CYBER SECURITY

Comprehensive Learning Material

UNIT I	Introduction to Cyber Security
UNIT II	Attacks and Countermeasures
UNIT III	Reconnaissance
UNIT IV	Intrusion Detection
UNIT V	Intrusion Prevention

Prepared for Academic Use | All Five Units | ~50 Pages

TABLE OF CONTENTS

UNIT I INTRODUCTION

1.1 Cyber Security – Overview

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

It encompasses multiple layers of protection spread across the computers, networks, programs, and data that one intends to keep safe. In an organisation, people, processes, and technology must all complement one another to create an effective defence from cyber-attacks.

Why is Cyber Security Important?

- Growing dependence on digital infrastructure in every sector
- Rise in financially motivated cybercrime (ransomware, fraud)
- Nation-state sponsored espionage and sabotage
- Protecting personal privacy and sensitive data
- Compliance with regulatory requirements (GDPR, IT Act, HIPAA)

1.2 The CIA Triad

The CIA Triad is the foundational model of information security, representing the three core goals that any secure system must achieve:

CIA Component	Description & Techniques
Confidentiality	Ensuring information is accessible only to those authorised to access it. Techniques: encryption, access controls, data masking.
Integrity	Safeguarding the accuracy and completeness of information. Techniques: hashing (SHA-256), digital signatures, checksums.
Availability	Ensuring authorised users have reliable, timely access to information. Techniques: redundancy, backups, DDoS mitigation, uptime monitoring.

■ *Beyond CIA, modern frameworks add Authentication, Non-repudiation, and Accountability to form an extended security model.*

1.3 History of the Internet & Its Impact

Key Milestones

Year	Milestone
1969	ARPANET – First packet-switched network connecting 4 US universities
1974	TCP/IP protocol suite proposed by Cerf & Kahn

Year	Milestone
1983	DNS (Domain Name System) introduced
1991	World Wide Web invented by Tim Berners-Lee
1993	Mosaic browser – Internet goes public
1995	Amazon & eBay launch – e-commerce era begins
2004	Facebook & social media era begins
2010+	Mobile Internet, Cloud Computing, IoT explosion
2020+	AI-driven services, 5G, edge computing

Impact of the Internet

Positive Impacts

- Global communication and information sharing
- E-commerce and digital economy
- Online education and e-governance
- Telemedicine and remote work

Negative Impacts / Risks

- Cybercrime and fraud
- Privacy violations and surveillance
- Misinformation and fake news
- Addiction and mental health issues

1.4 Cybercrime – Definition & History

Cybercrime is criminal activity that either targets or uses a computer, a computer network, or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money, though cybercrime can also be politically motivated.

Historical Timeline of Cybercrime

Era	Development
1970s	Phone phreaking – manipulating telephone systems; early hacking culture
1980s	First computer viruses; Kevin Mitnick's exploits; 'War Games' (1983 film)
1988	Morris Worm – first Internet worm, infected ~6000 machines
1990s	Credit card fraud, early malware, defacement attacks
2000s	Organised cybercrime, botnets, phishing, identity theft
2010s	Nation-state attacks (Stuxnet), mega data breaches, ransomware
2020s	Supply-chain attacks, AI-powered attacks, deepfake fraud

Reasons for Cybercrime Growth

- Anonymity offered by the Internet
- High financial gain with low risk of physical confrontation
- Weak security practices by individuals and organisations
- Rapid technological growth outpacing security measures
- Availability of hacking tools on dark web

1.5 Classification of Cybercrimes

By Target

Category	Examples
Crimes against Individuals	Identity theft, cyberstalking, phishing, harassment, defamation
Crimes against Property	Hacking, virus attacks, copyright infringement, data theft
Crimes against Organisations	Corporate espionage, DDoS, ransomware, insider threats
Crimes against Society/Government	Cyber terrorism, critical infrastructure attacks, propaganda

Cyber Criminals – Classification

Script Kiddies

Unskilled individuals using pre-written tools/scripts without understanding

Hacktivists

Politically or ideologically motivated hackers (e.g., Anonymous)

Cybercriminals

Financially motivated; organised crime groups

Insider Threats

Disgruntled or malicious employees with internal access

Nation-State Actors

Government-sponsored espionage (APT groups)

Cyber Terrorists

Use cyberspace to cause terror, disrupt critical services

1.6 Global Perspective & Cyber Laws

Global Perspective on Cybercrime

Cybercrime is a transnational problem. Jurisdictional challenges, lack of international cooperation, and varying legal frameworks make investigation and prosecution difficult. Key international bodies include INTERPOL, the UN Group of Governmental Experts (GGE), and the Budapest Convention on Cybercrime (2001), the first international treaty on cybercrime.

