Group IA08 – Spring 2024

fpt university – captsone project

DoS/DDoS Pentest Report {init\_address}

{init\_scannedDate} – {init\_scannedTime}

Table of Contents

[1 Penetration Testing Scope Statement 2](#_heading=h.gjdgxs)

[∙ Risk Classifications 2](#_heading=h.30j0zll)

[∙ Exploitation Likelihood Classifications 2](#_heading=h.1fob9te)

[∙ Business Impact Classifications 2](#_heading=h.3znysh7)

[∙ Remediation Difficulty Classifications 2](#_heading=h.2et92p0)

[2 Report Summary 2](#_heading=h.tyjcwt)

[Reconnaissance 2](#_heading=h.3dy6vkm)

[DoS and DDoS Pentest Summary 3](#_heading=h.1t3h5sf)

[3 Recommendation 3](#_heading=h.2s8eyo1)

[4 Reconnaissance Pentest Activities 3](#_heading=h.17dp8vu)

[5.1 DoS Pentest Activities 6](#_heading=h.3rdcrjn)

[Layer 3: 6](#_heading=h.26in1rg)

[Layer 4: 6](#_heading=h.lnxbz9)

[Layer 7: 7](#_heading=h.35nkun2)

[5.2 DDoS Pentest Activities 7](#_heading=h.1ksv4uv)

[Layer 3: 7](#_heading=h.44sinio)

[Layer 4: 7](#_heading=h.2jxsxqh)

[Layer 7: 8](#_heading=h.z337ya)

# 1 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. |

# 2 Report Summary

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

# Reconnaissance

Number or port open:

# DoS and DDoS Pentest Summary

|  |  |  |
| --- | --- | --- |
| Attack type | DoS | DDoS |
| Layer 3 | | |
| ICMP Flood | Affected | Affected |
| Layer 4 | | |
| TCP Reset Flood | Affected | Affected |
| TCP SYN FIN Flood | Affected | Unaffected |
| TCP PUSH ACK Flood | Affected | Unaffected |
| TCP FIN Flood | Affected | Affected |
| UDP Flood | Affected | Affected |
| Layer 7 | | |
|  |  |  |

# 3 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

# 4 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}

# 5.1 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}

# 5.2 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}