**Mr Robot Report**

Name:Saurabh Jawade

Date: 03/08/25

**Table of Contents**

|  |  |
| --- | --- |
|  [Executive Summary](#executive-summary) | 3 |
|  [Machine & Environment Details](#machine--environment-details) | 4 |
|  [Enumeration](#4-enumeration) | 4-5 |
| * [ARP Scan](#41-arp-scan) | 4 |
| * [Web Scanning (Nikto)](#42-web-scanning-nikto) | 5 |
|  [Credential Disclosure](#5-credential-disclosure) | 5-7 |
|  [Initial Access](#6-initial-access) | 8 |
|  [Post-Exploitation (User: daemon)](#7-post-exploitation-user-daemon) | 12 |
|  [Privilege Escalation to Robot](#8-privilege-escalation-to-robot) | 12 |
|  [Privilege Escalation to Root](#9-privilege-escalation-to-root) | 14 |
|  [Flags Summary](#10-flags-summary) | 14 |
|  [Conclusion](#11-conclusion) | 15 |

**Executive Summary**

The Mr. Robot machine was exploited through a series of web and system-level attacks. A leaked base64-encoded credential allowed login into WordPress, where a reverse shell was uploaded via the 404.php template. This gave low-level access as daemon. From there, an MD5 hash was found and cracked to access the robot user. Finally, a SUID-enabled nmap binary was used to escalate to root, allowing capture of all three flags.

**Summary of Results**

**Target IP**: 192.168.148.139

**Tools Used**: Nikto, nmap, Python reverse shell

**Credential Found**: elliot:ER28-0652 (from license.txt)

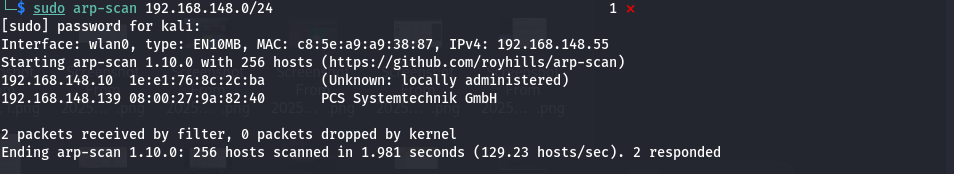
**Initial Access**: Reverse shell via WordPress 404.php

**Privilege Escalation 1**: Cracked MD5 hash → robot access

**Privilege Escalation 2**: Used nmap --interactive → root

**Flags Collected**:

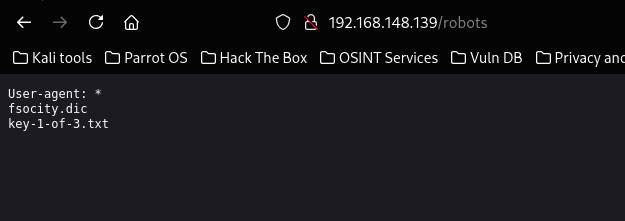
* Key 1: 073403c8a58a1f80d943455fb30724b9
* Key 2: 822c73956184f694993bede3eb39f959
* Key 3: 04787ddef27c3dee1ee161b21670b4e4
* **Target Information**
* **Machine Name**: Mr. Robot
* **Attacker OS**: Kali Linux
* **IP Address**: 192.168.148.139
* **Enumeration**
* **ARP Scan** : arp-scan is a command-line tool that uses the ARP protocol to discover and fingerprint IP hosts on the local network.
* **Discovered live host**: 192.168.148.139



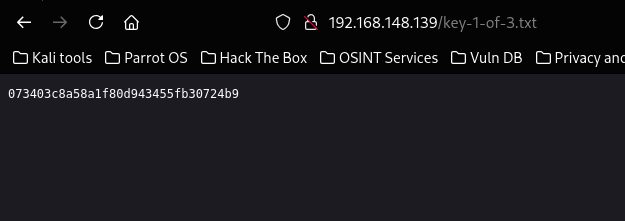
* **Nikto Scan :** Nikto is a free and open-source web server scanner used to identify potential security vulnerabilities and configuration issues in web servers.

