple services on various ports

```
Nmap scan report for 192.168.1.25
Host is up (0.00014s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Microsoft ESMTP 6.0.2600.2180
80/tcp   open  http          Microsoft IIS httpd 5.1
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1028/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:0C:29:EC:B4:A9 (VMware)
Service Info: Host: WINXP.AOE.local; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:w
indows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.12 seconds
msf > services 192.168.1.25

Services
========

host          port  proto  name          state  info
----          ----  -----  ----          -----  ----
192.168.1.25  25    tcp    smtp          open
192.168.1.25  80    tcp    http          open
192.168.1.25  135   tcp    msrpc         open
192.168.1.25  139   tcp    netbios-ssn   open
192.168.1.25  443   tcp    https         open
192.168.1.25  445   tcp    microsoft-ds  open
192.168.1.25  1028  tcp    unknown       open
192.168.1.25  3389  tcp    ms-wbt-server  open
```

After discovering services running on the windows XP devices; perform SMB enumeration with metasploit and windows module

- Use msf> search windows
- Msf > post/gather/windows to display options

```
msf > search post/windows/gather

Matching Modules
================

   Name                                                Disclosure Date  Rank    Description
   ----                                                ---------------  ----    -----------
   auxiliary/parser/unattend                                            normal  Auxilliary Parser Windows Unattend Passwords
   post/windows/gather/ad_to_sqlite                                     normal  AD Computer, Group and Recursive User Membership to Local SQLite DB
   post/windows/gather/arp_scanner                                      normal  Windows Gather ARP Scanner
   post/windows/gather/bitcoin_jacker                                   normal  Windows Gather Bitcoin Wallet
   post/windows/gather/bitlocker_fvek                                   normal  Bitlocker Master Key (FVEK) Extraction
   post/windows/gather/cachedump                                        normal  Windows Gather Credential Cache Dump
   post/windows/gather/checkvm                                          normal  Windows Gather Virtual Environment Detection
   post/windows/gather/credentials/avira_password                       normal  Windows Gather Avira Password Extraction
   post/windows/gather/credentials/bulletproof_ftp                      normal  Windows Gather BulletProof FTP Client Saved Password Extraction
   post/windows/gather/credentials/coreftp                              normal  Windows Gather CoreFTP Saved Password Extraction
   post/windows/gather/credentials/credential_collector                 normal  Windows Gather Credential Collector
   post/windows/gather/credentials/domain_hashdump                      normal  Windows Domain Controller Hashdump
