INFOSEC

Tools & Resources for Cybersecurity Operations

Offline Reference Artifact for in-Demand and High Impact Cybersecurity Tools & Capabilities

Consolidated & Organized by Reece Niemuth

Red Team-Related content inspiration and selected content are derived from INFOSEC HOUSE.

Table of Contents

NOTICE

Please review any possible updates for highest accuracy and volume of helpful content. Document is retained on my GitHub Cyber Portfolio Repository. Live updates can also be found absent of the Blue-Team resources can be found on the INFOSEC GitHub community contributed resource.

Application Programming Interfaces (APIs)

Documentation

- **MindAPI** – Organize API security assessments

Manipulation & Testing

- **Arjun** – HTTP parameter discovery
- **Astra** – Automated REST API security testing
- **Apache JMeter** – Functional & load testing
- **Automatic API Attack Tool** – Spec-driven attack generation
- **Burp Suite** – Intercept, test, exploit APIs
- **Fiddler Everywhere** – HTTP(S) traffic inspection
- **Hoppscotch** – Functional, security, load testing
- **HttpMaster** – HTTP testing & debugging
- **Insomnia** – REST, SOAP, GraphQL, gRPC testing
- **Karate** – API test automation
- **Kiterunner** – Contextual API content discovery
- **Postman** – API development & testing platform
- **SoapUI** – Functional & security testing
- **Taurus** – Test automation framework
- **Test Mace** – Cross-platform API testing
- **vRESTng** – Automated API test cases & validation

Training / Labs

- **crAPI** – Vulnerable API training lab
- **Damn Vulnerable GraphQL App** – GraphQL security practice
- **DVMS** – Vulnerable microservices (OWASP API Top 10)
- **dvws-node** – Vulnerable web service
- **Kontra** – Interactive API security training
- **VAmPI** – Vulnerable REST API (OWASP API Top 10)
- **vAPI** – Self-hosted vulnerable API exercises

Standards & Guidance

- **OWASP API Security Top 10**
- **OpenAPI Specification (OAS)**
- **NIST SP 800-53 (AC, IA, AU, SI)**
- **Cloud provider API security docs**

Protection & Enforcement

- **API Gateways** – AWS API Gateway, Azure APIM, Kong, Apigee, NGINX
- **API WAFs** – AWS WAF, Cloudflare API Shield, Imperva, F5
- **Runtime API Security** – Salt Security, Noname Security, Cequence
- **Controls** – Schema validation, rate limiting, auth enforcement

Logging & Detection

- **Logs** – API Gateway logs, CloudTrail, Azure Monitor, Envoy/NGINX
- **SIEM** – Splunk, Elastic, Sentinel
- **Detections** – Enumeration, token abuse, scraping, anomalies

Identity & Access

- **Auth Platforms** – Okta, Auth0, Entra ID, AWS Cognito
- **Auth Methods** – OAuth2, OIDC, mTLS
- **Secrets** – Secrets Manager, Key Vault, HashiCorp Vault
- **Access** – Least privilege, scoped tokens

Response & Hardening

- API token compromise response
- Abuse & enumeration investigation
- CI/CD API security testing
- Contract & schema validation

Asset Management

Discovery & Enumeration

- **Nmap** – Host discovery, service enumeration
- **Masscan** – Large-scale network discovery
- **Netdiscover** – ARP-based asset discovery
- **ARP-scan** – Local network enumeration
- **BloodHound (Data Collection)** – Endpoint and identity mapping

Situational Awareness

- **Ping / Traceroute** – Network reachability mapping
- **SNMP enumeration tools** – Device & service discovery
- **LDAP enumeration** – Domain asset visibility

Asset & Inventory Management

- **GLPI** – Asset management, ITIL service desk, license tracking
- **Lansweeper** – Centralized IT asset inventory
- **OCS Inventory NG / OSCInventory-NG** – Endpoint inventory & web console
- **Ralph** – CMDB & data center asset management
- **Snipe-IT** – Asset and license management

Monitoring & Telemetry

- **Zabbix** – Real-time monitoring of networks, servers, VMs, apps, cloud
- **Agent-based monitoring** – Host health & availability
- **SNMP / WMI telemetry** – Device status monitoring

Cloud & Hybrid Visibility

- **AWS Config / Azure Resource Graph** – Cloud asset tracking
- **Endpoint agents** – Coverage validation
- **CMDB integration** – Source-of-truth asset records

Security Use Cases

- Unknown / unmanaged asset detection
- Endpoint coverage validation (EDR, logging)
- Inventory-to-risk correlation
- Audit & compliance readiness

Helpful Cybersecurity Blogs

Corporate / Research Blogs

- **Not So Secure** – Exploit & attack research
- **Orange Cyberdefense** – Offensive & adversary research
- **Security Weekly** – Red team, exploits, tooling
- **Trustwave** – Threat & vulnerability research

Personal / Independent Blogs

- **0xSP** – Red team cheat sheets
- **Archangel Amael** – Offensive research
- **Attack and Defense** – Exploit & defense analysis
- **Brendon** – Computer security & C programming
- **carnal0wnage** – CVE research
- **Coldwind** – Offensive research
- **Corelan** – Exploit development
- **Darknet.org.uk** – Pentesting & exploits
- **Digi Ninja** – Red team tooling
- **GnuCitizen** – Offensive research
- **Great Scott Gadgets** – Hardware security
- **ihazomgsecurityskills** – Offensive techniques
- **Mad Irish** – Exploit research
- **Memset** – Security research
- **MG.LOL / Myne-us** – Hardware security research
- **Pentest Blog** – Vulnerability research (PRODAFT)
- **Primal Cerebral** – Vulnerability research (PRODAFT)
- **Ross Mark** – Pentesting & exploit dev
- **Reusable Security** – Passwords, crypto, general security
- **Security Reliks** – Offensive research
- **Security Sift** – CTFs, Windows research
- **Sirdarckcat** – Web app security
- **Spy Logic** – Offensive research
- **Strolling Infosec** – Offensive techniques
- **Weapons of Mass Analysis** – Exploit research
- **Wirewatcher** – Offensive security research

Corporate / Vendor Blogs

- **Microsoft Security Blog** – Detection, Windows, Defender
- **Google Project Zero** – Vulnerability research & mitigation
- **AWS Security Blog** – Cloud security & logging
- **CISA Blog** – Federal guidance & advisories
- **CrowdStrike Blog** – Threat intelligence & detections
- **Palo Alto Unit 42** – Malware & IR research
- **Mandiant / Google Cloud Security** – Incident response
- **Elastic Security Blog** – Detection engineering & hunting
- **Splunk Security Blog** – SIEM, detections, SOC ops

Practitioner / Community Blogs

- **SANS Blue Team Blog** – Detection & IR practices
- **DFIR Report** – Incident response case studies
- **Blue Team Labs Online** – Defensive labs & writeups
- **MITRE ATT&CK Blog** – TTP analysis & mappings
- **Threat Hunter Playbook** – Hunting methodologies

Bug Bounty

Cheatsheets / Roadmaps

- **Bug Bounty Roadmaps** – Structured learning paths & methodology checklists

Program Rules & Scope

- **HackWithGoodFaith** – Understand scope, safe harbor, and disclosure rules

Bug Bounty Platforms

- **Bugcrowd** – Crowdsourced vulnerability discovery
- **HackerOne** – Industry-standard hacker-powered security platform
- **huntr** – Open-source focused bug bounty board
- **Intigriti** – European bug bounty platform
- **Safe Hats** – Managed bug bounty programs
- **Synack** – Private, vetted researcher platform
- **Yes We Hack** – Global bug bounty & disclosure platform

Program Management

- Bug bounty program design & scoping
- Safe harbor & legal alignment
- Researcher communication workflows
- Duplicate & severity management

Intake & Triage

- **HackerOne / Bugcrowd (Program Owner View)** – Report intake & tracking
- **CVSS scoring** – Impact & risk prioritization
- **False positive validation**
- **SLA tracking**

Remediation & Tracking

- Vulnerability lifecycle management
- Engineering handoff & fix validation
- Regression testing
- Closure verification

Governance & Risk

- Vulnerability trend analysis
- Root cause identification
- Control gap analysis
- Metrics for leadership & audits

Blue-Team Use Cases

- Supplement internal pentesting
- Discover unknown attack paths
- Validate security controls
- Reduce external attack surface

Command & Control - C2

C2 Frameworks

- **C3** – Rapid prototyping of custom C2 channels
- **Cobalt Strike** – Adversary simulation & red team ops
- **Covenant** – Collaborative .NET C2 framework
- **Loki** – Node.js C2 for Electron-based script-jacking
- **Merlin** – HTTP/2 C2 server & agent (Go)
- **Nighthawk** – OPSEC-focused, highly malleable implant
- **OcraC2** – Encrypted multifunctional C2 framework
- **phpsploit** – PHP-based webserver C2 backdoor
- **PoshC2** – Proxy-aware C2 for post-exploitation
- **Pupy** – Cross-platform C2 & post-exploitation (Python/C)
- **SILENTTRINITY** – Async post-exploitation agent (.NET/Python)
- **Sliver** – mTLS, WireGuard, HTTP(S), DNS C2
- **Thanatos** – Mythic C2 agent (Rust)
- **TrevorC2** – Covert C2 tunneled through legitimate websites

C2 Detection & Analytics

- **Beaconing Detection** – Periodic traffic analysis
- **Protocol Abuse Detection** – DNS, HTTP(S), mTLS misuse
- **JA3 / TLS Fingerprinting**
- **Behavioral Analytics** – Long-lived sessions, low-and-slow traffic

Network & Endpoint Telemetry

- **Network Logs** – Proxy, firewall, DNS, NetFlow
- **EDR/XDR** – Process + network correlation
- **PowerShell / Script Logging** – AMSI, ScriptBlock
- **Command-line Auditing**

Threat Intelligence

- **C2 Infrastructure Tracking**
- **Known C2 Signatures & IOCs**
- **MITRE ATT&CK (TA0011 – C2)**
- **ISAC / Vendor Threat Feeds**

Prevention & Containment

- Egress filtering & allow-listing
- DNS logging & sinkholing
- TLS inspection (where permitted)
- Network segmentation

Incident Response

- C2 isolation & host containment
- Memory & process inspection
- Infrastructure blocking
- Post-incident hunting & rule tuning

Cheat Sheets

API & Application Security

- **OWASP API Top 10** – Common API vulnerabilities
- **OWASP API Security Checklist** – API attack surface coverage
- **OWASP REST Security Cheat Sheet**
- **OWASP REST Assessment Cheat Sheet**
- **OWASP GraphQL Cheat Sheet**
- **Web API Pentesting (GitBook)** – Practical API attack techniques

Offensive Techniques

- **Active Directory Cheat Sheet** – Enumeration & attack methods
- **Binary Exploitation Notes** – Memory corruption & exploitation
- **The Hacker Recipes** – Practical hacking guides
- **Red Teaming Experiments** – Red team tradecraft
- **Packet Life** – Network & protocol wall posters
- **OWASP Cheat Sheet Series** – AppSec attack techniques

Defensive Security

- **AD Kill Chain – Attack & Defense** – Active Directory attack detection & mitigation

Secure Design & Hardening

- **OWASP API Security Checklist** – Defensive API controls
- **OWASP REST / GraphQL Security Cheat Sheets** – Secure implementation guidance
- **OWASP Microservices Security** – Service-to-service defense patterns

Detection & Response

- **OWASP Cheat Sheet Series (Defensive Use)** – Secure coding & mitigation
- **MITRE ATT&CK Cheat Sheets** – Detection & coverage mapping
- **IR Playbooks & Runbooks** – Response quick-reference guides

Governance & Assurance

- Secure configuration baselines
- Control validation checklists
- Audit & inspection prep sheets

Cloud & Containers

AWS
- **pacu** – AWS exploitation framework
- **WeirdAAL** – AWS attack library
- **GreyHat Warfare** – Search exposed cloud buckets
- **ScoutSuite** – Multi-cloud security auditing
- **Cloudsplaining** – Identify least-privilege violations

Azure
- **Azurcar** – Azure security auditing
- **ScoutSuite** – Multi-cloud auditing

Buckets & Storage
- **OpenBuckets** – Discover public/misconfigured buckets (AWS, Azure, GCP, etc.)

