Group SP24IA08

fpt university – captsone project

**DoS/DDoS Pentest Report {init\_address}**

{init\_scannedDate} – {init\_scannedTime}

Table of

Contents

[1 Penetration Testing Scope Statement 2](#_Toc164638181)

* [Risk Classifications 2](#_Toc164638182)
* [Exploitation Likelihood Classifications 2](#_Toc164638183)
* [Business Impact Classifications 3](#_Toc164638184)
* [Remediation Difficulty Classifications 3](#_Toc164638185)

[2 Report Summaries 4](#_Toc164638186)

* [Reconnaissance summary 4](#_Toc164638187)
* [DoS and DDoS Pentest summary 4](#_Toc164638188)

[3 Recommendation 6](#_Toc164638189)

[4 Reconnaissance Activities 7](#_Toc164638190)

[5 Exploitation Activities 7](#_Toc164638190)

[5.1 DoS Pentest Activities 7](#_Toc164638191)

[5.2 DDoS Pentest Activities 7](#_Toc164638194)

# Penetration Testing Scope Statement

## Risk Classifications

|  |  |  |
| --- | --- | --- |
| **Level** | **Score** | **Description** |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classifications

|  |  |
| --- | --- |
| **Likelihood** | **Description** |
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

## Business Impact Classifications

|  |  |
| --- | --- |
| **Impact** | **Description** |
| **Major** | Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage. |
| **Moderate** | Successful exploitation may cause significant disruptions to non-critical business functions. |
| **Minor** | Successful exploitation may affect few users, without causing much disruption to routine business functions. |

## Remediation Difficulty Classifications

|  |  |
| --- | --- |
| **Difficulty** | **Description** |
| **Hard** | Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions. |
| **Moderate** | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| **Easy** | Remediation can be accomplished in a short amount of time, with little difficulty. |

# Report Summary

This section contains quick performed summary on {init\_address}

## Reconnaissance Summary

Scanned Date: **{init\_scannedDate}**

Scanned Time: **{init\_scannedTime}**

Number or port open: **{sum\_recon\_portCount}** ports / 1000 common ports

Found Potential Vulnerability: **{sum\_recon\_cveCount}** CVEs

## Exploitation Summary

### Total attacks:

* Total DoS & DDoS: 32 attacks
* Attacked:
  + Layer 3- Network Layer: **1 attack**
  + Layer 4 – Transport Layer: **5 attacks**
  + Layer 7 – Application Layer**: 10 attacks**

# Recommendation

1. TCP Reset flood:

* Enable SYN cookies on the server to mitigate SYN flood attacks
* Implement rate limiting for TCP connections
* Use a load balancer or reverse proxy to distribute traffic across multiple servers
* Upgrade network infrastructure to handle higher bandwidth and connection rates

1. TCP: SYN FIN Flood:

* Configure firewall rules to block SYN-FIN packets
* Implement TCP stack hardening techniques on the server
* Use a DDoS mitigation service or appliance to filter malicious traffic

1. TCP: PUSH ACK Flood:

* Configure firewall rules to block PUSH-ACK packets
* Implement rate limiting for TCP connections
* Use a DDoS mitigation service or appliance to filter malicious traffic

1. TCP: FIN flood:

* Configure firewall rules to block FIN packets without an established connection
* Implement TCP stack hardening techniques on the server
* Use a DDoS mitigation service or appliance to filter malicious traffic

1. UDP Flood:

* Implement rate limiting for UDP traffic
* Use a DDoS mitigation service or appliance to filter malicious traffic
* Upgrade network infrastructure to handle higher bandwidth and packet rates

# Reconnaissance Pentest Activities

* **Scanner:** nmap
* **Scanned time:** {recon\_scannedTime}

Each port Information:

{#reconPorts}

|  |  |  |
| --- | --- | --- |
| Port | {reconPort\_number} | |
| Service | Name | {reconPort\_service\_name} |
| Product | {reconPort\_service\_product} |
| Version | {reconPort\_service\_version} |

{/reconPorts}

# 5. Exploitation Activities

### 5.1 DoS Pentest Activities

{#dos}

#### {attack\_layer}:

{#attack\_type}

##### {attack\_mainType} Attacks:

{#attack\_details}

|  |  |  |
| --- | --- | --- |
| Types of attack | | {attackType} |
| Used service | | {toolName} |
| Status | | {isSuccess} |
| Describe | Average Ping | {attack\_avg} ms |
| Max Ping | {attack\_max} ms |
| Packet Loss Percentage | {attack\_packetLoss} % |

{/attack\_details}

{/attack\_type}

{/dos}

### 5.1 DDoS Pentest Activities

{#ddos}

#### {attack\_layer}:

{#attack\_type}

##### {attack\_mainType} Attacks:

{#attack\_details}

|  |  |  |
| --- | --- | --- |
| Types of attack | | {attackType} |
| Used service | | {toolName} |
| Status | | {isSuccess} |
| Describe | Average Ping | {attack\_avg} ms |
| Max Ping | {attack\_max} ms |
| Packet Loss Percentage | {attack\_packetLoss} % |

{/attack\_details}

{/attack\_type}

{/ddos}