Tools of the Trade

Tool	Description
PowerView/ SharpView	A PowerShell tool and a .NET port of the same used to gain situational awareness in AD. These tools can be used as replacements for various Windows `net*` commands and more. PowerView and SharpView can help us gather much of the data that BloodHound does, but it requires more work to make meaningful relationships among all of the data points. These tools are great for checking what additional access we may have with a new set of credentials, targeting specific users or computers, or finding some "quick wins" such as users that can be attacked via Kerberoasting or ASREPRoasting.
BloodHound	Used to visually map out AD relationships and help plan attack paths that may otherwise go unnoticed. Uses the SharpHound PowerShell or C# ingestor to gather data to later be imported into the BloodHound JavaScript (Electron) application with a Neo4j database for graphical analysis of the AD environment.
SharpHound	The C# data collector to gather information from Active Directory about varying AD objects such as users, groups, computers, ACLs, GPOs, user and computer attributes, user sessions, and more. The tool produces JSON files which can then be ingested into the BloodHound GUI tool for analysis.
BloodHound.py	A Python-based BloodHound ingestor based on the Impacket toolkit. It supports most BloodHound collection methods and can be run from a non-domain joined attack host. The output can be ingested into the BloodHound GUI for analysis.
Kerbrute	A tool written in Go that uses Kerberos Pre-Authentication to enumerate Active Directory accounts, perform password spraying, and brute-forcing.
Impacket toolkit	A collection of tools written in Python for interacting with network protocols. The suite of tools contains various scripts for enumerating and attacking Active Directory.
Responder	Responder is a purpose-built tool to poison LLMNR, NBT-NS, and MDNS, with many different functions.
Inveigh.ps1	Similar to Responder, a PowerShell tool for performing various network spoofing and poisoning attacks.
C# Inveigh (InveighZero)	The C# version of Inveigh with a semi-interactive console for interacting with captured data such as username and password hashes.
rpcinfo	The rpcinfo utility is used to query the status of an RPC program or enumerate the list of available RPC services on a remote host. The "-p" option is used to specify the target host. For example the command "rpcinfo -p 10.0.0.1" will return a list of all the RPC services available on the remote host, along with their program number, version number, and protocol. Note that this command must be run with sufficient privileges.
rpcclient	A part of the Samba suite on Linux distributions that can be used to perform a variety of Active Directory enumeration tasks via the remote RPC service.
CrackMapExec (CME)	CME is an enumeration, attack, and post-exploitation toolkit which can help us greatly in enumeration and performing attacks with the data we gather. CME attempts to "live off the land" and abuse built-in AD features and protocols like SMB, WMI, WinRM, and MSSQL.
Rubeus	Rubeus is a C# tool built for Kerberos Abuse.

Tool	Description
GetUserSPNs.py	Another Impacket module geared towards finding Service Principal names tied to normal users.
Hashcat	A great hash cracking and password recovery tool.
enum4linux	A tool for enumerating information from Windows and Samba systems.
enum4linux-ng	A rework of the original Enum4linux tool that works a bit differently.
ldapsearch	Built-in interface for interacting with the LDAP protocol.
windapsearch	A Python script used to enumerate AD users, groups, and computers using LDAP queries. Useful for automating custom LDAP queries.
DomainPasswordSpray.ps1	DomainPasswordSpray is a tool written in PowerShell to perform a password spray attack against users of a domain.
LAPSToolkit	The toolkit includes functions written in PowerShell that leverage PowerView to audit and attack Active Directory environments that have deployed Microsoft's Local Administrator Password Solution (LAPS).
smbmap	SMB share enumeration across a domain.
psexec.py	Part of the Impacket toolkit, it provides us with Psexec-like functionality in the form of a semi-interactive shell.
wmiexec.py	Part of the Impacket toolkit, it provides the capability of command execution over WMI.
Snaffler	Useful for finding information (such as credentials) in Active Directory on computers with accessible file shares.
smbserver.py	Simple SMB server execution for interaction with Windows hosts. Easy way to transfer files within a network.
setspn.exe	Adds, reads, modifies and deletes the Service Principal Names (SPN) directory property for an Active Directory service account.
Mimikatz	Performs many functions. Notably, pass-the-hash attacks, extracting plaintext passwords, and Kerberos ticket extraction from memory on a host.
secretsdump.py	Remotely dump SAM and LSA secrets from a host.
evil-winrm	Provides us with an interactive shell on a host over the WinRM protocol.
mssqlclient.py	Part of the Impacket toolkit, it provides the ability to interact with MSSQL databases.
noPac.py	Exploit combo using CVE-2021-42278 and CVE-2021-42287 to impersonate DA from standard domain user.
rpcdump.py	Part of the Impacket toolset, RPC endpoint mapper.
CVE-2021-1675.py	Printnightmare PoC in python.
ntlmrelayx.py	Part of the Impacket toolset, it performs SMB relay attacks.
PetitPotam.py	PoC tool for CVE-2021-36942 to coerce Windows hosts to authenticate to other machines via MS-EFSRPC EfsRpcOpenFileRaw or other functions.

Tool	Description
gettgtpkinit.py	Tool for manipulating certificates and TGTs.
getnthash.py	This tool will use an existing TGT to request a PAC for the current user using U2U.
adidnsdump	A tool for enumerating and dumping DNS records from a domain. Similar to performing a DNS Zone transfer.
gpp-decrypt	Extracts usernames and passwords from Group Policy preferences files.
GetNPUsers.py	Part of the Impacket toolkit. Used to perform the ASREPRoasting attack to list and obtain AS-REP hashes for users with the 'Do not require Kerberos preauthentication' set. These hashes are then fed into a tool such as Hashcat for attempts at offline password cracking.
lookupsid.py	SID bruteforcing tool.
ticketer.py	A tool for creation and customization of TGT/TGS tickets. It can be used for Golden Ticket creation, child to parent trust attacks, etc.
raiseChild.py	Part of the Impacket toolkit, It is a tool for automated child to parent domain privilege escalation.
Active Directory Explorer	Active Directory Explorer (AD Explorer) is an AD viewer and editor. It can be used to navigate an AD database and view object properties and attributes. It can also be used to save a snapshot of an AD database for offline analysis. When an AD snapshot is loaded, it can be explored as a live version of the database. It can also be used to compare two AD database snapshots to see changes in objects, attributes, and security permissions.
PingCastle	Used for auditing the security level of an AD environment based on a risk assessment and maturity framework (based on CMMI adapted to AD security).
Group3r	Group3r is useful for auditing and finding security misconfigurations in AD Group Policy Objects (GPO).
ADRecon	A tool used to extract various data from a target AD environment. The data can be output in Microsoft Excel format with summary views and analysis to assist with analysis and paint a picture of the environment's overall security state.

Revision #2
Created 2025-02-06 21:19:59 UTC by Ryan
Updated 2025-02-12 01:11:17 UTC by Ryan