Lab 3: General Assessment

In this lab you will perform steps of an assessment:

- Gather Information: e.g., about a company, range of IP addresses, etc.
- Scan IP addresses: e.g., what services are running on the associated IP addresses
- Fingerprinting: e.g., what web servers, accounts, etc.
- Reporting: summarise the gathered intel

Of course, we will not wildly target a real entity, but perform the critical steps on our metasploitable VMs.

As this lab builds the foundations for future labs, please create a document from your notes on each point. That way, you can go back to your findings and do not have to redo every scan every week. Also, this will create the most suitable documentation for you on how to use the different tools for future reference. At the end of the course, you will hand in the document as a "lab report", which is the second of the exam-qualifying assignments.

To this end, please note that all questions (or paragraphs) marked with † should be answered in the report which you submit as assignment 2. You are free to include additional notes to help you retrace your steps later.

Imporant: In case of trouble, please make sure you read the whole document. Then, consider using the internet, discord, TA's, and/or teacher to solve the issue. Ideally in that order. :-)

Preconditions: Installed VMs

This assessment is targeting the metasploitable VMs. If you do not have enough disk space to set them all up, please check if you can find a partner with which you can share the disk load. Otherwise, you can wait with the Windows part until the Windows VM comes into the focus of the lecture.

Finding information with whois

1. Try to gather information on SDU with whois.
2. Try whois on the \emph{IP address} of www.sdu.dk .
3. †What do you learn about SDU's network? In the protocol, note the IP range.
4. Are there other Networking-Services @SDU which you could try?
5. †What is the whois information for nextcloud.sdu.dk ? What do you observe in comparison to the whois-information you gathered for www.sdu.dk.
6. Important: You can also perform whois on domains, for example sdu.dk, but -- depending on the implementation -- only on the registered domain,

not any hosts in it. But you can use whois on the IP addresses associated to the hosts.

Question: nmap

Nmap scans can be set up to evade firewalls. Which tags would you use for:

- †Send packets with specified ip options
- †Spoof your MAC address

Scanning the Metasploitable VMs

Use Nmap, to scan and find out information about Metasploitable-3, both Windows and Ubuntu. In your use of Nmap compare your SYN scan vs the Connect scan vs the scan with the tag that enables OS detection, version detection, script scanning. Take notes of the results for all three and discuss differences and pros and cons based on your observation.

Scanning with Legion

Use Legion to assess the vulnerabilities in Metasploitable-3 (both Windows and Ubuntu). Legion should come pre-installed in Kali.

Scanning with Nessus

Use Nessus to assess the vulnerabilities in Metasploitable-3 (both Windows and Ubuntu). Please follow the instructions from the Installing Nessus section below. GVM is a fork of Nessus, after the latter became closed source.

Scanning with the Greenbone Vulnerability Manager (gvm)

Use GVM to assess the vulnerabilities in Metasploitable-3 (both Windows and Ubuntu). Please follow the instructions from the Installing & Setting up GVM section below.

Trouble Shooting

- In case you get the UI but no scan options are available, please wait for the system to be fully initialised. Check the Greenbone Trouble-Shooting section below for more information.

- If you are using the Kali image with pre-installed GVM, note the username/password for the Web UI in the setup descriptions.
- In case of trouble with GVM, i.e., you are running out of disk space, things just not working, contact us. From a course perspective, it is more important that you complete Legion and Nessus, but for practical reasons, having the freely available working GVM is more valuable.

Comparing the Tools

†Compare your results from each of the previous activities in each question (e.g., sparta vs nessus vs openvas). Take notes & discuss overlaps and differences in results, pros and cons, ease of use for each tool.

---

†Collecting the Assessment Information

Find possible vulnerabilities with metasploitable3 (both Windows and Ubuntu). State tools and resources used and then select 4 vulnerable services for each of the metasploitable VMs for which you document:

1. †Service, port number and version number, e.g., FTP 21 vxxxx
2. †Describe or explain at least one vulnerability that you found for that service, i.e., what is the underlying issue and what can be achieved? How severe is that issue? (You do not have to state how to exploit the vulnerability or go into technical details. We will look into this later btw. the intricate technicalities are mostly outside the scope of the course.) But make sure you describe what possible outcomes of the exploit are, what the impact for a real system were and how criticial you would assess the issue due to the effects, i.e., argue for your assessment.
3. †For each of the vulnerabilities in the previous point, note the CVE and/or Source of information about the vulnerability for that version. Using metasploit's info command might help you here, if you want to go to the command line.