   post/windows/gather/credentials/dyndns                               normal  Windows Gather DynDNS Client Password Extractor
   post/windows/gather/credentials/enum_cred_store                      normal  Windows Gather Credential Store Enumeration and Decryption Module
   post/windows/gather/credentials/enum_laps                            normal  Windows Gather Credentials Local Administrator Password Solution
   post/windows/gather/credentials/enum_picasa_pwds                     normal  Windows Gather Google Picasa Password Extractor
   post/windows/gather/credentials/epo_sql                              normal  Windows Gather McAfee ePO 4.6 Config SQL Credentials
   post/windows/gather/credentials/filezilla_server                     normal  Windows Gather FileZilla FTP Server Credential Collection
   post/windows/gather/credentials/flashfxp                             normal  Windows Gather FlashFXP Saved Password Extraction
   post/windows/gather/credentials/ftpnavigator                         normal  Windows Gather FTP Navigator Saved Password Extraction
   post/windows/gather/credentials/ftpx                                 normal  Windows Gather FTP Explorer (FTPX) Credential Extraction
   post/windows/gather/credentials/gpp                                  normal  Windows Gather Group Policy Preference Saved Passwords
   post/windows/gather/credentials/heidisql                             normal  Windows Gather HeidiSQL Saved Password Extraction
   post/windows/gather/credentials/idm                                  normal  Windows Gather Internet Download Manager (IDM) Password Extractor
   post/windows/gather/credentials/imail                                normal  Windows Gather IPSwitch iMail User Data Enumeration
   post/windows/gather/credentials/imvu                                 normal  Windows Gather Credentials IMVU Game Client
   post/windows/gather/credentials/mcafee_vse_hashdump                  normal  McAfee Virus Scan Enterprise Password Hashes Dump
   post/windows/gather/credentials/meebo                                normal  Windows Gather Meebo Password Extractor
   post/windows/gather/credentials/mremote                              normal  Windows Gather mRemote Saved Password Extraction
   post/windows/gather/credentials/mssql_local_hashdump                 normal  Windows Gather Local SQL Server Hash Dump
   post/windows/gather/credentials/nimbuzz                              normal  Windows Gather Nimbuzz Instant Messenger Password Extractor
   post/windows/gather/credentials/outlook                              normal  Windows Gather Microsoft Outlook Saved Password Extraction
   post/windows/gather/credentials/razer_synapse                        normal  Windows Gather Razer Synapse Password Extraction
   post/windows/gather/credentials/razorsql                             normal  Windows Gather RazorSQL Credentials
   post/windows/gather/credentials/rdc_manager_creds                    normal  Windows Gather Remote Desktop Connection Manager Saved Password Extraction
```

```
