**Linux & Python Project No.1 SDA Academy**

Title: Report for the SDA.vm and the automation process of enumeration and password cracking with Python.

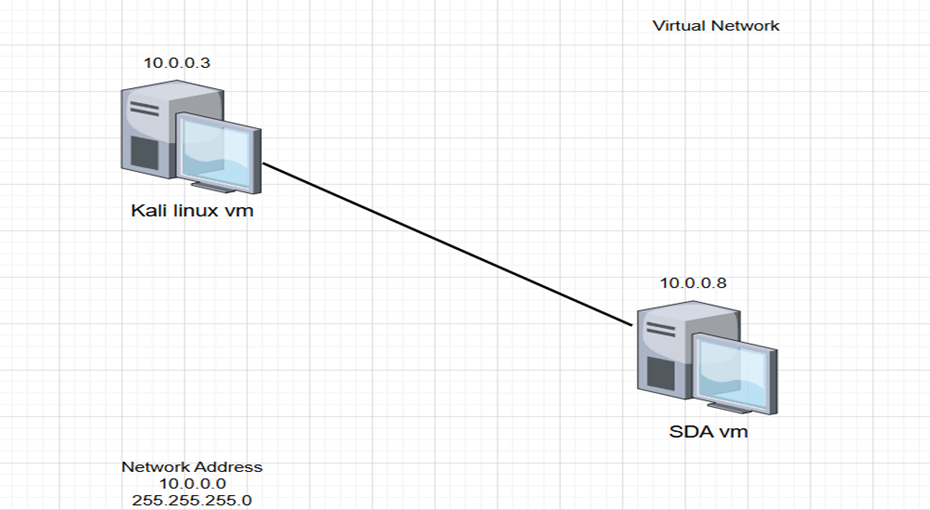
Group members:

Klevis

Arbri

Argjent

**Topology of the Lab**

****

We are going to work with different hypervisor platforms to “hack” the

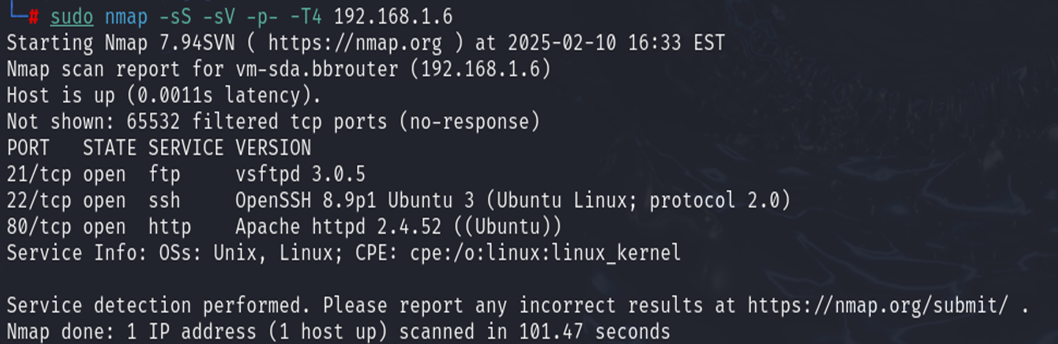
SDA.vm manually first and then automate it.

**Recon & Enumeration Phase**

* **Nmap** Scan (Checking for open ports and service versions)

Command:

**sudo nmap** -sS -sV -p- -T4 192.168.1.6



We have 3 open ports. The last one port 80 (Apache) or Web application is perfect way. It may have misconfigurations or some other kind of webapp vulnerabilities.

Also we are going to give the below command to see if there are any frameworks.

**whatweb** 192.168.1.6



After that I gave the **curl** command to view the page source code for comments or functions.

**curl** 192.168.1.6

A computer screen shot

AI-generated content may be incorrect.

We found a base 64 encoded. The best way is to decode it with online site such as <https://www.base64decode.org/>

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Message gives us details on how to enumerate the webapp.

A screenshot of a computer

AI-generated content may be incorrect.

We proceeded to download the list and used **gobuster** to look for directories.

* **GoBuster brute-forcing Directories**

**gobuster** dir -u http://192.168.1.6 -w directory-list-lowercase-2.3-medium.txt

A screenshot of a computer

AI-generated content may be incorrect.

