Eoin Dalton

20070289

Metasploit

Research Project

Network & System Security

Abstract

In this report I will be researching Metasploit. It will look at who and when it was created how it have evolved over the years. There will also be a practical element where I will conduct an experiment and show and explain with the aid screen shots.

Contents

Introduction

For Network and System Security we were asked to choose a topic. The topic I have chosen is Metasploit, as I had heard a lot about this tool but never got around to using it and this was my perfect chance. In this report I will start with a short description of how and what Metasploit is, I will then talk about what I would like to accomplish with Metasploit in the theory section and I will then move onto the technical detail. This will explain how I am going to install and configure all the tools needed for the report. In the experiment section I will aim to exploit a Metasploitable machine purposely configured to be vulnerable to be exploited. I will also go through the steps involved in the exploit in detail. I will finish with my conclusion.

Description

The Metasploit Project is an opensource security platform that helps network administrators and security professionals discover security vulnerabilities. It also helps them penetration testing on their own systems through a built-in set of modules. It is one of the most used tools of its kind in the world for penetration testing and exploit development and vulnerability research. The software its self was developed by HD Moore in 2003, “as a public resource for exploit project” (Marquez, n.d.). One of Moore’s aim was to build a tool that even novice users could use. Metasploit framework merges most resent vulnerabilities into a single location. Moore wrote the whole framework in the programming language “Perl” but in version 3 it got a complete over haul and was rewritten in the powerful scripting language “Ruby” and “now boasts the power of automation due to the nature of Ruby’s status as an object-oriented language” (Marquez, n.d.). In 2009 Metasploit was acquired by Rapid 7 (BussinessWire, 2009).

Since Rapid 7 took over Metasploit they have released some commercial versions of the software for security professionals as well as enhancing the framework its self. Having so many vulnerabilities in a single location helps developers to develop code to patch the vulnerabilities more rapidly.

Metasploit comes in three variants, they provide a free community version, Metasploit Pro is aimed at penetration testers and IT security teams. Metasploit Express is aimed at security teams to learn and verify security vulnerabilities. Each edition comes with different features. Metasploit community edition comes with features such as network-host identification and ports scanning and many more. For more information see the link in references below (Offensive-security.com, 2018). Metasploit Pro comes with wizards and meta-modules. Meta-modules are a set of security tasks that are automated and are designed to aid security teams to perform their job more effectively. Metasploit Express was designed in 2010 and one of the main features is it provides automated evidence collection and a user-friendly interface ("What Is Metasploit? - Infosec Addicts, 2018).

Metasploit consists of modules, these modules are pre-written scripts that can be used by the users. “A payload in Metasploit refers to an exploit” (Offensive Security, 2018). The module is a piece of malicious code that exploits the target. I feel more time would be needed to test all functionality and commands. There are search functions built where one can search just

about anything in their database and users can also search exploits, operating system type and the dates the exploits occurred.

Theory

What I wanted to look at was how to gain remote access to a machine. I first downloaded a Windows XP iso image for penetration testing, after a couple of days attempting I found that the image I downloaded was patched and not vulnerable to remote access exploit. I tried Google for an unpatched version but to no avail. My next option was to download a Metasploitable instance from Rapid 7. These are instances that are purposely left unpatched for penetration testing. I was then able to gain remote access like I had planned.

Technical details

From a technical point of view for this experiment I need to use Metasploit, there are a few different ways I can go about this, I can download Metasploit directly to my Windows machine or I could install it as a virtual machine. I used the virtual machine method. I had already installed VMWare, so all that was needed was an iso image of Kali Linux and a Metasploitable Linux instance. Once the vm's were installed I needed to configure Kali. The first thing I done was to update the sources.list directory as Kali only came with one source. I done this through the Kali.org website found at https://docs.kali.org/general-use/kali-linux-sources-list-repositories . The next step was to update and upgrade, this is done through the terminal and once this was complete I was ready for penetration testing.

