

VU LEARNING HUB

vulearninghub.xyz

HANDOUT

CS315

Network Security

CS315 by VU Learning HUB

Prepared for VU students • Free study resources

<https://vulearninghub.xyz>

CS315 - Network Security

A structured study handout compiled from the course's lecture topics. Read each topic's objectives first, study the key concepts, then use the summary and exam tips for revision.

CS315

Network Security

Based on 45 lecture topics

Compiled for VU students as a structured study guide

*Concepts are summarized in the writer's own words;
use alongside your lecture videos for best results.*

Contents

Unit 1: Security Fundamentals	3
Topic 1: What Is Network Security	3
Topic 2: Threats, Attacks, and Adversaries	4
Topic 3: Security Policies and Risk Management	5
Topic 4: Access Control Models	5
Topic 5: Security Ethics and Law	6
Unit 2: Cryptography Foundations	7
Topic 6: Classical Ciphers	7
Topic 7: Symmetric Encryption: DES and AES	8
Topic 8: Public-Key Cryptography: RSA	8
Topic 9: Hashes and Message Integrity	9
Topic 10: Digital Signatures and PKI	10
Unit 3: Network Defense Technologies	11
Topic 11: Firewalls	11
Topic 12: Intrusion Detection and Prevention	12
Topic 13: VPNs and Secure Tunneling	12
Topic 14: Wireless Network Security	13
Topic 15: Network Segmentation and Zero Trust	14
Unit 4: Common Attacks and Defenses	15
Topic 16: Malware: Viruses, Worms, Trojans, Ransomware	15
Topic 17: Denial of Service Attacks	16
Topic 18: Phishing and Social Engineering	16
Topic 19: Man-in-the-Middle and Spoofing	17
Topic 20: Password Attacks and Authentication Bypasses	18
Unit 5: Application and Data Security	19
Topic 21: Web Application Security: OWASP Top 10	19
Topic 22: Email Security	19
Topic 23: Database and Data Protection	20
Topic 24: Secure Software Development	21
Topic 25: Incident Response and Digital Forensics	22
Glossary of Key Terms	22

Course Introduction

Network Security studies how to protect computer networks and the data flowing through them from attacks, theft, and disruption. As businesses, governments, and daily life move online, network security has become one of computing's most critical fields.

The course begins with security fundamentals: the CIA triad (confidentiality, integrity, availability), threats, vulnerabilities, and risk. Students then learn cryptography - the mathematical foundation of security - including symmetric and asymmetric encryption, hashes, and digital signatures.

Later units cover network defense in depth: firewalls, intrusion detection, VPNs, and wireless security; common attacks (DoS, phishing, malware, man-in-the-middle) and how they work; web and email security; and security management including policies, incident response, and ethical/legal issues. The goal is a security mindset: thinking like both defender and attacker.

How to use this handout: Each topic lists its learning objectives, explains the key concepts in simple words, defines important terms, gives an example where helpful, and closes with a summary plus exam tips. Topics marked **Very important** deserve extra revision.

Unit 1: Security Fundamentals

Topic 1: What Is Network Security

Learning Objectives

- Define network security
- Explain the CIA triad
- Describe the threat landscape

Key Concepts

Network security protects the usability, reliability, integrity, and safety of networks and data. It spans hardware, software, policies, and people - technology alone never suffices.

The CIA triad defines security goals: Confidentiality (only authorized access - encryption, access control), Integrity (data unaltered - hashes, signatures), Availability (systems reachable when needed - redundancy, DoS defense). Later additions: Authentication (proving identity), Non-repudiation (cannot deny actions), and Accountability.

The threat landscape includes cybercriminals (profit), nation-states (espionage), hackers (ideology), and insiders (malice or mistakes). Attack costs run to trillions globally; Pakistan's growing digital economy faces phishing, ransomware, and banking fraud daily.

Key Points

- Network security protects networks, data, and services across tech, policy, and people.
- CIA triad: Confidentiality, Integrity, Availability - plus authentication and non-repudiation.
- Threat actors: criminals, states, hackers, insiders.

Key Terms

CIA triad: Confidentiality, Integrity, Availability: core security goals.

Threat: A potential cause of harm, e.g. a hacker.

Vulnerability: A weakness a threat can exploit.

Risk: Threat exploiting vulnerability causing impact.

Example

- *Ransomware encrypting a hospital's records attacks availability and confidentiality.*

Summary: Security pursues CIA goals against diverse threats exploiting vulnerabilities.

Exam Tips

- ★ Very important: the CIA triad with one mechanism each.
- ★ Remember threat vs. vulnerability vs. risk.

Topic 2: Threats, Attacks, and Adversaries

Learning Objectives

- Classify security threats
- Describe attack categories
- Explain the cyber kill chain

Key Concepts

Threats split into: interception (eavesdropping), interruption (DoS), modification (tampering), and fabrication (forgery) - mapping to CIA violations. Attacks may be passive (monitoring, traffic analysis - hard to detect) or active (modification, DoS - easier to detect).