****

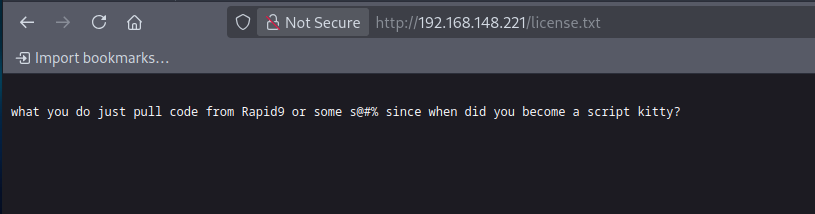
* **Credential Disclosure**
* Checked for robots
* http://192.168.148.139/robots

****

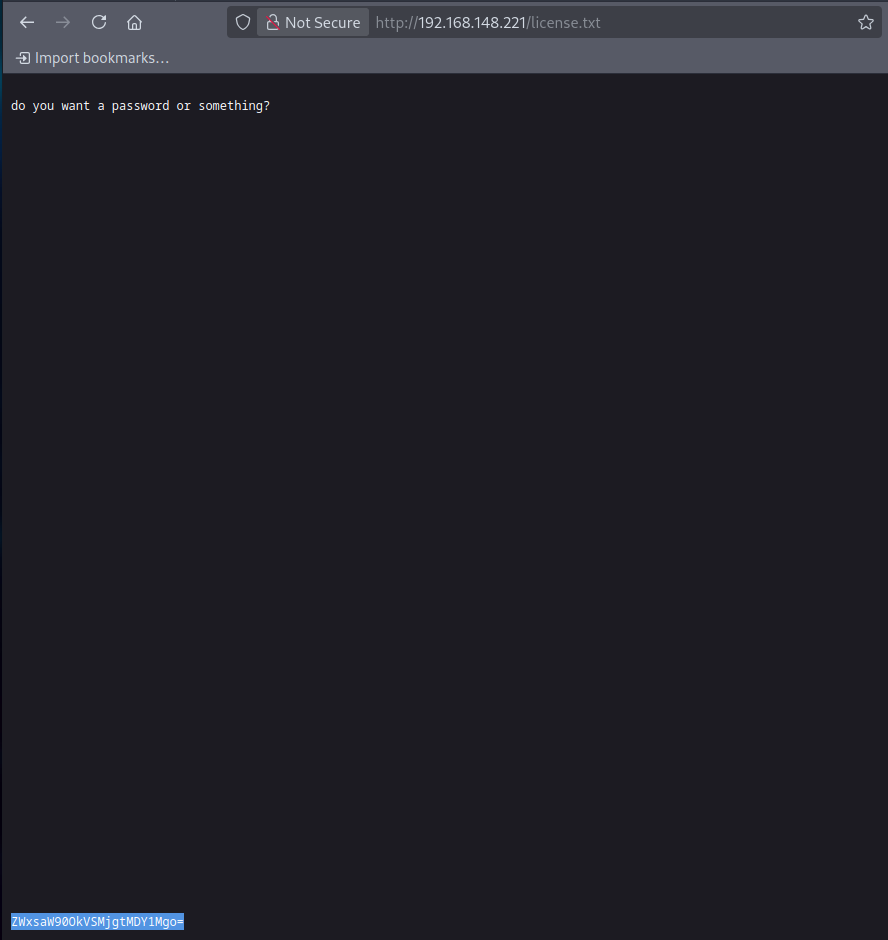
* Found : **key-1-of-3.txt**



* Also, we found in a publicly accessible license.txt file.
* <http://192.168.148.139/license.txt>



