Report

Task 1: Introduction to Network Security Basics

Name-Neha Kumari

Mail id- [nehaguptacom04@gmail.com](mailto:nehaguptacom04@gmail.com)

**Summary of the network threats:-**

Network research threats are potential security vulnerabilities or risks that can be exploited by attackers to gain unauthorized access to a network, steal sensitive information, or disrupt network operations. Here's a summary of some common network research threats:

1. Reconnaissance Attacks: Attackers gather information about the target network, its infrastructure, and its defenses. This can include:

- Scanning for open ports and services

- Identifying network devices and their IP addresses

- Gathering information about network topology and routing

2. Network Scanning and Probing: Attackers use tools like Nmap, Zenmap, or Nessus to scan networks for open ports, running services, and vulnerabilities. They may also probe for weak or default credentials.

3. Man-in-the-Middle (MitM) Attacks: Attackers intercept and potentially alter communication between two parties without their knowledge. Examples include:

- ARP spoofing

- DNS spoofing

- SSL/TLS stripping

4. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: Attackers overwhelm network resources or infrastructure, making services unavailable to legitimate users.

5. Network Sniffing: Attackers capture and analyze network traffic to extract sensitive information, such as passwords, credit card numbers, or other personal data.

6. Wireless Network Attacks: Attackers target wireless networks using techniques like:

- Rogue access points

- Evil twin attacks

- WEP/WPA/WPA2 cracking

7. Phishing and Spear-Phishing: Attackers trick users into revealing sensitive information or downloading malware through deceptive emails or messages.

8. Malware and Ransomware: Attackers deploy malicious software that can steal data, encrypt files, or disrupt network operations.

9. Advanced Persistent Threats (APTs): Sophisticated and targeted attacks by threat actors, often state-sponsored, that aim to gain long-term access to a network for stealing information or disrupting operations.

10. Zero-Day Exploits: Attackers exploit previously unknown vulnerabilities in software or hardware before a patch is available.

11. DNS Attacks: Attackers exploit vulnerabilities in the Domain Name System (DNS) to redirect traffic, steal data, or disrupt services. Examples include:

- DNS cache poisoning

- DNS tunneling

- DNS amplification attacks

12. Password Attacks: Attackers use techniques like brute force, dictionary attacks, or social engineering to gain unauthorized access to systems or data.

13. Insider Threats: Malicious or negligent actions by employees, contractors, or partners that can lead to data breaches or other security incidents.

14. Supply Chain Attacks: Attackers target third-party vendors, suppliers, or partners to gain access to a primary target's network.

**The security measures implemented and why: -**

In the context of network research threats, here are some security measures that can be implemented and the reasons behind each:

1. Network Segmentation:

- Why: Segmenting the network into smaller, isolated segments reduces the attack surface and limits the spread of threats. Even if one segment is compromised, others remain protected.

- How: Use firewalls, VLANs, and access control lists (ACLs) to divide the network.

2. Intrusion Detection and Prevention Systems (IDPS):

- Why: IDPS can detect and prevent network attacks by monitoring traffic for suspicious activities or policy violations.

- How: Deploy IDS/IPS appliances or software solutions that analyze network traffic and log activities.

3. Regular Patching and Updates:

- Why: Keeping systems and software up-to-date protects against known vulnerabilities that attackers can exploit.

- How: Implement a patch management process to ensure timely updates and patch deployments.

4. Strong Access Controls:

- Why: Restricting access to network resources based on the principle of least privilege reduces the risk of unauthorized access and potential damage.

- How: Implement role-based access control (RBAC), multi-factor authentication (MFA), and regular access reviews.

5. Network Monitoring and Logging:

- Why: Continuous monitoring and logging help detect anomalies, investigate incidents, and maintain compliance.

- How: Use security information and event management (SIEM) systems to collect, analyze, and store logs from various network devices and systems.

6. Encryption:

- Why: Encrypting data at rest and in transit protects sensitive information from unauthorized access, even if intercepted.

- How: Implement encryption protocols like TLS/SSL for data in transit and AES for data at rest.

7. Employee Training and Awareness:

- Why: Educating employees about security threats and best practices reduces the risk of human error and improves overall security posture.

- How: Conduct regular training sessions, phishing simulations, and awareness campaigns.

8. Secure Configuration Management:

- Why: Properly configuring network devices and systems minimizes vulnerabilities and reduces the attack surface.

- How: Follow security best practices and use configuration management tools to enforce secure configurations.

9. Regular Penetration Testing and Vulnerability Assessments:

- Why: Proactive testing identifies vulnerabilities and weaknesses that can be exploited by attackers.

- How: Conduct regular penetration tests and vulnerability assessments using tools like Nessus, Nmap, and Metasploit.

10. Incident Response Plan:

- Why: A well-defined incident response plan helps minimize damage and quickly recover from security incidents.

- How: Develop, test, and maintain an incident response plan that includes procedures for detection, analysis, containment, eradication, and recovery.

11. Secure Wireless Networks:

- Why: Wireless networks can be particularly vulnerable to attacks. Securing them protects both the network and the data transmitted over it.

- How: Implement strong encryption (WPA3), change default SSIDs and passwords, and regularly update wireless devices.

12. DNS Security (DNSSEC):

- Why: DNSSEC protects against DNS-based attacks by ensuring the authenticity and integrity of DNS records.

- \*\*How\*\*: Implement DNSSEC to digitally sign DNS records and validate their authenticity.

13. Email Security:

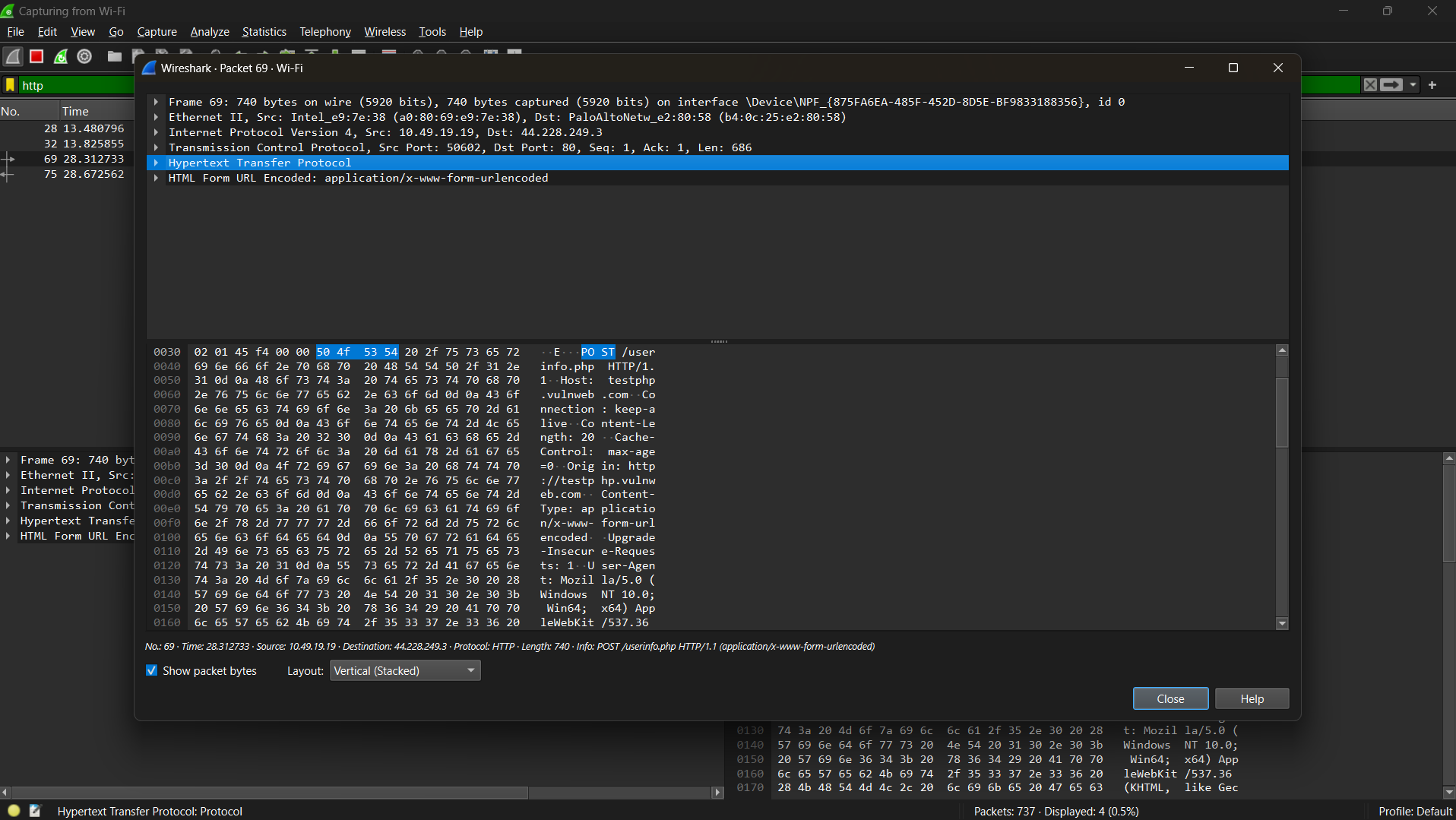
- Why: Email is a common vector for phishing and malware attacks. Enhancing email security reduces these risks.

- How: Implement email filtering, anti-spam solutions, and user education to recognize and avoid phishing attempts.

14. Regular Backups:

- Why: Regular backups ensure that critical data can be restored in the event of a ransomware attack or data loss.

- How: Implement a backup strategy that includes regular, automated backups and secure offsite storage.



The image shows a Wireshark capture of network traffic, specifically focusing on an HTTP POST request. Here's a breakdown of the components:

1. Frame Information:

- Frame 69: Indicates this is the 69th packet captured.

- 740 bytes captured: Total size of the packet captured.

- Ethernet II: The packet is using Ethernet II framing.

- Source and Destination MAC Addresses: Shows the source and destination MAC addresses of the devices involved in the communication.

2. IP Layer:

- Internet Protocol Version 4 (IPv4): Indicates the use of IPv4 for the packet.

- Source and Destination IP Addresses: The IP addresses of the source (10.49.19.19) and destination (44.228.249.3) devices.

3. Transport Layer:

- Transmission Control Protocol (TCP): Indicates the use of TCP for reliable communication.

- Source and Destination Ports: Source port (50602) and destination port (80, which is standard for HTTP).

4. Application Layer:

- Hypertext Transfer Protocol (HTTP): The application layer protocol being used.

- Request Type: It shows a POST request to `/user/info.php`, indicating data is being sent to this endpoint.

- Content Type: The request is using `application/x-www-form-URL encoded`, which is common for form submissions.

5. Payload Data:

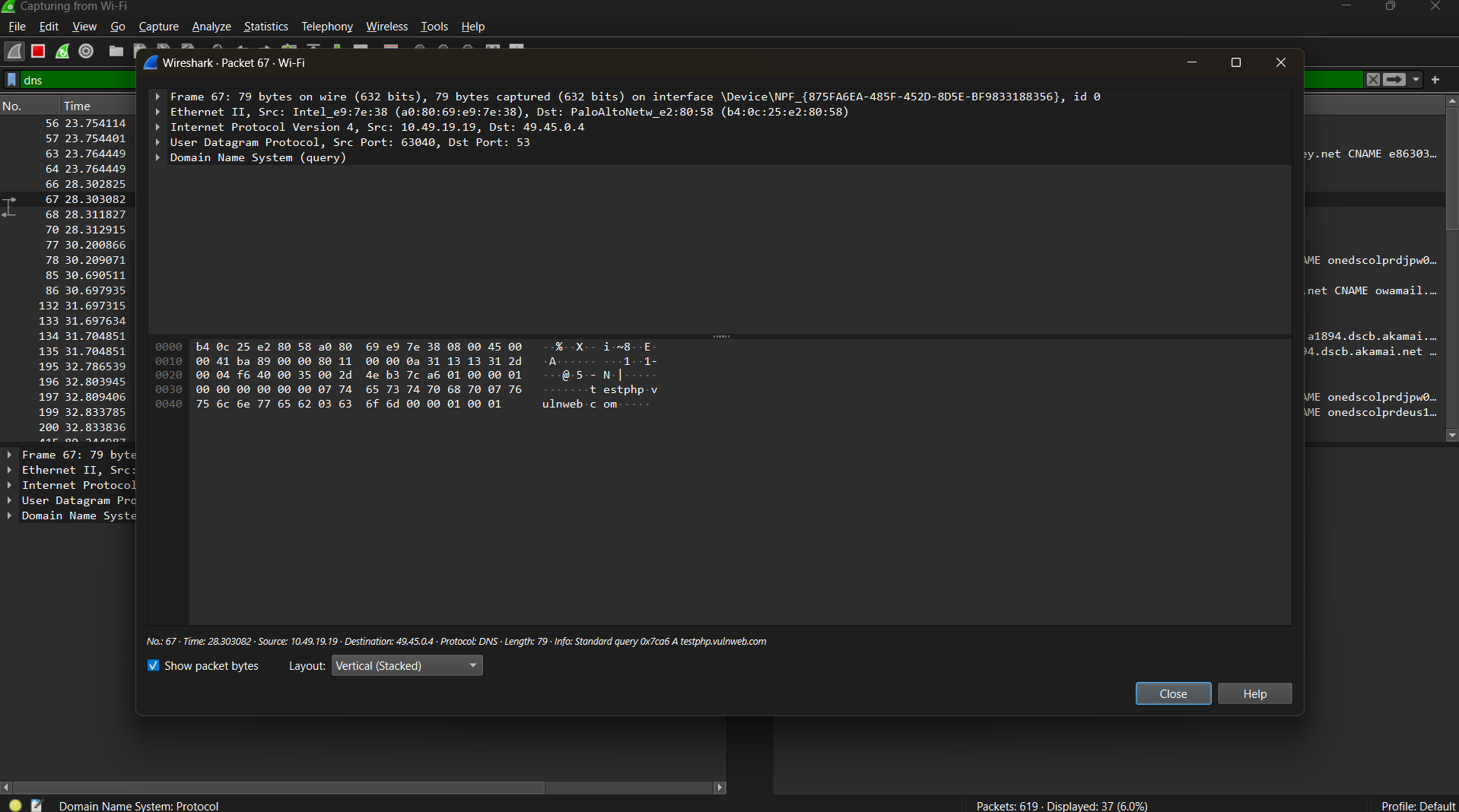
- The hex and ASCII representation of the packet data. The ASCII section shows the headers and values being sent in the POST request, including:

- Host: `testphp.vulnweb.com`

- User-Agent: Information about the client making the request (in this case, a browser on Windows 10).

6. Additional Information:

- The bottom pane shows the raw bytes of the packet, allowing for detailed inspection of the data being transmitted.



The image depicts a Wireshark capture of a DNS query. Here's a detailed breakdown of the components:

1. Frame Information:

- Frame 67: Indicates this is the 67th packet captured.

- 79 bytes captured: Total size of the packet captured.

- Ethernet II: The packet is using Ethernet II framing.

- Source and Destination MAC Addresses: Displays the source (Intel MAC address) and destination MAC addresses involved in the communication.

2. IP Layer:

- Internet Protocol Version 4 (IPv4): Indicates that IPv4 is being used.

- Source and Destination IP Addresses: The source IP (10.49.19.19) and destination IP (49.45.0.4) are shown.

3. Transport Layer:

- User Datagram Protocol (UDP): This packet uses UDP, which is connectionless and typically used for DNS queries.

- Source and Destination Ports: The source port (63040) and destination port (53, which is standard for DNS).

4. Application Layer:

- Domain Name System (DNS): The application layer protocol being used.

- Query Type: The query is a standard DNS query for an A record (address record) for the domain `testphp.vulnweb.com`.

5. Payload Data:

- The hex and ASCII representation of the packet data. The ASCII section shows the DNS query details, including:

- Transaction ID: A unique identifier for the DNS query.

- Flags: Indicate the type of query (standard in this case).

- Question Section: Contains the domain name being queried (`testphp.vulnweb.com`).

6. Additional Information:

- The bottom pane shows the raw bytes of the packet, allowing for detailed inspection of the data being transmitted.

**A discussion on how these basic security measures help protect the network.**

Basic security measures are essential for protecting a network from various threats and vulnerabilities. Here’s a discussion on how these measures contribute to overall network security:

1. Firewalls

- Function: Firewalls act as a barrier between trusted internal networks and untrusted external networks. They monitor and control incoming and outgoing network traffic based on predetermined security rules.

- Protection: By filtering traffic, firewalls can block unauthorized access and prevent malicious data from entering the network. This helps to mitigate threats such as hacking attempts, malware infections, and data breaches.

2. Intrusion Detection and Prevention Systems (IDPS)

- Function: IDPS monitor network traffic for suspicious activities and known threats. They can alert administrators or take action to block potential threats.

- Protection: These systems help in early detection of attacks, allowing for quick response to security incidents. They can identify patterns indicative of attacks, such as denial-of-service (DoS) attempts or unauthorized access.

3. Encryption

- Function: Encryption transforms data into a secure format that can only be read by someone with the appropriate decryption key.

- Protection: By encrypting sensitive data, organizations can protect it from eavesdropping and interception during transmission. This is crucial for safeguarding personal information, financial transactions, and confidential communications.

4. Access Control

- Function: Access control mechanisms determine who can access specific resources within the network.

- Protection: Implementing strong access controls ensures that only authorized users can access sensitive information and systems. This reduces the risk of insider threats and unauthorized access, which can lead to data breaches.

5. Regular Software Updates and Patch Management

- Function: Keeping software and systems updated ensures that known vulnerabilities are patched.

- Protection: Regular updates minimize the risk of exploitation from outdated software. Cyber attackers often target known vulnerabilities, and timely patching can thwart these attempts.

6. Network Segmentation

- Function: Network segmentation involves dividing a network into smaller, isolated segments.

- Protection: By segmenting the network, organizations can contain potential breaches, limiting an attacker’s ability to move laterally within the network. This also helps in applying tailored security policies to different segments.

7. Security Awareness Training

- Function: Training employees on security best practices and awareness of potential threats.

- Protection: Educated users are less likely to fall victim to phishing attacks or social engineering tactics. Promoting a culture of security awareness helps strengthen the overall security posture of the organization.

8. Backup and Recovery Solutions

- Function: Regularly backing up data ensures that critical information can be restored in case of data loss events, such as ransomware attacks or hardware failures.

- Protection: Effective backup solutions provide a safety net, allowing organizations to recover quickly and minimize downtime in the event of a security incident.