Active Directory Pentest

1. Reconnaissance

- External Recon
  - OSINT (LinkedIn, hunter.io, dehashed)
  - DNS enumeration (dnsrecon, dnsenum)
  - Subdomain enumeration (amass, subfinder)
  - Email harvesting (theHarvester)
  - Breach data / credential stuffing lists
  - Shodan / Censys for exposed services
- Internal Recon (Unauthenticated)
  - Network discovery (nmap, fping, netdiscover)
  - Identify Domain Controllers (port 88/389/636)
  - Responder analyze mode (-A)
  - ARP scan / broadcast traffic capture
  - LDAP anonymous bind
  - SMB null session (enum4linux-ng)
  - RPC null session (rpcclient -U "")
- Domain Information
  - Domain name / FQDN
  - Forest / domain trusts
  - Domain functional level
  - Naming context / sites

2. Initial Access (No Creds)

- Network Poisoning / Coercion
  - LLMNR / NBT-NS poisoning (Responder)
  - mDNS poisoning
  - IPv6 DHCP / WPAD attacks (mitm6)
  - SMB relay (ntlmrelayx)
  - LDAP / LDAPS relay
  - HTTP -> LDAP relay (ADCS ESC8)
  - PetitPotam / PrinterBug / DFSCoerce coercion
- Pre-auth Kerberos Attacks
  - Username enumeration (Kerbrute userenum)
  - AS-REP Roasting (DONT_REQ_PREAUTH users)
  - Timeroast (RID brute via NTP)
- Password Attacks
  - Password spraying (kerbrute, NetExec)
  - Avoid lockout - check policy first
  - Common: Season+Year, Company+123, Welcome1
  - Targeted brute force on identified users
- Service Exploitation
  - ZeroLogon (CVE-2020-1472)
  - PrintNightmare (CVE-2021-1675/34527)
  - noPac / sAMAccountName spoofing (CVE-2021-42278/42287)
  - EternalBlue / unpatched SMBv1
  - Exchange (ProxyShell, ProxyLogon, ProxyNotShell)
- Anonymous Access
  - SMB shares with NULL session
  - Snaffler / MANSPIDER for share content
  - LDAP anonymous queries
  - Unauthenticated RPC interfaces
- Phishing / Initial Foothold
  - HTML smuggling, ISO/LNK delivery
  - OAuth consent phishing (Entra ID)
  - Device code phishing

3. Authenticated Enumeration

- BloodHound / SharpHound
  - SharpHound -c All / DCOnly
  - Python collector (bloodhound-python)
  - ldeep / RustHound / SOAPHound
  - Find shortest path to Domain Admin
  - Custom Cypher queries (Kerberoastable, unconstrained)
- Users / Groups / Computers
  - PowerView: Get-NetUser, Get-NetGroup, Get-NetComputer
  - ADSearch / ldapsearch / windapsearch
  - net group "Domain Admins" /domain
  - Check description fields for passwords
  - Find admin users (adminCount=1)
- Shares / Files
  - SMBMap, smbclient, NetExec --shares
  - Snaffler (find passwords in shares)
  - SYSVOL Groups.xml (cpassword)
  - Manspider / FindStr keyword hunts
- Trust / Forest
  - Get-NetForest / Get-NetForestTrust
  - Get-NetDomainTrust
  - nltest /domain_trusts /all_trusts
- ACL / ACE Abuse Paths
  - GenericAll / GenericWrite
  - WriteOwner / WriteDACL
  - ForceChangePassword
  - AddMember
  - ReadLAPSPassword (ms-Mcs-AdmPwd)
  - ReadGMSAPassword
- GPO / OU Enumeration
  - Get-NetGPO, Get-DomainOU
  - GPO permissions abuse (SharpGPOAbuse)
- ADCS Enumeration
  - Certipy find / Certify find
  - Identify vulnerable templates (ESC1-ESC15)
- MSSQL / Service Discovery
  - Get-SQLInstanceDomain / mssqlclient.py
  - Service Principal Names (setspn -T)