Containers & Kubernetes
- **IceKube** – K8s attack path discovery
- **Docker Daemon Attack Surface** – Docker security review areas

Git & Source Exposure
- **gitrob** – GitHub org reconnaissance
- **GitRoller** – Git reconnaissance
- **Yar** – Repo & org reconnaissance
- **truffleHog** – High-entropy secret discovery
- **gitleaks** – Secrets scanning
- **shhgit** – Exposed secrets discovery
- **go-gitaudit** – Git repo auditing

Cloud Security Posture
- **Prowler** – AWS best practices, IR readiness, hardening
- **ScoutSuite** – Continuous multi-cloud posture assessment
- **Cloudsplaining** – IAM least-privilege enforcement

Containers & Kubernetes Security
- **Trivy** – Vulnerabilities, misconfigurations, secrets, SBOM
- **Grype** – Container & filesystem vulnerability scanning
- **Clair** – Static container image analysis
- **Dockle** – Container image best-practice linting
- **Checkov** – IaC & container security (shift-left)

Supply Chain & SBOM
- **Syft** – Generate SBOMs from images & filesystems
- **ScanCode Toolkit** – License & dependency inventory

Secrets Management
- **gitleaks / truffleHog** – Prevent secret leakage
- **CI/CD secret scanning**
- **Cloud secrets managers** (AWS SM, Key Vault)

Detection & Response
- Cloud audit logs (CloudTrail, Azure Activity Logs)
- Runtime container alerts
- IAM abuse & anomalous API call detection

Collaboration

Tracking & Collaboration Frameworks

- **Dradis** – Centralized collaboration, findings tracking, reporting
- **Mythic** – Collaborative red team C2 & operation management

Live Collaboration

- **tmate** – Real-time terminal sharing for joint operations
- **Shared attack logs & notes** – Operator coordination

Case Management & Coordination

- **ServiceNow SecOps** – Incident & case tracking
- **Jira / GitHub Issues** – Finding & remediation tracking
- **IR ticketing systems** – Incident lifecycle management

Real-Time Collaboration

- **Secure chat platforms** – Slack, Teams (IR channels)
- **Screen & terminal sharing** – Incident analysis collaboration
- **War room workflows** – Coordinated response

Documentation & Knowledge Sharing

- **Confluence / Wikis** – Playbooks, procedures, lessons learned
- **Runbooks & SOPs** – Standardized response actions
- **Evidence repositories** – Centralized artifacts & logs

Governance & Oversight

- Approval workflows
- Audit trails
- After-action reporting

Cracking

Password Cracking Tools

- **Cain & Abel** – Password recovery for Windows systems
- **Hashcat** – High-performance password cracking engine
- **Hydra** – Online password brute-forcing
- **John the Ripper** – Password auditing & recovery
- **NPK** – Distributed hash-cracking platform

Credential Protection

- Strong password policies
- Password hashing (bcrypt, scrypt, Argon2)
- MFA enforcement
- Credential rotation

Detection & Monitoring

- Brute-force detection
- Authentication failure analytics
- Password spray detection
- SIEM correlation rules

Prevention & Hardening

- Rate limiting & account lockouts
- Adaptive authentication
- CAPTCHA / challenge-response
- Service account hygiene

Auditing & Validation

- Password audit reviews
- Compromised credential monitoring
- Red-team findings remediation
- Policy compliance checks

Cryptography

Key & Crypto Weakness Discovery

- **Badkeys** – Detect weak, reused, or vulnerable public keys
- **RsaCtfTool** – RSA attack automation (weak keys, padding, exponents)
- **XORTool** – Analyze and break XOR-based encryption
- **HashPump** – Exploit hash length extension attacks

Crypto Analysis & Attacks

- Weak key detection (small key sizes, reuse)
- Improper randomness & entropy issues
- Broken or deprecated algorithms (MD5, SHA-1, DES)
- Improper TLS / certificate usage
- Padding oracle & timing attacks

Practical Use Cases

- Exploit misconfigured TLS
- Break improperly generated keys
- Abuse insecure crypto implementations

Key Management

- **KMS / HSMs** – AWS KMS, Azure Key Vault, GCP KMS
- Secure key generation & rotation
- Hardware-backed key protection
- Separation of key usage & access

Encryption Standards

- Strong algorithms (AES-256, RSA-2048+, ECC)
- Approved hash functions (SHA-256/384)
- TLS 1.2 / 1.3 enforcement
- Certificate lifecycle management

Detection & Validation

- Weak crypto configuration scanning
- Certificate expiration & misuse monitoring
- TLS inspection & validation
- FIPS compliance checks (where required)

Governance & Compliance

- Crypto policies & standards
- Approved algorithm lists
- NIST & FIPS alignment
- Audit evidence & key usage logs

CTF - Offensive & Defensive

Continuous Platforms

- **Crackmes** – Reverse engineering practice
- **CryptoHack** – Modern cryptography challenges
- **CTF Challenge** – Vulnerable web apps w/ realistic infra
- **CTFLearn** – Beginner-friendly CTF learning
- **CTFtime** – CTF events, rankings, team coordination
- **DomGoat** – DOM & client-side security challenges
- **Hack The Box** – Offensive labs & real-world scenarios
- **Nightmare** – Binary exploitation & RE course
- **Offensive Security (Proving Grounds)** – Standalone pentest labs
- **pwnable.tw / pwnable.kr / pwnable.xyz** – Binary exploitation challenges
- **ringzer0ctf** – Mixed-discipline CTF challenges
- **ROP Emporium** – Return-Oriented Programming challenges
- **Roppers Academy** – ROP fundamentals
- **TryHackMe (King of the Hill)** – Competitive offensive labs
- **VulnHub** – Downloadable vulnerable machines

Seasonal / Competitive

- **Hack-A-Sat** – USAF / USSF space-focused CTF

Blue-Team CTF & Labs

- **Blue Team Labs Online** – Detection & IR-focused challenges
- **Purple-team labs** – Attack → detect → respond exercises
- **Defensive CTFs** – Log analysis, alert tuning, IR scenarios

Defensive Skill Development

- Log analysis & SIEM challenges
- Incident response simulations
- Malware triage & forensics challenges
- Detection engineering exercises

Team & Process Benefits

- Improve alert triage speed
- Validate detection coverage
- Practice coordinated response
- Identify logging gaps

Data Exfiltration & Defense

Physical Attack Platforms

- **P4wnP1 ALOA** – Raspberry Pi Zero W platform for physical pentesting & red teaming

Exfiltration & Covert Channels (Software + Hardware-Assisted)

- **Cloakify** – Data exfiltration in plain sight
- **DET (Data Exfiltration Toolkit)** – Multi-channel exfiltration framework
- **DNSExfiltrator** – Data exfiltration over DNS
- **Exphil** – Data exfiltration PoC scripts
- **IPv6Exfil** – Exfiltration via IPv6 AAAA records
- **LNKUp** – Malicious LNK payload generation for exfiltration
- **PowerExfil** – PowerShell-based exfiltration scripts
- **PyExfil** – Python-based exfiltration tooling
- **SG1** – Encryption, exfiltration & covert comms toolkit
- **XXEtimes** – OOB XXE data exfiltration

Physical Security Controls

- Controlled access to endpoints & ports
- USB device control & blocking
- Secure workstation policies
- Hardware asset accountability

Endpoint & Peripheral Protection

- Device control (USB, HID, storage)
- EDR monitoring of removable media
- PowerShell & script execution logging
- Application allow-listing

Network & Egress Controls

- DNS monitoring & anomaly detection
- Egress filtering & protocol allow-lists
- TLS inspection (where permitted)
- Covert channel detection

Detection & Response

- Physical intrusion indicators
- Suspicious peripheral behavior
- Abnormal DNS / IPv6 traffic analysis
- Endpoint isolation & forensic review

Default Passwords

Default and Common Usernames and Passwords are Collected and Stored on INFOSEC GitHub Repository

- *Access this Collection Here: https://infosec.house/passwords/all_default_combos.txt*

Core Guidance (What "Good" Looks Like)

- Eliminate vendor default credentials **before production**
- Enforce **unique credentials per system**
- Disable or rename default / built-in accounts where possible
- Require **MFA** for all administrative access
- Rotate credentials after install, reset, or compromise
- Treat service accounts as **high-value assets**

Discovery & Validation Tools

- **Nmap NSE** – http-default-accounts, ftp-anon, ssh-auth-methods
- **Nessus / Qualys** – Default credential & weak password checks
- **OpenVAS / Greenbone** – Default login detection
- **CIS-CAT** – Baseline checks for default accounts
- **Lynis** – Linux local account & auth auditing
- **PowerShell AD Audits** – Find unused / default domain accounts

Cloud & Platform Checks

- **AWS IAM Access Analyzer** – Over-permissive / unused identities
- **Azure AD Identity Secure Score** – Weak & default account risks
- **GCP IAM Recommender** – Excessive permissions & unused accounts
- **Kubernetes** – Default service account usage audits

Prevention & Hardening

- Enforce password policies (length, complexity, rotation)
- Disable anonymous & guest access
- Lock down management interfaces
- Apply CIS Benchmarks during build
- Use **Just-Enough-Administration (JEA)**

Secrets & Credential Management

- **Password Managers** – Enterprise vaults (CyberArk, Vault, 1Password)
- **Secrets Managers** – AWS Secrets Manager, Azure Key Vault
- **Credential Rotation Automation**
- Avoid hard-coded credentials