The Indian IT Act, 2000 (Amended 2008)

The Information Technology Act, 2000 is the primary legislation governing cyber activities in India. It provides legal recognition to electronic transactions and addresses cybercrimes.

Section	Provision
Section 43	Penalty for unauthorised access, downloading, copying, damage to computers
Section 65	Tampering with computer source documents – up to 3 years imprisonment
Section 66	Computer-related offences (hacking) – up to 3 years / Rs. 5 lakh fine
Section 66A	Sending offensive messages (struck down by SC in 2015)
Section 66B	Dishonestly receiving stolen computer resources
Section 66C	Identity theft – up to 3 years / Rs. 1 lakh fine
Section 66D	Cheating by impersonation using computer resources
Section 66E	Violation of privacy – publishing private images
Section 66F	Cyber terrorism – life imprisonment
Section 67	Publishing obscene material in electronic form
Section 72	Breach of confidentiality and privacy

■ *CERT-In (Computer Emergency Response Team – India) operates under the IT Act to coordinate responses to cybersecurity incidents.*

Need for Cyber Security

- Protect sensitive personal and financial data from theft
- Ensure business continuity and prevent costly downtime
- Guard national critical infrastructure (power, banking, defence)
- Comply with data protection regulations
- Maintain public trust in digital systems and e-governance
- Prevent cyber espionage and intellectual property theft

UNIT I KEY TAKEAWAYS

✔ CIA Triad: Confidentiality, Integrity, Availability	✔ India's IT Act 2000 is the primary cyber law
✔ Internet evolved from ARPANET (1969) to global infrastructure	✔ Cyber criminals range from script kiddies to nation-state actors

✔ Cybercrime classified by target: individuals, property, organisations	✔ CERT-In coordinates India's cybersecurity incident response

UNIT II ATTACKS AND COUNTERMEASURES

2.1 OWASP – Open Web Application Security Project

OWASP is an open-community foundation dedicated to improving the security of software. It provides free resources, tools, and standards. The OWASP Top 10 is the most widely recognised list of critical web application security risks.

ID	Risk	Description
A01:2021	Broken Access Control	Improper enforcement of restrictions on authenticated users
A02:2021	Cryptographic Failures	Weak/missing encryption of sensitive data
A03:2021	Injection	SQL, NoSQL, OS, LDAP injection flaws
A04:2021	Insecure Design	Flaws in architecture and design patterns
A05:2021	Security Misconfiguration	Default configs, unnecessary features enabled
A06:2021	Vulnerable Components	Using libraries with known vulnerabilities
A07:2021	Authentication Failures	Weak passwords, session management flaws
A08:2021	Software & Data Integrity Failures	Insecure CI/CD pipelines, updates
A09:2021	Security Logging Failures	Insufficient monitoring and logging
A10:2021	Server-Side Request Forgery	SSRF attacks bypassing firewall filters

2.2 Types of Malicious Attacks

Scope of Cyber-Attacks

Cyber-attacks can target any layer of the computing stack: hardware, firmware, OS, applications, networks, or end users. The scope ranges from targeted attacks on a single system to massive campaigns affecting millions of users globally.

Security Breach vs. Data Breach

Security Breach

Any incident that results in unauthorised access to computer data, applications, networks, or devices, regardless of whether data was stolen.

Data Breach

A security incident in which information is accessed without authorisation and data is actually exfiltrated or disclosed.

Common Attack Types

Phishing

Fraudulent emails/websites mimicking legitimate entities to steal credentials or install malware.

Spear Phishing

Targeted phishing aimed at specific individuals using personalised content.

Vishing

Voice phishing – attackers call targets impersonating banks or IT support.