For us the most interesting directory was **/requests**.

A screenshot of a computer

AI-generated content may be incorrect.

**urgent.txt**

A screenshot of a computer

AI-generated content may be incorrect.

The user has as username a planet name. We are going to make a list of planets using ChatGPT then put them on a list and use hydra to Brute-Force on the SSH service. Based on urgent.txt, we should use rockyou-10 passwords list.

A screenshot of a chat

AI-generated content may be incorrect.

* **Brute-Forcing SSH Logins using Hydra**

hydra -L planets.txt -P rockyou-10.txt ssh://192.168.1.6 -t 4

A screen shot of a computer

AI-generated content may be incorrect.

**Credentials**

uranus: butterfly

Now we’re going to login with SSH and see for possible privilege escalation ways to get into root.

We logged in on uranus user and found the first flag: **user.txt**

A screenshot of a computer

AI-generated content may be incorrect.

* **Flag**: flag{h4ck3r}
* **Privilege Escalation to root user**

Now that we are logged in we’re going to see what permissions as uranus user we have using **sudo -l** command.

A black screen with white text

AI-generated content may be incorrect.

We don’t have permissions to run sudo command with uranus. Now, let's try to see the last commands they’ve executed on the machine.

A screenshot of a computer

AI-generated content may be incorrect.

Accessing the **.bash\_history** file

A screenshot of a computer

AI-generated content may be incorrect.

We got another Base64 message, We are going to decode it and see what it says.

Decoding Base64 found from **.bash\_history**

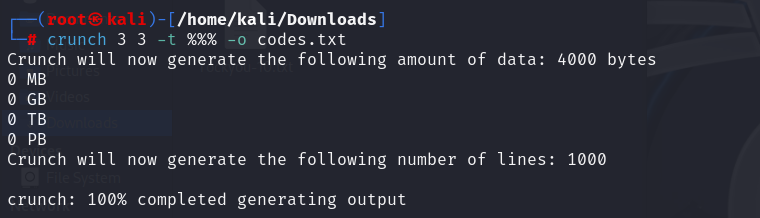
A screenshot of a computer

AI-generated content may be incorrect.

The root user has a 3-digit code. Crunch is a tool that generate a list of 3-digit codes from 000 to 999. We should use hydra tool to brute-force root user.

**Using crunch to generate 3-digit codes**

**crunch** 3 3 -t %%% -o codes.txt

****

Now we’re going to use hydra again to brute-force root user.

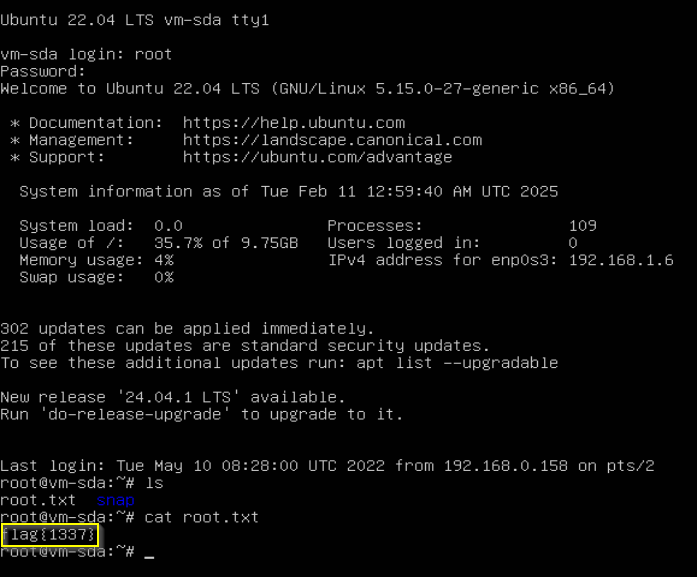
**hydra** -l root -P codes.txt ssh://192.168.1.6 -t 4

A screenshot of a computer program

AI-generated content may be incorrect.

root:666

Accessing root user with found credentials



* **Flag** flag{1337}

Another topic is the automation of tasks using Python3 and Scapy. The script will be uploaded on a GitHub repo..