The cyber kill chain models attack stages: reconnaissance (researching targets), weaponization (crafting malware), delivery (phishing email), exploitation (running code), installation (persistence), command-and-control (remote control), and actions on objectives (data theft). Defenders can break the chain at any stage.

Understanding adversary thinking - what they want, what they can do - focuses defenses on realistic scenarios rather than movie plots.

Key Points

- Threat types: interception, interruption, modification, fabrication.
- Passive (monitoring) vs. active (altering/disrupting) attacks.
- Kill chain: recon to actions on objectives; break any link.

Key Terms

Kill chain: The staged model of a cyber attack.

Passive attack: Monitoring without altering systems.

Active attack: Modifying or disrupting systems.

Example

- *Phishing email (delivery) -> malicious attachment (exploitation) -> ransomware (actions).*

Summary: Classifying threats and modeling attack stages focuses defense where it counts.

Exam Tips

- ★ Key point: the four threat types mapped to CIA.
- ★ Remember kill chain stages.

Topic 3: Security Policies and Risk Management

Learning Objectives

- Explain security policy purposes
- Describe risk assessment
- Outline defense in depth

Key Concepts

A security policy states what is protected, from whom, and the rules everyone follows - acceptable use, password requirements, data classification, incident reporting. Without policy, technology is directionless.

Risk management: identify assets, enumerate threats and vulnerabilities, estimate likelihood and impact, then treat risks - avoid, mitigate (controls), transfer (insurance), or accept. Quantitative ($ALE = SLE \times ARO$) and qualitative (high/medium/low matrices) approaches both work.

Defense in depth layers controls: if one fails, others hold - firewalls, IDS, encryption, access control, training, backups. No single control is enough; security is a process of layered, updated defenses.

Key Points

- Policy directs technology; risk management prioritizes spending.
- Risk treatment: avoid, mitigate, transfer, accept.
- Defense in depth: layered controls so no single failure is fatal.

Key Terms

Security policy: Rules governing protection of assets.

Risk assessment: Identifying and evaluating security risks.

Defense in depth: Layered security controls.

Example

- *A bank layers firewalls, encryption, fraud monitoring, and staff training.*

Summary: Policy, risk analysis, and layered defenses organize security effort.

Exam Tips

- ★ Very important: defense in depth concept.
- ★ Remember the four risk treatments.

Topic 4: Access Control Models

Learning Objectives

- Explain authentication, authorization, accounting
- Compare DAC, MAC, RBAC
- Discuss password security

Key Concepts

Access control answers: who are you (authentication), what may you do (authorization), and what did you do (accounting/audit). Authentication factors: something you know (password), have (token/phone), are (biometrics) - multi-factor combines them.

Models: Discretionary (DAC - owners grant access, e.g. file sharing), Mandatory (MAC - system labels enforce policy, e.g. military classifications), Role-Based (RBAC - permissions attach to job roles, e.g. 'accountant'). RBAC dominates enterprises as roles match organizations.

Password realities: humans pick weak, reused passwords - hence password managers, MFA everywhere important, and biometrics for convenience. Account lockout and breach monitoring add layers.

Key Points

- AAA: authentication, authorization, accounting.
- DAC (owner-granted), MAC (label-enforced), RBAC (role-based).
- MFA defeats password weakness; managers help.

Key Terms

Authentication: Verifying identity.

Authorization: Granting permissions.

MFA: Multi-factor authentication.

RBAC: Role-based access control.

Example

- A university's LMS: students (role) can submit; teachers can grade.

Summary: Access control proves identity, grants least privilege, and logs actions.

Exam Tips

- ★ Key point: DAC vs. MAC vs. RBAC.
- ★ Remember the three authentication factors.

Topic 5: Security Ethics and Law

Learning Objectives

- Discuss hacker ethics
- Outline cybercrime law in Pakistan
- Explain responsible disclosure

Key Concepts

Ethics: white-hat hackers test with permission to improve security; black-hats exploit illegally; grey-hats straddle the line. Professionals follow codes: do no harm, respect privacy, stay within authorized scope - unauthorized 'helpful' hacking is still illegal.

Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 criminalizes unauthorized access, data theft, cyberterrorism, and online harassment, with FIA's Cybercrime Wing investigating. Penalties include imprisonment and fines; the law also covers service providers' obligations.

Responsible disclosure: researchers privately notify vendors, allow fix time, then publish - balancing public safety against vendor accountability. Bug bounty programs formalize this cooperation.

Key Points

- White-hat (authorized) vs. black-hat (criminal) vs. grey-hat.
- PECA 2016: Pakistan's cybercrime law; FIA investigates.

- Responsible disclosure: private notice, fix time, then publish.

Key Terms

PECA 2016: Prevention of Electronic Crimes Act, Pakistan.

White-hat hacker: An authorized security tester.

Responsible disclosure: Coordinated vulnerability reporting.

Example

- A researcher reports a bank's flaw privately: the bank fixes it and pays a bounty.

Summary: Law and ethics channel hacking skill toward defense, not crime.