4. Credential Theft

- Offline Roasting
  - Kerberoasting (Rubeus, GetUserSPNs.py)
  - AS-REP Roasting (Rubeus, GetNPUsers.py)
  - Hashcat modes 13100 / 18200
  - Targeted Kerberoasting (set SPN via GenericWrite)
- On-host Credential Dumping
  - LSASS (Mimikatz sekurlsa::logonpasswords)
  - lsassy / nanodump / pypykatz
  - comsvcs.dll MiniDump
  - SAM / SYSTEM / SECURITY hives
  - DPAPI master keys + blobs
  - Credential Manager (vaultcli)
  - Browser credentials (SharpChromium, SharpDPAPI)
  - WDigest / TSPKG cleartext (force with reg key)
  - Cached domain creds (mscash2)
- Domain-wide Credentials
  - DCSync (lsadump::dcsync)
  - NTDS.dit + SYSTEM hive (vssadmin / ntdsutil)
  - secretsdump.py
- Special Sources
  - LAPS passwords (ms-Mcs-AdmPwd, msLAPS-Password)
  - gMSA password (msDS-ManagedPassword, gMSADumper)
  - Unattend.xml / sysprep / answer files
  - GPP cpassword (Groups.xml, gpp-decrypt)
  - KeePass / Bitwarden vaults
  - PuTTY / WinSCP / RDP saved sessions

5. Privilege Escalation

- Local Windows PrivEsc
  - winPEAS / PowerUp / Seatbelt
  - Unquoted service paths
  - Weak service permissions / DLL hijack
  - AlwaysInstallElevated
  - Token impersonation - Potato family
  - - JuicyPotato / RoguePotato
  - - PrintSpoofer / GodPotato / EfsPotato
  - UAC bypass (fodhelper, sdclt, slui)
  - Kernel exploits (last resort)
- ACL Abuse
  - GenericAll on user -> reset password / shadow creds
  - GenericAll on group -> Add-DomainGroupMember
  - GenericWrite on user -> set SPN -> Kerberoast
  - WriteDACL -> grant self DCSync
  - WriteOwner -> take ownership -> WriteDACL
  - WriteSPN -> Targeted Kerberoasting
  - GenericWrite on computer -> RBCD attack
- Kerberos Delegation
  - Unconstrained Delegation - capture TGTs (Rubeus monitor)
  - Constrained Delegation (S4U2Self/S4U2Proxy)
  - Resource-Based Constrained Delegation (RBCD)
  - - msDS-AllowedToActOnBehalfOfOtherIdentity
  - - Combined with MachineAccountQuota=10
- ADCS Abuse (Certipy)
  - ESC1 - Enrollee supplies subject + client auth
  - ESC2 - Any Purpose EKU
  - ESC3 - Enrollment Agent
  - ESC4 - Vulnerable template ACL
  - ESC5 - CA / object ACL
  - ESC6 - EDITF_ATTRIBUTESUBJECTALTNAME2
  - ESC7 - CA officer / manager rights
  - ESC8 - HTTP enrollment NTLM relay
  - ESC9 / ESC10 - weak certificate mapping
  - ESC11 - RPC relay to ICertPassage
  - ESC13 - OID group link abuse
  - ESC14 / ESC15 - schema / altSecID abuse
- GPO Abuse
  - SharpGPOAbuse - add scheduled task / local admin
  - PowerGPOAbuse
- Coercion + Relay Combos
  - PetitPotam -> ADCS HTTP (ESC8) -> DA cert
  - PrinterBug -> Unconstrained DC -> TGT
  - DFSCoerce -> LDAPS relay -> RBCD
- Notable CVEs
  - ZeroLogon (CVE-2020-1472)
  - PrintNightmare (CVE-2021-1675 / 34527)
  - noPac (CVE-2021-42278 + 42287)
  - CertiFried (CVE-2022-26923)
  - KrbRelayUp

6. Lateral Movement

- Pass-the-Hash (NTLM)
  - NetExec smb -H <hash>
  - Mimikatz sekurlsa::pth
  - impacket-* with -hashes
- Pass-the-Ticket (Kerberos)
  - Rubeus ptt /ticket:
  - Mimikatz kerberos::ptt
  - ccache files (KRB5CCNAME)
- Overpass-the-Hash
  - NTLM -> Kerberos TGT (Rubeus asktgt)
- Pass-the-Certificate
  - Certipy auth - PKINIT to TGT + NT hash
- Shadow Credentials
  - msDS-KeyCredentialLink (Whisker / Certipy)
- Remote Execution
  - PsExec / SMBExec (445)
  - WMIExec / wmic (135 + DCOM)
  - WinRM / Evil-WinRM (5985 / 5986)
  - DCOM (MMC20.Application, ShellWindows)
  - atexec / scheduled tasks
  - services.msc / sc.exe
  - RDP / xfreerdp /pth:
  - SSH (Windows 2019+)
- Pivoting / Tunneling
  - Chisel / Ligolo-ng
  - SOCKS via SSH / proxychains
  - Cobalt Strike SMB/TCP beacons

