TRAINING NAME: Hacking Active Directory: Detecting and Mitigating Compromises

DURATION: 5 days

## TRAINING OVERVIEW:

The training starts by building a complete hands-on lab from scratch. Participants configure Windows 11 to run Hyper-V, then create virtual machines for Windows Server 2019, Windows Server 2022, Windows Server 2025, Windows 11, a Wazuh SIEM server on Ubuntu, and a Kali Linux attacker machine. They install Wazuh agents on the domain controller and the Windows 11 client, and finish with a final preparation phase so that all machines are ready for the attack exercises.

With the lab in place, participants work through the main Active Directory attack paths, from initial access to domain compromise and persistence, using the LSHIFT methodology (Learn, Scan, Hack, Identify hacking attempt, Fix it, Test the fix). Covered techniques include poisoning and relaying, AS-REP roasting, Kerberoasting, password spraying, Group Policy Preferences password exposure, MachineAccountQuota abuse and unconstrained delegation, Pass-the-Hash, Pass-the-Ticket, Golden Ticket and Silver Ticket, DCSync, Skeleton Key, AD CS misconfigurations (E1 to E13) and Golden Certificate attacks, one-way domain trust compromise with SID History abuse, and Microsoft Entra Connect and Golden SAML compromise. For each technique, participants study how the attack works and how to mitigate it, scan the environment to find the weakness, exploit it, identify the attack in the logs and SIEM, apply the fix, and verify that the attack no longer works.

Participants use tools like Nmap for scanning, NetExec for domain enumeration and abuse, Hashcat for offline hash cracking, Bloodhound for AD enumeration, Responder and ntlmrelayx for poisoning and relaying, Mimikatz and Rubeus for ticket and credential attacks, Certipy for AD CS abuse, etc, including Wazuh for attack detection and confirmation. Because every module is built around both attack and defense, participants leave with a repeatable process for finding, proving, detecting, and closing Active Directory weaknesses. The lab VMs remain available after the training so participants can keep practicing.

## KEY LEARNING OUTCOMES:

- Build a functional Active Directory attack and defence lab using Hyper-V, Windows Server, Windows 11, and Kali Linux.
- Deploy and configure Wazuh (server, components, and agents) to monitor domain controllers and Windows clients.
- Perform poisoning and relaying attacks and understand how to disable the protocols that enable them.
- Enumerate users and perform password spraying against an Active Directory domain.
- Execute AS-REP roasting and Kerberoasting attacks and crack the resulting hashes with hashcat.
- Recover credentials from Group Policy Preferences and understand why they are insecure.
- Exploit MachineAccountQuota and unconstrained delegation misconfigurations and understand how to remediate them.
- Abuse domain privileges with NetExec and detect Pass-the-Hash activity.
- Perform Pass-the-Hash and Pass-the-Ticket attacks and understand the conditions that enable them.
- Forge Golden Ticket and Silver Ticket tickets and understand how they provide persistence.

- Perform DCSync attacks and deploy a Skeleton Key and understand the conditions that enable them.
- Identify and exploit AD CS misconfigurations (E1 to E13) and abuse a stolen CA key to forge Golden Certificates.
- Compromise a one-way domain trust and abuse SID History to escalate privileges across domains.
- Identify weaknesses in Microsoft Entra Connect and Golden SAML attacks against federated identity.
- Detect each attack in Windows event logs and Wazuh alerts.
- Apply and test fixes for each vulnerability using the LSHIFT methodology.

## THIS TRAINING IS IDEAL FOR:

- Penetration testers who want hands-on experience attacking Active Directory and hybrid identity environments.
- Red and blue team members who need to understand both attack paths and detection.
- Active Directory administrators who want to find and fix weaknesses in their own environments.

## PREREQUISITES:

- Working knowledge of Windows Server and Active Directory administration.
- Basic knowledge of Kerberos and NTLM authentication.
- Basic Linux command-line skills.
- Hardware capable of running multiple virtual machines under Hyper-V.

## TRAINING AGENDA:

Lab preparation covers the lab look and feel, prerequisites, and architecture (schematics). Participants configure Windows 10/11 to use Hyper-V, including installation, functionality checks, and Hyper-V basics. They then download the required files and build the Windows Server 2019, 2022, and 2025 VMs and the Windows 11 VM. Next, they install and configure the Wazuh server on Ubuntu, including its components, UI connection, and networking. They install Wazuh agents on the domain controller and Windows 11, set up the Kali Linux VM (IP address, resolution, and SSH server), and complete the final preparation steps for all VMs.