Smishing

SMS-based phishing attacks.

Malware

Malicious software including viruses, worms, trojans, spyware, adware.

Ransomware

Encrypts victim's data and demands payment for decryption key. (e.g., WannaCry, Ryuk)

DDoS

Distributed Denial-of-Service – overwhelming a server with traffic from many sources.

Man-in-the-Middle

Attacker secretly intercepts and possibly alters communication between two parties.

SQL Injection

Inserting malicious SQL code into input fields to manipulate databases.

Cross-Site Scripting (XSS)

Injecting malicious scripts into web pages viewed by other users.

Zero-Day Exploit

Attack targeting a previously unknown vulnerability before a patch is available.

Brute Force

Systematically checking all possible passwords until the correct one is found.

Credential Stuffing

Using stolen username/password lists to gain unauthorised access.

DNS Poisoning

Corrupting DNS cache to redirect users to malicious websites.

2.3 Malicious Software & Common Attack Vectors

Type	Behaviour	Examples/Notes
Virus	Attaches to legitimate files; requires user action to spread	Boot sector, macro viruses
Worm	Self-replicating; spreads without user action via networks	Morris Worm, Conficker
Trojan	Disguised as legitimate software; creates backdoors	Remote Access Trojans (RATs)
Spyware	Covertly monitors user activity, captures keystrokes	Keyloggers, screen capturers
Adware	Displays unwanted ads; may track browsing	Often bundled with free software
Rootkit	Hides malicious activity by modifying OS	Extremely hard to detect/remove
Botnet	Network of infected machines controlled remotely	Used for spam, DDoS, mining
Ransomware	Encrypts files; demands ransom	WannaCry, Petya, LockBit

Common Attack Vectors

- Email attachments and phishing links
- Malicious websites and drive-by downloads
- Removable media (USB drives)
- Software vulnerabilities and unpatched systems
- Insider threats and misconfigurations
- Third-party software and supply chain compromises
- Social engineering of employees

2.4 Social Engineering Attacks

Social engineering exploits human psychology rather than technical vulnerabilities. Attackers manipulate individuals into performing actions or divulging confidential information.

Technique	Description	Example
Pretexting	Creating a fabricated scenario (pretext) to extract information	Impersonating IT support, HR
Baiting	Luring victims with something enticing (free USB drive with malware)	USB drops in car parks
Quid Pro Quo	Offering a service in exchange for information	'Free IT support' calls
Tailgating	Physically following an authorised person into a restricted area	Badge surfing
Whaling	Spear phishing targeting senior executives (CEOs, CFOs)	CEO fraud, BEC scams

2.5 Wireless & Web Application Attacks

Wireless Network Attacks

Evil Twin Attack

Setting up a rogue Wi-Fi access point to intercept traffic.

WEP/WPA Cracking

Exploiting weak wireless encryption protocols to gain network access.

Wardriving

Driving around with a laptop/device to discover and map wireless networks.

Packet Sniffing

Capturing wireless packets in promiscuous mode to extract sensitive data.

Deauthentication Attack

Forcing a client off a Wi-Fi network by sending forged deauth frames.

Web Application Attacks

SQL Injection (SQLi)

Attacker inserts SQL code into input fields; can dump entire database.

Cross-Site Scripting (XSS)

Injecting client-side scripts into pages viewed by other users.

Cross-Site Request Forgery (CSRF)

Tricks a user's browser into submitting unwanted requests.

Directory Traversal

Accessing files outside the web root using ../sequences.

Remote File Inclusion (RFI)

Including a remote malicious file via vulnerable PHP scripts.

Clickjacking

Tricking users into clicking hidden elements overlaid on a page.