Monitoring & Detection

- Failed authentication alerting
- Password spraying detection
- Login attempts against default usernames
- SIEM correlation for auth abuse

E-Mail

MX & Mail Infrastructure

- **MX-Takeover** – Detect misconfigured MX records & takeover risk
- **DNS enumeration tools** – Identify mail servers & providers
- **Open relay testing** – Identify misconfigured SMTP relays

Phishing & Abuse

- Phishing infrastructure setup
- Spoofed sender testing
- Attachment & link delivery testing
- Mail gateway bypass techniques

Mail Authentication Weaknesses

- Missing or misconfigured **SPF / DKIM / DMARC**
- Weak domain alignment
- Legacy mail protocol abuse

Mail Authentication & DNS

- **SPF** – Authorized sender enforcement
- **DKIM** – Message integrity & authenticity
- **DMARC** – Policy enforcement & reporting
- **MX record validation** – Prevent mail routing abuse

Secure Email Gateways

- **Proofpoint**
- **Mimecast**
- **Microsoft Defender for Office 365**
- **Google Workspace Security**

Monitoring & Detection

- DMARC aggregate & forensic reports
- Phishing detection & alerting
- Attachment & URL detonation
- Domain spoofing monitoring

User & Process Controls

- Phishing awareness training
- User-reported phishing workflows
- Incident response playbooks
- Mailbox compromise response

Editors and Viewers

Data Inspection & Manipulation

- **BStrings** – Enhanced strings extraction
- **CyberChef** – Data decode, transform, and manipulate
- **Hardcodes** – Discover hardcoded secrets in source code
- **Hexed.it** – Browser-based hex editor
- **Hexyl** – CLI hex viewer

Recon & Analysis Support

- **dsieve** – Subdomain filtering & enrichment
- Binary & memory artifact inspection
- Payload crafting & data decoding

Artifact Analysis & Forensics

- **CyberChef** – Decode logs, malware artifacts, and encodings
- **BStrings** – Extract indicators from binaries
- **Hexyl / Hex Editors** – File & memory inspection
- **Hardcodes** – Identify embedded secrets in code

Detection & Validation

- Indicator extraction & enrichment
- Suspicious file content review
- Log normalization & decoding

Secure Development & Review

- Source code inspection
- Secrets discovery & removal
- Validation of third-party artifacts

Education

Offensive Training & Labs

- **Offensive Security** – Hands-on pentesting & exploit development
- **Hack The Box Academy** – Offensive skill paths & labs
- **Pentester Academy** – Pentesting techniques & labs
- **PentesterLab** – Web exploitation training
- **PortSwigger Web Security Academy** – Web app attacks
- **Hacker101** – Web security fundamentals
- **PWN College / pwn.guide** – Binary exploitation & RE
- **Bust-A-Kube** – Attacking Kubernetes clusters

Bug Bounty & AppSec

- **Bug Bounty Hunter** – Bug bounty learning paths
- **Kontra** – Application security training
- **Hacksplaining** – Secure coding & attack concepts

Defensive & DFIR Training

- **SANS Institute** – SOC, DFIR, Blue team training & certs
- **Antisyphon InfoSec Training** – Practical Blue/Purple courses
- **DFIR Diva** – Curated DFIR & Blue-team resources
- **Cybrary** – Blue-team, SOC, and cloud security paths
- **INE / eLearnSecurity** – Defensive & cloud security training
- **Infosec Institute** – Defensive skills & certifications

Foundations & Certification Prep

- **Professor Messer** – IT & security fundamentals
- **TestOut** – Ethical Hacker & defensive labs
- **Pluralsight** – Secure development & cloud fundamentals
- **Udemy** – Broad security learning (varies by course)
- **ICS Learn** – Introductory information security

Career & Continuous Learning

- **AQ Answers** – Free courses, workshops, jobs
- **CoursesOnline** – Training catalog & discovery
- **ITOnlineLearning** – Security & behavioral analytics

Emulation

Adversary Emulation Frameworks

- **CALDERA** – Automated adversary emulation platform
- **DumpsterFire** – Modular, time-delayed security event simulation
- **SILVER** – Adversary emulation framework

Red-Team Use Cases

- Simulate real-world threat actors
- Validate attack chains & TTPs
- Exercise lateral movement & persistence
- Test detection & response readiness

Detection Validation

- Use emulation to validate alert coverage
- Map activity to **MITRE ATT&CK**
- Identify detection gaps & blind spots

SOC & IR Exercises

- Purple-team simulations
- Tabletop + live-fire exercises
- Response workflow validation

Improvement & Tuning

- Detection rule refinement
- Logging gap identification
- Response playbook validation

Endpoint Protection

Anti-Virus

- **Avast** – Ensure privacy, security, and performance with complete endpoint protection
- **Avira** – Lightweight antivirus with fast deployment
- **BitDefender** – Threat prevention, detection, and response solutions
- **ClamAV** – Open-source antivirus engine for malware detection
- **Emsisoft** – Malware protection with behavior-based detection
- **ESET** – Lightweight antivirus and endpoint security
- **F-Secure** – Enterprise and consumer endpoint protection
- **G-Data** – Malware detection and endpoint defense
- **Kaspersky** – Endpoint Security Cloud platform
- **Malwarebytes** – Protection against malware, ransomware, and malicious sites
- **McAfee** – Cross-platform antivirus and identity protection
- **Norton** – Consumer and enterprise antivirus solutions
- **Objective-See** – macOS-focused security tools
- **Panda** – Next-generation endpoint protection
- **Sophos** – Antivirus with exploit prevention and ransomware protection
- **Trend Micro** – Enterprise endpoint and cloud workload security
- **Webroot** – Cloud-based endpoint and threat intelligence protection

EDR (Endpoint Detection & Response)

- **Carbon Black** – Threat hunting and IR with continuous endpoint visibility
- **Cisco Secure Endpoint** – Cloud-native endpoint protection and response
- **Comodo** – Endpoint protection with threat hunting
- **Cortex XDR (Palo Alto)** – AI-driven endpoint detection and response
- **Cylance** – AI-based malware prevention
- **Cynet** – XDR platform with automated response
- **ESET (EDR)** – Endpoint visibility, breach detection, and response
- **FireEye** – Intelligence-led endpoint security
- **FTK Enterprise** – Endpoint data visibility for investigations
- **Intercept X (Sophos)** – XDR-driven endpoint protection
- **McAfee MVISION** – Endpoint security with integrated XDR
- **N-able** – Automated endpoint protection
- **SanerNow** – Endpoint risk detection and remediation
- **SentinelOne** – Autonomous XDR endpoint protection
- **Symantec Endpoint Security Enterprise** – Advanced endpoint threat prevention
- **WatchGuard** – Next-gen endpoint security platform
- **Wazuh** – Endpoint monitoring, intrusion detection, and compliance

Endpoint Protection Platforms

- **Microsoft Defender for Endpoint** – Native Windows EDR/XDR with deep telemetry
- **CrowdStrike Falcon** – Cloud-native EDR/XDR with threat intelligence
- **SentinelOne** – Autonomous prevention, detection, and response
- **Sophos Intercept X** – Anti-ransomware and behavioral detection
- **Carbon Black** – Enterprise EDR and threat hunting
- **Cortex XDR** – Endpoint + network + cloud correlation

Detection & Monitoring

- **Script Logging (AMSI)** – PowerShell and script inspection
- **Behavioral Analytics** – Identify anomalous execution
- **Threat Hunting** – Proactive detection of stealthy activity

Evasion

Anti-Virus Evasion

- **Shellter** – Dynamic shellcode injection framework designed to evade AV
- **Veil** – Generates payloads that bypass common anti-virus solutions

ELF Obfuscation

- **ELFcrypt** – Simple ELF crypter using RC4 encryption

Obfuscation

- **IPObfuscator** – Converts IP addresses into DWORD format to evade detection

Memory Evasion

- **NimShellcodeFluctuation** – Shellcode fluctuation PoC implemented in Nim
- **ShellcodeFluctuation** – Memory-based shellcode mutation to evade signatures

Detection Engineering

- **Behavior-based detection** – Identify abnormal process behavior
- **AMSI inspection** – Detect obfuscated and in-memory scripts
- **Command-line logging** – Capture encoded and suspicious execution
- **Memory scanning** – Detect injected or unpacked shellcode

Endpoint Telemetry

- **Process ancestry tracking** – Identify parent/child abuse
- **Module & DLL load monitoring** – Catch reflective loading
- **Sysmon** – High-fidelity endpoint telemetry
- **EDR memory analysis** – Detect in-memory payloads

Prevention & Hardening

- **Application control** – Block unknown binaries
- **Script block logging** – PowerShell, WMI, LOLBins
- **Exploit mitigation** – DEP, ASR rules, exploit guards
- **Least privilege enforcement** – Limit execution context

Threat Hunting & Response

- Hunt for encoded commands & entropy anomalies
- Identify long-lived suspicious processes
- Isolate compromised endpoints
- Tune detections based on red-team tradecraft

Exploits

Browser Exploitation

- **BeEF** – Browser Exploitation Framework for client-side attacks

Exploit Databases & Research

- **0-Day Today (TOR)** – Marketplace and database for exploits and zero-days
- **Exploit Database** – Public exploit repository maintained by Offensive Security
- **Sploitus** – Aggregates newest exploits across multiple sources
- **SecurityFocus** – Vulnerability research, advisories, and technical papers

Platform & Kernel Exploits

- **Android Kernel Exploits** – Android kernel vulnerability exploits
- **Linux Kernel Exploits** – Linux privilege escalation exploits
- **macOS Kernel Exploits** – macOS kernel vulnerabilities
- **Windows Kernel Exploits** – Windows kernel exploitation techniques
- **Windows Rootkits** – Persistent kernel-level malware

Vulnerability Intelligence

- **NIST NVD** – Official CVE vulnerability database

Vulnerability Intelligence & Tracking

- **NIST NVD** – CVE tracking and severity scoring
- **Vendor advisories** – Patch and mitigation guidance
- **Threat intelligence feeds** – Exploit-in-the-wild awareness

Detection & Prevention

- **EDR / XDR** – Detect exploit behavior and post-exploitation activity
- **Exploit mitigation** – DEP, ASR rules, exploit guards
- **Browser isolation** – Reduce client-side exploit impact
- **Application sandboxing** – Contain exploitation attempts

Patch & Configuration Management

- **Patch management systems** – Timely vulnerability remediation
- **Configuration hardening** – Reduce exploitability
- **Attack surface reduction** – Disable unnecessary services

Validation & Assurance

- **Vulnerability scanners** – Identify exploitable weaknesses
- **Pen test findings review** – Confirm real-world risk
- **Exploit attempt alerting** – SIEM correlation for exploit chains

Firewalls

Firewall Hardware (Targeted)

- **Netgate** – pfSense-based firewall, VPN, and routing appliances
- **UniFi** – Enterprise-grade networking and security appliances
- **Untangle** – Cloud-managed network security framework