Experiments

The experiment I was most interested in was backdoors where a user can get remote access to a machine. The machine in question was the Metasploitable Linux machine that I spoke about in the technical details section of this report. I have was able to do this by following a tutorial found at https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guideuseus this gives a step by step guide on how this is achieved.

The exploit targets port 6667 which runs an IRC server. IRC is defined as an "Internet Chat Relay" this is an application layer protocol that allows users on the IRC network to communicate with each other through text (Mirc.com, 2018). This version had a backdoor that can be triggered by the letters AB, following by a system command (Metasploit.help.rapid7.com, 2018).

I am going to demonstrate to you the different ways of this exploit. The first demonstration will be done through the terminal in Kali and the second demonstration will be done via the Metasploit terminal. In Metasploit it takes just three commands to exploit the target, whereas in Kali this can take many commands. For testing purposes, I created a directory on the Desktop of the target called "this_is_cool " Please see figure 1 below. "Let me begin!!"

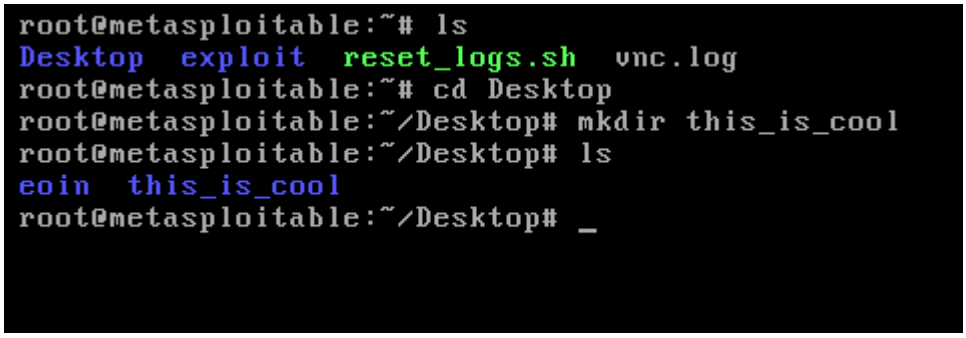

FIGURE 1: CREATING DIRECTORY ON TARGET DESKTOP

The first step was to set up my target machine, I just needed to login with the username and password as msfadmin. Using this command (rlogin -l root 192.168.99.131)please see figure 2 below, it allows you to check if you have rsh (remote shell) client running on the machine.

