Cross-Chapter Engagement & MITRE ATT&CK Vocabulary Reference

8,967 words · ~41 min read

---

*Cross-chapter shared reference primarily for `vca-pen-101` (Penetration Testing). Secondary cross-references from `vca-adv-101` (Adversarial Capstone), `vca-adv-102` (AI & Agentic Security), and `vca-sec-101` (Foundations / Defense). Companion handouts: `cross-chapter-cve-class-vocabulary-reference.md` (classical CVE families) and `cross-chapter-llm-asi-vocabulary-reference.md` (LLM-era taxonomy). *

Purpose. Single canonical academy-wide vocabulary set for the engagement-lifecycle methodology, the MITRE ATT&CK Enterprise matrix, the OWASP Top 10 (web apps, current edition), and the OSCP-prep procedural vocabulary. Belt-3 PEN-101 graduates need to **recognize the ATT&CK tactics and named techniques when they read incident-response write-ups**, **name the engagement-lifecycle phases when they discuss scope and reporting with clients**, and **deploy the OSCP-prep methodology vocabulary when they sit the OffSec PEN-200 examination**. This handout supplies the vocabulary scaffold; PEN-101 labs supply the methodology-tier reproduction work against intentionally-vulnerable lab harnesses under explicit `--authorized-by` discipline.

Print and pin during PEN-101 Week 1 (Engagement lifecycle), Week 5 (Vulnerability identification), Week 7 (Exploitation I), Week 9 (Post-exploitation), Week 10 (Lateral movement), and Week 11 (Reporting). Cross-track pickup at SEC-101 Module 5 (Authentication architectures), ADV-101 Week 1 (Belt-5 vocabulary onboarding), and ADV-102 Week 4 (AI-era ATT&CK extensions).

---

§1: Purpose and scope

This handout is the academy's **vocabulary-tier set** for offensive-direction engagement work: a deliberately taxonomic reference that names the seven engagement-lifecycle phases the PEN-101 syllabus follows, walks ~40 MITRE ATT&CK technique IDs across the eleven tactics most relevant to entry-tier penetration testing, names the OWASP Top 10 (2021 edition) at full taxonomy depth with CWE pairings, and supplies the OSCP-prep

methodology vocabulary the OffSec PEN-200 examination assumes. It is **not** a methodology reference (PEN-101 labs supply that), **not** an exploit-development handbook (RE-201 + Part-II RE electives + post-academy work like OSED / GXPN cover that), and **not** a tradecraft manual for unauthorized testing (every offensive technique named carries the implicit reminder that legitimate exercise requires `--authorized-by` clearance against intentionally-vulnerable lab harnesses, never against production systems).

The scope this handout covers. Four taxonomies that together compose the entry-tier penetration-tester's working vocabulary: the seven-phase engagement lifecycle (§5), the MITRE ATT&CK Enterprise matrix at PEN-101 depth (§2), the OWASP Top 10 web-application vulnerability taxonomy (§4), and the OSCP-prep procedural vocabulary (§3). The four taxonomies are not exhaustive (Active-Directory-specific TTPs, container-and-Kubernetes attack surfaces, cloud-native engagement patterns, and operational-technology engagement work each warrant their own future handouts), but they cover the recognition-level vocabulary a Belt-3 PEN-101 graduate needs for OSCP-prep + report writing + first-engagement client conversations during their first one to three years of professional practice.

The vocabulary-tier vs methodology-tier distinction. A vocabulary-tier handout teaches students to **recognize and name** what they encounter in disclosure write-ups, incident-response post-mortems, and client-side debriefs. A methodology-tier handout teaches students to **reproduce, exploit, or defend against** the technique. The two tiers serve different pedagogical purposes and should not be conflated. PEN-101's primary teaching surface is eleven graded labs plus a five-day simulated capstone engagement, all reproduced at methodology depth against intentionally-vulnerable lab harnesses; this handout's ~40 ATT&CK technique IDs and ~10 methodology-vocab entries sit at vocabulary depth so the Belt-3 graduate can hold a competent engagement-discipline conversation alongside their reproduced labs. Per the discovery-learning approach (`project_discovery-learning approach.md`), vocabulary scaffolding intentionally leaves space for students to discover detail through hands-on lab encounters; the rows below are anchors, not exhaustive treatments.

Worked-example anchor. Section §6 supplies one canonical OSCP-style chain at structural depth: SMB null-session enumeration (T1135) into service-version banner identification, public-exploit module review, Linux kernel privilege-escalation via OverlayFS (CVE-2021-3493; T1068), pass-the-hash lateral movement (T1550.002), and the four-section reporting discipline (executive summary, methodology, findings, remediation). The chain is structural rather than implementation: the methodology depth lives in PEN-101 labs; this handout shows the vocabulary of how to **narrate** the

engagement to a client. The pedagogical thesis is that one structural worked example of this quality (named techniques + public CVE anchor + four-section report shape) buys more career-long retention than many additional taxonomy rows, because the engagement-narrative pattern it grounds generalizes far beyond the specific chain into every engagement the graduate will write up for the rest of their career.

Citation discipline. Every ATT&CK technique ID in this handout follows the MITRE ATT&CK Enterprise matrix as published at `attack.mitre.org` (Enterprise-matrix v15.x is the version current at authoring time). CWE pairings follow MITRE conventions per `cwe.mitre.org`. OWASP Top 10 references follow the OWASP project page at `owasp.org/Top10/` (2021 edition canonical at authoring; the OWASP project republishes every three to four years and the next-edition reference will trigger a v2 update of this handout). Tool names (Mimikatz, BloodHound, Impacket, CrackMapExec, Nessus, Nuclei, Burp Suite, Metasploit, Hashcat, LinPEAS, WinPEAS, sqlmap, ffuf, dirsearch, Responder, NetExec) are cited as named tooling without reproducing their command-line syntax; PEN-101 labs supply the syntax against `--authorized-by` lab targets. Where a public incident or known TTP is named, the public report (CISA KEV catalog entry, MITRE ATT&CK technique page, vendor PSIRT advisory, conference talk write-up) is the authoritative source.

Authorized-by discipline. Every offensive technique mentioned in this handout carries the implicit reminder that legitimate exercise requires explicit written authorization against intentionally-vulnerable lab harnesses, not against production systems. PEN-101 Lab 1 is the canonical anchor for the Rules-of-Engagement (ROE) document drafting practice; the academy's lab harness is fully `--authorized-by` covered for student exercise; the OSCP examination provides explicit time-windowed authorization against OffSec lab infrastructure. The vocabulary in this handout describes what a penetration tester does **under that authorization** and explicitly does not describe how to operate without it. The Professional ethics is covered at PEN-101 Week 1 and SEC-101's Coordinated Vulnerability Disclosure module; this handout sits inside that ethical scope and assumes the reader has internalized it.

---

§2: MITRE ATT&CK Enterprise matrix walk (PEN-101 vocab-tier)

The MITRE ATT&CK Enterprise matrix names tactics (the high-level adversary goals) and techniques (the specific behaviors that achieve those goals). The 14 ATT&CK Enterprise tactics span the full adversary lifecycle from reconnaissance through impact; PEN-101 emphasizes the eleven tactics that align with engagement-tier activity (Reconnaissance

and Resource Development happen before authorized engagement begins; the ATT&CK Pre-Compromise tactics are out-of-scope for PEN-101 vocabulary). The technique IDs below are the recognize-and-name set for Belt-3 PEN-101 graduates; sub-techniques (e.g., T1078.001 Default Accounts, T1078.002 Domain Accounts, T1078.003 Local Accounts, T1078.004 Cloud Accounts) are referenced under the parent technique at this level and named explicitly under the §6 worked example.

§2.1 Initial Access (TA0001)

The Initial Access tactic covers how an adversary first enters the target environment. PEN-101 Lab 6 + Lab 7 reproduce several Initial Access techniques against intentionally-vulnerable lab harnesses; the OSCP examination requires fluency across most of this row.

Technique ID	Name	One-line shape
T1078	Valid Accounts	Authenticate using legitimate credentials (default, domain, local, cloud sub-techniques)
T1190	Exploit Public-Facing Application	Reach RCE through internet-exposed service vulnerability
T1133	External Remote Services	Authenticate to externally-exposed remote-access service (VPN, RDP, SSH, Citrix)
T1566	Phishing	Deliver attacker-controlled content via spear-phishing email or attachment
T1199	Trusted Relationship	Compromise via a trusted third-party connection (MSP, supplier, contractor)
T1195	Supply Chain Compromise	Compromise via tainted software, hardware, or update channel before delivery

T1078 Valid Accounts is the highest-frequency Initial Access technique in real-world incident reports because credential reuse, password spraying, and credential-stuffing are pervasively effective against under-protected services. The four sub-techniques (T1078.001 Default Accounts, T1078.002 Domain Accounts, T1078.003 Local Accounts, T1078.004 Cloud Accounts) name the credential scope; PEN-101 Lab 6 reproduces credential-spray against an intentionally-vulnerable lab Active Directory under `--authorized-by` discipline using CrackMapExec / NetExec.