   post/windows/gather/enum_dirperms                                    normal     Windows Gather Directory Permissions Enumeration
   post/windows/gather/enum_domain                                      normal     Windows Gather Enumerate Domain
   post/windows/gather/enum_domain_group_users                          normal     Windows Gather Enumerate Domain Group
   post/windows/gather/enum_domain_tokens                               normal     Windows Gather Enumerate Domain Tokens
   post/windows/gather/enum_domain_users                                normal     Windows Gather Enumerate Active Domain Users
   post/windows/gather/enum_domains                                     normal     Windows Gather Domain Enumeration
   post/windows/gather/enum_emet                                        normal     Windows Gather EMET Protected Paths
   post/windows/gather/enum_files                                       normal     Windows Gather Generic File Collection
   post/windows/gather/enum_hostfile                                    normal     Windows Gather Windows Host File Enumeration
   post/windows/gather/enum_ie                                          normal     Windows Gather Internet Explorer User Data Enumeration
   post/windows/gather/enum_logged_on_users                             normal     Windows Gather Logged On User Enumeration (Registry)
   post/windows/gather/enum_ms_product_keys                             normal     Windows Gather Product Key
   post/windows/gather/enum_muicache                                    normal     Windows Gather Enum User MUICache
   post/windows/gather/enum_patches                                     normal     Windows Gather Applied Patches
   post/windows/gather/enum_powershell_env                              normal     Windows Gather Powershell Environment Setting Enumeration
   post/windows/gather/enum_prefetch                                    normal     Windows Gather Prefetch File Information
   post/windows/gather/enum_proxy                                       normal     Windows Gather Proxy Setting
   post/windows/gather/enum_putty_saved_sessions                        normal     PuTTY Saved Sessions Enumeration Module
   post/windows/gather/enum_services                                    normal     Windows Gather Service Info Enumeration
   post/windows/gather/enum_shares                                      normal     Windows Gather SMB Share Enumeration via Registry
   post/windows/gather/enum_snmp                                        normal     Windows Gather SNMP Settings Enumeration (Registry)
   post/windows/gather/enum_termserv                                    normal     Windows Gather Terminal Server Client Connection Information
Dumper
   post/windows/gather/enum_tokens                                      normal     Windows Gather Enumerate Domain Admin Tokens (Token Hunter)
   post/windows/gather/enum_tomcat                                      normal     Windows Gather Apache Tomcat Enumeration
