MINOR PROJECT REPORT

SUBMITTED BY Garima Bisht

**Introduction:**

The project yielded significant insights into the security status of the Cold Box application and underscored the necessity of continual security testing and risk management. Through the identification and resolution of potential vulnerabilities, the project played a pivotal role in mitigating the risk of successful cyber-attacks on the application, safeguarding both the organization and its users. The recommendations outlined in the project offer a blueprint for enhancing the overall security stance of the Cold Box application and can inform future security testing endeavors.

**Methodology:**

The tools and techniques which I have used in this project are

* Nmap
* Network scanning
* Wpscan for enumeration
* Reverse shell
* Netcat for port scanning, listening and redirecting
* Privilege escalation

**Findings:**

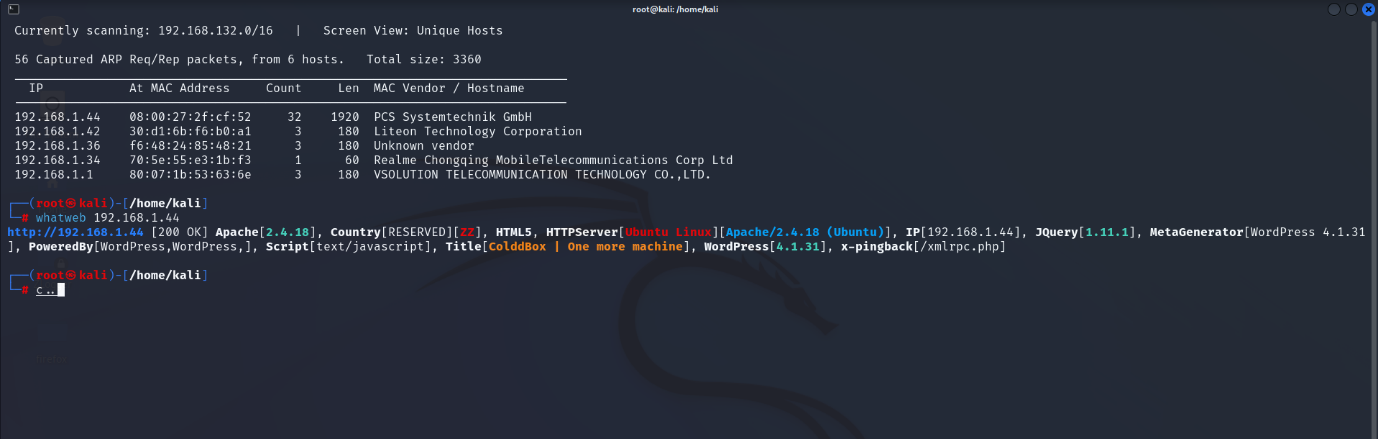
Starting with how I downloaded cold box machine in my system

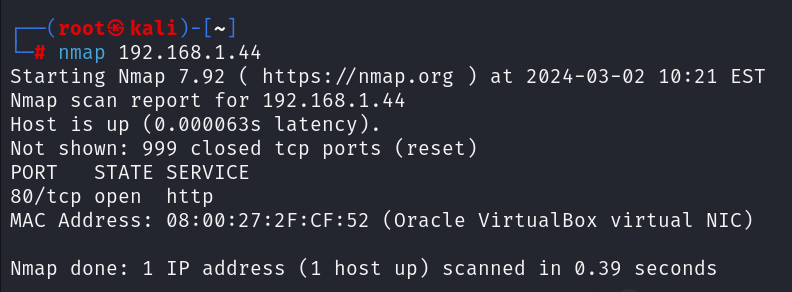
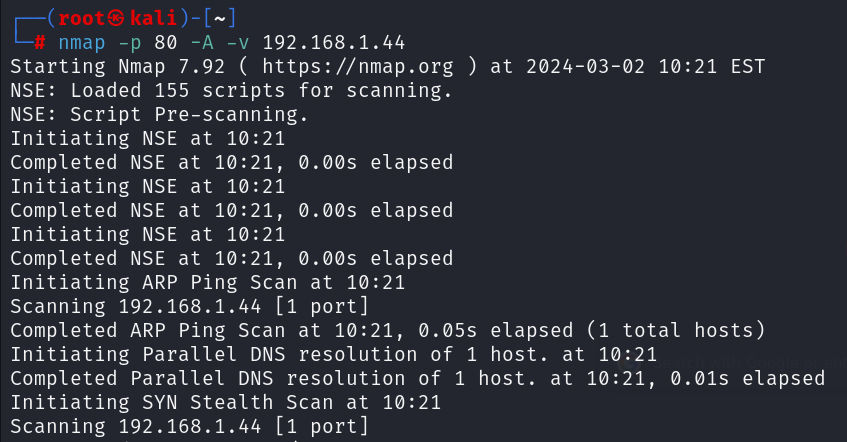
You can use vulnhub website