2.6 Attack Tools & Countermeasures

Common Attack Tools (for Awareness)

Tool	Purpose
Metasploit	Penetration testing framework with extensive exploit modules
Nmap	Network scanning and host discovery
Wireshark	Network packet analyser / sniffer
John the Ripper	Password cracking tool
Aircrack-ng	Wi-Fi security auditing suite
Burp Suite	Web application security testing proxy

Tool	Purpose
SQLmap	Automated SQL injection tool

Countermeasures

- Keep systems and software patched and updated
- Use strong, unique passwords and multi-factor authentication (MFA)
- Deploy firewalls, IDS/IPS, and endpoint protection
- Conduct regular security awareness training for employees
- Perform periodic vulnerability assessments and penetration testing
- Implement data encryption at rest and in transit
- Follow the principle of least privilege for access control
- Maintain regular, tested backups (3-2-1 rule)

UNIT II KEY TAKEAWAYS

✔ OWASP Top 10 identifies critical web app risks	✔ Social engineering exploits human psychology
✔ Attacks target technical AND human vulnerabilities	✔ Wireless networks face unique attack surfaces
✔ Malware includes viruses, worms, trojans, ransomware	✔ Countermeasures must be layered (defence-in-depth)

UNIT III RECONNAISSANCE

3.1 Reconnaissance – Overview

Reconnaissance (Recon) is the first phase of the ethical hacking / penetration testing methodology. It involves gathering as much information as possible about a target system, network, or organisation before launching an attack. Proper recon gives attackers (or pen testers) a roadmap of the attack surface.

Type	Description
Passive Reconnaissance	Gathering information without direct interaction with the target. Target is unaware. E.g., WHOIS, Google, social media searches.
Active Reconnaissance	Direct interaction with target systems. May trigger IDS alerts. E.g., port scanning, banner grabbing, ping sweeps.

3.2 Footprinting Tools

theHarvester

An OSINT (Open-Source Intelligence) tool that collects email addresses, subdomains, IPs, and URLs from public sources like Google, Bing, LinkedIn, Shodan, and more.

Example Commands:

- theHarvester -d example.com -b google
- theHarvester -d example.com -b all -l 500

WHOIS

Queries domain registration databases to obtain registrant details, name servers, registration/expiry dates, and contact information. Useful for identifying domain owners.

Example Commands:

- whois example.com
- whois 192.168.1.1

Netcraft

Web-based service that reveals operating system, web server software, hosting history, SSL certificate details, and site technology stack. Useful for profiling web infrastructure.

Example Commands:

- https://sitereport.netcraft.com/?url=example.com (browser-based)

Host Command

DNS lookup utility for converting hostnames to IP addresses and vice versa. Also retrieves MX, NS, and other DNS records.

Example Commands:

- host example.com
- host -t mx example.com
- host -t ns example.com

3.3 Extracting Information from DNS

DNS (Domain Name System) is a goldmine for reconnaissance. Attackers query DNS records to map a network's infrastructure.

Record	Purpose	Example
A	Maps hostname to IPv4 address	www.example.com → 93.184.216.34
AAAA	Maps hostname to IPv6 address	IPv6 address of host
MX	Mail exchange server	mail.example.com
NS	Authoritative name servers	ns1.example.com
TXT	Text records (SPF, DKIM, verification)	'v=spf1 include:...'
SOA	Start of Authority – primary DNS info	Serial, refresh, retry values
CNAME	Canonical name / alias	www → example.com

DNS Zone Transfer (AXFR)

A zone transfer (AXFR) copies the entire DNS zone file from a master to a slave server. If misconfigured, an attacker can retrieve ALL DNS records for a domain, revealing internal hostnames, mail servers, and server IPs.

- Command: dig axfr @ns1.example.com example.com

■ *Mitigation: Restrict zone transfers to authorised secondary name servers only.*

Extracting Information from E-mail Servers

E-mail headers contain valuable recon data: originating IP, mail server software/version, routing path, and timestamps. Tools like MXToolbox can reveal mail server configurations.

- MX record lookup reveals mail server hostnames
- Connecting to SMTP server and running EHLO/VRFY/EXPN commands
- Email header analysis reveals internal mail relay IPs
- User enumeration via VRFY command (if enabled)

3.4 Scanning – Concepts and Methodology

Scanning is the next phase after footprinting. It involves probing live systems to identify open ports, running services, OS types, and vulnerabilities.

Type	Purpose	Common Tools
Port Scanning	Identifies open TCP/UDP ports and associated services	nmap, masscan, netcat
Network Scanning	Discovers live hosts and network topology	nmap -sn, arp-scan, ping sweep
Vulnerability Scanning	Identifies known vulnerabilities in services	Nessus, OpenVAS, Nikto

Scanning Methodology

- Step 1: Check for live systems using ICMP (ping sweep)
- Step 2: Identify open ports (TCP/UDP port scan)
- Step 3: Fingerprint OS and service versions
- Step 4: Identify vulnerabilities using a vulnerability scanner
- Step 5: Map network topology and trust relationships
- Step 6: Document findings for exploitation phase

Ping Sweep Techniques

A ping sweep sends ICMP Echo Requests to a range of IP addresses to identify live hosts. Tools and methods:

- fping -g 192.168.1.0/24 – fast parallel pinging
- nmap -sn 192.168.1.0/24 – nmap ping scan (no port scan)
- ping -b 192.168.1.255 – broadcast ping (less reliable)
- hping3 – advanced packet crafting for custom pings

3.5 Nmap – Network Mapper

Nmap is the industry-standard open-source tool for network discovery and security auditing. It uses raw IP packets to determine which hosts are alive, which ports are open, what services run, the OS, and firewall characteristics.

Switch	Description
-sS	TCP SYN scan (stealth scan) – sends SYN, does not complete handshake
-sT	TCP Connect scan – full 3-way handshake; slower, more detectable
-sU	UDP scan – slower; checks UDP services like DNS, SNMP
-sN	TCP Null scan – no flags set; can evade some firewalls
-sF	TCP FIN scan – only FIN flag; used for OS fingerprinting
-sX	Xmas scan – FIN+PSH+URG flags set
-O	OS detection / fingerprinting
-sV	Version detection for services running on open ports
-A	Aggressive scan: OS detection + version + traceroute + scripts
-p	Specify port(s): -p 80, -p 1-1024, -p- (all 65535)
-T0 to -T5	Timing templates: 0=paranoid, 3=normal, 5=insane
--script	Run NSE (Nmap Scripting Engine) scripts for vulnerability detection
-v / -vv	Verbose / very verbose output
-oN / -oX	Output to Normal / XML file
-Pn	Skip host discovery; treat all hosts as online

Example Nmap Commands

- nmap 192.168.1.1 → Basic scan of single host
- nmap -sS -O 192.168.1.0/24 → SYN scan + OS detection on subnet
- nmap -A -T4 scanme.nmap.org → Aggressive fast scan
- nmap -p 22,80,443 10.0.0.1 → Scan specific ports
- nmap --script vuln 10.0.0.1 → Run vulnerability scripts

UNIT III KEY TAKEAWAYS

✔ Passive recon: WHOIS, Netcraft, theHarvester	✔ Nmap is the standard tool for network scanning
✔ Active recon: port scanning, ping sweeps, DNS queries	✔ Vulnerability scanning follows port scanning
✔ DNS zone transfers can expose entire network maps	✔ Nmap NSE scripts automate vulnerability detection

UNIT IV INTRUSION DETECTION

4.1 Intrusion Detection Systems – Overview

An Intrusion Detection System (IDS) is a device or software application that monitors a network or system for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator or collected centrally using a SIEM (Security Information and Event Management) system.

IDS Detection Methods

Method	Description	Examples
Signature-Based (Misuse Detection)	Compares activity against a database of known attack signatures. Fast and accurate for known threats; cannot detect zero-days.	Snort, Suricata
Anomaly-Based	Establishes a baseline of normal behaviour; alerts on deviations. Detects unknown attacks; higher false positive rate.	ML-based IDS
Stateful Protocol Analysis	Compares observed protocol behaviour against predetermined profiles of acceptable use.	Enterprise IDS

4.2 Host-Based Intrusion Detection (HIDS)

HIDS monitors and analyses the internals of a computing system. It runs on individual hosts and examines log files, file system integrity, running processes, and system calls.

How HIDS Works

- Monitors system call activity and logs
- Checks file integrity using cryptographic hashes (MD5, SHA-256)
- Analyses user login/logout events and privilege escalations
- Monitors registry changes (Windows) and cron job modifications
- Detects rootkits by comparing kernel data structures

Advantages and Disadvantages

Advantages	Disadvantages
Can detect attacks that don't traverse network	Uses host CPU/memory resources
Monitors encrypted traffic after decryption	Must be installed on every monitored host
Provides forensic evidence	Can be disabled by attacker with root access
No network modifications needed	Does not detect network-wide attacks

■ *Popular HIDS tools: OSSEC, Tripwire, AIDE (Advanced Intrusion Detection Environment), Wazuh*

4.3 Network-Based Intrusion Detection (NIDS)

NIDS captures and analyses network packets in real time to detect suspicious patterns. It operates at the network level and monitors traffic flowing across a network segment.

NIDS Placement

- Before the firewall – catches all external attack attempts
- After the firewall – monitors traffic that passed firewall rules
- On DMZ segment – monitors traffic to publicly accessible servers
- On internal network segments – detects lateral movement

Advantages and Disadvantages

Advantages	Disadvantages
One sensor protects entire network segment	Cannot inspect encrypted traffic
Transparent to users and applications	High traffic volumes cause packet drops
Attacker cannot easily disable it	Cannot analyse host-level events
Detects network-wide attack patterns	Susceptible to evasion via fragmentation

4.4 Distributed / Hybrid IDS

A Distributed IDS (DIDS) combines multiple HIDS and NIDS sensors deployed across an enterprise, feeding data to a centralised management console for correlation and analysis.

Architecture Components

Sensors/Agents

Collect raw data from hosts and network segments

Local Analysers

Process data locally and generate alerts

Central Manager

Correlates alerts from multiple sensors; provides unified view

Management Console

Allows administrators to configure, monitor, and respond

■ *SIEM (Security Information and Event Management) platforms like Splunk, IBM QRadar, and Microsoft Sentinel implement distributed IDS concepts at enterprise scale.*

4.5 IDMEF & Honeypots

Intrusion Detection Message Exchange Format (IDMEF)

IDMEF (RFC 4765) is a standardised XML-based format for representing and exchanging intrusion detection alerts between IDS sensors, analysers, and management consoles. It ensures interoperability between products from different vendors.

Key IDMEF Fields

Field	Description
Classifier	Type and name of the detected attack
Assessment	Severity, confidence, and impact of the alert
Source	Origin of the attack (IP, port, protocol)
Target	Intended victim of the attack
AdditionalData	Supplementary information (log excerpts, payloads)

Honeypots

A honeypot is a deliberately vulnerable decoy system designed to lure attackers, study their techniques, and detect intrusions. It has no production value, so any interaction with it is inherently suspicious.

Type	Description	Examples
Low-Interaction Honeypot	Simulates limited services; low risk; easy to deploy	Honeyd, KFSensor
High-Interaction Honeypot	Full operating system; real services; detailed intelligence; higher risk	Specter, Honeynet
Research Honeypot	Used to study attacker behaviour and develop defences	Honeynet Project systems
Production Honeypot	Deployed alongside production systems to detect and deflect attacks	Commercial products

4.6 Snort – Example IDS

Snort is a free, open-source NIDS/NIPS (Network Intrusion Detection and Prevention System) developed by Martin Roesch in 1998, now maintained by Cisco. It uses a rule-based language to define what constitutes suspicious traffic.

Snort Architecture

Packet Decoder

Captures packets from network interfaces

Preprocessors

Normalise/reassemble packets before analysis (HTTP normaliser, frag3)

