

Introduction to Cyber Security

Definition –

Cyber Security refers to practices, technologies, and processes designed to protect networks, devices, programs, and data from cyber threats.

Importance –

It safeguards sensitive information, prevents cyber-attacks, and ensures the confidentiality, integrity, and availability of data.

Types of Cyber Threats

Malware – Viruses, worms, trojans, ransomware, and spyware.

Phishing – Fraudulent attempts to steal sensitive information.

Denial of Service (DoS) Attacks – Overloading systems to make them unavailable.

Man-in-the-Middle (MitM) Attacks – Interception of communication.

SQL Injection – Exploiting database vulnerabilities.

Cont..

- **Career Opportunities in Cyber Security**
- Ethical Hacker
- Cyber Security Analyst
- Security Consultant
- Penetration Tester
- Chief Information Security Officer (CISO)

- **Future of Cyber Security**
- Artificial Intelligence (AI) in security.
- Blockchain for secure transactions.
- Zero Trust Security Model.
- Growing demand for cybersecurity professionals.

Conclusion – Cyber Security is essential in today's digital world to protect data, privacy, and critical systems from cyber threats.

Classification of Cyber Security

- **Network Security**
 - Protects computer networks from unauthorized access, attacks, or misuse.
 - Includes firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs).
- **Information Security**
 - Focuses on protecting data from unauthorized access, modification, or deletion.
 - Uses encryption, access controls, and data loss prevention (DLP) techniques.
- **Application Security**
 - Secures software and applications from vulnerabilities.
 - Includes security patches, code reviews, and secure coding practices.
- **Cloud Security**
 - Protects cloud-based applications, services, and storage.
 - Uses encryption, identity management, and security monitoring.

Cont...

- **Endpoint Security**
 - Protects individual devices such as computers, mobile phones, and IoT devices.
 - Uses antivirus software, endpoint detection, and response (EDR) solutions.
- **Operational Security (OPSEC)**
 - Ensures secure operational processes and protects critical business data.
 - Involves risk assessments, compliance policies, and security awareness training.
- **Cryptography**
 - Secures data through encryption techniques to prevent unauthorized access.
 - Includes symmetric and asymmetric encryption, hashing, and digital signatures.
- **Internet of Things (IoT) Security**
 - Protects connected devices and smart systems from cyber threats.
 - Uses authentication, firmware updates, and network segmentation

Cont...

Identity and Access Management (IAM)

- Manages user access and authentication to ensure only authorized users can access systems.
- Uses multi-factor authentication (MFA) and single sign-on (SSO).

- **Artificial Intelligence and Machine Learning Security**

- Protects AI/ML models from adversarial attacks and data poisoning.
- Uses secure model training, threat detection algorithms, and anomaly detection.

- **Incident Response and Forensics**

- Focuses on detecting, responding to, and recovering from security incidents.
- Includes security event monitoring, digital forensics, and post-attack analysis.

- **Cyber Threat Intelligence (CTI)**

- Gathers and analyzes information about cyber threats to prevent attacks.
- Includes threat hunting, malware analysis, and vulnerability assessments.

Motives of Cyber Security

- Cyber security aims to protect digital systems, networks, and data from various threats.
- The key motives include:
- **Confidentiality** – Ensuring sensitive data is accessible only to authorized individuals.
- **Integrity** – Preventing unauthorized alterations to data and maintaining its accuracy.
- **Availability** – Ensuring data and services are accessible when needed.
- **Authentication** – Verifying the identity of users and systems to prevent unauthorized access.
- **Non-repudiation** – Ensuring that a party cannot deny the authenticity of a transaction.
- **Resilience** – Ensuring business continuity and recovery from cyber attacks.
- **Compliance** – Adhering to legal and regulatory frameworks (e.g., GDPR, HIPAA, ISO 27001).

Methods of Cyber Security

Firewalls – Act as a barrier between trusted and untrusted networks, blocking unauthorized traffic.

Encryption – Converts data into a secure format to prevent unauthorized access.

Antivirus and Anti-malware – Detects, prevents, and removes malicious software.

Multi-Factor Authentication (MFA) – Adds an extra layer of security beyond passwords.

Intrusion Detection and Prevention Systems (IDPS) – Monitors network activity for suspicious behavior.

Penetration Testing (Ethical Hacking) – Simulates cyber attacks to identify vulnerabilities

Methods of Cyber Security

Security Patching and Updates – Regularly updates software to fix security flaws.

Access Control – Restricts access based on user roles and permissions.

Data Loss Prevention (DLP) – Prevents sensitive data from being leaked or stolen.

Security Information and Event Management (SIEM) – Collects and analyzes security data for threat detection.

Cyber Threat Intelligence (CTI) – Gathers information on emerging cyber threats to enhance security defenses.

Incident Response and Forensics – Investigates cyber incidents and implements recovery measures.

, Common Cyber Security: Identity theft

- **Definition-** Identity theft occurs when someone steals another person's personal or financial information to commit fraud or unauthorized activities.
- **Common Types of Identity Theft**
- **Financial Identity Theft** – Stealing credit card or bank details to make unauthorized transactions.
- **Medical Identity Theft** – Using stolen personal data to obtain medical treatment or benefits.
- **Criminal Identity Theft** – Using another person's identity when arrested or committing crimes.
- **Synthetic Identity Theft** – Creating fake identities by combining real and fake information.
- **Tax Identity Theft** – Using someone's Social Security Number (SSN) to file fraudulent tax returns.
- **Social Media Identity Theft** – Hacking social media accounts to impersonate someone.

Cont..

- **Methods Used by Cybercriminals**
- **Phishing Attacks** – Fraudulent emails or websites trick users into revealing sensitive information.
- **Data Breaches** – Hackers steal personal data from companies or databases.
- **Malware and Spyware** – Malicious software is installed to capture personal information.
- **Skimming** – Criminals use card readers to copy credit/debit card information.
- **Social Engineering** – Manipulating people into sharing confidential data.
- **Dumpster Diving** – Retrieving personal information from discarded documents.
- .

Cont..

- **Consequences of Identity Theft**
- **Financial Loss** – Unauthorized transactions, loans, or credit card misuse.
- **Legal Issues** – Victims may face legal trouble if their identity is used for crimes.
- **Credit Score Damage** – Fraudulent transactions can lower a victim's credit rating.
- **Emotional Distress** – Stress, anxiety, and loss of trust in digital systems.
- **Reputation Damage** – Fake accounts and fraud can harm personal or professional reputation.

Cont..

- **Prevention and Protection Measures**
- **Use Strong, Unique Passwords** – Enable two-factor authentication (2FA).
- **Monitor Bank and Credit Card Statements** – Regularly check for unauthorized transactions.
- **Be Cautious with Personal Information** – Avoid sharing sensitive data online or over the phone.
- **Shred Sensitive Documents** – Destroy personal papers before disposal.
- **Install Security Software** – Use antivirus, anti-malware, and firewalls.
- **Use Secure Websites** – Ensure websites use HTTPS before entering personal data.
- **Freeze Credit Reports** – Prevent criminals from opening accounts in your name

Phishing in Cyber Security

- **1. Definition**
- Phishing is a cyber-attack where attackers impersonate a trusted entity to deceive individuals into revealing sensitive information, such as login credentials, financial details, or personal data.

Common Types of Phishing Attacks

- **Email Phishing** – Fraudulent emails pretending to be from legitimate organizations to steal information.
- **Spear Phishing** – Targeted phishing attack aimed at specific individuals or organizations.
- **Whaling** – Phishing attack targeting high-profile executives or decision-makers.
- **Smishing (SMS Phishing)** – Fraudulent text messages trick victims into clicking malicious links
- **Vishing (Voice Phishing)** – Attackers use phone calls to manipulate victims into sharing sensitive data.
- **Clone Phishing** – Attackers copy legitimate emails but replace links with malicious ones.
- **Angler Phishing** – Using social media to trick users into providing credentials or personal data.

Common Methods Used in Phishing

- **Fake Emails and Messages** – Fraudulent emails that appear legitimate.
- **Spoofed Websites** – Imitation websites that steal user credentials.
- **Malicious Attachments** – Files containing malware to steal data.
- **Deceptive Links** – URLs that lead to fake login pages or malware downloads.
- **Urgency Tactics** – Messages that create panic to make users act quickly (e.g., "Your account will be suspended!").

Consequences of Phishing

- **Financial Loss** – Unauthorized transactions and stolen banking details.
- **Data Breaches** – Exposure of sensitive business or personal data.
- **Identity Theft** – Stolen personal information used for fraudulent activities.
- **Reputation Damage** – Loss of trust and credibility for individuals or organizations.
- **Malware Infections** – Ransomware, spyware, or other malware attacks.

Prevention and Protection Against Phishing

- **Verify Email Senders** – Check for suspicious email addresses.
- **Do Not Click on Unknown Links** – Hover over links before clicking to check authenticity.
- **Enable Multi-Factor Authentication (MFA)** – Adds an extra layer of security.
- **Use Security Software** – Install antivirus, firewalls, and anti-phishing tools.
- **Educate and Train Employees** – Awareness programs to identify phishing attempts.
- **Monitor Financial Transactions** – Regularly check for unauthorized activity.
- **Report Phishing Attempts** – Report suspicious emails to IT security teams or authorities.

Ransomware in Cyber Security

- **Definition**
- Ransomware is a type of malicious software (malware) that encrypts a victim's data or locks them out of their system, demanding a ransom payment for decryption or access restoration.

Cont...

- Common Types of Ransomware.
- **Crypto Ransomware** – Encrypts files and demands payment for the decryption key.
- **Locker Ransomware** – Locks the entire system or device, preventing access.
- **Scareware** – Displays fake alerts claiming the system is infected, urging victims to pay for removal.
- **Doxware (Leakware)** – Threatens to release sensitive data unless a ransom is paid.
- **RaaS (Ransomware-as-a-Service)** – Cybercriminals rent out ransomware tools to other hackers for profit.

How Ransomware Spreads

- **Phishing Emails** – Malicious attachments or links trick users into downloading ransomware.
- **Malvertising** – Fake online advertisements that trigger ransomware downloads.
- **Exploit Kits** – Automated tools that exploit system vulnerabilities to deliver ransomware.
- **Remote Desktop Protocol (RDP) Attacks** – Hackers gain access to a system using weak credentials.
- **Software Vulnerabilities** – Outdated applications and operating systems exploited for infection.
- **USB Devices and External Media** – Infected storage devices spreading ransomware when connected.

Consequences of Ransomware Attacks

- **Financial Loss** – Ransom payments can range from hundreds to millions of dollars.
- **Data Loss** – Encrypted data may be lost if no backups exist.
- **Business Disruptions** – Organizations may experience downtime, affecting operations.
- **Reputation Damage** – Loss of trust from customers and stakeholders.
- **Legal and Compliance Issues** – Regulatory penalties if sensitive data is exposed.

Prevention and Protection Against Ransomware

- **Regular Data Backups** – Maintain offline and cloud backups of critical data.
- **Use Strong Security Software** – Install antivirus, firewalls, and endpoint protection tools.
- **Enable Multi-Factor Authentication (MFA)** – Prevent unauthorized system access.
- **Patch and Update Software** – Keep operating systems and applications up to date.
- **Avoid Clicking on Suspicious Links and Emails** – Verify sender authenticity before opening attachments.
- **Disable Unused Remote Access** – Restrict RDP and use VPNs for secure remote access.
- **Implement Network Segmentation** – Isolate critical systems to limit ransomware spread.
- **Educate and Train Employees** – Conduct security awareness programs on ransomware threats.

Cyberstalking in Cyber Security

- **Definition**
- Cyberstalking is the use of digital platforms, such as social media, emails, or messaging apps, to harass, intimidate, or monitor an individual repeatedly.

Common Methods of Cyberstalking

- **Social Media Harassment** – Posting threatening messages, comments, or fake profiles.
- **Email and Text Harassment** – Sending abusive or threatening emails and messages.
- **Tracking and Monitoring** – Using spyware or GPS tracking to monitor someone's movements.
- **Doxxing** – Publishing personal information (address, phone number) online to harass victims.
- **Impersonation** – Creating fake profiles to defame or manipulate the victim.
- **Hacking Personal Accounts** – Gaining unauthorized access to social media, email, or financial accounts.

Consequences of Cyberstalking

- **Emotional and Psychological Distress** – Anxiety, fear, and depression.
- **Privacy Invasion** – Personal data and activities being constantly monitored.
- **Reputation Damage** – Spreading false information about the victim.
- **Physical Safety Risks** – Risk of real-world stalking and threats.
- **Legal Consequences** – Many countries have laws against cyberstalking, leading to criminal charges.

Prevention and Protection Against Cyberstalking

- **Strengthen Privacy Settings** – Limit personal information on social media.
- **Use Strong Passwords and MFA** – Prevent unauthorized account access.
- **Block and Report Stalkers** – Immediately block and report suspicious accounts.
- **Avoid Sharing Location Online** – Disable location tracking on apps.
- **Keep Digital Evidence** – Save messages, emails, and screenshots as proof.
- **Seek Legal Help** – Report cyberstalking to law enforcement authorities.

Credit Card Frauds in Cyber Security

- **Definition**
- Credit card fraud is a type of financial cybercrime where criminals use stolen credit card information to make unauthorized transactions.

Common Types of Credit Card Fraud

- **Card-Not-Present (CNP) Fraud** – Using stolen card details for online or phone transactions.
- **Card Skimming** – Installing devices on ATMs or card readers to steal card information.
- **Phishing Attacks** – Fake emails or websites trick victims into sharing card details.
- **Account Takeover** – Hackers gain access to a cardholder's account and make fraudulent purchases.
- **Fake Card Creation** – Using stolen data to create counterfeit cards.
- **Identity Theft Fraud** – Criminals use stolen personal data to apply for new credit cards.

Consequences of Credit Card Fraud

- **Financial Loss** – Unauthorized transactions and stolen funds.
- **Damage to Credit Score** – Fraudulent activity can negatively affect credit ratings.
- **Legal Complications** – Victims may face disputes over fraudulent transactions.
- **Loss of Personal Data** – If fraud occurs due to phishing or data breaches.
- **Banking Inconvenience** – Victims may need to cancel cards and update account information

Prevention and Protection Against Credit Card Fraud

- **Enable Transaction Alerts** – Receive notifications for every card transaction.
- **Use Secure Payment Methods** – Prefer virtual cards or digital wallets for online transactions.
- **Monitor Bank Statements Regularly** – Check for unauthorized transactions.
- **Avoid Public Wi-Fi for Transactions** – Use a secure network for banking activities.
- **Do Not Share Card Details Online** – Avoid sharing sensitive information via email or messages.
- **Use Strong Passwords and MFA** – Secure online banking and payment accounts.
- **Report Lost or Stolen Cards Immediately** – Notify the bank to block and replace the card.

CIA Triad in Cyber Security

- **Confidentiality**
- **Definition:** Protecting information from unauthorized access and ensuring that only authorized users can view sensitive data.
- **Key Aspects:**
- **Access Control** – Restricting access based on roles and permissions.
- **Data Encryption** – Securing data by converting it into an unreadable format.
- **Multi-Factor Authentication (MFA)** – Adding extra layers of security to prevent unauthorized access.
- **Data Masking** – Concealing sensitive data to protect privacy.
- **Network Security Measures** – Firewalls, VPNs, and intrusion prevention systems (IPS).

Cont..

- **Examples:**
- Encrypting sensitive emails before sending them.
- Using strong passwords and biometric authentication.
- Implementing least privilege access for employees.

Integrity

- **Definition:** Ensuring that data remains accurate, consistent, and unaltered without authorization.
- **Key Aspects:**
- **Checksums and Hashing** – Verifying data integrity using cryptographic hash functions.
- **Data Validation** – Ensuring only correct and authorized changes are made to data.
- **Access Logs and Audit Trails** – Tracking changes to detect unauthorized modifications.
- **Digital Signatures** – Ensuring authenticity and integrity of data transmissions.
- **Version Control** – Keeping track of changes and allowing data recovery.

Cont..

- **Examples:**
- Using SHA-256 hashing to verify file integrity.
- Implementing blockchain for tamper-proof transactions.
- Checking digital signatures to verify document authenticity.

Availability

- **Definition:** Ensuring that data and services are accessible and operational whenever needed.
- **Key Aspects:**
- **Redundancy and Backup Systems** – Using multiple data centers and cloud storage.
- **Disaster Recovery Planning** – Ensuring business continuity in case of cyberattacks or failures.
- **Load Balancing** – Distributing network traffic to prevent overloads.
- **DDoS Protection** – Implementing security measures against denial-of-service attacks.
- **Regular System Maintenance** – Keeping hardware and software updated to prevent failures.

Cont..

- **Examples:**
- Using RAID storage to prevent data loss.
- Having backup servers to ensure service continuity.
- Implementing failover systems in case of hardware failures

Ethical Hacking: Introduction

- **Definition:** Ethical hacking refers to the practice of legally breaking into computers and devices to test an organization's defenses.
- **Purpose:** It is conducted to identify security vulnerabilities and strengthen systems before malicious hackers can exploit them.
- **Legal Aspect:** Ethical hackers have official permission from the organization they are testing, differentiating them from cybercriminals.
- **Other Names:** Also known as penetration testing, white-hat hacking, or red teaming.
- **Types of Ethical Hackers:** Includes white-hat hackers, security researchers, and penetration testers.
- **Skills Required:** Knowledge of programming, networking, operating systems, cryptography, and cybersecurity tools.
- **Methodology:** Ethical hacking follows a structured process, including reconnaissance, scanning, gaining access, maintaining access, and covering tracks.

Ethical Hacking: Introduction

- **Common Tools:** Tools like Kali Linux, Metasploit, Nmap, Wireshark, Burp Suite, and John the Ripper are used for ethical hacking.
- **Ethical Hacking vs. Black-Hat Hacking:** Unlike black-hat hackers, ethical hackers work with authorization and aim to improve security, not exploit it.
- **Industries Using Ethical Hacking:** Banking, healthcare, government, IT firms, and e-commerce heavily rely on ethical hackers for security.
- **Certifications:** Popular ethical hacking certifications include CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), and CISSP (Certified Information Systems Security Professional).
- **Future Scope:** With increasing cyber threats, ethical hacking is becoming a crucial aspect of cybersecurity, ensuring data protection and system integrity.

Need of Ethical Hacking

- **Prevent Cyber Attacks** – Ethical hacking helps organizations identify and fix security vulnerabilities before malicious hackers exploit them.
- **Data Protection** – Safeguards sensitive data from unauthorized access, theft, or leaks, ensuring confidentiality and integrity.
- **Identifying System Weaknesses** – Helps in finding loopholes in networks, applications, and systems to strengthen security measures.
- **Securing Financial Transactions** – Ensures the safety of online banking, digital payments, and financial transactions from cyber fraud.

Need of Ethical Hacking

- **Compliance with Security Regulations** – Many industries require ethical hacking to meet legal and regulatory cybersecurity standards (e.g., GDPR, HIPAA, ISO 27001).
- **Enhancing Cloud Security** – As businesses shift to cloud platforms, ethical hacking ensures secure cloud infrastructure and prevents breaches.
- **Protecting IoT Devices** – Identifies vulnerabilities in smart devices, preventing unauthorized access and data misuse.
- **Preventing Identity Theft** – Helps in securing personal and corporate identities from phishing, social engineering, and credential theft.

Need of Ethical Hacking

- **Reducing Business Losses** – Cyberattacks cause financial and reputational damage; ethical hacking minimizes risks and protects business continuity.
- **Testing Incident Response Plans** – Helps organizations prepare for cyber incidents by simulating attacks and evaluating response strategies.
- **Fostering Trust and Reputation** – Companies with strong cybersecurity measures gain customer trust and maintain a positive market reputation.
- **National Security & Cyber Warfare Protection** – Governments use ethical hacking to defend against cyber espionage, terrorism, and cyber warfare threats.

Types of Ethical Hacking

- **Network Hacking** – Identifies security vulnerabilities in network infrastructure, such as firewalls, routers, and switches, to prevent unauthorized access.
- **Web Application Hacking** – Focuses on finding and fixing security flaws in websites and web applications, including SQL injection, XSS (Cross-Site Scripting), and CSRF (Cross-Site Request Forgery).
- **System Hacking** – Involves penetration testing of computer systems to detect and mitigate security weaknesses in operating systems and software.
- **Wireless Network Hacking** – Targets Wi-Fi networks to assess encryption strength, detect unauthorized devices, and prevent attacks like rogue access points and Wi-Fi sniffing.
- **Social Engineering** – Exploits human psychology rather than technical vulnerabilities to trick users into revealing sensitive information (e.g., phishing, baiting, pretexting).

Types of Ethical Hacking

- **Cloud Hacking** – Evaluates the security of cloud platforms and services, ensuring data protection and preventing unauthorized cloud access.
- **IoT Hacking** – Identifies weaknesses in smart devices (e.g., security cameras, smart home systems, medical devices) to prevent unauthorized access and data breaches.
- **Mobile Hacking** – Assesses security flaws in mobile applications and operating systems (Android, iOS) to prevent data leaks and malware attacks.
- **Email Hacking** – Tests the security of email communication systems to prevent phishing attacks, email spoofing, and unauthorized access.
- **Cryptographic Hacking** – Examines encryption algorithms and security protocols to identify weaknesses and improve data confidentiality.

UNIT 2

- **Security Attacks: Types of Attacks**
- **1. Network Attacks**
- **Denial of Service (DoS) & Distributed DoS (DDoS):** Overwhelming a system or network with excessive requests to make it unavailable.
- **Man-in-the-Middle (MitM):** Intercepting and altering communication between two parties without their knowledge.
- **Packet Sniffing:** Capturing network traffic to steal sensitive information.
- **IP Spoofing:** Masquerading as a trusted IP address to gain unauthorized access.
- **2. Malware Attacks**
- **Viruses:** Malicious programs that attach to files and spread.
- **Worms:** Self-replicating malware that spreads without human intervention.
- **Trojans:** Malware disguised as legitimate software.
- **Ransomware:** Encrypts files and demands payment for decryption.
- **Spyware:** Secretly monitors and collects user activity.
- **Adware:** Displays unwanted advertisements and may track user behavior.

Cont..

- **3. Web-Based Attacks**
- **SQL Injection:** Injecting malicious SQL queries to access or manipulate a database.
- **Cross-Site Scripting (XSS):** Injecting malicious scripts into webpages to steal user data.
- **Cross-Site Request Forgery (CSRF):** Trick users into executing unwanted actions on a website.
- **Phishing:** Fake emails or websites that trick users into revealing sensitive information.
- **4. Insider Threats**
- **Malicious Insiders:** Employees or contractors misusing their access for personal gain.
- **Unintentional Insiders:** Employees who unknowingly cause security breaches by mishandling data.
- **5. Cryptographic Attacks**
- **Brute Force Attack:** Trying all possible passwords until one is found.
- **Dictionary Attack:** Using a list of common passwords to gain access.
- **Man-in-the-Middle (MitM) on Encryption:** Intercepting encrypted data and attempting to decrypt it.
- **Replay Attack:** Reusing captured authentication data to gain unauthorized access.

Cont..

- **6. Physical Attacks**
- **Hardware Tampering:** Physically altering devices to compromise security.
- **Social Engineering:** Manipulating individuals into divulging confidential information.
- **Shoulder Surfing:** Watching users enter passwords or sensitive data.
- **Dumpster Diving:** Searching for confidential information in discarded materials.
- **7. IoT and Wireless Attacks**
- **Evil Twin Attack:** Creating a fake Wi-Fi network to steal data.
- **Bluetooth Hacking:** Exploiting vulnerabilities in Bluetooth connections.
- **RFID & NFC Attacks:** Skimming data from contactless cards and devices.

Cont..

- **6. Physical Attacks**
- **Hardware Tampering:** Physically altering devices to compromise security.
- **Social Engineering:** Manipulating individuals into divulging confidential information.
- **Shoulder Surfing:** Watching users enter passwords or sensitive data.
- **Dumpster Diving:** Searching for confidential information in discarded materials.
- **7. IoT and Wireless Attacks**
- **Evil Twin Attack:** Creating a fake Wi-Fi network to steal data.
- **Bluetooth Hacking:** Exploiting vulnerabilities in Bluetooth connections.
- **RFID & NFC Attacks:** Skimming data from contactless cards and devices.

Unit 3 : Cyber Security Tools

- **Introduction (Vulnerability Scanners: Nessus)**
- Nessus is a widely-used vulnerability scanning tool developed by **Tenable Inc.**
- It identifies and detects vulnerabilities, misconfigurations, and compliance issues in IT systems.
- **Purpose :**
- To **scan networks, systems, and applications** for security weaknesses.
- Helps organizations detect vulnerabilities before malicious actors exploit them.
- **Features**
- **Comprehensive Vulnerability Detection:** Identifies vulnerabilities like misconfigurations, weak passwords, and missing patches.
- **Policy Compliance Audits:** Checks for compliance with security standards (e.g., PCI DSS, HIPAA).
- **Customizable Scans:** Allows creation of custom policies and scan templates.
- **Continuous Updates:** Regularly updated with new vulnerability signatures.
- **Reports and Analytics:** Generates detailed reports with risk ratings and remediation steps.

Unit 3 : Cyber Security Tools

- **Types of Scans**
- **Network Scanning:** Detects open ports and services.
- **Credentialed Scanning:** Authenticated scans for deeper insights.
- **Uncredentialed Scanning:** External scanning without system access.
- **Malware Detection:** Identifies known malware and backdoors.

- **Deployment Options**
- **Nessus Essentials:** Free version for personal use (up to 16 IPs).
- **Nessus Professional:** Paid version for enterprise-level scanning.
- **Nessus Manager:** Centralized management and advanced collaboration.
- **Nessus Cloud:** Cloud-based vulnerability management.
- **Advantages**
- **User-Friendly Interface:** Intuitive web-based interface.
- **High Accuracy:** Low false-positive rate due to thorough checks.
- **Automation:** Supports scheduled and automated scans.
- **Wide Platform Support:** Works across various OS (Windows, Linux, macOS, etc.).

Unit 3 : Cyber Security Tools

- **Use Cases**
 - **Enterprise Security:** Identify vulnerabilities in large IT infrastructures.
 - **Compliance Audits:** Ensure adherence to industry standards.
 - **Penetration Testing:** Pre-assessment for security tests.
 - **Incident Response:** Identify and remediate post-incident vulnerabilities.
- **Limitations**
 - **Resource Intensive:** High CPU and bandwidth consumption during scans.
 - **Complex Configurations:** Requires technical expertise for advanced use.
 - **Licensing Costs:** Paid versions can be expensive for small businesses.
- **Alternatives**
 - OpenVAS (Open-source alternative)
 - QualysGuard
 - Rapid7 Nexpose
- **Conclusion**
- Nessus is a **robust and versatile** vulnerability scanning tool ideal for businesses seeking **proactive security** and **compliance management**.

Unit 3 : Cyber Security Tools

- **Install and Set Up Nessus**
- **Download Nessus:**
 - Go to the official Tenable website.
 - Choose the appropriate version (Nessus Essentials, Professional, or Expert).
- **Install Nessus:**
 - For **Windows**: Run the .exe installer.
 - For **Linux**: Use the .rpm or .deb package and install it via terminal:
 - `sudo dpkg -i Nessus-x.x.x.deb` # For Debian/Ubuntu
 - `sudo rpm -ivh Nessus-x.x.x.rpm` # For RedHat/CentOS

Unit 3 : Cyber Security Tools

- **Start the Nessus Service:**
- Windows: Starts automatically after installation.
- Linux: Use this command to start the service
 - `sudo systemctl start nessusd`
- **Access the Web Interface:**
- Open a browser and navigate to:arduino
 - <https://localhost:8834>
- **Activate Nessus:**
 - Enter the **Activation Code** (from the Tenable website).
 - Choose **Nessus Essentials (Free)** or **Nessus Professional (Paid)**.

Unit 3 : Cyber Security Tools

- **Configure Nessus for Scanning**
- **1. Login to Nessus:**
 - Enter your credentials in the web interface.
- **Create a New Scan:**
 - Click on “**New Scan**” > Choose a **Scan Template** (e.g., Basic Network Scan).
- **2. Configure Scan Settings:**
 - **Name:** Set a descriptive name for the scan.
 - **Targets:** Enter IP addresses, domains, or ranges (e.g., 192.168.1.1/24).
 - **Scan Policy:** Customize scanning depth (e.g., **Credentialed** for in-depth analysis).
- **Add Credentials (Optional):**
 - For deeper scanning, provide SSH (Linux) or Windows credentials.
 - Go to **Credentials** tab > Add new login information.

Unit 3 : Cyber Security Tools

- **3 . Run and Monitor the Scan**
- **Start the Scan:**
 - Click **Launch** to begin scanning the specified targets.
- **Monitor Scan Progress:**
 - View real-time scan status on the dashboard.
 - Large networks may take longer to complete.
- **4. Analyze Scan Results**
- **View Results:**
 - Once completed, click on the scan name to see the details.
- **Understand Vulnerabilities:**
 - **Severity Levels:**
 - Critical (Red) – Immediate action required.
 - High (Orange) – Major risks.
 - Medium (Yellow) – Moderate risks.
 - Low (Blue) – Minor issues.

Unit 3 : Cyber Security Tools

- **5. Export and Share Reports**

- **Generate Reports:**

- Go to the completed scan > Click **Export**.
- Choose **Formats**: PDF, CSV, HTML, or Nessus format.

- **Share Reports:**

- Send reports to your security team for mitigation.

6. Automate and Schedule Scans

- **Schedule a Scan:**

- While creating a new scan, go to **Schedule**.
- Set up daily, weekly, or monthly scans for continuous monitoring.

Unit 3 : Cyber Security Tools

- **7. Update Nessus Regularly**
- **Update Plugins:**
 - Ensure Nessus is updated to detect the latest vulnerabilities.
 - Use the command:
 - `sudo systemctl restart nessusd`
- **8. Best Practices for Nessus Usage**
- **Use Credentialed Scans:** For better detection of internal vulnerabilities.
- **Segment Networks:** Scan different network zones separately.
- **Prioritize Critical Issues:** Focus on resolving **high** and **critical** vulnerabilities first.
- **Review Regularly:** Schedule periodic reviews and scans for new vulnerabilities.

OpenVAS (Open Vulnerability Assessment System)

- **Definition:** OpenVAS is an open-source vulnerability scanner used to detect security vulnerabilities in systems and networks.
- **Purpose:**
 - It helps identify weaknesses, misconfigurations, and vulnerabilities that could be exploited by malicious actors.
- **Components:**
 - **OpenVAS Scanner:** Performs the actual scanning and vulnerability tests.
 - **Greenbone Security Assistant (GSA):** Web-based user interface for managing and viewing scan results.
 - **OpenVAS Manager:** Manages scan configurations, schedules, and result storage.
 - **Network Vulnerability Tests (NVTs):** Database of scripts used to detect vulnerabilities.

Cont..

- **Features:**
- **Comprehensive Scanning:** Supports thousands of vulnerability tests across different platforms.
- **Regular Updates:** Continuously updated NVT database for detecting new vulnerabilities.
- **Customizable Scans:** Users can configure specific scans based on target systems or services.
- **Reporting:** Generates detailed reports with vulnerability findings and remediation suggestions.
- **Automation:** Allows scheduled scans for continuous monitoring.
- **Integration:** Compatible with other security tools for enhanced threat detection.
- **Use Cases:**
- **Network Security Audits:** Identifying open ports, misconfigurations, and software vulnerabilities.
- **Compliance Checks:** Ensuring systems meet security standards (e.g., PCI-DSS, GDPR).
- **Penetration Testing Support:** Providing initial vulnerability data for security testing.
- **Continuous Monitoring:** Regularly scanning critical assets to detect new vulnerabilities.

Cont...

- **Installation Platforms:**
 - Available for **Linux-based** systems (commonly installed on Debian, Ubuntu, and CentOS).
 - Can also be deployed via Docker or virtual machines.
- **Advantages:**
 - **Free and Open-Source:** Cost-effective and transparent.
 - **Scalability:** Suitable for both small networks and large enterprises.
 - **Community Support:** Backed by a robust open-source community.
- **Disadvantages:**
 - **Resource-Intensive:** Requires significant CPU and memory during scans.
 - **Complex Setup:** Initial configuration can be challenging for beginners.
 - **False Positives:** May generate false alerts that require manual verification.
- **Alternatives:**
 - Nessus (commercial), Qualys, and Nexpose.
- **Maintainers:**
- Developed and maintained by **Greenbone Networks**.

Web Application Vulnerability Scanner: Burp Suite

- **Definition:**
 - Burp Suite is a popular **web application security testing tool** used to identify and exploit vulnerabilities in web applications.
 - It is widely used by **penetration testers, security researchers, and ethical hackers.**
-
- **2. Versions of Burp Suite:**
 - **Community Edition (Free):** Basic features for manual testing.
 - **Professional Edition (Paid):** Advanced scanning, automation, and reporting capabilities.
 - **Enterprise Edition (Paid):** Scalable solution with automation for continuous security testing.

Cont....

- **Key Features:**
- **Intercepting Proxy:** Captures and modifies HTTP(S) traffic between the browser and web application.
- **Spider (Web Crawler):** Automatically maps the target application's structure.
- **Active Scanner:** Automatically identifies vulnerabilities (available in Professional and Enterprise).
- **Passive Scanner:** Detects vulnerabilities by analyzing traffic without actively interacting with the server.
- **Intruder:** Automates customized attacks (e.g., brute force, parameter fuzzing).
- **Repeater:** Allows manual modification and re-sending of HTTP requests for testing.
- **Sequencer:** Analyzes randomness in session tokens to identify weak session management.
- **Extender:** Supports third-party extensions for additional functionality.
- **Collaborator:** Identifies out-of-band vulnerabilities (e.g., SSRF, blind XSS)

Cont....

- **Common Use Cases:**
- **Testing for OWASP Top 10 vulnerabilities** (e.g., XSS, SQL Injection, CSRF, etc.).
- **Intercepting and manipulating requests/responses** for manual security testing.
- **Automated vulnerability scanning** for quick identification of security issues.
- **Brute-force attacks** on login forms and parameter manipulation.
- **Analyzing session management** for weaknesses (e.g., session fixation, cookie issues).
- **Advantages:**
- **Comprehensive Testing Suite:** Covers both **manual** and **automated** testing.
- **Customizable:** Highly extensible with **Burp Extensions** through the BApp Store.
- **User-Friendly:** Intuitive interface with powerful visualization tools.
- **Automation & Manual Testing:** Combines **automated scanning** with **manual attack** capabilities.
- **Regular Updates:** Frequent updates to address **new vulnerabilities** and features

Cont..

- **Disadvantages:**
- **Costly Professional Version:** Full-featured versions require paid licenses.
- **Resource-Intensive:** Requires substantial **CPU and memory** for large-scale scanning.
- **Learning Curve:** Advanced features demand **technical knowledge**.

- **Supported Platforms:**
- **Cross-Platform:** Available for **Windows, macOS, and Linux**.

- **Popular Alternatives:**
- **OWASP ZAP (Free)** – Open-source alternative.
- **Acunetix** – Automated web vulnerability scanner.
- **Netsparker** – Automated and manual web testing.

Cont..

- **Typical Workflow in Burp Suite:**
- **Set up proxy** to intercept and analyze web traffic.
- **Crawl the application** using the Spider tool.
- **Scan for vulnerabilities** using the Active Scanner.
- **Manually test** with tools like Repeater and Intruder.
- **Analyze findings** and generate detailed reports.

How to Operate Web Application Vulnerability Scanner: Burp Suite

1. Installation & Setup

- **Download Burp Suite:**
 - Visit the **PortSwigger** website and download **Burp Suite** (Community, Professional, or Enterprise edition).
- **Install Burp Suite:**
 - Follow the installation process for your operating system (Windows, macOS, Linux).
- **Launch Burp Suite:**
 - Open Burp Suite and select:
 - **Temporary Project** (for one-time use).
 - **New Project** (for saving workspaces).
 - Choose **Use Burp Defaults** for a quick start.

2 Configuring Proxy Settings

- **Set Up Burp Proxy:**
 - Go to **Proxy** → **Options** and ensure the default listener is on **127.0.0.1:8080**.
- **Configure Browser Proxy:**
 - Set your browser's proxy settings to:
 - **IP Address:** 127.0.0.1
 - **Port:** 8080
 - You can also use **Burp's embedded browser** for easier configuration.

How to Operate Web Application Vulnerability Scanner: Burp Suite

Install Burp's CA Certificate (for HTTPS interception):

- Visit <http://burpsuite> in your proxy-configured browser.
- Download and install the **CA Certificate** in your browser's **trusted root** section.

3. Intercepting and Analyzing Web Traffic

• Enable Intercept Mode:

- Go to **Proxy** → **Intercept** and click **Intercept is on** to capture HTTP/S requests.

• Capture and Modify Requests:

- Intercept and inspect traffic between your browser and the target.
- Modify headers, cookies, or parameters in real time.

• Forward Requests:

- Use **Forward** to send the request to the server or **Drop** to block it.

4. Performing a Website Scan

• Target Configuration:

- Go to **Target** → **Scope** and add the domain you want to scan.
- This limits testing to **in-scope** URLs.

• Active Scan (Automated Testing – Paid Feature):

- Right-click on a request and select **Do an Active Scan**.
- Burp will search for vulnerabilities like **SQL Injection**, **XSS**, **CSRF**, etc.

• Passive Scan (Community Edition Available):

- Automatically analyzes traffic for vulnerabilities without interacting with the server.

How to Operate Web Application Vulnerability Scanner: Burp Suite

5. Manual Testing Tools

- **Intruder (Automate Attacks):**
 - Use for **brute-force**, **fuzzing**, and **parameter testing**.
 - Set a target request and customize payloads (e.g., password lists).
- **Repeater (Manual Request Testing):**
 - Send individual requests for manual analysis.
 - Modify parameters and observe server responses.
- **Decoder (Data Encoding & Decoding):**
 - Encode or decode values (e.g., Base64, URL encoding) during testing.
- **Sequencer (Token Analysis):**
 - Analyze session randomness to identify weak session tokens.

6. Generating Reports

- **View Scan Results:**
 - Go to **Dashboard** or **Issue Activity** for a summary of detected vulnerabilities.
- **Export Reports:**
 - **Right-click** on a target and select **Generate HTML/XML Report** for sharing findings.

How to Operate Web Application Vulnerability Scanner: Burp Suite

7. Best Practices for Using Burp Suite

- Always **define scope** to avoid unauthorized scanning.
- Use **Intercept** only when needed to avoid disrupting traffic.
- Perform **manual testing** alongside automated scans for deeper insights.
- **Update Burp Suite** regularly for the latest vulnerability checks.
- Respect **legal and ethical guidelines** – always obtain permission before scanning.

8. Useful Shortcuts in Burp Suite

- **Ctrl + I**: Send request to Intruder.
- **Ctrl + R**: Send request to Repeater.
- **Ctrl + Shift + D**: Send to Decoder.
- **Ctrl + F**: Search in request/response.

OWASP ZAP (Zed Attack Proxy)

- **1. Definition:**
- OWASP ZAP (Zed Attack Proxy) is a **free, open-source web application security scanner** used to find vulnerabilities in web applications.
- It is developed and maintained by the **Open Web Application Security Project (OWASP)** community.
- **2. Purpose:**
- Identifies **security vulnerabilities** in web applications.
- Supports **manual** and **automated** testing.
- Ideal for both **beginners** and **experienced** security testers.
- **3. Key Features:**
- **Intercepting Proxy:** Captures and modifies HTTP/S requests and responses.
- **Automated Scanner:** Quickly identifies common vulnerabilities (e.g., XSS, SQL Injection).
- **Passive Scanning:** Analyzes traffic without interacting with the server.
- **Active Scanning:** Actively probes for vulnerabilities (potentially intrusive).
- **Spider (Web Crawler):** Automatically maps out application structure by crawling URLs.
- **Fuzzer:** Tests for hidden vulnerabilities by injecting payloads.
- **Plug-n-Hack Support:** Seamless browser integration for better traffic capture.
- **Session Management:** Handles cookies, authentication, and CSRF tokens.
- **API Integration:** Supports REST APIs for CI/CD and automation.
- **Add-ons:** Extend functionality with ZAP's extensive plugin marketplace.

OWASP ZAP (Zed Attack Proxy)

- **Installation & Platforms:**
- Supports **Windows, macOS, Linux, and Docker.**
- Easy to install via **.exe, .dmg, or .jar** files.

Typical Workflow in ZAP:

- **Set Up ZAP:** Install and launch the tool.
- **Configure Proxy:** Set your browser's proxy to **127.0.0.1:8080** for traffic capture.
- **Explore Target:** Use **Manual Browsing** or **Spider** to map the web application.
- **Scan for Vulnerabilities:** Run **Active Scan** for in-depth testing.
- **Analyze Results:** Review the **Alerts** tab for detected issues.
- **Report Generation:** Export findings to **HTML, XML, or JSON.**

6. Common Use Cases:

- **Security Audits:** Identify vulnerabilities in web apps.
- **Penetration Testing:** Assist in manual and automated security tests.
- **DevOps Integration:** Use in CI/CD pipelines for **automated security checks.**
- **Training Tool:** Ideal for learning and practicing web security.

OWASP ZAP (Zed Attack Proxy)

7. Vulnerabilities Detected by ZAP:

- **Cross-Site Scripting (XSS)**
- **SQL Injection**
- **Broken Authentication**
- **Insecure Direct Object References (IDOR)**
- **CSRF (Cross-Site Request Forgery)**
- **Security Misconfigurations**
- **Information Disclosure**

8. Advantages:

- **Free and Open-Source:** No licensing fees.
- **Beginner-Friendly:** Easy to use with a simple GUI.
- **Extensive Documentation:** Community-driven guides and tutorials.
- **Customizable:** Supports **add-ons** for extended functionality.
- **Automation Support:** Useful for continuous security testing (CI/CD).

9. Disadvantages:

- **Performance:** Slower on large applications compared to premium scanners.
- **False Positives:** Requires manual verification of findings.
- **Learning Curve:** Advanced features require in-depth knowledge.

OWASP ZAP (Zed Attack Proxy)

Comparison with Alternatives:

- **OWASP ZAP vs. Burp Suite:** ZAP is **free**, while Burp Suite's advanced features require a **paid** license.
- **ZAP vs. Nikto:** ZAP provides **active and passive scanning**, while Nikto focuses on **server vulnerabilities**.
- **ZAP vs. Nessus:** Nessus focuses on **network vulnerabilities**, while ZAP targets **web applications**.

11. Best Practices for Using ZAP:

- Always define your **target scope** to avoid unintended attacks.
- Perform **passive scans** before **active scans** to minimize disruption.
- Regularly **update** ZAP for the latest vulnerabilities and add-ons.
- Use in a **staging environment** to prevent harming live systems.
- Integrate with **CI/CD pipelines** for ongoing security monitoring.

How to Operate OWASP ZAP (Zed Attack Proxy)

- **Download OWASP ZAP:**
 - Visit the official website: <https://www.zaproxy.org/>
 - Download the appropriate version for **Windows**, **macOS**, **Linux**, or **Docker**.
- **Install ZAP:**
 - Follow the installation instructions for your operating system.
 - Launch ZAP after installation.
- **Select a Session Type:**
 - **New Session:** Start fresh for each test.
 - **Persisted Session:** Save your work for future analysis.
 - **Load Session:** Resume a previous session.

How to Operate OWASP ZAP (Zed Attack Proxy)

- **Setting Up Proxy Configuration**
- **Start ZAP Proxy:**
 - By default, ZAP listens on **127.0.0.1:8080**.
- **Configure Browser Proxy:**
 - Set your browser to use **127.0.0.1:8080** as the **HTTP/S proxy**.
 - Alternatively, use ZAP's built-in browser for easier traffic capture.
- **Install ZAP's CA Certificate (For HTTPS Traffic Interception):**
 - Go to **Tools → Options → Dynamic SSL Certificates**.
 - Export the certificate and install it in your browser's **trusted certificates** section.


How to Operate OWASP ZAP (Zed Attack Proxy)

- **Exploring and Scanning a Target**
- **Set Target Scope:**
 - Go to **Scope Control** and define the application you want to test.
 - This helps avoid scanning unintended websites.
- **Explore the Application:**
 - **Manual Browsing:** Browse the target site while ZAP captures requests.
 - **Spider (Crawling):** Automatically map the application's structure.
 - Go to **Spider** → **Start a New Scan** and enter the target URL.
- **Active Scan (Automated Vulnerability Detection):**
 - Right-click the target in the **Sites** panel → **Attack** → **Active Scan**.
 - This actively probes for vulnerabilities like **XSS**, **SQL Injection**, and **CSRF**.
- **Passive Scan (Non-Intrusive Analysis):**
 - Automatically analyzes traffic captured by the proxy without interacting with the target system.


Cont..

- **Using ZAP's Key Tools**
- **Manual Request Testing (Request Editor):**
 - Use **Request Editor** to modify and replay HTTP requests.
- **Fuzzer (Brute-Force Testing):**
 - Right-click a request → **Attack** → **Fuzz**.
 - Select fields to **fuzz** (e.g., parameters, cookies) and provide payload lists.
- **Forced Browse (Hidden Resource Discovery):**
 - Use the **Forced Browse** tool to discover hidden directories or files.
- **WebSockets Testing:**
 - Intercept and analyze **WebSocket** messages via the **WebSockets** tab.

Cont..

- **Analyzing Scan Results**
- **View Alerts:**
 - Check the **Alerts** tab for detected vulnerabilities, their severity, and remediation suggestions.
- **Session Management:**
 - Handle complex **authentication flows** using ZAP's session tracking.
- **Generate Reports:**
 - Export findings: **Report** → **Generate HTML/XML Report** for documentation.
-  **6. Automating Scans**
- **Command-Line Mode:**
 - Use ZAP in **headless mode** for automated scans in CI/CD pipelines.
- `zap.sh -cmd -quickurl http://yourtarget.com -quickout report.html`
- **ZAP API:**
- Use the **REST API** to integrate ZAP with automation frameworks.

Cont...

- **Best Practices for Using ZAP**
- **Define Scope:** Limit testing to authorized domains.
- **Passive First:** Perform **passive scans** before **active scans**.
- **Regular Updates:** Keep ZAP and add-ons up to date.
- **Manual Verification:** Validate results to filter out **false positives**.
- **Ethical Testing:** Always get permission before scanning.
-  **8. Useful Shortcuts in ZAP**
- **Ctrl + Shift + I:** Open the **Intercept** tab.
- **Ctrl + T:** Open the **Spider** tool.
- **Ctrl + Shift + F:** Open the **Fuzzer** tool.
- **Ctrl + S:** Save the current session.

Nmap (Network Mapper) – Network Vulnerability Scanner

- **Purpose:**
 - Nmap is an open-source tool used for network discovery, port scanning, and vulnerability detection.
- **Open Source:**
 - Free to use under the GNU General Public License (GPL).
- **Port Scanning:**
 - Identifies open ports and the services running on them.
- **Operating System Detection:**
 - Determines the target system's OS using TCP/IP stack fingerprinting.
- **Service Version Detection:**
 - Identifies the version of software running on open ports.
- **Vulnerability Detection:**
 - Detects common vulnerabilities using Nmap Scripting Engine (NSE).
- **Network Mapping:**
 - Maps large networks, revealing hosts, services, and firewall settings.

Nmap (Network Mapper) – Network Vulnerability Scanner

- **Customizable Scans:**
 - Supports different scan types (TCP, UDP, SYN, ICMP, etc.) and advanced options.
- **Compatibility:**
 - Works on Linux, Windows, and macOS.
- **Output Formats:**
 - Supports various report formats (XML, grepable, and normal text).
- **Stealth Scanning:**
 - Provides low-profile scanning to evade detection (e.g., SYN and Idle scans).
- **Installation:**
 - Can be installed via package managers (e.g., `sudo apt install nmap` on Linux).
- **Common Use Cases:**
 - Penetration testing, network auditing, and security analysis.

Nmap working

- **Install Nmap**
- **On Linux (Debian/Ubuntu)**
 - `sudo apt update`
 - `sudo apt install nmap`
- **On Windows:**
 - Download from
<https://nmap.org/download.html>

Cont..

- **Basic Nmap Scan**
- **Simple Host Scan:**
Scan a target for open ports and services.
- `nmap <target>`
- `nmap 192.168.1.1`
- `nmap example.com` (for website scanning)
- `nmap -F <target>`
- `nmap -T4 -A -v <target>`
- (-A enables OS detection, version detection, script scanning, and traceroute.)
- `nmap -p 22,80,443 <target>`
- (Scans only ports 22, 80, and 443.)
- `nmap 192.168.1.1-100` (for specific range of ip address)

Cont...

- `nmap -O <target>` (OS detection)
- `nmap -sV <target>` (Identifies versions of detected services.)
- `nmap --script vuln <target>`
- (Runs vulnerability detection scripts.)
- `nmap -oN output.txt <target>`
- (save result to a file)
- `nmap -oA output <target>`
- (save in multiple format)
- `nmap -sS -sV -O -T4 -p- --script vuln 192.168.1.1`
- (Performs a full port scan, OS detection, service detection, and vulnerability check.)

Nikto – Web Server Vulnerability Scanner

- **Purpose:** Scans web servers for vulnerabilities, misconfigurations, and outdated software.
- **Open Source:** Free to use and customizable under the GNU General Public License (GPL).
- **Vulnerability Detection:** Identifies over 6,700 security issues, including dangerous files and software misconfigurations.
- **Compatibility:** Works on Linux, Windows (via Perl), and macOS.
- **SSL/TLS Support:** Scans HTTPS sites and detects SSL/TLS misconfigurations.
- **Reporting:** Outputs reports in multiple formats (HTML, CSV, XML, etc.) for analysis.
- **Virtual Host Scanning:** Supports scanning multiple domains on the same server.
- **Customization:** Allows custom test creation and plugin usage.
- **Proxy Support:** Can perform scans through HTTP/SOCKS proxies.
- **Usage:** Ideal for penetration testing, vulnerability assessments, and compliance checks.

Log Manipulation Tool in Metasploit Framework

- **Metasploit Framework Overview**
- An open-source penetration testing framework developed by Rapid7.
- Provides a collection of exploits, payloads, and auxiliary modules for security testing.
- **Log Manipulation in Metasploit**
- Attackers use Metasploit to manipulate system and application logs.
- Helps in covering tracks after exploiting a system.
- **Modules for Log Manipulation**
- **meterpreter**: Provides capabilities to clear or modify logs.
- **clearev**: A built-in Meterpreter command to erase Windows Event Logs.
- **EventLogEdit** (custom scripts): Used to modify or forge log entries.
- **Clearing System Logs**
- `run post/windows/manage/clearev`: Clears security, application, and system logs.
- Useful for hiding evidence of exploitation.

Log Manipulation Tool in Metasploit Framework

- **Modifying Log Files**
 - Requires elevated privileges to tamper with system logs.
 - Attackers use PowerShell scripts or custom payloads to edit logs.
- **Evading Detection**
 - Logs can be manipulated to mislead forensic analysis.
 - Time-stamping, fake entries, or log deletion can be used.
- **Forensic Countermeasures**
 - Security teams monitor unexpected log deletions or modifications.
 - Use of SIEM tools to detect anomalies in logging behavior.
- **Legal and Ethical Considerations**
 - Unauthorized log manipulation is illegal and unethical.
 - Used only for ethical hacking, penetration testing, and security research.

Detailed Guide on Log Manipulation Using Metasploit Framework

- **Introduction to Log Manipulation in Metasploit**
- Metasploit Framework is widely used for penetration testing, but attackers also leverage it to manipulate system logs, covering their tracks after exploitation. This guide explores different techniques for log clearing, modification, and forensic countermeasures.

Setting Up Metasploit for Log Manipulation

- **Launch Metasploit Framework**
- Open a terminal and start Metasploit:
-msfconsole
- **Gain a Meterpreter Session**
- To manipulate logs, you need a **Meterpreter session**. Use an exploit like:

```
Use exploit/windows/smb/ms17_010_eternalblue  
set RHOST <target-IP>  
exploit
```

Once the exploit is successful, you will have a **Meterpreter shell**.

- **Clearing System Logs in Windows**
- Metasploit provides a **built-in log-clearing tool** for Windows event logs.
- **Step 1: Run the Clearev Command**
- In a Meterpreter session, type:
--- clearev

This deletes:

Security logs
Application logs
System logs

- **Verify Log Deletion**
- To confirm the logs are cleared, run:
---wevtutil el

Cont.

- **Manually Modifying Logs**
- **Using PowerShell in Meterpreter**
- Open a PowerShell session in Meterpreter:
 - load powershell
 - powershell_shell

Modify event logs with:

```
Write-EventLog -LogName Application -Source  
"Security" -EntryType Information -EventID  
1000 -Message "System is normal"
```

This creates a **fake log entry** to mislead forensic investigators.

Cont..

- **Advanced Log Manipulation**
- **Using Windows Event Manipulation Tool**
- Attackers may use the following commands:
- **Delete Specific Log Entries**

```
---wevtutil cl Security
```

Backup and Remove Logs

```
wevtutil epl System C:\logs\backup.evtx
```

```
del C:\logs\backup.evtx
```

- **Using Custom Scripts for Log Injection**

- A Python script can be used to inject logs:

```
---import os
```

```
---os.system("eventcreate /ID 1000 /L APPLICATION /T  
INFORMATION /SO FakeLog /D 'This is a test log'")
```

Cont..

- **Evading Log Monitoring Systems**
- **Disabling Event Logging Services**

Stop-Service EventLog -Force

-----Stop-Service EventLog -Force

Tampering with Log Files

Takeown /F

C:\Windows\System32\winevt\Logs*.evtx

Cont..

Allows modifying or deleting logs manually.

- **Countermeasures for Defenders**
- **Monitor Log Deletion Attempts** using SIEM tools.
Use Log Forwarding (e.g., ELK Stack, Splunk) to prevent local tampering.
Enable Tamper Protection on event logs.
- **8. Ethical and Legal Considerations**
- **Unauthorized log manipulation is illegal** under cybersecurity laws like the **CFAA (U.S.)** and **GDPR (EU)**.
Use these techniques only for **authorized penetration testing and security research**.

Unit IV

- **1. Governance & Policy Requirements**
- **Documented BC/DR Policies:** Formal, approved policies that define scope, roles, and responsibilities.
- **Executive Sponsorship:** Senior management support for BC/DR initiatives.
- **Compliance & Legal:** Alignment with industry regulations (e.g., ISO 22301, NIST, GDPR, HIPAA).
- **2. Risk Assessment & Business Impact Analysis (BIA)**
- **Risk Identification:** Understand potential threats (natural disasters, cyberattacks, human error, etc.).
- **Impact Analysis:** Assess financial, operational, legal, and reputational impacts of disruptions.
- **Critical Process Identification:** Determine mission-critical functions and their dependencies.
- **3. Recovery Objectives**
- **RTO (Recovery Time Objective):** Maximum acceptable time to restore a process/system.
- **RPO (Recovery Point Objective):** Maximum tolerable data loss measured in time.
- **4. Backup & Data Protection**
- **Regular Backups:** Frequent and automated backups of critical systems and data.
- **Offsite/Cloud Storage:** Redundant, geographically separate storage.
- **Encryption & Security:** Data must be encrypted in transit and at rest.
- **5. Disaster Recovery Infrastructure**
- **DR Site(s):** Hot, warm, or cold sites ready for failover.
- **Redundancy & Failover Mechanisms:** Systems with high availability (HA) configurations.
- **Automation:** Automated DR orchestration to speed up recovery.

Unit IV

- **6. Roles & Responsibilities**
- **BC/DR Team:** Defined personnel responsible for activating and executing plans.
- **Communication Plan:** Internal and external stakeholder notification processes.
- **Third-Party Coordination:** DR expectations for vendors, partners, and service providers.
- **7. Plan Development**
- **Business Continuity Plan (BCP):** Procedures for maintaining business functions during a crisis.
- **Disaster Recovery Plan (DRP):** Steps to restore IT infrastructure and data.
- **Crisis Management Plan:** High-level response coordination and decision-making.
- **8. Testing & Exercises**
- **Regular Testing:** Tabletop exercises, simulations, and full-scale drills.
- **Plan Review:** Annual or semi-annual reviews and updates.
- **Lessons Learned:** Post-mortem analysis and continuous improvement.
- **9. Monitoring & Metrics**
- **BC/DR KPIs:** Track metrics like time to recovery, test success rate, incident frequency.
- **Audit Readiness:** Documentation of tests, changes, and incidents for auditors.
- **10. Training & Awareness**
- **Employee Training:** Awareness programs for all staff.
- **Role-Specific Training:** Advanced training for the BC/DR team.

Unit IV

- **Phase 1: Reconnaissance (Information Gathering)**
- Reconnaissance is the **first and one of the most crucial phases** of a penetration test. It involves gathering as much information as possible about the target system, network, or application—**without actually interacting** with it in a way that would trigger detection or alarms.
- There are **two types of reconnaissance**:
- **1. Passive Reconnaissance**
- Information is gathered **without directly engaging** the target.
- Involves using **public sources** such as:
 - WHOIS records
 - DNS lookups
 - Social media and company websites
 - Archive.org (Wayback Machine)
 - Google hacking (Google dorks)
 - Public documents (PDFs, DOCs, etc.)
 - Website mirroring tools like **HTTrack**

Unit IV

- **HTTrack in Reconnaissance**
- **What is HTTrack?**
- **HTTrack** is a **free and open-source website copier** that allows you to download an entire website—including HTML, images, JavaScript, and directory structure—for offline analysis.
- **Use case in pentesting:** Helps analyze the **website structure, resources, and hidden files** *without alerting the target*.
- **Key Features:**
- **Offline browsing** of websites
- Preserves **directory and link structure**
- Allows exclusion or inclusion of specific file types
- Useful in **fingerprinting** the website technologies and structure

Unit IV

- **How HTTrack Helps in Pentesting:**
- **Purpose** Benefit to the Tester
- **Analyze Website Layout** Understand how the site is built and organized
- **Discover Hidden Pages** May reveal admin pages or unused URLs
- **Check for Exposed Data** Sometimes sensitive data is unintentionally public
- **Identify Technologies** Based on files and code, you can guess the tech stack
- **Offline Testing** Safely analyze without touching the live server

Unit IV

- **Basic HTTrack Usage (CLI or GUI)**
- **Example (CLI on Linux):**
- **`httrack https://example.com -O /path/to/save/files +*.example.com/* -v`**
- `https://example.com`: target URL
- `-O`: output directory
- `+*.example.com/*`: ensures subdomains are included
- `-v`: verbose mode
- **Ethical Reminder:**
- HTTrack should **only be used on websites you own or have permission to test**. Unauthorized use can be considered illegal or unethical.

Unit IV

- **What are Google Directives?**
- **Google Directives** (or **Google operators**) are **special commands** that refine search queries to extract more specific and sometimes sensitive results from Google's massive index of the web.
- These are incredibly useful for **penetration testers, bug bounty hunters, and security researchers** to discover:
 - Sensitive files
 - Misconfigured servers
 - Login pages
 - Admin portals
 - Exposed credentials
 - Publicly indexed devices and cameras

Harvester

- **Definition: What is a Harvester?**
 - A **Harvester** is a tool designed to **gather publicly available information** about a target entity (such as a company, organization, or individual) from open sources.
 - It **automates the reconnaissance process**, making it easier and faster to collect valuable intelligence that could be used in penetration testing or malicious attacks.
-
- **2. Purpose of Using a Harvester**
 - The **main goal** of a harvester is to **collect preliminary information** about a target without actively engaging with the target's systems (this is known as **passive reconnaissance**).
 - It helps identify potential **weaknesses** or **entry points** before conducting further attacks or security audits.

Sources Harvesters Pull Information From

- **Search engines:** Google, Bing, Yahoo
- **Social networks:** LinkedIn, Facebook, Twitter
- **DNS databases:** DNSDumpster, Netcraft
- **Public code repositories:** GitHub, GitLab
- **Company websites:** Crawling pages to extract emails, employee names, etc.
- **WHOIS records:** For domain ownership details
- **Paste sites:** Like Pastebin, where leaked data may be found

Typical Users of Harvester Tools

- **Ethical Hackers / Penetration Testers:**
Use it to **simulate attacks** during security audits and help organizations **fix vulnerabilities** before bad actors find them.
- **Malicious Hackers / Threat Actors:**
Use harvesters to gather information to **plan attacks, phishing campaigns, or social engineering** strategies.
- **Security Researchers:**
Use harvesters to **analyze digital footprints** and **track potential exposures** for companies or individuals.

- **Popular Harvester Tools**

- **TheHarvester:**

The most widely used tool for OSINT gathering. It is open-source and can query multiple sources like Google, LinkedIn, Bing, and others.

- **Maltego:**

More advanced, with visualization capabilities, showing relationships between entities.

- **Recon-ng:**

A full reconnaissance framework with modules for automation.

- **Types of Data Harvesters Collect**

- **Emails:**

Employee emails are important for **phishing attacks** or **credential stuffing**.

- **Usernames:**

Useful to attempt **brute-force attacks** or impersonation.

- **Subdomains:**

Discovering subdomains helps find **less secure servers** that could be entry points.

- **IP addresses:**

Mapping servers and networks for **scanning vulnerabilities**.

- **Employee Information:**

Full names, job roles, location — very useful for **social engineering**.

Cont..

- **How Harvesters Work (Detailed Mechanism)**
- **Step 1: Input Target Information**
User provides a domain name (e.g., example.com) or company name.
- **Step 2: Query Open Sources**
The harvester tool sends **search queries** to engines and public databases using target information.
- **Step 3: Scraping and Parsing**
It extracts relevant information like emails, IPs, and usernames from search results or API responses.
- **Step 4: Organizing Data**
The information is organized into structured reports (tables, lists, visual graphs).
- **Step 5: Analysis**
Analysts or hackers study the collected data to **plan further actions**.
- **8. Usage Scenarios for Harvesters**
- **Red Team Exercises:**
To mimic how real-world attackers would gather information before breaching a system.
- **Vulnerability Assessments:**
Understand what is publicly visible and potentially exploitable.
- **Incident Response:**
After a breach, investigators use harvesters to see what data was exposed online.
- **Brand Protection:**
Companies monitor their public digital footprint using harvesters to **detect impersonation** or **data leaks** early.

Cont...

- **Risks Involved with Harvesting**
- **For Organizations:**
 - Employees' emails could be used for **targeted phishing**.
 - Subdomains could lead to **server exploitation**.
 - IP ranges could allow **network scanning and attacks**.
- **For Individuals:**
 - Exposure of personal emails, addresses, job titles can lead to **identity theft** or **fraud**.

Defense Against Information Harvesting

- **Minimize Public Exposure:**
 - Limit information about employees and emails on public websites.
- **Use Email Aliases:**
 - Instead of direct emails, use forms or temporary addresses.
- **Monitor Public Data:**
 - Regularly scan what information is visible online about your company using OSINT tools.
- **Security Awareness Training:**
 - Educate employees about **phishing** and **social engineering** tactics.
- **Technical Protections:**
 - Use CAPTCHA challenges to prevent automated data scraping.
 - Configure DNS settings to limit exposure (e.g., avoid wild DNS entries).

WHOIS

- **Definition:**
- WHOIS is a query and response protocol used to obtain **information about domain names**, IP addresses, and autonomous systems.
- **Purpose:**
- It helps identify **who owns a domain name**, **when it was registered**, and **who manages it**.
- **Information Provided:**
- Registrant name
- Registrant organization
- Contact emails
- Domain creation, update, and expiry dates
- Registrar (company managing the domain)
- Name servers

- **Common Uses in Cybersecurity:**
- **Finding the owner** of a suspicious website.
- **Tracing cyber attacks** back to domain registrations.
- **Monitoring** domain expiration to **prevent domain hijacking**.
- **Example Tools:**
- Online Whois lookup sites (e.g., whois.com)
- Command-line tool (whois example.com)
- **Important Note:**
- Some domain owners use **privacy protection services** to hide their WHOIS details.

NETCRAFT

- **Definition:**
- Netcraft is a **cybersecurity service** providing information about websites, including **hosting details, technology stack, SSL certificates, and uptime monitoring.**
- **Purpose:**
- It helps collect **OSINT (Open Source Intelligence)** about a website's infrastructure.
- **Information Provided:**
- Hosting provider
- IP address
- Server technology (e.g., Apache, Nginx)
- SSL certificate details
- Site history (when domains were hosted, moved, or taken down)
- Risk ratings (such as **phishing site detection**)

Cont..

- **Common Uses in Cybersecurity:**
- **Mapping target infrastructure** during reconnaissance.
- **Identifying outdated or vulnerable server software.**
- **Monitoring sites for phishing or malware activity.**
- **Example Services:**
- toolbar.netcraft.com (browser extension for site risk checks)
- Netcraft Site Report tool
- **Important Note:**
- Netcraft's data is very useful for **threat intelligence** and **web application security audits.**

HOST

- **Definition:**
- host is a **simple command-line utility** used for **DNS lookups** to retrieve information about domain names and IP addresses.
- **Purpose:**
- It helps **resolve domain names** to their corresponding **IP addresses** and **vice versa**.
- **Information Provided:**
- IP address of a domain
- Domain's name servers (NS records)
- Mail servers (MX records)
- Text records (TXT) such as SPF, DKIM information

Cont..

- **Common Uses in Cybersecurity:**
- **Finding the IP address** of a domain for further scanning.
- **Discovering DNS misconfigurations.**
- **Collecting subdomains** if wildcard entries are found.
- **Checking email server configurations** to spot spoofing vulnerabilities.
- **Example Commands:**
- `host example.com` (basic lookup)
- `host -t mx example.com` (look up mail servers)
- **Important Note:**
- `host` is a **lightweight** but **powerful tool** for basic DNS reconnaissance, especially before starting network scanning.

Fierce

- **Definition:**
- **Fierce** is a **domain scanner** designed to **locate non-contiguous IP space** and **hostnames** against a specified domain.
- **Purpose:**
- It performs **DNS reconnaissance** to **find subdomains, hidden hosts**, and **network infrastructure** related to a domain.
- **Key Functions:**
- Brute-force DNS (guessing subdomains using a wordlist).
- Locate nearby IPs in the target's network range.
- Identify misconfigured DNS servers.
- Perform zone transfers (if the DNS server allows it).

Cont...

- **Common Uses:**
- **Mapping domain infrastructure** before attacking or auditing.
- **Finding hidden servers** that are not indexed publicly.
- **Example Usage:**
- `fierce --domain example.com`
- **Important Note:**
- Fierce is especially useful for **internal pentests** and **red team exercises**, but it **does not perform actual exploitation** — just information gathering.

Other Tools to Extract Information from DNS

- **Dig (Domain Information Groper)**
- **Definition:**
- A powerful **command-line DNS lookup** tool.
- **Purpose:**
- Retrieve various DNS records like A, AAAA, MX, TXT, NS.
- **Key Functions:**
- Check DNS resolution accuracy.
- Analyze DNS response times.
- Fetch complete DNS zone information (if available).
- **Example Usage:**
- `dig example.com` (A record)
- `dig MX example.com` (Mail servers)
- `dig AXFR example.com @nameserver` (Zone transfer attempt)

Nslookup

- **Definition:**
- A basic tool to **query DNS servers** and obtain domain name or IP address mapping.
- **Purpose:**
- Test and troubleshoot DNS problems.
- **Key Functions:**
- Resolve domain names to IPs.
- Get mail server (MX) records.
- **Example Usage:**
- `nslookup example.com`
- `nslookup -type=mx example.com`

DNSenum

- **Definition:**
- An **automated script** designed for **DNS enumeration**.
- **Purpose:**
- Gather extensive DNS information automatically.
- **Key Functions:**
- Subdomain brute-forcing.
- Zone transfer checking.
- Finding IP ranges.
- WHOIS lookups.
- **Example Usage:**
- `dnsenum example.com`
- **Important Note:**
- DNSenum is often used in **CTF competitions** and **penetration testing** engagements.

DNSRecon

- **Definition:**
- A Python-based tool for **advanced DNS enumeration**.
- **Purpose:**
- Perform **standard record retrieval, brute-forcing, reverse lookups, and zone transfers**.
- **Key Functions:**
- Standard record enumeration (A, NS, SOA, MX, TXT).
- Brute force subdomains with custom wordlists.
- Reverse lookups over IP ranges.
- **Example Usage:**
- `dnsrecon -d example.com`
- **Important Note:**
- DNSRecon can **save output** into different formats for later analysis.



MetaGooFil

- **Definition:**
- **MetaGooFil** is an **information gathering (OSINT)** tool used to **extract metadata** from **public documents** (PDFs, DOCs, PPTs, XLSs, etc.) available on a target's website.
- **Purpose:**
- To **discover sensitive information** hidden in document metadata, which can reveal details about an organization's **infrastructure** and **employees**.
- **Key Functions:**
- Search public documents linked to a domain.
- Download documents and extract metadata.
- Identify usernames, software versions, machine names, and paths.
- **Common Metadata Extracted:**
- Author/Username
- Software name and version
- Operating system information
- File paths and directory structures

Cont..

- **How It Works:**
- Performs **Google dorking** (advanced search queries) to find documents.
- Downloads the files automatically.
- Analyzes the metadata embedded inside them.
- **Common Uses in Cybersecurity:**
- **Penetration testers** use it to gather technical details.
- **Attackers** can use it for **social engineering** and **targeted attacks**.
- **Security teams** use it to **audit public exposure** of sensitive metadata.
- **Example:**
- Finding the Windows version used by a company based on Word document metadata can help an attacker craft specific exploits.
- **Important Note:**
- Organizations should **sanitize documents** before publishing to avoid leaking sensitive metadata.


CThreat Agent – Attack of Drones

- **Definition:**
- **Attack of Drones** refers to the **threat agent** where **unmanned aerial vehicles (UAVs)** (drones) are used as a **vector for cyberattacks or physical attacks**.
-  **Purpose:**
- Drones can be weaponized or used to carry **malicious hardware/software** to perform **cyber-physical attacks**.
-  **Key Attack Vectors:**
- **Network intrusion:** Dropping rogue Wi-Fi access points to hijack connections.
- **Surveillance:** Spying on secure facilities, recording video/audio.
- **Payload delivery:** Dropping malicious USBs, hardware trojans, or explosives.
- **Signal jamming:** Jamming Wi-Fi, GPS, or other communications.

Cont..

- **Examples of Drone-based Threats:**
- A drone hovering outside an office to intercept Wi-Fi signals (e.g., using tools like WiFi Pineapple).
- Dropping malware-infected USB drives inside a company premises (USB drop attack).
- Using drones to map facility layouts using cameras for later attacks.
- **Common Uses in Cybersecurity:**
- **Red teams** simulate drone attacks to test organization defenses.
- **Military and critical infrastructure** are primary targets for real-world drone threats.
- **Real Incidents:**
- Drones have been used to **smuggle malware** into secure areas.
- Some criminals have used drones to **disable security cameras** or **deliver hacking devices**.

Cont..

- **Important Note:**
- Drone attacks combine **cybersecurity risks** with **physical security risks** — a growing area known as **cyber-physical security**.
-  **Defenses Against Drone Threats:**
- Use **drone detection systems** (radar, RF scanners, cameras).
- Implement **no-fly zones** and **geofencing**.
- **Monitor and secure wireless networks** from external threats.

Sifting through the Intel to Find Attackable Targets.

- **Definition:**
- After gathering a large amount of **raw intelligence (OSINT)** about a target, this step involves **analyzing, filtering, and prioritizing** the collected data to find **real, exploitable attack surfaces**.

Cont..

- **Data Collection Phase**
- Initially, huge volumes of information are collected:
 - Domains, IP addresses, subdomains
 - Email addresses, employee names
 - Document metadata, technology stacks
 - Physical addresses and organizational charts
- **2. Filtering Relevant Information**
- Not all collected data is useful.
- Sifting involves **removing irrelevant or redundant information** and **keeping high-value data**, like:
 - Live IPs and active domains
 - Emails of technical staff (good phishing targets)
 - Exposed internal documents
 - Servers running outdated software

Cont..

- **Identifying Valuable Assets**
- After cleaning the data, focus shifts to **assets that matter**, such as:
 - Public-facing servers (web servers, email servers)
 - Outdated systems (legacy portals)
 - Employee credentials (for phishing or credential stuffing)
 - Unsecured APIs and databases
- **4. Prioritizing Targets**
- Targets are **ranked** based on how vulnerable they might be and how critical they are.
- Factors considered include:
 - Exposure to the internet
 - Known vulnerabilities (CVE records)
 - Lack of security protections (e.g., missing SSL, open ports)
 - Accessibility without authentication

Cont..

- **Analyzing Attack Vectors**
- For each high-priority target, potential **attack methods** are identified:
 - Phishing attacks (using email intel)
 - Web application attacks (using exposed web servers)
 - Network intrusions (using vulnerable services)
 - Social engineering (using employee info)
- **6. Documenting Findings**
- Clear documentation of:
 - What information was collected
 - What targets were found
 - Why these targets are considered attackable
 - What potential impact an attack could have
- **7. Feedback Loop (Continuous Refinement)**
- As new intel is gathered, analysts keep **reassessing targets**.
- Attackable surfaces **change over time** as companies update their systems or leak new data.