NATIONAL INSTITUTE OF BUSINESS MANAGEMENT

School of Computing

BSc (Hons) Ethical Hacking and Network Security

Higher National Diploma in Network Engineering (HNDNE)

Batch – HNDNE24.1F

Network Security - Coursework Part-2

Lecturer: Mr. Indunil Daluwatte

Prepared by,

COHNDNE241-047 G W J K Bhashana

COHNDNE241F-043 K A D Harshamal

COHNDNE241F-046 B Gajaana

COHNDNE241F-022 D T P Ladduwahetti

COHNDNE241F-003 B T N Perera

Modern Network Security Threats

1a. Discuss Three Common Types of Malware

1. Virus

A virus is a type of malicious code that latches onto clean files and proliferates to other files upon execution. Most of the time, it requires user action to spread, such as opening an infected email attachment or running a compromised application. Viruses can:

- Corrupt or delete files.
- Slow down system performance.
- Change the configurations to disrupt system functionalities.

Example: The Melissa virus spread by attachment in an email message containing a Word document. If opened, the virus replicated by sending itself to the first 50 entries in address books of the victim.

2. Worm

Worms are self-contained worm programs, generatively replicating to spread across networks without requiring a host file. They take advantage of system vulnerabilities and are engineered to spread rapidly and without human intervention. Worms can:

- Cause network congestion.
- Consume excessive bandwidth.
- Open backdoors for additional malware.

Example: WannaCry ransomware leveraged worm-like behavior by exploiting a Windows vulnerability called EternalBlue, thereby infecting thousands of computers globally in a few hours.

3. Ransomware

Ransomware encrypts files on a victim's system and demands money, usually in cryptocurrency, in exchange for the decryption key. It targets individuals and organizations, with great operational disruptions caused by it. The most common delivery method for ransomware is via phishing emails or vulnerabilities in software.

Example: The Locky Ransomware campaign, in particular, started encrypting patient's data and demanding payments to regain access, targeting healthcare organizations.

.

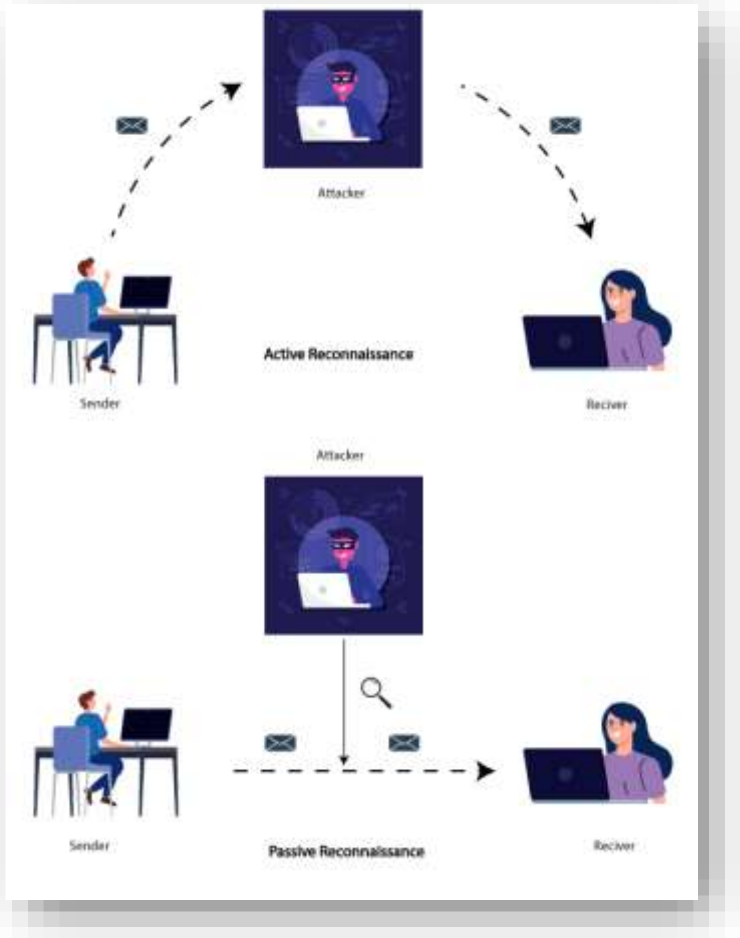
Comparison Table:

Malware Type	**Dependency on Host**	**Propagation Method**	**Primary Impact**
Virus	Needs a host file	User interaction	Corrupts files and disrupts systems
Worm	Standalone	Exploits vulnerabilities	Network congestion and potential backdoors
Ransomware	Standalone	Phishing or exploits	Encrypts files, demands ransom

1b. Reconnaissance Attack

Reconnaissance attacks involve gathering intelligence about a network to identify vulnerabilities for future exploitation. Attackers may use tools such as ping sweeps, port scanners, and protocol analyzers.

Figure Description:



Types of Reconnaissance Attacks

Passive Reconnaissance

- Passive reconnaissance refers to the attacker gathering information without directly interacting with the target.
    - Example: monitoring public websites, social media, DNS records, or WHOIS data.
    - Objective: To gather openly available information like IP addresses, Email Ids, employee names, or infrastructure details.

Active Reconnaissance

- Active reconnaissance involves the adversary interacting with the targeted network or systems to gain specific information.
    - Examples: port scanning, system pinging, or service probing.

- Tools Used: Nmap, Nessus, Wireshark.
- Goal: Recognize available ports, running services, software versions, or possible vulnerabilities.

1c. Penetration Testing Tools

Types of Tools:

1. **Network Scanners (e.g., Nmap):**

   Network scanners are important in mapping network architecture and identifying potential vulnerabilities. A typical example of a network scanner, the Network Mapper or Nmap, is able to:

   - Detect active devices on the network.
   - Identify active ports and the services running over them.
   - Perform OS fingerprinting to detect the OS of the connected devices.
   - Review firewall rules and configurations.

   Why It Matters: In identifying opened ports and their respective running services, administrators are able to identify misconfigured services and those not necessary, adding to the attack surface. For example, attackers might use an opened port for an unused service.

2. **Vulnerability Scanners (e.g., Nessus):**

   Vulnerability Scanners, like Nessus, perform deep scans on networked systems to show known weaknesses. They do the following:

   - Identify obsolete versions of software and uninstalled patches.
   - Identify weak configuration-both in terms of wrong permissions and services exposed unnecessarily.
   - Identify vulnerabilities that are commonly associated with SQL injection, cross-site scripting, and buffer overflow.

   Why It Matters: This completes the vulnerability reporting in Nessus so that the network administrator can prioritize patching proactively.

3. **Exploitation Tools (e.g., Metasploit):**

   Metasploit is one of the most powerful tools for validating vulnerabilities by attempting to exploit them. It can:

   - Simulate actual attacks to test the security defenses.
   - Verify identified vulnerabilities (via tools such as Nessus) can be successfully exploited.
   - Assess the impacts of successful exploitation: unauthorized access, privilege escalation, and other.

     Why It Matters: Metasploit applies to any organization's understanding of the real-world effects of vulnerabilities. Testing exploits in a controlled fashion builds effective countermeasures that allow them to fend off an in-the-wild attack.

4. **Password Cracking Tools (John the Ripper):**

   Password cracking utilities like John the Ripper check the strength of user credentials. They are capable of:

   - Engage in dictionary attacks, brute-force attacks, and hybrid techniques.
   - Identify weak passwords, such as common or reused ones.
   - Identify where password policies need to be improved (e.g., length, complexity).

   Why It's Important: Inadequate password security represents a serious vulnerability for any would-be attackers. John the Ripper allows system administrators to improve password protocols by identifying and replacing weak passwords.

5. **Web Application Testing Tools (for example, Burp Suite):**

   A great utility for web application security testing, including features such as:

   - Discover vulnerabilities: SQL injection, XSS, and authentication bypass vulnerabilities.
   - Perform automated and manual testing of HTTP requests and responses.
   - Analyze session tokens, cookies, and user input validation.

   Why It Matters: Since many businesses depend on web-based applications, their security becomes a very important issue for the protection of data leakage and unauthorized access.

Scenario: Using Penetration Testing Tools to Improve Network Security

To illustrate how these disparate tools come together to secure a network, the following is a case study:

Network Scanning with Nmap:

Perform an initial scan of the network to identify active hosts and open ports.

- Example: Using nmap -sV 192.168.1.0/24 to find all active devices, services running on open ports, and their versions.

outcome: Several devices are found, including a web server listening on port 80, a file server listening on port 21 (FTP), and a workstation that has an open SSH port (22).

Vulnerability Assessment Using Nessus:

Develop and implement Nessus to scan the identified systems for possible vulnerabilities.

- Nessus reports that the web server is running an outdated version of Apache, which has a known vulnerability (CVE).

outcome: The old Apache server was found to be a high-risk vulnerability that requires immediate action.

Exploitation Testing with Metasploit:

Use Metasploit in a controlled testing environment to validate the vulnerability of Apache.

- Running the Metasploit `exploit/unix/http/apache_mod_cgi_bash_env_exec` module, in order to exploit the web server.

Outcome: Successful exploitation shows how an attacker can get remote access to the server, and this definitely emphasizes the urgency of patching the vulnerability.

Password Strength Assessment with John the Ripper:

Run John the Ripper against the system hashes to crack weak user passwords. It could break quite a lot of them passwords like password123 and admin, weak passwords that people use very commonly.

Outcome: Analysis has identified weak passwords; hence, strong recommendations are made to enforce a stronger password policy, such as a minimum 12-character password with a mix of uppercase, lowercase, numbers, and symbols.

Web Application Testing with Burp Suite:

Test the organization's internal web applications for vulnerabilities.

- Example: Burp Suite flags issues like input fields vulnerable to XSS and improper session handling.

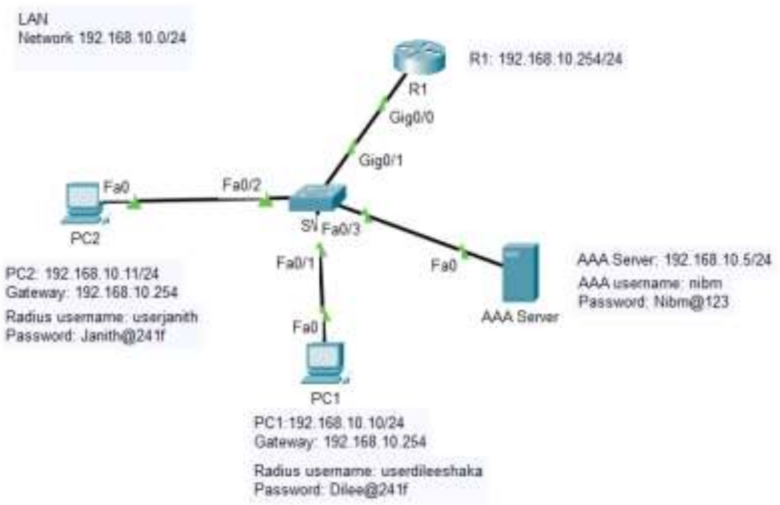
Outcome: Identify and address vulnerabilities through input validation, proper session management, and securing user authentication mechanisms.

AAA Framework

2a. Necessity of AAA

Authentication, Authorization, and Accounting (AAA) ensure secure access to network resources and maintain accountability.

Explanation of the Figure



Authentication Phase:

- It initiates the connection by providing credentials through the host, including a username and password.
- The RADIUS client (router/switch) forwards an Access-Request to the RADIUS server.
- The RADIUS server authenticates the credentials provided and responds with an Access-Accept message.

Authorization Stage:

- The RADIUS server can return rights after successful authentication based on the policy implemented.
- Permissions will define what resources on a network the host can access.

Accounting stage:

- Once access is granted, the RADIUS client sends an Accounting-Request-start message for logging purposes for the session details.

- The host utilizes resources, concurrently documenting usage information such as session length and bandwidth consumption.
- An Accounting Request stop message is sent when the session is over; the server responds with an acknowledge.

Justification of AAA in the Network

AAA implementation is quite indispensable concerning network security, as it**:**

- ❖ **Centralizes authentication**: For instance, a RADIUS server provides a single location to manage user credentials that minimizes administrator complexity.
- ❖ **Improves access control**: Only authenticated users can access the network, preventing unauthorized devices from connecting.
- ❖ **Monitors and Records Utilization**: Accounting procedure logs events generated by users, providing detailed session data for auditing and troubleshooting purposes. Scales Well for Larger Networks: As such, AAA shows effective scaling, thus becoming very suitable for multi-site networks like the London and Coventry offices.

2b. Authentication Methods

1. **Local Authentication**

   Local authentication is an authentication process in which a network device, such as a router, switch, or server, authenticates users' credentials locally without dependence on an external server; the usernames and passwords are stored locally in the configuration of the device.

   Mechanism of Operation:

   - A user trying to log in submits a username and password.
   - The device checks the credentials against its local database.
   - If the credentials match, access is granted; otherwise, access is denied.

   Advantages:

   - Easy to set up and deploy, at least in small networks.
   - Does not rely on external servers, so it still works if the network connection is down.

   Disadvantage:

   - Not scalable: Credentials management on multiple devices becomes cumbersome in large networks.
   - Absence of centralization: The lack of centralized oversight contributes to inefficiencies in user management. Limited security features: Inadequate logging, accounting, or the setting of advanced authorization policies.

2. Authentication by Server (RADIUS)

RADIUS (Remote Authentication Dial-In User Service) is a server based authentication protocol commonly used for centralized network access control. It operates over UDP and combines authentication, authorization, and accounting (AAA).

Mechanism of Operation:

- The user initiates a connection and sends authentication credentials to a RADIUS client (router or switch).
- The RADIUS client sends the credentials to the RADIUS server for verification.
- The RADIUS server authenticates the credentials against its database.
- If successful, the server sends back an Access-Accept message, which provides access. Otherwise, it will send an Access-Reject.

Advantage:

- Centralized Authentication: The user's credentials and policies are stored in one place (RADIUS server).
- Scalability: Suitable for large networks with many devices and users.
- AAA Features: Provides accounting logs that track user activity, session duration, and data usage.
- Flexibility: Supports multiple authentication protocols, including PAP, CHAP, and EAP.

Disadvantage:

- Less granular authorization: RADIUS combines authentication and authorization, which can limit flexibility. Uses UDP: The connection is less reliable compared to protocols that use TCP (e.g., TACACS+).

3. TACACS+ Authentication

TACACS+ (Terminal Access Controller Access Control System Plus) is a proprietary AAA protocol from Cisco. It runs on top of TCP, so it's more reliable and secure than RADIUS. The TACACS+ separates authentication, authorization, and accounting, giving more control over user access.

Mechanism of Function:

- A user sends credentials to the network device.
- The device forwards the credentials to the TACACS+ server for verification.
- The server authenticates the credentials and checks user permissions (authorization) separately.

- TACACS+ also keeps detailed accounting records to make auditing processes easier.

Advantage:

- Granular Control: Authentication, authorization, and accounting are managed separately. This permits fine-grained control over user permissions.
- Improved Security: It uses TCP and provides reliable communication, with the encryption of the payload, not just the passwords.
- Centralized Management: Consolidates user administration across all network devices.
- Flexible Authorization: Allows administrators to set some policies defining what actions the specific user will execute while logging in.

Disadvantage:

- Complex Configuration: Setting up TACACS+ requires more effort and expertise compared to local authentication. Vendor Specific: Mostly Cisco standard, though widely supported in other systems.

Recommendation

TACACS+ is preferable to Local Authentication and RADIUS for several reasons in order to ensure that the authentication process is secure, scalable, and efficient:

- ❖ **Granular Control:** TACACS+ offers precise management of authentication, authorization, and accounting processes, rendering it appropriate for extensive and intricate network environments.
- ❖ **Security:** Unlike RADIUS, which encrypts only passwords, TACACS+ encrypts the whole communication payload for better protection from interception.
- ❖ **Reliability:** Reliability is ensured by using TCP, which provides reliable communication between network devices and the TACACS+ server.
- ❖ **Centralized Management:** TACACS+ allows administrators to manage user credentials and access policies from a centralized server, which improves both scalability and operational efficiency.

2c. Configuring Server-Based AAA with RADIUS.

Step 1: Understand the Components

- ▪ **AAA Server:** The RADIUS server, which handles authentication requests, manages permissions, and logs access/accounting information.
- ▪ **AAA Clients:** Routers, switches, or firewalls that request user authentication and authorization from the RADIUS server are collectively called as **network access devices (NADs)**.

- **User Database:** A central repository, usually stored in the RADIUS server or connected to an external source such as LDAP or Active Directory, that contains user credentials and their associated roles.

Step 2: Prepare the RADIUS Server

1. Install RADIUS Server Software

Use software like:

- FreeRADIUS: open-source RADIUS implementation.
- Microsoft NPS (Network Policy Server): Windows based RADIUS solution.
- Cisco ISE (Identity Services Engine): Advanced RADIUS and access control.

2. Establish User and Group Configurations

- Integrate user accounts and assign roles to the RADIUS server.
  - Example (FreeRADIUS):
    - `user1 Cleartext-Password := "password123"`

3. Clarify Policies

- Establish authentication mechanisms such as passwords and certificates.
- Assign roles or permissions based on group membership.

4. Allow RADIUS Communication Ports End

- Ensure that UDP ports 1812 (authentication) and 1813 (accounting) are open between AAA clients and the RADIUS server.

Step 3: Enable AAA on the Network Device

Enable AAA features on devices like Cisco routers, switches, or firewalls.

1. Enable AAA Globally

```
aaa new-model
```

2. Define the RADIUS Server

- Specify the RADIUS server IP address and shared secret.

```
radius server RADIUS-SERVER
address ipv4 <RADIUS_IP>
key <SHARED_SECRET>
```

3. Configure Authentication

- Define a method list for login authentication:
    - First, try RADIUS; fall back to the local database if RADIUS is unavailable.

```
aaa authentication login default group radius local
```

4. Configure Authorization (Optional)

- Control user access to specific CLI commands or device resources:

```
aaa authorization exec default group radius local
```

5. Configure Accounting (Optional)

- Enable logging of user activities for auditing purposes:

```
aaa accounting exec default start-stop group radius
```

6. Apply AAA to Device Access

- Apply the defined authentication method to console or VTY lines:

```
line vty 0 15
login authentication default
```

Step 4: Test and Validate the Configuration

1. User Authentication Testing

- Perform a login attempt using the created user account to validate whether the networking device can talk to the RADIUS server.

2. Logs Verification

- Check the RADIUS server logs for authentication-requests and responses.
- Perform the debugging commands for Cisco devices:

```
debug aaa authentication
Debug radius
```

Step 5: Enhance Security

1. Leverage secure shared secrets.

- Ensure that the shared secret between the RADIUS server and AAA client is complex and secure.

2. Secure communication

- IPsec, DTLS, or SSH could be used to secure device-to-device communication.

3. RBAC: Role-Based Access Control

- Establish roles of access by detecting responsibilities and reduce the risk of unauthorized access.

Step 6: Troubleshoot Configuration

Prevalent Challenges and Solutions

- Authentication Failure Verify username/password within the RADIUS database. Also, check that the shared secret at both ends is similar.
- RADIUS Server Not Responding: Network connections should be checked, besides opening UDP ports 1812/1813.
- Misconfigured Policy: The review and correction of mismatched policies for user roles or groups.

Firewalls

3a. Benefits and Limitations of Firewalls

Benefits:

1. Protects against unauthorized access by filtering traffic.
2. Monitors and controls incoming/outgoing data flows.
3. Shields internal networks from external threats such as DDoS attacks.

Limitations:

1. Cannot mitigate insider threats or social engineering attacks.
2. Limited effectiveness against encrypted traffic without additional tools.
3. Requires regular updates and expert management to stay effective.

3b. Types of Firewalls

Firewall Type	**Features**	**Use Case**
Packet Filtering	Filters based on IP, port, and protocol.	Basic network protection.
Stateful Inspection	Tracks session states for dynamic filtering.	Medium sized networks with dynamic traffic.
Application Layer	Examines application specific data.	Enterprises needing granular traffic control.
NextGeneration (NGFW)	Integrates advanced features like IDS/IPS.	High security environments with evolving threats.

3c. Importance of Zone-Based Policy Firewalls

Importance of Zone-Based Policy Firewalls.

The Zone-Based Policy Firewall is the new generation of firewalls that segment different parts of network traffic into distinct zones and apply policy controls to manage the flow between the different zones. This becomes quite important as it can supply consistency, logic, and scalability in approaches to network security.

Granular Control: It enables administrators to define precise policies regarding the flow of traffic across zones using ZBPF.

- Example: This would yield zones like "Internal," "DMZ" (demilitarized zone), and "Untrusted" (Internet). Only "Internal" to "DMZ" traffic is allowed to pass for specific services like HTTP and DNS, while all traffic from "Untrusted" to "Internal" is denied.

Segmentation-Based Security: Isolation of different segments prevents lateral movements if an attack of any sort occurs.

- Scenario: if malware breaks into the "Guest Wi-Fi" zone, policies will prevent it from reaching the "Internal" zone where sensitive corporate data is.

Policy-Based Flexibility: There is ease in the definition, administration, and auditing of policies in ZBPFs because policies are attributed to logical zones rather than specific interfaces.

- Scenario: An e-commerce company might create one zone for Web Servers, another for Payment Processing, and another for User Data. Policies may confine communications by the payment processing zone to only communicate with authenticated systems.

Prevention against unauthorized access: Traffic between zones is explicitly allowed or denied based on policies. This zero-trust model enhances security. Within an industrial enterprise, "Industrial Control System" space is to be treated as restricted, granting access only with approved maintenance devices to decrease the risk of possible sabotage.

Scalability and Automation: If a zone has increasing devices or networks, there is no need to alter a single firewall rule since policies applied on the zone are applied automatically.

- Scenario: A logistics company expands its warehouse management system. By placing the new devices in the existing "Warehouse" zone, they will inherit all pre-defined security policies. Visibility and Logging: ZBPFs allow better logging and monitoring for traffic across zones, making it easier for administrators to identify abnormal activities. Example: Anomalous traffic sourced from the "Internal" zone and destined for the "Untrusted" zone can trigger an alert for investigation.

Conclusion

- The network design for the head offices in London and Coventry was well designed and implemented using the Cisco Packet Tracer tool. The design focused on building robust connectivity with high levels of security and functionality across the different departments. For network integrity, different security measures such as device hardening, VLAN setup, and mitigation techniques against ARP spoofing, VLAN hopping, and DHCP spoofing were implemented.

Future Recommendations

1. Enhanced Monitoring and Maintenance:

- Network Monitoring: Implement a network monitoring solution to provide real-time performance monitoring and anomaly detection, such as SolarWinds or PRTG.
- Schedule periodic penetration tests to identify and patch the vulnerabilities.

2. Adoption of Advanced Security Measures:

- Implement next-generation firewalls that have much better visibility into traffic with modern threat protection.
- Employ endpoint security for devices that connect to a network.

3. Scalability and Improvements:

- Design a scalable network that allows the addition of devices, users, and offices in the near future.
- Increase internal network connectivity to higher bandwidths to support organizational needs when they exceed the current capacity of 25 Mbps.

4. Employee Training and Awareness:

- Provide regular training to employees on cybersecurity to reduce risks such as phishing and social engineering.

5. Automation and AI Integration:

Identify how AI-powered threat detection and response are being automated using such tools. Automate backup and update of configurations to ensure network resilience and reduce networking downtime. Systematic Analysis of Security Protocols: Perform annual reviews of security procedures to update for newly identified risks and compliance requirements.

****