PROJECT REPORT: PURPLE TEAM ACTIVE DIRECTORY LAB

1. Executive Summary

This project involved the design, deployment, exploitation, and hardening of a corporate Active Directory (AD) environment. The objective was to simulate a real-world "Purple Team" engagement, where offensive (Red Team) attacks are performed to validate security, followed by defensive (Blue Team) measures to mitigate vulnerabilities.

The project successfully demonstrated the full lifecycle of a cyberattack:

Infrastructure: Built a segmented enterprise network using VirtualBox, Windows Server 2022, and Windows 11.

Offense: Compromised the domain using industry-standard tools (Nmap, Evil-WinRM, Impacket) to achieve remote code execution and credential dumping.

Defense: Implemented robust hardening measures using AppLocker and Windows Firewall to neutralize standard attacks.

Advanced Simulation: Executed advanced evasion techniques (LOLBins/MSBuild) to bypass the implemented security controls, demonstrating the need for continuous monitoring.

2. Technical Architecture & Setup

2.1 Virtualization Strategy

To simulate a realistic corporate environment while maintaining security, a Dual-Adapter Network Architecture was implemented in Oracle VirtualBox:

Adapter 1 (NAT): Provided internet access for updates and package installation.

Adapter 2 (Internal Network - intnet): Created a strictly isolated communication channel between the Domain Controller, Client, and Attacker machine. This prevented attack traffic from leaking to the physical host network.

2.2 Domain Infrastructure

Domain Controller (DC):

OS: Windows Server 2022

Hostname: DC-Server

IP Address: 192.168.10.5 (Static)

Roles: Active Directory Domain Services (AD DS), DNS Server.

Domain Name: hackerlab.local

Client Workstation:

OS: Windows 11 Enterprise

Hostname: Win11-Client

IP Address: 192.168.10.4 (Static)

Domain Join: Successfully joined to hackerlab.local.

Attacker Machine:

OS: Kali Linux 2024

IP Address: 192.168.10.10 (Static)

2.3 User Management

Administrator: Domain Admin with full privileges.

John Parker: Created as a "Standard User" to simulate a regular employee with limited permissions, serving as the primary target for lateral movement and privilege escalation testing.

3. Phase 1: Red Team Operations (The Attack)

3.1 Reconnaissance (Network Mapping)

Used Nmap to identify live hosts and open services on the internal network.

Command: nmap -sn 192.168.10.0/24 identified the DC (.5) and Client (.4).

Service Scan: nmap -sV -O 192.168.10.5 revealed critical open ports:

Port 53: DNS

Port 88: Kerberos (Confirming AD Environment)

Port 445: SMB (File Sharing)

Port 5985: WinRM (Windows Remote Management)

3.2 Enumeration (Intelligence Gathering)

Used Enum4linux to query the Domain Controller without initial credentials.

Command: enum4linux -a 192.168.10.5

Outcome: Successfully dumped the Password Policy (Minimum length: 7 characters) and the User List, identifying "John Parker" as a potential target.

3.3 Exploitation (Gaining Access)

Utilized Evil-WinRM to exploit the open Management Port (5985). Using compromised credentials, a fully interactive PowerShell session was established on the Domain Controller.

Command: evil-winrm -i 192.168.10.5 -u Administrator -p 'Password'

Result: Achieved Remote Code Execution (RCE) on the server.

3.4 Post-Exploitation (Persistence & Looting)

Persistence: Created a backdoor account named backup_service and added it to the "Domain Admins" group to maintain access if the original password changed.

Credential Dumping: Used Impacket-secretsdump to perform a "DCSync" attack.

Result: Successfully extracted the NTLM Hashes for all users, including the KRBTGT account, enabling Golden Ticket attacks.

4. Phase 2: Blue Team Defense (Hardening)

4.1 Forensic Analysis

Conducted an investigation to detect the attack using Windows Event Viewer and Sysmon.

Event ID 4720: Detected the creation of the unauthorized user hacker_spy.

Event ID 4624: Traced the source IP of the attack back to 192.168.10.10 (Kali Linux).

Sysmon Event ID 1: Captured the exact malicious command line used by the attacker: net user hacker_spy /add.

4.2 Application Whitelisting (AppLocker)

Deployed a "Zero Trust" execution policy using Group Policy Objects (GPO).

Policy Goal: Prevent standard users (like John) from running command-line tools used by hackers.

Implementation:

Created Allow Rules for system files (C:\Windows*) to ensure OS stability.

Created strict Deny Rules using Wildcard Paths (*\cmd.exe, *\powershell.exe) to block execution regardless of file location.

Result: When the attacker attempted to spawn a shell via WinRM, the attack failed with "This program is blocked by group policy," successfully neutralizing the standard exploit.

4.3 Network Hardening (Firewall)

Configured Windows Defender Firewall to simulate a secure corporate environment.

Policy: Firewall enabled on all profiles (Domain/Private/Public).

Exceptions: Created specific Allow Rules for ICMP (Ping), SMB (445), and WinRM (5985) to allow necessary business traffic while blocking unauthorized ports.

5. Phase 3: Advanced Adversary Simulation (The Bypass)

5.1 The Challenge

With AppLocker blocking cmd.exe and Windows Defender Real-Time Protection enabled, standard attacks failed. The goal was to simulate an Advanced Persistent Threat (APT) bypassing these controls.

5.2 Antivirus Evasion (Obfuscation)

Technique: Used C# string manipulation to hide the malicious payload.

Method: Instead of writing "cmd.exe" (which triggers AV signatures), the code split the string into variables: string a = "cm"; string b = "d.exe";.

Result: Windows Defender scanned the file but failed to detect the malicious intent.

5.3 AppLocker Bypass (LOLBins)

Technique: "Living Off The Land" (LOLBins).

Method: Used the trusted Microsoft binary MSBuild.exe to compile and execute the malicious C# XML file in memory.

Execution: C:\Windows\Microsoft.NET\Framework64\...\MSBuild.exe C:\Temp\bypass.xml

Outcome: Successfully executed arbitrary code (popped calc.exe) despite AppLocker being active, proving the need for advanced monitoring (EDR/SIEM) in addition to blocking rules.

6. Conclusion

This project successfully demonstrated the cat-and-mouse game of modern cybersecurity. By building the infrastructure from scratch, I gained deep insight into:

Identity Management: How Active Directory structures and authenticates users.

Offensive Methodologies: How attackers map networks and pivot using built-in tools.

Defensive Architecture: How to implement "Defense in Depth" using GPO, AppLocker, and Firewalls.

Resilience: The limitations of static defenses and the importance of behavioral analysis (Sysmon/Logs) to catch advanced evasions.