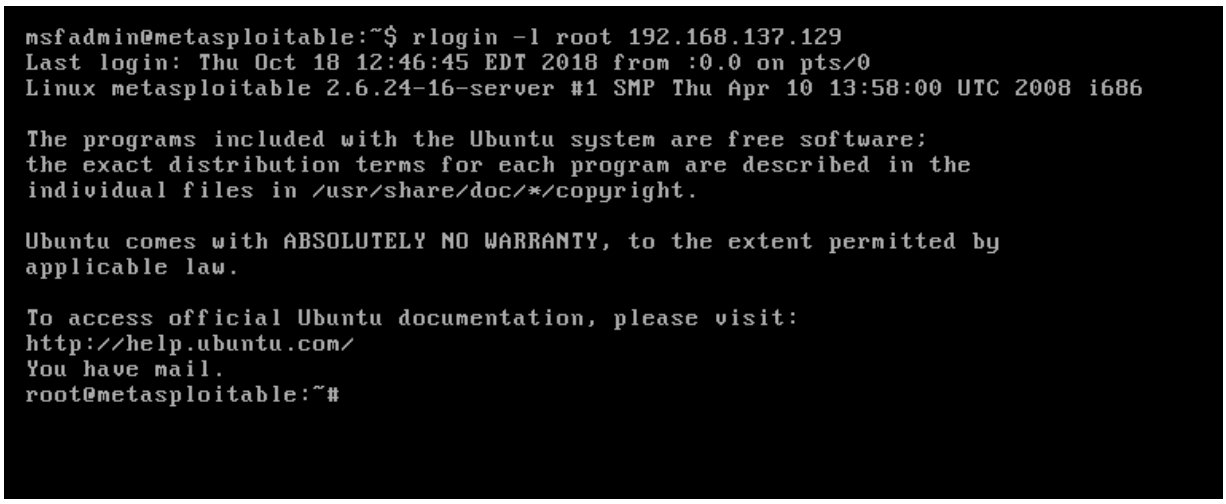

FIGURE 2: CHECK FOR REMOTE SHELL CONNECTION

I then switched to kali and If you see figure 3, I am checking all open ports on the target with (nmap -p0-65535 192.168.137.129) nmap is a tool that comes built into Kali and used for network scanning. The p in the command stands for port and its going to scan from port 0 to 65535 on the target IP address.

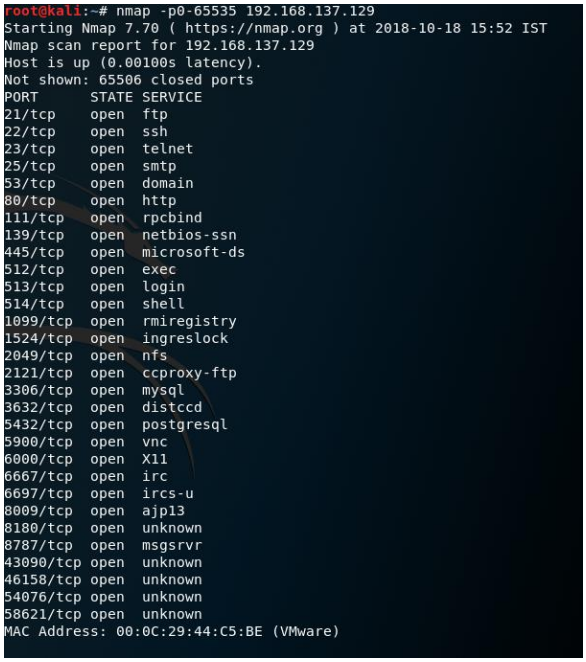

FIGURE 3: NMAP PORT SCAN

The next step was to check the available remote call to the target, and check the service's that is running, that is done with the following command: rpcinfo -p 192.168.99.131. The rpcinfo stands for remote call protocol and this is to all ports on the target. Please see figure 4. The aim of this is to target port 2049 which is a network file system andI will try to mount this to my Kali instance.

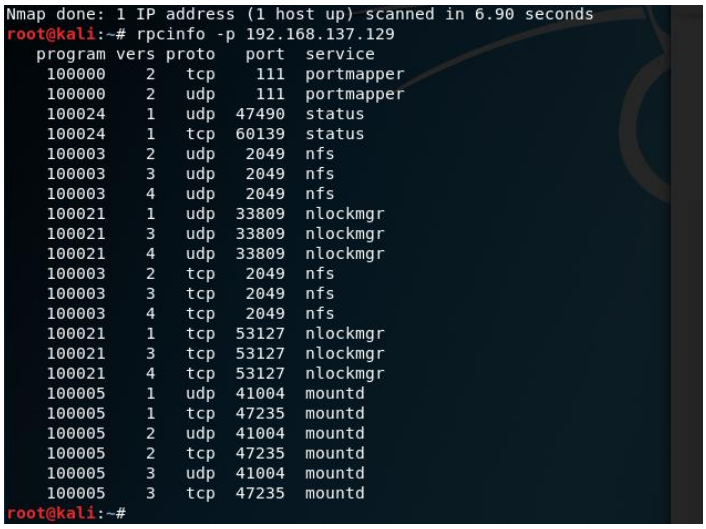

FIGURE 4: RPCINFO SCAN

The next step will involve creating public and private SSH RSA keys. Please see figure 5. This is done because we are trying to connect via SSH service.

```
root@kali:~# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:3+/PcrKfFj9atYUaS4Bj2GoalXCIFmiUa/m5mbMIT2Q root@kali
The key's randomart image is:
+---[RSA 2048]----+
|.ooo...          |
|.oo .o + .       |
|..o   + = .      |
| +   . o . .   . |
|. E o o S   o . o|
| o o +   . o + .+|
|. . =     . +  oo|
|.o.=         .+++|
| ...o        o*O=|
+----[SHA256]-----+
root@kali:~#
```

FIGURE 5: GENERATING RSA KEYS

If you see figure 6 I created a directory to mount the file system too. In the next command it says mount the nfs from the target to the directory I have just created. In the next command it is checking to see if I have a public key on my keyring called authorized_keys directory. If it finds the key it is successful and I can use SSH, if not it will prompt me for a key. As I have already created the key it will allow the SSH connection. This is so the keys can be verified and once that is done the file system is unmounted. After that I connect via ssh.

```
root@kali:~# mkdir /tmp/r00t
root@kali:~# mount -t nfs 192.168.137.129:/ /tmp/r00t/
root@kali:~# cat ~/.ssh/id_rsa.pub >> /tmp/r00t/root/.ssh/authorized_keys
root@kali:~# umount /tmp/r00t
root@kali:~# ssh root@192.168.137.129
Last login: Thu Oct 18 15:22:54 2018 from 192.168.137.129
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

FIGURE 6: MOUNT NFS

Now I have remote access to the target machine and I do an “ls” command where I can see all the directories. I can change directories to the desktop and can see the directory I created on the target machine called “this_is_cool”. Please see figure 7.

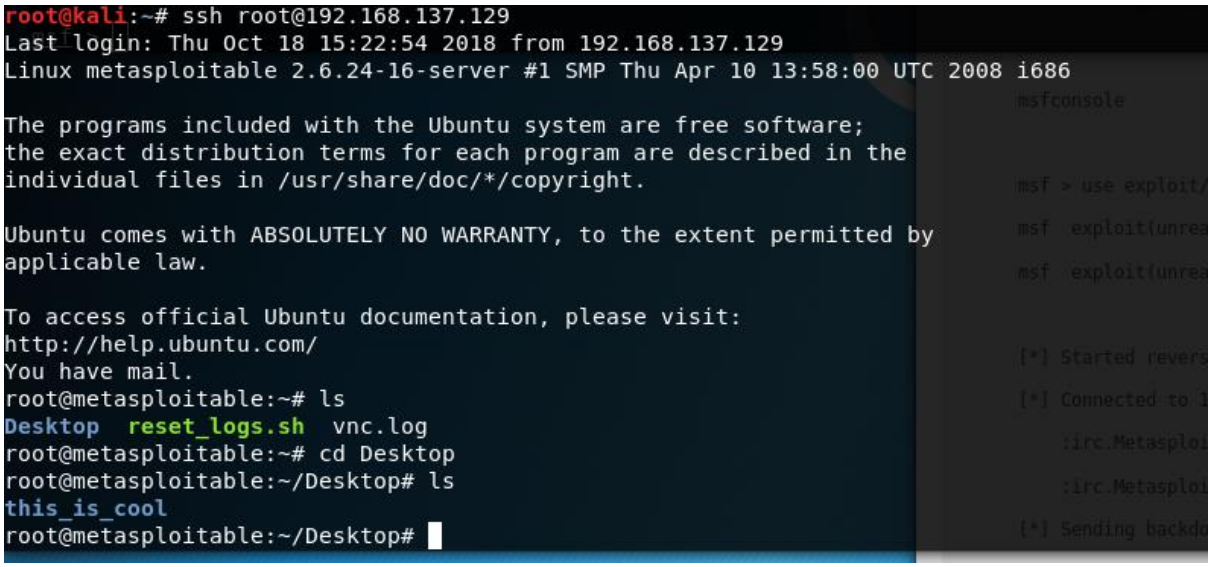

FIGURE 7: SHOWING DIRECTORY CREATED ON TARGET

I went to Metasploit for the next part of the experiment. The next part was more simple, in that it only had three commands. Please see figure 8.

The first command below selects the module in Metasploit that I was going to use for the exploit :

“exploit/unix/irc/unreal_ircd_3281backdoor”.