T1190 Exploit Public-Facing Application is what makes patch-management organizational discipline matter. The technique covers any RCE reached through an internet-exposed vulnerability, ranging from Apache Struts (CVE-2017-5638) through Log4Shell (CVE-2021-44228) through MOVEit (CVE-2023-34362) through Citrix Bleed (CVE-2023-4966). PEN-101 Lab 7 reproduces a public-CVE Metasploit module against a containerized harness; the academy's `cross-chapter-cve-class-vocabulary-reference.md` carries the cross-family CVE catalog.

T1133 External Remote Services covers VPN, RDP, SSH, and Citrix-style access endpoints. Initial-access via valid VPN credentials is operationally distinct from RCE because the access does not require an exploit; the technique frequently chains with T1078 Valid Accounts.

T1566 Phishing is named at vocabulary-tier; PEN-101 does not reproduce phishing at methodology depth (the PEN-200 social-engineering module covers it under explicit OffSec-controlled scope). Belt-3 graduates should recognize the three sub-techniques (T1566.001 Spearphishing Attachment, T1566.002 Spearphishing Link, T1566.003 Spearphishing via Service) and the canonical defensive controls (DMARC, attachment sandboxing, employee training).

T1199 Trusted Relationship is the supply-chain-via-relationship technique: the attacker compromises a managed-service-provider, a contractor, or a connected partner and uses the trusted relationship to reach the target. SolarWinds SUNBURST (CVE-2020-10148) is the textbook anchor; ConnectWise ScreenConnect (CVE-2024-1709) is the recent MSP-targeting case.

T1195 Supply Chain Compromise is named alongside T1199 because both are supply-chain-shaped, but T1195 specifically covers the build-or-distribution channel compromise (XZ-Utils CVE-2024-3094 anchor; Hugging Face transformers `pickle` CVE-2024-3568 for the AI-era variant).

§2.2 Execution (TA0002)

Execution covers running attacker-controlled code on the target. PEN-101 Lab 7 + Lab 8 reproduce several Execution techniques.

Technique ID	Name	One-line shape
T1059	Command and Scripting Interpreter	Execute via shell, PowerShell, Python, JavaScript, AppleScript, Visual Basic
T1106	Native API	Invoke OS-native API directly to execute (bypasses cmd-line / shell logging)
T1129	Shared Modules	Load DLL or shared library to execute attacker code in trusted process
T1203	Exploitation for Client Execution	Trigger client-side code via malicious document or browser content
T1559	Inter-Process Communication	Execute via COM, DDE, XPC, or other IPC mechanism
T1569	System Services	Execute via Windows service, systemd unit, or launchd item

T1059 Command and Scripting Interpreter is the most frequently used Execution technique in real-world incident reports. The eight sub-techniques name the canonical interpreter languages (T1059.001 PowerShell, T1059.002 AppleScript, T1059.003 Windows Command Shell, T1059.004 Unix Shell, T1059.005 Visual Basic, T1059.006 Python, T1059.007 JavaScript, T1059.008 Network Device CLI); PEN-101 Labs 7-9 use bash + PowerShell + Python at all three exploit / post-exploit / privilege-escalation tiers under `--authorized-by` discipline.

T1106 Native API matters because cmd-line / shell logging is the primary defensive telemetry surface for T1059 detection; calling Win32 APIs directly (`CreateProcess` from inline shellcode; `NtCreateProcess` from rootkit domain) bypasses the shell-history log entirely. The academy's defensive-pairing in SEC-101 covers ETW / Sysmon as the deeper telemetry layer that catches T1106.

T1203 Exploitation for Client Execution covers browser exploits, malicious-document macros, and PDF exploits; PEN-101 does not reproduce client-side exploitation at methodology depth (the academy's RE-201 covers client-exploit reverse-engineering at engagement depth).

§2.3 Persistence (TA0003)

Persistence covers maintaining attacker access across reboots, credential rotations, and configuration changes. PEN-101 Lab 9 reproduces several Persistence techniques.

Technique ID	Name	One-line shape
T1098	Account Manipulation	Modify account properties to maintain access (add SSH key, change password, grant role)
T1136	Create Account	Create new local, domain, or cloud account
T1543	Create or Modify System Process	Install service, daemon, or scheduled task that re-runs attacker code
T1547	Boot or Logon Autostart Execution	Add to registry Run key, Startup folder, plist, systemd autostart
T1574	Hijack Execution Flow	DLL search-order hijack, COR_PROFILER, LD_PRELOAD, dylib hijack
T1505	Server Software Component	Install web shell, IIS module, SQL Server stored procedure
T1053	Scheduled Task/Job	cron, at, schtasks, launchd-scheduled

T1098 Account Manipulation versus T1136 Create Account is a distinction worth holding: T1098 modifies an existing account (frequently more stealthy because the account is legitimate); T1136 adds a new one. PEN-101 Lab 9 covers both at vocabulary depth; the OSCP examination tests both.

T1547 Boot or Logon Autostart Execution has fourteen sub-techniques, ranging from registry Run keys (T1547.001) through Active Setup (T1547.014). At PEN-101 vocabulary depth, students should recognize the three most-cited (T1547.001 Registry Run Keys, T1547.006 Kernel Modules, T1547.013 XDG Autostart Entries) and know the parent technique covers the family.

T1505 Server Software Component covers web shells (T1505.003) most prominently; PEN-101 Lab 8 reproduces a web shell against a containerized harness using a public payload library (no fabricated payloads).

§2.4 Privilege Escalation (TA0004)

Privilege Escalation covers gaining higher permissions than the initial access provided. PEN-101 Lab 9 is the dedicated privilege-escalation lab; the OSCP examination tests Linux + Windows privilege escalation extensively.

Technique ID	Name	One-line shape
T1068	Exploitation for Privilege Escalation	Kernel CVE, SUID binary CVE, sudo CVE
T1078	Valid Accounts	Authenticate to a higher-privileged account (cross-tactic with Initial Access)
T1134	Access Token Manipulation	Steal or impersonate access token (Windows; SeImpersonatePrivilege)
T1548	Abuse Elevation Control Mechanism	UAC bypass, sudo cache abuse, setuid/setgid abuse
T1574	Hijack Execution Flow	(cross-tactic with Persistence) DLL search order, LD_PRELOAD elevation
T1611	Escape to Host	Container escape (Docker, Kubernetes, runc)

T1068 Exploitation for Privilege Escalation is the kernel-CVE family; the academy's worked example (§6) anchors on CVE-2021-3493 (Linux OverlayFS), a publicly-disclosed and fully-patched local privilege-escalation in the Linux kernel's OverlayFS module that allowed any local user to escalate to root via specific xattr handling. PEN-101 Lab 9 reproduces the CVE against a containerized vulnerable-kernel harness under `--authorized-by` discipline.

T1134 Access Token Manipulation covers the Windows-specific token-impersonation domain (`SeImpersonatePrivilege`, `SeAssignPrimaryTokenPrivilege`, RoguePotato / JuicyPotato / PrintSpoofer / GodPotato exploit families). Belt-3 graduates should recognize the family by name; methodology depth lives at ADV-101.

T1548 Abuse Elevation Control Mechanism has four sub-techniques: T1548.001 Setuid and Setgid, T1548.002 Bypass User Account Control, T1548.003 Sudo and Sudo Caching, T1548.004 Elevated Execution with Prompt. PEN-101 Lab 9 covers .001 + .003 against Linux harnesses; .002 + .004 are Windows-specific and covered at vocabulary tier only.

T1611 Escape to Host covers container escapes; PEN-101 does not reproduce container escapes at methodology depth (academy's CON-301 covers them; ADV-101 references them in Belt-5 reading).

§2.5 Defense Evasion (TA0005)

Defense Evasion covers avoiding detection by security controls. PEN-101 Week 7 + Week 9 reference several Defense Evasion techniques in operational-security contexts.

Technique ID	Name	One-line shape
T1027	Obfuscated Files or Information	Encrypted, packed, encoded, or steganographic payload
T1036	Masquerading	Rename payload to system-binary name, mimic legitimate file metadata
T1055	Process Injection	Reflective DLL injection, hollowing, doppelgänging, herpaderping
T1070	Indicator Removal	Clear logs, delete files, timestomp, mailbox-rule removal
T1112	Modify Registry	Disable Defender, disable AMSI, modify run-key Persistence
T1140	Deobfuscate/Decode Files or Information	Decode payload at runtime to evade static detection
T1218	System Binary Proxy Execution	LOLBins (rundll32, regsvr32, mshta, certutil, msiexec)

T1027 Obfuscated Files or Information is the parent for the obfuscation family; the academy covers it at vocabulary-tier only because obfuscation methodology shifts month-to-month and the vocabulary stays stable.

T1055 Process Injection has thirteen sub-techniques (T1055.001 DLL Injection through T1055.013 Process Doppelgänging); Belt-3 graduates should recognize the parent technique and the three most-cited sub-techniques (T1055.001 DLL Injection, T1055.012 Process Hollowing, T1055.013 Process Doppelgänging).

T1218 System Binary Proxy Execution is the LOLBin (Living-Off-the-Land Binary) family; the LOLBAS project at `lolbas-project.github.io` curates the canonical Windows-LOLBin reference. PEN-101 Week 9 references the family for vocabulary work; ADV-101 deepens to specific LOLBin selection per engagement.

§2.6 Credential Access (TA0006)

Credential Access covers obtaining account credentials for subsequent use. PEN-101 Lab 9 + Lab 10 reproduce several Credential Access techniques.

Technique ID	Name	One-line shape
T1003	OS Credential Dumping	LSASS, SAM, NTDS.dit, /etc/shadow, keychain
T1110	Brute Force	Password guessing, password cracking, credential stuffing
T1212	Exploitation for Credential Access	Heartbleed-class memory disclosure, Citrix-Bleed-class session-token leak
T1539	Steal Web Session Cookie	Browser cookie database theft, session-token grab
T1552	Unsecured Credentials	Find credentials in files, cmdline history, registry, group policy preferences
T1555	Credentials from Password Stores	Browser saved passwords, password manager secrets, Windows Credential Manager
T1556	Modify Authentication Process	Skeleton key, password filter DLL, custom SSP
T1558	Steal or Forge Kerberos Tickets	Kerberoasting, AS-REP roasting, Golden / Silver / Diamond tickets

T1003 OS Credential Dumping is the canonical Credential Access technique; the seven sub-techniques (T1003.001 LSASS Memory through T1003.007 Proc Filesystem) name the OS-specific credential stores. Mimikatz is the canonical tool for T1003.001 LSASS dumping; secretsdump.py from Impacket is the canonical tool for T1003.003 NTDS.dit dumping. PEN-101 Lab 9 reproduces credential-dumping against intentionally-vulnerable lab Active Directory under `--authorized-by` discipline.

T1110 Brute Force has four sub-techniques: T1110.001 Password Guessing, T1110.002 Password Cracking (Hashcat / John family), T1110.003 Password Spraying, T1110.004 Credential Stuffing. PEN-101 Lab 5 + Lab 6 reproduce T1110.002 + T1110.003 against academy lab harnesses.

T1552 Unsecured Credentials is the Belt-3 graduate's canonical reminder that secrets-in-source-code, secrets-in-config-files, secrets-in-environment-variables, and secrets-in-bash-history are all named TTPs that defenders look for and attackers exploit. The seven sub-techniques include T1552.001 Credentials In Files, T1552.004 Private Keys, T1552.006 Group Policy Preferences (gpp-decrypt anchor).

T1558 Steal or Forge Kerberos Tickets is the Active-Directory-specific credential-attack family; the four sub-techniques (T1558.001 Golden Ticket, T1558.002 Silver Ticket, T1558.003 Kerberoasting, T1558.004 AS-REP Roasting) compose the Active-Directory-pentest core. Kerberoast (T1558.003) is reproduced in PEN-101 Lab 10 against academy lab AD using Impacket's GetUserSPNs.py + Hashcat for the offline crack.

§2.7 Discovery (TA0007)

Discovery covers situational-awareness gathering after initial access. PEN-101 Lab 9 covers Discovery extensively.

Technique ID	Name	One-line shape
T1018	Remote System Discovery	Enumerate hosts on the network
T1049	System Network Connections Discovery	netstat / ss / ESTABLISHED-connection enumeration
T1057	Process Discovery	ps / Get-Process / running-processes enumeration
T1069	Permission Groups Discovery	groups / net group / AD group enumeration
T1083	File and Directory Discovery	find / dir / Get-ChildItem with target patterns
T1087	Account Discovery	net user / Get-LocalUser / Get-ADUser enumeration
T1135	Network Share Discovery	smbclient / net view / share enumeration
T1518	Software Discovery	Installed-software enumeration; antivirus identification

T1135 Network Share Discovery is the SMB-share enumeration anchor referenced in the §6 worked example; SMB null-session enumeration against a misconfigured server discloses share names and (with weak ACLs) share contents. The academy's Lab 3 + Lab 9 reproduce this against intentionally-vulnerable lab harnesses using smbclient + smbmap + crackmapexec under `--authorized-by` discipline.

T1018 Remote System Discovery covers post-access network mapping; nmap-on-the-target, ping-sweeps, ARP scans. The discovery happens after authorization (Initial Access), not before; engagement-tier rules apply.

T1087 Account Discovery has four sub-techniques (T1087.001 Local Account, T1087.002 Domain Account, T1087.003 Email Account, T1087.004 Cloud Account); BloodHound's data-collection phase (SharpHound) is the canonical T1087.002 tool, exercised in PEN-101 Lab 10.

§2.8 Lateral Movement (TA0008)

Lateral Movement covers expanding access from initial foothold to additional systems. PEN-101 Lab 10 is the dedicated lateral-movement lab.

Technique ID	Name	One-line shape
T1021	Remote Services	RDP, SSH, SMB, WinRM, VNC, DCOM lateral movement
T1080	Taint Shared Content	Modify a shared file or share to spread on access
T1210	Exploitation of Remote Services	EternalBlue, BlueKeep, ProxyLogon-class internal exploitation
T1534	Internal Spearphishing	Use internal email account to deliver phishing to other employees
T1550	Use Alternate Authentication Material	Pass-the-hash, pass-the-ticket, web session cookie
T1563	Remote Service Session Hijacking	RDP session hijack, SSH session hijack
T1570	Lateral Tool Transfer	Copy tools to additional hosts after foothold

T1021 Remote Services is the parent for the canonical lateral-movement family; the seven sub-techniques (T1021.001 RDP, T1021.002 SMB/Windows Admin Shares, T1021.003 DCOM, T1021.004 SSH, T1021.005 VNC, T1021.006 WinRM, T1021.007 Cloud Services) name the canonical protocols. PEN-101 Lab 10 reproduces T1021.002 and T1021.006 against intentionally-vulnerable lab AD; the OSCP examination tests T1021.001 + T1021.002 + T1021.006 + T1021.004 commonly.

T1550 Use Alternate Authentication Material is the pass-the-hash / pass-the-ticket family; the four sub-techniques are T1550.001 Application Access Token, T1550.002 Pass the Hash, T1550.003 Pass the Ticket, T1550.004 Web Session Cookie. T1550.002 (pass-the-hash) is the §6 worked-example anchor for lateral movement; Impacket's psexec.py / wmiexec.py / smbexec.py + CrackMapExec are the canonical tools, exercised in PEN-101 Lab 10 under `--authorized-by` discipline.

T1210 Exploitation of Remote Services covers internal-network unauthenticated RCE: EternalBlue (CVE-2017-0144) against unpatched SMBv1, BlueKeep (CVE-2019-0708) against unpatched RDP, ProxyLogon (CVE-2021-26855) against on-prem Exchange. The academy's `cross-chapter-cve-class-vocabulary-reference.md` carries the cross-family CVE catalog.

§2.9 Collection (TA0009)

Collection covers gathering data of interest from the target environment. PEN-101 references Collection at vocab-tier only; the OSCP examination has limited Collection emphasis.

Technique ID	Name	One-line shape
T1005	Data from Local System	Find and collect files of interest on the compromised host
T1056	Input Capture	Keylogger, browser-credential interceptor
T1113	Screen Capture	Screenshot the user's session
T1185	Browser Session Hijacking	Inject into running browser process to capture session
T1213	Data from Information Repositories	SharePoint, Confluence, Jira, code repositories enumeration
T1217	Browser Information Discovery	Bookmarks, history, saved-form-data enumeration

The Collection family at vocab-tier is most useful for **understanding what defenders flag during incident response**: SOC analysts watch for T1005 large-file-archive operations, T1056 keylogger artifacts, T1213 cross-repository sweeps. Belt-3 graduates should recognize the names; methodology depth is at ADV-101 + ADV-102.

§2.10 Command and Control (TA0011)

Command and Control covers maintaining communication channels with the compromised host. PEN-101 references C2 at vocab-tier; Cobalt Strike is named as the canonical commercial C2 framework; Sliver / Mythic / Havoc as canonical open-source alternatives.

Technique ID	Name	One-line shape
T1001	Data Obfuscation	Steganography, custom encoding in C2 traffic
T1071	Application Layer Protocol	HTTPS / DNS / SMTP / IRC / WebSocket as C2 channel
T1090	Proxy	Internal proxy, external proxy, multi-hop proxy, domain fronting
T1095	Non-Application Layer Protocol	ICMP tunneling, raw-socket C2
T1102	Web Service	Pastebin, social-media platforms, code-repository services as dead drops
T1219	Remote Access Software	Legitimate RMM tool (TeamViewer, AnyDesk, ScreenConnect) repurposed for C2
T1568	Dynamic Resolution	DGA (domain generation algorithm), fast-flux DNS
T1573	Encrypted Channel	TLS-encrypted C2, custom symmetric encryption

T1071 Application Layer Protocol has four sub-techniques (T1071.001 Web Protocols, T1071.002 File Transfer Protocols, T1071.003 Mail Protocols, T1071.004 DNS); HTTPS-shaped C2 (T1071.001) is the most-encountered sub-technique because TLS-on-443 blends with normal web traffic.

T1090 Proxy has four sub-techniques: T1090.001 Internal Proxy, T1090.002 External Proxy, T1090.003 Multi-hop Proxy, T1090.004 Domain Fronting. SOCKS-proxy chaining (T1090.001 + T1090.003) is the foundational pivoting techniques exercised in PEN-101 Lab 10.

T1219 Remote Access Software is the pattern of legitimate-RMM-tool abuse: ScreenConnect (CVE-2024-1709 anchor), TeamViewer, AnyDesk. Defenders flag the family because the binaries are signed and the network traffic is legitimate-looking; behavioral telemetry (unusual-time-of-day activation, post-compromise installation) is the detection domain.

§2.11 Exfiltration (TA0010)

Exfiltration covers moving collected data out of the target environment. PEN-101 references Exfiltration at vocab-tier; engagement-tier exfiltration reproduction lives at ADV-101.

Technique ID	Name	One-line shape
T1029	Scheduled Transfer	Time-delayed exfiltration to evade volume-detection
T1041	Exfiltration Over C2 Channel	Reuse the C2 channel for data exfiltration
T1048	Exfiltration Over Alternative Protocol	DNS exfiltration, ICMP exfiltration, FTP-out
T1052	Exfiltration Over Physical Medium	USB drive, HID device, printed paper
T1567	Exfiltration Over Web Service	Pastebin, GitHub, cloud-storage upload

T1048 Exfiltration Over Alternative Protocol covers the canonical detection-evasion exfiltration channels; DNS exfiltration (T1048.003) is the most-encountered sub-technique because outbound-DNS is rarely fully blocked. The academy's `cross-chapter-net-101-anchor-reading-guide.md` covers the wire-protocol vocabulary the Belt-3 graduate uses to recognize DNS-tunneled exfiltration in Wireshark captures.

T1567 Exfiltration Over Web Service is the GitHub-gist / Pastebin / cloud-storage pattern; the technique blends with normal user behavior because the destination services are legitimately used.

§2.12 Impact (TA0040)

Impact covers data-destructive or availability-destructive actions. PEN-101 does not reproduce Impact techniques at methodology depth (legitimate engagements rarely include Impact authorization; the academy's red-team-style tests stop short of destructive action by default).

Technique ID	Name	One-line shape
T1485	Data Destruction	Overwrite or delete files
T1486	Data Encrypted for Impact	Ransomware encryption
T1489	Service Stop	Stop services to disrupt availability
T1490	Inhibit System Recovery	Delete shadow copies, disable backups, remove recovery partitions
T1491	Defacement	Modify visual content (T1491.001 Internal, T1491.002 External)
T1496	Resource Hijacking	Cryptomining, botnet recruitment
T1498	Network Denial of Service	DDoS via network resource exhaustion

The Impact family is recognize-only at PEN-101 level; Belt-3 graduates should know the family exists, name the canonical techniques, and recognize the techniques in incident-response write-ups. Reproduction depth is out-of-scope for engagement-tier penetration testing absent specific destructive-test authorization (which is rare and tightly-scoped when granted).

---

§3: OSCP-prep methodology vocabulary

The OffSec PEN-200 / OSCP+ examination tests engagement-discipline procedural fluency under time pressure: students attack a network of target machines, achieve specific objectives, and write a client-style report within a 24-hour-plus-24-hour window. The methodology vocabulary below is the procedural vocabulary the OSCP examination assumes; PEN-101 Labs 1-11 reproduce each entry against `--authorized-by` lab harnesses.

Reconnaissance discipline (passive / active / OSINT taxonomy). Passive reconnaissance gathers information about the target without sending packets to the target's infrastructure; the canonical sources are WHOIS records, certificate-transparency logs (crt.sh, censys.io), DNS records (NSLOOKUP, dig, dnsrecon), public Git repositories, social-media tradecraft, and search-operator literacy (Google dorks). Active reconnaissance does send packets to the target; the canonical tools are nmap, Masscan, ping, and traceroute. The OSCP examination requires fluency in both; PEN-101 Lab 2 + Lab 3 reproduce both.

Enumeration discipline (port scanning, service identification, banner grabbing, version enumeration). Enumeration deepens the reconnaissance output: port scanning (nmap with -sS / -sT / -sU and timing templates) identifies open ports; service identification (nmap -sV / banner grabbing via netcat / curl with verbose headers) names the service running; version enumeration narrows to specific software releases that may have known vulnerabilities. The discipline question is "what services are running, and which versions, with what configuration?" PEN-101 Lab 3 reproduces the discipline against intentionally-vulnerable lab harnesses; the OSCP examination tests it on every target.

Vulnerability identification (Nessus / OpenVAS / Nikto / nmap NSE). Vulnerability scanners automate the matching of identified service-versions against known-vulnerability databases; Nessus is the commercial tool of choice (the academy lab harness includes a Nessus Essentials license), OpenVAS / Greenbone Vulnerability Manager is the open-source alternative, Nikto is the legacy web-server-scanner, nmap NSE scripts (--script vuln) cover a curated subset. Belt-3 graduates should be able to run Nessus against an authorized lab target, triage findings by exploitability and CVSS score, and produce a prioritized remediation list. PEN-101 Lab 5 reproduces this against the academy lab harness.

Exploitation primitives (public-exploit-database review / Metasploit module use / manual exploitation). The Exploit Database (exploit-db.com) is the canonical public-exploit reference; Searchsploit is its command-line companion. Metasploit's module catalog (msfconsole's `search` command) covers the curated exploit set against well-known CVEs. Manual exploitation (writing the exploit script in Python or Ruby from a public PoC) is the OSCP examination's distinguishing register; the OSCP+ revision specifically de-emphasizes pure Metasploit reliance and tests manual-exploitation fluency. PEN-101 Lab 7 reproduces both Metasploit-module and manual-exploitation registers.

Post-exploitation discipline (situational awareness / privilege enumeration / credential harvesting). Post-exploitation begins immediately after foothold: situational awareness (whoami / id / hostname / uname / Get-ComputerInfo), privilege enumeration (sudo -l / id; whoami /priv), credential harvesting (history / .bash_history / config files / browser saved-passwords / AppData credential stores). The discipline question is "what does this foothold give me, and what's the next move?" PEN-101 Lab 9 reproduces the discipline against intentionally-vulnerable lab harnesses using LinPEAS + WinPEAS as the canonical privilege-enumeration tools.

Privilege escalation (Linux: kernel + sudo + cron + SUID + capabilities; Windows: token + service + AlwaysInstallElevated + UAC bypass). Privilege escalation has two parallel taxonomies. Linux escalation: kernel-CVE-driven (T1068 anchor; LinPEAS surfaces candidates); sudo-driven (sudo -l for cached entries; weak sudoers config; sudo CVEs like CVE-2021-3156 Baron Samedit); cron-driven (writeable cron scripts; world-writeable cron directories); SUID-driven (find / -perm -4000; GTFOBins for binary abuse); capabilities-driven (getcap for Linux capabilities-with-SUID-equivalent power). Windows escalation: token impersonation (SeImpersonatePrivilege; PrintSpoofer / GodPotato); service-permission abuse (sc qc / accesschk; weakly-permissioned services); AlwaysInstallElevated registry key; UAC bypass (Fodhelper, ComputerDefaults, eventvwr techniques). PEN-101 Lab 9 reproduces both Linux and Windows escalation techniques against academy lab harnesses; the OSCP examination tests both at every level.