Firewall Software (Targeted)

- **ClearOS** – Linux-based SME network gateway
- **Endian** – Turn-key Linux firewall and security appliance
- **IPFire** – Open-source Linux firewall
- **OPNsense** – Open-source FreeBSD firewall platform
- **pfSense** – FreeBSD-based firewall using PF
- **Shorewall** – Linux firewall configuration framework
- **Sophos XG** – Unified firewall with IPS, VPN, and web filtering
- **VyOS** – Open-source router and firewall platform

Web Application Firewalls (Targeted)

- **Lua Resty WAF** – High-performance OpenResty-based WAF
- **ModSecurity** – Open-source cross-platform WAF engine
- **NAXSI** – NGINX-focused high-performance WAF
- **Predator** – Anti-automation protection system
- **Shadow Daemon** – Web application firewall server
- **Vulture** – Open-source WAF

WAF Identification, Testing & Bypass

- **Awesome WAF – Known Bypasses** – Collection of known WAF bypass techniques
- **Abuse SSL Bypass** – Bypass WAFs via SSL/TLS cipher abuse
- **FTW** – Framework for Testing WAF detection logic
- **gotestwaf** – Test WAF detection and bypass behavior
- **hakoriginfinder** – Discover origin servers behind reverse proxies
- **IdentYwaf** – Blind WAF fingerprinting
- **Lightbulb Framework** – WAF auditing toolkit
- **WAF Bench** – Measure WAF performance
- **WAF Bypass** – DNS history-based WAF bypass checks
- **WAF Ninja** – Tools to attack WAF protections
- **WAF Tester** – Automated WAF testing
- **wafw00f** – Identify and fingerprint WAF products
- **WhatWaf** – Detect and bypass WAF and protection systems

Network Firewalls

- **pfSense / OPNsense** – Stateful firewalling, VPN, IDS/IPS
- **Sophos XG** – Unified firewall with threat prevention
- **Netgate** – Enterprise firewall appliances
- **VyOS** – Routing and firewall enforcement

Web Application Firewalls (WAF)

- **ModSecurity** – Rule-based web attack prevention
- **NAXSI** – NGINX-focused anomaly detection
- **Lua Resty WAF** – High-performance request inspection
- **Cloud WAFs** – AWS WAF, Azure WAF, Cloudflare

Detection & Monitoring

- **WAF logs** – Injection, traversal, automation attempts
- **SIEM correlation** – Network + app-layer alerting

Response & Validation

- Rule tuning from attack telemetry
- Origin IP protection
- Rate limiting & bot mitigation
- Purple-team WAF testing feedback

Forensics

Blockchain
- **Orbit** – Blockchain transaction investigation and analysis tool

Browser Forensics
- **Hindsight** – Chrome/Chromium browser forensic analysis

Disk Images
- **AFFLIBv3** – Advanced Forensic Format (AFF) disk imaging library
- **Autopsy** – GUI forensic platform built on The Sleuth Kit
- **DMG2IMG** – Convert Apple DMG images to standard disk images

Images & Documents
- **Disk Drill** – File recovery for Mac and Windows
- **Exiftool** – Read, write, and edit metadata
- **FOCA** – Extract metadata and hidden information from documents

Mobile
- **Andriller** – Forensically sound Android acquisition tool

Malware / Analysis Scripts
- **DissectingMalwa.re Lab** – Malware analysis & reverse engineering setup scripts

SQL
- **DFIR SQL Query** – SQL queries for DFIR investigations

Data Analysis
- **Beagle** – Transform security logs into investigative graphs

Windows Artifacts
- **AmcacheParser** – Parse amcache.hve execution artifacts
- **AppCompatCacheParser** – Shimcache (AppCompatCache) parser
- **Auditpol** – View and manage Windows audit policies
- **EvtxECmd** – Windows Event Log parser
- **ExtensionBlocks** – Parse ShellBag extension blocks
- **iisGeolocate** – Geolocate IPs from IIS logs
- **JLECmd** – Jump List artifact parser
- **KAPE** – Artifact collection and triage framework
- **LECmd / Lnk** – LNK file analysis
- **MFT / MFTECmd** – NTFS Master File Table parsing
- **OleCF** – OLE compound file processing
- **PECmd / Prefetch** – Windows Prefetch analysis
- **RBCmd** – Recycle Bin artifact parsing
- **Registry / Registry Explorer** – Offline Windows Registry parsing
- **SDB** – Shim database parsing
- **SQLECmd** – SQLite artifact parsing
- **SrumECmd** – SRUM activity analysis
- **SumECmd** – User Access Log parsing
- **TLEFilePlugins** – Timeline Explorer CSV parsing
- **USBDevices** – USB history extraction from Registry
- **VSCMount** – Volume Shadow Copy mounting
- **WinSearchDBAnalyzer** – Windows Search database parsing
- **WtTCmd** – Windows Timeline database parsing

Incident Response & DFIR
- **Autopsy / Sleuth Kit** – Full disk & file system investigations
- **KAPE** – Rapid artifact collection during IR
- **Velociraptor / GRR** – Live endpoint forensic collection
- **Memory acquisition tools** – Volatile evidence capture

Log & Timeline Analysis
- **EvtxECmd / Beagle** – Event log analysis & correlation
- **SRUM / Prefetch / Amcache** – Execution & usage tracking

Governance, Risk, and Compliance (GRC)

Control Weakness Discovery

- **Policy Gap Analysis** – Identify missing, outdated, or unenforced policies
- **Control Mapping Review** – Find unmapped or improperly implemented controls
- **Evidence Validation Testing** – Challenge accuracy and freshness of evidence

Audit & Compliance Evasion (Simulation)

- **Documentation Review** – Identify boilerplate, copy-paste, or stale artifacts
- **Process Walkthroughs** – Expose gaps between written policy and real practice
- **Interview-Based Testing** – Assess staff awareness and procedural consistency

Risk Exploitation

- **Risk Register Analysis** – Identify accepted risks with high residual exposure
- **Exception Abuse** – Leverage overly broad or permanent risk acceptances
- **Inherited Control Assumptions** – Challenge unsupported inherited controls

GRC Platforms & Tooling

- **ServiceNow GRC** – Enterprise risk, compliance, and audit management
- **RSA Archer** – Risk management and regulatory compliance
- **OneTrust GRC** – Privacy, risk, and compliance automation
- **Drata / Vanta** – Continuous compliance monitoring
- **JupiterOne** – Asset-centric cyber risk management

Frameworks & Standards

- **NIST RMF** – Risk-based security authorization framework
- **NIST SP 800-53** – Security and privacy control catalog
- **ISO/IEC 27001** – Information security management system (ISMS)
- **SOC 2** – Trust services criteria
- **CIS Critical Security Controls** – Prioritized defensive safeguards

Risk Management

- **Risk Registers** – Threat, vulnerability, and impact tracking
- **Risk Assessments (RA)** – Likelihood × impact analysis
- **POA&M Tracking** – Remediation planning and accountability
- **Risk Acceptance** – Formal residual risk decisions

Compliance & Audit Readiness

- **Policy & Procedure Management** – Versioned, approved governance artifacts
- **Control Evidence Repositories** – Centralized audit evidence
- **Continuous Monitoring** – Control effectiveness validation
- **Inspection / Audit Prep** – Readiness checklists and walkthroughs

Governance Operations

- Roles & responsibilities (ISSO, AO, System Owner)
- Metrics & reporting for leadership
- Exception management & expiration tracking
- Lessons learned & governance improvement

Hardware

General Hardware

- **Arduino** – Open-source electronic prototyping platform for interactive hardware projects
- **Raspberry Pi** – Low-cost single-board computer for custom tooling and implants
- **USB Armory Mk II** – Open-source flash-drive-sized computer for security research

Equipment / Implants

- **Attify Badge** – Hardware security assessment tool for embedded device interfaces
- **DigiSpark** – ATtiny85-based microcontroller for small form-factor payloads
- **GoodFET** – Embedded bus adapter and JTAG interface for microcontrollers
- **GreatFET One** – Hardware hacking and reverse-engineering platform
- **O.MG Cable** – Covert cable with remote execution and stealth capabilities
- **OpticSpy** – Platform for experimenting with optical data transmission
- **Throwing Star LAN Tap / Pro** – Passive Ethernet tap for traffic monitoring

Reference & Layouts

- **Pinouts** – Connector, SBC, dev board, and chip layout reference

Stores & Supply

- **Hacker Gadgets** – Pentest and hacking hardware supplier
- **Hacker Warehouse** – Computer security hardware and tools
- **Hak5** – Authorized pentest and red-team hardware
- **Red Team Tools** – Physical red-team products

Physical Security Controls

- **Port security** – USB, Ethernet, and peripheral restrictions
- **Device control solutions** – Block unauthorized HID and storage devices
- **Tamper-evident seals** – Detect physical compromise
- **Asset tagging & tracking** – Prevent rogue device insertion

Endpoint & Peripheral Protection

- **USB device monitoring** – Detect rogue or emulated devices
- **EDR peripheral telemetry** – Identify abnormal HID behavior
- **Application allow-listing** – Prevent payload execution
- **BIOS / UEFI protections** – Secure boot and firmware integrity

Network Defense

- **Network Access Control (NAC)** – Enforce authenticated device access
- **ARP / MAC anomaly detection** – Identify taps and rogue hardware
- **Switch port monitoring** – Detect passive taps and link anomalies

Detection & Response

- **Physical inspection procedures** – Desk, port, and cable checks
- **SIEM correlation** – USB + process + network events
- **Incident response playbooks** – Hardware compromise handling
- **Forensic acquisition** – Preserve compromised devices

Honeypots

Honeypot Frameworks

- **Cowrie** – SSH/Telnet honeypot for credential harvesting and session capture
- **DemonHunter** – Distributed honeypot deployment framework
- **Dionaea** – Malware-focused honeypot capturing exploits and payloads
- **HellPot** – Infinite honeypot designed to trap and loop bots
- **HoneyTrap** – Advanced modular honeypot framework
- **MHN (Modern Honey Network)** – Centralized honeypot management platform
- **SNARE** – Reactive next-generation honeypot
- **TANNER** – HTTP-based honeypot backend
- **THUG** – Low-interaction honeyclient for malicious web content
- **T-Pot** – All-in-one multi-honeypot platform

Data Processing & Analysis

- **Mnemosyne** – Normalize and enrich honeypot event data

Threat Detection & Early Warning

- **Cowrie / Dionaea** – Detect credential stuffing, scanning, and malware delivery
- **T-Pot** – Rapid deployment of diverse honeypots for visibility
- **MHN** – Centralized honeypot telemetry and alerting

Intelligence Collection

- **Mnemosyne** – Normalize honeypot data for SIEM ingestion
- **IOC extraction** – IPs, domains, payload hashes
- **TTP mapping** – Align activity to MITRE ATT&CK

