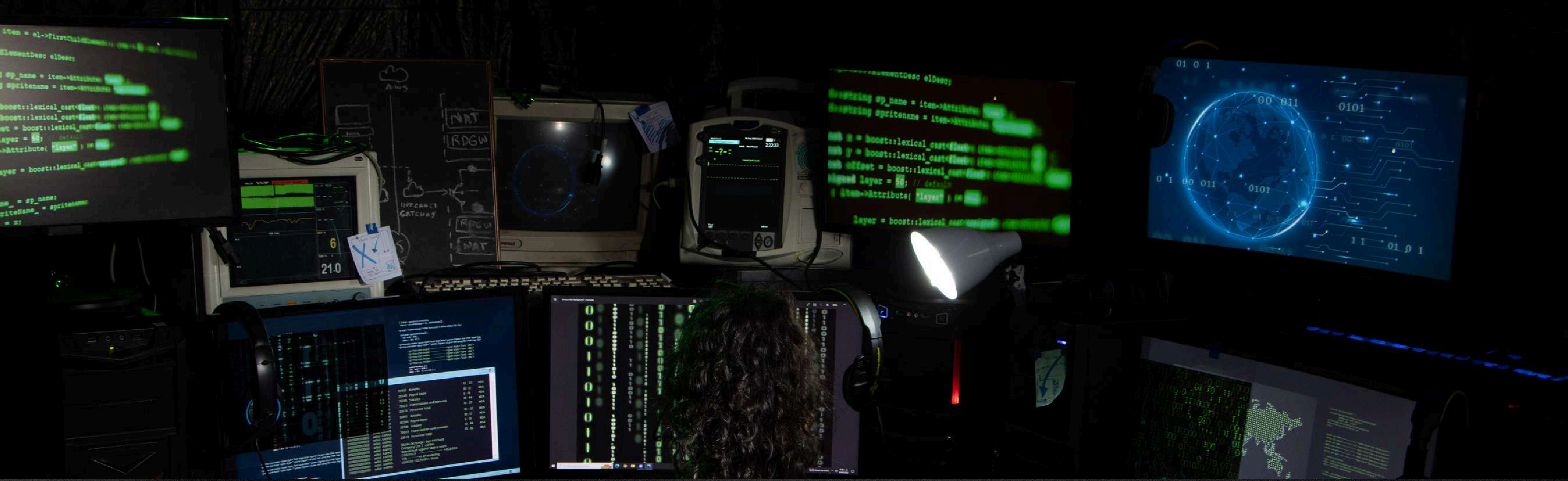
PAVAN SAXENA

IM ROOTKID



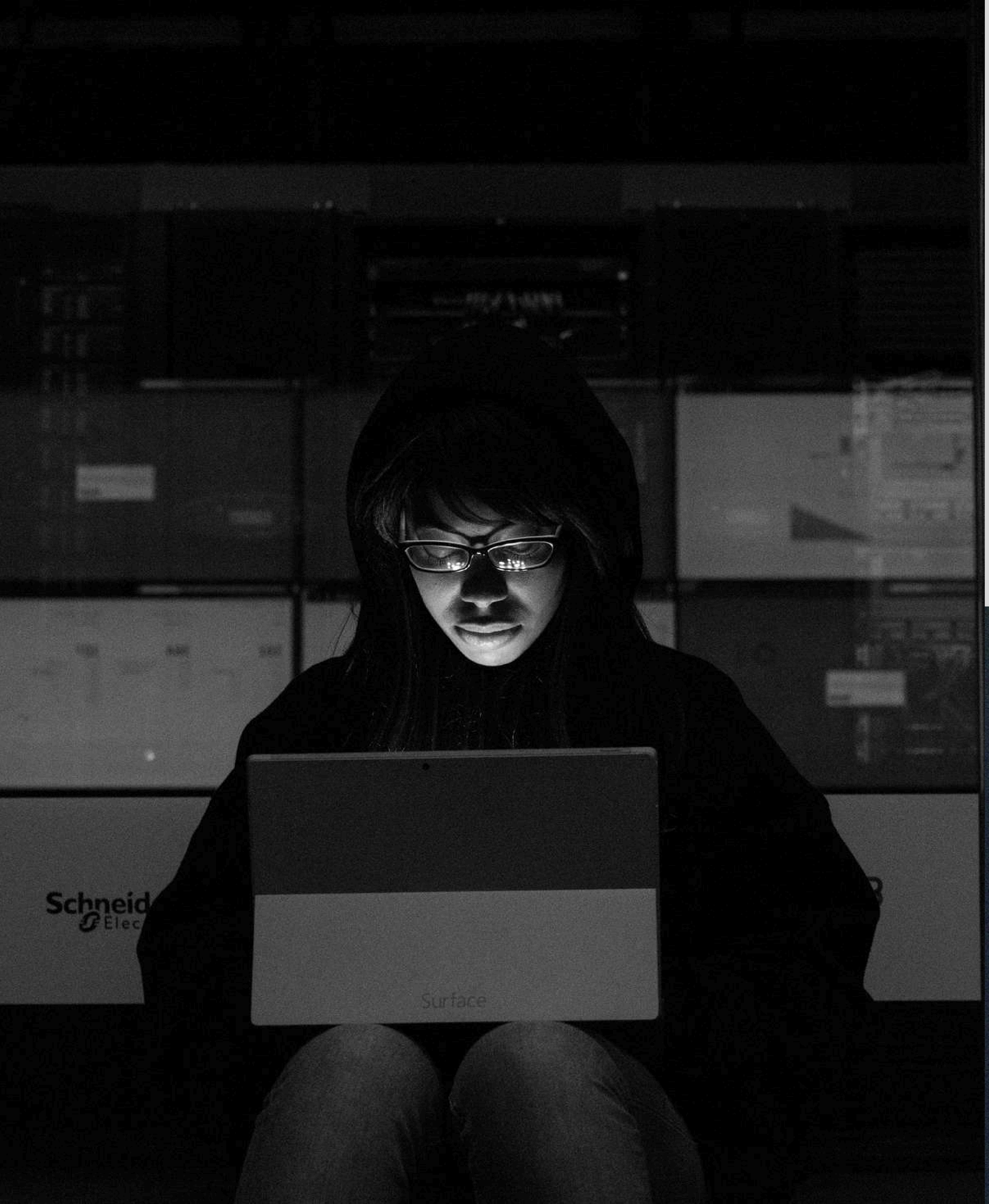
HACK THE NETWORK: POST-EXPLOITATION AND THE ART OF PIVOTING

AGENDA

- Discussions on Post-Exploitation
- Discussions on Network Pivoting
- Tools & Techniques
- Q&A

AUDIENCE CHECK

Let's see who the real hackers are in the room :)



WHAT IS POST-EXPLOITATION

POST-EXPLOITATION

Post-Exploitation is the phase after an attacker gains access to a system.

It focuses on:

- Maintaining access
- Privilege escalation
- Lateral movement

MAINTAINING ACCESS

Create Backdoors:

Use remote access tool (e.g., Netcat, Meterpreter)

Establish Persistence Mechanisms:

Registry edits (Windows) or Cron jobs or rc.local (Linux)

Create Additional User Accounts:

Add hidden admin accounts or Change existing credentials or SSH keys

Encrypted Communication Channels

Use HTTPS, SSH, or VPN tunnels

Technique	Tools & Utilities
Create Backdoors	- **Netcat** (nc, ncat) – simple reverse shell
	- **Metasploit (Meterpreter)**
	- **Cobalt Strike**
	- **Plink** (from PuTTY)
Establish Persistence Mechanisms	- **Metasploit Persistence Module**
	- **Empire** (PowerShell agents)
	- **Scheduled Tasks (schtasks)**
	- **Registry scripts / WMI**
Create Additional User Accounts	- **net user** / **net localgroup** (Windows)
	- **useradd** / **passwd** (Linux)
	- **Metasploit**'s add_user script
Set Up Encrypted Channels	- **OpenSSH / Reverse SSH**
	- **Ncat with SSL**
	- **Cobalt Strike HTTPS Beacon**
	- **Chisel** (TCP tunneling)
	- **Ngrok** (Quick HTTPS tunnels)
	- **Iodine / DNSCat2** (Covert tunneling)

PRIVILEGE ESCALATION

Privilege Escalation is the process of exploiting a flaw, misconfiguration, or vulnerability to gain higher-level permissions (like admin or root) on a system or network than initially granted.

PRIVILEGE ESCALATION

System Enumeration

OS, users, groups, permissions

Misconfigurations

Weak permissions, exposed services

Exploitation

Unpatched software or kernel flaws

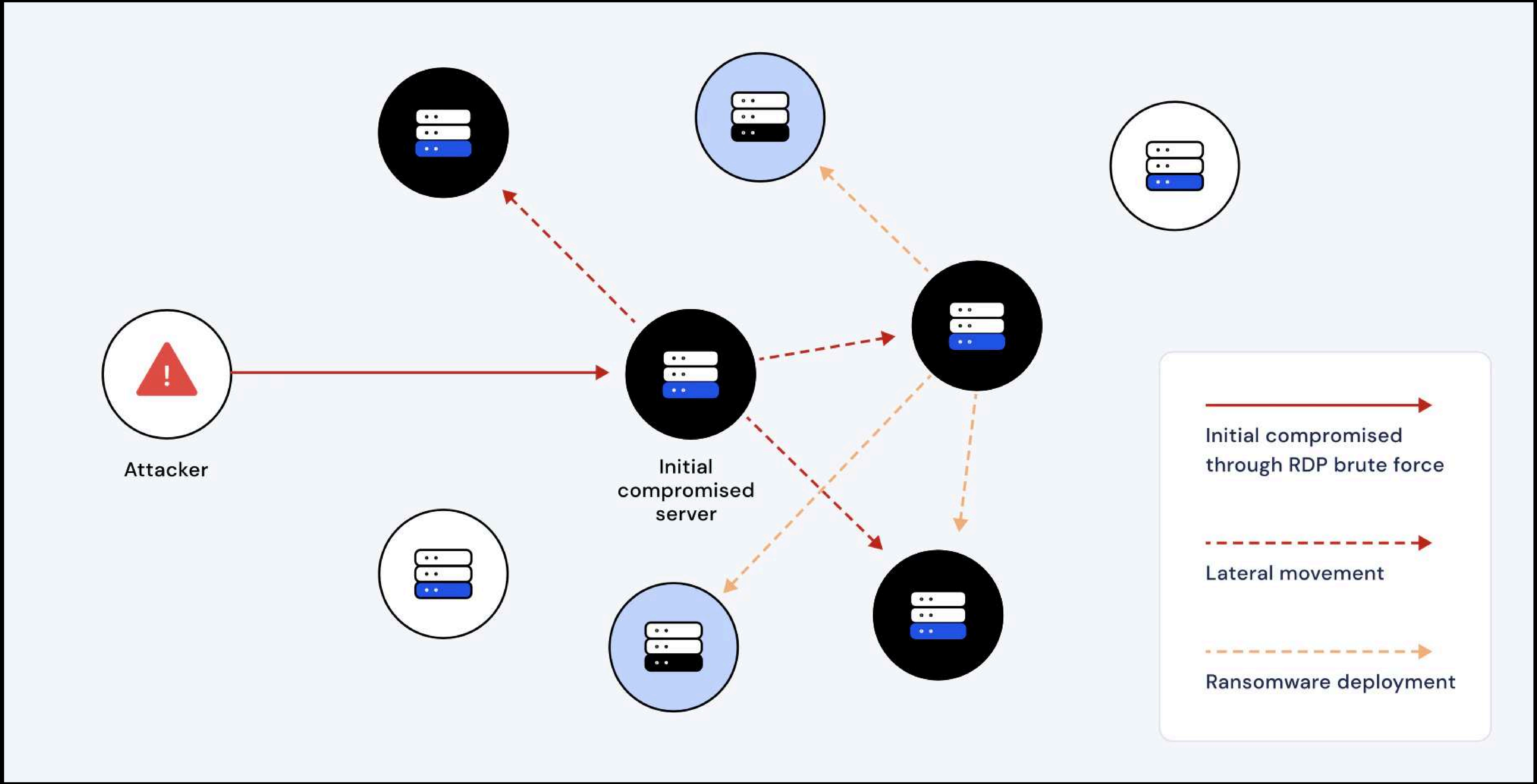
Credential Access

Password dumps, token stealing

I have a detailed presentation on privilege escalation for Linux systems, which you can find hosted on my GitHub.

LATERAL MOVEMENT

Lateral Movement is when an attacker moves from one system to another inside a network after getting initial access.


Attacker
Initial compromised server
Initial compromised through RDP brute force
Lateral movement
Ransomware deployment

LATERAL MOVEMENT

Credential Theft

Use tools like Mimikatz to steal usernames & passwords.

Pass-the-Hash / Pass-the-Ticket

Reuse stolen credentials to access other systems.

Active Directory Abuse

Query AD for target systems/users using BloodHound or ADFind.

