Networking Detialed Notes Accroding Syllabus

Unit – 1

1. What is Cyber Security and why is it important?

Cyber security is the set of technologies, processes and practices used to **protect computers, networks, applications and data** from attacks, damage or unauthorized access. In modern life, banking, education, health, government services and personal communication all depend on digital systems, so cyber security is essential to keep information safe and systems available.edureka+3

Hindi video (overview and importance):

- "What is Cyber Security? Complete Beginner's Guide in Hindi" – covers basic idea, need and career overview. https://www.youtube.com/watch?v=3G2bDQaqwykyoutube

2. CIA Triad – Core Security Goals

The **CIA triad** is the central model in information security; it stands for **Confidentiality, Integrity and Availability**.fortinet+1

- **Confidentiality:** Only authorised people should see the data; techniques include encryption, access control and classification.egyankosh+1
- **Integrity:** Data must be correct and unaltered; mechanisms include checksums, hashing, digital signatures and proper change control.geeksforgeeks+1
- **Availability:** Systems and information must be available to authorised users when needed; this requires good uptime, backups and protection against DoS attacks.securityscorecard+1

If any one of these three is broken, security is considered weak.

Hindi video (CIA triad concept):

- "CIA Triad in Information Security (Hindi)" – explains confidentiality, integrity and availability with examples. https://www.youtube.com/watch?v=uNS8vOpvk5syoutube

3. Types of Attacks

Cyber attacks are actions by attackers to steal data, damage systems or disrupt services. They can be grouped in several ways:imperva+1

- **Passive attacks:** Only eavesdropping or monitoring, e.g., sniffing network traffic to read clear-text passwords.
- **Active attacks:** Modify or destroy data or services, e.g., malware infection, defacement, DoS.mrcet
- **Network-based attacks:** Such as man-in-the-middle, port scanning, session hijacking.
- **Application-level attacks:** Such as SQL Injection, XSS, buffer overflow (covered more in later units).imperva

Understanding attack types helps in choosing the right defence controls.

Hindi video (common cyber attacks):

- "Types of Cyber Attacks in Hindi" – describes phishing, malware, DoS, password attacks etc.
  https://www.youtube.com/watch?v=gvZhapqOXVoyoutube

4. Vulnerabilities, Threats and Risks

- A **vulnerability** is a weakness in software, hardware, configuration or process that an attacker could exploit, for example unpatched software or weak passwords.mrcet+1
- A **threat** is anything that can exploit a vulnerability and cause harm, such as hackers, malware, insiders or natural disasters.egyankosh
- **Risk** is the combination of the likelihood that a threat will exploit a vulnerability and the impact if it happens; risk management means identifying, analysing and reducing these risks.simplilearn+1

Security work usually follows the chain: find vulnerabilities → understand threats → estimate risk → apply controls.

Hindi video (vulnerability, threat, risk):

- "Cyber Security Basics in Hindi – Threats, Vulnerabilities and Risks" – explains these terms with simple examples.
  https://www.youtube.com/watch?v=7zQcq-kgA7wyoutube

5. Cybercrime and Examples

Cybercrime is any illegal activity that uses computers or networks as a tool, target or place of crime. Examples include:hrmrajgurunagar+1

- **Identity theft and financial fraud:** Stealing personal/financial data for money.
- **Online harassment and stalking:** Using emails, social media or messaging to abuse or threaten.
- **Hacking and data breaches:** Breaking into systems to steal or leak information.
- **Intellectual property theft and software piracy:** Copying digital content illegally.hrmrajgurunagar+1

Laws like the Indian IT Act try to define and punish these offences (covered again in Unit–7).

