WINDOWS DEFENDER

AIM: To Prevent PC against latest threats using Windows Defender.

DESCRIPTION : Microsoft Defender for Endpoint (formerly Windows Defender Advanced Threat Protection) is a post-breach security solution that helps detect, investigate, and respond to threats within a network. Unlike traditional antivirus software, it complements antivirus tools by focusing on post-attack analysis and remediation. It continuously monitors endpoints to identify vulnerabilities, provides exposure scores, and recommends fixes. Through attack surface reduction, it limits potential entry points for cyberattacks by restricting untrusted applications, websites, and files. Using Microsoft's advanced machine learning and cloud-based protection, it offers next-generation defense against emerging threats. Its endpoint detection and response (EDR) features deliver real-time alerts, detailed investigations, and guided remediation steps, all accessible through a centralized dashboard for effective threat management.

PROCEDURE :

1. Open **Windows Security** from **Start menu**
2. Go to **Virus and threat protection** and use **quick scan**
3. To enable protection, click on **manage settings** and turn on **real-time protection**
4. Enable **Cloud - delivered protection** and click on **check for updates** to check for updates
5. Enable **automatic sample submission** for advanced threat detection
6. Run a **full scan**
7. Take required actions on **threats**, if any have occurred

NMAP AIM : To familiarize network discovery and security auditing using Nmap

DESCRIPTION : Nmap (Network Mapper) is a free, open-source tool used for network discovery and vulnerability scanning. It helps network administrators identify live hosts, open ports, running services, operating systems, and potential security risks by sending specially crafted IP packets and analyzing their responses. The results include detailed information such as port numbers, protocols, service names, and their states (open, closed, filtered, or unfiltered). **Key features of Nmap** include **Host Discovery** (identifying active devices on a network), **Port Scanning** (finding open ports on target hosts), **Version Detection** (determining the application name and version running on network services), and **OS Detection** (identifying the operating system and hardware details). As an active information-gathering tool, Nmap performs several scanning steps—finding live machines, discovering open ports, scanning beyond intrusion detection systems (IDS), and identifying vulnerabilities—to locate exploitable communication channels and strengthen network security.

PROCEDURE: Open the Terminal in Kali Linux OS and type nmap.

STEP 1: FIND LIVE MACHINES , Ping Sweep/Scan (-sP) is used to find live machines from a range of IP addresses. It sends ICMP echo request to multiple machines.
Command: nmap –Sp<targetip>

STEP 2: DISCOVER OPEN PORTS, In computer networking, a port is a communication endpoint.
Command: nmap –p<port> -v<target>

a)TCP Connect Scan [-sT]
Introduction: TCP Connect scan detects open ports by **three way handshake**. It is also referred as **FULL OPEN Scan**. **Command:** nmap -sT <target> **For example:** nmap -sT 172.16.4.51

b) SYN Stealth Scan [-sS]
Introduction: It is based upon **TCP handshake**. It is also referred as **HALF OPEN Scan**. In this type of scan, Nmap sends SYN packet:

- If port is open - it responds with **ACK**.
- If port is closed - it responds with **RST**.
- If port is filtered - it simply drops **SYN packet**.

Command: nmap -sS -A -O <target> -p <port> (where **-A** is Aggressive scan, **-O** is operating system)

c) UDP Scan [-sU]
Introduction: This type of scan is used to scan **UDP ports**. Nmap sends the **0 byte UDP packets**. If source receives an **ICMP Port Unreachable message**, then the Port is closed.

STEP 3: SCANNING BEYOND FIREWALL, : Nmap provides feature to control time options– [-T]. The timings are: Paranoid [-T0], Sneaky [-T1], Polite [-T2], Normal [-T3], Aggressive [-T4], and Insane [-T5].
Command: nmap -T[0-5] [target]

STEP 4: IDENTIFY VULNERABILITIES, After finding the open ports and services running on it, this step identifies the vulnerabilities associated with the open ports.
Command: nmap -p 445 --script=smb-vuln*<target>

STEGANOGRAPHIC TOOLS , AIM :To hide the secret data from unauthorized users in order to prevent confidentiality,integrity and availability of data.

