Group IA08 – Spring 2024

fpt university – captsone project

DoS/DDoS Pentest Report 192.168.133.130

2024-04-18 – 2:05:40 AM

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 192.168.133.130

# 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:** undefined

Each port Information:

|  |  |  |
| --- | --- | --- |
| Port | 21 | |
| Service | Name | ftp |
| Product | vsftpd |
| Version | 2.3.4 |

|  |  |  |
| --- | --- | --- |
| Port | 22 | |
| Service | Name | ssh |
| Product | OpenSSH |
| Version | 4.7p1 Debian 8ubuntu1 |

|  |  |  |
| --- | --- | --- |
| Port | 23 | |
| Service | Name | telnet |
| Product | Linux telnetd |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 25 | |
| Service | Name | smtp |
| Product | Postfix smtpd |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 53 | |
| Service | Name | domain |
| Product | ISC BIND |
| Version | 9.4.2 |

|  |  |  |
| --- | --- | --- |
| Port | 80 | |
| Service | Name | http |
| Product | Apache httpd |
| Version | 2.2.8 |

|  |  |  |
| --- | --- | --- |
| Port | 139 | |
| Service | Name | netbios-ssn |
| Product | Samba smbd |
| Version | 3.X - 4.X |

|  |  |  |
| --- | --- | --- |
| Port | 445 | |
| Service | Name | netbios-ssn |
| Product | Samba smbd |
| Version | 3.0.20-Debian |

|  |  |  |
| --- | --- | --- |
| Port | 512 | |
| Service | Name | exec |
| Product | netkit-rsh rexecd |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 513 | |
| Service | Name | login |
| Product | OpenBSD or Solaris rlogind |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 1099 | |
| Service | Name | java-rmi |
| Product | GNU Classpath grmiregistry |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 1524 | |
| Service | Name | bindshell |
| Product | Metasploitable root shell |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 3306 | |
| Service | Name | mysql |
| Product | MySQL |
| Version | 5.0.51a-3ubuntu5 |

|  |  |  |
| --- | --- | --- |
| Port | 5432 | |
| Service | Name | postgresql |
| Product | PostgreSQL DB |
| Version | 8.3.0 - 8.3.7 |

|  |  |  |
| --- | --- | --- |
| Port | 5900 | |
| Service | Name | vnc |
| Product | VNC |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 6667 | |
| Service | Name | irc |
| Product | UnrealIRCd |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 8009 | |
| Service | Name | ajp13 |
| Product | Apache Jserv |
| Version |  |

|  |  |  |
| --- | --- | --- |
| Port | 8180 | |
| Service | Name | http |
| Product | Apache Tomcat/Coyote JSP engine |
| Version | 1.1 |

# 5.1 DoS Pentest Activities

## Layer 3:

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | ICMP Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 2.335 ms |
| Max Ping | 7.267 ms |
| Packet Loss Percentage | 11.7647 % |

## Layer 4:

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP Reset Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 4.882 ms |
| Max Ping | 11.274 ms |
| Packet Loss Percentage | 35.2941 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP SYN FIN Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 4.765 ms |
| Max Ping | 12.655 ms |
| Packet Loss Percentage | 35.2941 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP PUSH ACK Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 3.523 ms |
| Max Ping | 11.098 ms |
| Packet Loss Percentage | 17.6471 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP FIN Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 4.713 ms |
| Max Ping | 16.012 ms |
| Packet Loss Percentage | 29.4118 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | UDP Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 2.94 ms |
| Max Ping | 16.299 ms |
| Packet Loss Percentage | 11.7647 % |

## Layer 7:

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | GET Flood |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.181 ms |
| Max Ping | 0.291 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | POST Flood |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.271 ms |
| Max Ping | 0.427 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | GET Method with more header |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.16 ms |
| Max Ping | 0.295 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | HEAD Flood |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.143 ms |
| Max Ping | 0.212 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Null UserAgent Flood |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.282 ms |
| Max Ping | 0.417 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Random Cookie Flood |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.208 ms |
| Max Ping | 0.322 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Slowloris |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.302 ms |
| Max Ping | 0.397 ms |
| Packet Loss Percentage | 0 % |

## Layer 7:

### Other Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Sends HTTP packets with high byte |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.114 ms |
| Max Ping | 0.12 ms |
| Packet Loss Percentage | 0 % |

### Other Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Reading data slowly |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.114 ms |
| Max Ping | 0.117 ms |
| Packet Loss Percentage | 0 % |

### Other Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Bypasses normal AntiDDoS |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.113 ms |
| Max Ping | 0.12 ms |
| Packet Loss Percentage | 0 % |

# 5.2 DDoS Pentest Activities

## Layer 3:

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | ICMP Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 4.711 ms |
| Max Ping | 14.864 ms |
| Packet Loss Percentage | 47.0588 % |

## Layer 4:

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP Reset Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 5.623 ms |
| Max Ping | 15.029 ms |
| Packet Loss Percentage | 52.9412 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP SYN FIN Flood |
| Used service | | HPing3 |
| Status | | Failure |
| Describe | Average Ping | 10.601 ms |
| Max Ping | 39.51 ms |
| Packet Loss Percentage | 5.88235 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP PUSH ACK Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 4.349 ms |
| Max Ping | 17.48 ms |
| Packet Loss Percentage | 11.7647 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | TCP FIN Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 1.017 ms |
| Max Ping | 2.746 ms |
| Packet Loss Percentage | 35.2941 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | UDP Flood |
| Used service | | HPing3 |
| Status | | Success |
| Describe | Average Ping | 49.666 ms |
| Max Ping | 630.723 ms |
| Packet Loss Percentage | 23.5294 % |

## Layer 7:

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | GET Flood |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.219 ms |
| Max Ping | 0.35 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | POST Flood |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.738 ms |
| Max Ping | 1.186 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | GET Method with more header |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 1.086 ms |
| Max Ping | 1.538 ms |
| Packet Loss Percentage | 0 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | HEAD Flood |
| Used service | | MHDDoS |
| Status | | Success |
| Describe | Average Ping | 0.268 ms |
| Max Ping | 0.479 ms |
| Packet Loss Percentage | 28.57142857142857 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Null UserAgent Flood |
| Used service | | MHDDoS |
| Status | | Success |
| Describe | Average Ping | 1.534 ms |
| Max Ping | 2.383 ms |
| Packet Loss Percentage | 28.57142857142857 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Random Cookie Flood |
| Used service | | MHDDoS |
| Status | | Success |
| Describe | Average Ping | 1.104 ms |
| Max Ping | 1.521 ms |
| Packet Loss Percentage | 25 % |

### Flood Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Slowloris |
| Used service | | MHDDoS |
| Status | | Success |
| Describe | Average Ping | 0.844 ms |
| Max Ping | 1.074 ms |
| Packet Loss Percentage | 25 % |

## Layer 7:

### Other Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Sends HTTP packets with high byte |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.23 ms |
| Max Ping | 0.331 ms |
| Packet Loss Percentage | 0 % |

### Other Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Reading data slowly |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.364 ms |
| Max Ping | 1.023 ms |
| Packet Loss Percentage | 0 % |

### Other Attacks:

|  |  |  |
| --- | --- | --- |
| Types of attack | | Bypasses normal AntiDDoS |
| Used service | | MHDDoS |
| Status | | Failure |
| Describe | Average Ping | 0.478 ms |
| Max Ping | 0.982 ms |
| Packet Loss Percentage | 0 % |