VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE - 3

DATE: 30.07.2020

Preparation:

1. Install VMWare Workstation Pro

https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

2. Install Kali Linux inside this VMWare Workstation

https://www.kali.org/downloads/

(Kali linux 64-bit installer)

Good Reference:

- https://www.shaileshjha.com/how-to-install-kali-linux-in-vmware-player-vmware-tools/

Cheat Sheets (All possible Commands with NMAP)

- https://resources.infosecinstitute.com/nmap-cheat-sheet/#gref
- https://www.stationx.net/nmap-cheat-sheet/
- https://www.tutorialspoint.com/nmap-cheat-sheet

Suggested Site to Test:

- nmap.org
- scname.nmap.org

Implement the following in NMAP:

1. Perform host discovery (You can do sniffing using Wireshark and know about a connected host)
2. Identify Which hosts are up now? Apply ping sweeping (Port Sweeping)
3. Use the TCP "ping" option with a ping scan with a flag to target port (Ping Sweeping)
4. scan all the TCP ports
5. Save the results in xml file
6. Save the results in a tex
7. Find out if a host/network is protected by a firewall

CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT
EXERCISE - 3

DATE: 30.07.2020

8. Scan a host when protected by the firewall
9. Scan a firewall for security weakness
10. Cloak a scan with decoys
11. Bypass Firewall (locally) (MAC Address spoofing)
12. Bypass Firewall
13. Find out Version Info
14. Check if a web server is vulnerable to directory traversal by attempting to retrieve /etc/passwd or \boot.ini
15. Test a web server for vulnerability to the Slowloris DoS attack by launching a Slowloris attack
16. Do Google safe browsing api
17. Grep public emails using nmap
18. Discover hostnames pointing to the same IP address
19. Discover hostnames by brute forcing DNS records
20. Validate your network broadcast
21. If a computer is up, which services (TCP and UDP) are open on it?
22. Determine the Operating system and its possible version that is running on each alive computer

Note :

- In a word document, copy the command you have used for each task and show the screen shot for each step output.
- The IP address of your machine has to appear (ipconfig/ifconfig command) in each screen shot (For reliability)