Name:	**Mehran Ali**
Company	**Internee.pk**
Program:	**Internship**
Task id	TSK-000-181

Task Details

Task Cybersecurity Fundamentals:

Category Cyber Security

Learn the basics of cybersecurity, including threats, vulnerabilities, and risk management.

What is Cyber Security?

- Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.
- It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks, and technologies.

Threats:

- **Malware**: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Examples include viruses, worms, Trojans, and ransomware.
- **Phishing**: Attempts to trick individuals into revealing sensitive information, such as passwords or financial details, through deceptive emails, messages, or websites.
- **Denial of Service (DoS) / Distributed Denial of Service (DDoS)**: Overloading a system or network with excessive traffic to disrupt normal operation and make services unavailable to legitimate users.
- **Insider Threats**: Risks posed by individuals within an organization who misuse their access privileges to steal data, sabotage systems, or carry out other malicious activities.
- **Advanced Persistent Threats (APTs)**: Sophisticated, long-term cyberattacks orchestrated by skilled adversaries targeting specific organizations or individuals to steal sensitive information or disrupt operations.

Vulnerabilities:

- **Software Vulnerabilities:** Weaknesses in software applications or operating systems that can be exploited to compromise system integrity or confidentiality. These may include unpatched software, insecure configurations, or design flaws.
- **Human Vulnerabilities**: Employees or users who inadvertently or intentionally compromise security through actions such as falling victim to phishing scams, sharing passwords, or neglecting security best practices.
- **Infrastructure Vulnerabilities**: Weaknesses in network devices, servers, and other hardware components that can be exploited to gain unauthorized access or disrupt services. Examples include misconfigured firewalls, outdated firmware, and weak encryption protocols.

Risk Management:

- **Risk Assessment**: Identifying, analyzing, and evaluating potential cybersecurity risks to an organization's assets, including data, systems, and operations.
- **Risk Mitigation**: Implementing controls and measures to reduce the likelihood and impact of identified risks. This may involve applying security patches, implementing access controls, and providing security awareness training.
- **Incident Response**: Developing and implementing plans and procedures to detect, respond to, and recover from cybersecurity incidents effectively. This includes establishing communication channels, defining roles and responsibilities, and conducting post-incident reviews to identify lessons learned.
- **Compliance and Regulations**: Ensuring compliance with relevant laws, regulations, and industry standards governing cybersecurity practices. This may include data protection laws (e.g., GDPR, CCPA), industry-specific

regulations (e.g., PCI DSS for payment card industry), and international standards (e.g., ISO 27001).

Understand common attack vectors and security best practices.

1. **Phishing Attacks**:
    - **Attack Vector**: Phishing attacks involve tricking individuals into divulging sensitive information such as login credentials or financial details by impersonating trusted entities via emails, messages, or websites.
    - **Best Practices**:
        - Educate users about recognizing phishing attempts through security awareness training.
        - Implement email filtering and anti-phishing tools to detect and block suspicious emails.
        - Encourage users to verify the legitimacy of requests for sensitive information before responding.
2. **Malware Infections**:
    - **Attack Vector**: Malware, including viruses, Trojans, worms, and ransomware, can infect systems through malicious email attachments, compromised websites, or removable media.
    - **Best Practices**:
        - Keep software and operating systems up-to-date with the latest security patches and updates.
        - Deploy antivirus and anti-malware software to detect and remove malicious software.
        - Exercise caution when downloading files or clicking on links from unknown or untrusted sources.
3. **Password Attacks**:

- **Attack Vector**: Password attacks involve attempting to guess or steal user passwords through methods such as brute-force attacks, dictionary attacks, or password phishing.
- **Best Practices**:
  - Enforce strong password policies, including requirements for length, complexity, and regular expiration.
  - Implement multi-factor authentication (MFA) to add an extra layer of security beyond passwords.
  - Encourage users to use unique passwords for each account and to avoid sharing passwords or writing them down.

