

RED TEAM DOS VULNERABILITY ASSESSMENT

Penetration Testing Report – May 2025

Rebecca Brown

**MediCare Health
Services**

Table of Contents

1: Executive Summary	3
2: Report Details and Team Information	4
2.1 Report Details	4
2.2 Team Members	4
2.3 Assessment Overview	4
3: Scope and Objectives	4
3.1 Assessment Scope	4
3.2 Test Objectives	4
3.3 Testing Limitations	5
4: Methodology	5
4.1 Testing Approach	5
4.2 Phase Breakdown	5
4.2.1 Reconnaissance Phase	5
4.2.2 Attack Planning Phase	5
4.2.3 Exploitation Phase	5
4.2.4 Analysis Phase	6
4.3 Tools and Techniques	6
5: Technical Findings	7
5.1 Network Discovery Results	7
5.2 Service Enumeration Results	7
5.3 Baseline Testing	8
6: Attack Execution and Results	10
6.1 Attack Methodology	10
6.2 Real-Time Monitoring	10
6.3 Attack Impact Results	11
6.4 Attack Effectiveness Analysis	13
7: Business Impact Assessment	15
7.1 Service Availability Impact	15
7.2 Healthcare-Specific Implications	15
7.3 Compliance and Regulatory Concerns	15
7.4 Financial Impact Assessment	16
8: Additional Security Observations	16
8.1 Secondary Vulnerabilities Identified	16

8.2 System Resilience Concerns	17
8.3 Risk Assessment Summary	17
9: Recommendations	18
9.1 Immediate Actions (Critical – Implement within 24-48 hours)	18
9.2 Short-term Improvements (1-4 weeks)	18
9.3 Long-term Improvements (1-6 months)	19
10: Conclusion	19
10.1 Assessment Summary.....	19
10.2 Key Findings	19
10.3 Overall Risk Assessment.....	19
10.4 Next Steps	19
APPENDICES.....	20
Appendix A: Technical Command Reference	20
Appendix B: Vulnerability Database References	20

1: Executive Summary

On 27th May, a Red Team DoS vulnerability assessment was carried out against MediCare Health Services' systems in order to evaluate its resilience against Denial-of-Service attacks. The assessment revealed critical security vulnerabilities that pose an immediate threat to patient care and business operations.

A simple 20-second SYN flood attack against the HTTP service resulted in complete system failure lasting over 30 minutes with no automatic recovery. This represents a critical 90:1 impact amplification ratio, where minimal attacker effort results in extensive disruption to operations. Reconnaissance also identified multiple critical vulnerabilities including backdoor access (CVE-2011-2523) and direct system compromise pathways.

In a healthcare environment, this vulnerability to DoS attacks would result in complete inaccessibility of patient portals, electronic medical records, and online appointment systems. The sustained outage poses direct patient safety risks and potential violations of privacy and healthcare regulations, including the Privacy Act 1988 and My Health Records Act 2012.

Immediate action within 24-48 hours is highly recommended to patch critical vulnerabilities and implement basic DoS protection. The overall security posture is assessed as **CRITICAL RISK**, requiring comprehensive remediation before the system can be considered safe for healthcare operations.

The demonstrated vulnerabilities present unacceptable risks for a healthcare organisation. Urgent implementation of security controls is essential to protect patient data and ensure service availability.

2: Report Details and Team Information

2.1 Report Details

Assessment Date	27 th May 2025
Report Date	1 st June 2025
Assessment Type	Red Team DoS/DDoS Vulnerability Assessment
Target Organisation	MediCare Health Services
Target System	Metasploitable 2 (Test Environment)

2.2 Team Members

Rebecca Brown – Penetration Tester and Security Analyst

2.3 Assessment Overview

This report documents the Red Team assessment component of a collaborative cybersecurity exercise targeting **MediCare Health Services**. The assessment focused specifically on evaluating system vulnerabilities to Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. This Red Team analysis will be integrated with Blue Team defensive responses and Purple Team strategic recommendations to provide a comprehensive security evaluation.

