Red Teaming Tools - Cheat Sheet

- What Is Red Teaming
- Reconnaissance
  - Web Recon & Asset Discovery
  - Cloud Recon
  - External Network & Infra Recon
  - Email & People OSINT
  - Identity & Metadata Profiling
  - OSINT Automation Frameworks
  - Initial Access & Payload Delivery
- Privilege Escalation Toolkit (Windows & Linux)
- Post-Exploitation and Lateral Movement
  - Post-Exploitation and Lateral Movement Tools (Windows)
  - Post-Exploitation and Lateral Movement Tools (Linux)
- Persistence and Defense Evasion
- Collection, Exfiltration, and Cleanup
- Command and Control (C2) & Reporting (Engagement Wrap-Up)

What Is Red Teaming

Red teaming is a security assessment technique that simulates the actions of a real-world attacker. Unlike traditional penetration testing, which focuses on identifying vulnerabilities within a defined scope, red teaming takes a broader, more adversarial approach. The engagement typically begins with minimal information, often limited to the name of the target organization, and without any internal access or credentials. From this starting point, the red team conducts reconnaissance, maps exposed infrastructure, and identifies potential entry points. These weak spots may include misconfigured servers, unsecured cloud storage, vulnerable web applications, or even human-based attack vectors such as phishing.

Once an initial foothold is gained, the red team proceeds based on the objective of the engagement, which might involve exfiltrating sensitive data, compromising specific internal systems, or demonstrating how deeply an attacker could infiltrate the environment. Throughout this process, the red team maintains operational security (OPSEC) to avoid detection, mimicking the behavior of advanced persistent threats. After gaining access, the team performs internal reconnaissance, escalates privileges, moves laterally within the network, and attempts to access high-value assets such as domain administrator accounts or root privileges in an infrastructure. The core purpose of red teaming is not just to break into systems, but to assess how effectively

an organization can detect, respond to, and recover from sophisticated, real-world attacks.

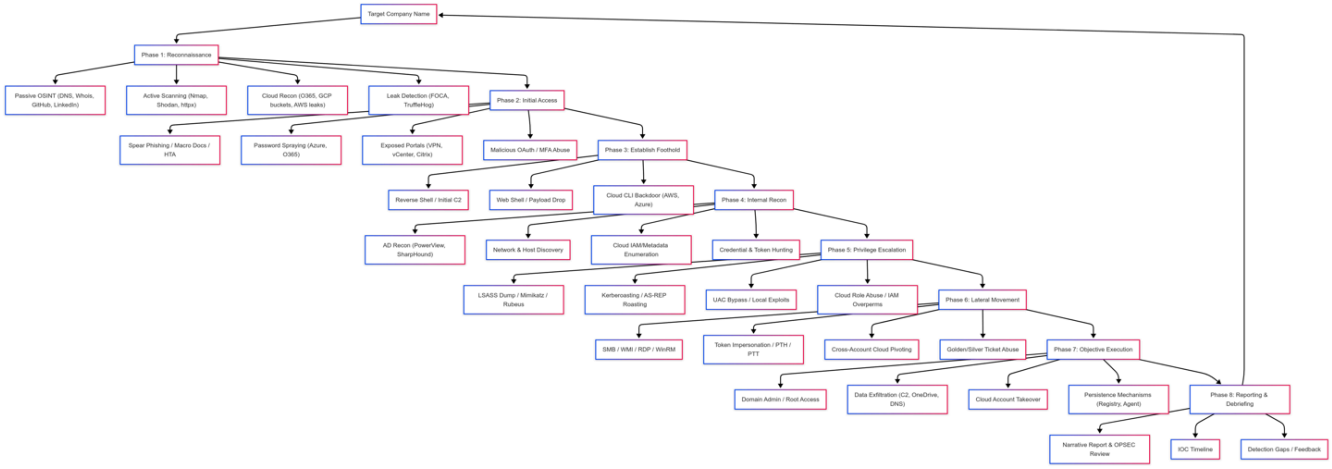


fig 1.0 - Red Teaming Phases Overview

Reconnaissance

Web Recon & Asset Discovery

Tool Name	Purpose	Description	GitHub Link
Subfinder	Passive subdomain enumeration	Identifies exposed apps and APIs using public data without interacting with the target.	GitHub - projectdiscovery/subfinder: Fast passive subdomain enumeration tool.
Amass	Deep OSINT subdomain discovery	Uncovers hidden or legacy domains using certificates, WHOIS, and internet datasets.	GitHub - owasp-amass/amass: In-depth attack surface mapping and asset discovery
httpx	Live HTTP/HTTPS probing	Extracts metadata from domains: status, redirects, IPs, tech stack. Helps prioritize targets.	GitHub - projectdiscovery/httpx: httpx is a fast and multi-purpose HTTP toolkit that allows running multiple probes using the retryablehttp library.

