Internet Security (IS)

Lab 1

Faculty of Architecture, Computing & Engineering

School of Applied Computing

Mount Pleasant Campus

Swansea

SA1 6ED

1.0 INTRODUCTION AND OBJECTIVES OF THE EXERCISES

In the lectures, you learnt about vulnerabilities, treats and attacks, security planning and policy, trust & identity planning, which are an essential factor in successfully protecting the network environment. Apply your understanding and knowledge from what you learnt in the lecture about these topics by doing the following lab, which is based on exploring and auditing a network using Nmap:

The purpose of today's laboratory exercise is to use **Nmap** (Zenmap is the official Nmap Gui) to do port scanning.

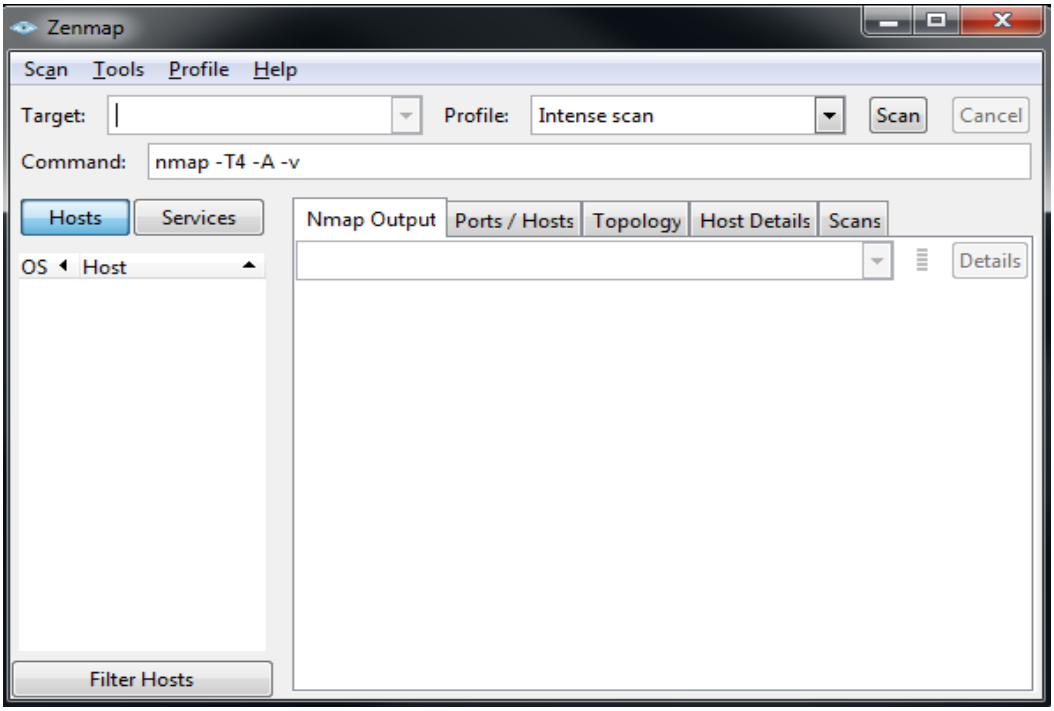
Following today's laboratory exercise you will be able to achieve the following:

- Scan TCP and UDP ports
- Analyse host details and their topology
- Determine the types of packets filters
- Record and save all scan reports
- Compare saved results for suspicious ports

Today's tasks:

1. Document all the IP addresses, open ports and closed ports, services, and protocols you discovered during the lab.

2. Launch Nmap (Zenmap)

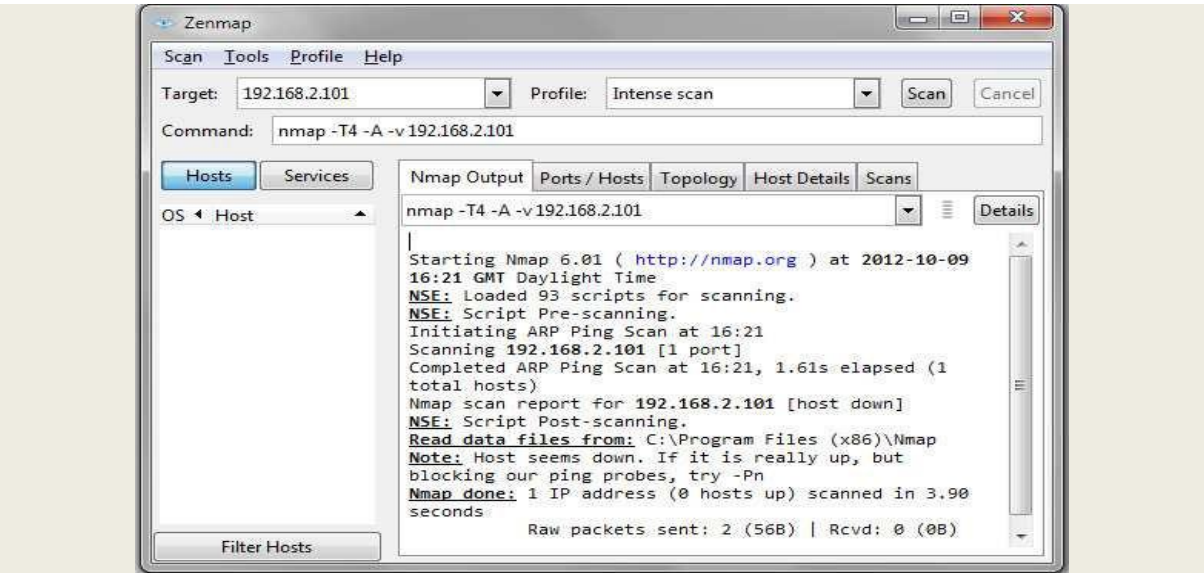


3. Enter the host Server IP Address (10.1.1.1) in the target: text field.You can perform a network inventory for the host machine.

4. In the Profile: text field, from drop-down list, select the type of profile you want to scan. For this lab, select Intense Scan.

5. Click scan to start scanning.

6. Nmap scans the provided IP address with Intense scan and display the scan results below the Nmap output tab.



7. Click on the Ports/Hosts tab to display more information on the scan results.

8. Nmap also displays the Port, Protocol, State, Service and Version of the scan.

9. Click the Topology tab to view Nmap's topology for the provided IP address in intense scan profile.

10. Click the Host Details tab to see the details of all hosts discovered during the intense scan profile.

11. Click the Scans tab to scan the details for provided IP addresses.

12. Now click the services tab located in the right pane of the window. This tab displays the list of services.

13. Click the http service to list all the HTTP Hostnames/ IP addresses, Ports, and their state (open/ closed)

14. Click the msrpc service to list of the Microsoft windows RPC.

15. Click the netbios- ssn service to list all NetBIOS hostnames.

16. Xmas scan sends a TCP frame to a remote device with URG, ACK,RST,SYN, and FIN flags set. FIN scans only with OS TCP/IP developed according to RFC 793. The current version of Microsoft Windows is not supported.

17. To perform Xmas Scan, you need to create a new profile. Click profile- New profile or Command Ctrl + P.

18. In the profile tab, enter Xmas Scan in the profile name text field.

19. Click the Scan tab, select Xmas Tree scan (-sX) from the TCP scans: drop-down list.

20. Select None in the Non-TCP scan: drop down and Aggressive (-T4) in the Timing template: and click save Changes.

21. Enter the IP address in the Target: field, select the Xmas scan option from the Profile: field and click Scan.

22. Nmap scans the target IP address provided and displays results in the Nmap Output tab.

23. Click the Services tab located at the right side of the pane. It displays all of the host services.

24. Click the Services tab, which lists all the host services.

25. Null scan works only if the operating system's TCP/IP implementation is developed according to RFC 793. In Null Scan, attackers send a TCP frame to a remote host with no flag.

26. To perform a Null Scan for a target IP address, create a new profile. Click profile- New profile or Command CTRL + P.

27. In the profile tab, input Null Scan in the Profile name text field.

28. Click the scan tab in the Profile Editor window. Now select the Null Scan (-sN) option from the TCP scan: drop down list.

29. Select None from the Non- TCP scan: drop-down field and select Aggressive (- T4) from the Timing template: drop - down field.

30. Click Save Changes to save the newly created profile.

31. In the main window of Zenmap, enter the target IP address to scan, select the Null Scan profile from the Profile drop -down list, and then click Scan.

32. Nmap scans the target IP address provided and displays results in the Nmap Output tab.

33. Click the Host Details tab to view the details of hosts, such as Hosts Status, Addresses, Open Ports, and Closed Ports.

34. Attackers send an ACK probe with a random sequence number. No response means the port is filtered, and an RST response means the port is not filtered.

35. To perform an ACK Flag Scan for a target IP address, create a new profile. Click Profile-New Profile.

36. In the Profile tab, input ACK Flag Scan in the Profile name text field.

37. To select the parameters for an ACK scan, click the Scan tab in the Profile Editor window, select ACK scan (-sA) from the Non-TCP scans: drop- down list, select None for all other fields but leave the Target: field empty.

38. Now click the Ping tab and check IPProbes (-PO) to probe the IP address and then click save changes.

39. In the Zenmap main window input the IP address of the target machine (in this lab 172.16.21.1) select ACK Flag Scan from Profile drop -down list, and click Scan.

40. Nmap scans the target IP address provided and displays results in Nmap Output tab.

41. To view more details regarding the hosts, click the Host Details tab.