

Forum: [Hack Forums](#)

Thread: [Black Hacking Info for beginners \[Huge amount of info\]](#)

player113223 - July 9, 2025, 12:10 pm

Reconnaissance and Information Gathering

These tools help you gather information about your target before launching an attack. Think of it as scoping out the enemy's territory.

EyeWitness: Takes screenshots of websites and gathers info about the server. It's like peeking through a window to see what's inside.

AWSBucketDump: Looks into AWS S3 buckets for sensitive data. Imagine it as rummaging through someone's digital storage locker.

AQUATONE: Scans for domain names to find hidden or forgotten websites. It's like looking for secret entrances to a building.

spooftcheck: Checks if a domain can be spoofed by examining SPF and DMARC records. It's like testing if you can trick someone into thinking you're someone else.

Nmap: Discovers hosts and services on a network. Think of it as drawing a map of all the computers and devices on a network.

dnsrecon: Enumerates DNS information. It's like asking around for the address of a secret hideout.

dirsearch: Brute forces directories and files on websites. Imagine it as trying every key in a huge key ring to unlock a door.

Sn1per: Automated pentest recon scanner. It's like having a robot scout out the enemy's base for you.

Social Mapper: Maps social media profiles across multiple platforms. It's like connecting the dots on a social media puzzle.

skiptracer: OSINT scraping framework for compiling PII. Think of it as gathering personal information from public sources.

FOCA: Finds metadata and hidden information in documents. It's like reading between the lines of a secret note.

theHarvester: Gathers subdomains, email addresses, and employee names from public sources. Imagine it as harvesting data from public fields.

Metagoofil: Extracts metadata from public documents. It's like digging for hidden treasures in old documents.

SimplyEmail: Email reconnaissance tool. Think of it as snooping through someone's email inbox.

truffleHog: Searches git repositories for secrets. It's like finding hidden passwords in someone's code.

pwnedOrNot: Checks if an email account has been compromised in a data breach. It's like asking if someone's email has been hacked before.

GitHarvester: Harvests information from GitHub. Imagine it as collecting intel from a developer's public workspace.

pwndb: Searches leaked credentials using the Onion service. It's like looking for stolen passwords in the dark web.

LinkedInt: LinkedIn reconnaissance tool. Think of it as spying on someone's professional network.

CrossLinked: Extracts valid employee names from an organization through search engine scraping. It's like making a list of all the people who work at a company.

findomain: Fast domain enumeration tool using Certificate Transparency logs. Imagine it as finding all the hidden domains owned by someone.

Exploitation and Payload Generation

These tools help you create and deliver malicious code to your target. It's like crafting a poisoned

arrow and aiming it at the enemy.

WinRAR RCE: Exploit for CVE-2018-20250. It's like finding a backdoor in WinRAR that lets you take control.

Composite Moniker: Exploit for CVE-2017-8570. Think of it as tricking a system into running your code by disguising it as something safe.

Exploit toolkit CVE-2017-8759: Tests Microsoft .NET Framework RCE. It's like finding a weak spot in the .NET Framework and exploiting it.

CVE-2017-11882 Exploit: Accepts long commands/code. Imagine it as overloading a system with too much data to make it crash.

Adobe Flash Exploit CVE-2018-4878. It's like finding a hole in Adobe Flash that lets you run your own code.

Exploit toolkit CVE-2017-0199: Tests Microsoft Office RCE. Think of it as tricking Microsoft Office into running your malicious code.

demiguise: HTA encryption tool for RedTeams. It's like disguising your code so it looks harmless.

Office-DDE-Payloads: Generates Office documents with DDE command execution. Imagine it as hiding your code inside a seemingly safe Office document.

CACTUSTORCH: Payload generation for adversary simulations. It's like creating fake attacks to test your defenses.

SharpShooter: Payload creation framework for CSharp. Think of it as a toolbox for creating malicious CSharp code.

Don't kill my cat: Generates obfuscated shellcode stored in polyglot images. It's like hiding your code inside an image so it's hard to detect.

Malicious Macro Generator: Generates obfuscated macros with AV/sandbox escape mechanisms. Imagine it as creating tricky macros that bypass antivirus software.

SCT Obfuscator: Cobalt Strike SCT payload obfuscator. It's like making your Cobalt Strike payloads harder to detect.

Invoke-Obfuscation: PowerShell obfuscator. Think of it as scrambling your PowerShell code so it's hard to read.

Invoke-CradleCrafter: PowerShell remote download cradle generator and obfuscator. It's like creating a nest for your malicious code to hatch from.

Invoke-DOSfuscation: Command obfuscation generator and detection test harness. Imagine it as making your commands hard to understand and detect.

morphHTA: Morphs Cobalt Strike's evil.HTA. It's like changing the shape of your malicious code to avoid detection.

Unicorn: PowerShell downgrade attack tool. Think of it as tricking a system into using an older, more vulnerable version of PowerShell.

Shellter: Dynamic shellcode injection tool. It's like injecting your code into a running program.

EmbedInHTML: Embeds and hides files in HTML. Imagine it as hiding your code inside a web page.

SigThief: Steals signatures and makes one invalid. It's like forging a digital signature to make your code look legitimate.

Veil: Generates metasploit payloads that bypass common anti-virus solutions. Think of it as creating payloads that trick antivirus software.

CheckPlease: Sandbox evasion modules. It's like teaching your code to escape from a sandbox environment.

Invoke-PSImage: Embeds PowerShell scripts in PNG files. Imagine it as hiding your code inside an image file.

LuckyStrike: Creates malicious Office macro documents. It's like creating a Trojan horse that looks like a safe Office document.