SOC Integration

- **SIEM ingestion** – Correlate honeypot alerts with network and endpoint logs
- **Threat hunting** – Pivot from honeypot hits to internal telemetry
- **Alert tuning** – Reduce false positives using deception signals

Response & Defense Improvement

- Block malicious IPs and infrastructure
- Update IDS/IPS and firewall rules
- Validate detection coverage
- Feed intel into vulnerability and patch prioritization

Identity & Access Management (IAM)

Credential Abuse & Discovery

- **Kerbrute** – Enumerate valid AD usernames via Kerberos
- **Spray365** – Azure AD password spraying framework
- **CredMaster** – Modular credential stuffing framework
- **Impacket** – Network protocol toolkit for auth abuse and lateral movement

Authentication Attacks

- **Mimikatz** – Credential extraction and token manipulation
- **Rubeus** – Kerberos abuse (AS-REP roasting, ticket attacks)
- **LaZagne** – Local credential recovery from applications
- **Responder** – LLMNR/NBT-NS poisoning for credential capture

Cloud & Identity Recon

- **AADInternals** – Azure AD reconnaissance and abuse testing
- **ROADtools** – Azure AD enumeration and attack path mapping
- **ScoutSuite (IAM focus)** – Identify over-permissive identities

IAM Platforms

- **Microsoft Entra ID (Azure AD)** – Cloud identity, MFA, conditional access
- **Active Directory** – Enterprise identity and authentication backbone
- **Okta** – Identity-as-a-Service and access governance
- **Ping Identity** – Federated identity and SSO
- **AWS IAM** – Cloud-native identity and permission management

Authentication & Authorization

- **MFA** – Phishing-resistant authentication (FIDO2, smart cards)
- **SSO** – Centralized authentication enforcement
- **RBAC / ABAC** – Role- and attribute-based access control
- **Privileged Access Management (PAM)** – Just-in-Time admin access

Identity Governance

- **Access Reviews** – Periodic entitlement validation
- **Lifecycle Management** – Joiner/Mover/Leaver automation
- **Service Account Hygiene** – Rotation and least privilege
- **Conditional Access** – Context-aware enforcement

Detection & Monitoring

- **Sign-in logs** – Failed auth, impossible travel, token abuse
- **UEBA** – Anomalous identity behavior detection
- **SIEM correlation** – Identity + endpoint + network signals
- **Password spray detection** – Early abuse identification

Hardening & Operations

- Disable legacy authentication
- Enforce least privilege by default
- Monitor and expire standing admin access
- Align to CIS & NIST identity controls

IDS / IPS

IDS / IPS Evasion & Testing

- **Traffic Fragmentation** – Evade signature-based detection
- **Protocol Abuse** – Exploit parser edge cases
- **Encoding & Obfuscation** – Bypass pattern matching
- **Low-and-Slow Attacks** – Avoid rate-based detection

Detection Validation

- **Custom Payload Testing** – Validate signature coverage
- **Rule Evasion Techniques** – Identify weak or outdated rules
- **Encrypted Traffic Abuse** – Hide activity in TLS
- **False-Negative Discovery** – Identify blind spots

IDS / IPS Platforms

- **CrowdSec** – Collaborative behavior-based IPS with community signals
- **Security Onion** – Enterprise threat hunting, NSM, and log management distro
- **SELKS** – Suricata-based IDS/IPS and network security monitoring
- **Snort** – Open-source signature-based intrusion detection
- **Suricata** – High-performance open-source threat detection engine

Detection Capabilities

- Signature-based detection
- Protocol anomaly detection
- Behavioral analysis
- Threat intelligence enrichment

Deployment & Operations

- Inline IPS vs passive IDS placement
- Network segmentation visibility
- Rule lifecycle management
- Performance tuning & packet loss monitoring

SOC Integration

- **SIEM ingestion** – Correlate alerts with endpoint and identity data
- **Threat hunting** – Pivot from IDS alerts to full attack chains
- **Alert tuning** – Reduce false positives

Response & Improvement

- Block malicious IPs and traffic
- Update rules from new threat intel
- Purple-team validation
- Continuous detection improvement

Incident Response

Identity & Access Impact

- **LogonTracer** – Visualize and analyze suspicious Windows logon activity

Data Exfiltration Awareness

- **LOTS Project** – Catalog of legitimate domains abused for phishing, C2, and exfiltration

IR Process Stress Testing

- Incident playbook walkthroughs
- Detection-to-response timing analysis
- Alert fatigue and escalation gap discovery
- Evidence availability testing

Incident Management Platforms

- **DFIRTrack** – Incident tracking and response coordination
- **FIR** – Fast Incident Response case management
- **TheHive** – Scalable open-source incident response platform
- **Wazuh** – Endpoint monitoring, detection, and response

Collection & Investigation

- **Velociraptor** – Endpoint artifact collection using VQL
- **Redline** – Host-based forensic investigation
- **ETWMonitor** – Detect suspicious activity via ETW logs
- **Log-MD** – Identify malware artifacts on Windows systems

Analysis & Enrichment

- **Cortex** – Observable analysis and active response automation
- **IoCextract** – Extract and normalize IOCs from text
- **IoC Radar** – Threat actor, malware, and attacker IOC feeds

IOC Scanning & Validation

- **Fenrir** – Lightweight bash IOC scanner
- **Loki** – IOC and YARA-based malware scanner
- **Thor Lite** – Free IOC and YARA scanner
- **Log4Shell Scanner** – IOC and YARA detection for Log4j

Persistence & Threat Hunting

- **PersistenceSniper** – Hunt Windows persistence mechanisms
- **YARA / yarGen** – Generate and deploy custom detection rules

Reporting & Closure

- Timeline reconstruction
- Impact assessment
- Lessons learned documentation
- Detection & control improvements

Linux

Auditing & Enumeration

- **Linux Exploit Suggester** – Identify potential local privilege escalation paths based on kernel and package versions

Cheatsheets & Abuse Paths

- **GTFOBins** – Curated list of Unix binaries that can bypass security restrictions in misconfigured systems

Post-Exploitation

- **EggShell** – Cross-platform remote administration tool for Linux/macOS/iOS
- **Mimipenguin** – Dump plaintext credentials from memory on Linux systems

System Hardening

- **CIS Benchmarks (Linux)** – Secure baseline configuration guidance
- **SELinux / AppArmor** – Mandatory access control enforcement
- **Least privilege** – Minimize sudo access and root usage
- **Package hygiene** – Remove unnecessary binaries and SUID files

Auditing & Monitoring

- **auditd** – Track privileged actions and system changes
- **journald / syslog** – Centralized log collection
- **File integrity monitoring (AIDE)** – Detect unauthorized changes
- **Process accounting** – Monitor command execution

Detection & Prevention

- **SUID/SGID monitoring** – Detect abuse-prone binaries
- **GTFOBins mapping** – Identify and restrict high-risk binaries
- **Kernel hardening** – Sysctl tuning and exploit mitigation
- **EDR for Linux** – Behavioral detection and response

Incident Response

- **Credential exposure checks** – Memory dump & log review
- **Persistence hunting** – Cron, systemd, rc scripts
- **Containment** – Kill malicious processes, rotate credentials
- **Forensic triage** – Timeline reconstruction from logs

Malware

Distribution & Analysis Platforms

- **ANY.RUN** – Interactive malware analysis for dynamic and static research
- **Contagio Malware Dump** – Curated malware samples and research archive
- **CAPE Sandbox** – Automated malware analysis and payload extraction
- **Das Malwerk** – Daily malware sample archive
- **Hatching Triage** – Scalable malware sandboxing platform
- **Hybrid Analysis** – Static and dynamic malware analysis service
- **InQuest** – Malware analysis and threat research platform
- **KernelMode.Info** – Reverse engineering and OS internals forum
- **Malshare** – Malware repository with YARA results
- **Malware Bazaar** – abuse.ch malware sharing project
- **Malware Samples** – Archive mapped to public threat reports
- **theZoo (Malware-DB)** – Public malware analysis repository
- **Objective-See** – macOS malware sample collection
- **PacketTotal** – PCAP analysis for malware traffic
- **PhishingKitTracker** – Phishing kit archive for forensic analysis
- **Polyswarm** – Threat intelligence marketplace
- **SNDBOX** – Malware sandbox platform
- **SoReL-20M** – Massive malware dataset (20M samples)
- **URLhaus** – Malware URL distribution tracking
- **VirusBay** – SOC-to-researcher malware collaboration platform
- **VirusShare** – Large-scale malware sharing repository
- **VirusSign** – High-quality malware sample collection
- **Virus Samples** – Archive of malicious payloads across architectures
- **VX-Underground** – Large historical malware archive
- **Yori** – Sandbox-based file analysis service

Emulation & Anti-Analysis

- **Al-Khaser** – Test malware techniques for sandbox and VM detection

Malware / Ransomware Development

- **Coldfire** – Golang malware development library
- **GonnaCry** – Linux ransomware implementation
- **Neurax** – Self-propagating malware framework

Malware Analysis & Sandboxing

- **ANY.RUN / Hybrid Analysis** – Dynamic malware behavior analysis
- **FileScan** – High-speed sandbox and IOC extraction
- **Malcore** – Scalable malware sandboxing
- **Hatching Triage** – Automated malware triage

Multi-Engine Scanning

- **VirusTotal** – File, hash, URL, and IP reputation analysis
- **Jotti** – Multi-AV malware scanning
- **Opswat MetaDefender** – File reputation and sandboxing
- **Kaspersky Threat Portal** – Indicator and file analysis

Ransomware Identification & Recovery

- **ID Ransomware** – Identify ransomware families
- **NoMoreRansom** – Decryption tools and recovery guidance

Threat Intelligence & IOC Handling

- **URLhaus / Malware Bazaar** – Malicious infrastructure tracking
- **Polyswarm** – Community-driven threat intelligence
- **IOC extraction** – Hashes, domains, IPs, YARA rules

Detection & Response

- **EDR/XDR** – Behavioral malware detection
- **YARA** – Signature-based malware detection

Mobile

Jailbreaking & Rooting (Access Enablement)

- **Magisk** – Systemless Android rooting and module framework
- **checkra1n** – Hardware-based iOS jailbreak (A5–A11 devices)
- **unc0ver** – Jailbreak tool for modern iOS versions
- **IPSW** – Download and manage Apple firmware images

Dynamic Analysis & Instrumentation

- **Frida** – Dynamic instrumentation for Android and iOS apps
- **Objection** – Runtime mobile app manipulation framework (Frida-based)
- **Drozer** – Android security testing framework
- **MITMProxy** – Intercept and modify mobile app traffic
- **TCPDump** – Network traffic capture on mobile devices

Static Analysis & Reverse Engineering

- **MobSF** – All-in-one mobile app security analysis framework
- **JADX** – Dex-to-Java Android decompiler
- **APKTool** – Decode and rebuild Android APKs
- **radare2 / Cutter** – Reverse engineering platform
- **Smali** – Dalvik bytecode assembler/disassembler