dnsx	DNS resolution	Filters valid domains post-enumeration. Supports wildcard checks and DNS takeover validation.	GitHub - projectdiscovery/dnsx: dnsx is a fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list of user-supplied resolvers.
nmap	Port scanning & banner grabbing	Identifies live hosts, services, versions. Works externally when scoped correctly.	Nmap: the Network Mapper - Free Security Scanner
gau	Archived URL discovery	Retrieves historical endpoints from Wayback Machine, AlienVault, and Common Crawl.	GitHub - lc/gau: Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl.
waybackurls	Wayback Machine URL pulling	Complements gau by strictly querying Internet Archive data. Useful for legacy route detection.	GitHub - tomnomnom/waybackurls: Fetch all the URLs that the Wayback Machine knows about for a domain
ffuf	Web fuzzer for directories/files	Discovers hidden folders, parameters, and debug routes quickly. Highly scriptable.	GitHub - ffuf/ffuf: Fast web fuzzer written in Go
dirsearch	Directory brute-forcer	Brute-forces for known folder/file paths using wordlists. Finds admin panels, backups, etc.	GitHub - maurosoria/dirsearch: Web path scanner

aquatone	Screenshot aggregator	Captures screenshots of all subdomains to visually identify interesting services or portals.	GitHub - michenriksen/aquatone: A Tool for Domain Flyovers
wafw00f	WAF/CDN detection	Detects common WAFs like Cloudflare, Akamai, etc. Helps plan bypasses or payload design.	GitHub - EnableSecurity/wafw00f: WAFW00F allows one to identify and fingerprint Web Application Firewall (WAF) products protecting a website.
whatweb	Web technology fingerprinting	Detects CMS, web frameworks, server banners, and more. Helps identify CVE exposure paths.	GitHub - urbanadventurer/WhatWeb: Next generation web scanner
asnlookup	ASN & Netblock mapping	Maps company IP ranges using ASN data. Reveals cloud services and legacy IP blocks.	GitHub - yassineaboukir/Asnlookup: Leverage ASN to look up IP addresses (IPv4 & IPv6) owned by a specific organization for reconnaissance purposes, then run port scanning on it.

Cloud Recon

Tool Name	Purpose	Why It Matters	GitHub Link
S3Scanner	AWS S3 bucket enumeration	Scans for public/misconfigured S3 buckets using brute force and recon wordlists. Great for	GitHub - sa7mon/S3Scanner: Scan for misconfigured S3 buckets across S3-compatible APIs!

		sensitive data discovery.	
GCPBucketBrute	GCP bucket brute-forcer	Discovers GCP cloud storage buckets by guessing names based on OSINT or brute-force lists.	GitHub - RhinoSecurityLabs/GCPBucketBrute: A script to enumerate Google Storage buckets, determine what access you have to them, and determine if they can be privilege escalated.
cloud_enum	AWS, Azure, GCP recon	Maps public cloud infrastructure using domain or company name. Identifies buckets, functions, and services.	GitHub - initstring/cloud_enum: Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud.
truffleHog	Secrets detection in git/code	Searches public repositories for leaked cloud secrets (e.g., AWS keys) using regex and entropy checks.	GitHub - trufflesecurity/trufflehog: Find, verify, and analyze leaked credentials
Shodan CLI	Internet-wide cloud host scanner	Leverages Shodan to find exposed ports, services, and misconfigured devices in cloud environments.	GitHub - achillean/shodan-python: The official Python library for Shodan
Censys CLI	Exposed services search engine	Searches exposed cloud assets and SSL certs using Censys. Good for cloud infra mapping.	GitHub - censys/censys-python: An easy-to-use and lightweight API wrapper for Censys APIs.

Bucket Finder	AWS bucket guesser	Bruteforces S3 bucket names based on keywords and domain names.	GitHub - gwen001/s3-buckets-finder: Find AWS S3 buckets and test their permissions.

External Network & Infra Recon

Tool Name	Purpose	Description	GitHub Link
Nmap	Network scanning & service enumeration	Identifies open ports, services, and banners of externally exposed IPs. Helps understand network surface.	Nmap: the Network Mapper - Free Security Scanner
Masscan	Fast port scanner	Extremely fast scanner to map open ports across large IP ranges. Good for mapping cloud infra quickly.	GitHub - robertdavidgraham/masscan: TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
Shodan CLI	Public service discovery	Finds exposed devices, services, and cloud assets indexed by Shodan. Useful for broad internet-facing asset hunting.	GitHub - achillean/shodan-python: The official Python library for Shodan
Censys CLI	Certificate and asset search	Discovers assets via SSL/TLS certs and metadata. Reveals unknown subdomains and IPs.	GitHub - censys/censys-python: An easy-to-use and lightweight API wrapper for Censys APIs.
Netcat	Network communication testing	Swiss-army knife for manual service interaction, banner	Ncat - Netcat for the 21st Century

		grabbing, and response behavior observation.	
ZMap	Internet-scale port scanning	Fast scanning engine to analyze full internet IP spaces. Requires permission and proper targeting.	GitHub - zmap/zmap: ZMap is a fast single packet network scanner designed for Internet-wide network surveys.
DNSTwist	Domain permutation & typo detection	Identifies potential phishing domains or typo-squats to detect malicious look-alikes.	GitHub - elceef/dnstwist: Domain name permutation engine for detecting homograph phishing attacks, typo squatting, and brand impersonation
Fierce	DNS-based network mapping	Performs DNS bruteforce and internal network mapping by querying authoritative nameservers.	GitHub - mschwager/fierce: A DNS reconnaissance tool for locating non-contiguous IP space.
ASNlookup	ASN ownership discovery	Identifies IP ranges associated with an organization. Great for understanding their public IP space.	GitHub - yassineaboukir/Asnlookup: Leverage ASN to look up IP addresses (IPv4 & IPv6) owned by a specific organization for reconnaissance purposes, then run port scanning on it.