   post/windows/gather/enum_trusted_locations                           normal     Windows Gather Microsoft Office Trusted Locations
   post/windows/gather/enum_unattend                                    normal     Windows Gather Unattended Answer File Enumeration
   post/windows/gather/file_from_raw_ntfs                               normal     Windows File Gather File from Raw NTFS
   post/windows/gather/forensics/browser_history                        normal     Windows Gather Skype, Firefox, and Chrome Artifacts
   post/windows/gather/forensics/duqu_check                             normal     Windows Gather Forensics Duqu Registry Check
   post/windows/gather/forensics/enum_drives                            normal     Windows Gather Physical Drives and Logical Volumes
   post/windows/gather/forensics/imager                                 normal     Windows Gather Forensic Imaging
   post/windows/gather/forensics/nbd_server                             normal     Windows Gather Local NBD Server
   post/windows/gather/forensics/recovery_files                         normal     Windows Gather Deleted Files Enumeration and Recovering
   post/windows/gather/hashdump                                         normal     Windows Gather Local User Account Password Hashes (Registry)
   post/windows/gather/local_admin_search_enum                          normal     Windows Gather Local Admin Search
   post/windows/gather/lsa_secrets                                      normal     Windows Enumerate LSA Secrets
   post/windows/gather/make_csv_orgchart                                normal     Generate CSV Organizational Chart Data Using Manager Informat
ion
   post/windows/gather/memory_grep                                      normal     Windows Gather Process Memory Grep
   post/windows/gather/netlm_downgrade                                  normal     Windows NetLM Downgrade Attack
   post/windows/gather/ntds_location                                    normal     Post Windows Gather NTDS.DIT Location
   post/windows/gather/outlook                                          normal     Windows Gather Outlook Email Messages
   post/windows/gather/phish_windows_credentials                        normal     Windows Gather User Credentials (phishing)
   post/windows/gather/resolve_sid                                      normal     Windows Gather Local User Account SID Lookup
   post/windows/gather/reverse_lookup                                   normal     Windows Gather IP Range Reverse Lookup
   post/windows/gather/screen_spy                                       normal     Windows Gather Screen Spy
   post/windows/gather/smart_hashdump                                   normal     Windows Gather Local and Domain Controller Account Password H
ashes
   post/windows/gather/tcpnetstat                                       normal     Windows Gather TCP Netstat
   post/windows/gather/usb_history                                      normal     Windows Gather USB Drive History