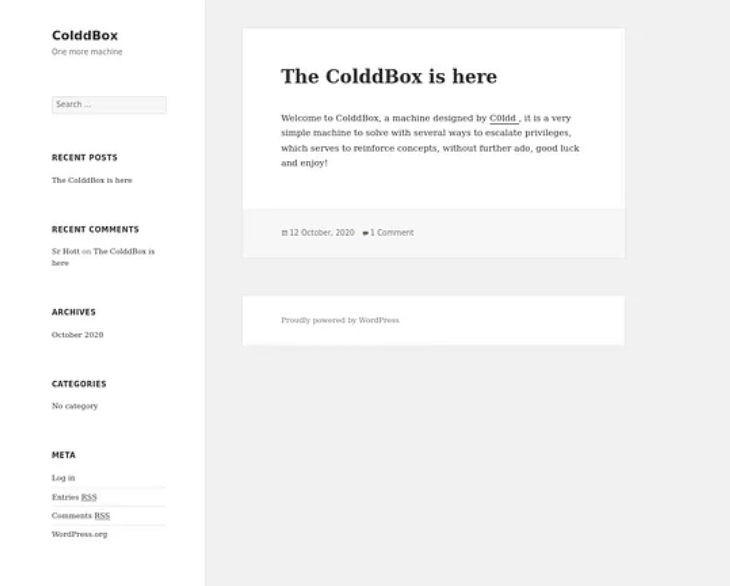
<https://www.vulnhub.com/entry/colddbox-easy,586/>

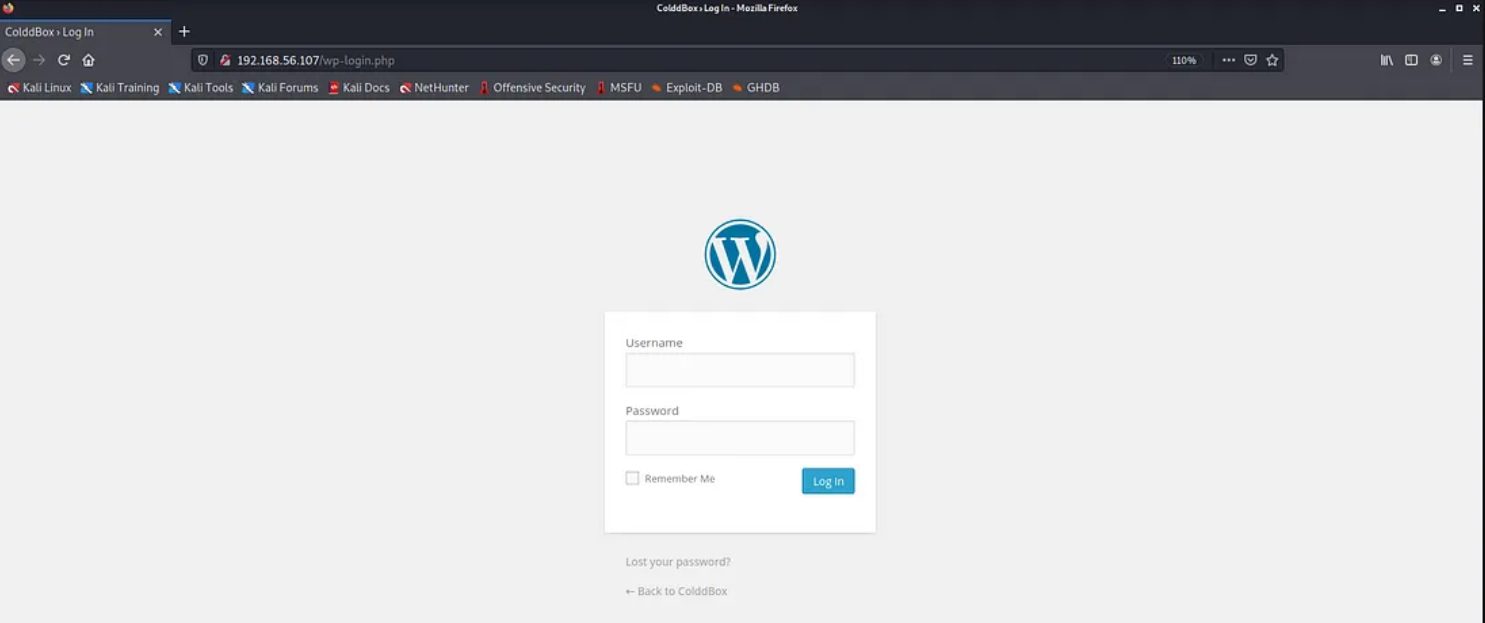
* I started my kali virtual machine and cold box (both on bridge network)