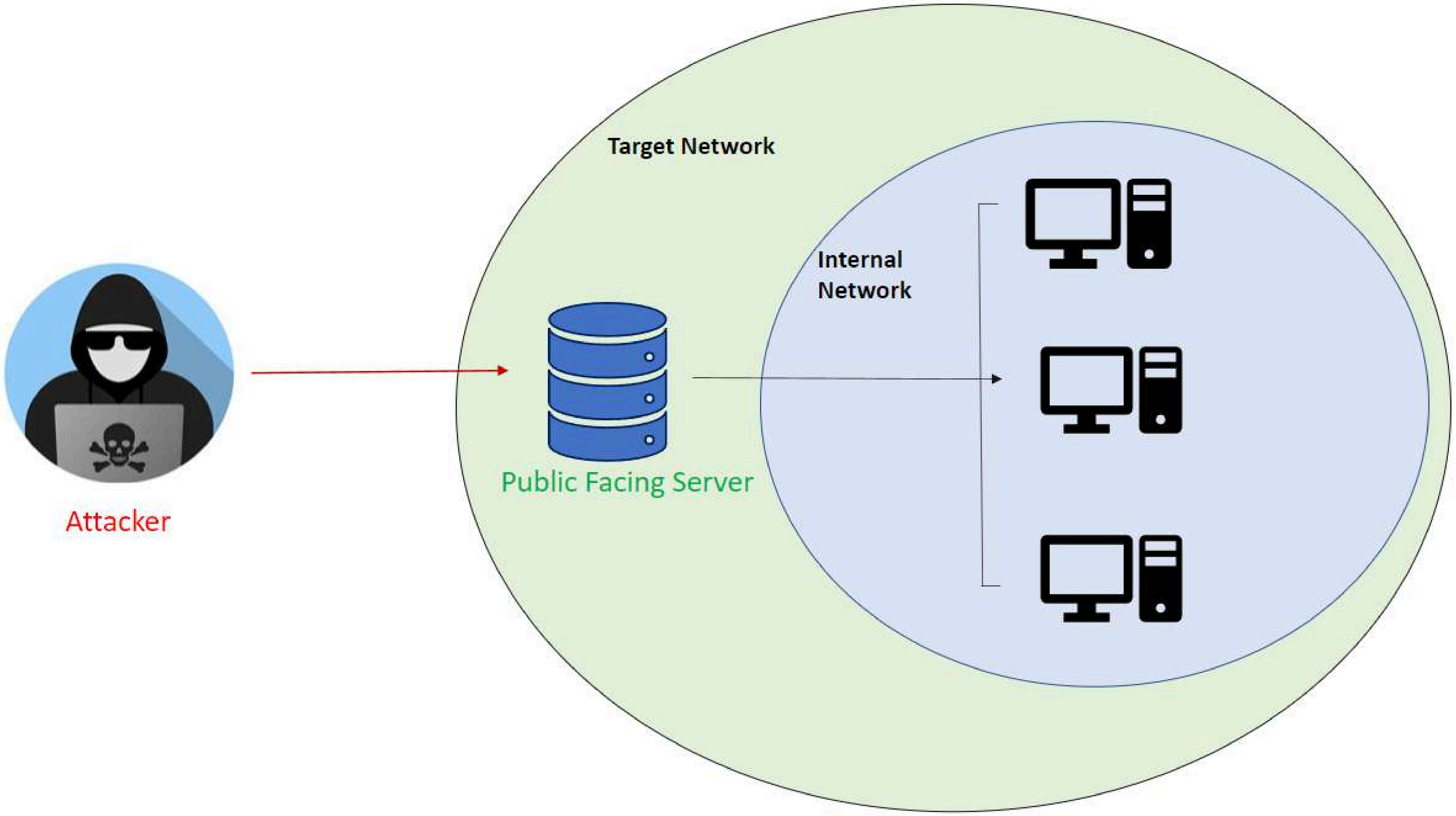
Exploiting Trust Relationships

Abuse shared drives, domain trust, or open SMB shares.

THE ART OF PIVOTING

WHAT IS PIVOTING?

Pivoting is a technique used to route traffic through a compromised system to access otherwise unreachable (internal) systems — usually in a different network segment or behind a firewall.


Target Network
Internal
Network
Attacker
Public Facing Server

PIVOTING

Port Forwarding

Redirects traffic from one port to another through a compromised system to access internal services.

SSH Tunneling

Creates secure encrypted tunnels (using SSH) to forward ports or entire sessions into a private network.

Meterpreter's route

Adds internal network routes in Metasploit to pivot traffic through an active Meterpreter session.

SOCKS Proxies (ProxyChains)

Chains your tools (like Nmap, curl) through a SOCKS proxy on a compromised host to reach internal systems.