   post/windows/gather/win_privs                                        normal     Windows Gather Privileges Enumeration
   post/windows/gather/wmic_command                                     normal     Windows Gather Run Specified WMIC Command
   post/windows/gather/word_unc_injector                                normal     Windows Gather Microsoft Office Word UNC Path Injector


msf > search grep 'smb' post/windows/gather
```

- Search grep ‘smb’ post/windows/gather

```
msf > nbtscan -v 192.168.1.25
[*] exec: nbtscan -v 192.168.1.25

Doing NBT name scan for addresses from 192.168.1.25


NetBIOS Name Table for Host 192.168.1.25:

Name             Service          Type
---------------------------------------
WINXP            <00>             UNIQUE
AOE              <00>              GROUP
WINXP            <20>             UNIQUE
AOE              <1e>              GROUP
AOE              <1d>             UNIQUE
[illegible]_MSBROWSE_[illegible] <01>              GROUP

Adapter address: 00:0c:29:ec:b4:a9
---------------------------------------
```

Part 4: Exploit Linux Hosts

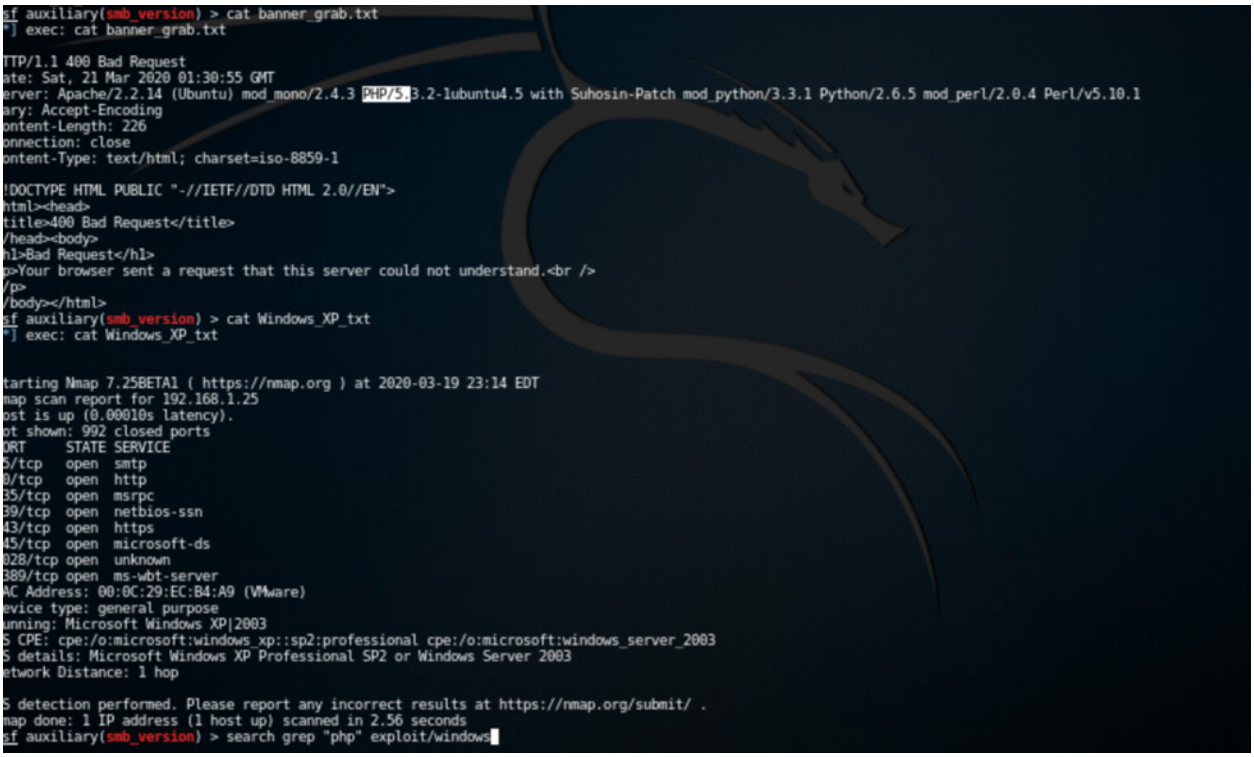
```
msf > nbtscan -v 192.168.1.25
[*] exec: nbtscan -v 192.168.1.25

Doing NBT name scan for addresses from 192.168.1.25


NetBIOS Name Table for Host 192.168.1.25:

Name             Service          Type
---------------------------------------
WINXP            <00>             UNIQUE
AOE              <00>              GROUP
WINXP            <20>             UNIQUE
AOE              <1e>              GROUP
AOE              <1d>             UNIQUE
[illegible]_MSBROWSE_[illegible] <01>              GROUP

Adapter address: 00:0c:29:ec:b4:a9
---------------------------------------
msf > nbtstat -v 192.168.1.25
[-] Unknown command: nbtstat.
msf > use  scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 192.168.1.25
RHOSTS => 192.168.1.25
msf auxiliary(smb_version) > run

[*] 192.168.1.25:445      - Host is running Windows XP SP2 (language:English) (name:WINXP) (domain:AOE)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

- Netbois allows us to discover domain names, OS versions, mac addresses etc

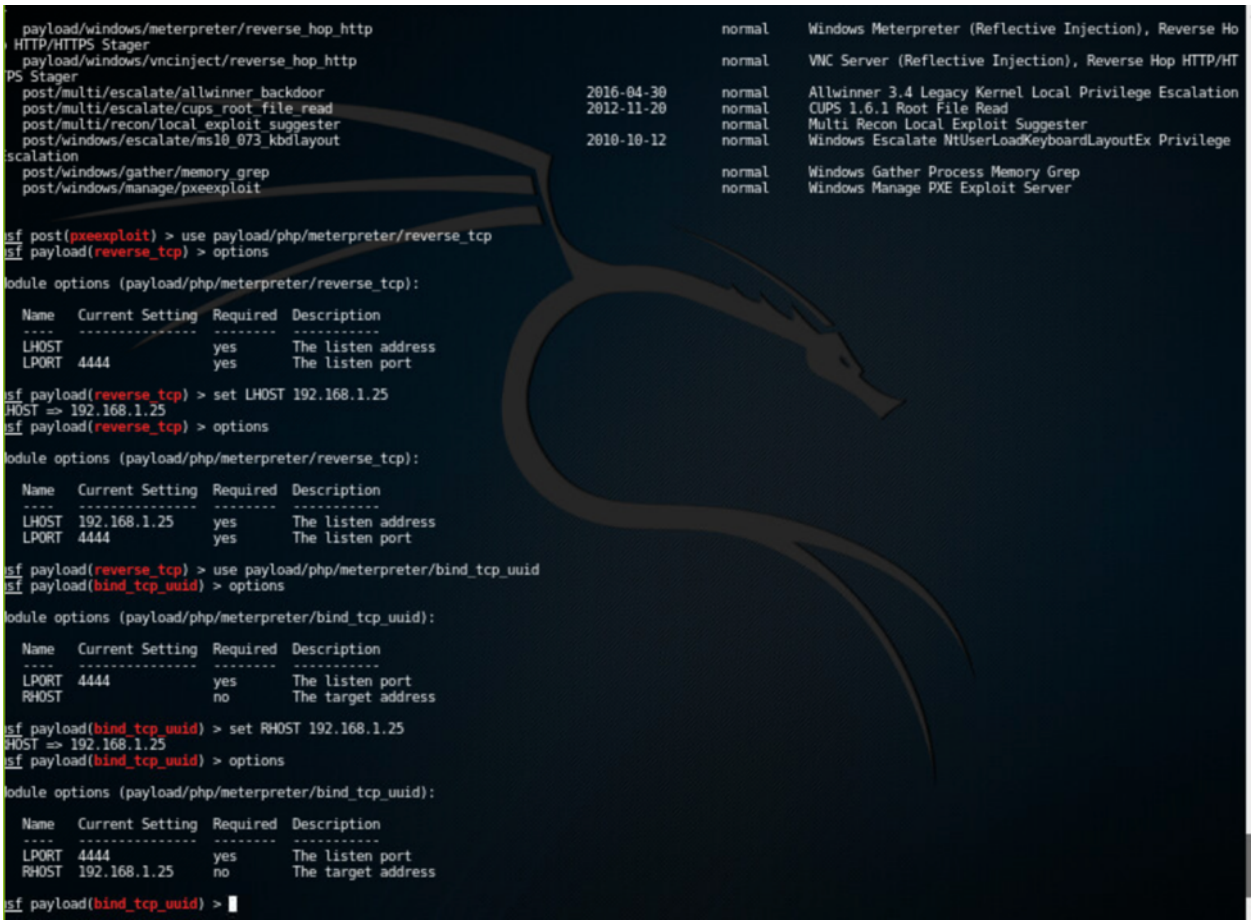
```
msf auxiliary(smb_version) >  cat banner_grab.txt
[*] exec:  cat banner_grab.txt

HTTP/1.1 400 Bad Request
Date: Sat, 21 Mar 2020 01:30:55 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Pytho
6.5 mod_perl/2.0.4 Perl/v5.10.1
Vary: Accept-Encoding
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
</body></html>
msf auxiliary(smb_version) >
```

- Find php exploits
- Use search grep “php” exploits/windows

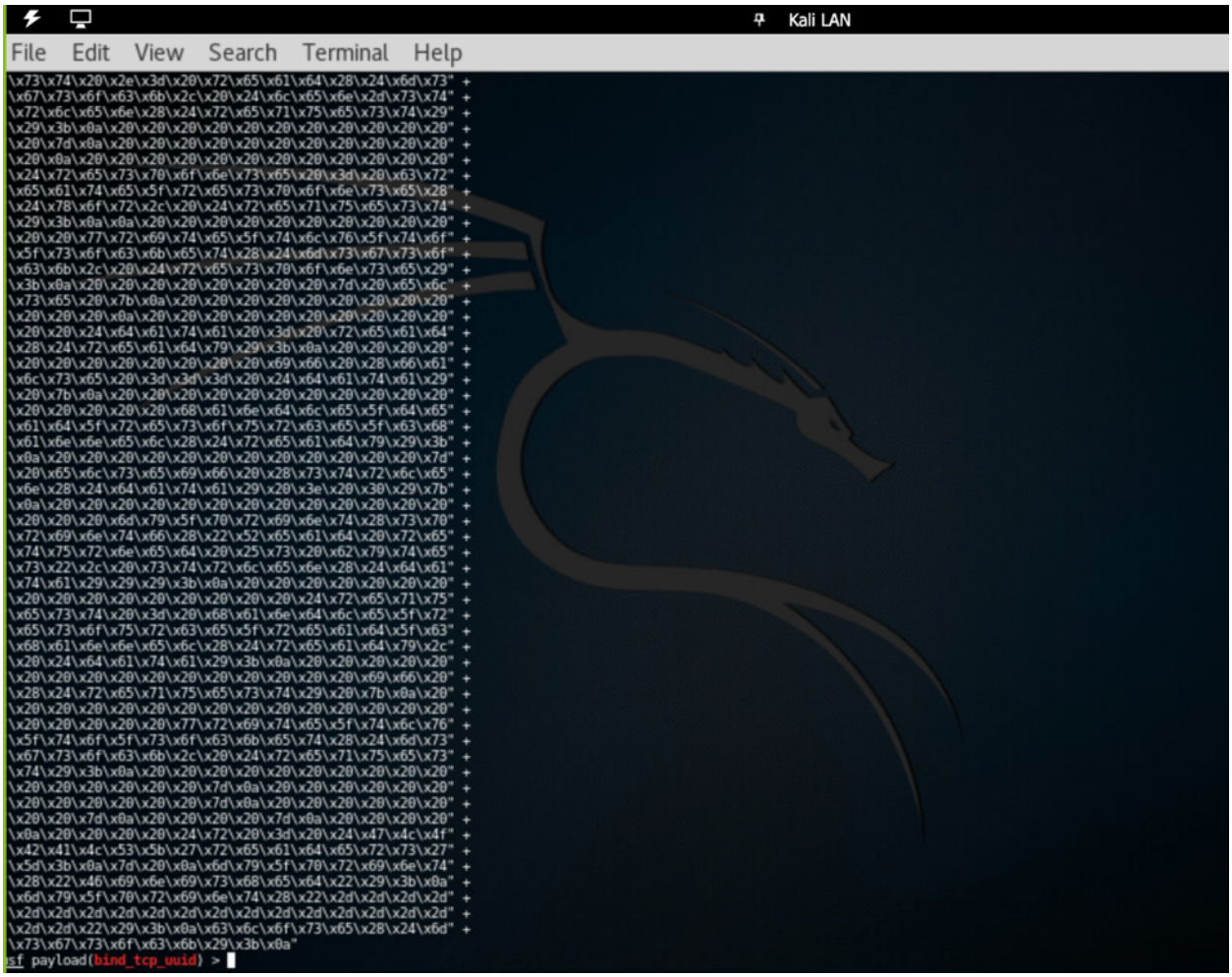
```
ution
   exploit/windows/tftp/opentftp_error_code                   2008-07-05       average    OpenTFTP SP 1.4 Error Packet Overflow
   exploit/windows/tftp/quick_tftp_pro_mode                   2008-03-27       good       Quick FTP Pro 2.1 Transfer-Mode Overflow
   exploit/windows/tftp/tftpd32_long_filename                 2002-11-19       average    TFTPD32 Long Filename Buffer Overflow