7. Domain Dominance

- DCSync
  - Replication rights (DS-Replication-Get-Changes-All)
  - Mimikatz lsadump::dcsync /user:krbtgt
  - secretsdump.py -just-dc
- DCShadow
  - Register rogue DC, push changes, deregister
- Krbtgt Manipulation
  - Golden Ticket (krbtgt NT hash / AES key)
  - Reset krbtgt twice for remediation
- Forest / Cross-domain
  - Inter-realm TGT (Golden across trusts)
  - SID History abuse (ExtraSids)
  - Trust key extraction
  - Foreign security principal abuse

8. Persistence

- Kerberos Tickets
  - Golden Ticket (forge any user)
  - Silver Ticket (single service)
  - Diamond Ticket (modify legitimate TGT)
  - Sapphire Ticket
- DC-resident
  - Skeleton Key (Mimikatz misc::skeleton)
  - DSRM password sync + RID 500 logon
  - Custom SSP (memssp)
  - LSA password filter DLL
- ACL Backdoors
  - AdminSDHolder ACE injection
  - DCSync rights to a low-priv user
  - Hidden objects (OWNER RIGHTS deny self ACE)
- Service / Object
  - Service registration
  - Scheduled tasks (SCHTASKS)
  - WMI event subscriptions
  - GPO modification
  - ADCS - issue long-lived smart card cert (ESC1/3)
  - Shadow Credentials (msDS-KeyCredentialLink)

9. Defense Evasion

- AMSI Bypass
  - amsiInitFailed patch
  - Hardware breakpoint AMSI bypass
- ETW Bypass
  - EtwEventWrite patch
  - ETW provider GUID disable
- Logging Evasion
  - ScriptBlock / Module logging bypass
  - PowerShell v2 downgrade
  - Sysmon rule gaps
- EDR / Defender
  - Direct / indirect syscalls (SysWhispers, Hell's Gate)
  - Unhooking ntdll
  - Process injection (early bird, mockingjay)
  - BYOVD - vulnerable driver
  - Defender exclusions abuse
- LOLBAS / Living off the Land
  - rundll32, regsvr32, mshta, msbuild
  - certutil download / decode
  - bitsadmin transfer
- Obfuscation
  - Invoke-Obfuscation
  - ConfuserEx for .NET
  - String encryption / AES payloads

10. Hybrid / Cloud (Entra ID + AD)

- Entra Connect / AAD Connect
  - MSOL_ account DCSync
  - ADSync service account abuse
  - Pass-through Auth agent abuse
- Federation
  - Golden SAML (ADFS token-signing cert)
  - ADFS DKM master key extraction
- Token / Refresh Token Theft
  - ROADtools / AADInternals
  - TokenTactics / TokenTacticsV2
  - Primary Refresh Token (PRT) theft
- Device Code / Illicit Consent
  - Device code phishing
  - OAuth app consent grant attacks

Toolbox

- Recon / Enumeration
  - BloodHound CE + SharpHound / bloodhound-python
  - PowerView / PowerSploit
  - ADRecon / PingCastle / Purple Knight
  - enum4linux-ng / ldapsearch / windapsearch
  - NetExec (formerly CrackMapExec)
- Credentials / Kerberos
  - Mimikatz / pypykatz / lsassy
  - Rubeus
  - Impacket suite (secretsdump, GetUserSPNs, ntlmrelayx)
  - Kerbrute
  - hashcat / john
- ADCS
  - Certipy-ad
  - Certify / ForgeCert
  - PSPKIAudit
- Coercion
  - PetitPotam.py
  - Coercer.py
  - DFSCoerce / PrinterBug
- Local PrivEsc
  - winPEAS / PowerUp / Seatbelt
  - SharpUp / SweetPotato / GodPotato
- C2 Frameworks
  - Cobalt Strike
  - Sliver / Mythic / Havoc / Brute Ratel
  - Nighthawk / PoshC2
- Post-Ex / Misc
  - Snaffler / Manspider
  - SharpDPAPI / SharpChromium
  - GhostPack suite
  - LAPSToolkit / gMSADumper

Methodology Loop

- 1. Recon -> 2. Foothold -> 3. Enumerate
- 4. Loot creds -> 5. Escalate -> 6. Move laterally
- Repeat 3-6 until 7. Domain Dominance
- 8. Establish persistence (with client approval)
- Document EVERYTHING (timestamps, hosts, evidence)
- Cleanup artifacts at end of engagement

www.hackingarticles.in

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles