

Assignment 2-

Vidit Sharma

21BCY10055

Date- 1/9/2023

Kali Linux Tools-

1. Nmap-

Nmap, short for "Network Mapper," is a powerful and versatile open-source network scanning tool used for network discovery and security auditing. It was originally developed by Gordon Lyon (also known as Fyodor Vaskovich) and has since gained widespread popularity among network administrators, security professionals, and ethical hackers. Nmap is available for multiple platforms, including Windows, Linux, and macOS.

It helps discover active hosts, open ports, and services on a network. Nmap's versatility extends to service and version detection, operating system identification, and custom scripting for advanced tasks. Network administrators, security experts, and ethical hackers rely on Nmap to assess network security, create network maps, and perform vulnerability scans. Its command-line interface and various output formats make it a flexible and powerful tool for network reconnaissance and auditing, but it should always be used responsibly and legally.

```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

(kali@kali)~$ nmap -sV -A vit.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 12:52 UTC
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.16s latency).
Other addresses for vit.ac.in (not scanned): 64:ff9b::88e9:90d
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      4.43.0
|_ fingerprint-strings:
|_   FourOhFourRequest:
|_     HTTP/1.0 302 Moved Temporarily
|_     Location: https://10.10.7.35/?_event_transid=4041259661&_event_clientip=49.15.241.129&_event_clientport=521626&_event_attackname=Server+Information+Leakage&_event_threatcategory=Information+Leakage
|_     Content-Length: 0
|_   GetRequest:
|_     HTTP/1.0 302 Moved Temporarily
|_     Location: https://10.10.7.35/
|_     Content-Length: 0
|_   HTTPOptions:
|_     HTTP/1.0 302 Moved Temporarily
|_     Location: https://10.10.7.35/?_event_transid=4041259050&_event_clientip=49.15.241.129&_event_clientport=521366&_event_attackname=HTTP+Method+Violation&_event_threatcategory=HTTP+RFC+Violations
|_     Content-Length: 0
|_   RTSPRequest:
|_     HTTP/1.0 302 Moved Temporarily
|_     Location: https://10.10.7.35/?_event_transid=4041259089&_event_clientip=49.15.241.129&_event_clientport=521426&_event_attackname=HTTP+RFC+Violation&_event_threatcategory=HTTP+RFC+Violations
|_     Content-Length: 0
|_   SIPOptions:
|_     HTTP/1.0 302 Moved Temporarily
|_     Location: https://10.10.7.35/?_event_transid=4041264687&_event_clientip=49.15.241.129&_event_clientport=555446&_event_attackname=HTTP+RFC+Violation&_event_threatcategory=HTTP+RFC+Violations
|_     Content-Length: 0
443/tcp    open  ssl/http Apache httpd (off)
|_   ssl-cert: Subject: commonName=vit.ac.in
|_   Subject Alternative Name: DNS:vit.ac.in, DNS:*.vit.ac.in
|_   Not valid before: 2023-09-04T00:00:00
|_   Not valid after: 2024-08-03T23:59:59
|_   ssl-date: TLS randomness does not represent time
|_   http-robots.txt: 46 disallowed entries (15 shown)
|_   / /?utm_* /includes/ /misc/ /modules/ /profiles/
|_   /scripts/ /themes /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_   /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_   tls-alpn:
|_     http/1.1
|_   http-generator: Drupal
|_   http-title: Vellore Institute of Technology | A Place to Learn, Chance to ...
|_   http-server-header: Apache
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-Port80-TCP:V=7.94I=7&D=9/6&T=64F8762D&P=x86_64-pc-linux-gnu&R(GetRe
SF:quest,54,"HTTP/1.0\x20302\x20MovedTemporarily\r\nLocation:\x20http
```

I scanned for the website vit.ac.in

Command used: `nmap -sV -A vit.ac.in`

Information obtained:

- 1. Open Ports:** The scan will identify which ports are open on the target server. This information helps you understand which services are accessible.
- 2. Service Versions:** Nmap will attempt to determine the specific software and version numbers of the services running on the open ports. This is valuable for identifying potential vulnerabilities and security risks.
- 3. OS Detection:** Nmap will try to identify the operating system of the target server based on various characteristics and responses. While this is not always accurate, it can provide insights into the underlying technology.
- 4. Aggressive Scan:** The `-A` option activates aggressive scanning, which includes OS detection, script scanning, and other advanced techniques to gather as much information as possible.
- 5. Service Detection:** In addition to version detection, Nmap will identify the service names associated with open ports.
- 6. Hostname:** If DNS resolution is successful, Nmap may display the resolved hostname of the target.

```
(kali@kali)-[~]
$ nmap -sV -A vit.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 12:52 UTC
Nmap scan report for vit.ac.in (136.233.9.13)
Host is up (0.16s latency).
Other addresses for vit.ac.in (not scanned): 64:ff9b::88e9:90d
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache/2.4.18 (Ubuntu)
```

Shodan search results for vit.ac.in. The interface shows a list of top ports (25, 443, 80, 587) and top organizations (Bharti Airtel Limited, Reliance Jio Infocomm Limited, Oracle Public Cloud, TATATELSERVICES). The main content area displays the Vellore Institute of Technology website with an SSL certificate details panel on the right. The certificate is issued by Sectigo RSA Domain Validation Secure Server CA and expires on Sun, 19 Nov 1978 05:00:00 GMT.

2. John The Ripper-

John the Ripper is a widely used open-source password cracking tool, invaluable for assessing password security. It operates by attempting various techniques, including dictionary and brute-force attacks, to crack password hashes rather than plaintext passwords. It supports numerous hash algorithms, custom wordlists, and rule-based

password variations. John is highly customizable and often used by security professionals to identify weak passwords and evaluate password policies. However, it should be used ethically and legally, with proper authorization, to avoid legal and ethical issues.

John the Ripper, often referred to as simply "John," is a popular open-source password cracking tool used by security professionals, system administrators, and ethical hackers to assess the strength of passwords and perform security audits. It is designed to help identify weak or easily guessable passwords in various password-protected files or systems.

```
(kali@kali)-[~]
└─$ sudo su
(root@kali)-[/home/kali]
└─$ john /etc/shadow
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 256/256 AVX2])
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
kali
(kali)
lg 0:00:00:00 DONE 1/3 (2023-09-06 14:58) 100.0g/s 76800p/s 76800c/s 76800C/s
kali..:k999999
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(root@kali)-[/home/kali]
└─$
```

Command used: `john /etc/shadow`

Information obtained:

Using this command you will get the password from the shadow file.