Labs & Practice

- **DIVA** – Damn Insecure and Vulnerable Android App
- **Injured Android** – CTF-style Android vulnerabilities
- **UnCrackable Apps** – Mobile reverse engineering challenges

App Protection & Hardening

- **DexGuard** – Advanced Android code hardening and obfuscation
- **ProGuard** – Code shrinking and obfuscation for Android apps
- **Runtime Integrity Checks** – Root / jailbreak detection
- **Certificate pinning** – Prevent MITM interception

Static & Dynamic Security Testing

- **MobSF** – Automated static and dynamic mobile app analysis
- **Oversecured** – Android vulnerability scanner for DevSecOps
- **Ostorlab** – Static taint analysis and mobile risk detection

Secure Development Practices

- Secure key storage (Android Keystore / iOS Keychain)
- Remove hardcoded secrets
- Enforce least-privilege permissions
- Secure IPC and intent handling

Detection & Response

- **MDM / MAM** – Enforce device compliance and posture
- **Mobile Threat Defense (MTD)** – Detect malicious apps and behavior
- **Network monitoring** – Detect suspicious mobile traffic
- **Incident response playbooks** – Mobile compromise handling

Network

Network Discovery & Auditing

- **Nmap** – Network mapper for host discovery and service enumeration
- **masscan** – High-speed TCP port scanner
- **RustScan** – Modern, fast port scanner with Nmap integration
- **naabu** – Reliable, simple port scanner written in Go

LAN / WAN Attacks & Manipulation

- **Scapy** – Interactive packet crafting and manipulation library
- **bettercap** – Network attack and monitoring framework
- **Impacket** – Python toolkit for low-level network protocol attacks
- **ettercap** – MITM framework for LAN attacks

Man-in-the-Middle

- **MITMProxy** – Intercept and modify HTTP/TLS traffic
- **Inveigh** – IPv4/IPv6 MITM and credential capture tool

Packet Capture & Analysis

- **tcpdump** – CLI packet capture and inspection
- **Wireshark** – Full-featured network protocol analyzer
- **NetworkMiner** – Passive network traffic analysis

DoS / Stress Testing *(Authorized Only)*

- **Slowloris** – HTTP connection starvation testing
- **HULK** – Obfuscated HTTP load testing
- **RUDY** – Slow POST DoS testing

Network Monitoring & Visibility

- **Zeek** – Network security monitoring and traffic analysis
- **Security Onion** – NSM, IDS, and threat hunting platform
- **Zabbix** – Network and infrastructure monitoring
- **Splunk** – Network telemetry ingestion and correlation

Packet Analysis & Forensics

- **Wireshark** – Protocol-level inspection and troubleshooting
- **tcpdump** – Targeted capture and triage
- **CloudShark** – Cloud-based PCAP analysis and sharing

Detection & Protection

- **IDS / IPS integration** – Detect scanning, MITM, and abuse
- **DLP monitoring** – Detect unauthorized data movement
- **TLS inspection (where permitted)** – Inspect encrypted traffic
- **Rate limiting** – Mitigate scanning and DoS attempts

Network Hardening

- Network segmentation & VLANs
- Least-privilege firewall rules
- Disable legacy protocols (LLMNR, NetBIOS where possible)
- Secure DNS and certificate management

Incident Response

- Identify malicious traffic patterns
- Contain affected segments
- Block malicious IPs and domains
- Feed indicators into SIEM and IDS

Operating Systems

Penetration Testing Distributions

- **Kali Linux** – Debian-based OS for pentesting and digital forensics
- **BlackArch** – Arch Linux-based penetration testing distribution
- **Parrot OS** – Security- and privacy-focused GNU/Linux distribution
- **SecBSD** – BSD-based OS for security research and pentesting

Containers & Portable Environments

- **Exegol** – Community-driven, fully featured hacking environment (Docker-based)
- **easyWSL** – Run Docker containers as WSL distributions

Virtualized Platforms

- **CommandoVM** – Windows-based offensive security VM
- **RedNix** – Hackable NixOS container environment

DFIR & Forensics Distributions

- **SANS SIFT** – Linux distribution for forensic analysis and IR
- **Tsurugi** – DFIR-focused Linux distribution
- **Bitscout** – LiveCD/USB for remote forensic acquisition
- **WinFE** – Windows Forensics Environment

Forensic Toolkits

- **The Sleuth Kit** – File system and disk forensic analysis toolkit

Operational Use

- Evidence acquisition & preservation
- Timeline reconstruction
- Malware and artifact analysis
- Incident response readiness

Operation Security

Anonymity & Browsing
- **TOR** – Anonymous communication network
- **I2P** – Peer-to-peer anonymous network layer
- **Pantoclick** – Analyze browser fingerprinting exposure
- **WEBKAY** – Reveal what information your browser leaks

VPN & Proxies
- **Mullvad VPN** – Privacy-focused VPN with minimal logging
- **ProtonVPN** – Swiss-based privacy VPN

Secure Communications
- **Signal** – Encrypted messaging for SMS and voice
- **Briar** – Peer-to-peer encrypted messaging (offline capable)
- **Element** – Secure messaging over Matrix

Secure Email
- **ProtonMail** – End-to-end encrypted email service
- **SecureDrop** – Secure document submission platform

Anti-Forensics & Data Destruction
- **Darik's Boot & Nuke (DBAN)** – Secure disk wiping tool
- **Wipe** – Secure file deletion utility
- **SetMACE** – Manipulate NTFS timestamps
- **USBKill** – USB-triggered system kill switch

Identity & Payment Privacy
- **Njalla** – Privacy-aware domain registration
- **Monero** – Privacy-focused cryptocurrency

OPSEC Governance
- Acceptable use & anonymity policy
- Logging and monitoring boundaries
- Encryption & key management standards
- Legal & compliance oversight

Detection & Monitoring
- **SIEM correlation** – VPN, TOR, proxy usage detection
- **DLP controls** – Monitor data movement
- **Network analytics** – Identify anonymization traffic patterns

Endpoint & System Controls
- Disable unauthorized VPNs and proxies
- Monitor USB insertion and device control
- Prevent unauthorized disk wiping tools
- Endpoint telemetry for anti-forensic behavior

Identity & Access Protection
- **Password managers** – Bitwarden, 1Password
- **MFA hardware** – YubiKey, Titan Security Key
- **MFA apps** – Microsoft Authenticator, Duo

Awareness & Training
- OPSEC training for staff
- Social engineering awareness
- Secure communications guidance
- Incident escalation procedures

OSINT

OSINT Frameworks & Platforms

- **OSINT Framework** – Curated collection of free OSINT resources
- **Maltego** – Graph-based link analysis and investigation platform
- **IntelOwl** – Aggregate OSINT and threat intelligence via a single API
- **Scrummage** – OSINT and threat-hunting automation framework
- **Photon** – High-speed web crawler for OSINT data collection

Data Breach & Credential Exposure

- **DeHashed** – Search leaked credentials and breached datasets
- **Have I Been Pwned** – Check email addresses against known breaches
- **Snusbase** – Index of breached databases and leaked information

Email & Account Enumeration

- **Holehe** – Identify services linked to an email address
- **WhatsMyName** – Username enumeration across platforms

Social Media & Identity

- **Sherlock** – Find social media accounts by username
- **Social Analyzer** – Analyze and correlate social profiles
- **Osintgram** – Instagram account OSINT analysis

Business & Corporate Intelligence

- **Corporation Wiki** – Corporate ownership and relationship data
- **OCCRP Aleph** – Global investigative journalism archive
- **OpenGov US** – Public U.S. government datasets

Exposure & Risk Monitoring

- **Have I Been Pwned** – Monitor organizational email exposure
- **DeHashed** – Identify leaked credentials impacting the enterprise
- **IntelOwl / OpenCTI** – Integrate OSINT into threat intelligence workflows

Brand & Identity Protection

- Monitor social media impersonation
- Track executive and employee exposure
- Identify fraudulent domains and profiles

Data Broker & Privacy Management

- Opt-out workflows for people-search services
- Reduce employee PII exposure
- Executive privacy protection programs

Threat Intelligence & SOC Use

- Enrich alerts with OSINT context
- Correlate external signals with internal telemetry
- Prioritize incidents using public-source intelligence

Governance & Awareness

- OSINT awareness training
- Acceptable use guidance
- Social media policy enforcement
- Insider risk considerations

Privilege Escalation

Linux Privilege Escalation

- **LinPEAS** – Enumerate misconfigurations, SUID binaries, credentials, and kernel exploits on Linux systems

macOS Privilege Escalation

- **LinPEAS (macOS)** – Identify privilege escalation paths on macOS hosts

Windows Privilege Escalation

- **PinkPanther** – Windows x64 kernel-mode token stealing shellcode

System Hardening

- Remove unnecessary SUID/SGID binaries
- Enforce least privilege and role separation
- Apply timely OS and kernel patches
- Harden sudo and admin group membership

Monitoring & Detection

- **EDR/XDR** – Detect privilege escalation behaviors
- **Audit logging** – Track privilege use and escalation attempts
- **Sysmon / auditd** – Monitor sensitive process and token activity

Configuration & Governance

- **CIS Benchmarks** – Secure baseline configurations
- **Configuration management** – Prevent drift
- **Privileged Access Management (PAM)** – Control and audit admin access

Incident Response

- Identify escalation paths used
- Rotate compromised credentials
- Remove persistence mechanisms
- Validate post-remediation posture

Reverse Engineering

Binary Analysis
- **angr** – Program analysis framework for symbolic execution and binary analysis
- **Detect It Easy (DiE)** – Identify file types, packers, and compilers across platforms

Debuggers
- **edb-debugger** – Cross-platform debugger for AArch32/x86/x64
- **Immunity Debugger** – Exploit development and malware analysis platform
- **OllyDbg** – 32-bit Windows assembler-level debugger
- **pwndbg** – GDB enhancement for exploit development and RE
- **x64dbg** – Open-source x64/x32 Windows debugger

Frameworks & Libraries
- **Capstone** – Disassembly framework supporting multiple architectures

Firmware & Hardware
- **Pinouts** – Hardware connector and chip layout reference

Mobile Reverse Engineering
- **Androguard** – Android app reverse engineering and malware analysis
- **Koodous** – Collaborative Android malware analysis platform
- **Quark** – Android malware analysis and scoring system

Sandboxing
- **Boxxy** – Linkable sandbox analysis explorer

Core RE Tooling
- **Binwalk** – Firmware analysis and extraction
- **Cutter** – Open-source reverse engineering platform (radare2 GUI)
- **Compiler Explorer** – Interactive compiler and assembly analysis
- **Ghidra** – Software reverse engineering framework
- **Hopper** – macOS/Linux disassembler and decompiler
- **IDA Pro** – Advanced commercial binary analysis platform
- **radare2** – CLI-based reverse engineering framework