3: Scope and Objectives

3.1 Assessment Scope

- Target network segment: 192.168.50.0/24
- Primary target system: Metasploitable 2 at 192.168.50.20
- Services tested: HTTP service (port 80)
- Test environment: *Controlled virtual lab*
- Attack vector focus: DoS/DDoS attacks

3.2 Test Objectives

1. Evaluate system vulnerability to DoS/DDoS attacks
2. Assess impact on service availability
3. Document attack methodology and effectiveness
4. Measure recovery capabilities
5. Provide actionable recommendations for defensive measures and security improvements

3.3 Testing Limitations

- Test conducted in isolated lab environment
- Single target system assessment
- Limited to DoS attack vectors (scope constraint)
- No testing of other attack vectors (by design)

4: Methodology

4.1 Testing Approach

The vulnerability assessment followed a structured penetration testing methodology of four distinct phases to ensure thorough testing and comprehensive evaluation and documentation. The phases used were:

1. Reconnaissance
2. Attack planning
3. Exploitation
4. Analysis

4.2 Phase Breakdown

4.2.1 Reconnaissance Phase

This phase was focused on gathering information about the target environment in order to build a complete picture of the attack surface without alerting defensive systems. Activities included:

- **Network discovery** using *ping sweeps* to identify active hosts,
- Comprehensive **service enumeration** to catalogue running services and versions; and
- **Vulnerability identification** to assess potential attack vectors.

4.2.2 Attack Planning Phase

This phase involved preparing the attack system for successful execution of the chosen exploitation. This involved:

- **Baseline service testing** to establish normal behaviour of target services for comparison,
- **Monitoring setup** to prepare for real-time observation of the attack impact; and
- Selecting the **attack vector**.

4.2.3 Exploitation Phase

In this phase, the DoS attack on the target system was executed and its effects monitored and documented. This included:

- **DoS attack** execution,
- Real-time monitoring of the target system's behaviour; and
- Documenting the results of the attack

4.2.4 Analysis Phase

This phase focused on analysing the impact of the DoS attack against the vulnerable system. The analysis covered:

- Assessment of the direct impact of target system behaviour,
- Analysis of the business implications of a successful DoS attack based on the observed impact; and
- Evaluation of the recovery time for impacted systems

4.3 Tools and Techniques

VMWare	Virtual environment management
Kali Linux	Primary attack platform
Nmap	Network discovery and service enumeration
hping3	SYN flood attack execution
curl/ping/watch	Service monitoring and impact measurement

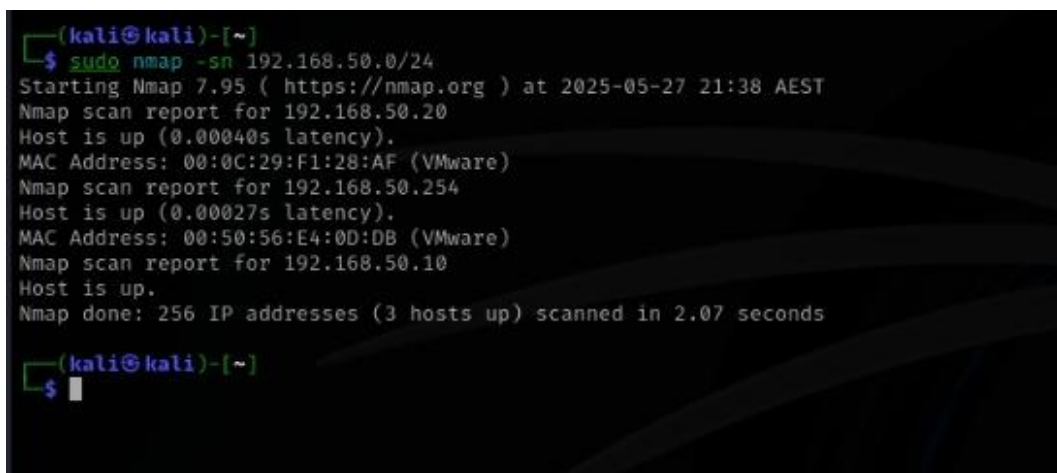
5: Technical Findings

This section presents the detailed results of the reconnaissance phase, including network discovery, enumeration, and vulnerability analysis. The findings revealed multiple critical vulnerabilities and guided the selection of the HTTP service as the primary target for DoS testing.

