Case 3

Cyber Security Assessment
Group 10

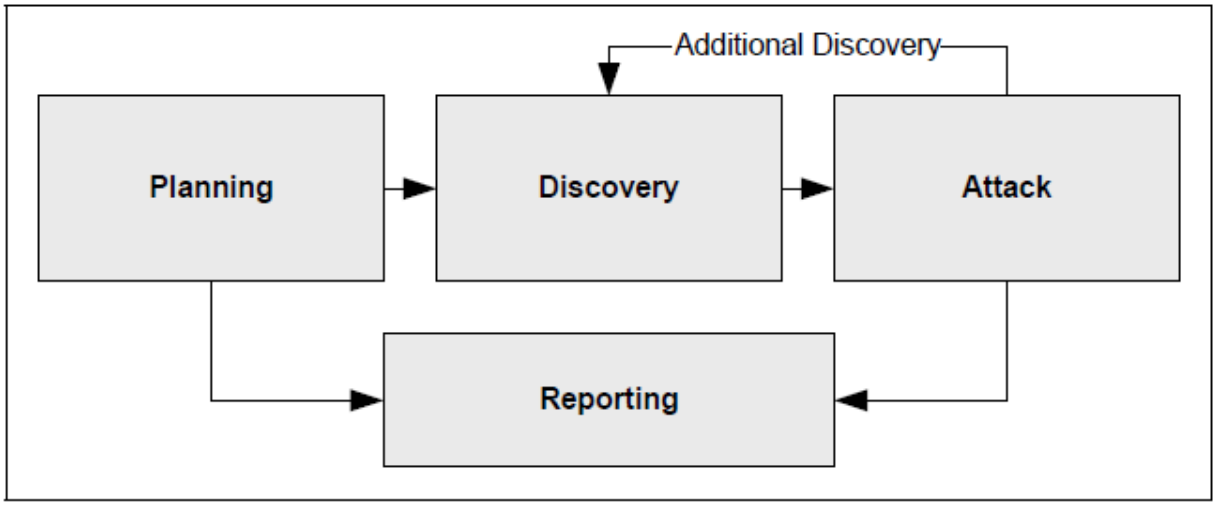
Participants

Athanasios Ntales (atnt3398)
Bilal Riaz (biri9477)
Chanchala Fernando (chfe1432)
Emad Abdulsamad (emab9908)
Lekhaz Adapa (lead3201)
Muhammad Usama Younas (muus4313)

In the previous case Radio Sweden assigned us to check the implementation of their network and system and identify all the existing threats. In the light of the previous case result Radio Sweden assigned us to check the possibility of defined threats and perform penetration testing on the network and different systems to evaluate the security protection level and set the required metrics and controls.

Penetration Testing:

Penetration testing is a reliable method of detecting vulnerabilities in systems and networks by scanning systems and networks for existing vulnerabilities and trying to exploit them to achieve goals of different attacks, gain access, or deny access to services (DoS). Penetration testing is performed through four phases: planning, discovery, attack, and reporting.



In this situation, the following procedures could be taken to run a penetration test against Radio Sweden's infrastructure:

1. **Planning:** The first phase would be to identify the scope of the penetration test, including the systems and network to be tested, source of possible attack, and the objectives of this penetration testing. Working closely with Radio Sweden's CTO ,Chief technology officer to identify critical assets that need testing and protection. The CTO could provide required information that helps to aid in the planning process.

2. **Discovery:** The second phase would be to discover the networks zones and topologies, existing systems and services in all zones, and scan for existing vulnerabilities in networks and systems. The discovery phase is performed through two stages.
   i) Intelligence gathering and scanning: In this stage we will apply network and port scanning to define the network topology and open ports in different systems. This might be accomplished with technologies such as Nmap, Shodan, and Google Dorking..

ii)Vulnerability Analysis: The identified systems and networks's open port will be subjected to vulnerability scans to identify existing vulnerabilities. Beside discovered vulnerabilities, vulnerabilities databases such as CVE details will be checked for none-discovered vulnerabilities. This would entail employing tools like Nessus, OpenVAS, or Qualys.

3. **Attack:** Once vulnerabilities have been identified, the next phase is to exploit them to obtain access to the target systems and networks, or escalate privileges. This may entail the use of tools such as Metasploit to custom-built exploits. In the attack phase different types of attack are performed, social engineering, denial of service, access control flaws, and escalate privileges. These attacks can be performed using attacking tools such as metasploit.The goal would be to get access to sensitive data or systems within the infrastructure of Radio Sweden.

4. **Reporting:** Following the completion of the penetration test, a report summarizing the results and recommendations for remediation should be delivered to Radio Sweden's CTO. The information should include a list of detected vulnerabilities, successful attacks, their severity, and mitigation recommendations.

Security Controls and Metrics:

Based on the potential vulnerabilities discovered during the penetration testing, Radio Sweden's cyber security posture could be improved by implementing the following security measures and metrics:

1. **Employee Training:** All employees should be trained on Cybersecurity best practices such as password management, phishing awareness, and reporting suspicious behavior regularly. This control's metrics could include the number of employees trained, the frequency with which they are trained, and the percentage of employees who report suspicious conduct.
2. **Firewall Configuration:** The firewall should be set up to restrict incoming and outgoing traffic to only the required ports and protocols. The number of firewall rules in place, the number of refused connections, and the proportion of blocked traffic could all be metrics for this control.
3. **Anti-Malware Software:** Anti-malware software should be installed and updated on all endpoints. The number of malware infections discovered, the frequency of updates, and the proportion of endpoints with up-to-date software could all be metrics for this control.
4. **Access Control:** Access to all systems and apps containing sensitive data should require multi-factor authentication. Metrics for this control could include the number of multi-factor authentication-enabled systems and apps, the percentage of successful multi-factor authentication logins, and the proportion of users that have activated multi-factor authentication.

5. **Monitoring and Auditing:** the monitoring and auditing system should be checked for logs and events related to our penetration testing and be improved to monitor and detect all discovered vulnerabilities in the network and system infrastructure.

6. **Backup and Disaster Recovery:** Backups of vital data should be taken regularly and securely kept off-site. In the case of a cyber attack, a disaster recovery strategy should also be in place to preserve business continuity. Metrics for this control could include backup frequency, time to recover from a disaster, and the proportion of essential data recovered successfully.
7. **Update and Patch:** All discovered vulnerabilities should be patched and all systems should be kept up to date to protect the system against any new attack vector.