Threat Modelling Report: Vulnerable Active Directory Domain

Executive Summary

This section of the penetration test report focuses on the Threat Modelling for the target domain – vulnAD.lab. By utilising tools such as PingCastle, Nmap, ldapsearch, and ADRecon, the tester discovered multiple critical vulnerabilities and assessed potential threats to the security posture of the domain.

The findings are categorised in accordance with the STRIDE methodology to prioritise the threats found effectively. The STRIDE methodology was employed to ensure proper evaluation of risks to confidentiality, integrity, and availability (CIA) of the AD domain.

1. Introduction

Automated tools and manual techniques were used to construct a detailed threat model for the vulnerable AD domain.

2. Methodology

The threat Modelling was conducted in accordance with the STRIDE methodology: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This method allowed for a comprehensive assessment of potential threats across various components of the AD domain. Key tools used in this phase included:

- **PingCastle**: For assessing AD health and identifying key risk indicators.
- **Nmap**: For service enumeration and identifying open ports/services.
- **ldapsearch**: For detailed enumeration of AD objects such as users, groups, and computers, in addition to specific targeted queries e.g. obtaining a list of all users, all admin users, all service accounts.
- **ADRecon**: For extracting a wide range of info from the AD environment to assess the configuration of the domain.

3. Key Findings

3.1 Spoofing Identity

- **Service Accounts Vulnerability**: Enumeration using the tools mentioned above revealed several service accounts with Service Principal Names (SPNs), susceptible to Kerberoasting attacks.

- **Weak Service Account Credentials**: ldapsearch and ADRecon revealed service accounts with weak or default passwords, making them prime targets for credential based attacks (credential spoofing to be specific).

3.2 Tampering

- **Group Policy Object Misconfigurations**: Analysis identified potential tampering risks due to misconfigured Group Policy Objects (GPOs).

3.3 Repudiation

- **Inadequate Logging**: The lack of Windows Event Forwarding (WEF), auditing and insufficient logging pose a threat to suspicious activity and undetected attacks.

3.4 Information Disclosure

- **Stale Objects and Unsecured LDAP**: Stale object rules identifying misconfigurations of the domain controller, ACLs and policy settings, in addition to unsecured LDAP bindings all of which could lead to the disclosure of unauthorised data.
- **Excessive User Privileges**: Nessus and ADRecon reports revealed users with excessive privileges, providing users with read and/or write access to protected objects in AD.
- **Insecure LDAP**: ldapsearch detected the use of unsecure/unencrypted LDAP.

3.5 Denial of Service

- **Service Availability Risks**: Identified critical AD services – EXC-SERVER, SQL-SERVER are potentially vulnerable to Denial of Service (DoS) attacks, impacting availability.
- **Unpatched Software & Updates:** Unpatched Windows updates from 2019 were reported. Security updates for DNS and .NET Framework are two of the vulnerabilities detected that offer DoS exploitation.

3.6 Elevation of Privilege

- **Insecure Group Memberships**: Certain user accounts have been identified with inappropriate group memberships, allowing potential privilege escalation.