Exam Tips

- ★ Key point: PECA 2016's scope.
- ★ Remember white vs. black hat.

Unit 2: Cryptography Foundations

Topic 6: Classical Ciphers

Learning Objectives

- Explain substitution and transposition
- Describe Caesar and Vigenere ciphers
- Discuss why classical ciphers fail

Key Concepts

Classical ciphers build intuition. Substitution replaces letters: the Caesar cipher shifts by 3 (A->D); monoalphabetic substitution uses scrambled alphabets - both broken by frequency analysis (E is commonest in English). The Vigenere cipher uses a repeating keyword for polyalphabetic substitution, resisting simple frequency analysis but broken by Kasiski examination.

Transposition rearranges letters (rail fence, columnar) - combined with substitution in products. Steganography hides messages' existence (invisible ink, image LSB) rather than their meaning.

Lesson: security through obscurity fails - Kerckhoffs's principle says security must rest in the key, not the method's secrecy. Modern ciphers assume attackers know the algorithm.

Key Points

- Substitution (Caesar, Vigenere) and transposition are classical techniques.
- Frequency analysis breaks simple substitution.
- Kerckhoffs's principle: security in the key, not secret methods.

Key Terms

Substitution cipher: Replacing plaintext letters with others.

Frequency analysis: Breaking ciphers via letter frequencies.

Kerckhoffs's principle: Security must depend only on key secrecy.

Example

- *ATTACK* shifted by 3 becomes *DWWDFN*.

Summary: Classical ciphers teach principles modern cryptography formalizes.

Exam Tips

- ★ Very important: Kerckhoffs's principle.
- ★ Remember Caesar and frequency analysis.

Topic 7: Symmetric Encryption: DES and AES

Learning Objectives

- Explain symmetric encryption
- Describe DES and AES
- Discuss key management challenges

Key Concepts

Symmetric encryption uses one shared secret key for encryption and decryption - fast and efficient for bulk data. DES (56-bit keys) was the standard until brute force broke it; Triple-DES extended its life. AES (128/192/256-bit keys, Rijndael) is the current standard - secure, fast in hardware, used everywhere from WhatsApp to banking.

Block ciphers encrypt fixed blocks; modes (ECB, CBC, CTR, GCM) handle longer messages - ECB's identical-block weakness is the classic warning (the ECB penguin). Stream ciphers encrypt bit-by-bit for real-time data.

The hard problem: key distribution - how do distant parties share the secret securely? And key management at scale (n users need $n(n-1)/2$ keys). This motivates public-key cryptography.

Key Points

- Symmetric: one shared key; fast; AES-128/256 is the standard.
- DES broken by brute force; ECB mode leaks patterns.
- Key distribution and management are the core challenges.

Key Terms

Symmetric encryption: Same key encrypts and decrypts.

AES: Advanced Encryption Standard.

Block cipher mode: How a block cipher handles long messages.

Example

- *WhatsApp messages are AES-encrypted: the key-exchange problem is solved asymmetrically.*

Summary: Symmetric crypto is fast but needs secure key sharing - solved by asymmetric methods.

Exam Tips

- ★ Very important: AES vs. DES and why DES failed.
- ★ Remember the key-distribution problem.

Topic 8: Public-Key Cryptography: RSA

Learning Objectives

- Explain public-key concepts
- Describe RSA key generation and use

- Discuss RSA security basis

Key Concepts

Public-key cryptography uses key pairs: a public key (shared openly) encrypts, the private key (kept secret) decrypts - solving key distribution. Digital signatures reverse the roles: sign with private, verify with public.

RSA: pick two large primes p, q ; $n = pq$; choose e coprime to $(p-1)(q-1)$; compute d as e 's inverse. Public: (e, n) ; private: (d, n) . Encryption: $c = m^e \bmod n$; decryption: $m = c^d \bmod n$. Security rests on factoring difficulty - factoring 2048-bit n is infeasible.

Uses: key exchange (encrypting session keys), digital signatures, certificates. RSA is slow - so hybrid systems use RSA to exchange keys, AES for data. Key sizes grow as factoring algorithms and computers improve.

Key Points

- Key pairs: public encrypts, private decrypts; enables signatures too.
- RSA security = difficulty of factoring large numbers.
- Hybrid use: RSA exchanges keys, AES encrypts data.

Key Terms

Public-key cryptography: Asymmetric encryption with key pairs.

RSA: The factoring-based public-key algorithm.

Hybrid cryptosystem: Asymmetric key exchange + symmetric bulk encryption.

Example

- A browser uses the bank's public key to send a session key. then AES for the session.

Summary: RSA's trapdoor (easy multiply, hard factor) enables secure communication without shared secrets.

Exam Tips

- ★ Very important: public vs. private key roles.
- ★ Remember factoring as RSA's security basis.

Topic 9: Hashes and Message Integrity

Learning Objectives

- Explain cryptographic hash functions
- Describe SHA family
- Explain HMAC and password hashing

Key Concepts

Hash functions compress any input to a fixed digest (SHA-256: 256 bits) with properties: one-way (cannot invert), collision-resistant (cannot find two inputs with same digest), and avalanche (tiny input change scrambles output). They detect any alteration - integrity's workhorse.