You can use the show options command to see what needs to be configured. I then set the remote host to 192.168.137.129.

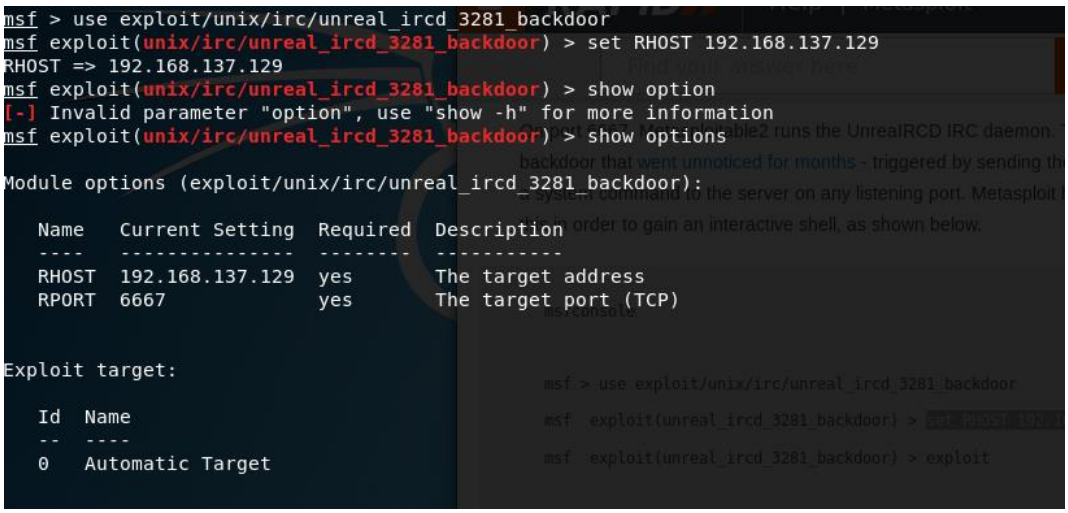

FIGURE 8: USING METASPLOIT TO GAIN ACCESS

The last command is to exploit the machine. Please see figure 9. As you can see below that the target has been accessed.

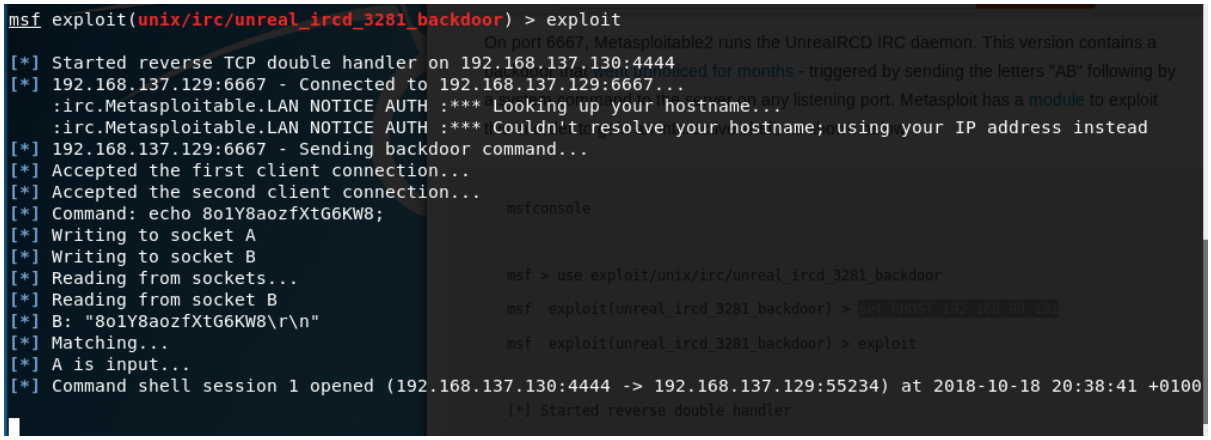

FIGURE 9: ACCESS GAINED ON TARGET

In figure 10 I am using the “ls” command to list all the directories on the target.

FIGURE 10: LIST DIRECTORIES

Finally, in figure 11 I am showing you the directory that was created on the desktop.

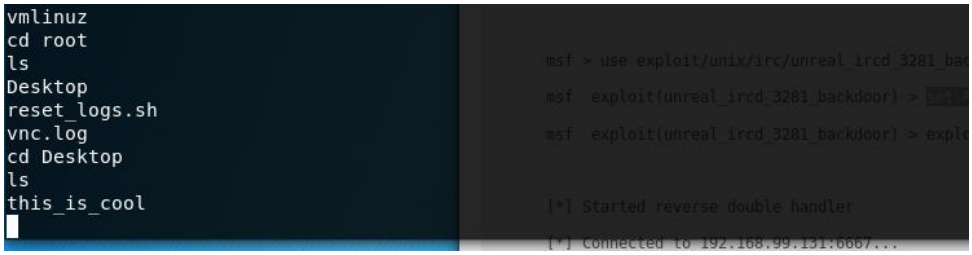

FIGURE 11: SHOWING THE DIRECTORY THROUGH METASPLOIT

Conclusions

I found this exercise to be both frustrating and interesting at the same time if that is possible. My problem is that I have had no bash scripting module throughout this course and that always stands to you when using any form of Linux. I spent many hours trying to gain access to a Windows XP laptop but to no avail. The problem is time and not having enough of it. In essence you could do a whole module on this tool as there is a lot to learn. For example, how to use each module and all the commands that are needed. One thing I would say is that it can cut the amount of work pen testers need to do in half, as doing it through the terminal on Kali has so much extra code involved. This repot gave me a good introduction to Metasploit. After I finish this course I will hope to spend a lot more time getting to know Metasploit and carrying out more penetration testing.

References