* Scroll down on that page

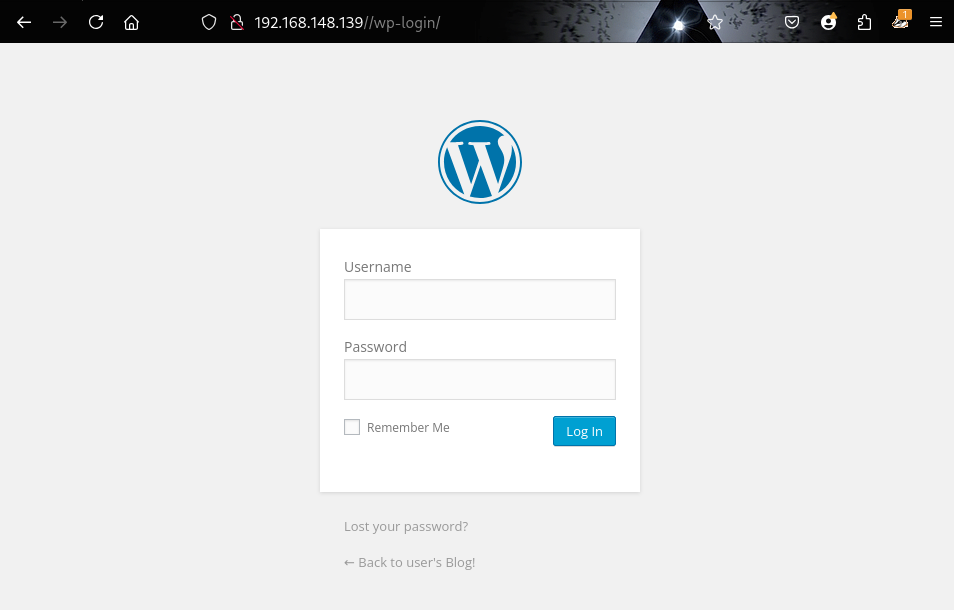


* **Base64 Decoded:**

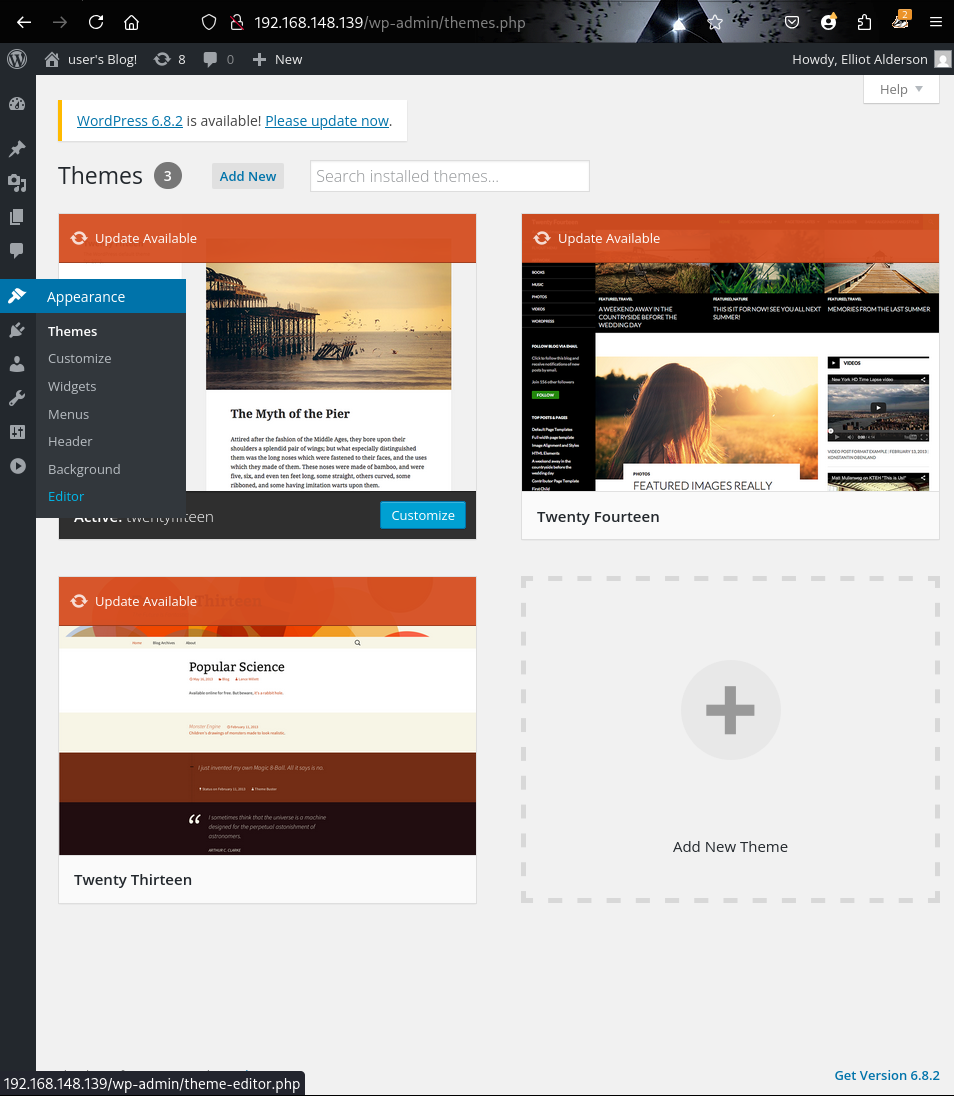
ZWxsaW90OkVSMjgtMDY1Mg== → **elliot:ER28-0652**

