Date

Page No.

Practical No: 6

Aim: Use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registers.

Relevant Course Outcome: Describe Ethical Hacking process and detect Network vulnerabilities.

Theoretical Background:

WHOIS is a protocol used to query databases that contain information about domain names and IP addresses. By querying WHOIS, it is possible to obtain information about the domain name owner, registration date, and contact details.

Dig (domain information groper) is a command-line tool used to query DNS Servers and obtain information about domain names, including IP addresses and DNS records.

Date

Page No.

Traceroute is a tool used to ~~query~~ ~~DNS~~ trace the path taken by packets from the source to the destination and identify any network issues.

Nslookup is another command-line tool used to query DNS servers and obtain information about domain names and IP addresses.

Implementation:

To gather information about a network or domain register using these tools, you can start by performing a WHOIS query to obtain information ~~a WHOIS~~ domain owner, registration date, and contact details. This information can be useful in identifying potential vulnerabilities and assessing the security posture of the target organization.

Next, you can use dig to obtain information about the domain name, including IP addresses and DNS records.

Date
Page No.

Traceroute can be used to identify the path taken by packets from the source to the destination and identify any network issues. This can help in identifying potential bottlenecks or routing issues that may impact the performance or security of the network.

Finally, nslookup can be used to query DNS servers and obtain information about domain names and IP addresses. This can be useful in identifying any potential misconfigurations or vulnerabilities in DNS infrastructure.

Network reconnaissance tools can be used in various scenarios, such as:

1. Network Security:

Network administrators and security professionals can use these tools to identify potential vulnerabilities and assess the security posture of the target network.

Date

Page No.

2. Troubleshooting Network Issues:

Network administrators can use tracer.

Conclusion: Thus, the use of reconnaissance tools like WHOIS, traceroute, nslookup to gather information about networks and domain registers is successfully performed.

Date

Page No.

Practical No: 7

Aim: Download and install nmap. Use it with different options to scan open ports, perform os fingerprinting, do a ping scan, tcp port scan, udp port scan, etc.

Relevant Course Outcome: Describe Ethical Hacking process and detect Network vulnerabilities.

Theoretical Background:

Nmap (Network Mapper) is a free and open-source tool used for network exploration, security auditing, and vulnerability scanning.

It is a command-line tool that allows users to scan hosts and services on a network, as well as perform advanced network reconnaissance.

Nmap uses various scanning techniques, including port scanning, version detection, os detection and network mapping, to gather information about the hosts and services on a network.

Here are the steps to download and use nmap for different types of scans:

1. Download and install nmap:

   link: https://nmap.org/download.html

   - Follow the installation instructions for your operating system.

2. Open the command prompt or terminal and navigate to the directory where nmap is installed.

3. To perform a ping scan, use following command:

   - 'nmap -sn <target_ip>'

   - This will scan the target IP address and check if it is up or not.

4. To perform a TCP port Scan, use the following command:

Date
Page No.

- 'nmap -sT <target_ip>'

- This will Scan the target IP address for open TCP ports.

5. To perform a UDP port Scan, use the following command:

- 'nmap -sU <target_ip>'

- This will Scan the target IP address for open UDP ports.

6. To perform OS fingerprinting, use following command:

- 'nmap -O <target_ip>'

- This will attempt to identify the operating system of target.

7. To Scan for all open ports, use the following command:

- 'nmap -p- <target_ip>'

Date

Page No.

-This will scan all possible ports on the target.

- Replace '<target_ip>' with the IP address or hostname of the target that you want to scan.

Conclusion: Installation of nmap is Successfully done.