5.1 Network Discovery Results

Using the Nmap network discovery command `nmap -sn 192.168.50.0/24` to scan the target network segment for active hosts, three hosts were identified:

IP Address	Host Identity
192.168.50.10	Attacking System (Kali Linux)
192.168.50.20	Target System (Metasploitable 2)
192.168.50.254	VMware DHCP Server



```
(kali@kali)-[~]
$ sudo nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 21:38 AEST
Nmap scan report for 192.168.50.20
Host is up (0.00040s latency).
MAC Address: 00:0C:29:F1:28:AF (VMware)
Nmap scan report for 192.168.50.254
Host is up (0.00027s latency).
MAC Address: 00:50:56:E4:0D:DB (VMware)
Nmap scan report for 192.168.50.10
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.07 seconds

(kali@kali)-[~]
$
```

FIGURE 1 - NMAP PING SWEEP REVEALING ACTIVE HOSTS IN TARGET NETWORK SEGMENT

This confirmed that the target system was accessible and no additional security devices were detected in the network path.

5.2 Service Enumeration Results

Following successful target identification, service enumeration was employed to discover open ports and running services with their versions in order to identify potential vulnerabilities to exploit. The timing of the scan required careful calibration through trial-and-error, initially using T4 (Aggressive) which caused the target system to become unresponsive. A T2 (Polite) scan was tried next, which maintained system stability but proved inefficient and was aborted after 25 minutes. A T3 (Normal) scan was finally selected to balance both system stability and scanning speed. The final command used to complete the enumeration scan was:

```
nmap -sV -p- -O --reason -T3 192.168.50.20
```



```

(kali@kali)-[~]
$ sudo nmap -sV -p- -O --reason -T3 192.168.50.20
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 22:03 AEST
Nmap scan report for 192.168.50.20
Host is up, received arp-response (0.00077s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 64  vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64  OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64  Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64  Postfix smtpd
53/tcp    open  domain       syn-ack ttl 64  ISC BIND 9.4.2
80/tcp    open  http         syn-ack ttl 64  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      syn-ack ttl 64  2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         syn-ack ttl 64  netkit-rsh rexecd
513/tcp   open  login        syn-ack ttl 64  OpenBSD or Solaris rlogind
514/tcp   open  shell        syn-ack ttl 64  Netkit rshd
1099/tcp  open  java-rmi     syn-ack ttl 64  GNU Classpath grmiregistry
1524/tcp  open  bindshell    syn-ack ttl 64  Metasploitable root shell
2049/tcp  open  nfs          syn-ack ttl 64  2-4 (RPC #100003)
2121/tcp  open  ftp          syn-ack ttl 64  ProFTPD 1.3.1
3306/tcp  open  mysql        syn-ack ttl 64  MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      syn-ack ttl 64  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   syn-ack ttl 64  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          syn-ack ttl 64  VNC (protocol 3.3)
6000/tcp  open  X11          syn-ack ttl 64  (access denied)
6667/tcp  open  irc          syn-ack ttl 64  UnrealIRCd
6697/tcp  open  irc          syn-ack ttl 64  UnrealIRCd
8009/tcp  open  ajp13        syn-ack ttl 64  Apache Jserv (Protocol v1.3)
8180/tcp  open  http         syn-ack ttl 64  Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          syn-ack ttl 64  Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
43620/tcp open  java-rmi     syn-ack ttl 64  GNU Classpath grmiregistry
44793/tcp open  nlockmgr     syn-ack ttl 64  1-4 (RPC #100021)
45439/tcp open  mountd       syn-ack ttl 64  1-3 (RPC #100005)
55334/tcp open  status       syn-ack ttl 64  1 (RPC #100024)
MAC Address: 00:0C:29:F1:28:AF (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 134.66 seconds

```

FIGURE 2 - COMPREHENSIVE PORT SCAN REVEALING MULTIPLE VULNERABLE SERVICES

CRITICAL VULNERABILITIES:

Port	Service	Version	Risk Level	CVE/Notes
21	FTP	vsftpd 2.3.4	Critical	CVE-2011-2523 (Backdoor)
22	SSH	OpenSSH 4.7p1	High	37 associated CVEs
80	HTTP	Apache 2.2.8	High	Primary DoS target
1524	bindshell	Root shell	Critical	Direct system access
3306	MySQL	5.0.51a	Medium	Database exposure

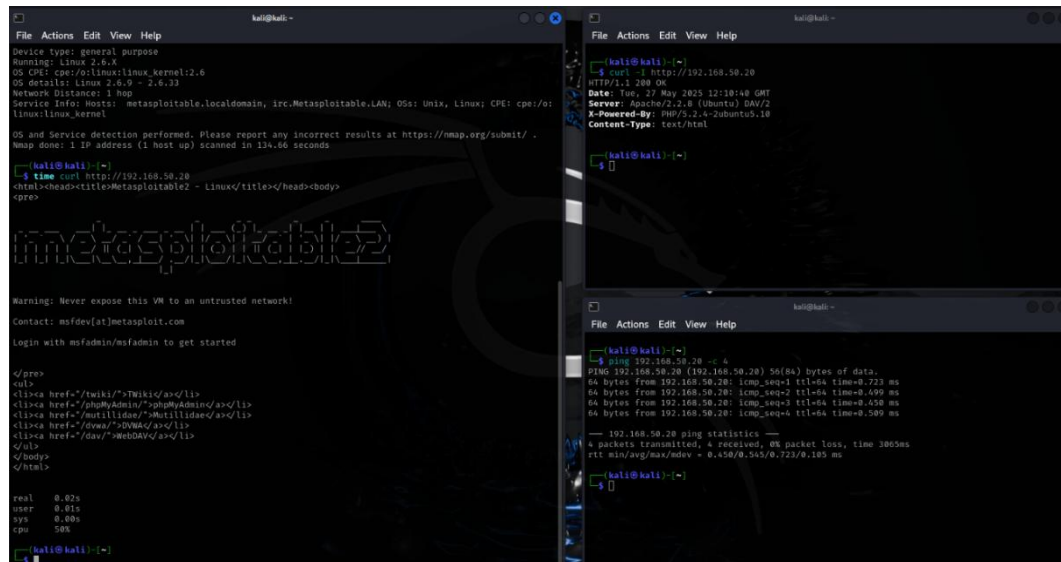
These findings revealed multiple attack vectors, with the HTTP service on port 80 selected as the primary target for DoS testing.

5.3 Baseline Testing

Prior to executing the DoS attack, a baseline of normal system behaviour was established for comparison with post-attack measurements to accurately assess the impact. This baseline

documentation ensures that any performance degradation can be attributed directly to the attack rather than pre-existing system issues.

HTTP headers were obtained using `curl -I http://192.168.50.20` and the responsiveness of the server `time curl http://192.168.50.20`. Network latency was tested with `ping 192.168.50.20`



The image displays three terminal windows from a Kali Linux environment. The leftmost window shows the Metasploit VM's configuration and a successful HTTP request to 192.168.50.20, returning a 200 OK status with HTML content. The middle window shows the output of a 'time curl' command, indicating a response time of 0.02 seconds. The rightmost window shows the output of a 'ping' command, indicating a network latency of less than 1ms.

```
File Actions Edit View Help
Device type: general purpose
Running: Linux 2.6.x
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, Src:Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 134.66 seconds

kali@kali:~$ time curl http://192.168.50.20
html<head><title>Metasploitable2 - Linux</title></head><body>
<pre>
Metasploitable2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

</pre>
</body>
</html>

real    0.02s
user    0.01s
sys     0.00s
cpu      50%

kali@kali:~$ curl -I http://192.168.50.20
HTTP/1.1 200 OK
Date: Tue, 27 May 2025 12:10:40 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.14
Content-Type: text/html

kali@kali:~$

kali@kali:~$ ping 192.168.50.20 -c 4
PING 192.168.50.20 (192.168.50.20) 56(84) bytes of data:
64 bytes from 192.168.50.20: icmp_seq=1 ttl=64 time=0.723 ms
64 bytes from 192.168.50.20: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 192.168.50.20: icmp_seq=3 ttl=64 time=0.450 ms
64 bytes from 192.168.50.20: icmp_seq=4 ttl=64 time=0.509 ms

--- 192.168.50.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/ndev = 0.450/0.545/0.723/0.105 ms

kali@kali:~$
```

FIGURE 3 - NORMAL SERVICE RESPONSE TIMES AND AVAILABILITY BEFORE ATTACK

BASELINE METRICS:

HTTP Response Time	0.02 seconds
Service Status	200 OK
Network Latency	<1ms ping response
Service Availability	100%

6: Attack Execution and Results

This section documents the execution of the DoS attack against the target system and the comprehensive monitoring of its impact. The attack successfully demonstrated critical vulnerabilities in the system's resilience to denial-of-service attacks, resulting in complete service unavailability that lasted well beyond the attack duration.

6.1 Attack Methodology

The DoS attack was executed using a **SYN flood** technique that targets the HTTP service on port 80 using the hping3 tool with the following command:

```
hping3 -S -p 80 -flood -rand-source 192.168.50.20
```

Attack Parameters:

- **Target Service:** Port 80 (HTTP)
- **Attack Method:** SYN flood with randomised source IP addresses
- **Duration:** 20 seconds (controlled)
- **Start Time:** 22:12:30
- **End Time:** 22:12:50

The attack was deliberately limited to 20 seconds to demonstrate impact while maintaining controlled testing conditions.

6.2 Real-Time Monitoring

In order to comprehensively document the impact of the attack, monitoring was setup across multiple terminals prior to attack execution. This allowed for real-time observation of any degradation of the service and loss of network connectivity.

Monitoring Configuration:

- **Terminal 1:** Attack execution (hping3 command)
- **Terminal 2:** HTTP service monitoring using `watch -n 1 "curl -s -I http://192.168.50.20 | head -1"`
- **Terminal 3:** Network connectivity monitoring using `watch -n 30 "ping 192.168.50.20 -c 4"`

This approach to monitoring provided continuous visibility to both service-level and network-level impacts throughout both the attack and recovery phases.

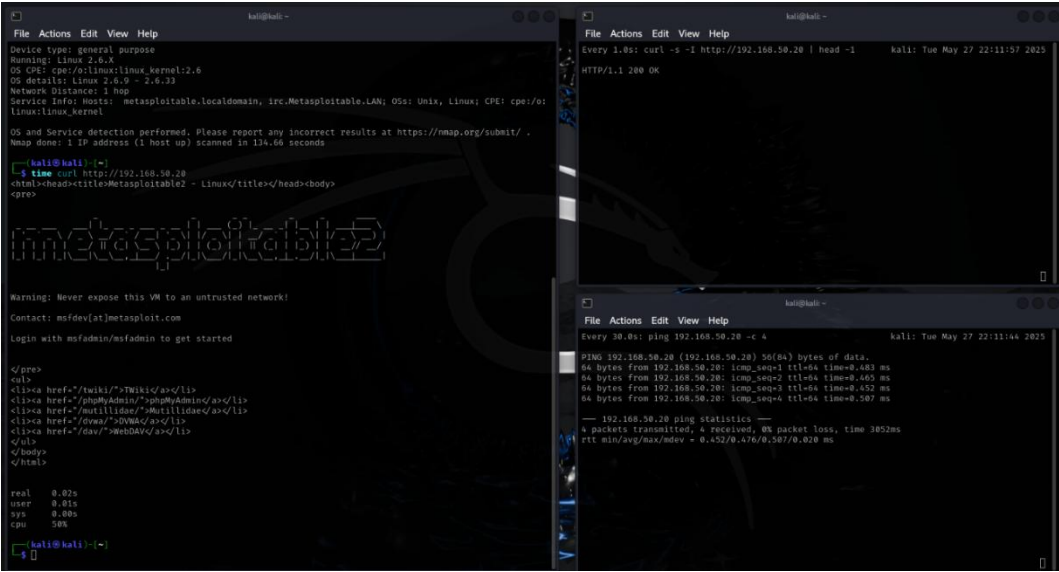


FIGURE 4 - MULTI-TERMINAL MONITORING CONFIGURATION FOR REAL-TIME IMPACT ASSESSMENT

6.3 Attack Impact Results

The DoS attack resulted in immediate and sustained service failure, demonstrating critical vulnerabilities in the target system’s resilience mechanisms.

ATTACK TIMELINE:

Time	HTTP Service Status	Network Connectivity	Overall Status
Pre-Attack	200 OK (0.02s response)	0% packet loss	Normal
22:12:30 (Attack Start)	Service degradation begins	Increasing packet loss	Failing
22:12:50 (Attack End)	Completely unresponsive	100% packet loss	Failed
+1 Minute	Completely unresponsive	100% packet loss	Failed
+30 Minutes	Completely unresponsive	100% packet loss	Failed

The attack launched successfully at 22:12:30 with monitoring systems immediately detecting service degradation. **Complete service failure** occurred withing seconds of the attack commencing, with both HTTP service monitoring and network connectivity tests failing simultaneously.

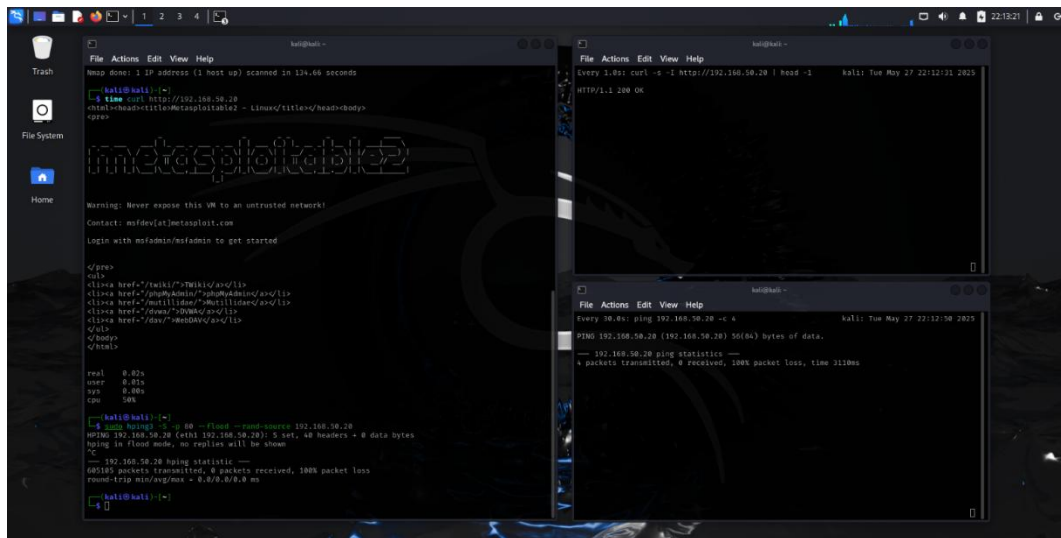


FIGURE 7 - 1 MINUTE POST-ATTACK

Figure 7: No recovery of targeted system detected one minute after attack initiation.

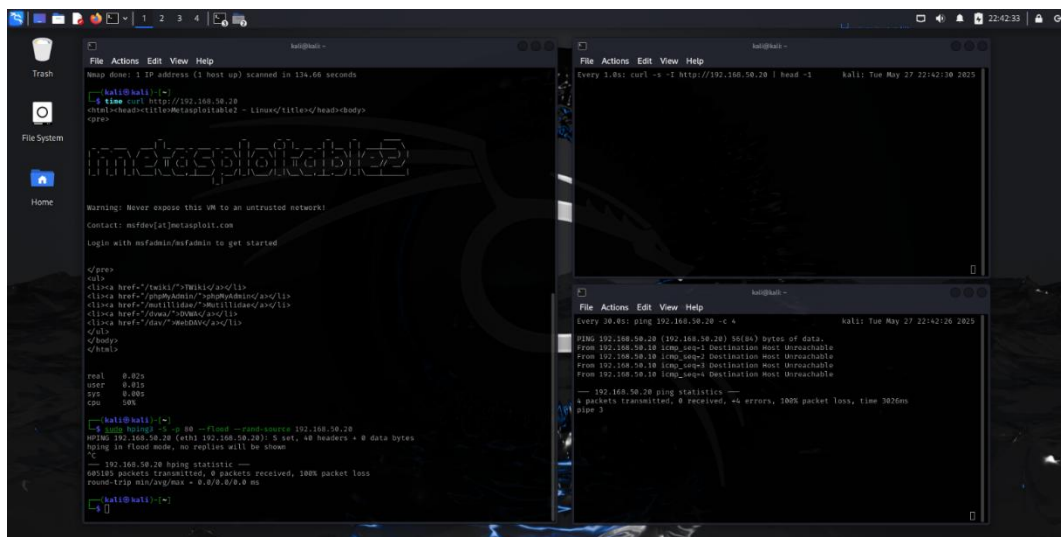


FIGURE 8 - 30 MINUTES POST-ATTACK

Figure 8: Sustained system outages continues 30 minutes after attack initiation.

Critical Finding: The target system showed no signs of automatic recovery even 30 minutes after the brief 20-second attack concluded, indicating a complete absence of resilience mechanisms.

6.4 Attack Effectiveness Analysis

The DoS attack showed exceptional effectiveness, achieving sustained service disruption fast beyond the attack duration.

Key Effectiveness Metrics:

- **Attack Duration:** 20 seconds
- **Impact Duration:** 30+ minutes (ongoing at assessment conclusion)
- **Impact Amplification Ratio:** 90:1 (impact time vs attack time)
- **Service Recovery:** Manual intervention required (no automatic recovery detected)

Critical Assessment: The amplification ratio shows that an attacker can make minimal effort and still result in extensive disruption to service operation. The target system's inability to automatically recover from a brief attack represents a **critical business continuity risk**, which is particularly concerning for a healthcare environment where service availability directly impacts patient care.

7: Business Impact Assessment

This section analyses the potential real-world consequences of the demonstrated DoS vulnerability within a healthcare environment, where system availability directly impacts patient safety and compliance with laws and regulations.

7.1 Service Availability Impact

The complete HTTP service outage lasting 30+ minutes would result in:

- **Patient portal completely inaccessible** – patients unable to view test results, schedule appointments, or communicate with providers
- **Online appointment scheduling system unavailable** – forcing manual phone-based scheduling with increased staff workload and phone-in wait times for patients
- **Electronic medical records system unreachable** – potential disruption to clinical workflows and patient care delivery
- **Telehealth services disrupted** – virtual consultations and remote monitoring capabilities offline

7.2 Healthcare-Specific Implications

Patient Safety Risks:

- Critical test results inaccessible during emergency situations
- Medication interaction checks unavailable at point of care
- Patient history and allergy information unreachable
- Delay in time-sensitive medical decisions

Operational Disruption:

- Staff forced to revert to manual, paper-based processes
- Increased workload on phone systems and administrative staff
- Potential delays in patient care
- Disruption to clinical workflows and efficiency

7.3 Compliance and Regulatory Concerns

Privacy and Healthcare Regulations:

- **Privacy Act 1988 violations** – inability to provide timely access to personal health information as required under Australian Privacy Principles
- **Notifiable Data Breaches (NDB) scheme obligations** – extended service outages may trigger breach notification requirements to the Office of the Australian Information Commissioner (OAIC)
- **My Health Records Act 2012 compliance issues** – if connected to the My Health Record system, outages could violate availability requirements
- **State health privacy legislation** – potential violations of Victorian health privacy laws regarding secure and available health information systems

- **Professional healthcare standards** – failure to maintain accessible patient records may breach professional practice standards

Regulatory Reporting Requirements:

- Incident reporting to relevant state health authorities
- Potential investigation by the OAIC if patient data accessibility is compromised
- Documentation requirements for business continuity failures

7.4 Financial Impact Assessment

Direct Costs:

- Revenue loss from cancelled or delayed appointments
- IT incident response and recovery costs
- Potential regulatory fines and penalties
- Staff overtime costs for manual processes
- Patient compensation for delayed care

Indirect Costs:

- Reputation damage and loss of patient trust
- Increased insurance premiums
- Investment in enhanced security infrastructure
- Staff training on manual backup procedures

8: Additional Security Observations

While DoS vulnerability assessment was the primary objective, reconnaissance activities revealed multiple critical security weaknesses that significantly compound the organisation's risk profile.

8.1 Secondary Vulnerabilities Identified

Critical Risk Vulnerabilities:

- **FTP Backdoor (Port 21):** vsftpd 2.3.4 contains a known backdoor vulnerability (CVE-2011-2523) enabling remote command execution
- **Direct System Access (Port 1524):** Bindshell service providing direct root-level command execution capability
- **Outdated SSH Service (Port 22):** OpenSSH 4.7p1 affected by 37 known CVEs, presenting multiple attack vectors

High Risk Vulnerabilities:

- **Database Exposure (Port 3306):** MySQL service accessible without proper network segmentation
- **Outdated Web Server:** Apache 2.2.8 running with known vulnerabilities

Risk Assessment: These vulnerabilities could enable complete system compromise extending far beyond service disruption to full data exfiltration and system control.

8.2 System Resilience Concerns

Complete System Failure Evidence: During initial testing phases, a similar DoS attack resulted in complete system failure with kernel-level errors, requiring full virtual machine restart. This demonstrates that DoS vulnerability extends beyond service disruption to potential complete system instability.

```
[ 408.076211] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 419.888472] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 431.690770] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 443.483052] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 455.275363] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 467.067669] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 478.859967] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 490.652259] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 502.444556] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 514.236847] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 526.039187] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 537.831439] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 549.623740] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 561.416049] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 573.208337] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 585.010626] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 596.802920] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 608.620113] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 620.407485] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 632.219751] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 644.012053] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 655.804358] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 667.596670] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
[ 679.388963] BUG: soft lockup - CPU#0 stuck for 11s! [swapper:0]
```

FIGURE 9 - COMPLETE SYSTEM FAILURE WITH KERNEL-LEVEL ERRORS OBSERVED DURING INITIAL TESTING

Recovery Mechanisms: No automatic recovery or failover systems were detected, indicating a complete reliance on manual intervention for service restoration.

8.3 Risk Assessment Summary

Overall Security Posture: **CRITICAL**

The combination of successful DoS vulnerability and multiple other critical security weaknesses presents an unacceptable risk level for a healthcare organisation that manages sensitive patient data.

Primary Risk Factors:

- **No resilience mechanisms** against service disruption attacks
- **Multiple pathways for complete system compromise** through backdoor vulnerabilities
- **Absence of network segmentation** protecting critical services
- **Outdated software stack** with numerous known vulnerabilities
- **No automated recovery capabilities** requiring manual intervention for all incidents

Threat Actor Implications:

- **Low-skill attackers** could cause significant service disruption with minimal effort (20-second attack = 30+ minute outage)
- **Advanced persistent threats** could leverage multiple attack vectors for complete network compromise
- **Insider threats** could exploit direct system access capabilities
- **Opportunistic attackers** could discover and exploit the numerous known vulnerabilities

Business Risk Classification: Given the healthcare context where system availability directly impacts patient safety and the demonstrated lack of basic security controls, this system presents an **immediate and critical risk** requiring urgent remediation.

9: Recommendations

The following recommendations are sorted by urgency and impact, with immediate actions needed to address critical vulnerabilities.

9.1 Immediate Actions (Critical – Implement within 24-48 hours)

1. Eliminate Critical Vulnerabilities

- Immediately disable or patch vsftpd 2.3.4 (backdoor vulnerability)
- Close port 1524 bindshell access
- Update OpenSSH to current stable version

2. Implement Basic DoS Protection

- Configure SYN flood protection on network devices
- Enable rate limiting on web servers
- Deploy basic DDoS mitigation at network perimeter

9.2 Short-term Improvements (1-4 weeks)

1. Network Security Hardening

- Implement network segmentation between DMZ and internal systems
- Deploy intrusion detection/prevention systems (IDS/IPS)
- Configure restrictive firewall rules limiting service exposure

2. Service Resilience

- Establish automated service monitoring and alerting
- Implement load balancing and failover mechanisms
- Configure automatic service restart capabilities

9.3 Long-term Improvements (1-6 months)

1. Comprehensive Security Program

- Regular penetration testing schedule (quarterly assessments)
- Staff security awareness training program
- Incident response plan testing and refinement

2. Business Continuity Enhancement

- Redundant service architectures across multiple locations
- Comprehensive backup and disaster recovery procedures
- Defined Recovery Time Objective (RTO) and Recovery Point Objectives (RPO)

10: Conclusion

10.1 Assessment Summary

This Red Team assessment successfully exposed critical vulnerabilities in the target system's resilience to DoS attacks and multiple additional security weaknesses. A simple 20-second SYN flood attack resulted in complete service unavailability lasting over 30 minutes with no automatic recovery.

10.2 Key Findings

- **DoS vulnerability confirmed:** 90:1 impact amplification ratio (20-second attack = 30+minute outage)
- **No resilience mechanisms detected:** Manual intervention required for service restoration
- **Multiple critical vulnerabilities identified:** Including backdoor access and direct system compromise paths
- **Significant business continuity risk:** Particularly concerning for healthcare operations

10.3 Overall Risk Assessment

Risk Level: *CRITICAL* – The combination of successful DoS vulnerability and additional critical security weaknesses presents unacceptable risk for a healthcare organisation.

10.4 Next Steps

1. Immediate implementation of critical security patches
2. Blue Team defensive response and remediation verification
3. Purple Team collaborative analysis for comprehensive security improvement
4. Follow-up assessment to validate remediation effectiveness

APPENDICES

Appendix A: Technical Command Reference

- Network discovery: `nmap -sn 192.168.50.0/24`
- Service enumeration: `nmap -sV -p- -O -reason -T3 192.168.50.20`
- DoS attack: `hping3 -S -p 80 -flood -rand-source 192.168.50.20`
- Service monitoring: `curl -I http://192.168.50.20,`
`time curl http://192.168.50.20`

Appendix B: Vulnerability Database References

- CVE-2011-2523: vsftpd 2.3.4 Backdoor
- OpenSSH 4.7p1: 37 associated CVEs
- Apache 2.2.8: Multiple known vulnerabilities