Email & People OSINT

Tool Name	**Type**	**Description**	**Link**

Hunter	Web App	Finds email addresses associated with a domain, validates deliverability, and discovers email formats.	Find email addresses and send cold emails • Hunter
EmailRep	API / Recon	Checks email reputation, breach history, social links, and malicious behavior indicators.	https://emailrep.io
Holehe	CLI Tool	Checks if an email address is used on 50+ websites by attempting password reset endpoints.	GitHub - megadose/holehe: holehe allows you to check if the mail is used on different sites like twitter, instagram and will retrieve information on sites with the forgotten password function.
WhatsMyName	Username OSINT	Checks for a username/email across hundreds of social platforms. Great for identity correlation.	GitHub - WebBreacher/WhatsMyName: This repository has the JSON file required to perform user enumeration on various websites.
Have I Been Pwned (HIBP)	Breach Database	Checks if an email or username has been part of known data breaches.	Have I Been Pwned: Check if your email address has been exposed in a data breach

theHarvester	CLI Tool	Collects email addresses and names from public sources such as search engines and PGP keyservers.	GitHub - laramies/theHarvester: E-mails, subdomains and names Harvester - OSINT
LinkedInt	OSINT Script	Scrapes LinkedIn (if cookies provided) to enumerate employees of a target company.	GitHub - vysecurity/LinkedInt: LinkedIn Recon Tool
PeopleFinderFree / FastPeopleSearch	Web Service	U.S.-based people search engine — useful for deanonymizing or mapping personal networks.	https://www.fastpeoplesearch.com
EmailFinder (Apollo / Skrapp / Lusha)	Web Services	Useful for discovering business contacts, professional email enrichment. **(Some require login)**	AI Sales Platform | Apollo.io - Outbound, Inbound & Automation / Skrapp.io | Find Emails & B2B Leads from LinkedIn
Google Dorking	Manual	Use specific queries like site:linkedin.com "@company.com" or "@domain.com" to find emails and profiles.	Manual via Google
GHunt	Gmail OSINT	Investigates Gmail addresses using metadata from Google services (YouTube, Docs, Calendar).	GitHub - mxrch/GHunt: 🕵️ Offensive Google framework.

Identity & Metadata Profiling

Tool Name	Purpose	Description	GitHub Link
ExifTool	Metadata extractor for files/images	Extracts hidden metadata (GPS, author, creation dates, device info) from PDFs, DOCs, images — useful for deanonymizing users or discovering leaks.	GitHub - exiftool/exiftool: ExifTool meta information reader/writer
Metagoofil	Public doc scraper + metadata parser	Searches Google for public PDFs, DOCs, XLS and extracts usernames, email formats, server paths, etc.	GitHub - opsdisk/metagoofil: Search Google and download specific file types
FOCA	Metadata extractor with GUI (Windows)	Automates metadata extraction from office files found online — great for non-tech users and targeting Windows infra.	GitHub - ElevenPaths/FOCA: Tool to find metadata and hidden information in the documents.
pdf-parser.py	PDF structure analysis	Analyzes embedded JavaScript, metadata, and structure in malicious or leaked PDFs.	GitHub - DidierStevens/DidierStevensSuite: Please no pull requests for this repository. Thanks!
oletools	Office doc analysis (macros & metadata)	Parses .doc/.xls/.ppt for macros, hidden streams, and metadata — useful in phishing investigations or file footprinting.	GitHub - decalage2/oletools: oletools - python tools to analyze MS OLE2 files (Structured Storage, Compound File Binary Format) and MS Office docu

			ments, for malware analysis, forensics and debugging.
strings (Sysinternals/Linux)	Basic string analysis	Extracts readable strings from binary files or documents. Good for finding usernames, paths, or keys within files.	Strings - Sysinternals

OSINT Automation Frameworks

Tool Name	Purpose	Description	
SpiderFoot	Full-spectrum OSINT automation	Provides a powerful web UI or CLI interface to automate recon using over 100 data sources — from domains to usernames.	GitHub - smicallef/spiderfoot: SpiderFoot automates OSINT for threat intelligence and mapping your attack surface.
ReconFTW	Automated recon pipeline	Orchestrates subfinder, amass, nuclei, gau, waybackurls, and more in a full recon chain with zero config.	GitHub - six2dez/reconftw: reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities
Osmedeus	Modular recon automation framework	Out-of-the-box automation for subdomains, port scans, screenshots, vuln scan, and more.	GitHub - j3ssie/osmedeus: A Workflow Engine for Offensive Security

		Suitable for continuous recon.	
sn0int	OSINT engine for identities	Graph-based identity correlation using usernames, emails, and domains. Extensible with custom modules.	GitHub - kpcyrd/sn0int: Semi-automatic OSINT framework and package manager
Maltego CE	Graphical OSINT mapping (GUI)	Visual link-analysis tool for mapping relationships between domains, emails, people, and infrastructure.	Downloads
Recon-ng	Metasploit-style OSINT framework	Modular and scriptable framework that pulls from multiple APIs. Ideal for CLI-based multi-vector recon.	GitHub - lanmaster53/recon-ng: Open Source Intelligence gathering tool aimed at reducing the time spent harvesting information from open sources.
H8mail	Email breach lookup tool	Finds data breaches, passwords, and leak info associated with target emails using multiple free services.	GitHub - khast3x/h8mail: Email OSINT & Password breach hunting tool, locally or using premium services. Supports chasing down related email
datasploit	Passive data correlation toolkit	Aggregates subdomain, email, phone, breach, and social info in a modular recon environment.	GitHub - DataSploit/datasploit: An #OSINT Framework to perform various recon techniques on Companies, People, Phone Number, Bitcoin Addresses, e

			tc., aggregate all the r aw data, and give dat a in multiple formats.