Uses: verifying downloads (compare published hashes), storing passwords (never plaintext!), digital signatures (sign the hash, not the message), and blockchains. MD5 and SHA-1 are broken (collisions found); SHA-256/3 are current.

Password hashing needs slowness: bcrypt, scrypt, Argon2 deliberately cost computation, defeating brute force; salting (random per-password values) defeats rainbow tables. HMAC combines hashes with secret keys for authenticated integrity.

Key Points

- Hashes: one-way, collision-resistant digests for integrity.
- SHA-256 current; MD5/SHA-1 broken.
- Passwords: salted slow hashes (bcrypt/Argon2); HMAC for keyed integrity.

Key Terms

Hash function: One-way compression to a fixed digest.

Collision: Two inputs with the same hash.

Salt: Random per-password value defeating precomputation.

HMAC: Keyed-hash message authentication code.

Example

- *A site stores `bcrypt(salt + password)`: breaches reveal no usable passwords.*

Summary: Hashes guarantee integrity; proper password hashing contains breach damage.

Exam Tips

- ★ Very important: hash properties.
- ★ Remember salting and why MD5 is dead.

Topic 10: Digital Signatures and PKI

Learning Objectives

- Explain digital signatures
- Describe certificates and PKI
- Discuss trust models

Key Concepts

Digital signatures provide authentication, integrity, and non-repudiation: hash the message, encrypt the hash with the sender's private key. Anyone verifies with the public key. RSA and ECDSA (elliptic-curve, smaller keys) are standard.

But whose public key? Certificates bind keys to identities, signed by Certificate Authorities (CAs). PKI (public key infrastructure) is the system of CAs, certificates, and revocation (CRLs, OCSP). Your browser trusts hundreds of pre-installed CA certificates - the padlock's basis.

Weaknesses: CA compromise (DigiNotar), phishing with valid certificates, and revocation failures. Certificate Transparency logs now audit issuance. Trust ultimately rests on the CA system - a known weak link.

Key Points

- Signatures: private-key signs hash; public-key verifies.
- Certificates bind keys to identities via CAs; PKI manages trust.
- Weaknesses: CA compromise, revocation gaps.

Key Terms

Digital signature: Private-key encryption of a message hash.

Certificate Authority: A trusted issuer of identity certificates.

PKI: The infrastructure of certificates and trust.

Non-repudiation: Inability to deny having signed.

Example

- *Software updates are signed: your OS verifies before installing.*

Summary: Signatures prove origin; PKI's CA trust makes keys meaningful.

Exam Tips

- ★ Very important: how signatures provide non-repudiation.
- ★ Remember the CA trust problem.

Unit 3: Network Defense Technologies

Topic 11: Firewalls

Learning Objectives

- Explain firewall purposes
- Compare firewall types
- Describe firewall limitations

Key Concepts

Firewalls enforce access policy at network boundaries: packet filters (inspect headers - fast, dumb), stateful inspection (track connections - the workhorse), and application proxies/NGFW (understand protocols, inspect content - smart, slower).

Rules order matters: first-match policies from specific to general, default-deny stance (block everything not explicitly allowed). DMZs isolate public servers from internal networks - a breached web server should not reach the database.

Limitations: firewalls cannot stop insider attacks, encrypted threats they cannot inspect, or social engineering. Misconfigured rules (any-any allow) are worse than none - they create false confidence. Egress filtering (controlling outbound traffic) catches malware calling home.

Key Points

- Types: packet filter, stateful, application/NGFW.
- Default-deny, ordered rules; DMZ isolates public servers.
- Cannot stop insiders, encrypted malware, or phishing.

Key Terms

Firewall: A boundary device enforcing traffic policy.

DMZ: Demilitarized zone: isolated public-server network.

Default-deny: Blocking everything not explicitly permitted.

Egress filtering: Controlling outbound traffic.

Example

- *A company firewall allows web/email out, blocks everything else inbound.*

Summary: Firewalls are essential boundary enforcement with well-understood limits.

Exam Tips

- ★ Key point: firewall types compared.
- ★ Remember default-deny and DMZ.

Topic 12: Intrusion Detection and Prevention

Learning Objectives

- Distinguish IDS and IPS
- Compare detection methods
- Discuss alert management

Key Concepts

IDS (intrusion detection) monitors and alerts; IPS (prevention) also blocks - inline placement lets it drop malicious packets. Network-based (NIDS) watches traffic; host-based (HIDS) watches system logs and files.

Detection methods: signature-based (known attack patterns - precise, misses novel attacks) and anomaly-based (deviations from baseline - catches novel, many false positives). Modern systems blend both with machine learning.

The operational challenge is alert fatigue: thousands of daily alerts bury real incidents. Tuning, correlation (SIEM systems), and skilled analysts matter more than the tool. Snort/Suricata are classic open-source NIDS.