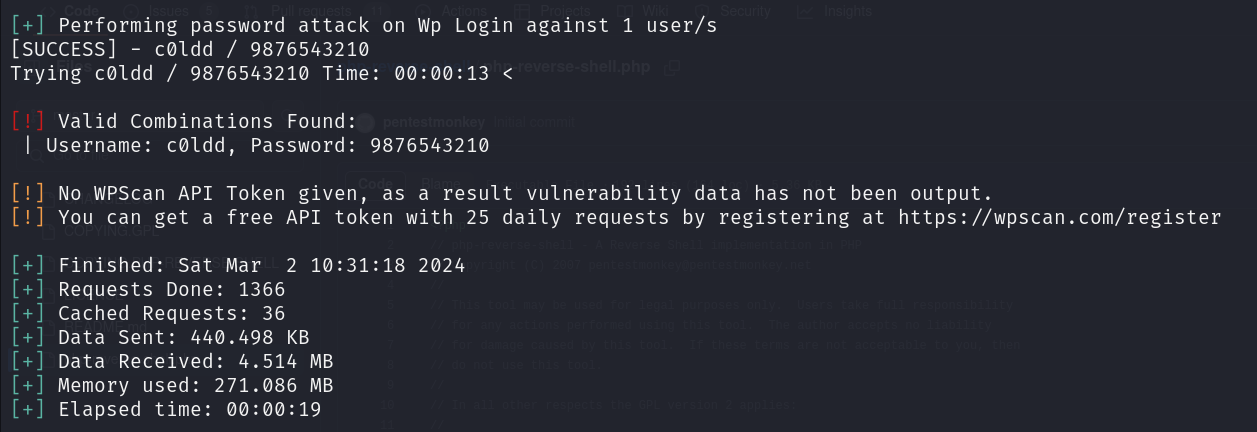
1. Use netdiscover command to find the Ip address of target machine
2. Use whatweb on each Ip to identify which one of the hosts is target. In this case first Ip which is 192.168.1.44 is the target machine.