A full assessment would need to include all services, all relevant vulnerabilities, and exploits.

---

†Completing the Assessment

†Create a final report, extending the collected information with an overall review of the security concerns in both the Metasploitable-3 Windows and Ubuntu systems, e.g., different criticality levels of the services (an overview of how bad the situation is) and which ones to to be prioritized when addressing security

issues (a selection of the most relevant issues for prioritisation). For this use a combination of the results from the tools that you used or one of the tools.

Installing & Setting up GVM

To install gvm, use:

```
apt install gvm gvm-tools greenbone-security-assistant nsis
```

Note, that this package is sensitive against data base updates. In case of trouble, it might be easiest to apt purge and reinstall.

To set up GVM, then

```
gvm-setup           # The first time
```

and check the setup is complete with

```
gvm-check-setup     # Until it works
```

i.e., you might need to create users, dbs, etc. pp., follow the guides if necessary

```
gvm-start           # To then get the webservice running
```

Note, whenever one of the script throws errors, it is due to missing quotation marks---great for a security product, yes---so, please fire up your favourite editor and put the (potentially empty variables) into quotation marks like this:

```
if [ $postgres_version = "" ]; then
```

becomes

```
if [ "$postgres_version" = "" ]; then
```

Finally, the web interface is available at 127.0.0.1:9392 .

To change the admin user's password, for example because you didn't write it down above, use

```
sudo runuser -u _gvm -- gvmd --user=admin --new-password=XYZ
```

To create the admin user

```
sudo runuser -u _gvm - gvmd --create-user=admin --new-password=XYZ
```

Also, on one machine, I had to adjust the data base port in /etc/postgresql/13/main/postgresql.conf from 5433 to 5432 to work.

Greenbone Trouble-Shooting

"Failed to find config "": this error occurs when GVM is still syncing / scanning its databases. Please come back later and check if meta data update is complete. (You can also check in the admin section.) Unfortunately, GVMs

error message is not helping you to locate the underlying issue nor does it display a busy indicator.

Installing Nessus

Instructions for installing Nessus and example for how to use it are below:

1. Visit the Nessus homepage.
2. Notice "Register for an Activation Code". Complete the Registration in order to get an Activation Code. (Do not use a fake email address because an activation code will be sent to the email. You will need it later.)
3. On the Downloads page, download "Nessus-8.15.2-debian6_amd64.deb", assuming a 64bit Kali.
4. Open a Linux terminal and navigate to where the downloaded file is.
5. Enter dpkg -i followed by the name of the dowloaded file. Press enter to begin the install process. (you can also enter the first character of the files name and then hit TAB. The full name should appear on your terminal). Installation may take a while as Nessus processes various plugins.
6. If all goes well and all plugins have been installed. You. should see the following and the end of the installation:
   - You can start nessusd by typing systemctl start nessusd.service
   - Then go to https://kali:8834/ to configure your scanner
7. To start Nessus enter the following:

   ```
   systemctl start nessusd.service
   ```

8. In your browser in Kali go to: https://kali:8834/
9. You will get a message that the "Connection is untrusted" or something similar. Click on "I Understand the Risks" and click "Add Exception", and then "Confirm Security Exception", or similar, depends on Browser and version. Make sure you do understand the risks. ;-)
10. On the web page, select "Nessus Essentials" and continue through the process.
11. Nessus will start downloading additional plugins and initialize. So wait. If it does not happen automatically then choose an option to download plugins.
12. Its ready for use :)

Example of use: on the top right corner locate "New Scan" and click on it. For a for a basic but full scan click on "Basic Network Scan". A form will show up. Give your scan any "Name". In the "Target" field is where you need to enter

the IP address of your target VM. When done, click on "Save". You scan will be listed in the next page. On the left-most column, locate a play-like button. Click on it to launch your scan. Now wait for your scan to complete.