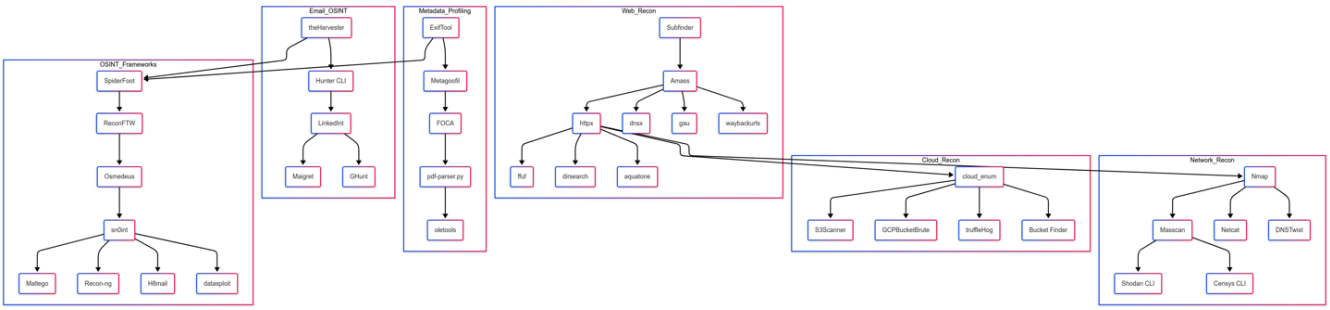


fig 2.0 - Initial Recon Channing Strategy

Initial Access & Payload Delivery

Tool Name	Purpose	Description	Link
Gophish	Phishing campaign platform	Easy-to-use platform for creating phishing emails, tracking opens, clicks, and submitted credentials.	GitHub - gophish/g ophish: Open-Source Phishing Toolkit
Evilginx2	Phishing proxy & session hijack	Captures 2FA-protected sessions using reverse proxy to clone login pages. Ideal for credential + session harvesting.	GitHub - kgretzky/e vilginx2: Standalone man-in-the-middle att ack framework used f or phishing login cred entials along with ses sion cookies, allowing for the bypass of 2-fa ctor authentication
Phishery	Word document macro generator	Injects macro payloads into Word docs that pull in remote payloads from HTTP servers. Great	GitHub - ryhanson/ phishery: An SSL Ena bled Basic Auth Crede ntial Harvester with a Word Document Tem plate URL Injector

		for phishing weaponization.	
MacroPack	Microsoft Office payload generator	Obfuscates and automates macro payload delivery for Word/Excel/PPT documents.	GitHub - sevagas/macro_pack: macro_pack is a tool by @EmericNasi used to automatize obfuscation and generation of Office documents, VB scripts, shortcuts, and other formats for pentest, demo, and social engineering assessments. The goal of macro_pack is to simplify exploitation, antimalware bypass, and automatize the process from malicious macro and script generation to final document generation. It also provides a lot of helpful features useful for redteam or security research.
Nishang	PowerShell offensive scripts	Includes scripts for payload delivery, privilege escalation, and C2 launch. Excellent for in-memory payload execution.	GitHub - samratashok/nishang: Nishang - Offensive PowerShell for red team, penetration testing and offensive security.
Unicorn	Powershell attack payload generator	Creates PowerShell-based shellcode injectors for	GitHub - trustedsec/unicorn: Unicorn is a simple tool for using a PowerShell downgra

		Metasploit, Cobalt Strike, etc.	de attack and inject s hellcode straight into memory. Based on M atthew Graeber's pow ershell attacks and th e powershell bypass t echnique presented b y David Kennedy (Tru stedSec) and Josh Kel ly at Defcon 18.
Shellter	PE file backdoor injector	Injects custom payloads into Windows binaries for evasive trojans. Supports dynamic backdooring of legitimate apps.	Download
Metasploit Framework	Exploits & payloads	Framework for delivering exploits and generating payloads. Supports MS Office, browser, and macro delivery vectors.	GitHub - rapid7/met asploit-framework: M etasploit Framework
msfvenom	Payload builder for Metasploit	Creates shellcode and trojan binaries across platforms. Customizable for stageless/staged payloads.	https://docs.metasploi t.com/docs/using-metasploit/msfvenom. html
Donut	.NET and PE in-memory loader	Generates shellcode for .NET assemblies and EXEs that can be injected into memory without touching disk.	GitHub - TheWover/ donut: Generates x86, x64, or AMD64+x86 position-independent shellcode that loads . NET Assemblies, PE fi

			les, and other Windows payloads from memory and runs them with parameters
Covenant	.NET C2 framework	A powerful, browser-based C2 for red teamers. Supports payload generation, listener setup, tasking, and more.	GitHub - cobbr/Covenant: Covenant is a collaborative .NET C2 framework for red teamers.
Sliver	Golang-based C2 framework	A modern alternative to Cobalt Strike. Offers encrypted payloads, implants, pivoting, and listener modules.	GitHub - BishopFox/sliver: Adversary Emulation Framework
MSBuild+Inline Tasks	Living-off-the-land payload	Executes payloads by abusing MSBuild on target Windows systems — no dropped binaries needed.	GitHub - Mr-Un1k0d3r/LOLBAS: Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)
DSViper	Custom payload builder to bypass Windows Defender and EDR	DSViper creates evasive PE payloads (EXE/DLL) using obfuscation and encryption. It supports DLL sideloading and shellcode injection, making it ideal for red team operations where stealth is critical.	GitHub - dagowda/DSViper: This is for Ethical Use only. The default automated binaries created are all burned. I have added the script to the repo to modify certain signatures and it will still work.

