



### Rules of engagement:

--Scan local lab system created for this class.

-- Documentation is expected for each task, With screenshot and explanation of why and the how.

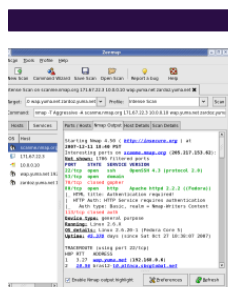
### Lab Setup:

Virtual Machine 1: Kali Linux

Virtual Machine 2: Metasploitable

Following tasks need to be completed using the Nmap tool. The lab has been designed to use the Nmap tools for the most fundamental test to attacking a vulnerable machine

For one of the tasks you would need to make use of the Zenmap tool (Nmap GUI). Currently Zenmap is only available on Windows and is a bit unstable with the Kali version. You can install the Windows version from <https://nmap.org/download.html>. You will be redirected to the download page. You need to select the download Nmap page, the screenshot will look like below:



Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. You can choose from a self-installer (includes dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

**Note:** The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install the [latest Npcap release](#).

The Nmap executable Windows installer can handle Npcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

**Latest stable release self-installer:** [nmap-7.91-setup.exe](#)  
**Latest Npcap release self-installer:** [npcapi-1.31.exe](#)

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

For those who prefer the command-line zip files ([Installation Instructions](#); [Usage Instructions](#)), they are still available. The Zenmap graphical interface is *not* included with these, so you need to run nmap.exe from a DOS/command window. Or you can download and install a superior command shell such as those included with the free [Cygwin system](#). Also, you need to run the Npcap and Microsoft Visual C++ 2013 Redistributable Package installers which are included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

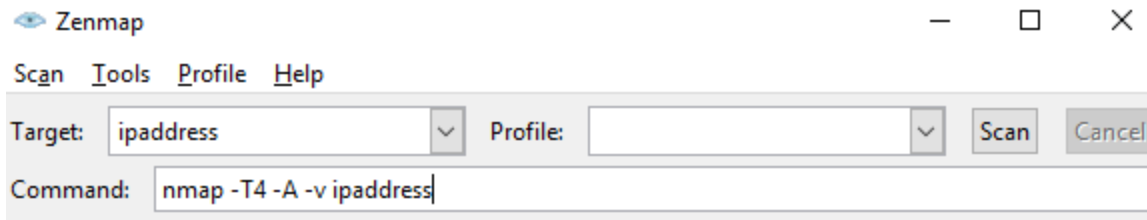
Latest [stable](#) command-line zipfile: [nmap-7.91-win32.zip](#)

### Task 1: Boot up all lab System

Using *nmap*, do a ping scan (`nmap -sP`) for the IP address in the local environment within the virtualbox machine. Also perform a port scan with `scanme.nmap.org`. Explain your finding about IP and ports.

**Task 2:** Use Zenmap from the instructions given above and perform different types of scan - Intense scan, Quick scan, regular scan and one more scan of your choice. Discuss the findings along with the similarities and differences between each scan

Refer to this image for starting scans:



**Task 3 :** Download metasploitable 2 from [Metasploitable - Browse /Metasploitable2 at SourceForge.net](#) (If already not done) and install it in the virtual machine. Instructions to install Metasploitable 2 is available here:

<https://www.wikigain.com/download-install-metasploitable-in-virtualbox/>

Make sure you don't expose this VM to the internet, Use host only network.

**Task 4 :** Start the Kali server and the metasploitable 2 server. Determine the IP address of the vulnerable machine and perform port scans and determine all ports open.

Nmap is already installed in kali , you will have to figure out the commands you need to find open vulnerable ports .

**Task 5: Create data file . --- First login to Metasploitable 2 from VM console ,**

**--- Create a text file using below command.**

**--- #echo hello hacker > /home/msfadmin/secret.txt**

**--- Check if file is there by command # cat /home/msfadmin/secret.txt**

**--- If you aware about linux command , feel free to make more text file. If not just secret.txt will do.**

Metasploitable 2 has multiple vulnerability you can exploit, You have full freedom to choice any. Pick any one vulnerable ports and Attack it.

Use Metasploit framework (MSF) from msfconsole to exploit the vulnerable service.

The task is complete once you have shell access of Metasploitable and are able read the **secret.txt**

--- Document your actions, commands and process you followed

**Task 6:** Explained two or three points as per your understanding with the concepts listed below.

**A.** Ping used in task 1 and 2.

**B.** Network ports

**C.** Vulnerable service

**D.** What is one step that can be taken in order defend against attack preformed in step 5

**Task 7: Perform a tcpdump on your machine and describe your findings.**