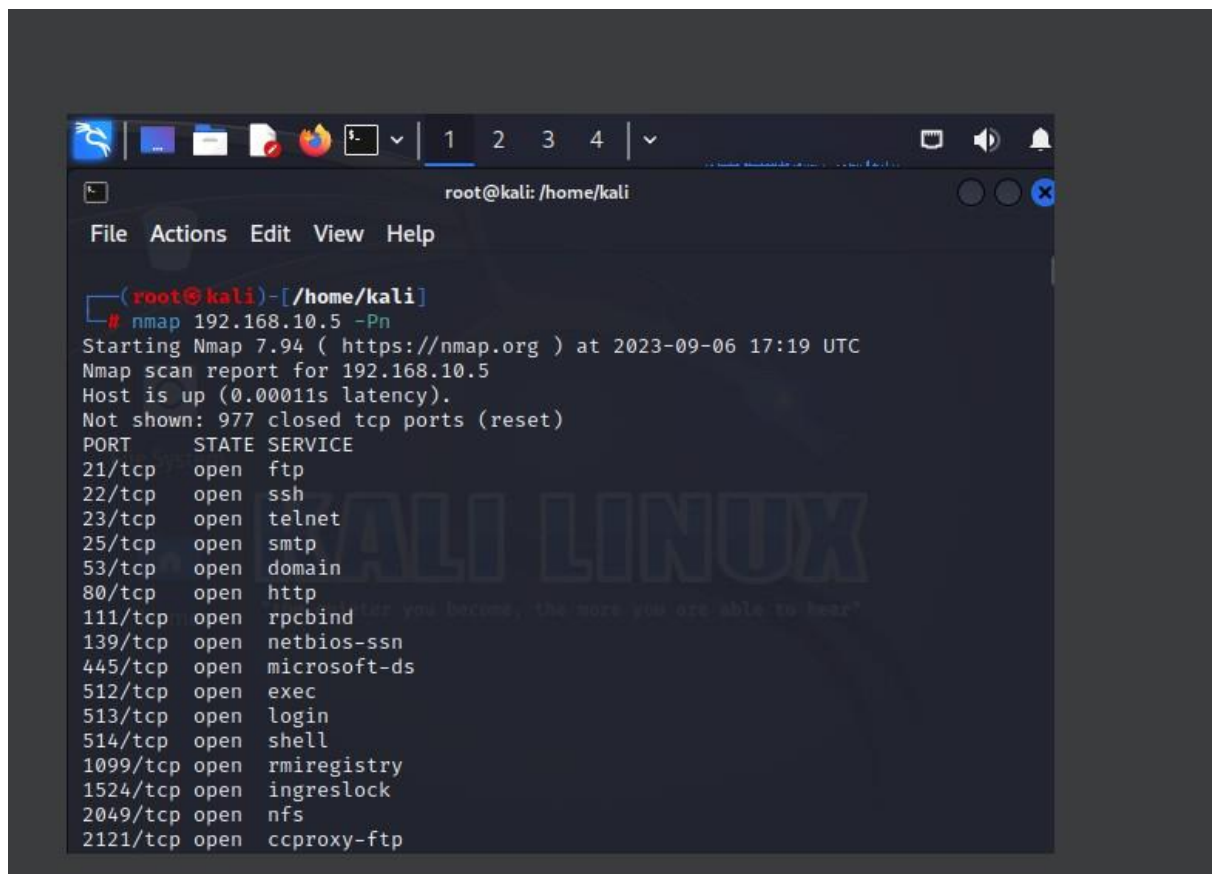
Username found: kali

Password found: kali

3. Metasploitable-

Metasploitable is a deliberately vulnerable virtual machine (VM) that is designed for educational and testing purposes in the field of cybersecurity. It is intentionally created with various security vulnerabilities and misconfigurations, allowing security professionals, penetration testers, and ethical hackers to practice and improve their skills in a controlled and safe environment.

It serves as a valuable tool for learning about common security issues, penetration testing, and security research. However, it should never be used in production environments and should only be accessed with proper authorization for ethical and educational purposes.



```
(root@kali)-[/home/kali]
# nmap 192.168.10.5 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 17:19 UTC
Nmap scan report for 192.168.10.5
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
```

We take Ip address of metasploitable to get information.

Command used: `nmap 192.168.10.5 -Pn`


```
root@kali: /home/kali
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

(root@kali)-[/home/kali]
# nmap 192.168.10.5 -Pn -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 17:20 UTC
Nmap scan report for 192.168.10.5
Host is up (0.000096s latency).
Not shown: 977 closed tcp ports (reset)
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         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
```

To get more information.

Command used: `nmap 192.168.10.5 -Pn -sV`

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# sudo msfconsole
[*] Starting thE Metasploit Framework console ... \
[*] Starting the Metasploit Framework console ... |
[*] Starting the Metasploit Framework console ... -

File System: ~:oDFo:~
~/ymM0dayMmy/.
--dHJ5aGFyZGVyIQ==--
~:sm@~Destroy.No.Data~s:~
~+h2~Maintain.No.Persistence~h+-
~:odNo2~Above.All.Else.Do.No.Harm~Ndo:~
./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
--++SecKCoin++e.AMd~ ~.-://///hbove.913.ElsMNh+-
~/./ssh/id_rsa.Des- ~htN01UserWroteMe!
```

To open metasploitable in kali linux.