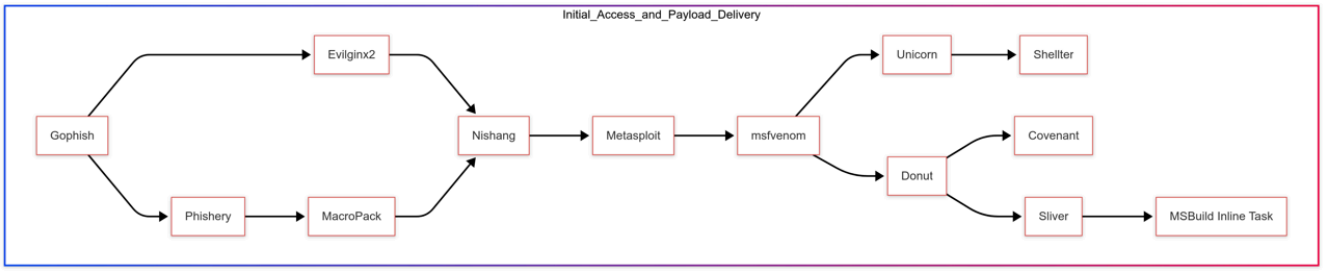


fig 3.0 - Initial Access Payload Delivery Chaining

Privilege Escalation Toolkit (Windows & Linux)

Tool Name	Platform	Description	GitHub Link
SharpUp	Windows	C# tool to enumerate privilege escalation vectors including service misconfigurations, UAC settings, and token privileges.	GitHub - GhostPack/SharpUp: SharpUp is a C# port of various PowerUp functionality.
Seatbelt	Windows	Security-oriented enumeration tool collecting information about installed software, tokens, credentials, UAC configs, and more.	GitHub - GhostPack/Seatbelt: Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.
WinPEAS	Windows	Privilege escalation auditing script detecting vulnerable services, scheduled tasks, registry issues, and more.	GitHub - peass-ng/PEASS-ng: PEASS - Privilege Escalation Awesome Scripts SUITE (with colors)
PowerUp	Windows	PowerShell module to discover misconfigurations that	PowerSploit/Privesc at master · PowerShellMafia/PowerSploit

		can allow privilege escalation including service abuse and insecure permissions.	
Watson	Windows	Identifies missing patches on Windows systems that may be exploited for privilege escalation through kernel vulnerabilities.	GitHub - rasta-mouse/Watson: Enumerate missing KBs and suggest exploits for useful Privilege Escalation vulnerabilities
SafetyKatz	Windows	Modified Mimikatz variant designed for safer in-memory credential dumping during post-exploitation.	GitHub - GhostPack/SafetyKatz: SafetyKatz is a combination of slightly modified version of @gentilkiwi's Mimikatz project and @subtee's .NET PE Loader
BadPotato / JuicyPotatoNG / RoguePotato	Windows	Exploitation frameworks for abusing token impersonation vulnerabilities to escalate from local service accounts to SYSTEM privileges.	GitHub - ohpe/juicy-potato: A sugared version of RottenPotatoNG, with a bit of juice, i.e. another Local Privilege Escalation tool, from a Windows Service Accounts to NT AUTHORITY\SYSTEM.

Tool Name	Platform	Description	GitHub Link
LinPEAS	Linux	Automated enumeration script for detecting privilege escalation paths such as SUID binaries,	GitHub - peass-ng/PEASS-ng: PEASS - Privilege Escalation Awesome Scripts SUITE (with colors)

		writable paths, kernel exploits, and weak services.	
Linux Smart Enumeration (LSE)	Linux	Focused and categorized local enumeration tool designed to highlight potential privilege escalation paths clearly.	GitHub - diego-treitos/linux-smart-enumeration: Linux enumeration tool for pentesting and CTFs with verbosity levels
BeRoot (Linux)	Linux	Post-exploitation script for discovering common Linux misconfigurations and vulnerabilities leading to privilege escalation.	GitHub - AlessandroZ/BeRoot: Privilege Escalation Project - Windows / Linux / Mac
pspy	Linux	Process snooping utility that allows detection of scripts, cron jobs, or binaries being executed by other users without root access.	GitHub - DominicBreuker/pspy: Monitor linux processes without root permissions
LES (Linux Exploit Suggester)	Linux	Scans the Linux system version and suggests known kernel exploits suitable for privilege escalation.	GitHub - The-Z-Labs/linux-exploit-suggester: Linux privilege escalation auditing tool
GTFOBins	Linux	Collection of Unix binaries that can be exploited by attackers to bypass local security restrictions	GTFOBins

		and escalate privileges.	