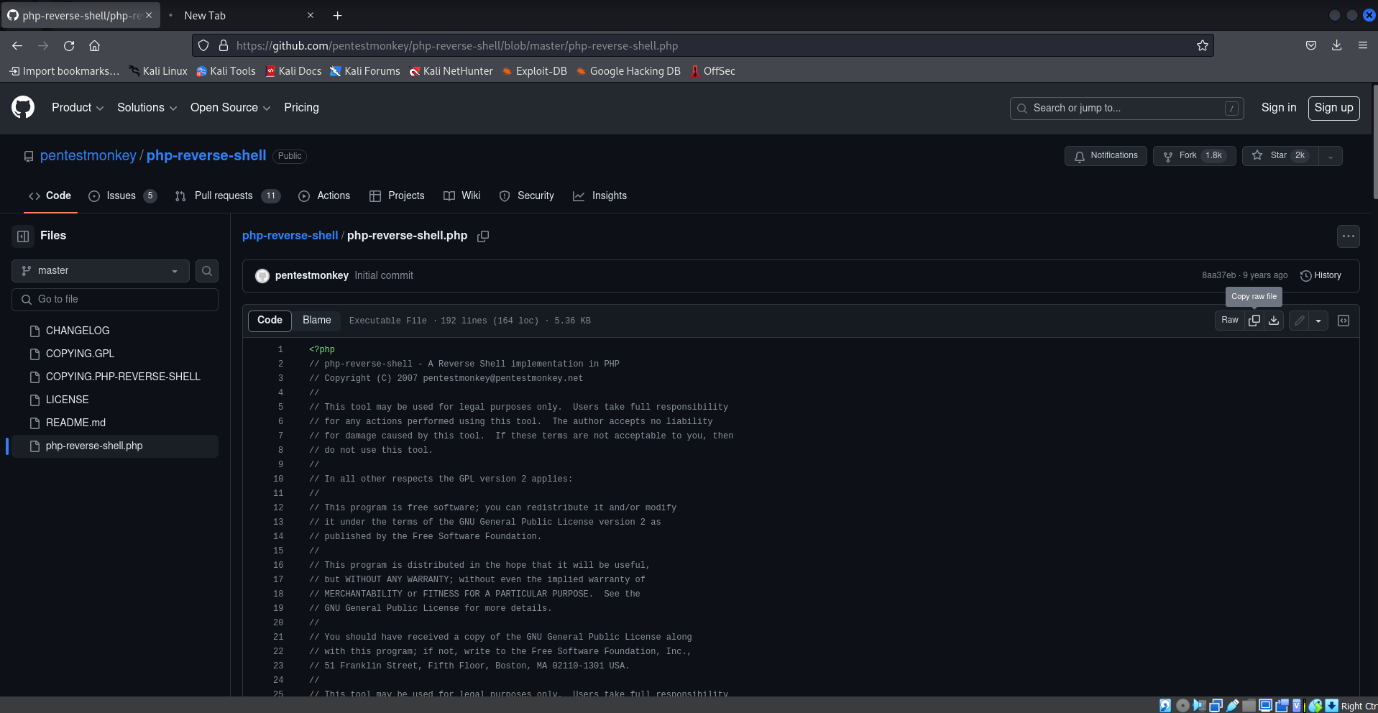
1. Now I have used nmap command “Nmap 192.168.1.44” to scan this ip and open ports. As we can see port 80 tcp is open
2. I used Nmap -p 80 -A -v (Ip) to scan port 80(-p), OS and service detection or aggressive scanning(-A) and scan version(-v)
3. Search the IP address on search engine
4. Go to login