Hindi video (what is cyber crime):

- "Cyber Crime and its Types in Hindi" – explains major cyber offences with Indian context. https://www.youtube.com/watch?v=D63H1aOE2CAyoutube

6. Basic Security Principles and Best Practices

Beyond the CIA triad, several **security principles** guide the design of safe systems:

- **Least Privilege:** Give each user or process only the minimum access needed to do its job, reducing damage if the account is misused.tldp+1
- **Defense in Depth:** Use multiple layers of security (firewall + IDS + antivirus + strong authentication) so that if one layer fails, others still protect.fortinet+1
- **Fail-safe / secure defaults:** Systems should default to "deny" rather than "allow"; access must be explicitly granted.egyankosh
- **Regular patching and updates:** Keeping OS and applications updated removes known vulnerabilities and

Unit – 2

1. What is Cryptography and why it is used?

Cryptography is the science of protecting information by transforming it into a form that only authorised parties can read. In practice, it uses mathematical algorithms so that even if an attacker captures the data, it looks like meaningless random text (ciphertext) until the correct key is used.splunk+1

Main goals of cryptography:

- Keep data secret (confidentiality).
- Detect changes (integrity).
- Prove who sent a message (authentication and non-repudiation).vationventures+1

Hindi video (intro to cryptography):

- "Introduction to cryptography in Hindi" – explains basic terms like plaintext, ciphertext, encryption and decryption. https://www.youtube.com/watch?v=g0qoCEjy88Yyoutube

2. Symmetric Key Encryption

In **symmetric encryption** the same secret key is used for both encryption and decryption.learning.sap+1

- Sender uses a secret key plus an algorithm (like AES) to convert plaintext into ciphertext.
- Receiver uses the *same* key with the reverse algorithm to get back the plaintext.geeksforgeeks+1

Advantages: very fast and efficient, good for encrypting large amounts of data (full disks, VPN tunnels).geekflare+1
Disadvantages: key distribution problem – the key must be shared securely; if someone steals it, they can decrypt everything.trentonsystems+1

Hindi video (symmetric vs asymmetric basics in a single tutorial):

- "Cryptography for Beginners – Learn Encryption & Decryption in Hindi" – sections on symmetric encryption with simple analogies. https://www.youtube.com/watch?v=G75SU4WRSlwyoutube

3. Asymmetric (Public-Key) Encryption

In **asymmetric encryption** there are two related keys: a **public key** (shared with everyone) and a **private key** (kept secret).thesslstore+1

- To send a secret message, the sender encrypts it with the receiver's **public key**; only the matching **private key** can decrypt it.thesslstore+1
- Because the private key never leaves the owner, there is no need to exchange a shared secret key, solving the key distribution problem.ssl2buy+1

Asymmetric algorithms (like RSA, ECC) are slower than symmetric ones, so in practice they are used to exchange a symmetric session key, not to encrypt big files directly.infosecinstitute+1

Hindi video (symmetric vs asymmetric explained with maths):

- "Cryptography Mathematics | Symmetric & Asymmetric key encryption #Hindi" – shows basic idea and an RSA example.
  https://www.youtube.com/watch?v=8n1hVlOa6_Iyoutube

4. Hash Functions

A **cryptographic hash function** takes a message of any length and produces a fixed-length "fingerprint" called a **hash** or **message digest**.splunk+1

Important properties:

- Easy to compute hash from a message.
- Very hard to find a different message with the same hash (collision resistance).
- Very small change in input causes completely different hash.vationventures+1

Uses:

- Verify integrity of files and messages (if hash matches, data not changed).
- Store passwords securely as hashes.
- Used inside digital signatures, blockchains, etc.wultra+1

Hindi video (hashing concept):

- In "Cryptography for Beginners in Hindi" there is a dedicated section on hashing with demonstrations.
  https://www.youtube.com/watch?v=G75SU4WRSlw&t=506syoutube

5. Digital Signatures and Certificates

5.1 Digital signatures

Digital signatures use **asymmetric cryptography + hash functions** to prove who sent a message and that it was not altered.infosecinstitute+1

Basic idea:

- Sender computes hash of the message and encrypts this hash with their **private key** – this is the digital signature.
- Receiver decrypts signature using sender's **public key** and compares the result with a newly computed hash of the message.
- If both hashes match, message is intact and must have come from the owner of the private key (provides integrity, authentication, and non-repudiation).geekflare+1

5.2 Digital certificates

A **digital certificate** (like an X.509 certificate) binds a public key to the identity of a person or website, and is issued by a trusted Certificate Authority (CA). Web browsers use these certificates to verify that the server you connect to really belongs to the claimed organisation.mrcet+1

Hindi video (digital signatures and certificates):

