CWL
CyberWarFare Labs

Active Directory Breached

Lateral Movement & Privilege Escalation

ABOUT CYBERWARFARE LABS

:

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

- Niche Cyber Range Labs
- Continuous Learning : Infinity Platform

About Speaker

Subhash Murugan

(Security Researcher)

He is deeply interested in Red Team operations, Active Directory security, Windows privilege escalation, and network attack techniques. In his free time, he enjoys studying adversarial TTPs, developing attack simulations, and experimenting with new tools in his personal homelab.

What is Active Directory (AD)?

Active Directory (AD) is Microsoft's centralized identity and access management system.

- User authentication
- Computer authentication
- Permissions & access
- Group Policies
- Network resources

Why Attackers Target AD

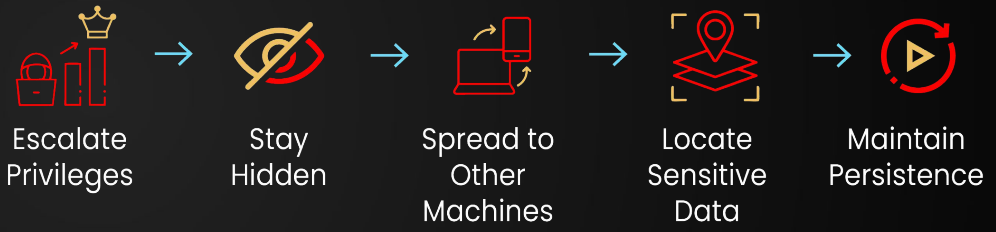
Attackers want AD access because it provides:

- Centralized authentication
- Control over all machines
- Access to domain admin privileges
- Ability to disable security tools
- Long-term persistence potential

What is Post-Exploitation?

The phase after attackers gain initial access.

- Escalate privileges
- Stay hidden
- Spread to other machines
- Locate sensitive data
- Maintain persistence



Why Privilege Escalation Matters

Privilege escalation allows them to:

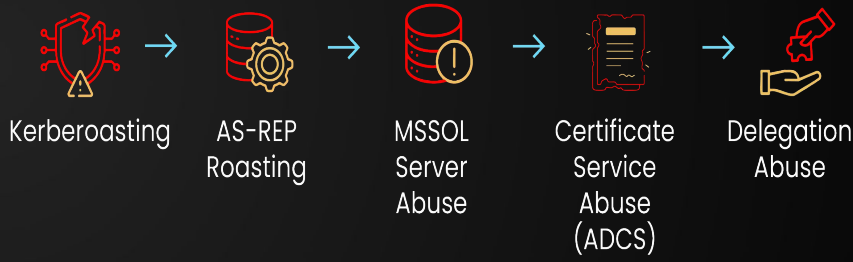
- Disable security tools
- Access confidential data
- Execute commands everywhere
- Control servers
- Become Domain Admin

Types of Privilege Escalation

1. Local Privilege Escalation (LPE)
   - From normal user → SYSTEM
   - Happens on a single machine
2. Domain Privilege Escalation (DPE)
   - From domain user → Domain Admin
   - Happens at AD level

Common Local Privilege Escalation Techniques

- Weak service permissions
- DLL hijacking
- Token impersonation (Potato attacks)
- Stored credentials
- Browser password dumping
- Kernel exploits
- Misconfigured scheduled tasks



Common Domain Privilege Escalation Techniques

- Kerberoasting
- AS-REP Roasting
- Weak ACL permissions
- MSSQL server abuse
- Certificate Service abuse (ADCS)
- Delegation Abuse

What is Lateral Movement?

Moving from one system to another inside the network.

- Reach Domain Controller
- Access mail servers
- Get to file/database servers
- Pivot into restricted subnets

Lateral Movement Techniques

- Pass-the-Hash
- Pass-the-Ticket
- Overpass-the-Hash
- WinRM / WMI / PsExec
- SMB Exec

What is ADCS (Active Directory Certificate Services)?

ADCS provides certificate-based authentication for:

- Users
- Computers
- Services
- VPN / Wi-Fi
- HTTPS

ADCS Vulnerabilities (ESC1–ESC8)

ESC1	User-Supplied Subject + ClientAuth
ESC2	Misconfigured Certificate Manager Approval
ESC3	Weak CA Permissions
ESC4	ESC1 + PKINIT
ESC5	Delegation Abuse
ESC6	Enrollment Agent Misuse
ESC7	Enterprise CA Misconfigurations
ESC8	Certificate Template Vulnerabilities

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **cyberwarfare.live**