|  |  |
| --- | --- |
|  |  |

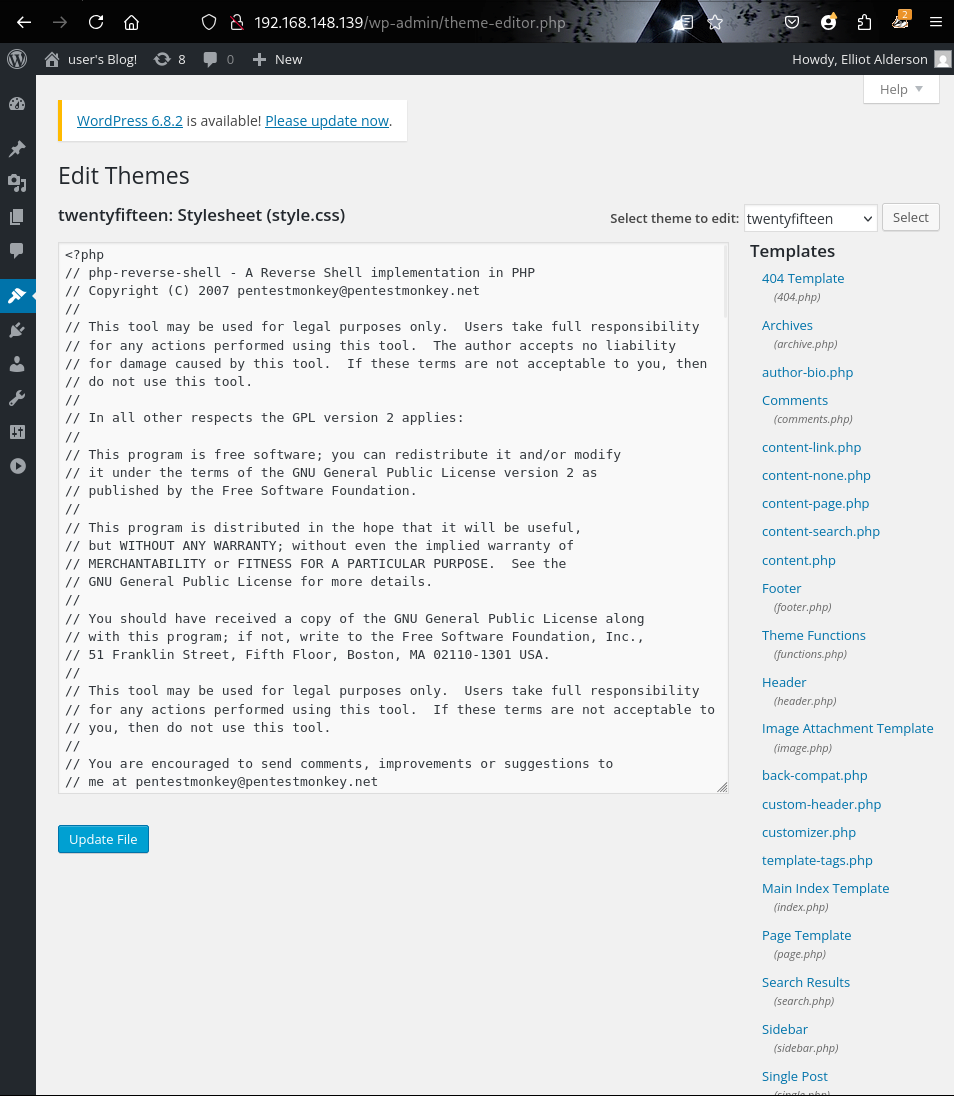
* **Initial Access**
* Using discovered credentials:
* Username: **elliot**
* Password: **ER28-0652**
* Login via WordPress panel