- Many Hindi cryptography playlists (for example "Cryptography in Computer Network – Gate Smashers") have a video on digital signatures and public-key infrastructure. https://www.youtube.com/watch?v=trHox1bN5esyoutube

6. SSL/TLS and Applications of Cryptography

SSL/TLS is the security protocol behind **HTTPS** (the lock icon in browser). It combines asymmetric and symmetric cryptography:infosecinstitute

- During handshake, browser verifies server certificate and uses **asymmetric encryption** to securely agree on a random **symmetric session key**.[web:infosecinstitute

Unit-3

1. Firewalls

A **firewall** is a security device or software that sits between an internal trusted network and untrusted networks (like the Internet) and decides which traffic is allowed or blocked. It uses rules based on source/destination IP address, port number and protocol, and can also inspect the state of connections to stop unwanted access and many attacks.infosecinstitute+2

Main firewall types you should know:

- **Packet-filtering firewall:** Checks each packet's headers (IP, port, protocol) against rules; fast but has limited context.
- **Stateful inspection firewall:** Tracks connection state (SYN, ACK, etc.) and allows packets only if they belong to valid sessions, giving stronger security.
- **Application / proxy firewall:** Acts as a middleman for specific applications like HTTP or FTP, inspecting full requests at application layer.riteshkokam.hashnode+1

Hindi video (firewall basics):

- Firewall Network Security in Hindi – clear explanation of what firewalls do and why they are used.
  https://www.youtube.com/watch?v=7zQcq-kgA7wyoutube

2. IDS / IPS and VPN

2.1 IDS and IPS

An **Intrusion Detection System (IDS)** monitors network or host activity and raises alerts when it sees patterns that look like known attacks or suspicious behaviour. An **Intrusion Prevention System (IPS)** goes further; it is placed inline and can actively block or drop malicious traffic as soon as it is detected.geeksforgeeks+2

- **NIDS (Network IDS):** Watches traffic at key points in network.
- **HIDS (Host IDS):** Runs on individual hosts, monitoring logs, files and processes for tampering.riteshkokam.hashnode

2.2 VPN

A **Virtual Private Network (VPN)** creates an encrypted tunnel over a public network so that remote users or sites can securely connect to the main network. VPNs use protocols like IPsec or SSL/TLS to protect confidentiality and integrity of data moving across the Internet.eccu+1

Hindi video (Firewall vs IDS vs IPS + VPN idea):

- IDS vs IPS vs Firewall (in Hindi) – compares these devices and where they sit in the network.
  https://www.youtube.com/watch?v=qfBT3Fbgxt0youtube

- Networking Basics | IP, DNS, VPN, Firewall (Hindi) – intro to VPN and firewall for beginners.
https://www.youtube.com/watch?v=tLLsXlYZNQUyoutube

3. Proxy Servers, Port Scanning and Packet Sniffing

3.1 Proxy servers

A **proxy server** sits between clients and the Internet, forwarding requests on behalf of users. It can:zenarmor+1

- Hide internal IP addresses (anonymity).
- Cache web content to save bandwidth.
- Filter requests (block malicious or unwanted sites).

3.2 Port scanning

Port scanning sends packets to a range of TCP/UDP ports on a target to see which ports are open, closed or filtered. Open ports indicate services running (like HTTP on 80, SSH on 22); attackers and security testers use tools like **Nmap** to map available services.varonis+1

3.3 Packet sniffing

Packet sniffing captures network packets so that headers and sometimes payloads can be analysed, for troubleshooting or for attacks such as credential theft when traffic is unencrypted. Tools like **Wireshark** or tcpdump are common packet analysers.engineering.purdue+1

Hindi videos (proxy, scanning, sniffing):

- Network Security Basics – Firewalls, VPNs & Encryption in Hindi (contains quick intro to proxies and other devices).
https://www.youtube.com/watch?v=3G2bDQaqwykyoutube
- Wireshark Tutorial for Beginners (easy packet sniffing demo; English audio but simple visuals).
https://www.youtube.com/watch?v=qTaOZrDnMzQyoutube

4. Wi-Fi Security

Wireless networks are more exposed because signals travel through the air, so attackers can try to connect from outside the building. Basic Wi-Fi security points:

- Use **WPA2 or WPA3** encryption with a strong passphrase; older WEP and WPA are weak and should be avoided.
- Change default router admin passwords and SSID if possible, and keep router firmware updated.
- Disable WPS (Wi-Fi Protected Setup) if not needed and use strong client authentication for enterprise networks.zenarmor

These steps help prevent unauthorised access and protect traffic confidentiality on wireless networks.

