Name: Aum Panchal

Reg No: 22BCE8203

Tools and Required Operating Systems

Guest Operating Systems (Virtual Machines)

To create a safe and controlled lab environment for conducting network analysis and simulating cyber attacks, two operating systems are deployed as guest machines using VirtualBox. These systems serve specific roles in the network setup.

1. Kali Linux

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is pre-loaded with numerous security-related tools such as Nmap, Hydra, Bettercap, and Yara, which are essential for ethical hacking and network testing. In this project, Kali Linux is used as the attacker machine for conducting network scans, spoofing attacks, phishing simulations, and brute-force attacks.

2. Windows 7

Windows 7 is used to simulate the victim machine in the network environment. Despite being outdated, it reflects the kind of legacy systems that are still found in many enterprise environments and are often targets of cyber attacks. This VM is used to observe the effects of attacks initiated from the Kali Linux machine and to capture relevant network traffic using Wireshark.

Tools Used in the Project

Below is a list of tools used in the project along with their descriptions and typical commands. These tools are instrumental in performing network discovery, traffic analysis, spoofing, phishing, brute-force attacks, and firewall configurations.

Nmap

Nmap (Network Mapper) is an open-source tool for network discovery and security auditing. It can be used to identify hosts and services on a network, thereby creating a 'map' of the network. Common scans include TCP SYN scan, OS detection, and service version detection.

- nmap -sS <target_ip> # TCP SYN scan
- nmap -O <target_ip> # OS detection
- nmap -sV <target_ip> # Service version detection

Maltego

Maltego is an open-source intelligence and forensics application. It offers graphical link analysis for gathering and connecting information for investigations. It is used to discover relationships between people, groups, websites, domains, and more.

- Launch from GUI: Applications -> Information Gathering -> Maltego
- Use transforms to gather OSINT on domains/IPs/emails

nslookup

nslookup is a network administration command-line tool used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping.

- nslookup <domain> # Basic DNS lookup
- nslookup -type=mx <domain> # Mail server lookup
- nslookup -type=ns <domain> # Name server lookup

Yara

YARA is a tool aimed at helping malware researchers identify and classify malware samples. It uses rules to find patterns in files or running processes.

- yara rule.yar <file> # Scan a file using a YARA rule
- yara -r rule.yar <directory> # Recursive directory scan

Hydra

Hydra is a very fast and flexible password cracking tool that supports numerous protocols to perform brute-force attacks.

- hydra -l admin -P passwords.txt ftp://<target_ip>
- hydra -V -f -l root -P /usr/share/wordlists/rockyou.txt ssh://<target_ip>

Zphisher

Zphisher is an advanced phishing toolkit used to simulate phishing attacks. It automates phishing site hosting and URL generation.

- ./zphisher.sh
- Choose a phishing template like Facebook or Instagram
- Send the link to a target and capture credentials

pfSense

pfSense is an open-source firewall/router software distribution based on FreeBSD. It provides a web interface to configure firewall rules, NAT, VPN, and traffic shaping.

- Access via browser: http://192.168.1.1
- Configure firewall and NAT rules, monitor traffic

Bettercap

Bettercap is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network. It can also be used for network reconnaissance and packet sniffing.

- bettercap -iface <interface> # Start Bettercap
- net.probe on; net.recon on # Discover hosts
- set arp.spoof.targets <target_ip>; arp.spoof on # Launch ARP spoofing