iGNITE Technologies

ACTIVE DIRECTORY

Penetration Testing + Red Team Tactics

www.hackingarticles.in

About Course

Active Directory (AD) is a Microsoft Windows Server-based directory service. Active Directory Domain Services (AD DS) manages directory data storage and makes it accessible to network users and administrators. For instance, AD DS maintains information about user accounts, like as user names, passwords, and phone numbers, and allows other legitimate users on the same network to access data.
Since the Active Directory is the controlling center in a network makes its jewel assets for an organization. Microsoft stated that more than 95 million AD accounts come under attack daily. In 2021, Azure Active Directory alone saw more than 25.6 billion brute force attacks. Unfortunately, too many of these attacks are succeeding. One of the primary reasons for this is that AD is notoriously difficult to secure.

Durations: 32 HOURS

Professionals who want to learn about the most common risks can benefit from this course. To begin, you'll do a sneak reconnaissance and enumeration of hosts, servers, services, and privileged users to identify them.
To wrap things up, you will learn how to conduct red team attacks on Active Directory by targeting common misconfigurations and leveraging genuine Windows/Active Directory features. In this course, you will learn How to Enforce Red Team Tactics to eliminate threats by simulating real attack scenarios by creating your own AD Pentest lab.

Threats to Active Directory Systems

1. Default Security Settings: Microsoft built a set of predetermined, default security settings for AD. These security settings may not be suitable for the needs of your organization. Furthermore, hackers are well-versed in these default security settings and will attempt to attack gaps and vulnerabilities.

2. Inappropriate Privileged Access: Domain user accounts and other administrative users may have full, privileged access to AD. Special categories of privileged accounts, referred to as superuser accounts, are generally utilized for administration by qualified IT personnel and offer nearly unrestricted command execution and system changes.

3. Inappropriate or Broad Access for Roles and Employees: Administrators can provide employees access to specific applications and data based on their positions. Access levels are determined by the roles assigned to individuals. It is critical to restrict access to individuals and roles to the levels necessary for them to accomplish their job tasks.

4. Unpatched Vulnerabilities: Cybercriminals can swiftly target unpatched apps, operating systems, and firmware on AD Servers, gaining a key first foothold in your environment.

5. Missing Monitoring Alerts: To better prevent or disrupt illegal access attempts in the future, IT managers must be informed of such incidents. If you don't have a clear Windows audit trail, it's impossible to tell legitimate and malicious access attempts apart, as well as any changes

Benefits

- Gain Exposure to Real-Time Pentesting & Red Team
- This course meets the requirements of NIST, MITRE ATTACK
- Building in-house lab for threat hunting
- Gain in-depth knowledge of APTs attack
- Hands-on exposure to AD tools such as Rubeus and Mimikatz.
- Unique tools and techniques for exploiting AD
- Latest attack such as zero day exploit.

Who should Join ?

- If you are an ethical hacker with Basic knowledge
- if you are a Network Security Engineer
- if you managed NOC and SOC
- If you are an Information Security Analyst
- If you are a Team leader of the Cyber Security Department
- if you handle the pre-sell department for VAPT services
- if you are a backend developer
- If you are a system administrator

Prerequisites

The candidate should have a basic understanding of Active Directory and Networking and also know the fundamental approach of system hacking.

iGNITE Technologies

AD INDEX

iGNITE Technologies

AD COURSE CONTENT

Module1: Initial Compromise

- Exploit unpatched, uncovered vulnerability to obtain received connection.
- Perform Application whitelisting Attack for executing the malicious script in the domain network
- Get hands-on expertise in setup an in-house Active Directory environment and gain offensive and defensive learning by simulating APT's Attack Scenarios.

Module2: Active Directory Enumeration

- Performing Domain Reconnaissance resources such as domains, users, groups, ACL, OU, Forest, Trust, and GPO will be done using Microsoft built-in utility
- Hunting and Mapping Active directory resources PowerShell's enumeration scripts, Bloodhound, RPCClient. We will also be seeking domain admins and users. In order to exploit the AD, such as Privilege escalation, lateral movement and persistence, we can use this information to expand our attack surface.

Module 3: Abusing Kerberos

- This module will help to understand KERBEROS & its Major Components also Kerberos Workflow using Messages for authentication.
- Discover Service Principal Names that are associated with a normal user account
- Kerberosting Attack is a technique to steal a service ticket or RC4 HMAC hash to a service account in a domain.
- AS-REP Roasting is a technique to get the AS-REP encrypted with the user's RC4-HMAC'd password.
- Kerberos Brute Force to identify user accounts without Kerberos pre-authentication.

