37 Essential Tools for Active Directory Penetration Testing

Enumeration & Intelligence Gathering

ACLight: Shed light on the darkness of AD permissions.

netview: View the network like never before—exploit the blind spots.

ADExplorer: Uncover hidden secrets within the AD infrastructure.

ADFind: Seek out valuable AD information.

ADForest: Explore the vast forest of Active Directory.

ADRecon: Scour the domain for valuable intelligence.

Vulnerability Scanning & Exploitation

nilm-scanner: Scan for vulnerable NTLM relays—exploit the weak!

ntimrelavx: Exploit NTLM relay vulnerabilities to compromise AD systems.

BloodHound.py: Unleash the power of BloodHound from Python.

Nmap: Perform network scanning and enumeration to gather information about the AD environment.

Post-Exploitation & Enumeration

CrackMapExec (CME): An offensive tool for post-exploitation and AD enumeration.

DomainPasswordSpray: Spray passwords to crack AD defenses.

DumpsterDiver: Dive into the dumpster of AD and extract treasures.

empire: Build your empire of chaos and mayhem.

37 Essential Tools for Active Directory Penetration Testing

PowerShell Tools

Powermad: Go mad with PowerShell—conquer AD with ease!

PowerSploit: Unleash the power of PowerShell for offensive AD operations.

PowerView: Empower your reconnaissance with this advanced PowerShell tool.

PowerShell Empire: Command and control framework for lateral movement and post-exploitation in AD.

Password Cracking & Credential Harvesting

Hydra: A fast and flexible password-cracking tool.

Get-GPPPassword: Steal Group Policy Preferences (GPP) passwords.

gpp-decrypt: Decrypt Group Policy Preferences like a champ.

John the Ripper: A widely used password-cracking tool.

Kerberos & Ticket Manipulation

kerbcrack: Crack Kerberos tickets and seize the throne.

Kekeo: Manipulate Kerberos tickets in AD.

Kerbrute: Brute force Kerberos passwords efficiently.

37 Essential Tools for Active Directory Penetration Testing

Miscellaneous Tools

Invoke-ACLpwn: Manipulate ACLs for domination.

Rubes: Exploit weak service account passwords and manipulate Kerberos tickets.

SharpHound: Sniff out security vulnerabilities.

Mitm6: Intercept IPv6 traffic and manipulate it for your cause.