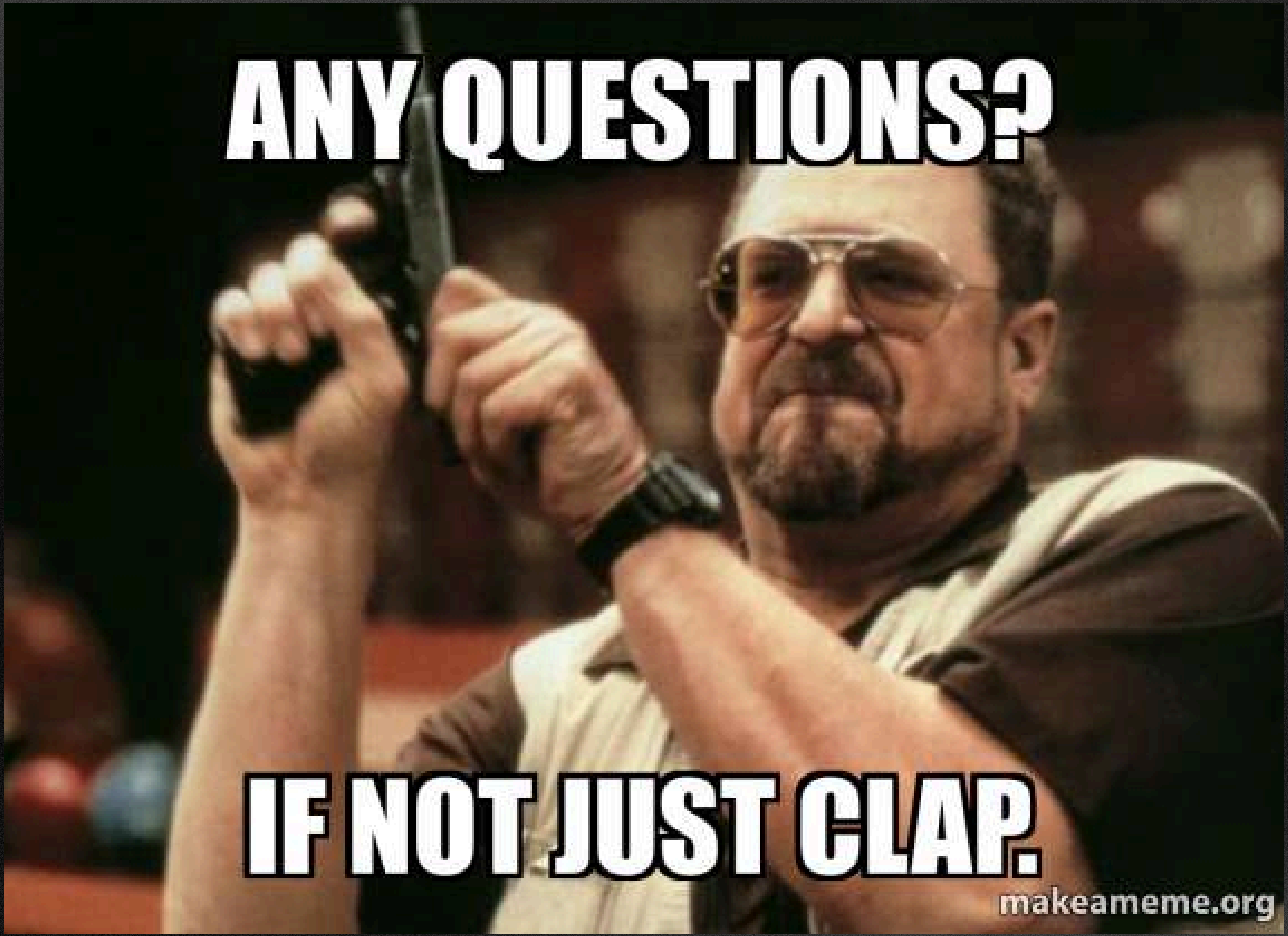
TOOLS

- Metasploit Framework
- Empire
- WinPEAS / LinPEAS
- PowerUp
- GTFOBins
- SudoKiller
- CrackMapExec
- Impacket toolkit
- ProxyChains
- SocksCap / Proxifier
- Plink
- PsExec (SysInternals)

PRACTICAL LABS

Topic	TryHackMe Machines / Rooms	Hack The Box Machines / Labs
Maintaining Access	- Post-Exploitation Basics- Threat Hunting: Foothold- Linux Incident Surface	- RastaLabs- Cybernetics- APTLabs
Privilege Escalation	- Linux & Windows Privesc Modules (THM Paths)- APT28 Inception Theory	- Lame (Linux)- Retired (Windows)- Zephyr, Orion, RPG (Pro Labs)
Lateral Movement	- Lateral Movement & Pivoting- Blizzard- XDR: Lateral Movement- Ctlister	- Orion- Alchemy- FullHouse- Hades (Pro Labs)
Pivoting	- Same as lateral movement (pivot labs included)- AD Module Rooms	- Pivoting & Port Forwarding (HTB Academy)- P.O.O, Orion (Pro Labs)

ANY QUESTIONS?


ANY QUESTIONS?
IF NOT JUST CLAP.
makeameme.org

CONNECT WITH ME:

THANK YOU
YOU'RE AWESOME