UEAMPUS
STUDY GUIDE

Level 5 Network Security

uecampus.com/

First published in 2026 by UE Campus

Unit specifications can be found on the UE Campus Portal: https://uecampus.com/

Contents

Using your Study Guide

Welcome to the study guide, designed to support you in completing your Level 5 Diploma in Information Technology.

This study guide follows the order of the syllabus, which is the basis for your studies. Each chapter starts by listing the syllabus learning outcomes covered and the assessment criteria.

Level 5 Units

The study guide includes a number of features to enhance your studies:

	**'Over to you:'** activities for you to apply what you have learned.
	**'Industry Insights:'** discover up-to-date trends, expert opinions, and real-world examples from the cybersecurity industry.
	**'Did you know?'** highlights interesting facts or surprising information to deepen your understanding.
	**'Case studies:'** realistic scenarios to reinforce and test your understanding.
	**'Revision on the go:'** use your phone camera to capture key pieces of learning and save them as revision notes.
	'Need to know:' key pieces of information highlighted in the text.
	**'Examples:'** illustrating points made in the text to show how it works in practice.

Note: Website addresses current as of March 2026.

Level 5 Network Security

About this unit

This unit aims to provide you with knowledge of network security issues in a networked environment and the processes for preventing and detecting common security incidents. Cybersecurity is one of the most critical and rapidly growing fields in information technology – every organisation, from small businesses to multinational corporations and government agencies, depends on secure networks to protect their data, operations, and reputation.

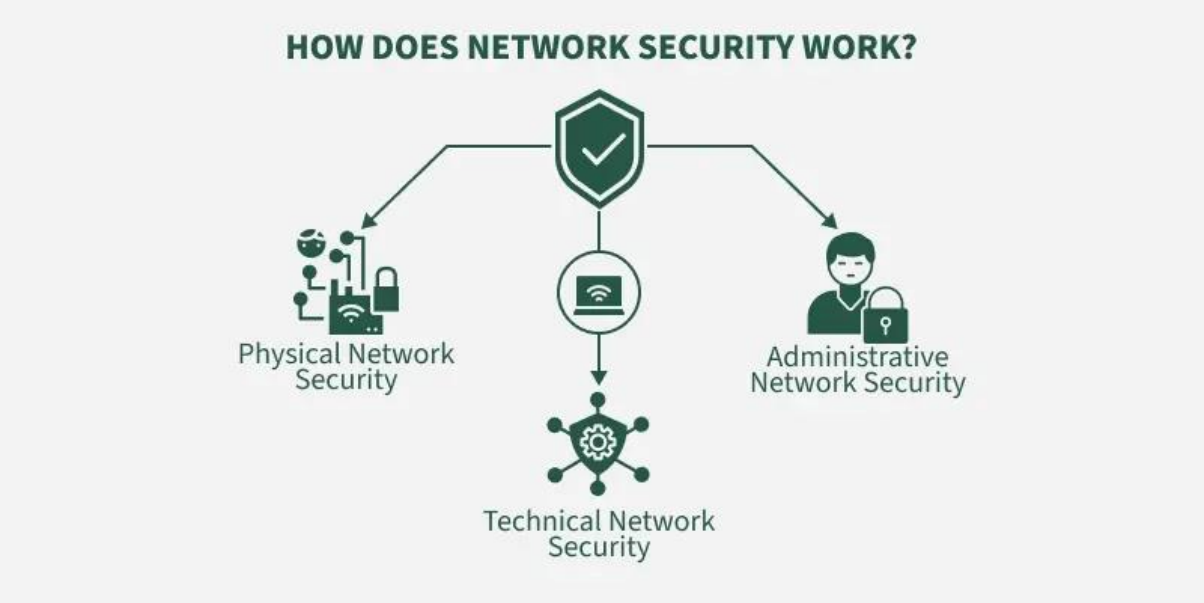
You will study the factors that affect network and computer security, identify common security issues, and analyse the emerging role of artificial intelligence in network defence. You will then examine methods of maintaining security, including authentication mechanisms, attack types and malicious codes, security tools, defensive practices across multiple domains (networks, remote access, email, web, wireless), and intrusion detection systems. The unit also covers physical security and disaster recovery planning.

By the end of this unit, you will understand the threat landscape, be able to select appropriate security measures for different scenarios, and appreciate the critical role that network security plays in every modern organisation.

Chapter One – Computer Network Security

Introduction

This chapter establishes the foundational understanding of computer network security. You will analyse the factors that make networks vulnerable, identify the common security issues that organisations face, and explore how artificial intelligence is transforming the way networks are defended. The cybersecurity landscape is constantly evolving as threat actors develop increasingly sophisticated methods of attack, making continuous learning essential for any IT professional.



Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand computer network security.**

Assessment Criteria

1.1 Analyse the factors that affect network and computer security.

1.2 Identify common security issues in a networked environment.

1.3 Analyse the role that artificial intelligence (AI) could have in defending networks.

1.1 Factors that affect network and computer security

Over to you – Video Watch: Network Security Fundamentals

Watch this YouTube video:

Title: Network Security Tutorial – Introduction to Network Security – Edureka

Duration: 28:07

Link: https://www.youtube.com/watch?v=UpVDuiVDm7E

After watching, list the five most important security threats discussed. For each, describe one countermeasure that could reduce the risk.

Understanding Security Threats

Network security is the practice of protecting the integrity, confidentiality, and availability of computer networks and data using a combination of technologies, policies, and practices. The CIA triad – Confidentiality, Integrity, and Availability – is the foundational model for information security:

- Confidentiality – ensuring that information is accessible only to those authorised to access it. Breaches of confidentiality include data theft, unauthorised access, and eavesdropping.
- Integrity – ensuring that information has not been altered or tampered with by unauthorised parties. Integrity violations include data modification, man-in-the-middle attacks, and file corruption.
- Availability – ensuring that information and systems are accessible to authorised users when needed. Availability threats include denial-of-service (DoS) attacks, hardware failure, and ransomware that encrypts systems.

Factors Affecting Network Security

Multiple factors influence the security posture of a network:

Human Factors

- Social engineering – manipulating people into revealing confidential information or performing actions that compromise security. Phishing, pretexting, baiting, and tailgating are common social engineering techniques.
- Insider threats – employees, contractors, or partners who intentionally or accidentally compromise security. Studies consistently show that insider threats account for a significant proportion of data breaches.
- Security awareness – the level of security knowledge and culture among staff. Organisations with strong security awareness training experience significantly fewer incidents.
- Password hygiene – weak, reused, or shared passwords remain one of the most common attack vectors. Enforcing strong password policies and multi-factor authentication dramatically reduces risk.

Technical Factors

- Network architecture – the design of the network, including segmentation, perimeter defences, and the principle of least privilege. A flat network with no segmentation is far more vulnerable than a properly segmented one.
- Software vulnerabilities – bugs and flaws in operating systems, applications, and firmware that can be exploited by attackers. Regular patching and updating is essential.
- Encryption – the use (or lack) of encryption for data at rest and in transit. Unencrypted data is vulnerable to interception and theft.
- Access control – how users, devices, and applications are authenticated and authorised. Windows Server access control, for example, uses Active Directory, Group Policy, NTFS permissions, and role-based access control (RBAC).
- Network devices – routers, switches, firewalls, and wireless access points all have security configurations that must be managed. Default credentials, unpatched firmware, and misconfigured access control lists (ACLs) are common weaknesses.

Environmental and Organisational Factors

- Physical security – physical access to network equipment, servers, and data centres must be controlled. An attacker with physical access can bypass most logical security controls.
- Regulatory compliance – organisations must comply with data protection regulations (UK GDPR, Data Protection Act 2018) and industry-specific standards (PCI DSS for payment card data, ISO 27001 for information security management).
- Budget and resources – security investments compete with other business priorities. Under-resourced security teams and outdated tools increase vulnerability.

- Business continuity planning – the presence (or absence) of disaster recovery plans, backup strategies, and incident response procedures affects an organisation's ability to recover from security incidents.

Network Security Topologies

The way a network is structured has direct security implications:

- Perimeter-based security – the traditional approach using firewalls and DMZs (demilitarised zones) to separate internal and external networks. Still relevant but insufficient on its own.
- Defence in depth – multiple layers of security controls (network, host, application, data) so that if one layer fails, others still protect the system.
- Zero Trust architecture – the modern approach that assumes no user or device is trusted by default, even if inside the network perimeter. Every access request is verified: 'never trust, always verify'. Zero Trust is increasingly adopted by organisations migrating to cloud services.
- Micro-segmentation – dividing the network into very small, isolated segments, limiting an attacker's ability to move laterally after gaining initial access.

Did you know?

According to IBM's 2024 Cost of a Data Breach Report, the average cost of a data breach globally was $4.88 million – the highest ever recorded. The UK average was £3.58 million. Healthcare was the most expensive industry for data breaches for the 14th consecutive year. Organisations that extensively used security AI and automation saved an average of $2.22 million per breach compared to those that did not use these technologies.

Over to you – Security Assessment

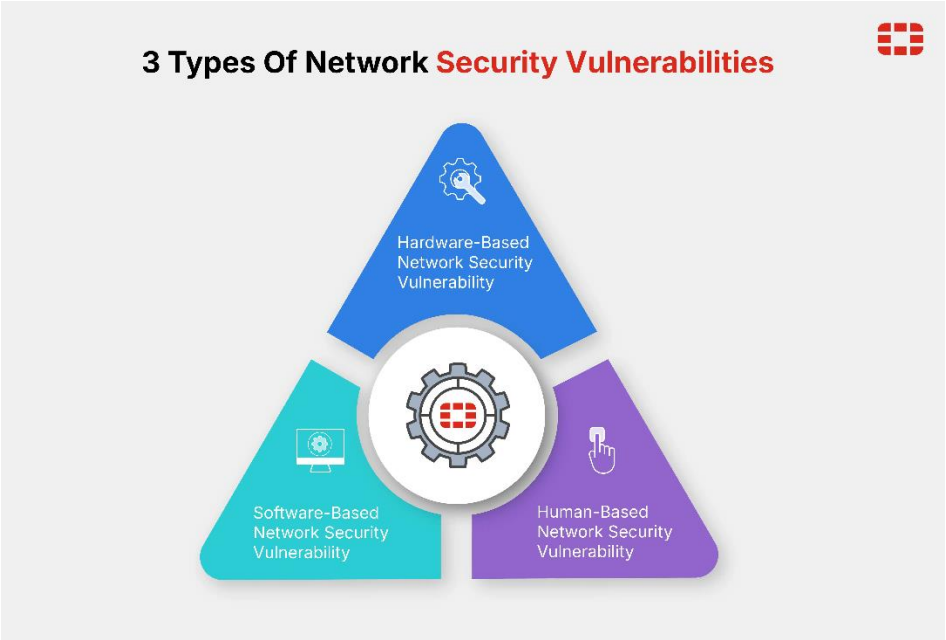
Conduct a high-level security assessment of your home or university network. Identify: (1) at least five potential vulnerabilities (consider human, technical, and physical factors), (2) the potential impact of each vulnerability being exploited, and (3) one recommended countermeasure for each. Present your findings in a vulnerability assessment table with columns for vulnerability, risk level (High/Medium/Low), potential impact, and recommended countermeasure.

1.2 Common security issues in a networked environment

This section identifies the most common security issues that organisations face in today's interconnected world. Understanding these issues is the first step toward defending against them.

Network-Level Security Issues

- Unauthorised access – gaining access to a network, system, or data without permission. This can occur through stolen credentials, exploitation of vulnerabilities, or social engineering.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) – overwhelming a network or service with traffic, making it unavailable to legitimate users. DDoS attacks use botnets (networks of compromised devices) to amplify the attack.
- Man-in-the-Middle (MitM) attacks – an attacker intercepts communication between two parties, potentially eavesdropping on or modifying the data. Common on unsecured Wi-Fi networks.
- Packet sniffing – capturing and analysing network traffic to extract sensitive information such as passwords, session tokens, or personal data. Tools like Wireshark can capture packets on a network.
- DNS spoofing/poisoning – corrupting DNS cache entries to redirect users to malicious websites.
- ARP spoofing – sending falsified ARP messages to link the attacker's MAC address with a legitimate IP address, enabling traffic interception.



Wireless Security Issues

- Rogue access points – unauthorised wireless access points connected to the network, potentially providing attackers with a backdoor.

- Evil twin attacks – a malicious access point that mimics a legitimate Wi-Fi network to trick users into connecting, enabling traffic interception.
- WPA/WPA2 vulnerabilities – while WPA3 is the current standard, many networks still use WPA2, which has known vulnerabilities (KRACK attack).
- War driving – scanning for and mapping wireless networks while driving, identifying vulnerable networks.

Email Security Issues

- Phishing – fraudulent emails designed to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Spear phishing targets specific individuals; whaling targets senior executives.
- Business Email Compromise (BEC) – attackers impersonate a trusted colleague or business partner to trick victims into transferring money or sensitive data.
- Email spoofing – sending emails with a forged sender address to appear as a trusted source.
- Malicious attachments – files containing malware delivered via email, often disguised as invoices, documents, or other business files.

Web Security Issues

- Cross-Site Scripting (XSS) – injecting malicious JavaScript into web pages viewed by other users.
- SQL injection – inserting malicious SQL queries through web forms to access or manipulate the database.
- Cross-Site Request Forgery (CSRF) – tricking a user's browser into making unauthorised requests to a web application where they are authenticated.
- Insecure APIs – poorly secured application programming interfaces that expose sensitive data or functionality.
- Certificate/TLS issues – expired, misconfigured, or absent SSL/TLS certificates that leave communications unencrypted.

Remote Access Security Issues

- VPN vulnerabilities – misconfigured or unpatched VPN servers can provide attackers with a direct path into the internal network.
- Remote Desktop Protocol (RDP) exposure – RDP services exposed to the internet are frequently targeted by brute-force and credential stuffing attacks.
- Weak remote authentication – remote access without multi-factor authentication is highly vulnerable to credential theft.
- Bring Your Own Device (BYOD) risks – personal devices connecting to the corporate network may lack security controls, creating vulnerabilities.

Transmission and Storage Media Security

- Data in transit – information moving across the network can be intercepted if not encrypted. TLS/SSL for web traffic, IPsec for VPN tunnels, and SSH for remote management are essential.
- Data at rest – stored data (on disks, databases, backups, USB drives) should be encrypted using AES-256 or similar strong encryption.
- Removable media – USB drives, external hard disks, and optical media can introduce malware or be used to exfiltrate data. Policies should restrict or monitor removable media use.

Industry Insight – The OWASP Top 10

The OWASP (Open Web Application Security Project) Top 10 is the most widely referenced document for web application security. The 2021 edition lists: Broken Access Control (#1), Cryptographic Failures (#2), Injection (#3), Insecure Design (#4), Security Misconfiguration (#5), Vulnerable and Outdated Components (#6), Identification and Authentication Failures (#7), Software and Data Integrity Failures (#8), Security Logging and Monitoring Failures (#9), and Server-Side Request Forgery (#10). Every IT professional should be familiar with these risks.

Visit: https://owasp.org/www-project-top-ten/

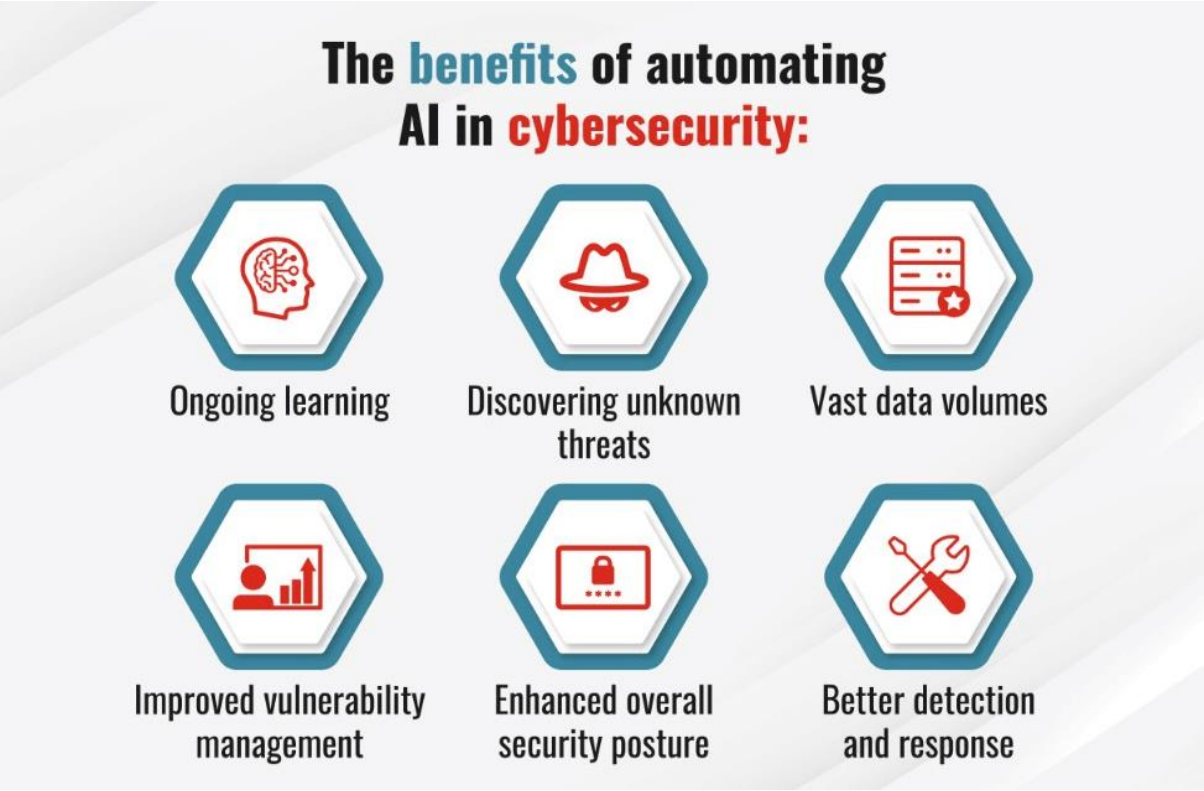
Case Study – Investigating a Security Incident

A medium-sized law firm reports that several staff members have received convincing emails appearing to come from the managing partner, requesting urgent bank transfers. Two staff members clicked the links in the emails and entered their Office 365 credentials on what turned out to be a phishing site. The attackers have now accessed the firm's email system and are sending further phishing emails from compromised accounts.

Task: Analyse this incident by: (1) identifying the type(s) of attack involved, (2) explaining how the attack succeeded (what security weaknesses were exploited), (3) listing the immediate response actions the firm should take, (4) recommending five security measures that would prevent a similar attack in the future, and (5) discussing the potential regulatory implications under UK GDPR. Write approximately 600 words.

1.3 The role of AI in defending networks

Artificial intelligence is rapidly transforming cybersecurity, offering powerful new capabilities for defending networks against increasingly sophisticated threats. As attack techniques become more automated and complex, AI-driven defence systems are becoming essential components of modern security architectures.



Over to you – Video Watch: AI in Cybersecurity

Watch this YouTube video:

Title: How AI is Changing Cybersecurity – IBM Technology

Duration: 8:12

Link: https://www.youtube.com/watch?v=6PMkAdwCVaU

After watching, list three specific ways AI can improve network security. For each, explain how it improves upon traditional (non-AI) approaches.

AI-Powered Threat Detection

Traditional security tools rely on signature-based detection – matching network activity against a database of known attack patterns. This approach fails against zero-day attacks (previously unknown threats) and sophisticated attacks that evade known signatures. AI-based systems use machine learning algorithms to analyse vast amounts of network data and identify anomalies that may indicate a threat:

- Behavioural analysis – AI models learn the normal behaviour patterns of users, devices, and applications on the network. When activity deviates significantly from the baseline (e.g. a user suddenly downloading large volumes of data at 3 AM, or an IoT device communicating with an unusual external server), the system raises an alert.
- Anomaly detection – unsupervised machine learning algorithms identify unusual patterns in network traffic, system logs, and user activity without needing pre-defined rules.
- Natural Language Processing (NLP) – AI analyses the text of emails, messages, and web pages to identify phishing attempts, social engineering, and malicious content with greater accuracy than rule-based filters.

AI for Automated Response

Security Orchestration, Automation, and Response (SOAR) platforms use AI to automate incident response:

- Automated containment – when a threat is detected, AI can automatically isolate the affected device or network segment, blocking the attacker's lateral movement before a human analyst responds.
- Automated triage – AI prioritises security alerts based on severity, affected assets, and context, reducing the workload on security analysts (who may face thousands of alerts daily).
- Playbook execution – AI follows pre-defined incident response playbooks, executing standard procedures (blocking IP addresses, resetting credentials, quarantining files) in seconds rather than hours.

AI in Vulnerability Management

AI helps organisations manage vulnerabilities more effectively:

- Predictive vulnerability scoring – AI predicts which vulnerabilities are most likely to be exploited, enabling organisations to prioritise patching based on actual risk rather than just CVSS scores.
- Attack surface monitoring – AI continuously scans and maps the organisation's digital footprint, identifying exposed assets, misconfigured services, and shadow IT.
- Threat intelligence analysis – AI processes and correlates threat intelligence feeds from multiple sources, identifying relevant threats faster than human analysts.

Challenges and Limitations of AI in Security

- Adversarial AI – attackers are also using AI to create more convincing phishing emails, generate deepfakes, automate attacks, and evade AI-based detection systems. This creates an AI-vs-AI arms race.
- False positives – AI systems can generate false positive alerts, overwhelming security teams. Balancing sensitivity (catching threats) with specificity (avoiding false alarms) is an ongoing challenge.

- Data quality and bias – AI models are only as good as the data they are trained on. Biased or incomplete training data can lead to blind spots.
- Explainability – complex AI models (especially deep learning) can be difficult to interpret. Security analysts need to understand why a system flagged an alert in order to respond appropriately.
- Skills gap – implementing and managing AI security tools requires specialists with expertise in both cybersecurity and machine learning, a combination that is in very short supply.

Did you know?

According to IBM's 2024 Cost of a Data Breach Report, organisations that extensively used security AI and automation identified and contained breaches 108 days faster than those that did not – and saved an average of $2.22 million per breach. Despite these benefits, only 28% of organisations reported extensive use of AI in their security operations, indicating significant room for growth.

Over to you – AI Security Research

Research one commercial AI-powered cybersecurity product (e.g. CrowdStrike Falcon, Darktrace, Microsoft Sentinel, or Palo Alto Cortex XDR). Write a 400-word evaluation covering: (1) what AI/ML techniques it uses, (2) what security functions it performs (detection, response, prediction), (3) its key strengths and limitations, and (4) the types of organisations it is best suited for. Include references to the vendor's documentation.

Reading List

- Ciampa, M. (2024). *CompTIA Security+ Guide to Network Security Fundamentals*. 8th edn. Boston: Cengage.
- Conklin, W.A. & White, G.B. (2023). *Principles of Computer Security*. 7th edn. New York: McGraw-Hill.
- Kim, D. & Solomon, M.G. (2024). *Fundamentals of Information Systems Security*. 5th edn. Burlington, MA: Jones & Bartlett Learning.
- Pfleeger, C.P. & Pfleeger, S.L. (2023). *Security in Computing*. 6th edn. Upper Saddle River, NJ: Pearson.
- Stallings, W. (2024). *Network Security Essentials: Applications and Standards*. 8th edn. Harlow: Pearson.
- Stewart, J.M. (2024). *CompTIA Security+ Study Guide: Exam SY0-701*. 9th edn. Indianapolis, IN: Sybex/Wiley.

Summary

In this chapter, you have developed a comprehensive understanding of computer network security. You have analysed the human, technical, environmental, and organisational factors that affect security, including the CIA triad, social engineering, network architecture, and regulatory compliance. You have identified common security issues across multiple domains: network-level attacks, wireless vulnerabilities, email threats, web application risks, remote access weaknesses, and storage media concerns. You have also analysed the transformative role of AI in network defence, including behavioural analysis, automated response, and vulnerability management, while acknowledging the challenges of adversarial AI and false positives.

Chapter Two – Methods of Maintaining Computer Security

Introduction

This chapter examines the practical methods and tools used to maintain computer and network security. You will study authentication mechanisms, understand the types of attacks and malicious code you need to defend against, learn to select appropriate security tools, evaluate defensive practices across networks, remote access, email, web, wireless, and messaging systems, and analyse the differences between network-based and host-based intrusion detection systems. This chapter also covers physical security and disaster recovery.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand methods of maintaining computer security.**

Assessment Criteria

2.1 Analyse the strengths and weaknesses of different methods of authentication.

2.2 Analyse the nature of different types of attack and malicious codes.

2.3 Select the security tool that is appropriate to the nature of the security issue.

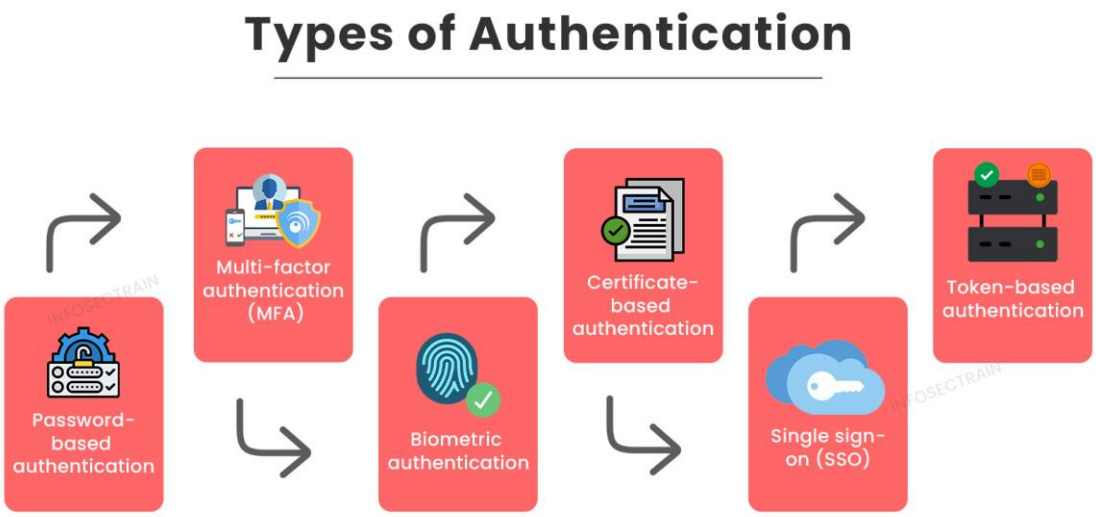
2.4 Evaluate practices that prevent common attacks from intruders (networks, remote access, email, web security, wireless and instant messaging).

2.5 Analyse the differences between network and host intrusion detection systems.

2.1 Authentication methods

Authentication is the process of verifying the identity of a user, device, or system. It answers the question: 'Are you who you claim to be?' Authentication is typically based on one or more of three factors:

- Something you know – passwords, PINs, security questions, passphrases.
- Something you have – smart cards, security tokens, mobile phones (for OTP codes), hardware keys (YubiKey).
- Something you are – biometrics: fingerprints, facial recognition, iris scans, voice recognition.



Password-Based Authentication

Strengths: universally understood, easy to implement, low cost. Weaknesses: vulnerable to brute-force attacks, dictionary attacks, credential stuffing, phishing, and poor user behaviour (weak passwords, password reuse). Best practices: enforce minimum length (12+ characters), require complexity, implement account lockout after failed attempts, use password managers, store passwords as salted hashes (bcrypt, Argon2).

Multi-Factor Authentication (MFA)

MFA requires two or more authentication factors from different categories. For example, a password (something you know) plus a one-time code sent to your phone (something you have). Strengths: dramatically reduces the risk of credential theft; even if a password is compromised, the attacker still needs the second factor. Weaknesses: adds friction to the login process; SMS-based MFA is vulnerable to SIM swapping; push notification fatigue can lead users to approve malicious requests.

Biometric Authentication

Strengths: convenient (you always have your fingerprint/face); difficult to share or steal (compared to passwords); increasingly accurate with modern sensors. Weaknesses: biometric data cannot be changed if compromised (unlike a password); privacy concerns around biometric data collection and storage; can be fooled by sophisticated spoofing (photographs, fake fingerprints); accessibility issues for users with certain disabilities; environmental factors (wet fingers, face masks) can affect accuracy.

Certificate-Based and Token-Based Authentication

Digital certificates (X.509) use public key cryptography to verify identity. Commonly used for website authentication (TLS certificates), VPN authentication, and email signing. Strengths: very strong security; machine-to-machine authentication. Weaknesses: complex to manage (certificate lifecycle, revocation); requires Public Key Infrastructure (PKI). Hardware tokens (YubiKey, FIDO2) provide strong phishing-resistant authentication. Strengths: extremely resistant to phishing (bound to specific domains); small and portable. Weaknesses: can be lost or broken; cost per device.

Single Sign-On (SSO) and Federated Authentication

SSO allows users to authenticate once and access multiple applications without re-entering credentials. Federated authentication (using protocols like SAML, OAuth 2.0, OpenID Connect) allows authentication across different organisations and domains. Strengths: improved user experience; reduced password fatigue; centralised access management. Weaknesses: a compromised SSO account grants access to all connected applications; dependency on the identity provider.

Over to you – Video Watch: Authentication and MFA

Watch this YouTube video:

Title: Multi-Factor Authentication Explained – Professor Messer

Duration: 7:44

Link: https://www.youtube.com/watch?v=HEONJxBKsAw

After watching, create a comparison table evaluating four authentication methods across the criteria of: security strength, user convenience, implementation cost, and common vulnerabilities.

Over to you – Authentication Evaluation

A healthcare organisation with 500 staff needs to upgrade its authentication system. Staff access patient records through a web application. Currently, the system uses only passwords (8-character minimum, no MFA). Recommend an authentication strategy that balances security and usability. Include: (1) the specific authentication methods you recommend and why, (2) how you would implement MFA, (3) how you would handle different user roles

(doctors, nurses, administrators), and (4) compliance considerations under UK GDPR. Write approximately 400 words.

2.2 Types of attack and malicious codes

Understanding the nature and mechanics of different attack types is essential for selecting appropriate defences.

Malware (Malicious Software)

- Virus – malicious code that attaches to a legitimate program or file and replicates when the infected file is executed. Requires user action to spread.
- Worm – self-replicating malware that spreads across networks without user interaction. Can cause massive damage through network congestion and payload delivery (e.g. WannaCry ransomware, 2017).
- Trojan Horse – malware disguised as legitimate software. Does not self-replicate but can open backdoors, steal data, or download additional malware.
- Ransomware – encrypts the victim's files or systems and demands payment for the decryption key. One of the most financially damaging attack types. Variants include crypto-ransomware (encrypts files) and locker ransomware (locks the entire system).
- Spyware – secretly monitors user activity (keystrokes, browsing history, screenshots) and transmits data to the attacker.
- Adware – displays unwanted advertisements, often bundled with free software. Can slow systems and sometimes serve as a vector for more serious malware.
- Rootkit – a stealthy type of malware designed to gain and maintain privileged access while hiding its presence from detection tools.
- Fileless malware – operates entirely in memory without writing files to disk, making it extremely difficult to detect with traditional antivirus tools.

Network Attacks

- Brute-force attacks – systematically trying every possible password combination until the correct one is found. Mitigated by account lockouts, rate limiting, and strong passwords.
- Dictionary attacks – using a pre-compiled list of common passwords and phrases. Faster than brute force but limited to known passwords.
- Credential stuffing – using stolen username/password combinations from previous data breaches to attempt login on other services (exploiting password reuse).
- SQL injection – inserting malicious SQL code through web application inputs to access or manipulate the database.
- Cross-Site Scripting (XSS) – injecting malicious JavaScript into web pages to steal session cookies, redirect users, or capture keystrokes.
- Session hijacking – stealing or forging a session token to impersonate an authenticated user.
- DNS tunnelling – using DNS queries and responses to exfiltrate data or establish command-and-control channels, bypassing traditional security controls.

Advanced Persistent Threats (APTs)

APTs are prolonged, targeted attacks by sophisticated threat actors (often nation-state sponsored) who gain access to a network and remain undetected for extended periods. APTs typically involve multiple stages: initial reconnaissance, initial compromise (often through spear phishing), establishing persistence, lateral movement through the network, data exfiltration, and maintaining access. APTs are among the most dangerous threats because of their stealth, sophistication, and persistence.

Did you know?

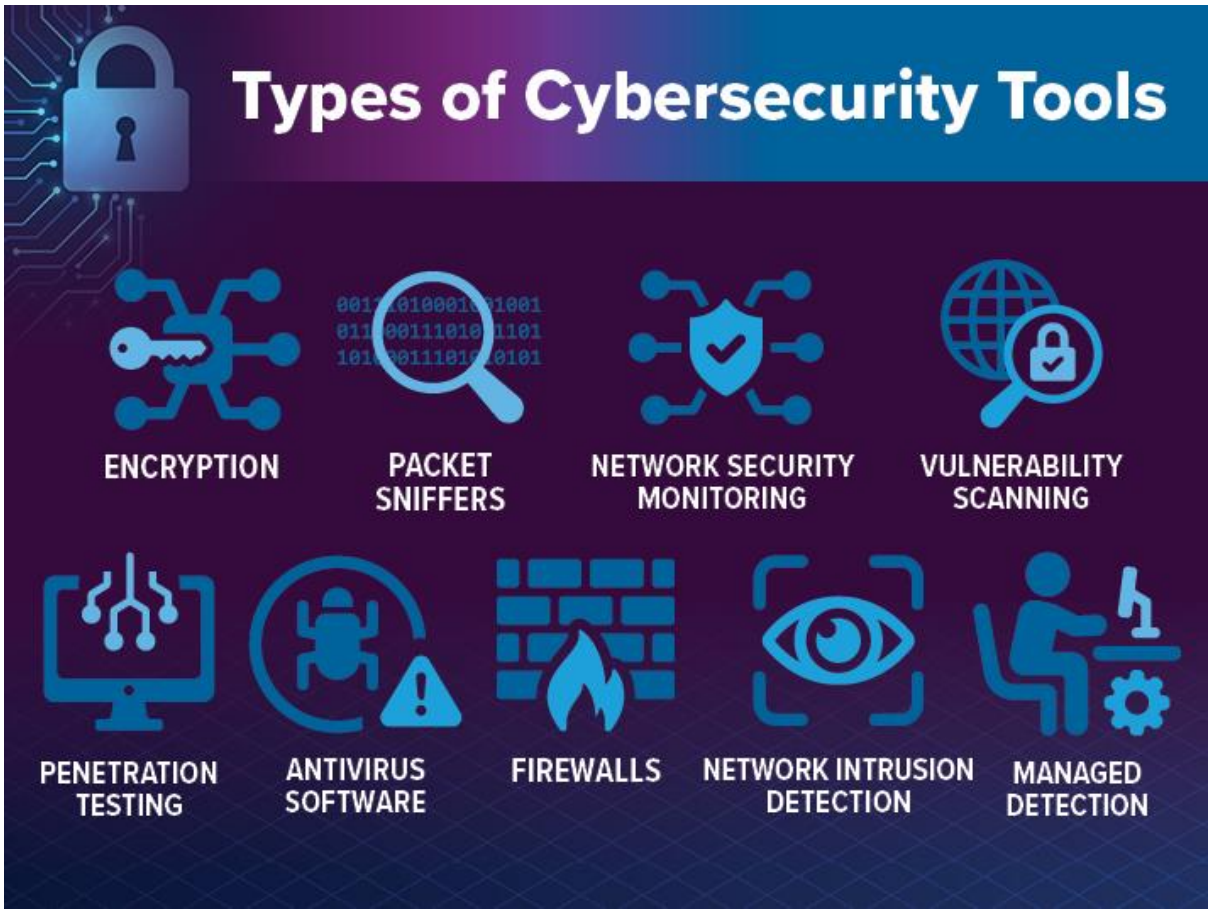
The WannaCry ransomware attack in May 2017 affected over 200,000 computers across 150 countries in a single day. The UK's National Health Service (NHS) was severely impacted, with hospitals forced to cancel operations and divert emergency patients. The attack exploited a Windows vulnerability called EternalBlue, for which Microsoft had released a patch two months earlier – but many NHS systems had not been updated. The incident dramatically highlighted the importance of timely patching and robust backup strategies.

Over to you – Malware Analysis

Choose one major cyberattack from the past five years (e.g. SolarWinds supply chain attack 2020, Colonial Pipeline ransomware 2021, MOVEit vulnerability 2023, or Change Healthcare attack 2024). Research and write a 500-word analysis covering: (1) the type of attack and malware used, (2) how the attackers gained initial access, (3) the impact (financial, operational, reputational), (4) the defensive failures that allowed the attack to succeed, and (5) lessons learned and recommendations.

2.3 Security tools

Selecting the right security tool for the right problem is a critical skill. This section surveys the key categories of security tools and their appropriate applications.



Firewalls

Firewalls control traffic between network segments based on predefined rules. Types include: packet-filtering firewalls (inspect individual packets against ACL rules), stateful inspection firewalls (track the state of active connections), application-layer firewalls / Web Application Firewalls (WAF) (inspect traffic at the application layer, blocking XSS and SQL injection), and next-generation firewalls (NGFW) (combine traditional firewall features with IPS, application awareness, and threat intelligence). Firewalls are appropriate for perimeter defence, network segmentation, and controlling access between zones.

Antivirus / Endpoint Detection and Response (EDR)

Traditional antivirus uses signature-based detection to identify known malware. Modern EDR solutions go further, using behavioural analysis, machine learning, and threat intelligence to detect and respond to advanced threats on endpoints (laptops, desktops, servers). Leading EDR platforms include CrowdStrike Falcon, Microsoft Defender for Endpoint, and SentinelOne. Appropriate for protecting all endpoints against malware, ransomware, and fileless attacks.

Security Information and Event Management (SIEM)

SIEM systems collect, aggregate, and analyse security logs from across the organisation (servers, firewalls, endpoints, applications). They provide real-time alerting, dashboards, and forensic investigation capabilities. Examples: Splunk, Microsoft Sentinel, IBM QRadar. Appropriate for centralised monitoring, compliance reporting, and incident investigation.

Vulnerability Scanners

Vulnerability scanners automatically identify known weaknesses in systems, applications, and network devices. Examples: Nessus, Qualys, OpenVAS. Appropriate for regular vulnerability assessments, compliance audits, and patch management prioritisation.

Encryption Tools

Encryption transforms data into an unreadable format that can only be decrypted with the correct key. Tools include: TLS/SSL (encrypting web traffic), BitLocker/FileVault (full-disk encryption), PGP/GPG (email encryption), IPsec (VPN tunnel encryption), and AES-256 (general-purpose data encryption). Appropriate for protecting data in transit and at rest.

Network Monitoring Tools

Tools that monitor network traffic for performance and security issues. Examples: Wireshark (packet analysis), Nagios (network monitoring), SolarWinds (network performance). Appropriate for troubleshooting, traffic analysis, and detecting anomalies.

Penetration Testing Tools

Tools used by security professionals to simulate attacks and identify vulnerabilities before real attackers do. Examples: Metasploit (exploitation framework), Nmap (network scanning), Burp Suite (web application testing), Kali Linux (dedicated security testing OS). Appropriate for proactive security assessments and red team exercises.

Case Study – Selecting Security Tools

A growing e-commerce company (50 employees, 10,000 daily website visitors) has experienced: (1) a recent DDoS attack on their web servers, (2) two employees who clicked on phishing emails, (3) a vulnerability scan revealing unpatched servers, and (4) no centralised log monitoring. Their annual security budget is £50,000.

Task: Recommend a security toolkit for this company. For each recommendation: identify the specific category of tool and a product example, explain which of the four issues it addresses, estimate the approximate cost, and justify why it is a priority within the budget constraints. Present as a prioritised table with justifications (approximately 500 words).

2.4 Practices that prevent common attacks

This section evaluates the defensive practices that organisations should implement across their key domains to prevent common attacks from intruders.

Network Security Practices

- Network segmentation – dividing the network into isolated segments (VLANs, subnets) to limit the blast radius of a breach and prevent lateral movement.
- Firewall configuration – implementing and maintaining firewall rules based on the principle of least privilege (deny all by default, allow only what is needed).
- Patch management – establishing a systematic process for identifying, testing, and deploying security patches to operating systems, applications, and firmware. Automated patch management tools (WSUS, SCCM, Intune) ensure timely updates.
- Network Access Control (NAC) – verifying the identity and security posture of devices before granting network access. Non-compliant devices are quarantined or given limited access.
- Regular vulnerability scanning and penetration testing – proactively identifying weaknesses before attackers do.

Remote Access Security

- VPN with strong encryption – using IPsec or WireGuard VPN tunnels for all remote connections, with AES-256 encryption.
- MFA for all remote access – no exceptions. Remote access without MFA is one of the most commonly exploited vulnerabilities.
- Zero Trust Network Access (ZTNA) – replacing traditional VPN with identity-aware, context-aware access that verifies every request.
- Session timeouts and monitoring – automatically terminating idle sessions and logging all remote access activity for audit.

Email Security Practices

- Email filtering and anti-phishing – deploying email security gateways that scan incoming emails for malware, phishing links, and suspicious attachments.
- SPF, DKIM, and DMARC – email authentication protocols that verify the sender's identity and prevent email spoofing. SPF specifies authorised mail servers; DKIM adds a digital signature; DMARC provides a policy for handling authentication failures.
- Security awareness training – regular, engaging training that teaches staff to recognise and report phishing attempts. Simulated phishing campaigns test and reinforce awareness.
- Data Loss Prevention (DLP) – tools that monitor outgoing email for sensitive data (credit card numbers, personal data, confidential documents) and block or encrypt it.

Web Security Practices

- HTTPS everywhere – enforcing TLS encryption on all web traffic using valid certificates. HSTS (HTTP Strict Transport Security) prevents downgrade attacks.
- Web Application Firewall (WAF) – filtering malicious web traffic (XSS, SQL injection, CSRF) before it reaches the application.
- Content Security Policy (CSP) – browser headers that restrict which scripts, styles, and resources can load on a web page, mitigating XSS attacks.
- Regular security testing – automated scanning (DAST/SAST) and manual penetration testing of web applications.

Wireless Security Practices

- WPA3 encryption – using the latest wireless encryption standard. Disabling legacy protocols (WEP, WPA).
- 802.1X authentication – requiring certificate-based or RADIUS authentication for wireless access (enterprise networks).
- Wireless intrusion detection/prevention – monitoring for rogue access points and evil twin attacks.
- Guest network isolation – separating guest Wi-Fi from the corporate network.

Instant Messaging Security

- End-to-end encryption – using messaging platforms that encrypt messages so only the sender and recipient can read them (e.g. Signal, Microsoft Teams with E2EE).
- Access controls and data retention – limiting who can create channels, share files, and access message archives.
- DLP integration – extending data loss prevention policies to messaging platforms to prevent sensitive data being shared over chat.

Physical Security

Physical security is often overlooked but is a critical component of overall security:

- Access controls – key cards, biometric entry systems, mantraps, and visitor logs for server rooms and data centres.
- CCTV and surveillance – monitoring physical access to sensitive areas.
- Environmental controls – fire suppression, temperature and humidity monitoring, and UPS (uninterruptible power supply) systems for server rooms.
- Clean desk policy – requiring staff to secure sensitive documents and lock screens when away from their desks.
- Secure disposal – shredding paper documents and securely wiping or destroying storage media before disposal.

Disaster Recovery and Business Continuity

Every organisation needs plans for recovering from security incidents and other disasters:

- Business Impact Analysis (BIA) – identifying critical systems and the maximum acceptable downtime for each.
- Disaster Recovery Plan (DRP) – detailed procedures for restoring IT systems after a disaster, including RTO (Recovery Time Objective) and RPO (Recovery Point Objective).
- Backup strategy – the 3-2-1 rule: 3 copies of data, on 2 different types of media, with 1 copy offsite/in the cloud. Regular testing of backup restoration is essential.
- Incident Response Plan (IRP) – predefined procedures for identifying, containing, eradicating, and recovering from security incidents, including communication plans and roles.
- Regular testing – tabletop exercises, simulation drills, and full disaster recovery tests to ensure plans work in practice.

Over to you – Video Watch: Disaster Recovery

Watch this YouTube video:

Title: Disaster Recovery Planning – Professor Messer

Duration: 4:23

Link: https://www.youtube.com/watch?v=cOHLMB2DRGY

After watching, explain the difference between RTO and RPO. For a bank's online banking system, what would appropriate RTO and RPO values be, and why?

Over to you – Security Policy Development

Develop a security policy document for a small business (20 employees) covering: (1) password policy (minimum requirements, MFA mandate), (2) email usage and phishing reporting procedures, (3) remote access policy (VPN, MFA, approved devices), (4) physical security requirements, and (5) incident response procedure (who to contact, immediate actions). Write approximately 600 words, using clear, actionable language suitable for a non-technical audience.

2.5 Network and host intrusion detection systems

Intrusion Detection Systems (IDS) monitor networks and systems for malicious activity or policy violations. They are a critical layer in defence-in-depth strategies. There are two primary types: network-based and host-based.

Network Intrusion Detection System (NIDS)

A NIDS monitors network traffic at strategic points (e.g. at the network perimeter or between segments) to detect suspicious activity. It analyses packets passing through the network and compares them against known attack signatures or behavioural baselines.

Strengths: monitors all traffic across the network segment; can detect network-level attacks (port scans, DDoS, lateral movement); does not require software installation on individual hosts; provides a broad view of network activity. Weaknesses: cannot inspect encrypted traffic (unless TLS inspection is implemented); high traffic volumes can overwhelm the system; generates false positives; cannot detect threats that do not traverse the monitored network segment. Examples: Snort (open-source), Suricata (open-source), Cisco Secure IDS.

Host Intrusion Detection System (HIDS)

A HIDS runs on individual hosts (servers, workstations) and monitors system-level activity: file system changes, registry modifications, log entries, process execution, and system calls.

Strengths: can detect host-specific threats (file modifications, privilege escalation, rootkits); works with encrypted traffic (since it monitors at the host level after decryption); provides detailed forensic information about activity on a specific system. Weaknesses: must be installed and managed on each host individually (scalability challenge); consumes host resources (CPU, memory); cannot detect network-level attacks. Examples: OSSEC (open-source), Tripwire, and most modern EDR solutions incorporate HIDS capabilities.

Intrusion Prevention Systems (IPS)

An IPS goes beyond detection to actively block malicious traffic in real time. While an IDS passively alerts, an IPS sits inline with network traffic and can drop, reject, or modify packets identified as malicious. The trade-off is that an IPS that generates false positives may block legitimate traffic, potentially causing business disruption.

Comparing NIDS and HIDS

Feature	NIDS	HIDS
Deployment	Network segment (sensor)	Individual host (agent)
Monitors	Network traffic (packets)	System activity (files, logs, processes)

Encrypted traffic	Cannot inspect (without TLS inspection)	Can monitor (operates after decryption)
Scope	Broad (entire network segment)	Narrow (single host)
Detection	Network attacks, scans, DDoS	File changes, rootkits, privilege escalation
Resource impact	Dedicated hardware/VM	Consumes host CPU/memory
Scalability	One sensor per segment	Agent per host (can be complex)
Examples	Snort, Suricata	OSSEC, Tripwire

In practice, organisations deploy both NIDS and HIDS as complementary layers. A NIDS provides the broad network view while HIDS provides the detailed host-level view. Together, they significantly improve an organisation's ability to detect and respond to threats.

Case Study – IDS Deployment

A university IT department manages a network with 5,000 student and staff devices, 50 servers, and a public-facing website. They have experienced: network scanning activity from external sources, a suspected compromise of a web server, and no current IDS deployment.

Task: Design an IDS deployment strategy for the university. Include: (1) where you would place NIDS sensors (identify specific network segments), (2) which servers would receive HIDS agents and why, (3) whether you would recommend IDS, IPS, or both for each deployment point, (4) one open-source and one commercial product recommendation with justification, and (5) how alerts would be monitored and responded to. Write approximately 500 words.

Reading List

- Ciampa, M. (2024). *CompTIA Security+ Guide to Network Security Fundamentals*. 8th edn. Boston: Cengage.
- Cole, E. (2023). *Network Security Bible*. 3rd edn. Indianapolis, IN: Wiley.
- Hadnagy, C. (2023). *Social Engineering: The Science of Human Hacking*. 3rd edn. Indianapolis, IN: Wiley.
- Kim, D. & Solomon, M.G. (2024). *Fundamentals of Information Systems Security*. 5th edn. Burlington, MA: Jones & Bartlett Learning.
- Stallings, W. (2024). *Network Security Essentials*. 8th edn. Harlow: Pearson.
- Stuttard, D. & Pinto, M. (2023). *The Web Application Hacker's Handbook*. 3rd edn. Indianapolis, IN: Wiley.

Summary

In this chapter, you have studied the practical methods for maintaining computer and network security. You have analysed authentication methods (passwords, MFA, biometrics, certificates, SSO) and their respective strengths and weaknesses. You have examined the nature of different attack types and malicious codes, from viruses and ransomware to APTs. You have learned to select appropriate security tools for different scenarios, including firewalls, EDR, SIEM, vulnerability scanners, and encryption. You have evaluated defensive practices across networks, remote access, email, web, wireless, messaging, physical security, and disaster recovery. Finally, you have analysed the differences between network-based and host-based intrusion detection systems and understood how they complement each other in a defence-in-depth strategy.

Glossary

Word / Term	Explanation
APT	Advanced Persistent Threat; a prolonged, targeted attack by sophisticated threat actors.
Authentication	The process of verifying the identity of a user, device, or system.
Availability	Ensuring systems and data are accessible to authorised users when needed (CIA triad).
Botnet	A network of compromised devices controlled by an attacker, often used for DDoS attacks.
CIA Triad	Confidentiality, Integrity, Availability – the foundational model for information security.
Confidentiality	Ensuring information is accessible only to authorised parties (CIA triad).
DDoS	Distributed Denial of Service; overwhelming a service with traffic from many sources.
DMARC	Domain-based Message Authentication, Reporting and Conformance; email authentication protocol.
EDR	Endpoint Detection and Response; security software that monitors and responds to threats on endpoints.
Encryption	Transforming data into unreadable format that can only be decrypted with the correct key.
Firewall	A network security device that monitors and controls incoming and outgoing traffic based on rules.
HIDS	Host Intrusion Detection System; monitors system-level activity on individual hosts.
IDS	Intrusion Detection System; monitors networks or systems for malicious activity.
Integrity	Ensuring information has not been altered by unauthorised parties (CIA triad).
IPS	Intrusion Prevention System; actively blocks malicious traffic in real time.
MFA	Multi-Factor Authentication; requiring two or more authentication factors.
NIDS	Network Intrusion Detection System; monitors network traffic for suspicious activity.
OWASP	Open Web Application Security Project; produces web security standards and the Top 10 list.
Patch Management	The process of identifying, testing, and deploying security updates to systems.
Phishing	Fraudulent communications designed to trick recipients into revealing sensitive information.
Ransomware	Malware that encrypts files or systems and demands payment for the decryption key.

RPO	Recovery Point Objective; the maximum acceptable amount of data loss measured in time.
RTO	Recovery Time Objective; the maximum acceptable downtime after an incident.
SIEM	Security Information and Event Management; centralised security log collection and analysis.
Social Engineering	Manipulating people into compromising security through psychological techniques.
SOAR	Security Orchestration, Automation and Response; platforms that automate incident response.
TLS	Transport Layer Security; protocol for encrypting data in transit over networks.
VPN	Virtual Private Network; encrypted tunnel for secure remote access.
WAF	Web Application Firewall; filters malicious web traffic targeting applications.
Zero Trust	A security model that assumes no user or device is trusted by default.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. The CIA triad stands for Confidentiality, Integrity, and Availability.
2. A worm requires user interaction to spread across a network.
3. WPA3 is the current recommended standard for wireless encryption.
4. A NIDS monitors activity on individual hosts.
5. Multi-factor authentication uses two or more factors from different categories.
6. SQL injection is a type of social engineering attack.
7. Zero Trust assumes no user or device is trusted by default.
8. Biometric data can easily be changed if compromised.
9. A firewall controls traffic between network segments based on rules.
10. Ransomware encrypts files and demands payment for the decryption key.
11. SPF, DKIM, and DMARC are wireless security protocols.
12. An IPS actively blocks malicious traffic, unlike an IDS which only alerts.
13. The 3-2-1 backup rule recommends 3 copies on 2 media types with 1 offsite.
14. Phishing is the most common form of social engineering.
15. EDR solutions only use signature-based detection.
16. Defence in depth uses multiple layers of security controls.
17. A rootkit is designed to be easily detected by antivirus software.
18. RPO measures the maximum acceptable downtime after an incident.
19. Certificate-based authentication uses public key cryptography.
20. AI-based security systems never produce false positive alerts.

Multiple Choice Questions

1. Which element of the CIA triad does a DDoS attack primarily target?

A. Confidentiality

B. Integrity

C. Availability

D. Authentication

2. Which type of malware disguises itself as legitimate software?

A. Worm

B. Virus

C. Trojan Horse

D. Adware

3. What does MFA stand for?

A. Multiple Firewall Architecture

B. Multi-Factor Authentication

C. Managed File Access

D. Master Forensic Analysis

4. Which tool is best for centralised log analysis and security monitoring?

A. Firewall

B. VPN

C. SIEM

D. Antivirus

5. The WannaCry attack in 2017 was which type of malware?

A. Spyware

B. Adware

C. Ransomware

D. Rootkit

6. Which email authentication protocol adds a digital signature to outgoing emails?

A. SPF

B. DKIM

C. DMARC

D. TLS

7. A HIDS monitors:

A. Network traffic

B. Wireless signals

C. Host system activity

D. Email content

8. Which security model follows the principle of 'never trust, always verify'?

A. Perimeter security

B. Defence in depth

C. Zero Trust

D. DMZ

9. What does RPO measure?

A. Maximum downtime

B. Maximum data loss in time

C. Recovery speed

D. Backup frequency

10. Which attack involves intercepting communication between two parties?

A. DDoS

B. Phishing

C. Man-in-the-Middle

D. Brute force

11. Fileless malware operates:

A. On USB drives only

B. Entirely in memory

C. Through email only

D. On mobile devices only

12. Which is NOT a factor of authentication?

A. Something you know

B. Something you have

C. Something you want

D. Something you are

13. The OWASP Top 10 #1 risk (2021) is:

A. SQL Injection

B. Broken Access Control

C. XSS

D. Cryptographic Failures

14. Which tool would you use to scan for network vulnerabilities?

A. Wireshark

B. Nessus

C. Snort

D. BitLocker

15. AI in cybersecurity improves detection by:

A. Replacing all human analysts

B. Identifying anomalies in behavioural patterns

C. Eliminating all false positives

D. Making encryption unnecessary

16. An evil twin attack targets:

A. Email systems

B. Wireless networks

C. Database servers

D. Physical access controls

17. The 3-2-1 backup strategy recommends:

A. 3 backups daily

B. 3 copies, 2 media types, 1 offsite

C. 3 encryption keys

D. 3 firewall rules

18. Credential stuffing exploits:

A. Weak encryption

B. Password reuse across services

C. Biometric failures

D. Firewall misconfigurations

19. Which is an open-source NIDS?

A. CrowdStrike

B. Splunk

C. Snort

D. BitLocker

20. According to IBM's 2024 report, security AI saves organisations an average of:

A. $500,000

B. $1 million

C. $2.22 million

D. $5 million

Answers to True/False Questions

1. *True*. CIA = Confidentiality, Integrity, Availability.

2. *False*. Worms self-replicate and spread without user interaction; viruses require user action.

3. *True*. WPA3 provides the strongest current wireless encryption standard.

4. *False*. NIDS monitors network traffic; HIDS monitors individual hosts.

5. *True*. MFA combines factors from different categories (know, have, are).

6. *False*. SQL injection is a technical attack targeting databases, not social engineering.

7. *True*. Zero Trust verifies every access request regardless of location or identity.

8. *False*. Biometric data (fingerprints, faces) cannot be changed like passwords can.

9. *True*. Firewalls enforce security policies by controlling traffic based on predefined rules.

10. *True*. Ransomware encrypts victim data and demands payment (cryptocurrency) for decryption.

11. *False*. SPF, DKIM, and DMARC are email authentication protocols, not wireless protocols.

12. *True*. IDS detects and alerts; IPS actively blocks malicious traffic.

13. *True*. 3 copies, 2 media types, 1 offsite – ensures resilience against data loss.

14. *True*. Phishing is the most common social engineering vector, accounting for the majority of breaches.

15. *False*. Modern EDR uses behavioural analysis, ML, and threat intelligence alongside signatures.

16. *True*. Defence in depth layers multiple controls so that failure of one does not compromise the whole.

17. *False*. Rootkits are specifically designed to hide their presence from detection tools.

18. *False*. RPO measures maximum acceptable data loss; RTO measures maximum acceptable downtime.

19. *True*. Digital certificates use public key cryptography (X.509) for identity verification.

20. *False*. AI systems can and do produce false positives; reducing them is an ongoing challenge.

Answers to Multiple Choice Questions

1. (C) Availability

2. (C) Trojan Horse

3. (B) Multi-Factor Authentication

4. (C) SIEM

5. (C) Ransomware

6. (B) DKIM

7. (C) Host system activity

8. (C) Zero Trust

9. (B) Maximum data loss in time

10. (C) Man-in-the-Middle

11. (B) Entirely in memory

12. (C) Something you want

13. (B) Broken Access Control

14. (B) Nessus

15. (B) Identifying anomalies in behavioural patterns

16. (B) Wireless networks

17. (B) 3 copies, 2 media types, 1 offsite

18. (B) Password reuse across services

19. (C) Snort

20. (C) $2.22 million