Lateral movement (pass-the-hash / kerberoasting / SMB relay / WinRM / RDP). Lateral movement covers expanding from initial foothold to additional systems. Pass-the-hash (T1550.002) replays a captured NTLM hash against another system without cracking it; kerberoasting (T1558.003) extracts service-account TGS tickets and cracks them offline; SMB relay (NTLM relay attack) replays NTLM authentication to a different target; WinRM (T1021.006) and RDP (T1021.001) are the canonical authenticated-lateral-movement protocols. Impacket (psexec.py / wmiexec.py / smbexec.py / GetUserSPNs.py / ntlmrelayx.py) is the canonical tool family; CrackMapExec / NetExec is the workflow-orchestration tool; BloodHound / SharpHound is the AD-graph-analysis tool. PEN-101 Lab 10 reproduces the full set against academy lab AD under `--authorized-by` discipline.

Pivoting (port forwarding / SOCKS proxying / SSH chains). Pivoting moves an attacker's traffic through a compromised host to reach internal-only targets. SSH local-port-forwarding (-L), remote-port-forwarding (-R), and SOCKS-proxy mode (-D) are the canonical SSH-side primitives; Chisel and Ligolo-ng are the canonical pivot-tool family the OSCP+ revision tests. PEN-101 Lab 10 reproduces SSH-tunnel-and-SOCKS chains; the OSCP+ revision additionally tests Chisel-shaped pivots.

Note-taking under pressure (OSCP-grade markdown discipline; chain-of-evidence preservation). The OSCP examination's report-writing window is 24 hours after the 24-hour examination window; note-taking under pressure during the exam is what makes report-writing tractable. The academy's recommended note structure: per-target markdown file with sections (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Post-Exploitation, Privilege Escalation, Lateral Movement, Findings); every command logged with timestamp; every screenshot named

systematically (target-host_step_description.png); every credential captured with source and use. Belt-3 graduates should practice the discipline during PEN-101 Labs 7-11 so it is in muscle memory before the OSCP examination.

Reporting (executive summary / methodology / findings / remediation; CVSSv3 scoring). The four-section client-style report is the OSCP examination's distinguishing deliverable. Executive summary: one to two pages, business-language, no tooling jargon. Methodology: the engagement-lifecycle phases the engagement followed. Findings: per-finding entries with CVSSv3 score, evidence (screenshots + commands + observed-state), exploitation narrative, remediation. Remediation: prioritized action list ordered by CVSSv3 score plus business risk. PEN-101 Lab 11 + the five-day capstone engagement both reproduce the four-section discipline; the OSCP examination assesses both the technical exploitation work and the report quality.

---

§4: OWASP Top 10 (2021 edition; web applications)

The OWASP Top 10 is the canonical web-application vulnerability taxonomy maintained by the OWASP Foundation. The current edition (2021) is canonical at authoring time; the project republishes every three to four years. PEN-101 Week 8 reproduces several rows against intentionally-vulnerable lab harnesses (DVWA, Juice Shop, WebGoat, custom containers). Cross-references to `cross-chapter-cve-class-vocabulary-reference.md` rows are noted where the same CWE appears.

Rank	Name	CWE pairing	Anchor incident
A01	Broken Access Control	CWE-22 / CWE-639 / CWE-285 / CWE-862	IDOR pervasive across the disclosure landscape
A02	Cryptographic Failures	CWE-259 / CWE-327 / CWE-331	Heartbleed CVE-2014-0160 (cross-cite §2 CVE-class handout)
A03	Injection	CWE-79 / CWE-89 / CWE-78 / CWE-643	MOVEit Transfer CVE-2023-34362 (SQLi); cross-cite §3 CVE-class handout
A04	Insecure Design	CWE-209 / CWE-256 / CWE-501 / CWE-522	Insecure-design failures (logic flaws; no canonical single CVE)
A05	Security Misconfiguration	CWE-16 / CWE-611	Default-credential exposure across the embedded-device landscape
A06	Vulnerable and Outdated Components	CWE-1104	Log4Shell CVE-2021-44228 (cross-cite §3 CVE-class handout)
A07	Identification and Authentication Failures	CWE-287 / CWE-307 / CWE-384	Citrix Bleed CVE-2023-4966 (cross-cite §4 CVE-class handout)
A08	Software and Data Integrity Failures	CWE-502 / CWE-829	XZ-Utils CVE-2024-3094 (cross-cite §4 CVE-class handout)
A09	Security Logging and Monitoring Failures	CWE-117 / CWE-223	Logging-failure as enabler of post-compromise dwell time
A10	Server-Side Request Forgery (SSRF)	CWE-918	Exchange ProxyLogon CVE-2021-26855 (cross-cite §4 CVE-class handout)

A01 Broken Access Control is the highest-ranked category in OWASP Top 10 (2021); it absorbed both A04 Insecure Direct Object References and A07 Missing Function Level Access Control from the 2017 edition. The canonical Belt-3 examples: IDOR (insecure direct object reference) where /api/user/12345 returns user 12345's data with no authorization check; horizontal privilege escalation between accounts at the same trust level; vertical privilege escalation between trust tiers (user-to-admin); CORS misconfiguration; CSRF where the framework does not auto-token form submissions. The defensive rule generalizes: **every request must be authorized at the action it is performing, not just at the session it is operating in.** PEN-101 Lab 4 + Lab 8 reproduce IDOR and horizontal escalation against academy lab harnesses.

A02 Cryptographic Failures absorbed the 2017 A03 Sensitive Data Exposure category and reframed it from "data exposure" to "cryptographic failures that lead to data exposure." The canonical Belt-3 examples: weak TLS configuration (Heartbleed; cipher-suite weaknesses; certificate-validation failures); password-storage weaknesses (no hashing; MD5 hashing; no salt; rainbow-table-vulnerable schemes); hardcoded keys in source code; predictable random-number generation. The defensive rule: **use the language and platform's modern crypto library; do not roll your own.** PEN-101 Lab 5 + Lab 8 reproduce cryptographic-failure findings against academy harnesses.

A03 Injection dropped from #1 in 2017 to #3 in 2021 because parameterized-query APIs and framework auto-escaping have made the class less common in modern codebases. The canonical Belt-3 examples: SQL injection (CWE-89), command injection (CWE-78), LDAP injection, NoSQL injection (CWE-943 in pairing), expression-language injection, server-side template injection (CWE-1336; LangChain Jinja2 anchor at `cross-chapter-cve-class-vocabulary-reference.md`). PEN-101 Week 8 reproduces SQLi against DVWA and academy harnesses; XSS (CWE-79) is also covered under A03 in the 2021 edition (the 2017 separate A07 Cross-Site Scripting was merged into A03).

A04 Insecure Design is new in 2021 and represents OWASP's recognition that some failure modes are architectural rather than implementation-level. The category covers missing rate-limiting in authentication flows, predictable resource generation, missing business-logic constraints, and threat-model-failed-to-address gaps. Defensive approaches: threat modeling, secure-by-design patterns, security-requirement specification at design time. SEC-101 Module 3 covers the defensive domain; PEN-101 covers the offensive recognition.

A05 Security Misconfiguration covers the broad pattern of "the system is configured in a way that exposes attack surface": default credentials still active, unnecessary services enabled, verbose error messages disclosing internal state, missing security headers (CSP, HSTS, X-Frame-Options), misconfigured CORS, exposed administrative interfaces, exposed cloud-storage buckets. PEN-101 Lab 4 + Lab 7 reproduce several misconfiguration findings against academy harnesses.

A06 Vulnerable and Outdated Components covers the use of dependencies with known vulnerabilities. The 2021 edition reflects the post-Log4Shell industry recognition that supply-chain dependency hygiene is operationally critical. Defensive approaches: SBOM generation (Software Bill of Materials), dependency-update automation (Dependabot, Renovate), CI-time vulnerability scanning, continuous monitoring against new CVE disclosures. PEN-101 references the category at vocabulary level; ADV-102 picks up the AI-supply-chain extension.

A07 Identification and Authentication Failures absorbed and reframed the 2017 A02 Broken Authentication. The canonical Belt-3 examples: credential-stuffing surfaces (no rate limiting, no detection, no MFA), session-management failures (predictable session IDs, no rotation post-authentication, no expiration, no logout invalidation), MFA-bypass surfaces (Citrix-Bleed-class session-token leak; SMS-OTP-interception; OAuth-misconfiguration). PEN-101 Lab 6 reproduces credential-stuffing against academy harnesses.

A08 Software and Data Integrity Failures is new in 2021 and absorbed the 2017 A08 Insecure Deserialization plus added supply-chain-integrity concerns. The canonical Belt-3 examples: insecure deserialization (CWE-502; pickle, Java serialization, .NET BinaryFormatter); CI/CD pipeline integrity (build-artifact tampering); auto-update channel integrity (SolarWinds anchor); container-image integrity (signing and provenance verification). The XZ-Utils anchor at `cross-chapter-cve-class-vocabulary-reference.md` cross-cites here.