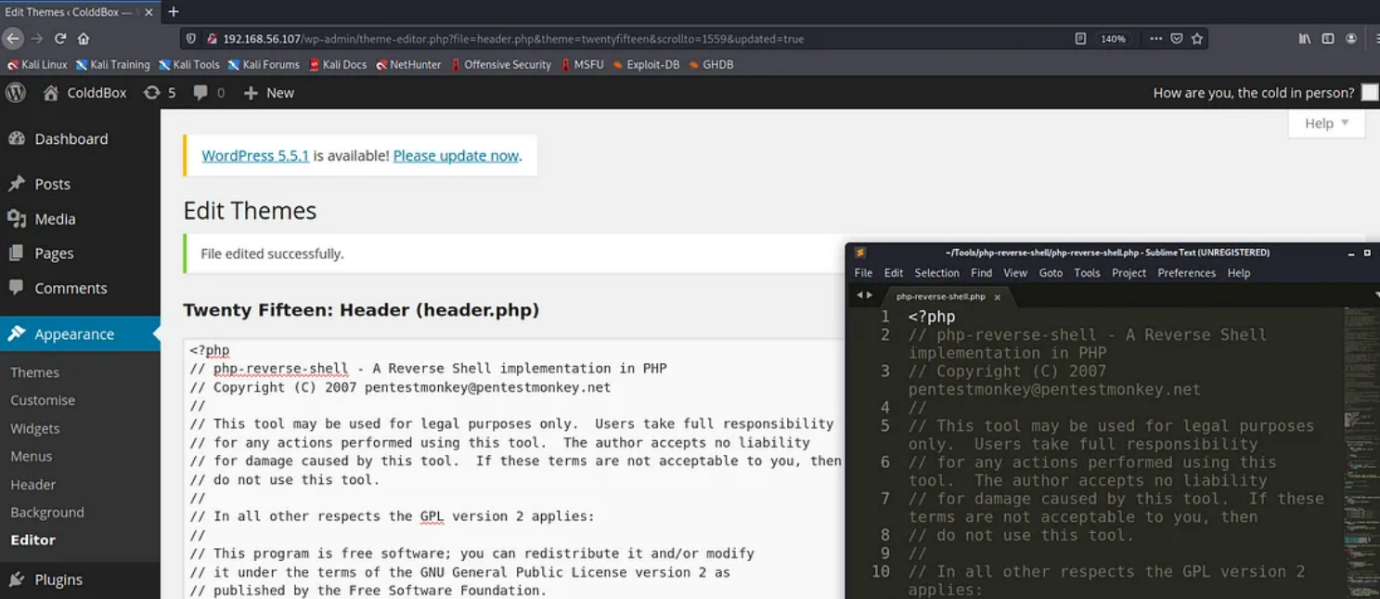




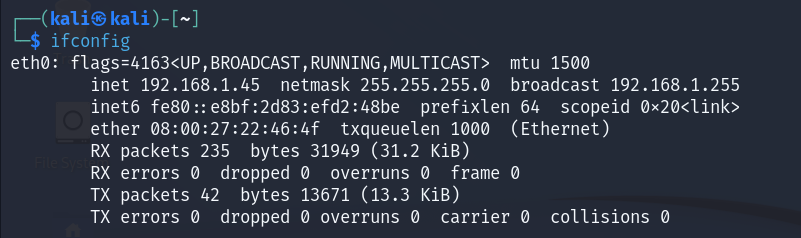
1. I used wpscan for enumeration and it lists username by brute forcing1212
2. Now take anyone of those usernames to brute force password. I took c0ldd and got password (9876543210)
3. Go back to login page and fill the credentials you have found

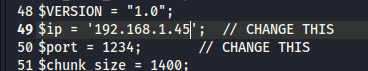


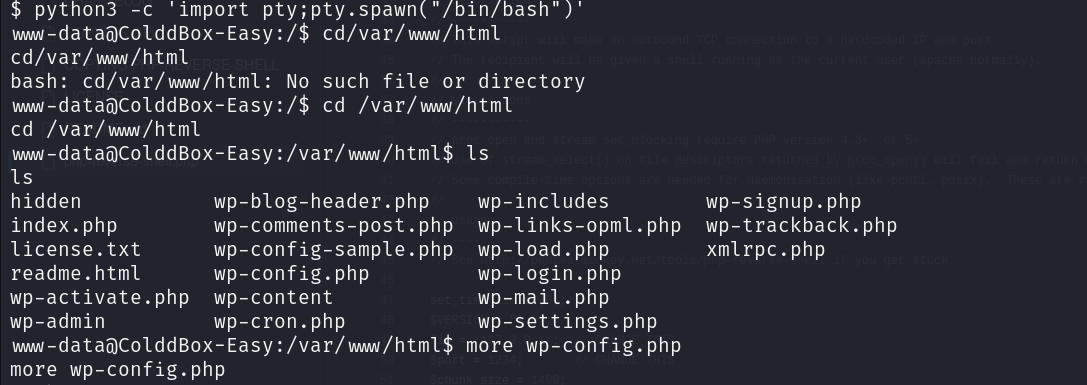
1. Now since I’m in the admin dashboard I can upload a reverse shell. So, upload reverse shell by modifying header.php