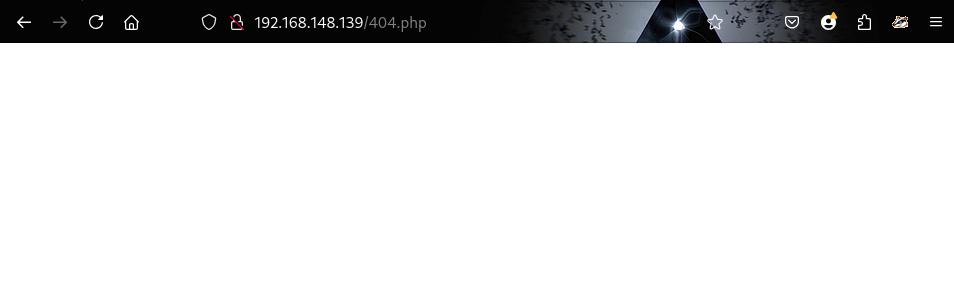
* So, check for any file uploads and webshells.
* Go to the Editor Page.

****

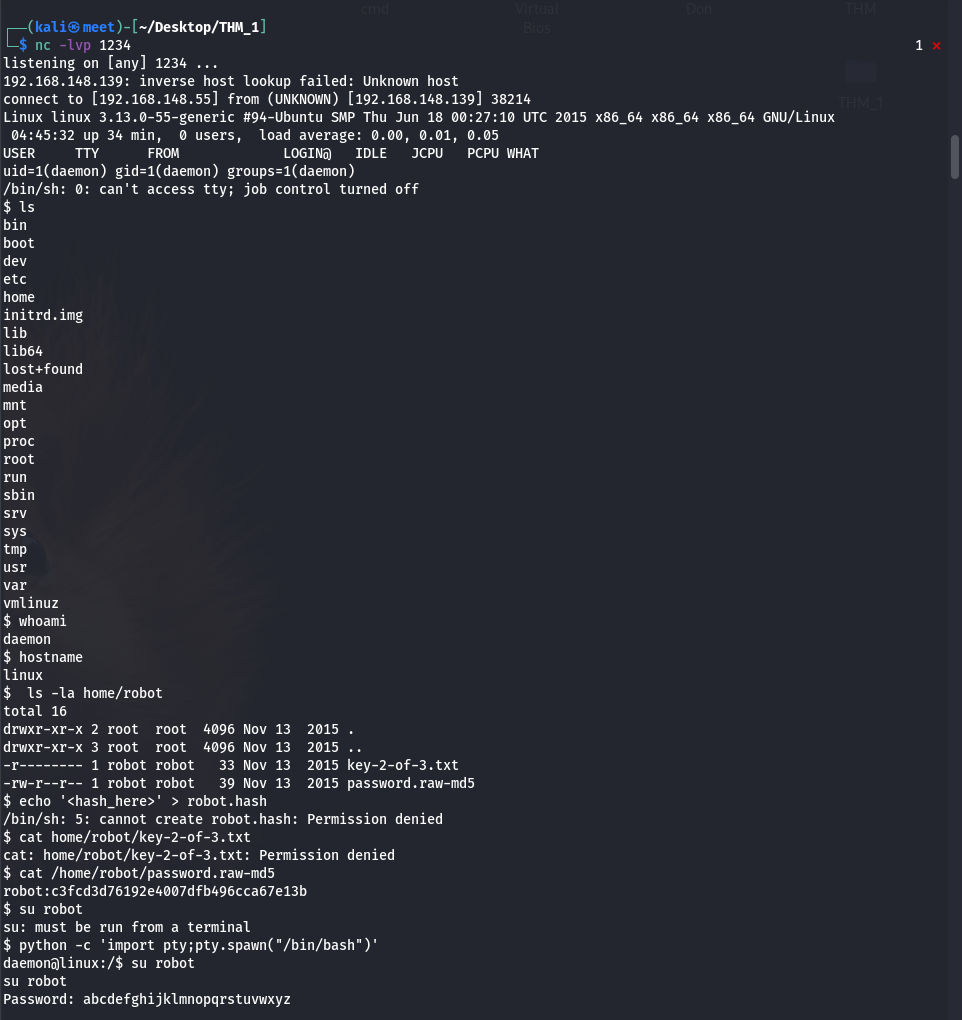
* We, see there is a 404 Template (404.php).
* So we can uplode a reverse shell php file and get shell access.

****

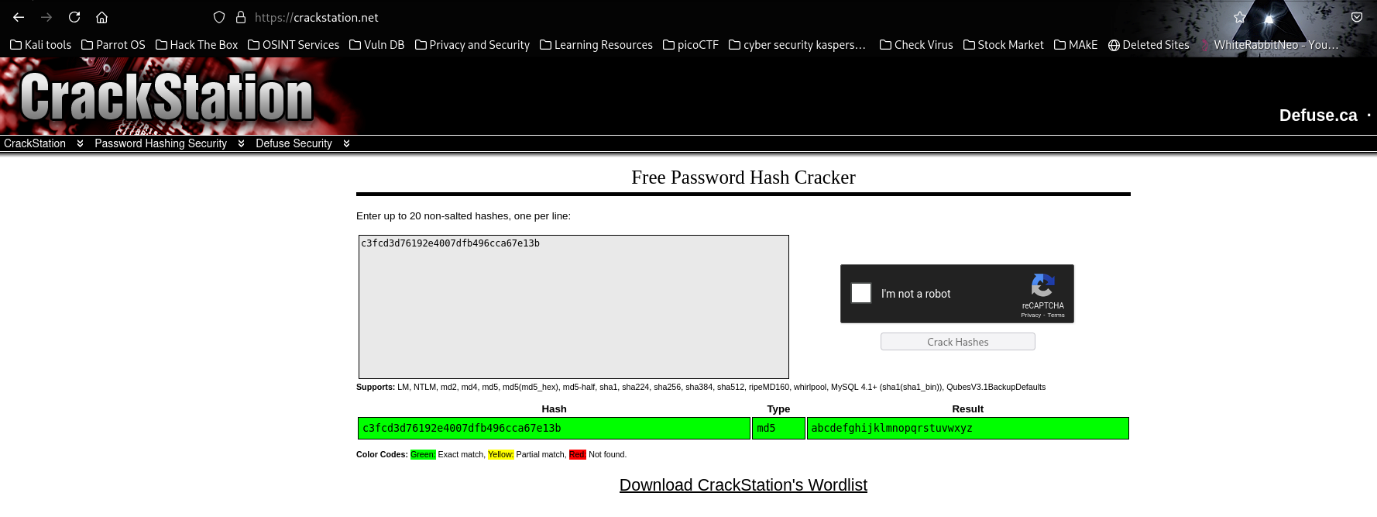
* Uploded a reverse shell file in the 404 Template.
* Run a non-existent page.
* <http://192.168.148.139/404.php>