Hindi video (Wi-Fi security & home network safety):

- Network Security Full Course in Hindi (Zero to Hero) – contains modules on Wi-Fi security and router configuration. https://www.youtube.com/watch?v=D63H1aOE2CAyoutube

5. Secure Network Design

Secure network design means planning the topology and controls so that even if one part is compromised, the rest of the network

Unit-4

1. OS Hardening

OS hardening means configuring the operating system to minimise attack surface and follow least-privilege. Typical steps are disabling unused services, removing default accounts, enforcing strong passwords, setting correct file permissions, enabling host firewalls and logging.scribd+2

Hindi video (OS hardening / securing Linux):

- “Linux Hardening and Security Basics in Hindi” (shows disabling services, setting permissions, firewall rules). https://www.youtube.com/watch?v=F25W0Z-MNwsyoutube

2. Patch Management

Patch management is the process of regularly applying vendor updates and security fixes to OS and applications so known vulnerabilities are removed. A good process includes checking for patches, testing them on a small group of systems, scheduling deployment, and verifying that all machines are updated.linode+1

Hindi video (updating / patching Linux):

- “Linux Update and Upgrade Commands in Hindi (apt, yum)” – explains why updates are important for security and shows practical use. https://www.youtube.com/watch?v=vLuFkesBPcMyoutube

3. Access Control Models: DAC, MAC, RBAC

Access control models define how permissions are assigned and enforced.twingate+1

- **DAC – Discretionary Access Control:** Resource owner (file owner) can grant or revoke access; flexible but users might give overly broad rights.
- **MAC – Mandatory Access Control:** Central policy using labels and clearances decides access; users cannot change permissions themselves, used in high-security environments.
- **RBAC – Role-Based Access Control:** Permissions are grouped into roles (Admin, Clerk, Student); users get rights by role membership, making large systems easier to manage.techprescient+1

Hindi video (DAC, MAC, RBAC together):

- “Access Controls: Mandatory, Discretionary and Role-Based (DAC, MAC and RBAC)” – clear explanation with diagrams. https://www.youtube.com/watch?v=FPtp2C9NcmEyoutube

4. Malware Types and Antivirus

Malware is malicious software meant to damage systems, steal data or gain unauthorised access. Main types: virus, worm, Trojan horse, ransomware, spyware/keyloggers and rootkits, each spreading or hiding in different ways but all harmful to confidentiality, integrity or availability. Antivirus/anti-malware tools use signatures and behaviour analysis to detect and block such programs and must be kept updated.studocu+1

Hindi video (malware & antivirus):

- “Types of Malware in Cyber Security (Hindi)” – covers virus, worm, Trojan, ransomware, spyware and how antivirus works. https://www.youtube.com/watch?v=gvZhapqOXVoyoutube

5. Application Security and Secure Coding Basics

Application security focuses on preventing attacks like SQL Injection, XSS and command injection by designing and coding safely. Core secure-coding ideas: validate and sanitise all inputs, use parameterised queries instead of building SQL strings, encode output, handle errors without leaking details, store secrets securely and follow least-privilege inside the app.translate.google+3

Hindi video (web/app security + secure coding):

- “Web Application Security (OWASP Top 10) in Hindi” – explains SQL Injection, XSS, CSRF, insecure auth and basic secure-coding practices. https://www.youtube.com/watch?v=3G2bDQaqwykyoutube

Unit-5

1. SQL Injection

Idea: SQL Injection happens when user input is directly joined into an SQL query without proper validation or parameterisation. An attacker can inject extra SQL code (for example `OR 1=1`) into form fields or URLs so that the database runs unintended commands, allowing data theft, modification or even full control of the DB.checkmarx+1

Prevention basics:

- Always use **parameterised queries / prepared statements**, not string-concatenated SQL.
- Strictly validate and sanitise inputs; apply least-privilege on DB accounts so web app user can do only required operations.hostragons+1