UEFI / Low-Level
- **UEFITool** – UEFI firmware image viewer and editor

Malware & Threat Analysis
- **Ghidra / IDA Pro** – Decompile and analyze malicious binaries
- **Detect It Easy** – Identify packing and obfuscation techniques
- **Binwalk** – Inspect firmware for embedded malware

Detection Engineering
- Derive **IOCs** and **YARA rules** from reversed samples
- Identify C2 protocols and encryption routines
- Map behavior to **MITRE ATT&CK**

DFIR & Incident Response
- Attribute malware families and variants
- Validate sandbox detections
- Support root-cause analysis and reporting

Secure Development & Validation
- Analyze third-party binaries and firmware
- Identify hardcoded secrets and unsafe logic
- Validate compiler and build artifacts

Training & Enablement
- **Ghidra Class (HackadayU)** – Foundational reverse engineering training

Reconnaissance

Cloud & Buckets
- **Greyhat Warfare** – Search scanned and archived cloud storage
- **OpenBuckets** – Discover public or misconfigured cloud buckets

Content Discovery & Fuzzing
- **DirBuster** – Multi-threaded directory and file brute-forcing
- **dirsearch** – Web path scanner
- **Feroxbuster** – Fast recursive content discovery (Rust)
- **ffuf** – High-speed web fuzzer
- **GoBuster** – Directory, DNS, and VHost busting
- **Hakrawler** – Fast web crawler for endpoint discovery
- **Kiterunner** – Contextual API content discovery
- **LinkFinder** – Extract endpoints from JavaScript
- **ParamSpider** – Parameter mining from web archives
- **xnLinkFinder** – Endpoint discovery from JavaScript
- **x8** – Hidden parameter discovery suite

DNS Enumeration
- **aiodnsbrute** – Asynchronous DNS brute forcing
- **dnsdumpster** – DNS recon and record lookup
- **dnsX** – Multi-purpose DNS toolkit
- **MassDNS** – High-performance bulk DNS resolution
- **SubBrute** – DNS meta-query spider

Domain & IP Enumeration
- **Amass** – In-depth attack surface mapping
- **Assetfinder** – Related domain discovery
- **crt.sh** – Certificate transparency search
- **findomain** – Domain discovery automation
- **httpx** – HTTP probing and service discovery
- **OneForAll** – Integrated subdomain enumeration
- **subfinder** – Passive subdomain discovery
- **sublist3r** – Fast subdomain enumeration

Dorking
- **Dorkbot** – Command-line Google dorking

Recon Frameworks
- **aut0rec0n** – Automated DNS, ports, and subdomain recon
- **FinalRecon** – All-in-one web reconnaissance
- **Osmedeus** – Automated recon and vulnerability scanning framework
- **ReconDog** – Reconnaissance Swiss Army knife
- **sn1per** – Attack surface discovery and prioritization

Search Engines & Archives
- **Censys** – Internet-wide scan data
- **Shodan** – IoT and exposed service search engine
- **Wayback Machine** – Historical web content
- **OnionScan** – TOR network scanner

Wordlists
- **SecLists** – Industry-standard wordlists
- **API Endpoints & Objects** – Common API fuzzing paths
- **Fuzz.txt** – Directory and file fuzzing list

Cloud Exposure Monitoring
- **Greyhat Warfare / OpenBuckets** – Detect accidental public storage

Continuous Monitoring
- **Websitewatcher** – Detect unauthorized website changes
- **sn1per** – Continuous attack surface monitoring

Shells

Generators

- **GoSH** – Golang reverse/bind shell generator
- **RevShells** – Feature-rich reverse shell generator
- **Shellerator** – CLI bind/reverse shell generator (multi-language)

Reverse Shells

- **GoodSpeed** – Manager for handling multiple reverse shells
- **ReverseSSH** – SSH-based reverse shell
- **Simple Reverse Shell** – Minimal shell designed to evade Windows Defender

Webshells

- **Gecko** – Advanced PHP web backdoor
- **JShell** – JavaScript shell via XSS
- **p0wny shell** – Single-file PHP webshell
- **PHP Reverse Shell** – Cross-platform PHP reverse shell
- **Red Team Cookbook Webshells** – Webshell reference collection
- **SharPyShell** – Obfuscated ASP.NET (C#) webshell
- **weevely3** – Weaponized PHP webshell framework

Detection & Monitoring

- **EDR / XDR Platforms** – Detect abnormal process spawning and outbound callbacks
- **WAF** – Block webshell upload and execution attempts
- **IDS/IPS (Snort, Suricata)** – Detect reverse shell traffic patterns

Hardening & Prevention

- **Application Allow-Listing** – Block unauthorized interpreters (cmd, powershell, bash)
- **Egress Filtering** – Restrict outbound traffic to prevent callbacks
- **Least Privilege** – Reduce shell impact if compromised

Threat Hunting

- **YARA Rules** – Detect known webshell signatures
- **File Integrity Monitoring** – Detect unauthorized webshell uploads
- **SIEM Correlation** – Identify suspicious parent/child process chains

Response

- Kill active sessions
- Rotate credentials
- Validate web root and application code integrity

SIEM & Log Management

Log Evasion & Tampering

- **wevtutil** – Clear or query Windows Event Logs
- **auditpol** – Modify Windows audit policy settings
- **Clear-EventLog (PowerShell)** – Clear Windows logs
- **Timestomp** – Manipulate file timestamps to evade timelines

Detection Testing & Simulation

- **Atomic Red Team** – Small, testable attack simulations to validate detections
- **Caldera** – Adversary emulation to test logging and alerting
- **PurpleSharp** – Automated adversary simulation for detection testing

Log Analysis (Attacker View)

- **Splunk (Search Only)** – Identify what defenders can see
- **ELK (Read-only)** – Validate attacker activity visibility
- **Sigma Rules (Offensive Review)** – Identify detection logic to evade

SIEM Platforms

- **Splunk** – Enterprise SIEM, analytics, and correlation
- **Elastic SIEM (ELK)** – Open-source log ingestion and detection
- **Microsoft Sentinel** – Cloud-native SIEM/SOAR
- **QRadar** – Enterprise threat detection and response
- **Graylog** – Centralized log management and analysis

Log Collection & Agents

- **Universal Forwarder (Splunk)** – Endpoint log forwarding
- **Filebeat / Winlogbeat** – Lightweight log shippers
- **Fluentd** – Unified log collection layer
- **NXLog** – Cross-platform log collection

Detection Engineering

- **Sigma** – Vendor-agnostic detection rules
- **MITRE ATT&CK** – Map detections to adversary techniques
- **Detection-as-Code** – Version-controlled detection logic

Correlation & Alerting

- **SOAR Platforms** – Automated triage and response
- **UEBA** – Behavioral anomaly detection
- **Risk-Based Alerting** – Reduce alert fatigue

Retention & Compliance

- **Log Retention Policies** – Meet regulatory requirements
- **Time Sync (NTP)** – Ensure forensic accuracy
- **Immutable Storage** – Protect logs from tampering

Social Engineering

Phishing Analysis & Tracking

- **Phishalytics** – Large-scale phishing data collection and analysis
- **Phishing Tracker** – Track phishing campaigns and takedown progress
- **PhishTank** – Community-driven phishing intelligence repository

Phishing Frameworks

- **espoofer** – Email spoofing and SPF/DKIM/DMARC bypass testing
- **Evilginx** – MITM phishing framework for credential and session theft
- **Fierce Phish** – Full-featured phishing engagement framework
- **GoPhish** – Enterprise phishing toolkit for simulations
- **Judas** – Pluggable phishing proxy
- **King Phisher** – User awareness testing via simulated phishing
- **Lucy** – Social engineering attack simulation platform
- **Modlishka** – Reverse proxy phishing framework (2FA bypass testing)
- **Phishing Frenzy** – Ruby-based phishing framework
- **ShellPhish** – Rapid phishing page replication tool
- **Social Engineering Toolkit (SET)** – Comprehensive social engineering framework
- **SocialFish** – Phishing framework for credential harvesting
- **SpeedPhish** – Fast deployment phishing framework
- **SPT Project** – Phishing education and simulation toolkit

SMS Phishing

- **SMSSpoof** – SMS sender ID spoofing tool

Email & Messaging Protection

- **Secure Email Gateways** – Detect and block phishing attempts
- **DMARC / SPF / DKIM** – Prevent email spoofing
- **SMS Filtering** – Block smishing attempts

Detection & Analysis

- **PhishTank / Abuse Feeds** – Identify known phishing campaigns
- **URL Reputation Services** – Detect malicious links
- **Spamhaus** – Authoritative threat intelligence provider for spam, phishing, botnets, and malicious IP/domain blocklists
- **SIEM Correlation** – Alert on user click behavior

Awareness & Training

- **GoPhish / King Phisher (Defensive Use)** – Run internal phishing simulations
- **Security Awareness Training** – Reduce user susceptibility
- **Just-In-Time Training** – Educate users after failed simulations

Response & Remediation

- Quarantine malicious emails
- Invalidate compromised credentials
- Block malicious domains and IPs

Threat Intel

APT & Campaign Research

- **Cybercrime Campaign Collections** – Curated APT and cybercriminal campaign tracking

Threat Intel Platforms (Adversary View)

- **MISP** – Open-source threat intelligence sharing platform
- **ARTIF** – Real-time threat intelligence framework based on reputation and history
- **ThreatIngestor** – Framework for consuming and normalizing threat feeds
- **ZeroBOX** – Collaborative threat intelligence dashboard

Paste Monitoring

- **Pastebin** – Monitor leaked credentials and data
- **Ghostbin** – Anonymous text sharing and data dumps

Ransomware Infrastructure (Research Only)

⚠️ *Research, tracking, and defensive analysis only*

- **REvil / Sodinokibi** – Ransomware leak site
- **Conti** – Ransomware operations and victim disclosures
- **CL0P** – Extortion-focused ransomware group
- **DarkSide** – Ransomware-as-a-Service infrastructure
- **Babuk / PYSA / Ragnar Locker / Avaddon** – Ransomware victim disclosure portals

TOR Intelligence & Recon

- **Ahmia** – Tor network search engine
- **Hoodle** – Deep web search engine
- **Sentor** – TOR-focused search engine
- **Onioff** – Onion URL inspection and analysis

Threat Intelligence Platforms

- **MISP** – Centralized IOC sharing and correlation
- **OpenCTI** – Threat intelligence lifecycle management
- **ThreatIngestor** – Normalize and feed TI into SIEM/SOAR
- **ZeroBOX** – Collaborative intelligence analysis

IOC & Reputation Feeds

- **Spamhaus** – Authoritative IP/domain blocklists for spam, phishing, botnets
- **Abuse.ch** – Malware, botnet, and ransomware indicators
- **VirusTotal** – File, hash, domain, and IP reputation

