

Introduction to Cyber Security

Introduction to Cyber Security – Study Notes

1. What Is Cyber Security?

- **Definition:** The practice of protecting computers, networks, programs, and data from unauthorized access, damage, or theft.
 - **Goal:** Ensure confidentiality, integrity, and availability of information (the **CIA Triad**).
-

2. Core Concepts

Concept	Description	Typical Controls
Confidentiality	Prevents unauthorized disclosure of data.	Encryption, access controls, VPNs
Integrity	Guarantees that data is accurate and unaltered.	Checksums, digital signatures, version control
Availability	Ensures that systems and data are accessible when needed.	Redundancy, load balancing, DDoS mitigation
Authentication	Verifies the identity of a user or device.	Passwords, biometrics, multi-factor authentication (MFA)
Authorization	Determines what an authenticated entity is allowed to do.	Role-based access control (RBAC), policy engines
Non-repudiation	Prevents denial of actions performed.	Audit logs, digital signatures

3. Threat Landscape

Threat Type	Example	Impact
Malware	Viruses, ransomware, trojans	Data loss, system disruption
Phishing	Deceptive emails, fake login pages	Credential theft
Man-in-the-Middle (MitM)	Intercepted network traffic	Data interception, session hijacking

Introduction to Cyber Security

Threat Type	Example	Impact
Denial of Service (DoS/DDoS)	Flooded servers	Service outage
Insider Threats	Disgruntled employee, accidental leak	Data breach, sabotage
Zero-Day Exploits	Unpatched software vulnerabilities	Remote code execution, privilege escalation

4. Key Security Domains

1. Network Security

- Firewalls, intrusion detection/prevention systems (IDS/IPS)
- Secure protocols (TLS, SSH)
- Network segmentation & VLANs

2. Endpoint Security

- Antivirus/anti-malware, host-based firewalls
- Device encryption, patch management

3. Application Security

- Secure coding practices (input validation, output encoding)
- Web application firewalls (WAF)
- Regular code reviews & penetration testing

4. Identity & Access Management (IAM)

- Centralized directory services (Active Directory, LDAP)
- MFA, Single Sign-On (SSO)

5. Data Security

- Encryption at rest & in transit
- Data loss prevention (DLP) solutions
- Backup & disaster recovery planning

Introduction to Cyber Security

6. Cloud Security

- Shared responsibility model
- Cloud Access Security Brokers (CASB)
- Secure configuration of services (IAM, storage buckets)

7. Operational Security (OpSec)

- Security policies & procedures
- Incident response planning
- Security awareness training

5. Common Security Frameworks & Standards

Framework / Standard	Primary Focus	Typical Use
ISO/IEC 27001	Information security management system (ISMS)	Enterprise-wide governance
NIST Cybersecurity Framework (CSF)	Identify?Protect?Detect?Respond?Recover	U.S. federal & private sector
CIS Controls	Prioritized set of best practices	Quick-start hardening