

Lab 07: Detection of vulnerabilities

First and last name:

Index number:

Used Lab equipment:

Group members:

Sending reports

Save the final document using Microsoft Print to PDF or a similar program. Finally, the completed report named index number should be uploaded to the eKursy (eCourses) platform in the appropriate section. For exercises carried out in groups, each person must send a report individually.

Introduction

According to NIST definition vulnerability is: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source". From the point of view of IT system security, early detection and elimination of known vulnerabilities is extremely important. Therefore, periodic tests are performed to detect new vulnerabilities in IT systems.

To complete the exercise you will need:

- PC with virtual environment;
- Kali Linux virtual machine;
- Tested virtual machine (Metasploitable 3).

Configure the virtual network in VirtualBox according to the diagram shown in Figure ???. When configuring the network settings, use the NAT Network option (the network will be hidden behind the NAT mechanism, but there will be access to the Internet).

Lab scenario

1 Start a test environment

Run all virtual machines. Login to Kali Linux machine (Kali Linux login: kali, password: kali) and check if communication is possible between the virtual machines. Note IP addresses are assigned to each. What tools did you use?

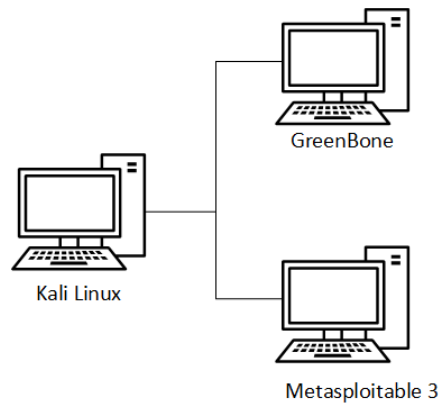


Figure 1: Diagram of virtual lab

2 Manual detection of vulnerabilities

Scan the test machine with nmap. Which ports were detected as open? How to check the software versions of the servers? Which nmap option did you use?

Search for vulnerabilities of detected software running on a test VM? How can these vulnerabilities be exploited? Write down the web addresses where you can find information about the vulnerabilities and a description of one vulnerability found

3 Detection of vulnerabilities with nmap

Search the directory where nmap scripts for vulnerability detection are located. How many scripts can you currently use? Write down the name of one script and explain what it can be used for.

Scan the test machine using the default set of scripts (`nmap -sC IP_target`). What vulnerabilities were detected. Write them down with a brief description.

First and last name:

How many scripts belong to this group (`nmap --script-help vuln`)? Scan test machine using "vuln" set of scripts and describe results.

Select one script from the "vuln" group and run it. Describe the script and the information you

obtained with it.

4 Additional scripts for nmap

According to information presented on following websides, instal and test two additional skripts:

- nmap-vulners: <https://github.com/vulnersCom/nmap-vulners>,
- vulscan: <https://github.com/scipag/vulscan>.

Describe the function of the scripts and your observations.

First and last name:

5 GreenBone

Greenbone is an automated vulnerability search tool. The tool is available for systems in the Linux family. You can install it yourself or use a virtual machine provided by the manufacturer. In its basic version, the tool is free of charge.

A virtual machine from GreenBone will be used during the exercises. To use this tool you need to:

- Login to the system (login: admin, password: admin) - see Fig 2:

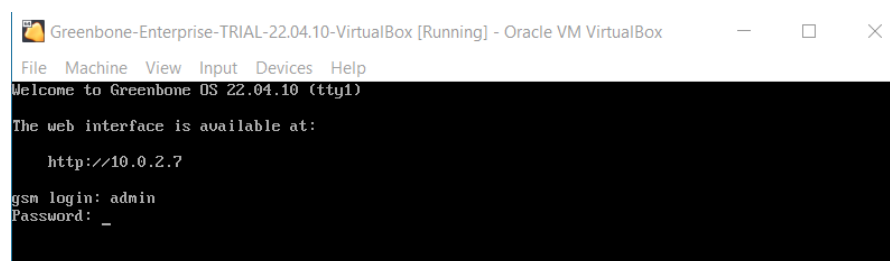


Figure 2: Login to the GreenBone VM

- Create a user for the vulnerability detection tool:
When you log in for the first time, you will see a message that the GreenBone tool is not fully configured (figure 2). Click Yes to continue.