   exploit/windows/tftp/tftpdwin_long_filename                2006-09-21       great      TFTPDWIN v0.4.2 Long Filename Buffer Overflow
   exploit/windows/tftp/tftpserver_wrq_bof                    2008-03-26       normal     TFTP Server for Windows 1.4 ST WRQ Buffer Overflow
   exploit/windows/tftp/threectftpsvc_long_mode               2006-11-27       great      3CTftpSvc TFTP Long Mode Buffer Overflow
   exploit/windows/unicenter/cam_log_security                 2005-08-22       great      CA CAM log_security() Stack Buffer Overflow (Win32)
   exploit/windows/vnc/realvnc_client                         2001-01-29       normal     RealVNC 3.3.7 Client Buffer Overflow
   exploit/windows/vnc/ultravnc_client                        2006-04-04       normal     UltraVNC 1.0.1 Client Buffer Overflow
   exploit/windows/vnc/ultravnc_viewer_bof                    2008-02-06       normal     UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
   exploit/windows/vnc/winvnc_http_get                        2001-01-29       average    WinVNC Web Server GET Overflow
   exploit/windows/vpn/safenet_ike_11                         2009-06-01       average    SafeNet SoftRemote IKE Service Buffer Overflow
   exploit/windows/winrm/winrm_script_exec                    2012-11-01       manual     WinRM Script Exec Remote Code Execution
   exploit/windows/wins/ms04_045_wins                         2004-12-14       great      MS04-045 Microsoft WINS Service Memory Overwrite
   nop/php/generic                                                             normal     PHP Nop Generator
   payload/cmd/unix/reverse_php_ssl                                            normal     Unix Command Shell, Reverse TCP SSL (via php)
   payload/generic/custom                                                      normal     Custom Payload
   payload/generic/shell_bind_tcp                                              normal     Generic Command Shell, Bind TCP Inline
   payload/generic/shell_reverse_tcp                                           normal     Generic Command Shell, Reverse TCP Inline
   payload/linux/mipsbe/reboot                                                 normal     Linux Reboot
   payload/linux/mipsle/reboot                                                 normal     Linux Reboot
   payload/php/bind_perl                                                       normal     PHP Command Shell, Bind TCP (via Perl)
   payload/php/bind_perl_ipv6                                                  normal     PHP Command Shell, Bind TCP (via perl) IPv6
   payload/php/bind_php                                                        normal     PHP Command Shell, Bind TCP (via PHP)
   payload/php/bind_php_ipv6                                                   normal     PHP Command Shell, Bind TCP (via php) IPv6
   payload/php/download_exec                                                   normal     PHP Executable Download and Execute
   payload/php/exec                                                            normal     PHP Execute Command