Ransomware Intelligence

- Monitor **leak sites** for early breach indicators
- Track **ransomware TTP evolution**
- Feed indicators into **EDR, SIEM, firewall, DNS filtering**

Detection & Response Integration

- **SIEM** – Correlate IOCs with logs
- **SOAR** – Automate blocking and response
- **YARA / Sigma** – Turn intelligence into detections

Governance & Use

- Validate sources
- Time-bound IOCs
- Prevent over-blocking and alert fatigue

Video Education Resources

Conferences & Talks

- **DEF CON (YouTube)** – Cutting-edge offensive research, tools, and techniques
- **BSides San Francisco (YouTube)** – Practical red team, AppSec, and exploit talks
- **Wild West Hackin' Fest (YouTube)** – Hands-on red team and adversary tradecraft

Documentaries & Deep Dives

- **The Hacker Wars** – Hacktivism, Anonymous, and modern cyber conflict
- **Earth's Most Wanted Hacker** – High-profile hacker case studies
- **Sammy Kamkar Takes Down Myspace** – Real-world exploitation story
- **How I Hacked the US Government at 16** – Early offensive learning path
- **ILOVEYOU / WannaCry Documentaries** – Malware evolution and impact
- **Hacker Breaks Down Hacking Scenes** – Realism vs fiction (Wired)

Livestreams

- **HackListX** – Curated hacking livestreams
- **InfoSec Streamers** – Active red team and CTF-focused streamers

Conferences & Defense Content

- **DEF CON Blue Team Villages** – Detection, IR, and defense strategies
- **BSides (Blue Talks)** – SOC operations, GRC, and DFIR insights

Documentaries & Awareness

- **Inside Russia's Hacker Underworld** – Threat actor ecosystems
- **Russia's Cyberwarfare in Ukraine** – Nation-state cyber operations
- **The Dark Side of the Web** – Criminal marketplaces and infrastructure
- **Cybersecurity Expert Answers Hacking Questions** – Public misconceptions explained
- **Hackers Find Missing People** – OSINT used for good

Training & Perspective

- **Wired / Bloomberg / Motherboard Cyber Series** – Threat analysis and response context

Vulnerability Scanners

Web & Application Scanning

- **Burp Suite** – Automated and manual web vulnerability discovery
- **ZAP (OWASP ZAP)** – Open-source web application scanner
- **Acunetix** – Automated web application security testing
- **WPScan** – WordPress vulnerability scanner

Network & Service Scanning

- **Nessus** – Comprehensive vulnerability discovery engine
- **Nexpose** – On-prem vulnerability scanner with risk scoring
- **OpenVAS** – Open-source full-featured vulnerability scanner

Fast & Targeted Scanning

- **nuclei** – Template-based, high-speed vulnerability scanner
- **Silver** – Mass scanning for vulnerable services
- **Striker** – Reconnaissance and vulnerability scanning suite

Enterprise Vulnerability Management

- **Nessus** – Continuous vulnerability assessment and prioritization
- **OpenVAS** – Open-source vulnerability management
- **ManageEngine** – Centralized vulnerability visibility and remediation tracking
- **AT&T Managed Vulnerability Program** – Outsourced vulnerability management

Cloud-Native Scanning

- **Amazon Inspector** – AWS workload vulnerability and compliance scanning
- **Alibaba Cloud Security Scanner** – ML-driven cloud security assessment

Application Security

- **Burp Suite / ZAP (Defensive Use)** – Secure SDLC testing and validation
- **Acunetix** – Continuous web application scanning

Automation & Coverage

- **nuclei** – Detection-as-code vulnerability templates
- **WPScan** – Monitor CMS exposure

Risk Management

- Integrate findings into **GRC**, **patch management**, and **SIEM**
- Prioritize by **exploitability and asset criticality**

Web Application

CORS
- **Corsy** – Automated scanner for CORS misconfigurations

Cross-Site Scripting (XSS)
- **XSS'OR** – JavaScript-based XSS exploitation toolkit
- **XSStrike** – Advanced XSS detection and exploitation framework

CRLF Injection
- **CRLFSuite** – HTTP response splitting and CRLF injection scanner

Cross-Site Request Forgery (CSRF)
- **Bolt** – Automated CSRF vulnerability scanner

Injection (SQL / Command / Template)
- **sqlmap** – Automated SQL injection and database takeover tool
- **Commix** – OS command injection detection and exploitation
- **tplmap** – Server-side template injection scanner and exploit tool

Directory Traversal / File Inclusion
- **dotdotpwn** – Directory traversal fuzzing tool
- **slipit** – ZipSlip archive exploitation utility
- **LFISuite** – Automated Local File Inclusion scanner
- **LFIFreak** – PHP LFI exploitation tool
- **Liffy** – PHP Local File Inclusion automation

HTTP & Protocol Abuse
- **TIDoS** – HTTP request smuggling detection tool
- **http-request-smuggling** – Request smuggling detection framework

Headers & TLS
- **Security Headers** – Analyze missing or misconfigured security headers
- **TLS-Scanner** – TLS server configuration assessment tool

Secure Configuration & Hardening
- **Security Headers** – Enforce CSP, HSTS, X-Frame-Options, and more
- **TLS-Scanner** – Validate strong TLS and cipher configurations

Validation & Testing
- **Burp Suite / ZAP (Defensive Use)** – Secure SDLC testing
- **Corsy** – Validate safe CORS policies
- **TIDoS / HTTP Smuggling Tools** – Ensure reverse proxy safety

Application Protection
- **WAFs** – Block XSS, SQLi, LFI, and command injection
- **Input Validation & Output Encoding** – Prevent injection classes
- **CSRF Tokens** – Mitigate cross-site request forgery

Detection & Monitoring
- **SIEM** – Correlate web application logs
- **EDR / RASP** – Detect runtime exploitation attempts

Remediation
- Patch vulnerable components
- Remove dangerous file handlers
- Validate authentication and authorization flows

Windows

Active Directory

- **Aced** – Parse and resolve targeted AD object DACLs
- **BadBlood** – Populate AD with realistic objects for testing
- **BloodHound** – Graph-based AD attack path analysis
- **Certify** – Active Directory Certificate Services abuse
- **CrackMapExec** – Swiss army knife for Windows/AD environments
- **SCCMHunter** – Identify and attack SCCM assets in AD
- **WinPwn** – Automated internal Windows/AD pentesting

Credentials & Secrets

- **LaZagne** – Credential recovery tool
- **Redsnarf** – OpSec-safe credential and hash extraction
- **SCOMDecrypt** – Decrypt stored SCOM RunAs credentials

Kerberos

- **Kerberoast** – Kerberos service ticket attacks
- **Rubeus** – Raw Kerberos interaction and abuse
- **Pykek** – Kerberos data manipulation library

Post-Exploitation

- **Mimikatz** – Windows credential extraction
- **CredNinja** – SMB credential validation at scale

PowerShell

- **iBombshell** – On-demand post-exploitation PowerShell shell
- **Pentestly** – Python/PowerShell pentesting framework
- **PowerShell Suite** – Collection of offensive PowerShell utilities
- **Stracciatella** – OpSec-safe PowerShell runspace with AMSI bypass

Exchange

- **MailSniper** – Search Exchange mailboxes
- **Ruler** – Abuse Exchange services

Memory & Kernel

- **Blackbone** – Manual DLL mapping
- **PPLdump** – Dump Protected Process Light memory
- **Fibratus** – Windows kernel exploration and tracing
- **Vergilius** – Undocumented Windows kernel structure reference

RDP & RPC

- **PowerRemoteDesktop** – PowerShell-based RDP
- **SharpRDP** – Authenticated RDP command execution
- **rpcenum** – RPC-based domain enumeration

Living Off the Land

- **LOLBAS** – Abuse native Windows binaries
- **Macshift** – MAC address manipulation
- **Windows-Pentest** – Windows attack automation scripts

Identity & AD Defense

- **BloodHound (Defensive Use)** – Identify and remediate attack paths
- **Tiered Admin Model** – Protect privileged accounts
- **Credential Guard / LSA Protection** – Prevent credential dumping

Hardening & Prevention

- **Disable NTLM Where Possible** – Reduce credential relay attacks
- **Harden ADCS** – Prevent certificate abuse
- **Least Privilege** – Reduce blast radius

Baselines & Governance

- **CIS Benchmarks / STIGs** – Secure Windows configurations
- **Audit Policies** – Ensure authentication and object access logging

Wireless

Wi-Fi

- **Aircrack-NG** – Full Wi-Fi security auditing suite
- **Kismet** – Wireless sniffer, WIDS, and recon framework
- **Wifite2** – Automated wireless attack framework
- **Wifiphisher** – Rogue AP and credential harvesting framework
- **MDK4** – Exploit IEEE 802.11 protocol weaknesses
- **PixieWPS** – Offline WPS brute-force attacks
- **Reaver** – WPS brute-force tool
- **bettercap** – MITM attacks for Wi-Fi, Bluetooth, HID, Ethernet

Bluetooth / BLE

- **BtleJuice** – BLE man-in-the-middle framework
- **BLESuite** – BLE device testing toolkit
- **Crackle** – Crack and decrypt BLE encryption
- **Sweyntooth** – BLE stack vulnerability exploitation
- **hcitool** – Bluetooth HCI interaction utility

Cellular

- **Crocodile Hunter** – Detect IMSI catchers and rogue base stations
- **Kalibrate** – GSM base station scanning and calibration

NFC / RFID

- **Proxmark** – RFID/NFC exploitation Swiss-army tool
- **MFOC** – MIFARE Classic offline cracker
- **MFCUK** – MIFARE Classic attack toolkit
- **NFCGate** – Capture and manipulate NFC traffic

Zigbee / Z-Wave

- **KillerBee** – ZigBee security research toolkit
- **KillerZee** – Z-Wave attack and evaluation framework

SDR

- **HackRF One** – Wide-band SDR for RF attacks
- **Ubertooth One** – Bluetooth experimentation platform
- **RTL-SDR / gqrx** – RF signal capture and analysis

Monitoring & Detection

- **Kismet (Defensive Use)** – Wireless IDS and rogue AP detection
- **AirCheck G3 Pro** – Enterprise Wi-Fi site survey and validation
- **Chanalyzer** – Spectrum analysis for interference detection

Hardening & Architecture

- Enforce **WPA3**, disable **WPS**, rotate PSKs
- Segment wireless from core networks
- Apply **802.1X / EAP-TLS** authentication

Bluetooth & IoT Defense

- Disable unused radios and pairing modes
- Patch BLE stacks vulnerable to **Sweyntooth-class flaws**
- Monitor BLE device inventories

Detection & Response

- **SIEM Integration** – Correlate wireless auth failures
- **EDR/XDR** – Detect lateral movement post-wireless access
- **Physical Security** – Control RF-accessible spaces

Validation

- Periodic **rogue AP hunts**
- Red-team-assisted wireless audits