Key Points

- IDS detects/alerts; IPS also blocks inline.
- Signatures (known attacks) vs. anomaly (novel, noisy).
- Alert fatigue is the real enemy; tuning and SIEM help.

Key Terms

IDS/IPS: Intrusion detection/prevention systems.

Signature: A known attack pattern.

SIEM: Security information and event management.

False positive: A benign event flagged as malicious.

Example

- *Snort flags a known exploit signature: analysts investigate the alert.*

Summary: Detection technology needs tuned operations to be useful.

Exam Tips

- ★ Key point: IDS vs. IPS.
- ★ Remember signature vs. anomaly trade-offs.

Topic 13: VPNs and Secure Tunneling

Learning Objectives

- Explain VPN purposes

- Describe VPN protocols
- Discuss VPN limitations

Key Concepts

VPNs create encrypted tunnels across untrusted networks: remote-access VPNs connect traveling workers to the office; site-to-site VPNs link branch offices. Protocols: IPsec (network-layer standard), SSL/TLS VPNs (browser/client-based), WireGuard (modern, fast).

Security properties: confidentiality (encrypted tunnel), authentication (endpoints verified), integrity. But VPNs only protect the tunnel - traffic exits decrypted at the far end, and the VPN provider (for consumer VPNs) sees everything.

Limitations: VPNs do not anonymize against the provider, cannot fix endpoint malware, and misconfigured split tunneling leaks traffic. Zero-trust architectures now supplement VPNs with per-resource authentication.

Key Points

- VPNs encrypt tunnels for remote access and site links.
- Protocols: IPsec, SSL/TLS, WireGuard.
- Protects the tunnel only; provider sees traffic; endpoint security still needed.

Key Terms

VPN: Virtual private network: encrypted tunnel over public networks.

IPsec: The standard network-layer VPN protocol suite.

Split tunneling: Routing only some traffic through the VPN.

Example

- *An employee on hotel Wi-Fi uses the corporate VPN to reach office servers safely.*

Summary: VPNs secure transit; they are one layer, not total protection.

Exam Tips

- ★ Key point: what VPNs do and don't protect.
- ★ Remember IPsec.

Topic 14: Wireless Network Security

Learning Objectives

- Explain Wi-Fi security evolution
- Describe WPA2/WPA3
- List wireless attack defenses

Key Concepts

Wi-Fi's broadcast nature invites eavesdropping. Evolution: WEP (broken - crackable in minutes), WPA (interim fix, also weak), WPA2 (AES-CCMP - strong with good passwords), WPA3 (stronger handshake, forward secrecy, easier IoT onboarding).

Attacks: evil-twin access points (fake hotspots harvesting credentials), deauthentication (kicking clients to capture handshakes), and KRACK (WPA2 handshake flaw, patched). Open hotspots expose all unencrypted traffic - hence HTTPS and VPNs matter.

Defenses: WPA3 or WPA2 with strong unique passphrases, disabling WPS, hiding SSIDs (minor help), enterprise 802.1X authentication for organizations, and never trusting open Wi-Fi for sensitive work without VPN.

Key Points

- WEP broken; WPA2 strong; WPA3 strongest.
- Attacks: evil twins, deauth, handshake capture.
- Strong passphrases, WPA3, VPN on open networks.

Key Terms

WEP/WPA2/WPA3: Successive Wi-Fi security protocols.

Evil twin: A rogue access point impersonating a legitimate one.

802.1X: Enterprise Wi-Fi authentication standard.

Example

- A cafe's open Wi-Fi is safe for browsing only with VPN active.

Summary: Wireless security evolved from broken WEP to robust WPA3; user habits complete it.

Exam Tips

- ★ Very important: WEP->WPA->WPA2->WPA3 evolution.
- ★ Remember evil twin attacks.

Topic 15: Network Segmentation and Zero Trust

Learning Objectives

- Explain segmentation benefits
- Describe VLANs and micro-segmentation
- Introduce zero-trust principles

Key Concepts

Segmentation divides networks so breaches stay contained: VLANs separate departments logically; firewalls between segments enforce policy; micro-segmentation isolates individual workloads (data centers). A compromised marketing PC should not reach finance servers.

Zero trust assumes breach: 'never trust, always verify' - every access authenticated regardless of network location, replacing the old castle-and-moat (hard perimeter, soft inside). Principles: verify explicitly, least privilege, assume breach.

Implementation: identity-aware proxies, device compliance checks, micro-segmentation, continuous monitoring. Organizations migrate gradually - inventory assets, protect crown jewels first, expand. The model suits cloud and remote work where perimeters dissolved.

Key Points

- Segmentation contains breaches; VLANs and micro-segmentation implement it.
- Zero trust: never trust, always verify; no implicit network trust.
- Principles: explicit verification, least privilege, assume breach.

Key Terms

Segmentation: Dividing networks to contain breaches.

Zero trust: Security model without implicit trust.

Least privilege: Minimum access needed for tasks.

Example

- *Guest Wi-Fi segmented from the company's internal servers.*

Summary: Modern defense contains and verifies rather than trusting perimeters.

