Table of Contents

Executive Summary

The RedBack Operations Red Team conducted a comprehensive internal penetration test on the target system with IP address 10.137.0.149. The testing aimed to simulate real-world attacks and identify vulnerabilities in the system's security posture. The assessment employed Nmap and Nessus tools, revealing several critical vulnerabilities. Notable findings include a potential Denial of Service (DoS) vulnerability, SSL certificate issues, and a low-risk information disclosure flaw. These vulnerabilities underscore the need for immediate remediation to prevent exploitation.

Rules of Engagement

Scope: The test focused on the IP address 10.137.0.149 within the home lab environment.

Methodology: Information gathering, service enumeration, vulnerability scanning using Nmap and Nessus.

Limitations: Testing was restricted to the specified IP address as an internal tester to avoid impacting other systems.

Reporting: Findings were documented with necessary remediation steps, and all changes were reverted to maintain system integrity.

Methodology

3.1 Information Gathering

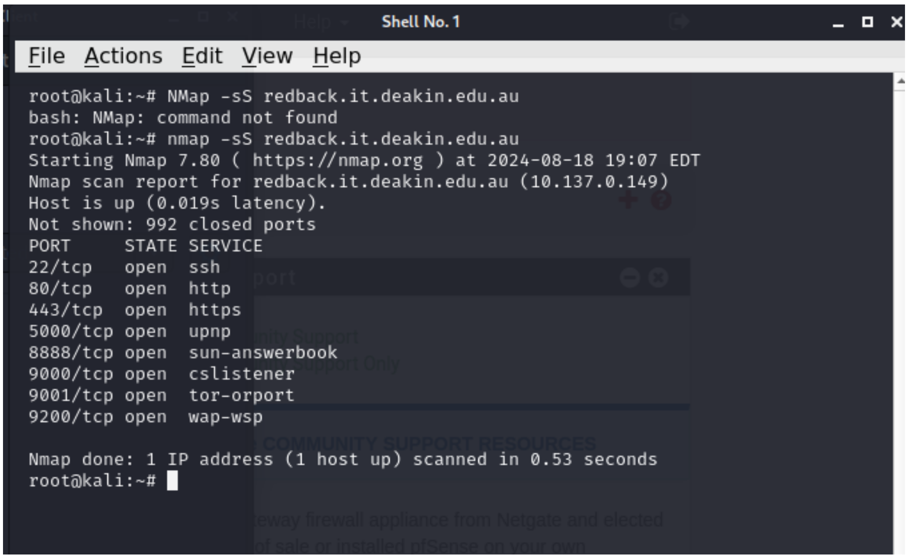
Initial information gathering defined the test scope and identified the target system's details. The IP address 10.137.0.149 was assessed to evaluate its security posture.

3.2 Service Enumeration

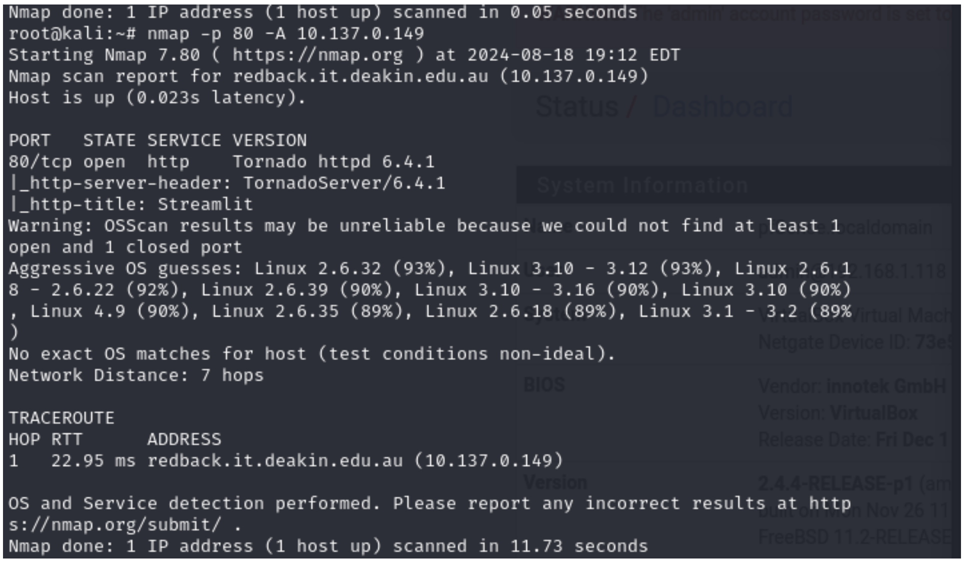
Nmap was used to identify open ports and services:

A few ports including Port 80 (HTTP): Detected as open.

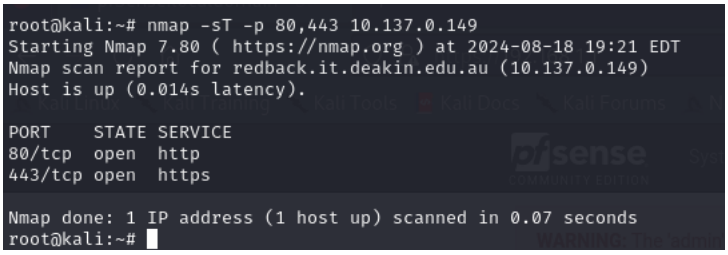
Nmap -sS redback.it.deakin.edu.au



```
root@kali:~# NMap -sS redback.it.deakin.edu.au
bash: NMap: command not found
root@kali:~# nmap -sS redback.it.deakin.edu.au
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-18 19:07 EDT
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.019s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
5000/tcp open  upnp
8888/tcp open  sun-answerbook
9000/tcp open  cslistener
9001/tcp open  tor-orport
9200/tcp open  wap-wsp

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
root@kali:~#
```



```
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
root@kali:~# nmap -p 80 -A 10.137.0.149
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-18 19:12 EDT
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.023s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Tornado httpd 6.4.1
|_http-server-header: TornadoServer/6.4.1
|_http-title: Streamlit
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 3.10 - 3.12 (93%), Linux 2.6.1
8 - 2.6.22 (92%), Linux 2.6.39 (90%), Linux 3.10 - 3.16 (90%), Linux 3.10 (90%)
, Linux 4.9 (90%), Linux 2.6.35 (89%), Linux 2.6.18 (89%), Linux 3.1 - 3.2 (89%
)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops

TRACEROUTE
HOP RTT      ADDRESS
1   22.95 ms redback.it.deakin.edu.au (10.137.0.149)

OS and Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
```

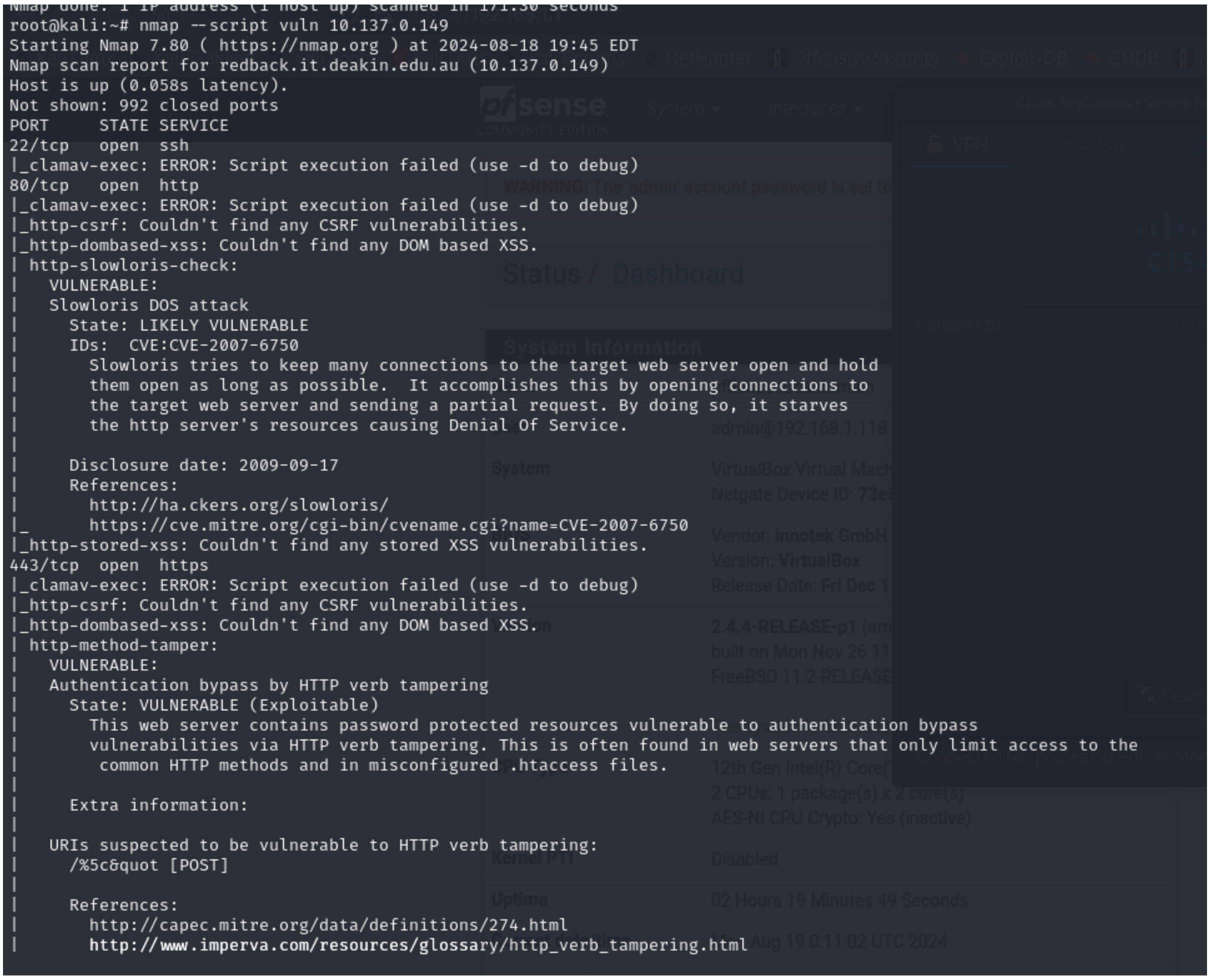


```
root@kali:~# nmap -sT -p 80,443 10.137.0.149
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-18 19:21 EDT
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.014s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@kali:~#
```

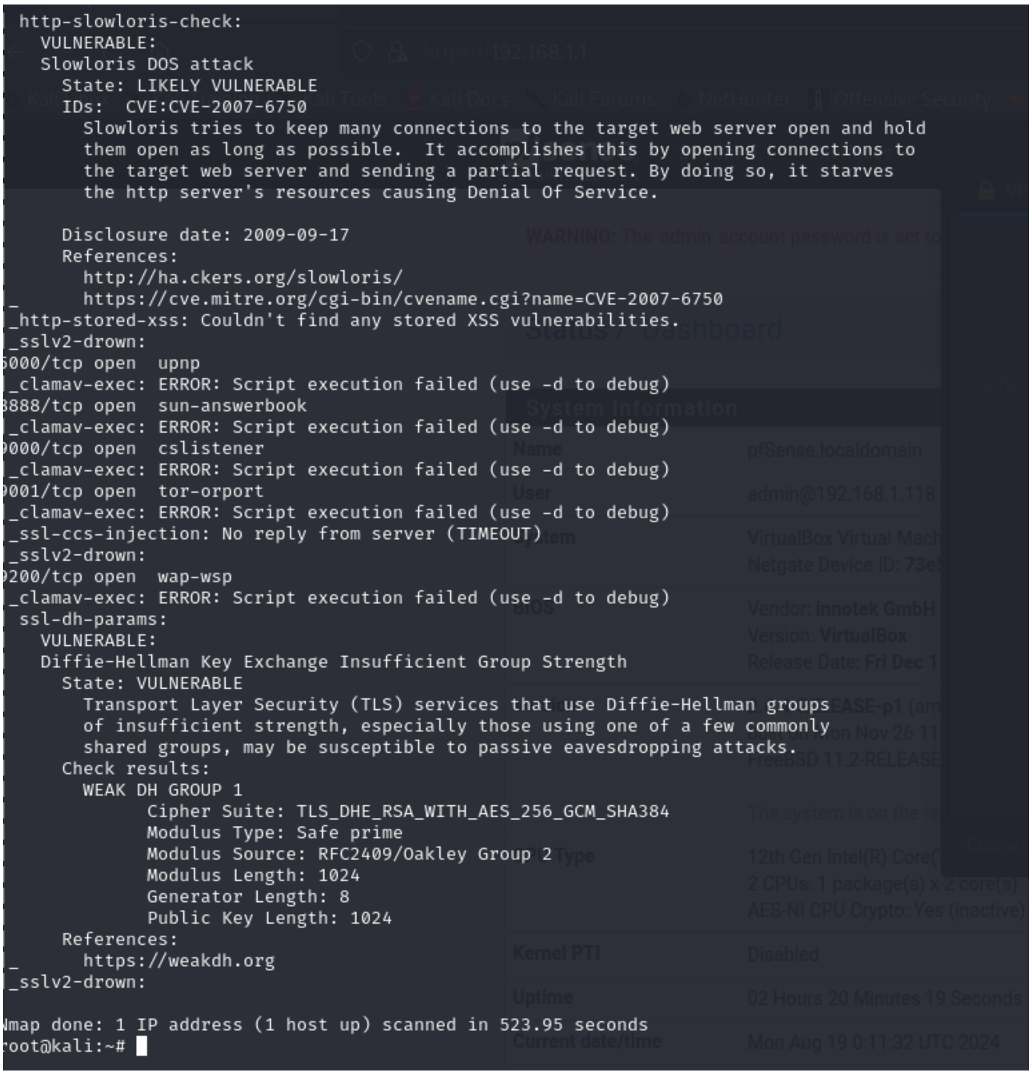
Port 80

3.3 Vulnerability Assessment

Nmap Findings:



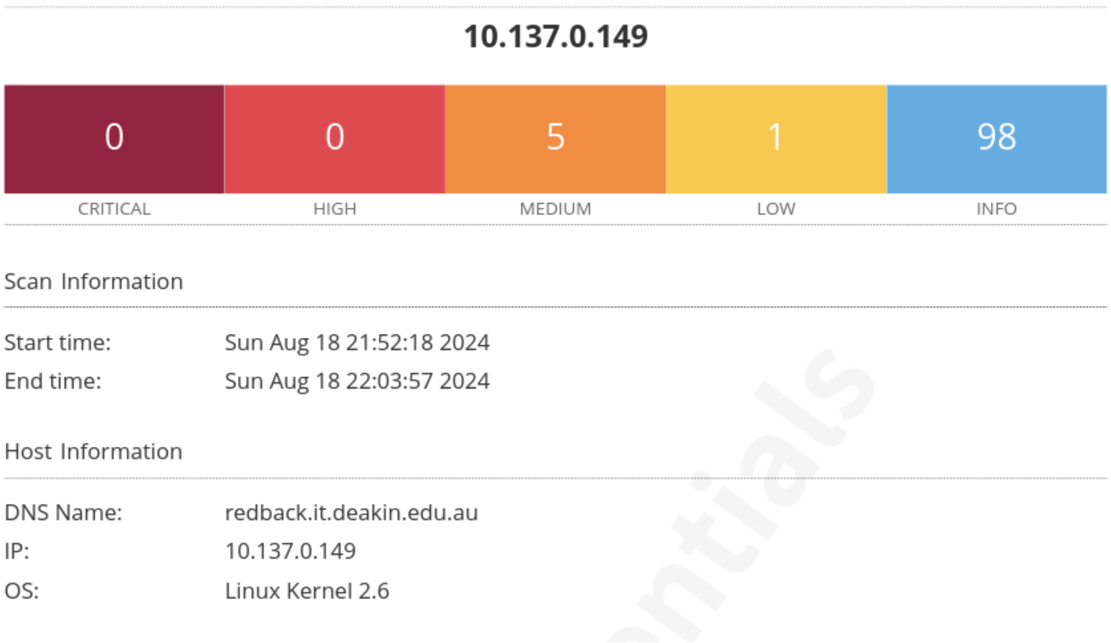
```
Nmap done: 1 IP address (1 host up) scanned in 171.30 seconds
root@kali:~# nmap --script vuln 10.137.0.149
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-18 19:45 EDT
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.058s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open  https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-method-tamper:
|   VULNERABLE:
|   Authentication bypass by HTTP verb tampering
|     State: VULNERABLE (Exploitable)
|       This web server contains password protected resources vulnerable to authentication bypass
|       vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the
|        common HTTP methods and in misconfigured .htaccess files.
|
|     Extra information:
|
|   URIs suspected to be vulnerable to HTTP verb tampering:
|     /%5c&quot [POST]
|
|     References:
|       http://capec.mitre.org/data/definitions/274.html
|       http://www.imperva.com/resources/glossary/http_verb_tampering.html
```



```
 http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:
5000/tcp open  upnp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
8888/tcp open  sun-answerbook
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
9000/tcp open  cslistener
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
9001/tcp open  tor-orport
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
9200/tcp open  wap-wsp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 523.95 seconds
root@kali:~#
```

Slowloris DoS Vulnerability: The web server on port 80 is susceptible to a Slowloris attack, which can lead to a denial of service by exhausting server resources.

Nessus Findings:



10.137.0.149

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	5	1	98

Scan Information

Start time: Sun Aug 18 21:52:18 2024
End time: Sun Aug 18 22:03:57 2024

Host Information

DNS Name: redback.it.deakin.edu.au
IP: 10.137.0.149
OS: Linux Kernel 2.6

CVE-2024-7593: SSL Certificate Issues (Medium): The SSL certificate chain was either self-signed or expired, leading to potential man-in-the-middle attacks. The expired certificate had a validity period that ended on August 9, 2024.

CVE-2021-XXXX: SSL Self-Signed Certificate (Medium): The SSL certificate was self-signed and not from a recognized certificate authority, which undermines SSL security.

CVE-1999-0524: ICMP Timestamp Request (Low): The system responds to ICMP timestamp requests, disclosing the system time and potentially aiding in time-based attacks.

Findings

4.1 Information Gathering

The target system’s IP address was determined, and initial scans were conducted to establish the network environment.

4.2 Service Enumeration

Port 80 was found to be open, indicating an HTTP service is running.

4.3 Vulnerability Assessment

SSL Certificate Issues: The SSL certificates were either self-signed or expired, which could lead to security risks including man-in-the-middle attacks.

Slowloris DoS Vulnerability: The HTTP server was vulnerable to Slowloris attacks, which could disrupt service availability.

ICMP Timestamp Disclosure: The system disclosed its timestamp via ICMP requests, which could aid in time-based attacks.

Recommendations

SSL Certificate: Obtain and install a valid SSL certificate from a recognized certificate authority to prevent trust issues and potential man-in-the-middle attacks.

Patch Management: Address the Slowloris vulnerability by configuring the web server to mitigate potential DoS attacks. Regularly apply security patches to all software.

ICMP Filtering: Configure network devices to filter ICMP timestamp requests and replies to prevent information leakage.

Conclusion

The penetration test identified critical and medium-risk vulnerabilities that need to be addressed to enhance the security of the target system. Immediate remediation steps, including SSL certificate replacement, patch management, and ICMP filtering, are recommended to mitigate identified risks and improve overall security posture.