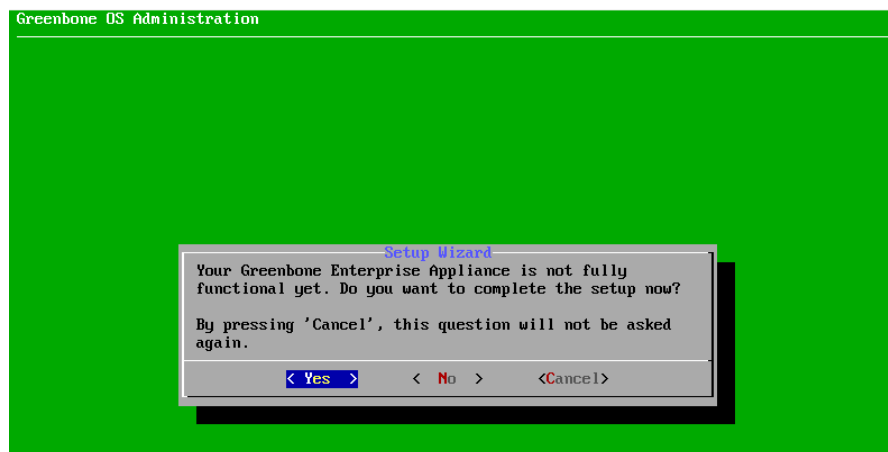


Figure 3: Greenbone Setup Wizard

And again click Yes:



Figure 4: Create Web Admin message

You can now create a new account for the administrator:

Once the tool administrator has been created, the tool will be launched. After waiting for a while, launch a browser on your Kali Linux machine and enter the IP address of the GreenBone machine in the address bar. Once logged in, the tool is ready to use. Define a new test target (IP address of the test machine) - menu Configuration. To run a scan from the Scans menu select the new scan, enter the previously defined scan as the target. Details can be found on the tool's website: <https://www.greenbone.net/>.

Learn how to create new scanning targets and how to perform the scanning process itself. Scan the test machine and describe what information was obtained.

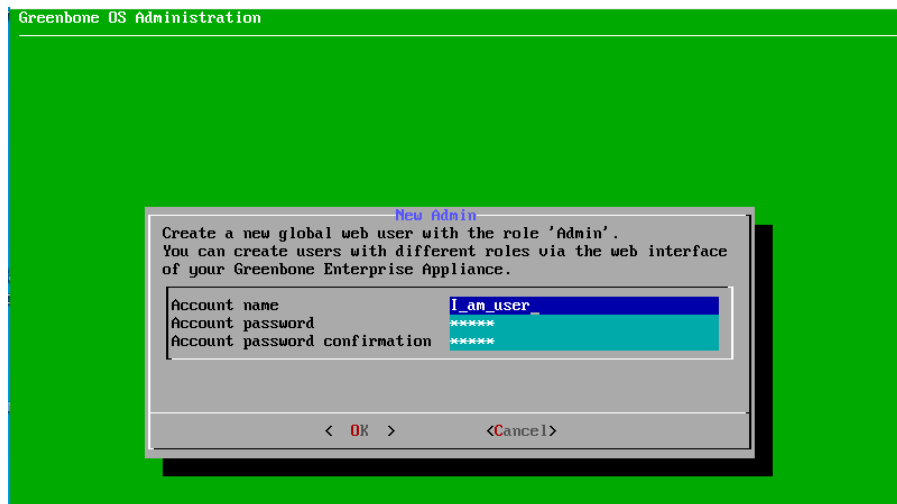


Figure 5: New Admin window

First and last name:

First and last name:

First and last name:
