ATTACKING ACTIVE DIRECTORY

Active Directory Enumeration&Attack 🕓14 hours of content | 100 hours of practice | Final project

1. Introduction to Active Directory

- What is Active Directory
- Importance and Role in Enterprise Information Systems
- Active Directory Structure
- Viewing Active Directory as a penetration tester

2. Domain Information Gathering

- Identifying the hosts present on the domain
- Identifying running services on the hosts
- Searching for services with anonymous access
- Enumerating valid usernames utilizing different TTP's

3. Getting a foothold on the domain

- LLMNR/NBT-NS Poisoning
- NTLM Relay
- Password Spaying
- ASREPRoast
- LDAP queries and anonymous binds
- Exploiting Vulnerable services

Credential Enumeration

4. Enumerating Domain Objects

- Domain users
- Domain Groups
- Domain computers
- Group Policy Objects (GPOs)
- Organizational Units (OUs)
- Service Principal Names (SPNs)
- Network Shares
- Security Controls

5. Getting Remote Connection

- Getting a GUI connection using RDP
- Obtaining shell access via Win-RM
- Accessing Other Hosts on the Domain using PSRemote
- Obtaining a Shell using PsExec/WMI

Domain Privileges Escalation

6. Getting Privileged access to the domain

- Utilizing Kerberoasting to Take Over Privileged Service Account
- Enumerating Delegations(Unconstrained/Constrained/Resource-based)
- Enumerating and Abusing ACL/ACE
- Stealing NTLM Credentials
- Searching network shares for credentials
- Checking for Password Reuse
- Searching for .kirbi Ticket Files
- Credential Hunting Methods
- Group Policy Preferences (GPP)

7. Leveraging Active Directory Attacks to Achieve Domain Compromise

- Utilizing Pass The Hash/Pass The Ticket to Impersonate Another User
- Dumping LAPS Passwords
- Using Silver/Golden Tickets to Impersonate Any User
- Executing DCSync to retrieve all of the hashes for the domain users
- Abusing the Print Spooler Service to Steal Credentials from Users
- Active Directory Certificate Theft
- RDP Session Hijacking
- MSSQL Abuse

8. Post-Exploitation & Persistence Methods

- Dumping the SAM Database
- Dumping the LSASS Process Memory
- Dumping NTDS.dit
- Creating a Skeleton Key
- Creating a Diamond Ticket
- Using DCShadow Attack

9.Enumerating and Attacking Domain Trusts

- What are Domain Trusts
- Domain Trusts Types
- Enumerating Domain Trusts Using Different TTPs
- Enumerating for Foreign Group Membership
- Cross-Forest Kerberoasting
- SID History Injection

ITSAFE
POWERED BY CYSOURCE

ATTACKING
ACTIVE DIRECTORY

Active Directory Information Gathering as anonymous (Passive Enumeration/ OSINT)

10. Gathering information about the Target

- Employee names
- Job rules
- Social media reconnaissance

11. Enumerating the IP space of the target

- Public-facing infrastructure
- Cloud presence
- DNS Records
- Domain information based on IP/DNS/public-facing website

12. Searching for data disclosures

- Looking for publicly accessible files(.pdf, .ppt, .docx, etc.)
- Public Github repositories to find sensitive information about the domain.
- Data breaches of leaked usernames, passwords, email addresses, etc.