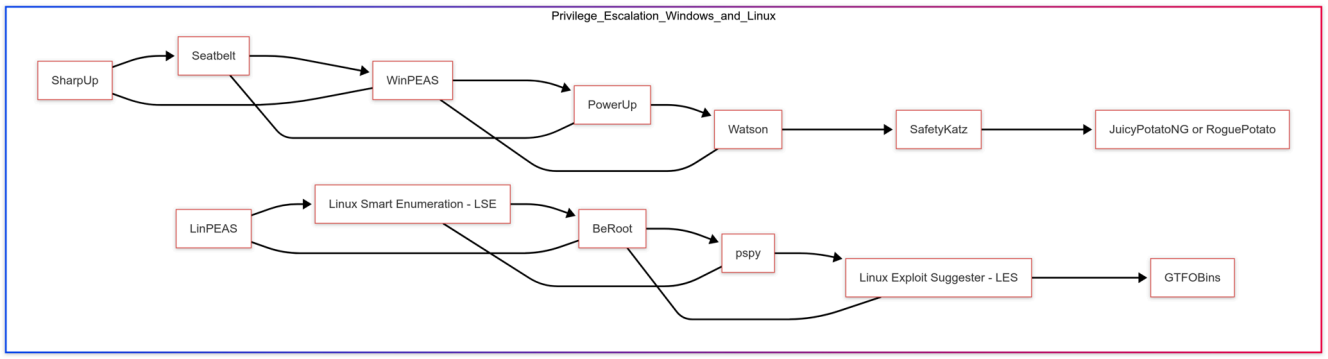


fig - 4.0 - Privilege escalation

Post-Exploitation and Lateral Movement

Post-Exploitation and Lateral Movement Tools (Windows)

Tool Name	Platform	Description	GitHub Link
Mimikatz	Windows	Credential extraction tool capable of pulling plaintext passwords, hashes, tickets, and keys from memory.	GitHub - gentilkiwi/mimikatz: A little tool to play with Windows security
Rubeus	Windows	Toolset for Kerberos abuse including ticket extraction, ticket forging, and pass-the-ticket attacks.	GitHub - GhostPack/Rubeus: Trying to tame the three-headed dog.
SharpHound	Windows	Active Directory enumeration tool used to gather data for BloodHound. Helps in identifying lateral movement paths inside domains.	GitHub - SpecterOps/SharpHound: C# Data Collector for BloodHound

BloodHound	Windows	Analysis platform that visualizes Active Directory objects and relationships to identify attack paths.	GitHub - SpecterOps/BloodHound-Legacy: Six Degrees of Domain Admin
Evil-WinRM	Windows	A post-exploitation WinRM shell for interacting with compromised Windows servers securely and stealthily.	GitHub - Hackplayers/evil-winrm: The ultimate WinRM shell for hacking/pentesting
CrackMapExec (CME)	Windows	Swiss army knife for internal network pentesting: password spraying, enumeration, exploitation, lateral movement across SMB, WinRM, MSSQL.	GitHub - byt3bl33d3r/CrackMapExec: A swiss army knife for pentesting networks
Covenant	Windows	Post-exploitation Command and Control (C2) framework with encrypted communication and multi-user management.	GitHub - cobbr/Covenant: Covenant is a collaborative .NET C2 framework for red teamers.
SharpMove	Windows	Tool for performing lateral movement operations using Windows native features such as DCOM, WMI, PSExec.	GitHub - SharpMove/SharpMove: Config files for my GitHub profile.

Post-Exploitation and Lateral Movement Tools (Linux)

Tool Name	Platform	Description	GitHub Link
Impacket (toolset)	Linux	Collection of Python scripts for network protocol abuse: SMB, Kerberos, NTLM relay, PSExec, WMIExec, and more.	GitHub - fortra/impacket: Impacket is a collection of Python classes for working with network protocols.
CrackMapExec (Linux Version)	Linux	Swiss army knife for network exploitation including SMB, LDAP enumeration, Kerberos abuse, and remote command execution.	GitHub - byt3bl33d3r/CrackMapExec: A swiss army knife for pentesting networks
Evil-SSDP	Linux	Tools to exploit Universal Plug and Play (UPnP) for lateral movement and device discovery in misconfigured networks.	GitHub - initstring/evil-ssdp: Spoof SSDP replies and create fake UPnP devices to phish for credentials and NetNTLM challenge/response.
Responder	Linux	LLMNR, NBT-NS, and MDNS poisoner for capturing network hashes and relaying authentication attempts in internal networks.	GitHub - lgandx/Responder: Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.
BloodHound-python	Linux	BloodHound data collector alternative	GitHub - dirkjanm/BloodHound.py: A Pyth

		written in Python, useful when Windows agents are detected.	on based ingestor for BloodHound
NTLMRelayX	Linux	NTLM relay attacks tool allowing abuse of SMB, HTTP, and LDAP relays for unauthorized authentication forwarding.	impacket/examples/ntlmrelayx.py at master · fortra/impacket