A09 Security Logging and Monitoring Failures covers the operational blind-spot pattern: insufficient logging, untimely alerting, missing audit trails, log-tampering surfaces. Defensive approaches: centralized logging (SIEM ingestion), log-integrity controls (signed logs, separate logging accounts), alert-escalation policies, table-top exercises for incident-response readiness. SEC-101 Module 6 covers the defensive monitoring coverage; PEN-101 Lab 11 reproduces the offensive techniques (post-compromise log-clearing under T1070 ATT&CK technique; defensive remediation in the Findings section of the engagement report).

A10 Server-Side Request Forgery (SSRF) is new in the top-10 (it was a less-prominent category in 2017). The 2021 promotion reflects cloud-native architecture's exposure to SSRF: cloud-metadata endpoints (AWS IMDSv1's 169.254.169.254 textbook; Azure / GCP equivalents), internal microservice calls without authentication, server-side webhook receivers. The Exchange ProxyLogon anchor at `cross-chapter-cve-class-vocabulary-reference.md` cross-cites here. PEN-101 Lab 8 references SSRF at vocab-tier; methodology-depth reproduction lives at ADV-101.

---

§5: Engagement-lifecycle phase vocabulary (seven-phase model)

The seven-phase engagement-lifecycle model is the academy's operating frame for PEN-101 syllabus structure and the OSCP examination's procedural scope. Each phase below names the canonical artifacts the phase produces, the discipline-tier the phase exercises, and the Lab-N anchor in PEN-101 where the phase is reproduced.

Phase 1: Pre-engagement (scoping; ROE; legal sign-off; `--authorized-by` discipline). The pre-engagement phase covers everything before the first packet leaves the tester's machine. Artifacts: Statement of Work (SOW) with scope boundaries (in-scope hosts, ports, protocols; out-of-scope items including production-disruptive testing absent specific authorization); Rules of Engagement (ROE) document covering test-window timing, communication channels, escalation procedures, evidence-handling discipline; legal sign-off from the client's authorized representative (the `--authorized-by` named individual); test-account provisioning and credential-handling protocol. PEN-101 Lab 1 reproduces the pre-engagement phase by drafting an ROE for a hypothetical SMB client; the discipline carries forward into every subsequent academy lab.

Phase 2: Reconnaissance (OSINT artifacts). The reconnaissance phase covers passive information-gathering before active scanning begins. Artifacts: a target-organization OSINT dossier (organizational chart, employee names, technology fingerprints, public-facing infrastructure, social-media tradecraft, certificate-transparency log entries, public Git repositories, third-party-service exposure). The discipline question is "what can I learn without touching the target?" PEN-101 Lab 2 reproduces the phase against an academy-supplied lab target organization; the OSCP examination tests passive-recon fluency.

Phase 3: Scanning + Enumeration (nmap output discipline; service-version artifacts). The scanning + enumeration phase covers active reconnaissance: port scanning, service identification, version enumeration, banner grabbing, web-directory enumeration, SMB enumeration, SNMP enumeration, AD enumeration. Artifacts: complete nmap output for the target scope (in canonical XML or grepable format), service-version table cross-referenced against known-vulnerability databases, web-server directory map (ffuf / dirsearch output), SMB-share inventory, AD-user-and-computer-and-group inventory. PEN-101 Lab 3 reproduces the phase against the academy lab network under `--authorized-by` discipline.

Phase 4: Vulnerability Analysis (CVSS / VPR / actionable findings). The vulnerability-analysis phase converts raw enumeration data into a triaged finding list. Artifacts: a vulnerability spreadsheet ordered by CVSSv3 base score; per-finding

evidence references (specific scan output, specific banner, specific CVE pairing); a candidate-exploit list ranked by reproducibility, reliability, and engagement-scope-impact. CVSSv3 (the Common Vulnerability Scoring System v3) is the academy canonical scoring framework; Tenable's VPR (Vulnerability Priority Rating) is the commercial alternative the Nessus tool surfaces; the discipline question is "which findings deserve the engagement's exploitation budget?" PEN-101 Lab 5 reproduces the phase using Nessus output against the academy lab harness.

Phase 5: Exploitation (proof-of-concept demonstration; chain-of-evidence). The exploitation phase reproduces the prioritized vulnerabilities under engagement scope. Artifacts: per-exploit transcript (commands, output, screenshots); per-exploit chain-of-evidence (timestamps, source-host, target-host, observed-state-change); per-exploit success-or-failure annotation with explanation. The discipline question is "did the exploit work, and what state did it leave the target in?" PEN-101 Lab 7 reproduces several exploitation primitives against intentionally-vulnerable lab targets (Metasploitable, DVWA, retired HackTheBox boxes); the OSCP examination tests exploitation fluency on every target.

Phase 6: Post-Exploitation (situational awareness; privilege enumeration; credential dumping). The post-exploitation phase covers what the tester does after foothold. Artifacts: per-host situational-awareness transcript (whoami, id, hostname, uname / Get-ComputerInfo output); per-host privilege-enumeration transcript (LinPEAS / WinPEAS output, GTFOBins / LOLBAS reference for surfaced primitives); per-host credential-harvesting record (credentials dumped, source, hash type, crack status); lateral-movement candidate list. PEN-101 Lab 9 + Lab 10 reproduce the phase against academy harnesses with explicit lab-AD lateral-movement scope.

Phase 7: Reporting (executive summary; methodology; findings; remediation). The reporting phase converts the engagement's evidence into a client-facing deliverable. Artifacts: a four-section engagement report covering executive summary (one to two pages, business-language), methodology (engagement-lifecycle phases the engagement followed), findings (per-finding entries with CVSSv3 score, evidence, exploitation narrative, remediation), remediation prioritization (action list ordered by CVSSv3 score plus business-risk weighting). PEN-101 Lab 11 + the five-day capstone engagement reproduce the reporting phase; the academy's two-tier rubric (five binary engagement-discipline gates plus a 40-30-30 technical-depth, report-craft, and engagement-discipline split) assesses the deliverable.

The seven-phase model is **sequential by default and iterative under pressure**: a Belt-3 PEN-101 graduate should be able to articulate the linear path; an OSCP-prep candidate should be able to discuss when re-entering an earlier phase is appropriate (e.g., post-exploitation enumeration discloses a new internal target, which sends the tester back to Phase 3 scanning against the new target before continuing).

---

§6: Worked-example anchor: textbook OSCP-style chain (structural depth)

This section walks one canonical OSCP-style engagement chain at structural depth: the goal is to demonstrate the **vocabulary of how to narrate the engagement** to a client, not the exploitation methodology depth (PEN-101 labs supply that). The chain anchors on publicly-disclosed and fully-patched CVEs and on academy-lab-reproducible techniques under `--authorized-by` discipline.

Engagement scenario (hypothetical). A small-enterprise client engaged the academy's pentest team for a one-week external + internal engagement against their main office network. The Statement of Work defines scope (the office network's three subnets; the file-and-print server; the Active Directory domain controllers; the developer workstations) and excludes scope (production cloud infrastructure; the customer-facing web application; any system in the executive suite). The Rules of Engagement specify the test window (Monday-Friday 0900-1700 local), the communication channel (encrypted Signal group with the client's CTO and SOC lead), the escalation procedure (tester texts the SOC lead within five minutes of any unexpected access or destructive-state observation), and the chain-of-evidence requirement (every command, screenshot, and credential captured to a separately-encrypted-disk engagement-folder).

Phase 2-3 (Recon + Scan + Enumeration). Passive reconnaissance against the client's domain registers their external IP space and identifies the SMB service exposed on the file-and-print server (this is unusual for a 2026-era network and immediately worth investigating). Active scanning with nmap (`-sV --script smb-enum-shares,smb-enum-users`) confirms the server runs Windows Server 2019, SMBv1 disabled, SMBv2 enabled, and reveals two shares with **null-session-readable** ACLs (T1135 Network Share Discovery technique). Belt-3 narrative shape: "Active enumeration of the file server identified two SMB shares accessible without authentication, disclosing internal directory structure and a backup script that referenced a domain service-account credential."

Phase 4 (Vulnerability Analysis). The disclosed backup script contains a hardcoded service-account password for `svc_backup@internal.corp` in plaintext. The Nessus scan against the file server flags a separate finding: the server runs a kernel version vulnerable to **CVE-2021-3493 (Linux OverlayFS local privilege escalation)**, an academy-canonical Linux kernel vulnerability that exposes a local privilege-escalation primitive via specific `setxattr` handling on overlayfs mounts. Two findings are now in scope for the engagement: (a) credential disclosure via misconfigured share ACLs, severity High (CVSSv3 7.5); (b) exploitable kernel CVE on the file server, severity Critical (CVSSv3 7.8 local).

