SAPIENCE EDU CONNECT INTERNSHIP

(**Cyber Security**)

NAME : KATAKAM LIKITH KUMAR

REPORT DATE :

EMAIL : likithkumarkatakam811@gmail.com

Week 3 : Introduction to Cybersecurity and Virtualization

- Task 1:

Objective : The objective of this internship was to gain hands-on experience in cybersecurity reconnaissance, network scanning, and vulnerability assessment. Using tools like whois, dig, nslookup, and nmap, the focus was on identifying network structures, detecting vulnerabilities, and analyzing security configurations to enhance cybersecurity awareness.

Introduction : In order to protect digital assets from any threats and attacks, cybersecurity is essential. The primary objective of this internship was practical experience with network scanning, vulnerability assessment, and cybersecurity reconnaissance. The internship sought to build a solid grasp of security technologies and methods utilized in actual cybercrime investigations through hands-on activities. The abilities acquired from this encounter help to improve defense tactics and general cybersecurity awareness.

Software and Hardware requirements :

Software :

- Oracle virtual Box or VMware software
- Kali Linux

Hardware :

- Computer or Laptop with Internet connectivity

Methodology :

The methodology ensured thorough data collection and assessment by using a methodical approach to cybersecurity analysis:

1. **Finding the Target IP Range:** The network to be scanned was identified.

2. **Footprinting & Information Gathering (whois):** Google.com's domain registration information was extracted in order to obtain administrative and ownership information.

3**. DNS Enumeration (nslookup, dig):** To comprehend network topology, domain names were resolved to IP addresses and DNS information was obtained.

4. **Network analysis (ip a, ip route):** To map out connection, local IP setups and routing information were examined.

5. **Active Scanning (nmap -sn, nmap -p-):** a port scan to find open and closed ports and a ping sweep to find live hosts.

6. **Service Enumeration & Banner Grabbing** (nmap): Made an effort to find services that were using open ports and took note of service banners for additional examination.

7**.OS Fingerprinting** (nmap -O): Determined the target's operating system by analyzing system responses.

8.**Vulnerability Assessment**: Checked for known vulnerabilities in services that were found using nmap --script vuln.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nslookup google.com
Server:         192.168.17.2
Address:        192.168.17.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.194.174
Name:   google.com
Address: 2404:6800:4002:823::200e


┌──(kali㉿kali)-[~]
└─$ dig google.com +short
142.250.194.174

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a6:b4:cd brd ff:ff:ff:ff:ff:ff
    inet 192.168.17.128/24 brd 192.168.17.255 scope global dynamic noprefixroute eth0
       valid_lft 1365sec preferred_lft 1365sec
    inet6 fe80::baca:73b5:437:71bf/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ip route
default via 192.168.17.2 dev eth0 proto dhcp src 192.168.17.128 metric 100
192.168.17.0/24 dev eth0 proto kernel scope link src 192.168.17.128 metric 100
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.17.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 06:21 EST
Nmap scan report for 192.168.17.128
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.17.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 06:21 EST
Nmap scan report for 192.168.17.128
Host is up (0.0000050s latency).
All 65535 scanned ports on 192.168.17.128 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

Conclusion :

This procedure describes a thorough method for evaluating network security, beginning with determining the target IP range and looking for active hosts. To obtain comprehensive system information, it uses port scanning, service enumeration, banner capturing, and OS fingerprinting. In order to enable proactive security measures, vulnerability assessments using Nmap assist uncover potential security flaws, while footprinting tools like Whois and Nslookup offer more insights.