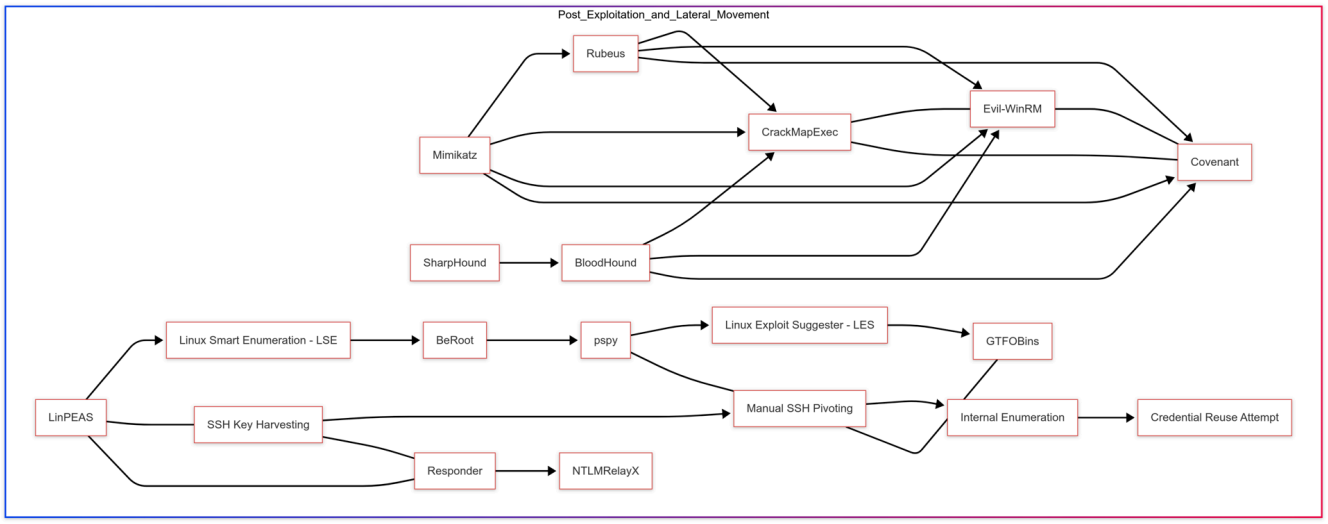


fig 5.0 - Post Exploitatio Chaining for both windows and linux

Persistence and Defense Evasion

Persistence and Defense Evasion Tools (Windows)

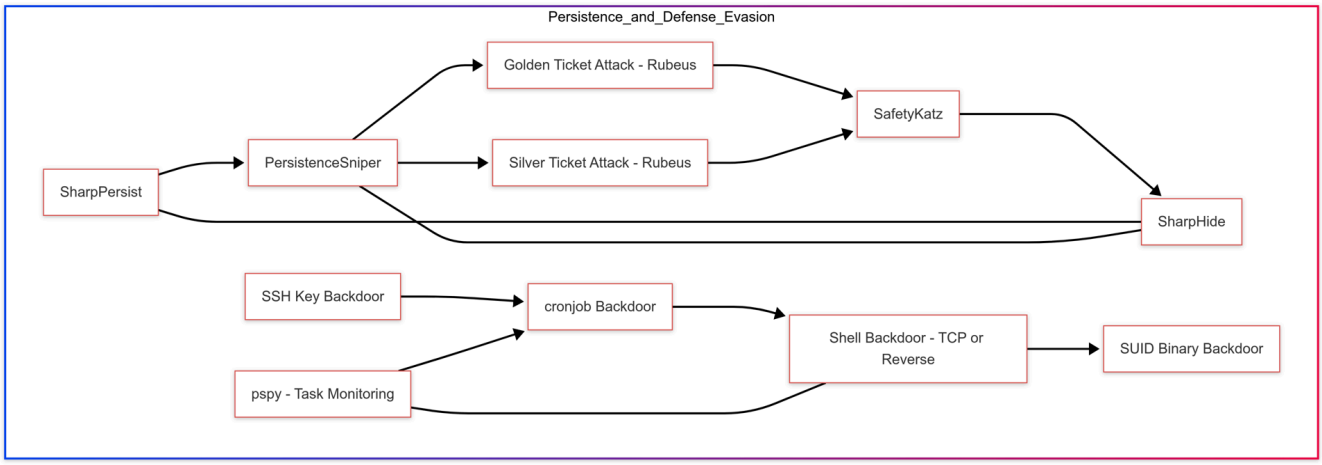
Tool Name	Platform	Description	GitHub Link
Evil-WinRM (Post-Exploitation Use)	Windows	Maintains access by executing payloads remotely over WinRM after compromise.	GitHub - Hackplayers/evil-winrm: The ultimate WinRM shell for hacking/pentesting
Golden Ticket Attack (Rubeus)	Windows	Abuse Kerberos Ticket Granting Tickets (TGTs) to create	GitHub - GhostPack/Rubeus: Trying to ta

		indefinite domain persistence without needing password resets.	me the three-headed dog.
Silver Ticket Attack (Rubeus)	Windows	Abuse service tickets to maintain persistence at the service level without hitting the domain controller.	GitHub - GhostPac k/Rubeus: Trying to ta me the three-headed dog.
SafetyKatz	Windows	Mimikatz derivative used to dump credentials without being easily caught by AV, aiding persistence access cycles.	GitHub - GhostPac k/SafetyKatz: SafetyK atz is a combination o f slightly modified ver sion of @gentilkiwi's Mimikatz project and @subtee's .NET PE Lo ader

Persistence and Defense Evasion Tools (Linux)

Tool Name	Platform	Description	GitHub Link
SSH Backdoor (manual or scripts)	Linux	Adding SSH public keys manually to .ssh/authorized_keys to maintain stealthy persistent access.	Manual / custom
cronjob backdoors (manual or LinPEAS findings)	Linux	Setting persistent reverse shells or payloads into crontab entries.	Built-in system feature
pspy (Post-Exploitation Use)	Linux	Monitor scheduled tasks and hijackable scripts to plant persistent access.	GitHub - DominicBr euker/pspy: Monitor li nux processes withou t root permissions

Shell Backdoor (TCP bind or reverse shells)	Linux	Setting simple shell scripts to rebind or reverse connection after reboot to attacker-controlled machine.	Manual
SUID Backdoor	Linux	Creating SUID binaries to allow privilege escalation or persistent local access even if regular access is revoked.	Manual creation



Collection, Exfiltration, and Cleanup

Collection and Exfiltration Tools (Windows)

