Cyber Security

Short notes for beginners · B.Tech CSE · BCA · Security+ · SOC analyst

Uncodemy Handwritten Notes · free for students

1. Cyber Security Basics

- **Cyber security** = protecting computers, networks, applications and data from attack, damage and unauthorised access. Goal: keep systems safe and working.
- **CIA triad**: Confidentiality (secret data stays secret), Integrity (data stays correct), Availability (service is up when needed). **AAA**: Authentication (who are you), Authorisation (what can you do), Accounting (what did you do).

Term	Meaning
Asset	Anything valuable: data, server, people, reputation
Threat	Something that can cause harm (hacker, malware, flood)
Vulnerability	A weakness (unpatched software, weak password)
Exploit	Method or code that uses a vulnerability
Risk	Chance of loss = likelihood x impact
Zero-day	Vulnerability with no patch available yet
Attack surface	All the points where an attacker can try to enter

- Domains: network security, application security, endpoint security, cloud security, information (data) security, identity and access management, IoT and OT security, security operations.
- Security controls: **preventive** (firewall, locks), **detective** (IDS, CCTV, logs), **corrective** (backup restore, patch). Also administrative (policy, training), technical and physical.

2. Cyber Threats and Malware

Threat	Description
Virus	Attaches to a file and spreads when it is run
Worm	Spreads by itself through the network
Trojan	Looks like a useful program, hides harmful code
Ransomware	Encrypts data and demands payment
Spyware / Keylogger	Secretly collects information or keystrokes
Rootkit	Hides deep in the OS to keep control
Botnet	Network of infected devices controlled remotely
Adware	Shows unwanted ads, may track users

- **Phishing**: fake emails or sites steal passwords and money (also vishing = voice call, smishing = SMS, spear phishing = targeted). **Social engineering** tricks people, and it is the most common way in.
- **DoS**: one source floods a service. **DDoS**: many sources (botnet) flood it. **MITM**: attacker sits between two parties. **SQL injection / XSS**: bad input attacks web apps. **Password attacks**: brute force, dictionary, credential stuffing.
- **APT** (Advanced Persistent Threat): skilled, long term, targeted attack, often by groups backed by a country. **Insider threat**: employee or partner who misuses access, by mistake or on purpose.

REMEMBER Over 90% of incidents start with human error or phishing. Tools help, but trained people are the strongest defence.

3. Networking Fundamentals

Layer	OSI name	Examples	Unit / device
7	Application	HTTP, FTP, SMTP, DNS	Data
6	Presentation	SSL/TLS, JPEG, encryption	Data
5	Session	NetBIOS, RPC, sessions	Data

Layer	OSI name	Examples	Unit / device
4	Transport	TCP, UDP, ports	Segment
3	Network	IP, ICMP, routing	Packet / router
2	Data link	Ethernet, ARP, MAC	Frame / switch
1	Physical	Cables, Wi-Fi signals	Bits / hub

- TCP/IP model has 4 layers: Application, Transport, Internet, Network Access. **TCP** is reliable and connection based (handshake SYN, SYN/ACK, ACK). **UDP** is fast and connectionless (video, DNS, gaming).
- **IP address** identifies a device on a network (IPv4 is 32 bit, IPv6 is 128 bit). **MAC address** is the hardware address (48 bit). **DNS** turns names into IPs. **DHCP** gives IPs automatically. **NAT** lets many private devices share one public IP.
- Private IPv4 ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Common secure ports: 22 SSH, 443 HTTPS, 993 IMAPS. Insecure: 23 Telnet, 21 FTP, 80 HTTP.

4. Network Security Devices

- **Firewall** filters traffic by rules. Types: packet filter (IP, port), stateful (tracks connections), proxy / application firewall, and **NGFW** (next generation, with deep inspection and user awareness).

Device / term	Purpose
IDS	Detects attacks and raises alerts (passive)
IPS	Detects and blocks attacks (inline)
WAF	Protects web applications from SQLi, XSS
VPN	Encrypted tunnel over the internet (IPsec, SSL VPN)
DMZ	Separate zone for public servers, away from the internal LAN
Proxy	Middle server that filters and caches web requests
Honeypot	Decoy system to study attackers
SIEM	Collects and correlates logs from everywhere

- **Segmentation** and VLANs limit how far an attacker can move. **Zero Trust** = never trust, always verify every user and device, give only the access that is needed.

- Wi-Fi: use WPA3 (or WPA2 with a strong passphrase), turn off WPS, change default admin passwords, use a guest network. WEP is broken and must not be used.

5. Cryptography

- **Encryption** converts plain text to cipher text with a key. **Symmetric**: one shared key, fast (AES). **Asymmetric**: public + private key pair (RSA, ECC), used for key exchange and signatures. **Hashing**: one-way fixed size fingerprint (SHA-256).

Algorithm	Type	Note
AES	Symmetric	128 / 192 / 256 bit keys, current standard
DES / 3DES	Symmetric	DES 56 bit is broken, 3DES is retired
RSA	Asymmetric	2048 bit or more
ECC	Asymmetric	Smaller keys than RSA for same strength
SHA-256	Hash	256 bit output, secure
MD5 / SHA-1	Hash	Collisions found, avoid

EXAMPLE A 128 bit AES key has 2^128 ≈ 3.4 x 10^38 possible keys. Even testing 10^12 keys per second would take about 10^19 years, so brute force is not practical.

- **Digital signature**: hash of the message signed with the sender's private key, proves identity and integrity. **PKI**: certificate authority (CA) issues digital certificates (X.509) that bind a public key to an identity. **TLS** uses these for HTTPS.
- Passwords must be stored as salted hashes (bcrypt, scrypt, Argon2), never as plain text. **Steganography** hides data inside images or audio.

6. Identity and Access Management

- **MFA** uses two or more factors: something you know (password, PIN), something you have (phone, token, security key), something you are (fingerprint, face). MFA stops most stolen password attacks.

- **Least privilege**: give only the minimum access needed. **RBAC**: access by role. **Separation of duties**: no single person controls a full critical process. **PAM**: tight control of admin accounts.
- **SSO** = one login for many apps. **OAuth 2.0** = delegated access, **OpenID Connect** = login on top of OAuth, **SAML** = enterprise SSO, **Kerberos** = ticket based authentication in Windows domains, **LDAP** = directory lookup.
- Good password practice: long passphrases (14+ characters), unique per site, use a password manager, never share via chat, check leaks (Have I Been Pwned). Biometrics cannot be changed, so protect them well.

7. Endpoint, Application and Cloud Security

- **Endpoint security**: antivirus, **EDR** (endpoint detection and response), disk encryption (BitLocker), automatic patches, USB control, and Mobile Device Management for phones.
- **Secure SDLC**: security from design to release: threat modelling, secure coding, code review, SAST / DAST testing, dependency scanning. See OWASP Top 10 for common web flaws.
- **Cloud security**: shared responsibility. The provider secures the cloud (data centres, hardware); the customer secures what is in the cloud (data, identities, configuration). Biggest risk: misconfiguration such as public storage buckets.
- **Patch management**: keep OS and apps updated. Backups follow the 3-2-1 rule: 3 copies, on 2 different media, 1 stored offsite or offline (protects from ransomware).
- Email security: SPF, DKIM and DMARC fight spoofing. Mobile: install apps from trusted stores only, use screen lock, keep OS updated.

8. SOC and Incident Response

- **SOC** (Security Operations Centre) monitors, detects and responds 24 x 7. Tiers: L1 triage alerts, L2 investigate, L3 hunt threats and handle complex cases. Core tool: **SIEM** (Splunk, QRadar, Sentinel, Wazuh).

IR phase (NIST)	What happens
Preparation	Plan, team, tools, training, backups
Detection and analysis	Spot and confirm the incident, find scope
Containment, eradication, recovery	Isolate, remove cause, restore systems
Post-incident activity	Lessons learned, report, improve

- **IoC** (indicator of compromise): bad IP, hash, domain. **Threat intelligence** shares known IoCs and attacker methods. **Digital forensics**: collect evidence in order of volatility (RAM first, then disk), keep chain of custody, use write blockers.
- **Vulnerability management**: scan → prioritise (CVSS score and business impact) → patch → verify. **Penetration test** = authorised simulated attack to find gaps.

9. Governance, Risk, Laws and Careers

- **Risk management**: identify assets and threats → assess likelihood and impact → treat by mitigate, transfer (insurance), avoid or accept → monitor.

EXAMPLE Asset value Rs 1,00,000, exposure factor 50% → SLE = 50,000. If it happens once in 5 years, ARO = 0.2. ALE = SLE x ARO = 50,000 x 0.2 = Rs 10,000 per year. A control costing less than this is worth it.

Standard / law	About
ISO/IEC 27001	International standard for an information security management system
NIST CSF	Identify, Protect, Detect, Respond, Recover (v2.0 adds Govern)
PCI DSS	Security rules for card payment data
GDPR	EU data protection law
IT Act 2000, DPDP Act 2023	India: cyber offences and personal data protection

- India: report cyber fraud on the National Cyber Crime portal (cybercrime.gov.in) or call helpline 1930 quickly, because early reporting helps freeze money. CERT-In handles incidents.
- Careers: SOC analyst, security engineer, pen tester, GRC analyst, cloud security engineer. Certifications: CompTIA Security+, CEH, CISSP, CISM, CCNA Security, AZ-500.

10. Most Asked Questions (practice)

1. Explain the CIA triad and AAA with examples.
2. Differentiate virus, worm, trojan and ransomware.
3. What is phishing? How can users and companies stop it?
4. Explain OSI layers with protocols and devices.
5. Firewall vs IDS vs IPS. What is a DMZ?
6. Symmetric vs asymmetric encryption. What is a digital signature?
7. What is MFA? Explain least privilege and RBAC.
8. Explain the incident response lifecycle.
9. What is risk? Calculate ALE with an example.
10. What is Zero Trust? Explain the shared responsibility model.

TIP Interviews: learn networking and Linux well, practise on TryHackMe SOC paths, and be ready to explain one real attack (like phishing or ransomware) step by step with the defence.