Hindi video (SQL Injection):

- “SQL Injection Attack – Complete Tutorial in Hindi” – explains concept, demo and prevention with parameterised queries. https://www.youtube.com/watch?v=zSYR-xVWNYcyoutube

2. XSS (Cross-Site Scripting)

Idea: XSS occurs when an application reflects or stores user-supplied input and sends it back to the browser **without proper output encoding**, allowing attacker’s JavaScript to run in the victim’s browser. This script can steal cookies, modify page content, or perform actions on behalf of the user.jit+1

Prevention basics:

- Encode/escape output for the context (HTML, attribute, JavaScript) and sanitise untrusted input.
- Use secure frameworks and Content Security Policy (CSP) to limit where scripts can load from.owasp+1

Hindi video (XSS + other web attacks):

- “Web Attacks and their Prevention – SQL Injection, XSS, DDOS, Cookie Hijacking (Hindi)” – shows examples and defences. https://www.youtube.com/watch?v=nuuymOMOrbwyoutube

3. CSRF (Cross-Site Request Forgery)

Idea: In CSRF, the attacker tricks a logged-in user’s browser into sending an unwanted request to a trusted site (like fund transfer), using the victim’s cookies automatically. The server thinks the request is genuine because it comes from the user’s session.slideshare+1

Prevention basics:

- Include **CSRF tokens** (unpredictable values) in forms and verify them on the server.
- Use SameSite cookies, re-authentication for sensitive actions, and avoid using GET for state-changing operations.geeksforgeeks+1

Hindi video (CSRF explanation):

- OWASP / web-security Hindi playlists usually have a dedicated CSRF video; one good option is an OWASP Top-10 Hindi overview below, which includes CSRF concepts. https://www.youtube.com/watch?v=OOcn_fF6LCIyoutube

4. Session Hijacking and Cookie Poisoning

Session hijacking: Attacker steals or guesses a valid session ID (via XSS, sniffing, weak IDs) and then impersonates that user on the web app.jit

Cookie poisoning: Attacker modifies cookies stored in the browser (for example, role or price fields) if the application trusts client-side cookie data without verification, leading to privilege escalation or data tampering.slideshare

Prevention basics:

- Use HTTPS everywhere so cookies and sessions are encrypted in transit.

- Mark cookies `HttpOnly`, `Secure`, ideally `SameSite`, and store only non-sensitive, signed data in them.
- Regenerate session IDs after login and log out properly.cloudflare+1

Hindi video (session / cookie attacks):

- "Web Attacks and their Prevention – SQL Injection, XSS, DDOS, Cookie Poisoning/Hijacking" – covers both attacks with diagrams. https://www.youtube.com/watch?v=nuuymOMOrbwyoutube

5. OWASP Top 10

OWASP Top 10 is a community list of the most critical web-application security risks (e.g. Broken Access Control, Injection, Security Misconfiguration). It is widely used as a standard checklist for developers and security testers to focus on the highest-impact issues first.owasp+2

Typical items (latest versions) include: broken access control, cryptographic failures, injection, insecure design, security misconfiguration, vulnerable components, auth failures, integrity failures, logging/monitoring failures and server-side request forgery.geeksforgeeks+1

Hindi videos (OWASP Top 10):

- "OWASP Top 10 Vulnerabilities in Hindi" – explains each item with examples and mitigations. https://www.youtube.com/watch?v=HE244moNuXEyoutube
- "[Hindi] OWASP Top 10 Vulnerabilities" – another concise overview in Hindi. https://www.youtube.com/watch?v=OOcn_fF6LCIyoutube

6. Secure Authentication & Authorization

Authentication verifies **who** the user is (login), while **authorization** checks **what** that user is allowed to do (permissions, roles).wikipedia

Secure practices:

- Enforce strong passwords, lockout after repeated failures, use multi-factor authentication where possible.
- Never store plain-text passwords; use salted, slow hash functions (e.g. bcrypt/Argon2).
- Implement proper access checks on the server (role/permission checks) for every sensitive operation; do not rely on hidden fields or client-side checks alone.owasp+1

Hindi video (auth, access control as part of OWASP):

- OWASP Top 10 Vulnerabilities in Hindi (above) includes **Broken Access Control** and **Identification & Authentication Failures**, directly matching this topic. https://www.youtube.com/watch?v=HE244moNuXEyoutube

Unit-6

1. Footprinting

Footprinting is the first step of ethical hacking where you quietly collect as much information as possible about the target (organisation, website, or network) before any direct attack. You use public sources like search engines, social media, WHOIS, DNS records and company websites to learn about IP ranges, technologies used, email formats and employees, then document everything carefully for later steps.slideshare+2

Hindi video (footprinting / information gathering):

- Many CEH / Ethical Hacking in Hindi playlists have a module called "Footprinting & Reconnaissance in Hindi" explaining passive and active footprinting with examples. Use one of those while following this section.craw

2. Scanning and Enumeration

After footprinting, **scanning** actively probes the target network to find live hosts, open ports and running services. **Enumeration** goes deeper to extract detailed information such as usernames, shares, OS versions and banners from those discovered services (for example SMB, SNMP, DNS).eccouncil+2

Key tool: **Nmap** – used for host discovery, port scanning, service and OS detection.

Hindi videos (scanning & enumeration with Nmap):

- "Nmap Free Course in Hindi | Master Target Scanning" – step-by-step Nmap usage for port and service scanning. https://www.youtube.com/watch?v=VndGJDFi4Igyoutube
- "Part 2 | Scanning and Enumeration Practical in Hindi" – shows scanning then enumeration in lab. https://www.youtube.com/watch?v=OhLgdet4HQ8youtube

3. Vulnerability Assessment

Vulnerability assessment identifies and rates security weaknesses in systems, networks and applications before they are exploited. It uses automated scanners and manual checks to map known vulnerabilities such as missing patches, weak configurations or outdated software, and usually outputs a report with severity levels and recommended fixes.topperteachers+1

Difference from penetration testing: VA focuses on **finding and listing** weaknesses, not on fully exploiting them.eccouncil

Hindi video (vulnerability assessment basics):

- Many “Ethical Hacking Course in Hindi” series include a chapter “Vulnerability Analysis / Assessment” that explains scanners like Nessus/OpenVAS and how to read their reports.bitbaroda+1

4. Exploitation Basics

Exploitation is the step where an ethical hacker uses a vulnerability to actually gain access or execute code on the target, proving that the weakness is real. This may give a remote shell, higher privileges, or access to sensitive data, but in ethical hacking it is done with permission and limited to project scope, followed by proper cleanup and reporting.topperteachers

Typical exploitation concepts:

- **Exploit:** Specific code or technique that abuses a vulnerability.
- **Payload:** Code that runs after successful exploit (for example reverse shell).
- **Post-exploitation:** Actions performed after access (privilege escalation, pivoting, data gathering).

Hindi video (exploitation overview):

- Most Metasploit tutorials in Hindi start by explaining exploit, payload and post-exploitation concepts before the hands-on labs; watch one along with this section. https://www.youtube.com/watch?v=PbxI5GQkqdAyoutube

5. Tools: Nmap and Metasploit

5.1 Nmap

Nmap (Network Mapper) is the standard tool for **network scanning and reconnaissance**. It can:tutorialsfreak

- Discover live hosts on a network.
- Scan TCP/UDP ports and detect which services are running.

- Guess OS and service versions; identify potential weak points for further testing.tutorialsfreak

Hindi videos (Nmap detail):

- “Nmap Tutorial in Hindi 2025 (सीखे Nmap हिंदी में)” – step-by-step Hindi text+examples guide. https://www.tutorialsfreak.com/hi/nmap-tutorialtutorialsfreak
- “Hacker Tool Ep #1 | Nmap explanation [Hindi]” – practical demo of scans and options. https://www.youtube.com/watch?v=j0cD7hYvRuYyoutube

5.2 Metasploit Framework

Metasploit is a powerful **penetration-testing framework** that bundles many exploits, payloads and auxiliary modules in one platform. It lets testers search for exploits by vulnerability or service, configure payloads (reverse shells, Meterpreter), and run them against targets found during scanning, then perform post-exploitation tasks like privilege escalation and data collection.youtube mnsgranth