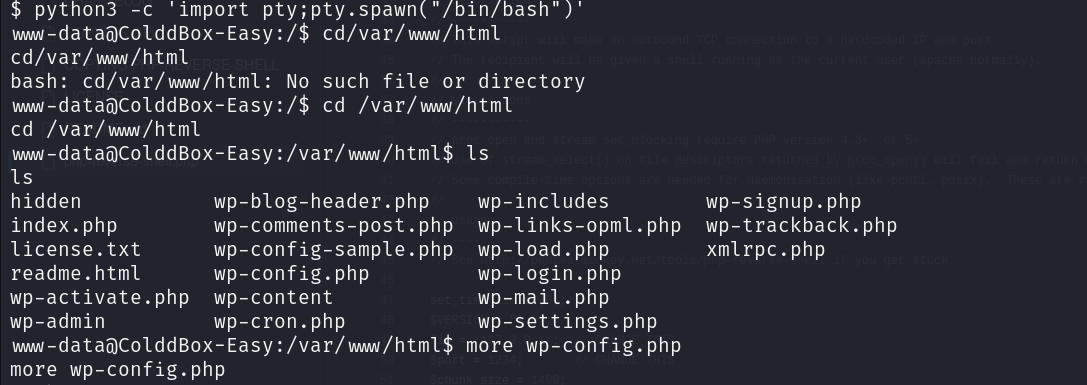


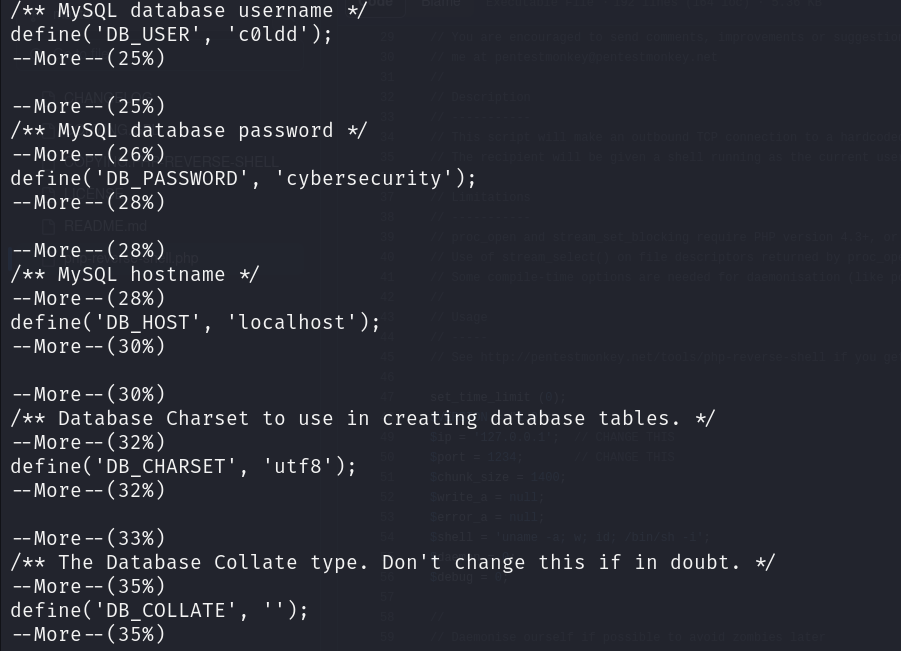
1. Now for reverse shell to perform we have to change our Ip address and port. So I used ifconfig to find my Ip address

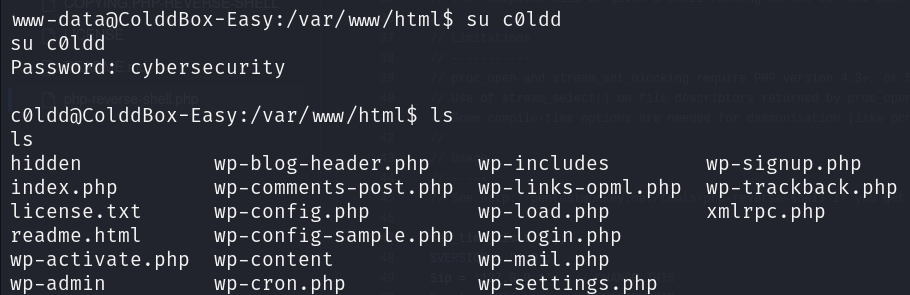


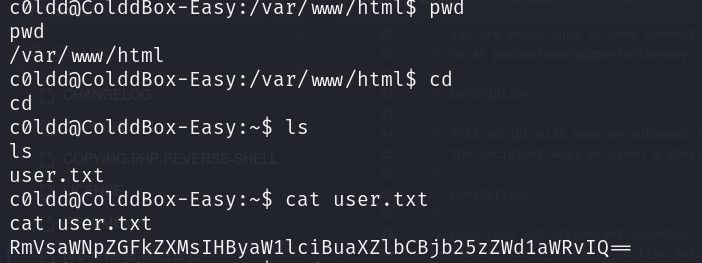
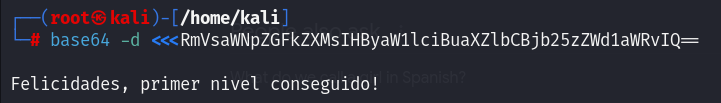


1. After changing Ip address, use Netcat to listen to port 1234 and open your python spawned shell. We can see all the php files here. Wp-config.php contains id and password for the database
2. Use more to see username and password on database file

