**Walkthrough - Haiku Pro Range 101**

World of Hiku (Haiku pro) is a open world cloud based network game/puzzles in which players can practice skills on real world scenarios that could be used in real life scenarios therefore helping cybersecurity students and professionals to test and enhance their abilities on red, blue teams.

* **Hiku pro membership**
* **Kali Linux**
* **Brute forcing basics**
* **Nmap basic knowledge (port scanning)**

**Information on Machine, objectives and goals:**

**Name**: Range 101

**IP Adress**: 10.75.101.168

**Operative System**: Kali Linux

**Step 1**: Reconnaissance ( 1st Flag)

By using the nmap network scanning tool one can perform a scan on active ports and services from the target IP, in this case () to identify open ports, important to scan all possible ports with proper arguments (refer to man on nmap, MAN). Gathering as much information as possible from target IP.

**Command Results**: nmap 10.75.10199

**A computer screen shot of a computer screen

Description automatically generated**

**Port 80 – HTTP**

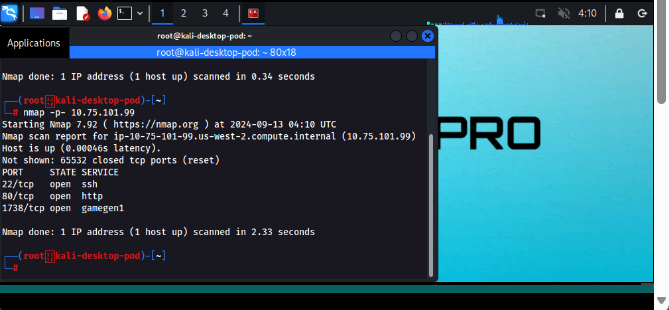
**Port 443 HTTPS**

**Port 1738 GameGen1**

Command: nmap -p- ()

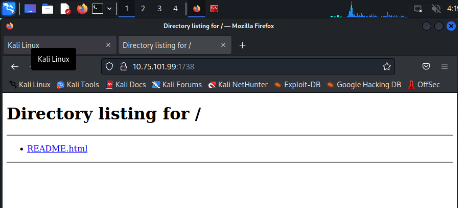
* Command scans all ports on the target IP.

Adding argument “-p-“ to a standard nmap () scan of while performing the scan will scan all possible ports, therefore discovering more services. Alternatively visiting the web page through the web browser is also a great way to obtain system and version information.

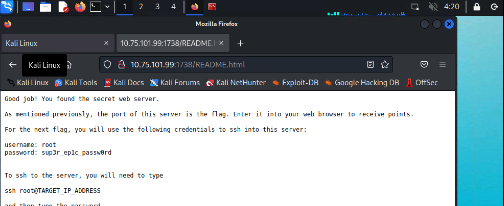
**Results: **

**Step 2: Exploit potential Vulnerabilities**

Visiting the additional port that was discovered either through curl or visiting the website on the port 1738 to examine any possible vulnerabilities or useful info to attempt to see any important information that could be useful.



Navigate to obtain details and possible sensitive information.



**Step 4- Attack**

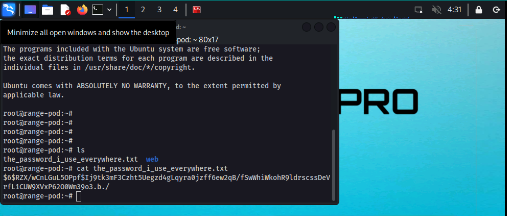
Since we found credentials to establish a remote connection, we can proceed to go ahead and examine the data accessible, looking for password file.

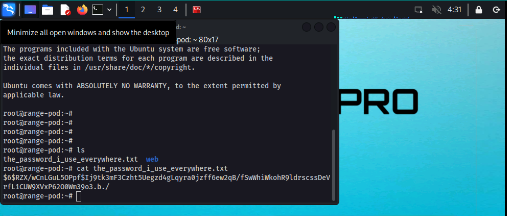
Running the **ls** command:

A screenshot of a computer

Description automatically generated

Run **Cat** command to see heading contents:



Step 5 - Password cracking: flag 2

Saving a file to later crack the encryption, in this case I saved it as “password.txt”.

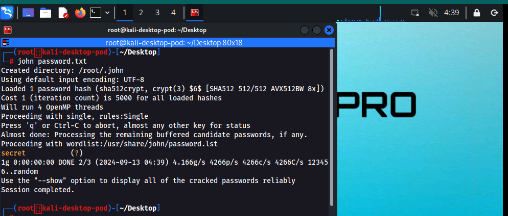


Left click > Open terminal here on the password.txt file

A screenshot of a computer

Description automatically generated

Running John the reaper (password cracking software) on the password.txt file.



Final step: Mission accomplished

The final flag is: secret

And that’s how the password was retrieved.

A screenshot of a video game

Description automatically generated

Here some overview of the completed task.

**Conclusion:** This webpage contained a lot on information vulnerable to be exploited therefore having unauthorized access to the network and performing a password cracking therefore obtaining credentials to have unauthorized access in the present or future**.**

**Ways to prevent this include**: Regular system and application updates,increase complexity on hash algorithm SHA-256, Implement a more robust security system, disable unnecessary services and or ports.