CYBERSECURITY EXAM CHEAT SHEET

1. NETWORKING FUNDAMENTALS

IP Addressing

Type	Range/Format	Example	Notes
IPv4 Private Class A	10.0.0.0/8	10.x.x.x	16M hosts
IPv4 Private Class B	172.16.0.0/12	172.16.x.x - 172.31.x.x	1M hosts
IPv4 Private Class C	192.168.0.0/16	192.168.x.x	65K hosts
Loopback	127.0.0.0/8	127.0.0.1	localhost
APIPA/Link-Local	169.254.0.0/16	169.254.x.x	Auto-assigned
Public IP	Everything else	8.8.8.8	Internet routable

IPv6 Address Types (from your PDF)

Prefix	Type	IPv4 Equivalent	Use
::/128	Unspecified	0.0.0.0	Source before learning own addr
::1/128	Loopback	127.0.0.1	Host talks to itself
::ffff/96	IPv4-Mapped	N/A	Embed IPv4 in IPv6
fc00::/7	ULA (Unique Local)	10.x, 172.16.x, 192.168.x	Private, not routed publicly
fe80::/10	Link-Local	169.254.0.0/16	Single link, not routed
2001:0000::/32	Teredo	N/A	IPv6 tunnel through IPv4 NAT
2001:db8::/32	Documentation	192.0.2.0/24, etc.	Examples only
2002::/16	6to4	N/A	IPv6 over IPv4 gateway
2000::/3	Global Unicast	Public IPs	Internet routable
ff00::/8	Multicast	224.0.0.0/4	Destination only, never source

Common Ports

Port	Service	Port	Service	Port	Service
20/21	FTP	80	HTTP	443	HTTPS
22	SSH	23	Telnet	25	SMTP
53	DNS	67/68	DHCP	110	POP3
143	IMAP	161/162	SNMP	389	LDAP
445	SMB	3306	MySQL	3389	RDP
5432	PostgreSQL	8080	HTTP Alt	1080	SOCKS Proxy

2. ESSENTIAL LINUX COMMANDS

Network Commands

Command	Description
`ip a / ifconfig`	Show all network interfaces and IP addresses
`ip route / route -n`	Show routing table
`hostname -I`	Show host IP addresses

`curl ifconfig.me`	Get PUBLIC IP address
`cat /etc/resolv.conf`	Show DNS servers
`netstat -tuln / ss -tuln`	Show listening ports (-t=TCP, -u=UDP, -l=listening, -n=numeric)
`netstat -antp`	Show all connections with PIDs
`ping -c 4 host`	Send 4 ICMP packets to host
`traceroute host`	Trace route to host
`nslookup domain / dig domain`	DNS lookup
`arp -a`	Show ARP cache
`tcpdump -i eth0`	Capture packets on interface
`tcpdump -i eth0 port 80`	Capture HTTP traffic only
`whois domain.com`	Get domain registration info

System Information Commands

Command	Description
`uname -a`	System info (kernel, hostname, architecture)
`cat /etc/os-release`	Linux distribution info
`whoami`	Current username
`id`	User ID, group ID, groups
`w / who`	Who is logged in
`last`	Login history
`ps aux`	All running processes
`top / htop`	Interactive process viewer
`free -h`	Memory usage (human readable)
`df -h`	Disk space usage
`lsblk`	List block devices
`cat /proc/cpuinfo`	CPU information
`dmesg | tail`	Kernel messages

File & Permission Commands

Command	Description
`ls -la`	List all files with permissions
`chmod 755 file`	rwxr-xr-x (owner:rwx, group:r-x, other:r-x)
`chmod u+x file`	Add execute permission for user
`chown user:group file`	Change ownership
`find / -perm -4000`	Find SUID files (privilege escalation)
`find / -name '*.conf'`	Find config files
`grep -r 'password' /etc`	Search for 'password' recursively
`cat /etc/passwd`	User accounts
`cat /etc/shadow`	Password hashes (root only)
`cat /etc/group`	Groups

Permission Numbers: r=4, w=2, x=1 → 755=rwxr-xr-x, 644=rw-r--r--, 777=rwxrwxrwx

3. SSH - SECURE SHELL

SSH Key Types (Best to Worst)

Algorithm	Recommendation	Notes
Ed25519	★★★ BEST	Most recommended, fast, secure
RSA (3072/4096-bit)	★★ Good	Must be ≥3072 bits; 1024-bit is UNSAFE
ECDSA	★ Acceptable	Depends on random number generation quality
DSA	✗ NEVER USE	Deprecated since OpenSSH 7, UNSAFE

SSH Commands

Generate Ed25519 key:

```
ssh-keygen -o -a 100 -t ed25519 -f ~/.ssh/id_ed25519 -C "email@host.com"
```

SSH Tools:

Tool	Purpose
ssh-keygen	Generate key pair (use once)
ssh-agent bash	Start agent for key forwarding
ssh-add ~/.ssh/id_ed25519	Add key to agent
ssh-add -l	List added keys
ssh -p PORT user@host	Connect to remote host
ssh -p 22 root@192.168.1.1	Connect as root on port 22

SSH Tunneling

Option	Type	Syntax	Description
-L	Local Forward	ssh -L local:dest:remote user@server	Forward local port to remote
-R	Remote Forward	ssh -R remote:dest:local user@server	Forward remote port to local
-D	SOCKS Proxy	ssh -D 1080 user@server	Create SOCKS proxy on local:1080
-J	ProxyJump	ssh -J jump@bastion user@target	Jump through bastion host
-N	No command	ssh -N -L ...	Don't execute remote command
-f	Background	ssh -f -D ...	Run SSH in background

Examples:

```
ssh -L 8080:10.0.1.5:80 user@gateway # Access 10.0.1.5:80 via localhost:8080
ssh -D 9050 -q -C -N -f user@proxy # SOCKS5 proxy on localhost:9050
ssh -J user@bastion1,user@bastion2 user@target # Multi-hop
```

4. NMAP - NETWORK SCANNER

Command	Description
nmap target	Basic scan (top 1000 ports)
nmap -sn 192.168.1.0/24	Ping sweep (host discovery, no port scan)
nmap -p 22,80,443 target	Scan specific ports
nmap -p- target	Scan ALL 65535 ports
nmap -sV target	Service version detection
nmap -O target	OS detection
nmap -A target	Aggressive: OS + version + scripts + traceroute
nmap -sS target	SYN stealth scan (half-open, root required)
nmap -sT target	TCP connect scan (full handshake)

`nmap -sU target`	UDP scan
`nmap -sC target`	Default scripts
`nmap --script vuln target`	Vulnerability scan scripts
`nmap -oN output.txt target`	Save normal output
`nmap -oX output.xml target`	Save XML output
`nmap -T4 target`	Timing: T0(paranoid)..T5(insane), T4=fast
`nmap -Pn target`	Skip host discovery (treat as up)

Full recon: `nmap -sV -sC -O -p- -T4 -oN scan.txt target`

5. PROXYCHAINS & SOCKS PROXIES

SOCKS Proxy Types

- **SOCKS4**: TCP only, no authentication, no UDP, no IPv6
- **SOCKS5**: TCP+UDP, authentication support, IPv6, DNS resolution

Proxychains Configuration (/etc/proxychains.conf)

```
# Chain types (uncomment one):
# dynamic_chain - skip dead proxies
# strict_chain - all proxies must work in order
# random_chain - random proxy order

# Proxy list at end of file:
[ProxyList]
socks5 127.0.0.1 9050 # Tor
socks5 127.0.0.1 1080 # SSH tunnel
```

Usage: `proxychains nmap -sT -Pn target`

Setup SSH SOCKS: `ssh -D 1080 -N -f user@proxy-server`

6. RECONNAISSANCE & INFORMATION GATHERING

Passive Recon (OSINT)

Tool/Technique	Purpose
`whois domain.com`	Domain registration info, owner, registrar
`dig domain.com ANY`	All DNS records
`nslookup -type=mx domain.com`	Mail server records
`host -t ns domain.com`	Name server records
`theHarvester`	Email, subdomains, names from public sources
`Shodan.io`	Search internet-connected devices
`Censys.io`	Certificate & host search
`Google Dorks`	site:, filetype:, intitle:, inurl:
`OSINT Framework`	Collection of OSINT tools

Active Recon

Tool/Technique	Purpose
`nmap (see section 4)`	Port scanning, service detection
`nikto -h target`	Web vulnerability scanner
`dirb http://target`	Directory/file bruteforcing
`gobuster dir -u URL -w wordlist`	Fast directory bruteforce
`enum4linux target`	SMB/Windows enumeration
`snmpwalk -v2c -c public target`	SNMP enumeration
`nbtscan 192.168.1.0/24`	NetBIOS scanner

7. NETWORK SNIFFING

Tool	Command/Usage
`tcpdump`	`tcpdump -i eth0 -w capture.pcap`
`tcpdump filter`	`tcpdump -i eth0 'port 80 and host 192.168.1.1'`
`Wireshark`	`GUI packet analyzer, open .pcap files`
`tshark`	`tshark -i eth0 -f 'tcp port 443'`
`ettercap`	`Man-in-the-middle, ARP spoofing`
`arpspoof`	`arpspoof -i eth0 -t victim gateway`
`bettercap`	`Modern MITM framework`