Module 4: Privilege Escalation

- Learn local privilege escalation on domain connecting computers.
- Abusing Resource-based constrained delegation which is the root cause of a privilege escalation technique stemming from an attribute "msDS-AllowedToActonBehalfOfOtherIdentity
- Enumeration and abusing special privileges assigned to user or service to escalate admin-level access.
- Learn the Zero-day-attack exploitation like NoPAC, SAM-Account Spoofing, PetitPotam NTLM Relay to ADCS Endpoints.

Module5: Credential Dumping

- Extracting TGT for those users that have the property 'Do not require Kerberos pre-authentication set (UF_DONT_REQUIRE_PREAUTH)
- Creating a bogus TGT to frame Golden Ticket Attack in order to request TGS for the given SPN service principal name.
- Creating a bogus TGS to frame Silver Ticket Attack
- DCSYNC: Typically impersonates a domain controller and requests other DC's for user credential data via GetNCChanges.
- Get the Domain computer password to bypass the Local Administrator Password Solution (LAPS).
- Obtain passwords and hashes stored inside SAM, Registry hive, Domain Cache Credential, NTDS.DIT, LSA|LSASS and etc.

Module 6: Lateral Movement

- Workstation takeover, also known as lateral movement, PetitPotam or PrinterBug, is an HTTP authentication that can be coerced and relayed to LDAP(S) on domain controllers.
- Extracting MIT Kerberos Credential Cache to use KERB5CCNAME pass the ccache (PTC) file for the requested service Domain
- Pass the Kerberos Ticket TGT extracted from LSASS.
- Access Domain Resource or services using Pass the Hash (PTH) attack and Over Pass the hash (OPTH) attack by using NTLM hash, NTLM (RC4), AES 256 key or AES 128 key.

Module7: Domain Persistence

- Golden Certificate Attack: This technique leverages the certificate-based authentication in AD enabled by default with the installation of ADCS (Active Directory Certificate Services) by forging a new certificate using the private key of the CA certificate.
- Computer Account: An attacker who has compromised a system with a local administrator account active and a computer/machine account added in the domain admins group, can use this to dump hashes in a domain that would allow him to escalate his privileges to Domain Controller and further, how computer accounts can be used by an attacker to gain persistence.
- DC Shadow: Manipulating Active Directory (AD) data, including objects and schemas, by registering and replicating the behaviour of a Domain Controller (DC). It simulates the behaviour of a Domain Controller (using protocols like RPC used only by DC) to inject its data, bypassing most of the common security controls and including your SIEM.
- MITRE Attack Technique for Tactic ID TA0003 which is used by various of APTs & threat Actors for creating a permanent backdoor in the domain controller. We will check how to use Directory Services Restore Mode (DSRM) for conducting a persistence attacker on the Domain controller.
- Persistence attack on Active Directory by abusing AdminSDHolder, Active Directory Domain Services uses AdminSDHolder, protected groups and Security Descriptor propagator (SD propagator or SDPROP for short) to secure privileged users and groups from unintentional modification.
- Using Skeleton Key attack to Tampers Kerberos and NTLM the authentication methods by creating the master password which is injected in the LASS process and Kerberos encryption will also be downgraded to an algorithm that doesn't support salt (RC4_HMAC_MD5)

Module8: Bonus Section

- Get Experience in Command & Control with PowerShell Empire
- Get to know A to Z on Mimikatz and Rubeus which are used by APTs
- Enhanced your Post Exploitation and Lateral movement Skillset with Python Libraries and Crackmapexec.

Contact US

PHONE

+91-9599387841 | +91 11 4510 3130

WHATSAPP

https://wa.me/message/HIOPPNENLOX6F1

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

https://www.linkedin.com/company/hackingarticles/

TWITTER

https://twitter.com/hackinarticles

GITHUB

https://github.com/Ignitetechnologies

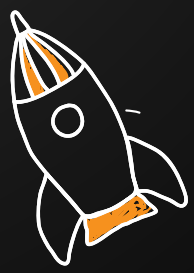
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

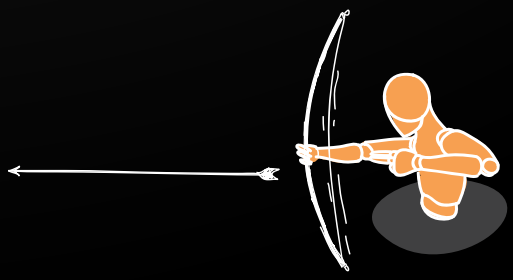
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux