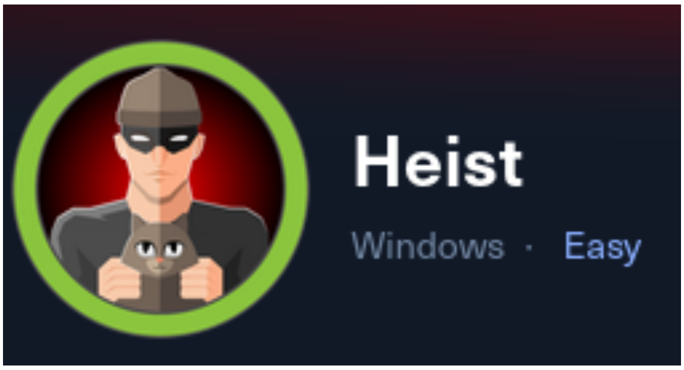
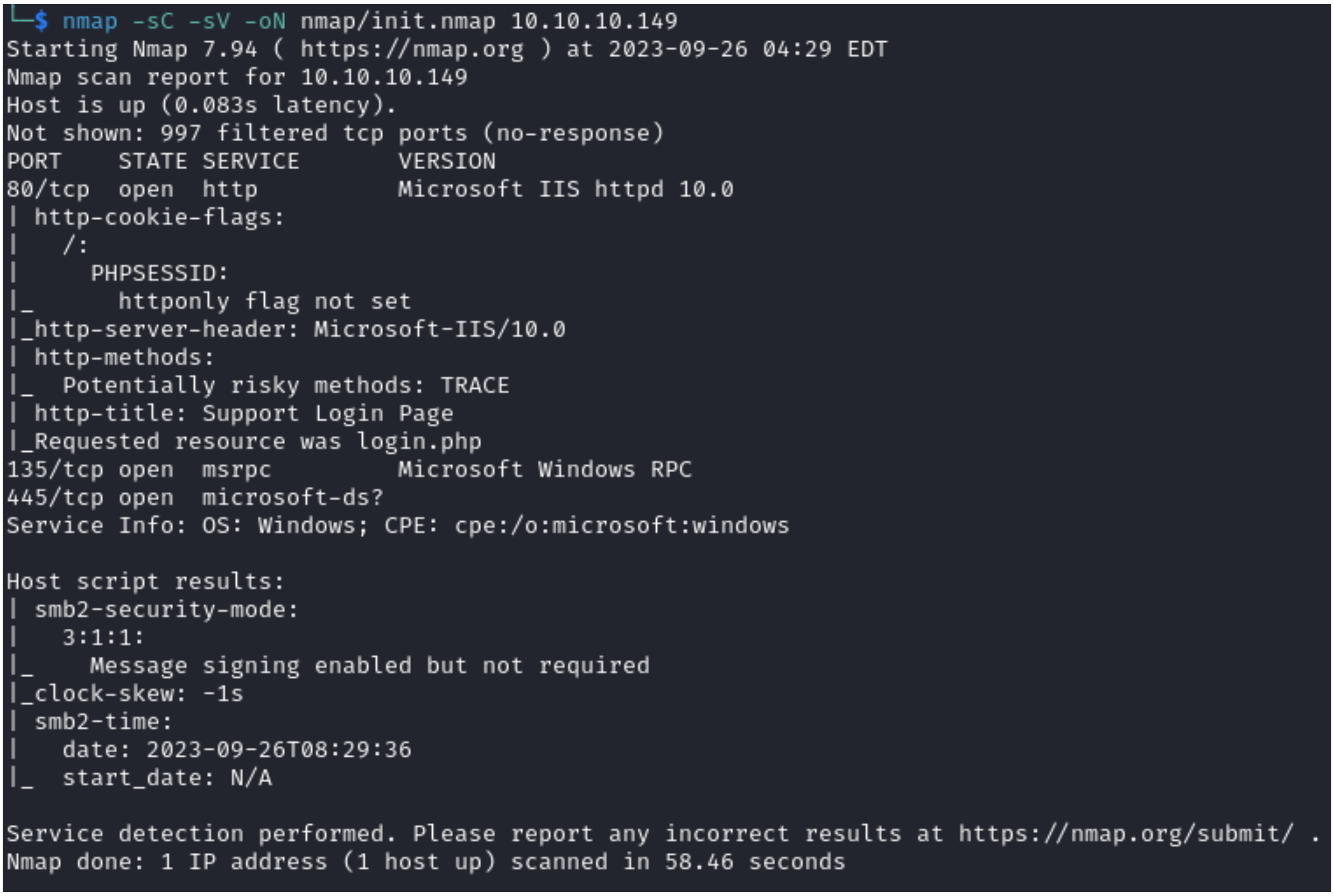
Heist



Enumeration

NMAP:



```
└─$ nmap -sC -sV -oN nmap/init.nmap 10.10.10.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-26 04:29 EDT
Nmap scan report for 10.10.10.149
Host is up (0.083s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
| http-title: Support Login Page
|_Requested resource was login.php
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -1s
| smb2-time:
|   date: 2023-09-26T08:29:36
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.46 seconds
```

SMB and RPC doesn't seem to allow anonymous/null authentication.

Moving on to the website:

Logging in as a guest, we see a support chat with a cisco configuration file containing password hashes

Two of which we crack with (https://github.com/theevilbit/ciscot7)
These are Cisco Type 7 decrypted passwords

rout3r:$uperP@ssword
admin:Q4)sJu\Y8qz*A3?d

The other secret is just an md5sum. We can crack this with hashcat

stealth1agent

Now we have 3 possible passwords, and we can create a wordlist of possible usernames using words from the website

Using the wordlists we have gathered, we can bruteforce smb using crackmapexec, and we find out these are valid creds:

Hazard:stealth1agent

Unfortunately, there aren't any shares we can read except IPC$ which usually has restricted access, and we don't have winrm access. Back to enumeration we go

IMPACKET:

lookupsid.py ‘hazard:stealth1agent’@10.10.10.149
-> gives us a list of valid users on the box

Manually:

rpcclient -U ‘hazard%stealth1agent’ 10.10.10.149
→ login to rpcclient

use lookupnames <user> to look up the sid of a specific user
use lookupsids to brute force other users (usually changing the RID by a few numbers reveals more users)

Now we have more usernames to work with.

Foothold

Doing more smb bruteforcing with crackmapexec, we find more valid creds:

Chase:Q4)sJu\Y8qz*A3?d

We find that these creds allow for winrm login!

Priv Esc

In Pogram Files, we see that firefox is installed, which is non-standard

Using powershell's Get-Process cmdlet, we see that firefox is indeed a currently running process. We can also take note of the PIDs of all of the firefox processes.

To view the processdump, we will use a tool called procdump64.exe which is a part of the Sysinternals Suite

```
.\procdump64.exe -ma <PID>
```

-> creates a dump file

grepping through the dump file, we are able to extract creds for the website login page

admin@support.htb : 4dD!5}x/re8]FBuZ

```
/usr/bin/impacket-psexec administrator:'4dD!5}x/re8]FBuZ'@10.10.10.149
```

WE ARE IN