Wireshark Filters: ip.addr==192.168.1.1 \| tcp.port==80 \| http \| dns \| tcp.flags.syn==1

8. VULNERABILITY FRAMEWORKS & STANDARDS

Acronym	Full Name	Description
CVE	Common Vulnerabilities & Exposures	Unique ID for known vulnerabilities (CVE-YYYY-NNNNN)
CWE	Common Weakness Enumeration	Catalog of software/hardware weakness types
CVSS	Common Vulnerability Scoring System	Severity score 0-10 (Low/Med/High/Critical)
CAPEC	Common Attack Pattern Enum.	Attack pattern classification
MITRE ATT&CK	Adversarial Tactics & Techniques	Knowledge base of adversary tactics/techniques
NVD	National Vulnerability Database	US govt CVE database with CVSS scores

CVSS Severity Scale

Score	0.0	0.1-3.9	4.0-6.9	7.0-8.9	9.0-10.0
Severity	None	Low	Medium	High	Critical

9. TRAFFIC LIGHT PROTOCOL (TLP v2.0)

Label	Sharing	Description
TLP:RED	NO sharing	Individual recipients only, highest sensitivity
TLP:AMBER	Organization + clients	Need-to-know basis within org (AMBER+STRICT = org only)
TLP:GREEN	Community only	Share with peers/partners, NOT public
TLP:CLEAR	Unlimited	Public release, no restrictions

10. CYBER KILL CHAIN & THREAT INTELLIGENCE

Lockheed Martin Cyber Kill Chain

Phase	Description	Example TTPs
1. Reconnaissance	Research, identify targets	OSINT, scanning, social engineering
2. Weaponization	Create deliverable payload	Exploit + backdoor, malicious doc
3. Delivery	Transmit weapon to target	Email, USB, web, exploit public apps
4. Exploitation	Trigger vulnerability	Buffer overflow, code execution
5. Installation	Install backdoor/RAT	Malware, webshell, scheduled tasks
6. Command & Control	Establish C2 channel	HTTP/HTTPS, DNS, custom protocols
7. Actions on Objectives	Achieve goals	Exfiltration, destruction, ransomware

Threat Intelligence Terms

Term	Definition
TTP	Tactics, Techniques, Procedures - adversary behavior patterns
IOC	Indicator of Compromise - artifacts (IPs, hashes, domains)
APT	Advanced Persistent Threat - sophisticated threat actor
ISAC	Information Sharing & Analysis Center
CTI	Cyber Threat Intelligence
MITRE ATT&CK	Framework mapping adversary TTPs
OSINT	Open Source Intelligence

11. NETWORK DEVICES & ARCHITECTURE

Device	OSI Layer	Function
Hub	Layer 1 (Physical)	Broadcasts to all ports, no intelligence
Switch	Layer 2 (Data Link)	Forwards based on MAC address, creates VLANs
Router	Layer 3 (Network)	Forwards based on IP, connects networks
Firewall	Layer 3-7	Filters traffic, stateful inspection, rules
Load Balancer	Layer 4-7	Distributes traffic across servers
Proxy	Layer 7 (Application)	Intermediary for requests, caching, filtering
IDS/IPS	Layer 3-7	Intrusion Detection/Prevention System
AS	Autonomous System	Network under single admin control (BGP)

12. DNS - DOMAIN NAME SYSTEM

Record	Purpose	Example
`A`	IPv4 address	example.com → 93.184.216.34
`AAAA`	IPv6 address	example.com → 2606:2800:...
`CNAME`	Alias/Canonical name	www → example.com
`MX`	Mail server	mail.example.com (priority 10)
`NS`	Name server	ns1.example.com
`TXT`	Text record	SPF, DKIM, verification
`PTR`	Reverse lookup	IP → hostname

SOA	Start of Authority	Primary NS, admin email, serial

Commands: `dig domain.com ANY | nslookup -type=mx domain.com | host -t ns domain.com`

13. QUICK COMMAND REFERENCE

Task	Command
My private IP	`ip a | hostname -I | ifconfig`
My public IP	`curl ifconfig.me | curl icanhazip.com`
Default gateway	`ip route | route -n | netstat -rn`
DNS servers	`cat /etc/resolv.conf`
Open ports (local)	`ss -tuln | netstat -tuln`
Scan network	`nmap -sn 192.168.1.0/24`
Scan all ports	`nmap -p- target`
Service versions	`nmap -sV target`
Create SOCKS proxy	`ssh -D 1080 -N user@host`
Use proxy	`proxychains nmap -sT target`
Capture traffic	`tcpdump -i eth0 -w out.pcap`
ARP table	`arp -a | ip neigh`
Routing table	`ip route | route -n`
Current user	`whoami | id`
Find SUID files	`find / -perm -4000 2>/dev/null`