Phase 5 (Exploitation). The tester authenticates to the file server via WinRM (T1021.006 Remote Services: Windows Remote Management) using the `svc_backup` credential (T1078 Valid Accounts). Initial access established on the file server with `svc_backup` privileges. Note discipline: every command logged with timestamp; the exact commands are not reproduced in this handout (PEN-101 Lab 6 + Lab 10 cover the methodology depth under `--authorized-by` discipline against academy lab targets).

Phase 6 (Post-Exploitation: T1068 Privilege Escalation via OverlayFS CVE). Post-exploitation enumeration via LinPEAS confirms the kernel-version exposure to CVE-2021-3493. The tester applies a public proof-of-concept exploit (publicly disclosed; available at exploit-db.com) that exercises the OverlayFS `setxattr` handling to escalate from `svc_backup` to `root` on the file server (T1068 Exploitation for Privilege Escalation technique). Root access established on the file server. From the privileged context, the tester reads `/etc/krb5.keytab` (or the Windows-equivalent if Active-Directory-integrated; the academy's lab AD pairs Linux file servers with AD via SSSD) and recovers an additional credential.

Phase 6 continued (T1003 OS Credential Dumping + T1550.002 Pass the Hash). The recovered credential includes an NTLM hash for the `Administrator` account on a Windows file server in the same network. The tester does not crack the hash (the hash is sufficient on its own for pass-the-hash); using Impacket's `psexec.py` (T1550.002 Pass the Hash sub-technique under T1550 Use Alternate Authentication Material), the tester authenticates to the Windows server and obtains SYSTEM-level command execution. Lateral movement (T1021.002 SMB/Windows Admin Shares sub-technique under T1021 Remote Services) is now established. Belt-3 narrative shape: "The recovered NTLM hash was replayed via pass-the-hash against the secondary Windows file server, providing administrative access without password cracking."

Phase 7 (Reporting; four-section engagement report). The engagement closes with a four-section report. Executive Summary (~1.5 pages, business language): "The Virtus Academy pentest team identified two High and one Critical severity findings during a one-week external + internal engagement. Compromise of the file-and-print server was achieved within the first day via misconfigured SMB share ACLs disclosing a service-account credential, then escalated to root via a known and patched Linux kernel vulnerability. Lateral movement to a secondary Windows file server was achieved via captured NTLM hash replay. We recommend immediate remediation of the share-ACL misconfiguration, kernel patching against CVE-2021-3493, and a domain-wide service-account credential rotation." Methodology (~1 page): names the seven engagement-lifecycle phases the engagement followed, the specific tools used in each phase. Findings (~3-4 pages, per-finding subsections): three findings with CVSSv3 scores, evidence references (commands and screenshots from the engagement folder), exploitation narrative, recommended remediation, references to relevant CVEs and ATT&CK technique IDs. Remediation (~0.5 pages, prioritized list): immediate (24-hour) actions, short-term (30-day) actions, long-term (90-day) architectural improvements.

The structural lesson. A Belt-3 PEN-101 graduate should be able to read this worked-example narrative and recognize **every named technique by ATT&CK ID**, **every named CVE by its anchor in the CVE-class vocabulary handout**, **every named tool's role in the engagement lifecycle**, and **every named report section's purpose in the four-section deliverable**. The exploitation methodology depth lives in PEN-101 Labs 6, 9, 10, and 11; this handout's job is to supply the vocabulary scaffold the graduate uses to discuss the engagement with a client, a SOC lead, a colleague preparing for OSCP, or a future employer reviewing the graduate's portfolio of academy capstone work.

---

§7: Cross-references

This handout is a **coordination artifact** for the cyber-track + adjacent-track curricula. Each cyber-track course page should cite this handout in its course-overview section, in catalog tone: *"For the engagement-lifecycle methodology and MITRE ATT&CK vocabulary set cited in this course's modules, see `handouts/cross-chapter-engagement-attck-vocabulary-reference.md`."* The handout itself is **not** inlined into any public catalog page (per the catalog-vs-classroom doctrine).

Course	Module / week / lab	Pickup purpose
`vca-pen-101`	Week 1 (Engagement lifecycle)	§5 seven-phase model + §3 OSCP-prep methodology vocabulary read end-to-end as the Belt-3 vocabulary baseline
`vca-pen-101`	Week 4 (Web-app reconnaissance)	§4 OWASP Top 10 walked at full taxonomy depth
`vca-pen-101`	Week 5 (Vulnerability identification)	§3 enumeration + vulnerability-identification methodology entries
`vca-pen-101`	Week 7 (Exploitation I)	§2.1 + §2.2 ATT&CK Initial Access and Execution rows
`vca-pen-101`	Week 9 (Post-exploitation)	§2.4 + §2.6 + §2.7 ATT&CK Privilege Escalation, Credential Access, and Discovery rows
`vca-pen-101`	Week 10 (Lateral movement)	§2.8 ATT&CK Lateral Movement row + §3 lateral-movement and pivoting methodology entries
`vca-pen-101`	Week 11 (Reporting)	§5 Phase 7 reporting discipline + §6 worked-example four-section report shape
`vca-pen-101`	Five-day capstone engagement	§6 worked-example structural template; students adapt the engagement narrative to their capstone target
`vca-adv-101`	Week 1 (Belt-5 vocabulary onboarding)	This handout cited as the Belt-3 procedural-vocabulary baseline; ADV-101 deepens into Belt-5
`vca-adv-101`	Belt-5 capstone	§2 ATT&CK matrix for adversary-emulation framing of the capstone scope
`vca-adv-102`	Week 4 (AI-era ATT&CK extensions)	Cross-reference to `cross-chapter-llm-asi-vocabulary-reference.md` for AI-era tactic + technique extensions
`vca-sec-101`	Module 5 (Authentication architectures)	§2.6 Credential Access + §4 A07 Identification and Authentication Failures
`vca-sec-101`	Module 6 (Logging and Monitoring)	§4 A09 Security Logging and Monitoring Failures + ATT&CK Defense Evasion T1070

Companion handouts on the handouts/ shelf:

- `handouts/cross-chapter-cve-class-vocabulary-reference.md`: classical CVE-class taxonomy with three families (memory-corruption + parser bugs; injection + deserialization; auth-bypass + supply-chain). This handout's §4 OWASP Top 10 rows cross-reference into the CVE-class handout where the same CWE + CVE anchor appears. The CVE-class handout's §5 worked Heartbleed PoC is the structural template this handout's §6 worked example mirrors at the engagement-narrative tier.
- `handouts/cross-chapter-llm-asi-vocabulary-reference.md`: LLM-era taxonomy for ADV-102 (companion handout authored same session). Cross-referenced from this handout's §2 ATT&CK Initial Access (T1195 Supply Chain Compromise) and §4 A06 + A08 OWASP rows where AI-supply-chain extensions apply.
- `handouts/cross-chapter-pen-101-anchor-reading-guide.md`: Belt-3 PEN-track anchor reading guide (companion handout authored 2026-05-07). Cross-referenced from this handout's §1 framing for the Heath Adams + OffSec PEN-200 + Stuttard-Pinto WAHH + Seitz-Arnold Black Hat Python anchor pair.
- `handouts/cross-chapter-net-101-anchor-reading-guide.md`: Belt-3 NET-track anchor reading guide. Cross-referenced from this handout's §2.11 Exfiltration row for the wire-protocol vocabulary the Belt-3 graduate uses to recognize DNS-tunneled exfiltration in Wireshark captures.