ClickOnceGenerator: Generates malicious ClickOnce applications. Think of it as creating a fake update that installs your malicious code.

macro_pack: Automates obfuscation and generation of MS Office documents. It's like a factory for creating tricky Office documents.

StarFighters: Empire launcher using JavaScript and VBScript. Imagine it as launching Empire attacks using different scripting languages.

nps_payload: Generates payloads for intrusion detection avoidance. It's like creating code that sneaks past intrusion detection systems.

The Social-Engineer Toolkit: Open-source penetration testing framework for social engineering. Think of it as a toolkit for tricking people into giving you information.

Phishery: Simple SSL-enabled HTTP server for phishing credentials. It's like setting up a fake website to steal login information.

PowerShdll: Runs PowerShell with rundll32 to bypass software restrictions. Imagine it as using a backdoor to run PowerShell when it's not allowed.

Ultimate AppLocker ByPass List: Documents techniques to bypass AppLocker. It's like a cheat sheet for getting around AppLocker restrictions.

Ruler: Interacts with Exchange servers remotely. Think of it as a tool for controlling Exchange servers from afar.

Generate-Macro: Generates malicious Office documents with specified payloads. It's like a macro generator that creates documents with your chosen malicious code.

Malicious Macro MSBuild Generator: Generates malicious macros using MSBuild. Imagine it as using MSBuild to create tricky macros.

Meta Twin: Clones file resources, including digital signatures. It's like making an exact copy of a file, including its digital signature.

[contract=tid]Start Contract[/contract]

???????????? - July 9, 2025, 12:43 pm

Here is a refined version of your post.

Passive & Active Recon Tools

- EyeWitness – Takes screenshots of websites and collects server details.
- AWSBucketDump – Scans AWS S3 buckets for exposed data.
- AQUATONE – Discovers subdomains and scans for forgotten assets.
- spoofcheck – Verifies SPF/DMARC records to check domain spoofability.
- Nmap – Network mapping and service enumeration.
- dnsrecon – Gathers DNS info including subdomains and records.
- dirsearch – Brute-forces web directories and files.
- Sn1per – Automated recon scanner for comprehensive intelligence.
- Social Mapper – Correlates social media profiles across platforms.
- skiptracer – OSINT scraping for personal data (PII).
- FOCA – Extracts metadata from documents (e.g., Office, PDF).
- theHarvester – Collects emails, subdomains, and employees.
- Metagoofil – Gathers metadata from public documents.
- SimplyEmail – Email-based recon and data harvesting.
- truffleHog – Searches for secrets in Git repos.
- pwnedOrNot – Checks email addresses against breach databases.
- GitHarvester – Scrapes GitHub for user/org-related data.
- pwndb – Leaked credentials search via onion services.
- LinkedInt – LinkedIn scraping for personnel mapping.
- CrossLinked – Extracts employee names from search engines.
- findomain – Fast subdomain enumeration using CT logs.

Exploitation and Payload Generation

These tools help build, obfuscate, and deliver payloads that bypass defenses.

Exploit Frameworks & Payload Kits

- WinRAR RCE (CVE-2018-20250) – Exploits old WinRAR path handling.
- Composite Moniker (CVE-2017-8570) – Weaponizes Office documents.
- Exploit toolkit CVE-2017-8759 – Targets .NET deserialization.
- CVE-2017-11882 Exploit – Malicious RTF that runs long commands.
- Adobe Flash Exploit (CVE-2018-4878) – Flash zero-day for RCE.
- Exploit toolkit CVE-2017-0199 – Office/HTA exploit delivery.
- demiguise – Encrypts HTA payloads for Red Team ops.

Payload Obfuscation and Delivery

- Office-DDE-Payloads – DDE execution inside Office docs.
- CACTUSTORCH – C# payload runner for simulated attacks.
- SharpShooter – CSharp payload generator for AV evasion.
- Don't Kill My Cat – Stores shellcode in polyglot images.
- Malicious Macro Generator – Obfuscates Office macros.
- SCT Obfuscator – Obfuscates Cobalt Strike SCT payloads.
- Invoke-Obfuscation – PowerShell script obfuscator.
- Invoke-CradleCrafter – Remote PowerShell cradle generator.
- Invoke-DOSfuscation – Command obfuscation and sandbox testing.
- morphHTA – HTA mutation for Cobalt Strike.
- Unicorn – Downgrades PowerShell for attack compatibility.
- Shellter – Injects shellcode into PE files.
- EmbedInHTML – Embeds payloads into HTML pages.
- SigThief – Clones or fakes PE file signatures.

AV/Sandbox Evasion Tools

- Veil – Metasploit payload obfuscation engine.
- CheckPlease – Sandbox detection and evasion modules.
- Invoke-PSImage – Embeds PowerShell scripts in images.
- LuckyStrike – Generates malicious Office macros with bypasses.
- ClickOnceGenerator – Builds malicious ClickOnce installers.
- macro_pack – Automates obfuscation of Office payloads.
- StarFighters – Empire payload launcher (JS/VBScript).
- nps_payload – Payloads tuned for IDS/IPS evasion.

Social Engineering & Delivery Tools

- SET (Social-Engineer Toolkit) – Framework for social engineering payloads.
- Phishery – Phishing server for SSL credential collection.
- PowerShdll – Executes PowerShell via rundll32.
- Ultimate AppLocker Bypass List – Cheat sheet for AppLocker bypasses.
- Ruler – Interacts with Outlook/Exchange for lateral movement.
- Generate-Macro – Creates macros with custom payloads.
- MSBuild Macro Generator – Embeds macros via MSBuild methods.
- Meta Twin – Clones file resources and digital signatures.

Hope it helps.