Exam Tips

- ★ Very important: zero-trust principles.
- ★ Remember segmentation's purpose.

Unit 4: Common Attacks and Defenses

Topic 16: Malware: Viruses, Worms, Trojans, Ransomware

Learning Objectives

- Classify malware types
- Explain ransomware economics
- Describe malware defenses

Key Concepts

Malware types: viruses (need host programs, spread via execution), worms (self-propagating across networks - WannaCry), trojans (disguised as legitimate software), spyware (steals data), rootkits (hide presence), and ransomware (encrypts data for payment).

Ransomware dominates: double extortion (encrypt + threaten to leak), RaaS (ransomware-as-a-service kits for affiliates), targeting backups first. Economics favor attackers - small ransoms from many victims; cryptocurrency enables payment.

Defenses: patched systems (WannaCry exploited patched vulnerabilities), reputable antivirus/EDR, email filtering, application whitelisting, network segmentation, and offline tested backups - the only reliable ransomware recovery. User training blocks the common delivery vectors.

Key Points

- Virus (host-needed), worm (self-spreading), trojan (disguised), ransomware (extortion).
- Ransomware: double extortion, RaaS; backups are the defense.
- Patch, filter, segment, train, back up offline.

Key Terms

Ransomware: Malware encrypting data for ransom.

RaaS: Ransomware-as-a-service.

EDR: Endpoint detection and response.

Rootkit: Malware hiding its presence.

Example

- *WannaCry worm spread globally via unpatched Windows SMB.*

Summary: Malware defense layers patching, filtering, and backups against evolving threats.

Exam Tips

- ★ Very important: malware types distinguished.
- ★ Remember offline backups vs. ransomware.

Topic 17: Denial of Service Attacks

Learning Objectives

- Explain DoS and DDoS
- Describe attack types
- Discuss mitigation

Key Concepts

DoS attacks exhaust resources to deny legitimate use; DDoS uses botnets (thousands of compromised devices) for scale - terabit attacks are now common. Types: volumetric (flood bandwidth - UDP amplification), protocol (SYN floods exhausting connection tables), and application-layer (slowloris tying up web servers with partial requests).

Amplification abuses open services (DNS, NTP): small queries trigger large responses toward the victim. IoT devices (weak default passwords) built the Mirai botnet.

Mitigation: overprovisioning, anycast distribution, scrubbing centers (traffic cleaned upstream), CDNs absorbing floods, rate limiting, and SYN cookies. No permanent fix - it is an arms race favoring attackers' cheap bots.

Key Points

- DDoS: botnet-powered resource exhaustion at massive scale.
- Types: volumetric, protocol, application-layer; amplification multiplies.
- Mitigation: scrubbing, CDN, anycast, rate limiting - an arms race.

Key Terms

DDoS: Distributed denial of service.

Botnet: A network of compromised devices.

Amplification: Tricking servers into large responses to victims.

Example

- *Mirai's IoT botnet launched record DDoS attacks in 2016.*

Summary: DoS defense absorbs and filters floods; scale favors attackers.

Exam Tips

- ★ Key point: the three attack types.
- ★ Remember botnets and amplification.

Topic 18: Phishing and Social Engineering

Learning Objectives

- Define social engineering
- Describe phishing variants
- Explain defenses

Key Concepts

Social engineering exploits humans, not code: phishing (fake emails/sites stealing credentials), spear phishing (targeted), whaling (executives), vishing (voice), smishing (SMS), and pretexting (invented scenarios). Pakistan's banking customers face constant fake bank SMS/calls.

Techniques: urgency ('account blocked!'), authority (fake boss/CEO fraud), and curiosity. Attackers research targets on social media for convincing pretexts.

Defenses: technical (spam filters, DMARC email authentication, browser warnings), procedural (verify requests through separate channels, dual authorization for payments), and training (simulated phishing, reporting culture). MFA blunts credential theft even when phishing succeeds.

Key Points

- Phishing variants: spear, whaling, vishing, smishing.
- Levers: urgency, authority, curiosity.
- Defense: filters, verification procedures, training, MFA.

Key Terms

Phishing: Fraudulent messages stealing credentials.

Spear phishing: Targeted phishing.

Pretexting: Inventing scenarios to extract information.

DMARC: Email authentication standard.

Example

- A 'bank' SMS with a link to 'verifv' an account - classic smishing.

Summary: Humans are the attack surface; layered technical and procedural defenses protect them.

Exam Tips

- ★ Very important: phishing variants.
- ★ Remember verification through separate channels.

Topic 19: Man-in-the-Middle and Spoofing

Learning Objectives

- Explain MITM attacks
- Describe ARP/DNS spoofing
- Discuss defenses

Key Concepts

Man-in-the-middle attackers secretly relay communications: ARP spoofing poisons local network mappings to route traffic through the attacker; DNS spoofing redirects domain lookups; rogue access points intercept Wi-Fi. Victims see normal-seeming connections.

With interception, attackers steal credentials, inject content, or strip encryption (SSL stripping downgrades HTTPS). Tools like Wireshark (defensive analysis) and attack frameworks demonstrate the techniques.