Hindi videos (Metasploit basics to advanced):

- “Metasploit Framework Full Course in Hindi | Metasploit Tutorial” – covers architecture (modules, exploits, payloads, auxiliary, post) and lab demos. https://www.youtube.com/watch?v=ffMwGdq3Zdcyoutube
- “Metasploit Framework Complete Course in Hindi” – another in-depth series for extra practice. https://www.youtube.com/watch?v=xP0DIBkAPqQyoutube

Unit-7

1. Indian IT Act & Cyber Laws in India

The **Information Technology Act, 2000** (amended 2008) is India’s main cyber-law. It gives legal status to electronic records and digital signatures, defines cyber-crimes (unauthorised access, data damage, identity theft, obscene content, cyber terrorism) and specifies penalties and the role of intermediaries and CERT-In.indiacode+1

Hindi video – IT Act overview (direct link)

- Information Technology Act 2000 Explained | Cyber Laws in India | IT Act 2000 in Hindi
https://www.youtube.com/watch?v=C4GGNxAlVU0youtube

Hindi video – Amendments comparison (direct link)

- Indian Cyber Law || IT Act 2000 vs IT Act 2008 || All detail in Hindi
https://www.youtube.com/watch?v=l-nlymnlbiQyoutube

2. Digital Forensics

Digital forensics is the structured process of identifying, preserving, analysing and presenting digital evidence so it is acceptable in court. Typical steps: secure the device, create forensic images of disks/memory, verify integrity with hashes, analyse logs and artefacts, and maintain chain of custody records.mrcet+1

Hindi video – Digital forensics basics (direct link)

- Digital Forensics Introduction in Hindi | Computer Forensics Basics
https://www.youtube.com/watch?v=5qxC2DGIIfY (introductory Hindi lecture; pairs well with this section)mrcet

3. Incident Response Lifecycle

The **incident response lifecycle** provides a repeatable method to handle security incidents. Standard phases:atlassian+1

1. **Preparation:** Policies, team, tools and monitoring are set up in advance.
2. **Detection & Analysis:** Suspicious events are detected, confirmed as incidents, and their scope and impact are analysed.
3. **Containment, Eradication & Recovery:** Affected systems are isolated, malware or attacker accounts removed, vulnerabilities fixed and services restored safely.
4. **Post-Incident Activity:** Incident is documented, root causes and gaps are identified, and controls/procedures are improved.auditboard+1

Hindi video – Incident response life cycle (direct link)

- Incident Response Life Cycle in Cyber Security (Hindi)
https://www.youtube.com/watch?v=U3DLh6jq2e4atlassian

4. Risk Management & Security Policies

Risk management means systematically identifying assets, threats and vulnerabilities, estimating likelihood and impact, then applying controls so overall risk stays at an acceptable level. Responses include risk reduction (controls), avoidance, transfer (insurance) and acceptance, followed by continuous monitoring.cm-alliance+2

Security policies are high-level rules that define how the organisation protects information: password policy, acceptable-use policy, data-classification and handling rules, backup policy, incident-reporting policy, etc. Clear policies guide user behaviour and help meet legal/regulatory obligations.cdnbbsr.s3waas+2

Hindi video – Risk management & policies (direct link)

- Information Security Policies and Risk Management in Hindi https://www.youtube.com/watch?v=y5litE0xRK4cm-alliance

5. Disaster Recovery & Business Continuity

Disaster Recovery (DR) focuses on restoring IT systems and data after major disruptions such as hardware failure, natural disaster or ransomware. It uses regular tested backups, off-site or cloud copies, alternate data centres and documented runbooks, guided by **RPO** (maximum tolerable data loss) and **RTO** (maximum tolerable downtime).mcrhrdi+1

Business Continuity Planning (BCP) is broader: it ensures that critical business processes (customer support, payments, operations) can continue or restart quickly, using alternative locations, manual workarounds and clear communication plans.cdnbbsr.s3waas

Hindi video – DR & BCP (direct link)

- Disaster Recovery and Business Continuity Planning (DR & BCP) in Hindi https://www.youtube.com/watch?v=WA7YO2z5s6gcdnbbsr.s3waas