Active Directory Enumeration Tools

Network & Domain Enumeration
- NetExec (NXC)
- enum4linux-ng
- rpcclient
- smbclient
- smbmap
- ldapsearch
- ldapdomaindump
- windapsearch
- adidnsdump

Credential Enumeration
- NetExec
- Kerbrute
- GetNPUsers.py
- GetUserSPNs.py
- Rubeus
- Certipy
- PKINITtools

PowerShell Enumeration
- PowerView
- SharpView
- PowerSploit
- Nishang

Active Directory Recon
- BloodHound CE
- SharpHound
- BloodHound.py
- PingCastle
- Purple Knight
- ADRecon
- ADExplorer
- ADExplorerSnapshot.py

Impacket Collection
- lookupsid.py
- GetADUsers.py
- GetNPUsers.py
- GetUserSPNs.py
- findDelegation.py
- secretsdump.py
- wmiexec.py
- psexec.py
- smbexec.py
- atexec.py
- rpcdump.py
- samrdump.py

Kerberos Enumeration
- Kerbrute
- Rubeus
- Kekeo
- Impacket
- PKINITtools

ADCS
- Certipy
- Certify
- ForgeCert
- PSPKIAudit

Group Policy Enumeration
- SharpGPOAbuse
- Grouper2
- PowerView

Local Enumeration
- Seatbelt
- winPEAS
- SharpUp
- Watson
- SharpEDRChecker

ACL Enumeration
- BloodHound
- PowerView
- dacledit.py
- BloodyAD

Trust Enumeration
- BloodHound
- nltest
- PowerView
- findDelegation.py

Password Policy Enumeration
- enum4linux-ng
- NetExec
- rpcclient
- ldapsearch

DNS Enumeration
- adidnsdump
- dnsenum
- dig
- nslookup

LDAP Enumeration
- ldapsearch
- windapsearch
- ldapdomaindump
- NetExec LDAP

Cloud & Hybrid AD
- AzureHound
- ROADtools
- AADInternals
- GraphRunner

Graph-Based Enumeration
- BloodHound CE
- AzureHound
- SharpHound
- BloodHound.py

SMB Enumeration
- smbmap
- smbclient
- NetExec SMB
- rpcclient

Comprehensive Frameworks
- NetExec
- BloodHound
- Impacket
- PowerView
- Certipy
- BloodyAD
- CrackHound
- PingCastle
- ADRecon

www.hackingarticles.in

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