STEGHIDE ,

DESCRIPTION Steghide is a free steganography program that allows you to hide secret files inside other files. Steganography means concealing information within something else. Steghide works by embedding your hidden data within an audio, image, or video file. To anyone else, this carrier file will look and sound normal. But it secretly contains your encrypted message or file. The Steghide tool lets you easily embed your hidden information and extract it again with a password. This provides a way to securely transmit messages or sensitive data over public networks or any system where privacy is needed.

PROCEDURE:

a. **Installation & Usage To use Steghide,** you first need to install it in Kali Linux. You can do this easily by typing the following command :

Command : sudo apt-get install steghide

- Steghide is controlled completely through the terminal command line interface in Kali Linux. To start using it, simply open a terminal window and type :
  Command : steghide
- Create a text file called " secret.txt " and add some simple secret message text to it. Save it in your working directory. Also place the image file you want to use to hide the data, like " gfg.jpg ", in the same folder. Open a terminal window and use the " steghide embed " command to embed " secret.txt " into " gfg.jpg ".
  Command : steghide embed -ef Secret.txt -ef gfg.jpg

It will ask you to create a password. Choose a strong password and enter it. This will be needed to extract the hidden data later. **Steghide** will embed "**secret.txt**" inside "**kevinmitnick.jpg**" using the password encryption .

Now the image file contains the secret data entirely hidden within it. You can safely share or store the image file like normal. When ready, use the following below command with the password to retrieve the embedded "**Secret.txt**" file.
Command: steghide extract -sf gfg.jpeg cat Secret.txt

You can also have **Steghide** show info about any files with embedded data. The below command will verify if a file has hidden content inside it:
Command: steghide info gfg.jpg

B. STEGOSUITE

DESCRIPTION StegoSuite is another free steganography program included in Kali Linux. It offers several steganography techniques in one toolkit. StegoSuite lets you hide information within images and audio files, just like Steghide. But it also includes additional steganography methods like hiding data in video files, OpenOffice documents, HTML web pages, and PDF files. The goal of StegoSuite is to provide an all-in-one steganography tool with many different hiding techniques. This gives users more options to conceal messages or files. Like Steghide, StegoSuite aims to securely embed secret data so it can't be detected by others. The carrier files look harmless, but they secretly hold encrypted messages.StegoSuite provides an easy-to-use interface and wizard for beginner users to start applying steganography. With both Steghide and StegoSuite, Kali Linux is well-equipped for basic steganography tasks.

PROCEDURE:

a. Installation & Usage StegoSuite is another free steganography tool included in Kali Linux. The main difference from Steghide is that StegoSuite provides a graphical interface, making it more user-friendly. To install StegoSuite, open a terminal and type :
Command : sudo apt-get install stegosuite

Once you have installed the StegoSuite package in Kali Linux, you can easily start using the program. Now you just need to type the following command to Launch the StegoSuite Tool**.**
Command: stegosuite gui

After that Click the " Browse Files " button and select the image you want to use to hide the text.

After Selecting the Image file Enter the secret text Message or Just Drag and Drop the " Secret.txt " file. Then Set the Password to Encrypt the Image file and Click on Embed. Follow the Steps as Shown in the Below GIF file.

After that you will see this New file created on the Desktop name " gfg_embed.png " this file include our hidden file in it.

Now the image file contains the secret data entirely hidden within it You can safely share or store the image file like normal. Whenever you want to see the Hidden Text file just use " stegosuite gui " Command and Select the New File that created onto our Desktop and Just type the Password and hit the Extract Button.

WIRESHARK

AIM: To provide deeper understanding of Network Protocol Analysis using Wireshark

DESCRIPTION : Wireshark is a free, open-source packet analyzer (a "sniffer" or network protocol analyzer) used for education, protocol development, network troubleshooting, and security analysis. It captures and inspects network traffic—putting the network interface into promiscuous mode to collect packets—and lets users filter and analyze communications between devices to troubleshoot latency, dropped packets, or malicious activity. Similar to tcpdump but with a graphical interface and richer filtering/sorting, Wireshark helps network and security engineers observe traffic flows, identify problems, and investigate attacks. Because switches may not forward all traffic to a single port, extended capture techniques such as network taps or port mirroring (sending copies of packets from one port to another) are often used to view traffic across a network.

Features of Wireshark:
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It is also useful in VoIP analysis.

1. Opening Wireshark:
   - Launch the Wireshark application on the system
2. Selecting an Interface
   - From the Wireshark interface, select the **NIC** (Network Interface Card) where packets are deployed
2. Observing Captured Packet
   - Note down the different types of packets shown in the **Capture** window
   - Some packets may be highlighted in different colours
   - Take screenshots of packets with different colours for reference
3. Capture and Stop options:
   - Explore the **Capture** menu and note the available options
   - Use the **Stop Capture** icon to end the capture process
4. Modifying Colouring rules:
   - Go to **Edit Preferences Appearance Colouring Rules**
   - Explore or change the default colouring rules to customize how different packets are displayed
5. Viewing I/O Graphs:
   - Navigate to **Statistics I/O Graphs** to view the graphical representation of captured traffic

   Exp: i) Filter: **ip.addr == 192.168.1.6** * This will filter only display packets where the **IP address 192.168.1.6** appears where the source or the destination.
   The IP address **192.168.1.6** appears where the source or the destination.
   ii) Filter: **ip.addr == 192.168.1.6 && ssdp** * This filter will show only **SSDP packets** where the source or destination is **192.168.1.6**
   iii) Filter: **ip.addr == 192.168.1.6 && !mdns** * This filter will display all packets involving **192.168.1.6** except **mDNS packets**
   iv) Filter: **ip.addr == 192.168.1.6 or udp** * This filter will display all packets involving **192.168.1.6** plus all **UDP packets** from anywhere
6. Saving/Documenting Results:
   - Save the **Capture file** if needed for further analysis

HTTRACK

AIM: To familiarize the cyber forensic tool httrack

DESCRIPTION: HTTrack is an easy-to-use offline browser utility. It allows you to download a World Wide Website from the Internet to a local directory, building recursively all directories, getting html, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online. HTTrack can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system. WinHTTrack (Windows release of HTTrack) and WebHTTrack (Linux/Unix release of HTTrack) are very similar, but not exactly identical. You may encounter minor differences (in the display, or in various options) between these two releases. The engine behind these two release is identical.

Procedure:

1. Open **HTTrack Website Copier**
    - Launch the **HTTrack** app from the system.
2. Create a New Project
    - Click on **Next**
    - Enter the **Project Name**
    - Optionally, enter a **Category** and select the **base path**.
    - Click **Next**
3. Enter Website URL
    - In the web address field, type / paste the desired **website address**.
    - If required, **multiple URLs** can be added.
    - For normal use, leave defaults.
    - Click **Next**
4. Set Preferences (optional)
    - You can adjust settings such as **download limits, filters**, or **proxy** if needed.
    - For normal use, leave defaults.
    - Click **Next**
5. Start Mirroring
    - Click **Finish** to begin the Website Copying.
    - **HTTrack** will start downloading and will show progress.
6. View the Mirrored Website
    - Once completed, **HTTrack** will provide an option to browse the **mirrored website**.
    - This opens a **duplicate local version** of the site in your browser.
7. Close / Exit
    - After verification, close the application.

WPScan AIM: To learn how to use WPScan to identify security vulnerabilities, enumerable users, and check for weak components (themes and plugins) in a target WordPress installation.

DESCRIPTION: WordPress is one of the most popular content management systems (CMS) on the internet. With its extensive plugin ecosystem and user-friendly interface, it powers a significant portion of websites across the globe. However, like any software, WordPress is not immune to security vulnerabilities. WPScan is a widely used WordPress vulnerability scanner. It's designed to help security professionals, developers, and website administrators identify security weaknesses in WordPress installations. WPScan leverages a database of known vulnerabilities, enumerates installed plugins and themes, and checks for misconfigurations. By regularly scanning your WordPress website, you can stay one step ahead of potential attackers and maintain a secure online presence.

Procedure:

How to use WPScan:

Note: For practical use in a lab, always target a legal, controlled environment.

1. Update the WPScan Vulnerability Database:

Before running any scan, ensure your database is up-to-date to check against the latest threats.

→ wpscan --update

2. Basic Vulnerability Scan:

This command performs a simple scan, checks the WP version, and attempts to detect known vulnerabilities in the core, plugins, and themes.

wpscan --url http://TARGET_WP_SITE/DOMAIN

3. Enumerating Users (-e u):

This is a a critical step for attackers as usernames are often the first part of a login credential needed for brute forcing.

→ wpscan --url http://TARGET_WP_SITE/DOMAIN --enumerate u

4. Enumerating Vulnerable Plugins (-e vp):

This command specifically looks for plugins that have known, documented vulnerabilities.

wpscan --url http://TARGET_WP_SITE/DOMAIN --enumerate vp

5. Full Aggressive Scan (Optional):

Use this to combine enumeration of usernames, plugins, and themes for a comprehensive report:

wpscan --url http://TARGET_WP_SITE/DOMAIN --enumerate u,vp,t

Result:

The tool WPScan was studied, analyzed and familiarized.

Nikto AIM: To understand and utilize Nikto to perform a basic web server scan, identify common server misconfigurations, and locate dangerous files or outdated software on a target web service.

DESCRIPTION: Nikto is a widely used, highly efficient, and flexible web server scanner that aids cybersecurity professionals, system administrators, and penetration testers in identifying and addressing potential security risks within web servers. Developed by Chris Sullo, this open-source tool is designed to uncover various security issues, such as outdated software, configuration errors, and potential vulnerabilities within web servers and web applications.

Procedure:

1. Basic Web Server Scan:

The most common command runs a default, comprehensive test against the target on standard HTTP port 80.

→ nikto -h http://TARGET_IP_OR_DOMAIN

eg: nikto -h http://kobu.co

2. Scanning a Specific Port:

If the web service is running on a non-standard port (eg: 8080), you must specify it using the -p flag.

→ nikto -h http://TARGET_IP_OR_DOMAIN -p 8080

eg: nikto -h http://kobu.co -p 8080

3. Scanning HTTPS (SSL/TLS) Enabled Sites:

Use the -ssl flag to force Nikto to scan over HTTPS instead of HTTP.

→ nikto -h https://TARGET_IP_OR_DOMAIN -ssl

eg: nikto -h https://kobu.co -ssl

4. Scanning a Specific Directory (CGI Directory Scan):

This command scans for CGI vulnerabilities in specified directories.

→ nikto -h http://TARGET_IP_OR_DOMAIN -Cgidirs

eg: nikto -h http://kobu.co -Cgidirs

5. Saving the Output to a File:

It's helpful to save the scan results for later analysis using the -o (output) flag.

→ nikto -h http://TARGET_IP_OR_DOMAIN -o FILENAME

eg: nikto -h http://kobu.co -o out.txt

John The Ripper AIM: To practice extracting password hashes and using John the Ripper (JTR) to crack them using both the built-in single mode and external Dictionary attack mode.

DESCRIPTION: John the Ripper is an open-source password security auditing and recovery tool. John the Ripper begins by reading password hashes from an input file. The tool's detection engine automatically identifies the hash format, though you can also specify the format manually. Based on your selected attack mode—such as a wordlist or incremental brute-force— the core engine generates password candidates. Each candidate is then hashed and compared against the target hashes. A successful match is logged, and the process continues until all candidates are checked.

Procedure:

1. Run Default Cracking Modes:

This is the simplest command. JTR automatically identifies the hash type and runs its default combination of single, wordlist, and incremental modes.

→ john hashfile.txt

2. Dictionary Attack (Wordlist Mode):

This is the most effective attack for weak passwords. It requires specifying a path to a wordlist.

→ john --wordlist=/usr/share/wordlists/rockyou.txt hashfile.txt

3. Specify Hash Format:

If JTR can't automatically detect the hash type, you may need to specify the format (eg: NTLM or Raw-MD5).

→ john --wordlist=/usr/share/wordlists/rockyou.txt hashfile.txt --format=Raw-MD5

4. Resuming an Interrupted Session:

If you stop the cracking process (eg: pressing Ctrl+C), you can resume it later.

→ john --restore