External primary sources (canonical citation for each taxonomy):

- MITRE ATT&CK Enterprise matrix: `attack.mitre.org` (Enterprise-matrix v15.x is current at authoring time)
- MITRE CWE: `cwe.mitre.org`
- OWASP Top 10 (2021 edition): `owasp.org/Top10/`
- CISA Known Exploited Vulnerabilities catalog: `cisa.gov/known-exploited-vulnerabilities-catalog`
- LOLBAS Project (Living-Off-the-Land Binaries): `lolbas-project.github.io`
- GTFOBins (Linux SUID-binary abuse techniques): `gtfobins.github.io`
- OWASP Cheat Sheet Series: `cheatsheetseries.owasp.org`
- OffSec PEN-200 / OSCP+ exam-topics page: `offsec.com/courses/pen-200`

---

§8: Decisions / Pedagogy / Supplements

Decisions

1. **~40 ATT&CK technique IDs across 11 tactics chosen over the full Enterprise matrix.** The full ATT&CK Enterprise matrix as of v15.x covers 14 tactics with hundreds of techniques and thousands of sub-techniques. This handout selects ~40 technique IDs weighted toward what PEN-101 labs exercise + what the OSCP examination tests + what real-world incident-response write-ups cite most frequently. The selection bias is deliberate: a Belt-3 graduate who can name 40 high-frequency techniques fluently is better-positioned than a graduate who can name 200 techniques shallowly. The full matrix remains the authoritative reference; this handout supplies the entry-tier scaffold.
2. **Eleven-tactic walk (excludes Reconnaissance + Resource Development + the Mobile and ICS adjacencies).** The Reconnaissance (TA0043) and Resource Development (TA0042) ATT&CK tactics happen before authorized engagement scope; PEN-101's pre-engagement phase covers the engagement-side analog under §5 Phase 1. The ATT&CK Mobile matrix and ICS matrix are out-of-scope for entry-tier PEN-101 (Mobile is RE-track adjacent; ICS is OT-track adjacent and forward-stretch for the academy).
3. **OWASP Top 10 (2021 edition) at full taxonomy depth.** The 2021 edition is canonical at authoring time; OWASP republishes every three to four years and the next-edition release will trigger a v2 update of this handout. The full ten-row walk is calibrated against the catalog page's commitment that PEN-101 graduates can "name and recognize the OWASP Top 10 (web apps) taxonomy."
4. **OSCP-prep methodology vocabulary at procedural-register depth.** Ten methodology entries cover the engagement-discipline language the OSCP examination assumes. Each entry is one paragraph at vocabulary-tier; methodology depth lives in PEN-101 labs. The distinction matters because the OSCP+ revision specifically de-emphasizes pure tool-reliance and tests the procedural-register fluency a vocabulary handout can prepare for.
5. **Worked-example anchor at structural depth, not implementation depth.** Section §6 demonstrates the engagement-narrative pattern using publicly-disclosed and fully-patched CVE anchors (CVE-2021-3493 OverlayFS) and academy-lab-reproducible techniques. The exploitation methodology depth is deliberately not reproduced in this handout: PEN-101 Labs 6, 9, 10, and 11 cover that depth against

`--authorized-by` lab targets. The handout's scope is the vocabulary of how to **narrate** the engagement, which is a distinct pedagogical skill from the methodology of how to **execute** the engagement.

6. **Authorized-by discipline pervasive throughout.** Every offensive technique mentioned in this handout carries the implicit reminder that legitimate exercise requires `--authorized-by` clearance against intentionally-vulnerable lab harnesses. The pervasive framing is not boilerplate; it is the academy's ethical-engagement discipline that distinguishes the academy's pentest curriculum from the broader hacking-tutorial content on the public internet. Belt-3 graduates should internalize the framing as professional habit.
7. **Citation discipline.** Every named tool (Mimikatz, BloodHound, CrackMapExec, Impacket, sqlmap, Nessus, Metasploit, Burp Suite, Hashcat, John, LinPEAS, WinPEAS, Chisel, Ligolo-ng) is cited at name-level only; command-line syntax is not reproduced because PEN-101 labs supply the syntax against `--authorized-by` lab targets. Every CVE reference has a public NVD entry. Every ATT&CK technique ID resolves to a public attack.mitre.org page. The discipline matches the parent CVE-class vocab handout's citation discipline.

Pedagogy

1. **Vocabulary-tier handouts decouple recognition from reproduction.** A Belt-3 PEN-101 graduate does not need to have personally reproduced 40 ATT&CK techniques end-to-end. They need to recognize the techniques when they read incident-response write-ups, name the engagement-lifecycle phases when they discuss scope with clients, and deploy the OSCP-prep methodology vocabulary when they sit the PEN-200 examination. This handout makes the recognition-tier scaffold explicit and reproducible; PEN-101 labs supply the methodology-tier reproduction work against intentionally-vulnerable lab harnesses. The two tiers are pedagogically distinct; confusing them produces curricula that are either under-rigorous (vocabulary without methodology) or unscaleable (every student reproduces every technique end-to-end).
2. **One worked-example narrative beats many additional ATT&CK rows.** The §6 worked example demonstrates the engagement-narrative pattern at structural depth: how to read an enumeration finding into a vulnerability-analysis triage, how to read a privilege-escalation success into a post-exploitation discovery, how to read a lateral-movement opportunity into a chain-of-evidence note, and how to read all of the above into a four-section client report. The pattern generalizes; every engagement

the Belt-3 graduate writes for the rest of their career will recapitulate the same shape. The pedagogical value of one worked engagement narrative of this quality exceeds the value of many additional taxonomy rows.

3. **The discovery-learning approach applies to procedural vocabulary scaffolding.** Per `project_discovery-learning approach.md`, vocabulary scaffolding intentionally leaves space for students to discover detail through hands-on lab encounters. This handout deliberately does not exhaust each tactic. The fourteenth ATT&CK Enterprise tactic (Reconnaissance + Resource Development pre-compromise; Impact destructive-action), Active Directory's full TTP catalogue, container-and-Kubernetes TTPs, cloud-native TTPs, and operational-technology TTPs are each named as future-handout supplements rather than crammed in. The student who encounters Active-Directory-specific kerberoasting for the first time during PEN-101 Lab 10 brings real curiosity to the AD-pentest vocabulary; the student who memorized the entire AD-pentest TTP catalogue in Week 1 of PEN-101 brings memorization fatigue.
4. **The cross-track table makes the handout's coordination role explicit.** Section §7's per-course-per-module coverage table turns this handout from "one more reference document" into a coordination artifact: every cyber-track course points back to it, every cyber-track student reads it at known points in their academy progression, and the academy's engagement-lifecycle plus ATT&CK-vocabulary coverage is auditable as a single matrix. This is the canonical-anchor pattern; the parent CVE-class handout instantiates the same pattern for the CVE-class taxonomy.
5. **Authorized-by discipline as professional habit.** The pervasive `--authorized-by` framing is the academy's commitment to producing graduates whose first instinct on encountering an interesting target is to ask "do I have written authorization?" rather than "what's the exploit?" The discipline distinguishes the academy's PEN-101 graduate from the broader hacking-tutorial internet; employers in the pentest market hire on exactly this distinction. PEN-101 Lab 1 + the five-day capstone engagement reinforce the discipline at lab-tier; this handout reinforces it at the vocabulary level; the OSCP examination's ROE adherence requirement reinforces it at the credential level.

Supplements

1. **`handouts/cross-chapter-active-directory-pentest-vocabulary.md` (forward-stretch).** Walks the AD-specific TTP catalogue at PEN-101 / ADV-101 vocabulary depth: domain-enumeration techniques (BloodHound / SharpHound / ldapsearch family),

kerberoasting + AS-REP roasting + Golden / Silver / Diamond tickets at depth, ACL-abuse techniques (DCSync, DCShadow, GenericAll, GenericWrite), Constrained / Unconstrained / Resource-Based Constrained Delegation, ADCS (Active Directory Certificate Services) abuse (ESC1 through ESC15). Estimated authoring LoE: ~3-4 hr Opus on `munsonj`. Forward-pointer for ADV-101 Belt-5 reading list.

2. **`handouts/cross-chapter-cloud-native-pentest-vocabulary.md` (forward-stretch).** Walks cloud-native attack surfaces: AWS / Azure / GCP IAM-misconfiguration family, container-escape techniques (T1611), Kubernetes attack surface (kubelet / etcd / RBAC), serverless attack surface, cloud-storage misconfiguration patterns. Estimated authoring LoE: ~4-5 hr Opus.
3. **`handouts/cross-chapter-attack-defense-pairings.md` (forward-stretch).** Maps each ATT&CK technique to the SEC-101 defensive control that detects or prevents it: T1003 OS Credential Dumping → LSASS protection (Credential Guard, RunAsPPL); T1071 Application Layer Protocol → DNS-traffic anomaly detection; T1027 Obfuscated Files or Information → ETW + Sysmon + AMSI integration. Reframes the academy's offensive-defensive split as paired primitives rather than separate tracks.
4. **`handouts/cross-chapter-osed-prep-vocabulary-reference.md` (forward-stretch; post-OSCP credential pathway).** Walks the OffSec OSED (Exploit Developer) examination's vocabulary: Windows kernel-exploit primitives, ROP chain construction, custom-shellcode authoring, AV / EDR evasion at named-technique depth. Pairs with RE-201 + ADV-101 capstone work; forward-stretch for graduates pursuing the OffSec post-OSCP credential pathway.
5. **A worked-example handout per ATT&CK tactic.** Section §6 walks one engagement chain at structural depth; future handouts could walk one chain per tactic (Initial-Access-only chain; Privilege-Escalation-only chain; Lateral-Movement-only chain) at deeper structural depth. The pedagogical value of multiple worked examples at consistent depth is higher than the same word-count distributed across additional taxonomy rows.