Poisoning and relaying attacks show how LLMNR, NBT-NS, and mDNS poisoning can capture NTLM authentication, and how that authentication can be relayed to other hosts. Participants learn the mitigations, such as disabling name-resolution fallbacks and enforcing SMB signing, scan for the conditions that allow relaying, capture and relay credentials, identify the attack in logs and alerts, and apply and test the fix.

AS-REP roasting explains how accounts with Kerberos pre-authentication disabled can be attacked, and how to mitigate this. Participants scan the domain with Nmap, enumerate users, and perform password spraying. They extract AS-REP hashes, crack them with hashcat, and use NetExec to abuse the compromised account. They then identify the attack in logs and alerts, apply the fix, and test that it works.

Kerberoasting covers how service account Kerberos tickets can be requested and cracked offline. Participants learn the attack and its mitigations, scan with Nmap, and perform password spraying.

They identify kerberoastable accounts, request and crack service tickets with hashcat, and abuse the domain with NetExec. They detect the attack through Kerberoasting and Pass-the-Hash detection rules in Wazuh, then apply the fix and test it.

Passwords in Group Policy Preferences (GPP) shows how credentials stored in legacy Group Policy Preferences files in SYSVOL can be read by any domain user and decrypted. Participants learn the mitigation, scan SYSVOL for stored credentials, recover and decrypt them, identify the access in logs, and apply and test the fix.

MachineAccountQuota and unconstrained delegation demonstrates how the default MachineAccountQuota allows any authenticated user to create computer accounts, and how unconstrained delegation allows a compromised server to capture reusable TGTs. Participants learn the mitigations, scan for the default quota and delegation settings, abuse both to escalate privileges, identify the attack in logs and alerts, and apply and test the fix.

Pass-the-Hash (PtH) demonstrates how stolen NTLM password hashes can be reused to authenticate to Windows systems and services without knowing the plaintext password. Participants learn the mitigation, exploit the weakness using NetExec, and identify the attack in Windows event logs and Wazuh alerts, building on the Pass-the-Hash detection introduced in the Kerberoasting module. They then apply and test the fix.

Pass-the-Ticket (PtT) demonstrates how stolen Kerberos tickets can be reused to access resources without knowing the password. Participants learn the mitigation, exploit the weakness, identify the attack, and apply and test the fix. The module then covers Golden Ticket and Silver Ticket attacks, in which participants forge TGTs and service tickets using the krbtgt or service account key, learn how these tickets persist, and detect and remediate them.

DCSync and Skeleton Key show how an account with replication rights can extract password hashes from a domain controller. Participants exploit the weakness, crack the resulting hashes, and identify the attack. They then apply and test the fix. The module then covers Skeleton Key, in which participants patch LSASS on a domain controller to accept a master password, and detect and remove the implant.

AD CS compromises (E1 to E13) cover thirteen escalation paths caused by misconfigured Active Directory Certificate Services templates and settings. For each path, participants learn the mitigation, scan for the misconfiguration, exploit it, identify the attack, and apply and test the fix. The module ends with Golden Certificate attacks, in which participants steal the CA private key, forge certificates for any identity, and learn how to protect and monitor the CA.

One-way domain trust compromise and SID History abuse demonstrates how a compromised trusted domain can be used to attack a trusting domain. Participants learn the trust and SID filtering mitigations, enumerate trusts, abuse SID History to gain privileges in the target domain, identify the attack, and apply and test the fix.

Hybrid identity: Microsoft Entra Connect and Golden SAML (DEMO only) shows how compromising the Entra Connect server can expose synchronization credentials and cloud administrative access, and how Golden SAML attacks can forge federated sign-ins when AD FS is used. Participants learn the mitigations, scan the hybrid configuration, exploit the weakness, identify the attack in logs, and apply and test the fix.

## ABOUT THE TRAINER:



Robert Petrunić works as a senior information security consultant in Eduron IS, the company dedicated to IT security education, penetration testing and computer forensics.

Robert is Microsoft certified trainer since 2002, EC-Council certified trainer since 2008 and $(ISC)^2$ certified trainer since 2014. Today, he lectures mostly hacking and security related courses for red teams and DFIR (Digital Forensics and Incident Response) related courses for blue team members. Since 2004, he worked primarily in the security field, and Microsoft acknowledged this in 2008 by assigning him the most valuable Microsoft professional recognition for nine years in a row.

For the last eighteen years, Robert has been working on programs related to ethical hacking and IT security awareness for systems administrators, developers, and IT security consultants. He is also often a lecturer at regional IT conferences.

Robert holds many industry certifications, including $(ISC)^2$ CISSP and CCSP, Offensive Security OSCP, OSCE and OSWP, EC-Council CPENT, CEH, CHFI, CND, and ECIH to name a few.