Defenses: encryption everywhere (HTTPS, TLS), certificate validation (rejecting bad certs - no click-through!), VPNs on untrusted networks, DNSSEC for DNS integrity, and network monitoring for spoofing anomalies.

Key Points

- MITM: secretly relaying/modifying communications.
- Techniques: ARP spoofing, DNS spoofing, evil twins, SSL stripping.
- Defense: TLS everywhere, cert validation, VPNs, DNSSEC.

Key Terms

MITM: Man-in-the-middle attack.

ARP spoofing: Poisoning address mappings to intercept traffic.

DNSSEC: Authenticated DNS responses.

Example

- *An attacker on cafe Wi-Fi ARP-spoofs to capture logins.*

Summary: Encryption with proper validation defeats interception.

Exam Tips

- ★ Key point: ARP vs. DNS spoofing.
- ★ Remember never click through cert warnings.

Topic 20: Password Attacks and Authentication Bypasses

Learning Objectives

- Describe password attack methods
- Explain MFA bypasses
- Discuss secure authentication design

Key Concepts

Password attacks: brute force (trying all), dictionary (common passwords), credential stuffing (reusing breached passwords - devastatingly effective), rainbow tables (precomputed hashes - defeated by salting), and keylogging.

MFA bypasses: SIM swapping (stealing phone numbers), phishing proxy pages relaying codes, and social-engineering help desks. Hence authenticator apps and hardware keys (FIDO2) beat SMS codes.

Secure design: rate limiting and lockouts, breach-corpus checks (rejecting known-compromised passwords), passwordless options (magic links, biometrics with fallback), and risk-based authentication (stepping up for unusual logins). Assume passwords leak; layer accordingly.

Key Points

- Attacks: brute force, dictionary, credential stuffing, keylogging.
- MFA bypasses: SIM swap, phishing proxies; prefer app/hardware keys.
- Design: rate limits, breach checks, passwordless, risk-based auth.

Key Terms

Credential stuffing: Trying breached passwords across sites.

SIM swapping: Hijacking a victim's phone number.

FIDO2: Hardware-key authentication standard.

Example

- A breached LinkedIn password unlocks the victim's bank via stuffing.

Summary: Passwords are weak; layered, phishing-resistant authentication replaces them.

Exam Tips

- ★ Very important: credential stuffing.
- ★ Remember SMS vs. app/hardware MFA.

Unit 5: Application and Data Security

Topic 21: Web Application Security: OWASP Top 10

Learning Objectives

- List major web vulnerabilities
- Explain injection attacks
- Describe XSS and CSRF

Key Concepts

The OWASP Top 10 catalogs web risks. Injection (SQL injection: ' OR '1'='1 in login forms) lets attackers run database commands - prevented by parameterized queries, never string concatenation. Broken authentication, sensitive data exposure, and XXE follow.

XSS (cross-site scripting): attacker scripts run in victims' browsers (stealing sessions) - stored XSS persists on the site; reflected comes via crafted links. Output encoding and CSP headers defend. CSRF tricks logged-in browsers into unwanted actions (bank transfers) - anti-CSRF tokens defend.

Secure development: validate input, encode output, use frameworks' protections, scan regularly, and patch dependencies - most breaches exploit known flaws.

Key Points

- Injection via unsanitized input; parameterized queries fix SQLi.
- XSS runs scripts in browsers; CSRF forges authenticated requests.
- Validate input, encode output, patch dependencies.

Key Terms

SQL injection: Malicious database commands via input fields.

XSS: Cross-site scripting.

CSRF: Cross-site request forgery.

OWASP: Open Web Application Security Project.

Example

- ' OR '1'='1' -- in a login box dumping the user table.

Summary: Web security is input handling done right, systematically.

Exam Tips

- ★ Very important: SQLi, XSS, CSRF - what each does.
- ★ Remember parameterized queries.

Topic 22: Email Security

Learning Objectives

- Explain email threats
- Describe SPF, DKIM, DMARC
- Discuss encryption (PGP/S-MIME)

Key Concepts

Email threats: phishing, malware attachments, business email compromise (BEC - fake executive wire requests costing billions), and spoofed senders. Email's open design invites forgery.

Authentication standards: SPF (which servers may send for a domain), DKIM (cryptographic signatures on messages), DMARC (policy tying them together, with reporting) - together they defeat exact-domain spoofing. Deployment is still incomplete globally.

Encryption: PGP/GPG (user-managed keys) and S-MIME (certificate-based) provide end-to-end confidentiality, but usability hurdles limit adoption; most protection comes from TLS in transit plus provider scanning. Organizations combine authentication, filtering, and training.

Key Points

- Threats: phishing, malware, BEC, spoofing.
- SPF + DKIM + DMARC authenticate senders.
- PGP/S-MIME encrypt; TLS protects transit.

Key Terms

BEC: Business email compromise.

SPF/DKIM/DMARC: Email authentication standards.

PGP: Pretty Good Privacy: email encryption.

Example

- *DMARC rejects a fake invoice 'from' the CEO's domain.*

Summary: Authenticate senders, encrypt sensitive mail, train users.

Exam Tips

- ★ Key point: what SPF, DKIM, DMARC each do.
- ★ Remember BEC.

Topic 23: Database and Data Protection

Learning Objectives

- Explain database security measures
- Discuss encryption at rest
- Describe data loss prevention

Key Concepts

Database security: harden configurations, least-privilege accounts (apps get minimal rights), patch DBMS, audit queries, and encrypt sensitive columns. SQL injection remains the top database threat - fix in the app layer.

Encryption at rest protects stored data (stolen disks yield nothing); key management (HSMs, rotation) decides real security. Tokenization replaces card numbers with tokens in payment systems.

Data loss prevention (DLP) monitors and blocks sensitive data leaving (USB blocks, email inspection). Backups - encrypted, offline, tested - complete the picture. Classify data (public/internal/confidential) to focus protection where it matters.

Key Points

- Harden, least-privilege, patch, audit databases.
- Encrypt at rest with proper key management.
- DLP blocks exfiltration; classified, backed-up data.

Key Terms

Encryption at rest: Protecting stored data.

Tokenization: Replacing sensitive values with tokens.

DLP: Data loss prevention.

Example

- *A stolen laptop's encrypted drive reveals nothing.*

Summary: Protect data where it lives, moves, and might leak.

Exam Tips

- ★ Key point: encryption at rest vs. in transit.
- ★ Remember least privilege for DB accounts.

Topic 24: Secure Software Development

Learning Objectives

- Introduce secure SDLC
- Explain threat modeling
- Discuss code review and testing

Key Concepts

Secure SDLC bakes security into each phase: requirements (abuse cases), design (threat modeling - 'what can go wrong?'), coding (safe functions, reviewed), testing (static/dynamic analysis, penetration tests), deployment (hardened configs), and maintenance (patching).

Threat modeling (STRIDE: spoofing, tampering, repudiation, info disclosure, DoS, elevation) systematically finds design flaws cheaply - fixing in design costs 100x less than in production.

Practices: static analysis (SAST) scans code, dynamic (DAST) tests running apps, dependency scanning catches vulnerable libraries, and bug bounties crowdsource testing. DevSecOps automates these into pipelines.

Key Points

- Security in every SDLC phase; threat modeling in design.
- STRIDE categorizes threats systematically.
- SAST, DAST, dependency scans, pentests, bounties.

Key Terms

Threat modeling: Systematic design-time security analysis.

STRIDE: Threat categories: spoofing, tampering, etc.

DevSecOps: Automated security in delivery pipelines.

Example

- *Threat-modeling a login flow reveals enumeration and brute-force risks early.*

Summary: Building security in beats bolting it on - by orders of magnitude.

Exam Tips

- ★ Key point: STRIDE categories.
- ★ Remember shift-left economics.

Topic 25: Incident Response and Digital Forensics

Learning Objectives

- Outline incident response phases
- Explain forensic principles
- Discuss business continuity

Key Concepts

Incident response (NIST): Preparation (plans, teams, tools), Detection & Analysis (triage alerts), Containment (isolate - short vs. long term), Eradication (remove cause), Recovery (restore services), Lessons Learned (improve). Speed with discipline - rushing destroys evidence.

Forensics: image drives write-blocked, hash to prove integrity, maintain chain of custody, analyze timelines and artifacts. Findings serve HR actions, legal cases, and insurance - mishandled evidence is inadmissible.

Business continuity/disaster recovery: BIA identifies critical processes, RTO/RPO set recovery targets, backups and alternate sites deliver them. Tabletop exercises test plans before real crises.

Key Points

- NIST phases: prepare, detect, contain, eradicate, recover, learn.
- Forensics: image, hash, chain of custody.
- BCP/DR with RTO/RPO targets; exercise plans.

Key Terms

Chain of custody: Documented evidence handling.

RTO/RPO: Recovery time/point objectives.

Tabletop exercise: Discussion-based incident drill.

Example

- *A ransomware playbook isolates hosts. restores from offline backups. reviews aaps.*

Summary: Prepared, practiced response turns breaches from disasters into incidents.

Exam Tips

- ★ Very important: NIST phases in order.
- ★ Remember chain of custody.

Glossary of Key Terms

CIA triad: Confidentiality, Integrity, Availability.

Firewall: A boundary device enforcing traffic policy.

AES: Advanced Encryption Standard for symmetric encryption.

RSA: Factoring-based public-key algorithm.

Hash function: One-way digest for integrity.

Digital signature: Private-key-signed hash proving origin.

VPN: Encrypted tunnel over public networks.

IDS/IPS: Intrusion detection/prevention systems.

DDoS: Distributed denial-of-service attack.

Phishing: Fraudulent messages stealing credentials.

Ransomware: Malware encrypting data for ransom.

SQL injection: Malicious database commands via inputs.

XSS: Cross-site scripting.

Zero trust: Security without implicit network trust.

PECA 2016: Pakistan's cybercrime law.