   payload/php/meterpreter/bind_tcp                                            normal     PHP Meterpreter, Bind TCP Stager
   payload/php/meterpreter/bind_tcp_ipv6                                       normal     PHP Meterpreter, Bind TCP Stager IPv6
   payload/php/meterpreter/bind_tcp_ipv6_uuid                                  normal     PHP Meterpreter, Bind TCP Stager IPv6 with UUID Suppor
t
   payload/php/meterpreter/bind_tcp_uuid                                       normal     PHP Meterpreter, Bind TCP Stager with UUID Support
   payload/php/meterpreter/reverse_tcp                                         normal     PHP Meterpreter, PHP Reverse TCP Stager
   payload/php/meterpreter/reverse_tcp_uuid                                    normal     PHP Meterpreter, PHP Reverse TCP Stager
   payload/php/meterpreter_reverse_tcp                                         normal     PHP Meterpreter, Reverse TCP Inline
   payload/php/reverse_perl                                                    normal     PHP Command, Double Reverse TCP Connection (via Perl)
   payload/php/reverse_php                                                     normal     PHP Command Shell, Reverse TCP (via PHP)
   payload/php/shell_findsock                                                  normal     PHP Command Shell, Find Sock
   payload/windows/dllinject/reverse_hop_http                                  normal     Reflective DLL Injection, Reverse Hop HTTP/HTTPS Stage
r
   payload/windows/meterpreter/reverse_hop_http                                normal     Windows Meterpreter (Reflective Injection), Reverse Ho
p HTTP/HTTPS Stager
   payload/windows/vncinject/reverse_hop_http                                  normal     VNC Server (Reflective Injection), Reverse Hop HTTP/HT
TPS Stager
   post/multi/escalate/allwinner_backdoor                     2016-04-30       normal     Allwinner 3.4 Legacy Kernel Local Privilege Escalation
   post/multi/escalate/cups_root_file_read                    2012-11-20       normal     CUPS 1.6.1 Root File Read
   post/multi/recon/local_exploit_suggester                                    normal     Multi Recon Local Exploit Suggester
   post/windows/escalate/ms10_073_kbdlayout                   2010-10-12       normal     Windows Escalate NtUserLoadKeyboardLayoutEx Privilege
Escalation
   post/windows/gather/memory_grep                                             normal     Windows Gather Process Memory Grep
   post/windows/manage/pxeexploit                                              normal     Windows Manage PXE Exploit Server
```



- I added additional files throughout the course of this assignment to store information
- Here Windows_XP_txt stores information about the XP device
- Banner_grab.txt stores information discovered in the netcat scan with GET



- 1) aux
- 2) exploit
- 3) payload – I chose 2 different php payloads; one with a bind and one without a bind – involving tcp reverse shell



- To check and see if payload successfully deployed