Tool Name	Platform	Description	GitHub Link
Rubeus	Windows	Collects Kerberos tickets, user sessions, and can exfiltrate sensitive credential artifacts.	GitHub - GhostPack/Rubeus: Trying to tame the three-headed dog.
Seatbelt	Windows	Collects detailed information about	GitHub - GhostPack/Seatbelt: Seatbelt is

		system artifacts including browser history, saved credentials, cloud service sessions, and tokens.	a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.
SharpHound (Data Collection Phase)	Windows	Collects extensive Active Directory object relationships and user rights useful for lateral movement and persistence planning.	GitHub - SpecterOps/SharpHound: C# Data Collector for BloodHound
LaZagne	Windows	Post-exploitation tool to collect passwords stored in common applications and the operating system.	GitHub - AlessandroZ/LaZagne: Credentials recovery project
SharpView	Windows	Enumerates user sessions, groups, ACLs, and other sensitive data in Active Directory for potential abuse and lateral movement.	GitHub - tevora-threat/SharpView: C# implementation of harmj0y's PowerView

Collection and Exfiltration Tools (Linux)

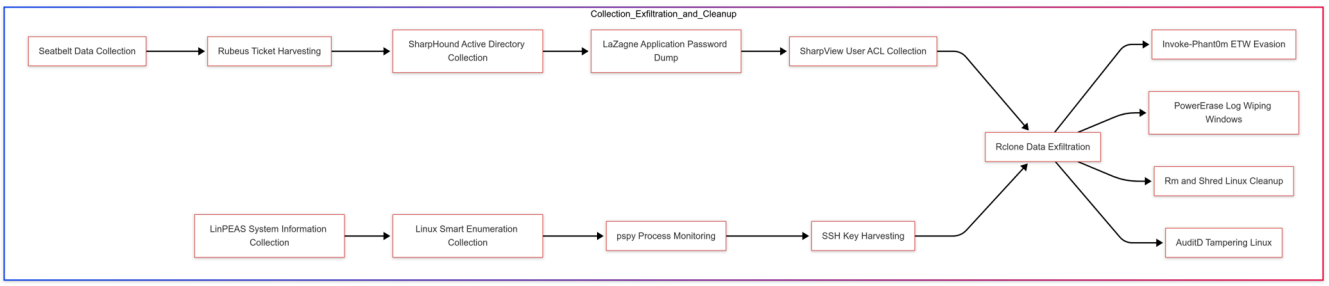
Tool Name	Platform	Description	GitHub Link
LinPEAS (Collection Phase)	Linux	Collects system information including SSH keys, password hashes, running services, and environment	GitHub - peass-ng/PEASS-ng: PEASS - Privilege Escalation Awesome Scripts SUITE (with colors)

		credentials for exploitation.	
Pspy (Process Snooping)	Linux	Collects live information about running processes, cron jobs, and services to identify sensitive operations.	GitHub - DominicBreuker/pspy: Monitor linux processes without root permissions
SSH Key Harvesting	Linux	Manual process of collecting all .ssh/authorized_keys and private key files across compromised systems.	Manual
Linux Smart Enumeration (Collection Mode)	Linux	Aggregates critical data about users, groups, SUID files, cron jobs, accessible NFS shares, and system information.	GitHub - diego-treitos/linux-smart-enumeration: Linux enumeration tool for pentesting and CTFs with verbosity levels
Rclone (Exfiltration)	Linux	Tool used for stealthily uploading collected files, credentials, and sensitive data to cloud storage platforms like Dropbox, Google Drive, or AWS.	Rclone

Cleanup Tools and Methods (Both Windows and Linux)

Tool Name	Platform	Description	GitHub Link
Invoke-Phant0m	Windows	PowerShell script to evade detection by disabling Event	GitHub - hlldz/Phant0m: Windows Event Log Killer

		Tracing for Windows (ETW) providers.	
Rm and Shred (Manual)	Linux	Native Unix commands (rm, shred) used to remove or overwrite artifacts such as uploaded scripts, output files, temporary binaries, or session artifacts.	Built-in
AuditD Tampering	Linux	Disable or tamper audit daemon rules to reduce monitoring visibility post-compromise.	Manual or scripted



Command and Control (C2) & Reporting (Engagement Wrap-Up)

Command and Control (C2) Tools

Tool Name	Platform	Description	GitHub Link
Covenant	Windows	C2 framework for .NET payloads with multi-user support, secure HTTP comms, tasking, keylogging, and persistence management.	GitHub - cobbr/Covenant: Covenant is a collaborative .NET C2 framework for red teamers.

Sliver	Cross-platform	Open-source Golang-based C2 framework supporting multiple OS implants, encrypted comms, user management, lateral movement.	GitHub - BishopFox/sliver: Adversary Emulation Framework
Mythic	Cross-platform	Modular and modern C2 platform supporting various agents (Linux, Windows, Mac) with UI, scripting, and OPSEC profiles.	GitHub - its-a-feature/Mythic: A collaborative, multi-platform, red teaming framework
Merlin	Windows/Linux	Encrypted post-exploitation agent using HTTP/2 and support for staging, shell execution, and file transfers.	GitHub - Ne0nd0g/merlin: Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.
Havoc	Windows/Linux	Modern post-exploitation framework with evasive implants, shellcode injection, and UI for coordination.	GitHub - HavocFramework/Havoc: The Havoc Framework

Reporting & Cleanup (End of Engagement)

Tool	Description
Markdown/Obsidian	Use structured markdown to document phase-by-phase activity, tools used, and timelines.

BloodHound Reports	Export AD graph data to include lateral paths and exposed objects in the report.
IOC Generation	Use custom scripts or tools like **Sigma**, **Velociraptor**, or **YARA** to provide Indicators of Compromise for blue team.
Final Cleanup Scripts	Use pre-written scripts to remove C2, persistence mechanisms, and wipe logs across endpoints.