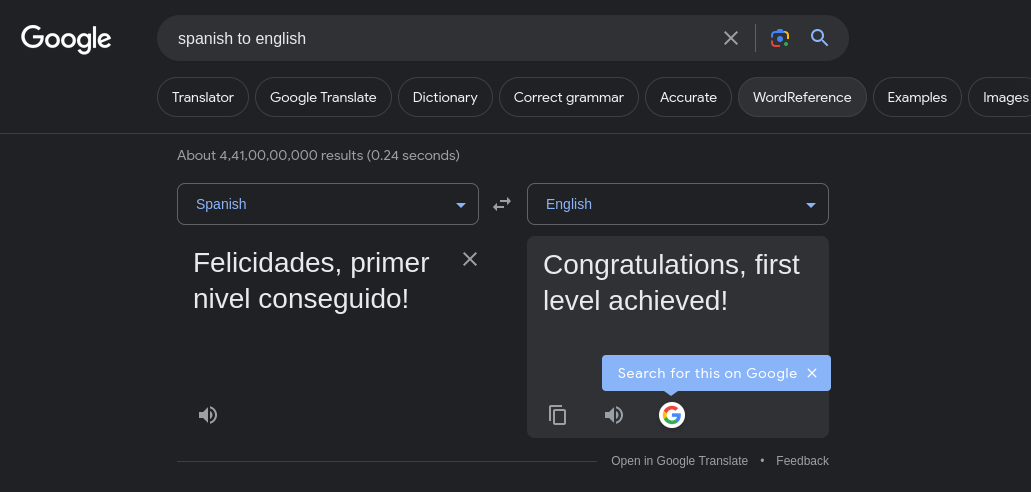


1. We can see username “c0ldd” and password “cybersecurity” and many other sensitive information like hostname, etc.
2. Use the found credentials to log into that account



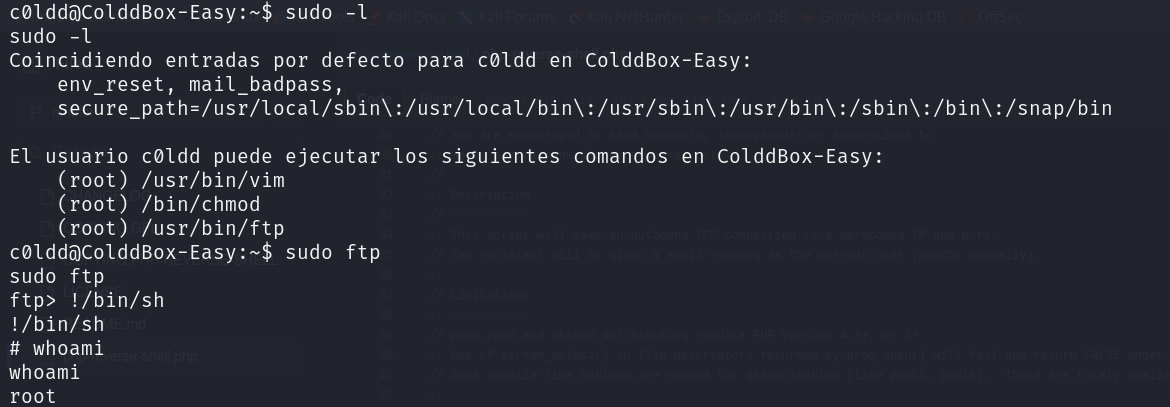
1. Since I don’t have root privileges so use “ls” command to list files present in this directory and I found a file names “user.txt”. I used “cat” command to read this file 
2. Decode the message inside the file