****

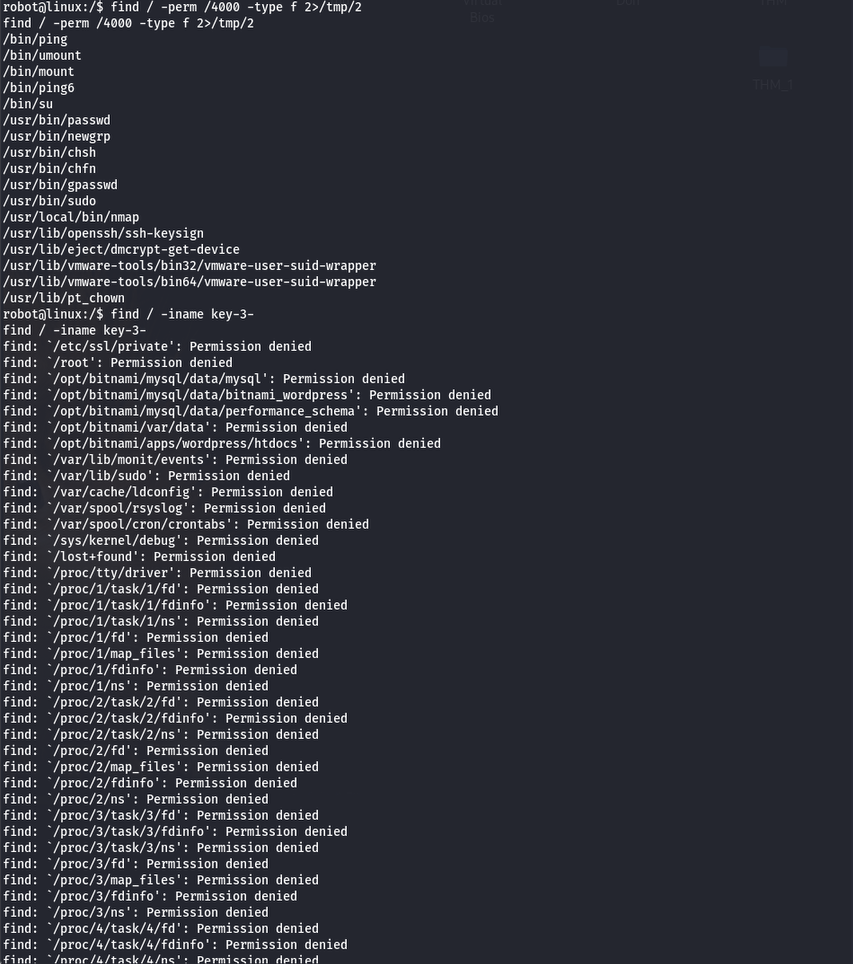
* We Received a successful callback on Kali using netcat.
* nc -lvp 1234

****

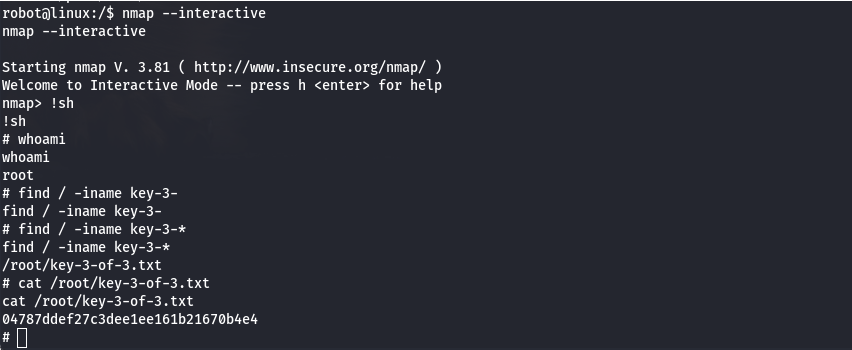
* **Privilege Escalation (of Robot User)**
* Checked hidden files of /home/robot/ and found key-2-of-3.txt and password.raw-md5
* cat: home/robot/key-2-of-3.txt: **Permission denied**
* Cat home/robot/password.raw-md5
* robot:c3fcd3d76192e4007dfb496cca67e13b
* It is an **MD5 hash. Using** online hash crackers
* <https://crackstation.net/>

****

* **Decrypted text :** abcdefghijklmnopqrstuvwxyz
* Get root of robot
* **$ python -c 'import pty;pty.spawn("/bin/bash")'**
* **daemon@linux:/$ su robot**
* **su robot**
* **Password: abcdefghijklmnopqrstuvwxyz**
* Now we cat the key-2-3.txt.
* robot@linux:/$ cat home/robot/key-2-of-3.txt
* cat home/robot/key-2-of-3.txt
* 822c73956184f694993bede3eb39f959
* Checked for binaries.
* find / -perm /4000 -type f 2>/tmp/2
* Now for 3th key, we know the key starting words key-3- so we can find this using find cmd.
* find / -iname key-3-
* **It** was denied the permission.

****

* But found /usr/local/bin/nmap
* Used interactive mode to gain root:

****

* Became root and read final key: **04787ddef27c3dee1ee161b21670b4e4**
* **All Flags**

1. **key-1-of-3.txt : 073403c8a58a1f80d943455fb30724b9**
2. **key-2-of-3.txt : 822c73956184f694993bede3eb39f959**
3. **key-3-of-3.txt : 04787ddef27c3dee1ee161b21670b4e4**