"BussinessWire (2009)". Rapid7 Acquires Metasploit. Businesswire.com. Available at: https://www.businesswire.com/news/home/20091021005675/en/Rapid7-Acquires-Metasploit [Accessed 11 Oct. 2018].

"Marquez, C (n.d.). An Analysis of the IDS Penetration Tool: Metasploit". [ebook] Available at: https://infosecwriters.com/text_resources/pdf/jmarquez_Metasploit.pdf [Accessed 11 Oct. 2018].

"Rapid7.com (2018) | Rapid 7". Available at: https://www.rapid7.com/db/modules/exploit/windows/dcerpc/ms03_026_dcom. [Accessed Web. 12 Oct. 2018].

"Mirc.com. (2018). mIRC: IRC Networks and Servers". [online] Mirc.com. Available at: https://www.mirc.com/servers.html [Accessed 18 Oct. 2018].

"Metasploit.help.rapid7.com. (2018)". Metasploitable 2 Exploitability Guide. [online] Available at: https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide [Accessed 18 Oct. 2018].

"Metasploit: Pen Testing Tool Features | Rapid7." (2018), Rapid7. Available at: https://www.rapid7.com/products/metasploit/features/ .[Accessed Web. 12 Oct. 2018.

"Offensive-security.com (2018)". Available at: https://www.offensive-security.com/metasploit-unleashed/msf-community-edition/ .[Accessed Web. 12 Oct. 2018].

"Offensive Security, 2018", Available at: https://www.offensive-security.com/metasploit-unleashed/payloads/. [Accessed Web. 12 Oct. 2018].

"What Is Metasploit? - Infosec Addicts | Cyber Security.", (2018), InfoSec Addicts. Available at: https://infosecaddicts.com/whats-metasploit/. [Accessed Web. 12 Oct. 2018].

Wonderhowto.com (2018) | Wonder How To Available at: https://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-and-gain-remote-access-pcs-running-windows-xp-0134709/. [Accessed Web. 12 Oct. 2018].