Detection Engine

Matches packets against rule set using pattern-matching algorithms

Output Plugins

Log alerts to console, syslog, database, unified2 binary format

Rules

Text-based signatures defining attack patterns

Snort Rule Structure

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"HTTP attack"; content:"../"; sid:1001;
rev:1;)
```

Part	Description
Action	alert / log / pass / drop / reject – what to do when rule matches
Protocol	tcp, udp, icmp, ip
Source	Source IP and port ($EXTERNAL_NET any)
Direction	-> (one-way) or <> (bidirectional)
Destination	Destination IP and port ($HOME_NET 80)
Options	msg (message), content (payload match), sid (rule ID), rev (revision)

Snort Operating Modes

Sniffer Mode

Reads packets and prints to console (snort -v)

Packet Logger Mode

Logs packets to disk for analysis (snort -l ./log)

NIDS Mode

Applies rule sets and generates alerts (snort -c snort.conf -A console)

UNIT IV KEY TAKEAWAYS

✔ IDS: signature-based vs anomaly-based detection	✔ IDMEF standardises IDS alert formats (RFC 4765)
✔ HIDS monitors individual hosts; NIDS monitors network	✔ Honeypots lure attackers and gather intelligence

✔ Distributed IDS correlates alerts from many sensors	✔ Snort uses rule-based detection; free and widely used

UNIT V INTRUSION PREVENTION

5.1 Need for Firewalls

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It establishes a barrier between a trusted internal network and untrusted external networks such as the Internet.

Why Firewalls are Necessary

- Prevent unauthorised access to internal networks
- Block known malicious IP addresses and traffic patterns
- Enforce network segmentation (separate DMZ, internal, external zones)
- Log all traffic for security auditing and forensics
- Protect against denial-of-service attacks
- Control which applications can access the Internet
- Comply with regulatory security requirements

5.2 Firewall Characteristics, Access Policy & Types

Firewall Characteristics

All traffic passes through it

Acts as a chokepoint for network traffic

Only authorised traffic allowed

Based on predefined security policy

Immune to penetration

Runs hardened, minimal OS

Audit and logging capability

Records all connection attempts

Access Policy Considerations

A firewall's effectiveness depends on its access policy – the rules determining what traffic is allowed or denied. Two primary philosophies:

Default-Deny (Whitelist)

Block everything; allow only explicitly permitted traffic. Most secure approach. Used in high-security environments.

Default-Allow (Blacklist)

Allow everything; block only known bad traffic. Easier to manage; less secure.

Types of Firewalls

Type	Description	OSI Layer
Packet Filtering Firewall	Examines packets at the network layer (IP/TCP/UDP headers). Stateless; fast; limited protection. Based on ACLs.	Layer 3/4
Stateful Inspection Firewall	Tracks the state of network connections. Understands TCP session context. Most common type.	Layer 3/4
Application Layer Firewall (Proxy)	Inspects application-layer data (HTTP, FTP, DNS). Deep packet inspection. Can detect application-level attacks.	Layer 7
Next-Generation Firewall (NGFW)	Combines stateful inspection with deep packet inspection, application awareness, IPS, SSL inspection, and threat intelligence.	All Layers
Web Application Firewall (WAF)	Specifically protects web applications; filters HTTP/HTTPS; defends against OWASP Top 10.	Layer 7
Circuit-Level Gateway	Works at session layer; monitors TCP handshaking; does not inspect payload content.	Layer 5

5.3 Firewall Basing, Location & Configuration

Firewall Basing Options

Dedicated Hardware Appliance

Purpose-built physical device; high performance; used in enterprise environments (Cisco ASA, Palo Alto, Fortinet).

Software Firewall

Runs on general-purpose OS; lower cost; suitable for SMBs (pfSense, iptables, Windows Defender Firewall).

Cloud-Based Firewall (FWaaS)

Firewall-as-a-Service; managed by cloud provider; scales with traffic (Zscaler, AWS Network Firewall).

Firewall Location & Configuration

Firewall placement determines which traffic is inspected and which zones are protected. Common configurations:

Configuration	Description
Single Firewall	Divides network into Internet, DMZ, and internal zones. Simple; cost-effective; suitable for SMBs.
Screened Subnet (DMZ)	Two firewalls: outer firewall protects DMZ; inner firewall protects internal LAN. Provides two layers of defence.
Dual-Homed Host	Single computer with two NICs; acts as gateway between two networks without IP routing.
Bastion Host	Hardened server placed in DMZ; provides specific public-facing services; minimally configured.

■ *The DMZ (Demilitarised Zone) architecture is the standard for organisations hosting public-facing services (web servers, mail servers). It isolates these from the trusted internal network.*

