VAPT Task 3

Theoretical Knowledge

1. Advanced Vulnerability Exploitation

A multi-stage attack in cybersecurity is a complex, multi-step intrusion designed to evade detection by breaking down a malicious operation into sequential phases, where each stage builds on the last to achieve the attacker's goal, like stealing data or deploying ransomware, often starting with a seemingly harmless action (like clicking a link) to gain initial access and then downloading more sophisticated tools or spreading laterally. These attacks are hard to spot because individual steps look benign, making it difficult for security systems to connect the dots and identify the full attack chain. In these kinds of hacks, the attackers don’t go after their victims’ networks directly. Instead, they penetrate the system of a third-party supplier with access to their targets’ network assets.

Solar Winds Cyber Attack

The SolarWinds assault was a typical supply chain attack. Many of SolarWinds’ customers use a system called Orion, which is a performance monitoring solution that tracks the status of SolarWinds' Orion customers. It has privileged access to gather performance data and other information from logs generated by customer IT assets. This made SolarWinds an ideal target for hackers who successfully gained access to several thousand companies' networks.

The SolarWinds cyber attack timeline stretched out over six months, during which time the hackers patiently and systematically executed their hack. Here are the most critical milestones in the attack:

- In September 2019, hackers were able to access the SolarWinds network.
- They started testing their code injection in Orion in October 2019.
- About four months later, they injected malicious code called Sunburst into Orion.
- On March 26, 2020, SolarWinds began distributing Orion updates that contained the hackers’ malicious code.

The malware spread as thousands of SolarWinds customers installed the malicious code in the hacked update. Once on a victim’s system, the malware gave hackers access to customer IT systems. At this point, the attackers could install more malware, which enabled them to spy on additional organizations.

2. Web Application Penetration Testing

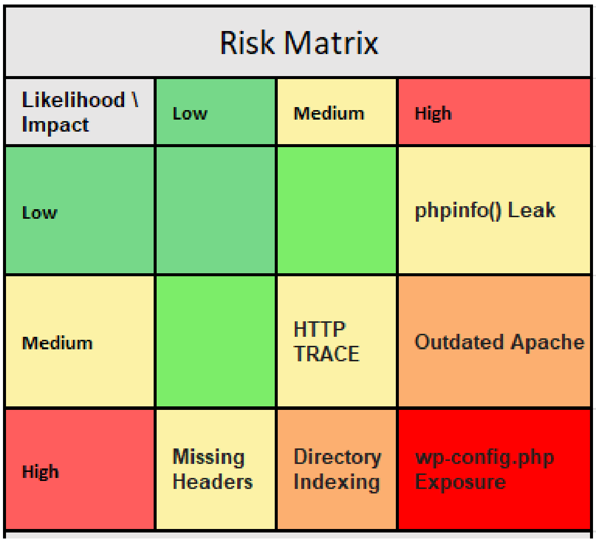
Burp Suite

Burp Suite is a web application security testing platform. It provides manual and automated tools to help cybersecurity professionals and developers identify vulnerabilities in web applications. Developed by PortSwigger, Burp Suite integrates into the testing process, offering a suite of modular tools for tasks such as scanning, crawling, and analysis. This platform is useful for both manual and automated testing, offering flexibility and integration capabilities. It supports numerous extensions, which allow users to tailor the suite to meet project needs. Security testers often rely on Burp Suite for its proxy features that enable the intercepting, inspecting, and altering of web traffic. The ease of use and step-by-step guidance also make it suitable for beginners.

Figure 1:Burp Suite

3. Reporting and Stakeholder Communication

A **Risk Rating** is a classification (like Low, Medium, High) that assesses an event's potential harm by combining its Likelihood (how often it might happen) and Severity (how bad it would be if it did), often by multiplying these two factors to prioritize risks for mitigation, helping organizations focus resources on the most significant threats.



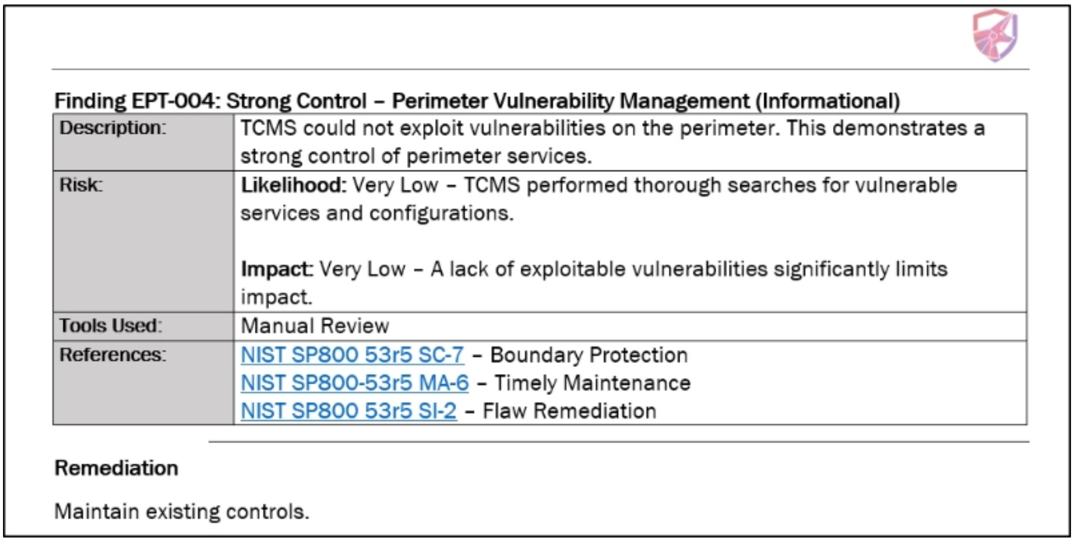
Risk Matrix

Likelihood \ Impact	Low	Medium	High
Low			phpinfo() Leak
Medium		HTTP TRACE	Outdated Apache
High	Missing Headers	Directory Indexing	wp-config.php Exposure

Figure 2:Sample Risk Matrix

Report creation tools

- **Dradis**: Popular open-source framework for collaboration and reporting
- **Serpico**: Simple and effective open-source report generation tool by Verizon
- **Ghostwriter**: Robust platform designed specifically for pentest operations and report writing
- **DefectDojo****: Open-source vulnerability management tool that correlates and de-duplicates findings
- **Plextrac** & **Faraday****: Commercial platforms with advanced features for managing the entire pentesting lifecycle



Finding EPT-004: Strong Control – Perimeter Vulnerability Management (Informational)

Description:	TCMS could not exploit vulnerabilities on the perimeter. This demonstrates a strong control of perimeter services.
Risk:	**Likelihood:** Very Low – TCMS performed thorough searches for vulnerable services and configurations. **Impact:** Very Low – A lack of exploitable vulnerabilities significantly limits impact.
Tools Used:	Manual Review
References:	NIST SP800 53r5 SC-7 – Boundary Protection NIST SP800-53r5 MA-6 – Timely Maintenance NIST SP800 53r5 SI-2 – Flaw Remediation

Remediation

Maintain existing controls.

Figure 3:Sample Pentest Report

References

[1] https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack
[2] https://cybersierra.co/blog/vapt-reports-samples-examples-templates/
[3] www.google.com