4. **Insider Threats**:
   - **Attack Vector**: Insider threats originate from individuals within an organization who misuse their access privileges to steal data, sabotage systems, or carry out other malicious activities.
   - **Best Practices**:
     - Implement least privilege access controls to limit users' access to only the resources and information necessary for their roles.
     - Monitor user activities and behavior for signs of unauthorized or suspicious behavior.
     - Provide ongoing security awareness training to educate employees about the risks of insider threats and how to report suspicious activities.
5. **Denial of Service (DoS) / Distributed Denial of Service (DDoS) Attacks**:
   - **Attack Vector**: DoS and DDoS attacks aim to disrupt or degrade the availability of services by overwhelming target systems or networks with excessive traffic.
   - **Best Practices**:
     - Implement network and application-level defenses, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and rate limiting.

- Use content delivery networks (CDNs) and DDoS mitigation services to absorb and filter malicious traffic.
- Develop incident response plans to quickly detect and mitigate the impact of DoS/DDoS attacks on critical services.

6. **Unpatched Software Vulnerabilities**:
    - **Attack Vector**: Attackers exploit vulnerabilities in software applications or operating systems that have not been patched or updated with security fixes.
    - **Best Practices**:
        - Establish patch management procedures to regularly apply security updates and patches to all systems and software.
        - Prioritize patching for critical vulnerabilities with known exploits or high severity ratings.
        - Use vulnerability scanning tools to identify and remediate unpatched vulnerabilities proactively.

Network Security and Penetration Testing:

Network security and penetration testing are critical aspects of cybersecurity aimed at safeguarding an organization's network infrastructure from unauthorized access, data breaches, and other security threats. Here's an overview of network security principles and the process of conducting penetration testing:

1. **Network Security Principles**:
    - **Perimeter Security**: Implementing firewalls, intrusion detection/prevention systems (IDS/IPS), and other network security devices to control inbound and outbound traffic and protect against unauthorized access.
    - **Access Control**: Enforcing access controls such as authentication mechanisms, role-based access control (RBAC), and virtual private

networks (VPNs) to restrict access to sensitive resources based on user roles and privileges.

- **Encryption**: Using encryption protocols such as SSL/TLS for securing data in transit and encrypting sensitive information stored on network devices and servers to prevent unauthorized interception and access.
- **Patch Management**: Regularly applying security updates and patches to network devices, servers, and applications to address known vulnerabilities and reduce the risk of exploitation.
- **Monitoring and Logging**: Deploying network monitoring tools and logging mechanisms to detect and respond to suspicious activities, intrusions, and security incidents in real-time.

2. **Penetration Testing**:

Penetration testing, also known as pen testing or ethical hacking, is the process of simulating cyber attacks on a network, system, or application to identify vulnerabilities and assess security controls. Here's an overview of the penetration testing process:

- **Planning and Preparation**: Define the scope, objectives, and rules of engagement for the penetration test. Obtain proper authorization from stakeholders and ensure compliance with legal and ethical guidelines.
- **Reconnaissance**: Gather information about the target network, including IP addresses, domain names, network topology, and potential entry points. Use passive techniques such as OSINT and active techniques such as network scanning to identify targets.
- **Vulnerability Analysis**: Identify and enumerate vulnerabilities in the target network, systems, and applications using tools such as Nmap, Nessus, or OpenVAS. Analyze the results to prioritize vulnerabilities based on severity and potential impact.
- **Exploitation**: Attempt to exploit identified vulnerabilities to gain unauthorized access, escalate privileges, or compromise sensitive data.

Use techniques such as SQL injection, buffer overflow, or social engineering to demonstrate the impact of successful attacks.

- **Post-Exploitation**: Maintain access to compromised systems and conduct further reconnaissance to gather additional information about the target environment. Document the techniques and tools used during the exploitation phase.
- **Reporting and Remediation**: Document the findings of the penetration test, including detailed descriptions of vulnerabilities, their potential impact, and recommended mitigation strategies. Present the findings to stakeholders and provide guidance on addressing identified weaknesses and improving overall security posture.

- Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.
- Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

Dive into network security concepts and practices.

Network Security Fundamentals:

- **Confidentiality**: Ensuring that sensitive information is accessible only to authorized individuals or systems.
- **Integrity**: Protecting data from unauthorized modification, ensuring that it remains accurate and trustworthy.

- **Availability**: Ensuring that network resources and services are accessible to authorized users when needed, without interruption or degradation.
- **Authentication**: Verifying the identity of users, devices, or services to ensure that only legitimate entities are granted access to network resources.
- **Authorization**: Granting or restricting access to network resources based on the authenticated identity and assigned permissions of users or devices.
- **Non-Repudiation**: Preventing individuals from denying their actions or transactions, typically achieved through techniques such as digital signatures or audit trails.

2. **Network Security Controls:**
   - **Firewalls**: Devices that control and monitor traffic between networks, enforcing security policies to allow or deny access based on predefined rules.
   - **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS):** Tools that monitor network traffic for signs of suspicious or malicious activity and can either detect or actively block such activity.
   - **Virtual Private Networks (VPNs)**: Encrypted tunnels that allow secure communication over untrusted networks, enabling remote access or connecting geographically distributed networks.
   - **Access Control Lists (ACLs)**: Lists of rules or filters applied to network devices to control traffic flow based on specified criteria such as source IP address, destination IP address, and port numbers.
   - **Encryption**: Techniques such as SSL/TLS for securing data in transit and encrypting sensitive information stored on network devices or servers.

- **Network Segmentation**: Dividing a network into smaller, isolated segments to contain security breaches and limit the spread of malicious activity.

3. **Best Practices for Network Security**:
   - **Regular Security Audits**: Conduct periodic assessments of network infrastructure, configurations, and security controls to identify weaknesses and areas for improvement.
   - **Patch Management**: Implement procedures to apply security patches and updates promptly to address known vulnerabilities in network devices, operating systems, and applications.
   - **User Awareness Training**: Educate users about common security threats, best practices for password management, and how to recognize and report suspicious activities.
   - **Strong Authentication**: Enforce the use of strong, unique passwords or implement multi-factor authentication (MFA) to enhance access control and prevent unauthorized access.
   - **Network Monitoring**: Deploy monitoring tools to detect and respond to anomalous behavior, unauthorized access attempts, and security incidents in real-time.
   - **Incident Response Plan**: Develop and maintain a comprehensive incident response plan outlining procedures for detecting, responding to, and recovering from cybersecurity incidents.

Explore penetration testing tools and methodologies.

Penetration testing tools and methodologies play a crucial role in identifying vulnerabilities and assessing the security posture of an organization's network, systems, and applications. Here's an overview of some common penetration testing tools and methodologies:

1. Penetration Testing Tools:

- **Nmap**: A powerful network scanning tool used for discovering hosts and services on a network, as well as identifying open ports, OS versions, and potential vulnerabilities.
- **Metasploit Framework**: An advanced penetration testing platform that enables testers to exploit known vulnerabilities, perform post-exploitation activities, and simulate real-world attacks.
- **Burp Suite**: A comprehensive web application security testing tool used for scanning, crawling, and exploiting vulnerabilities in web applications, including SQL injection, XSS, CSRF, and more.
- **OWASP ZAP (Zed Attack Proxy)**: An open-source web application security scanner that helps identify vulnerabilities and security issues in web applications, APIs, and microservices.
- **Nessus**: A vulnerability scanner that scans network devices and systems for known vulnerabilities, misconfigurations, and security weaknesses, providing detailed reports and remediation recommendations.
- **Wireshark**: A network protocol analyzer used for capturing and analyzing network traffic in real-time, helping to detect anomalies, identify security threats, and troubleshoot network issues.
- **Aircrack-ng**: A suite of tools for auditing wireless networks, including packet sniffing, packet injection, and cracking WEP/WPA/WPA2-PSK encryption keys.
- **John the Ripper**: A password cracking tool used to test the strength of passwords by attempting to crack password hashes obtained from various sources, such as password files or network captures.

2. Penetration Testing Methodologies:

- **Preparation**: Define the scope, objectives, and rules of engagement for the penetration test. Obtain proper authorization and gather necessary information about the target network, systems, and applications.
- **Reconnaissance**: Gather information about the target organization, including IP addresses, domain names, network topology, and potential entry points. Use passive techniques such as OSINT and active techniques such as network scanning to identify targets.
- **Vulnerability Analysis**: Identify and enumerate vulnerabilities in the target network, systems, and applications using tools such as Nmap, Nessus, or Burp Suite. Analyze the results to prioritize vulnerabilities based on severity and potential impact.
- **Exploitation**: Attempt to exploit identified vulnerabilities to gain unauthorized access, escalate privileges, or compromise sensitive data. Use techniques such as SQL injection, buffer overflow, or social engineering to demonstrate the impact of successful attacks.
- **Post-Exploitation**: Maintain access to compromised systems and conduct further reconnaissance to gather additional information about the target environment. Document the techniques and tools used during the exploitation phase.
- **Reporting and Remediation**: Document the findings of the penetration test, including detailed descriptions of vulnerabilities, their potential impact, and recommended mitigation strategies. Present the findings to stakeholders and provide guidance on addressing identified weaknesses and improving overall security posture.

Conduct ethical hacking exercises to identify and mitigate vulnerabilities.

batch script viruses

Batch Scripts are stored in simple text files containing lines with commands that get executed in sequence, one after the other. **Batch** files are often **used** to help load programs, run multiple processes at a time, and perform common or repetitive tasks. For example, a **batch** job could be **used** to back up files, process log files, run a series of calculations or diagnostics, or any other job that require multiple **commands** to run.

The steps to make this viruses executable are:

1 Make a text file

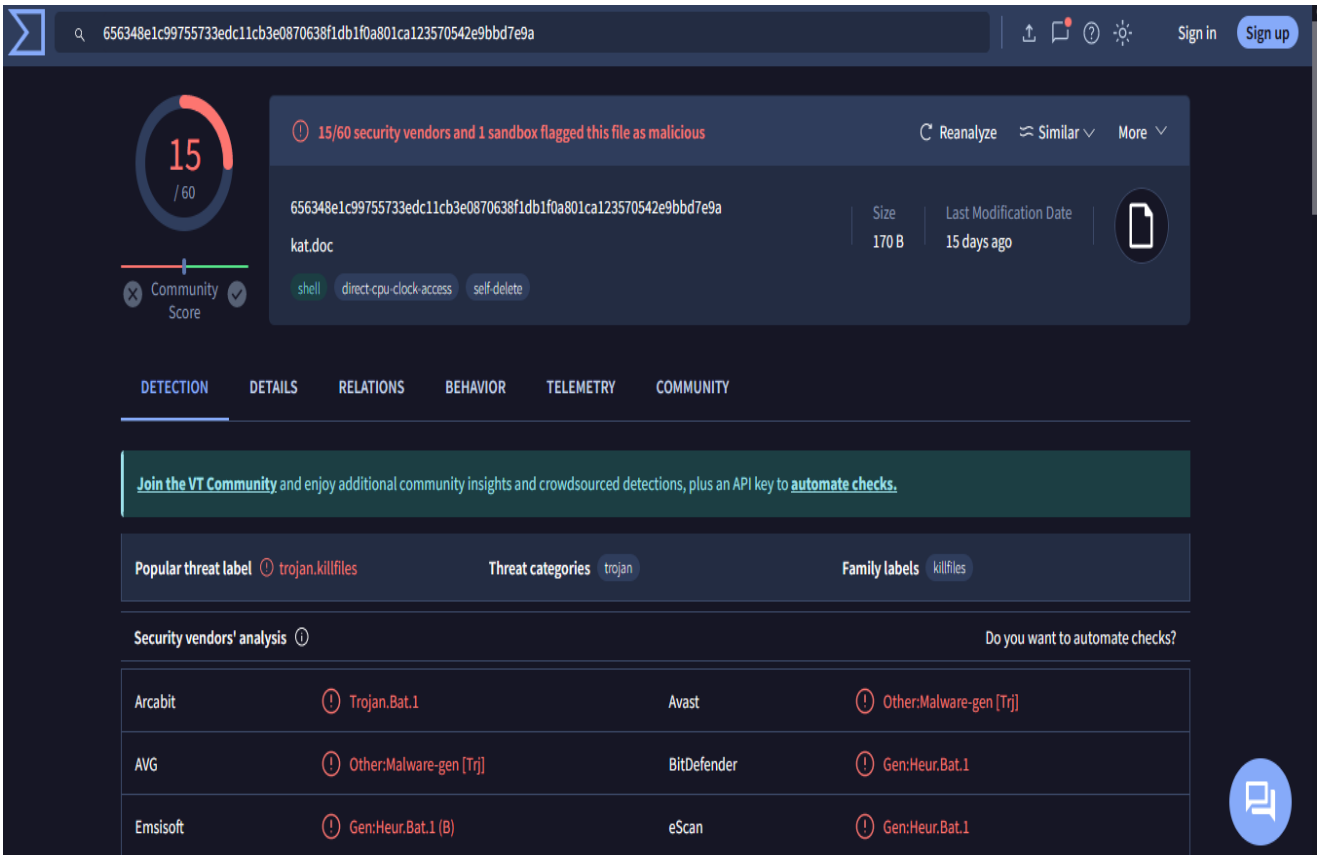
2 Paste code

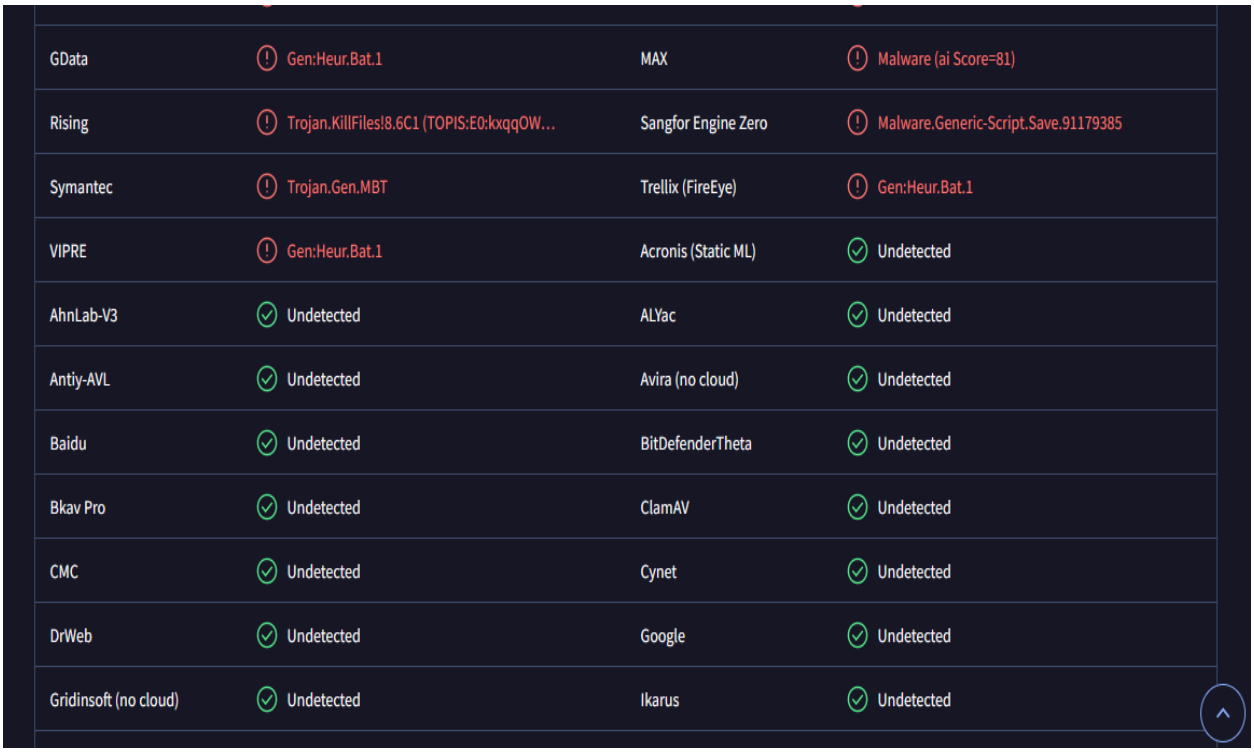
3 Save as all files with extension .bat (test.bat)

VIRUS 1 — DELETE ALL PARTITIONS

#Scan and Find Vulnerability

#Used Virustotal for scanning and Findings vulnerabilities





GData	Gen:Heur.Bat.1	MAX	Malware (ai Score=81)
Rising	Trojan.KillFiles!8.6C1 (TOPIS:E0:kxqqOW...	Sangfor Engine Zero	Malware.Generic-Script.Save.91179385
Symantec	Trojan.Gen.MBT	Trellix (FireEye)	Gen:Heur.Bat.1
VIPRE	Gen:Heur.Bat.1	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	Cynet	Undetected
DrWeb	Undetected	Google	Undetected
Gridinsoft (no cloud)	Undetected	Ikarus	Undetected

- **When file Scan if vulnerabilities find then delete the file or not open it and save your system.**

VAPT Report

Target URL: https://www.portent.com

Tool Used :WPScan

Technology used by URL :Wordpress

- ❖ Found By: Robots Txt (Aggressive Detection)
- ✓ Confidence: 100%

- ❖ https://www.portent.com/readme.html
- ✓ | Found By: Direct Access (Aggressive Detection)
- ✓ | Confidence: 100%

- ❖ https://www.portent.com/wp-content/backup-db/
  - ✓ Found By: Direct Access (Aggressive Detection)
  - ✓ Confidence: 70%

- ❖ This site has 'Must Use Plugins': https://www.portent.com/wp-content/mu-plugins/
  - ✓ Found By: Direct Access (Aggressive Detection)
  - ✓ Confidence: 80%

- ❖ WordPress version 6.0.1 identified (Insecure, released on 2022-07-12).
  - ✓ Found By: Unique Fingerprinting (Aggressive Detection)

- ❖ The main theme could not be detected.

15 vulnerabilities identified:

01. Title: WP < 6.0.2 - Reflected Cross-Site Scripting

    Fixed in: 6.0.2

02. Title: WP < 6.0.2 - Authenticated Stored Cross-Site Scripting

    Fixed in: 6.0.2

03. WP < 6.0.2 - SQLi via Link API

    Fixed in: 6.0.2

04. Title: WP < 6.0.3 - Stored XSS via wp-mail.php

    Fixed in: 6.0.3

05. WP < 6.0.3 - Open Redirect via wp_nonce_ays

    Fixed in: 6.0.3

06.Title: WP < 6.0.3 - Email Address Disclosure via wp-mail.php

07. Title: WP < 6.0.3 - Reflected XSS via SQLi in Media Library

    Fixed in: 6.0.3

08. Title: WP < 6.0.3 - CSRF in wp-trackback.php

    Fixed in: 6.0.3

09. Title: WP < 6.0.3 - Stored XSS via the Customizer

    Fixed in: 6.0.3

10. Title: WP < 6.0.3 - Stored XSS via Comment Editing

    Fixed in: 6.0.3

11. Title: WP < 6.0.3 - Content from Multipart Emails Leaked

    Fixed in: 6.0.3

12. Title: WP < 6.0.3 - SQLi in WP_Date_Query

    Fixed in: 6.0.3

13. Title: WP < 6.0.3 - Stored XSS via RSS Widget

    Fixed in: 6.0.3

14. Title: WP < 6.0.3 - Data Exposure via REST Terms/Tags Endpoint

    Fixed in: 6.0.3

15. Title: WP < 6.0.3 - Multiple Stored XSS via Gutenberg

    Fixed in: 6.0.3

Plugin(s) Identified:

- Gravityforms
  The version is out of date, the latest version is 2.6.7
- tablepress
- Enumerating Config Backups (via Aggressive Methods)
- WPVulnDB API OK