5.4 Intrusion Prevention Systems (IPS)

An IPS is an active security control that sits inline with network traffic and can not only detect threats (like an IDS) but also automatically take action to block or prevent malicious traffic in real time.

IDS vs IPS Comparison

Feature	IDS	IPS
Deployment	Out-of-band (passive)	Inline (active)
Response	Alerts only	Alerts + blocks/drops
Traffic Impact	No impact on traffic flow	Slight latency added
False Positive Risk	Generates false alarms	Can block legitimate traffic
Placement	Mirror/SPAN port	Inline between segments

Types of IPS

Type	Description
Network-Based IPS (NIPS)	Inline between network segments; analyses all passing traffic.
Host-Based IPS (HIPS)	Installed on individual hosts; monitors and controls process behaviour.
Wireless IPS (WIPS)	Monitors Wi-Fi networks for rogue access points and wireless attacks.
Network Behaviour Analysis (NBA)	Detects anomalous traffic patterns; effective against DDoS and new malware.

IPS Response Actions

- Drop malicious packets silently
- Send TCP RST to terminate malicious connections
- Block source IP address for a configurable period
- Rate-limit traffic from suspicious sources
- Quarantine infected hosts via VLAN reassignment
- Generate alerts and log evidence for forensics

5.5 Unified Threat Management (UTM)

Unified Threat Management (UTM) is an approach to network security where a single hardware or software appliance provides multiple security functions. UTM devices consolidate firewall, IDS/IPS, VPN, antivirus, content filtering, and more into a single platform.

UTM Components

Component	Function
Firewall	Stateful packet inspection and NAT
IDS/IPS	Signature and anomaly-based intrusion detection/prevention
VPN Gateway	IPsec and SSL VPN for remote access and site-to-site tunnels
Antivirus/Anti-malware	Real-time scanning of files traversing the gateway
Web Content Filter	Blocks access to inappropriate or malicious websites by category
Anti-spam	Filters inbound email for spam, phishing, and malware
Application Control	Identifies and controls applications regardless of port
Data Loss Prevention (DLP)	Prevents sensitive data from leaving the organisation
SSL Inspection	Decrypts and inspects HTTPS traffic for hidden threats

Example UTM Products

Product	Key Features
Fortinet FortiGate	Industry leader; FortiOS; comprehensive security fabric; high throughput
Sophos XG Firewall	Synchronised security with endpoint; deep learning-based threat detection
Check Point	Unified security management; ThreatCloud intelligence; SandBlast zero-day
Palo Alto Networks	Next-Gen firewall with WildFire sandboxing and Panorama management
pfSense + Snort	Open-source UTM solution; cost-effective for SMBs
Cisco Firepower	Cisco's NGFW/IPS platform; integrated with Talos threat intelligence

Advantages of UTM

- Simplified management through a single console
- Reduced cost compared to deploying separate point solutions
- Consistent security policies across all security functions
- Faster deployment and easier updates
- Integrated reporting and log correlation

Disadvantages of UTM

- Single point of failure if device fails
- Performance bottleneck when all features are enabled
- Less specialised than dedicated point solutions
- 'Jack of all trades, master of none' concern for high-security environments

5.6 Review Questions & Summary

Review Questions

- 1. What is the CIA Triad? Why is it fundamental to information security?
- 2. Differentiate between active and passive reconnaissance with examples.
- 3. Explain the OWASP Top 10 and why it is important for web developers.
- 4. Compare and contrast HIDS and NIDS. In what scenarios would you deploy each?
- 5. What is the difference between an IDS and an IPS? Can an IPS replace a firewall?
- 6. Describe the screened subnet (DMZ) firewall architecture.
- 7. Explain how Snort rules work. Write a sample rule to detect an ICMP ping scan.
- 8. What is a honeypot? Differentiate between high-interaction and low-interaction honeypots.
- 9. Explain social engineering attacks. Why are they difficult to prevent technically?
- 10. What is UTM? List its components and compare it with deploying individual security tools.
- 11. Explain the Nmap -sS (SYN scan) technique. Why is it called a stealth scan?
- 12. What are the provisions of Section 66F of the Indian IT Act?

UNIT V KEY TAKEAWAYS

✔ Firewalls are essential chokepoints in network security	✔ IPS is inline and actively blocks; IDS is passive
✔ Packet filter → Stateful → NGFW: increasing sophistication	✔ UTM consolidates multiple security functions
✔ DMZ architecture isolates public-facing servers	✔ Palo Alto, Fortinet, Sophos lead the UTM/NGFW market

END OF STUDY MATERIAL

All five units covered | Prepared for academic reference