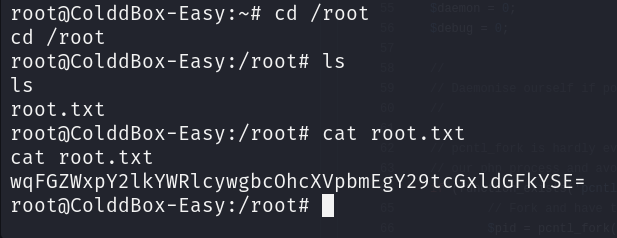
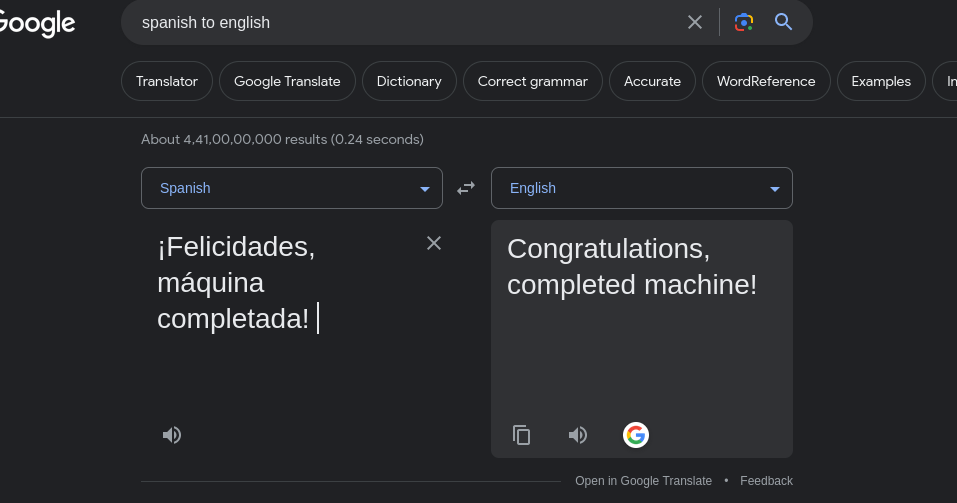
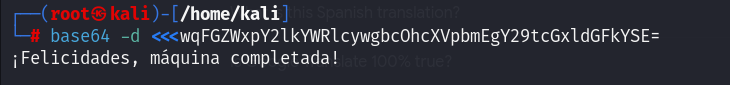
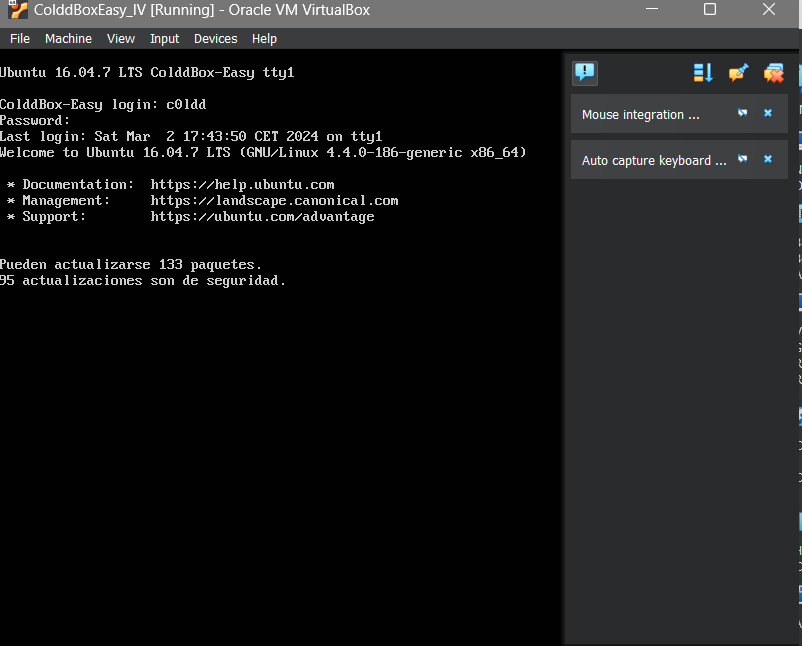
The message was in Spanish which translates to this(lvl 1 completed)



1. Going further into privilege escalation to get root permissions. I used sudo -l to list all the files which provide the root and use GTFOBins to exploit these binary files

I used sudo ftp to exploit them and then use whoami to check if I have root privileges



1. Now that I’m in root. I used cd / root to change directory and then used ls to list file. Now that I can see file named “root.txt”, I used cat to read it
2. I decode the message I found and translates it.
3. You can now try using the database credentials on coldbox machine since we have successfully hacked it

**Risk management:**

since we have successfully hacked into this machine, here are some risk management points to consider:

1. If a machine has been compromised, immediately isolate it from the network to prevent further unauthorized access or data exfiltration.
2. Conduct a forensic analysis regularly
3. Apply patches and updates to the system and software to address the vulnerabilities exploited during the attack to prevent similar incidents on future.
4. Change all passwords and credentials associated with compromised machine
5. Provide security awareness training to users and employees to educate them

**Conclusion:**

The "Pentesting on cold Box" project provided valuable insights into the security posture of a cold Box application and highlighted the importance of ongoing security testing and risk management. The project identified several vulnerabilities that could be exploited by attackers and provided actionable recommendations for remediation. By addressing these vulnerabilities, the organization can reduce the risk of a successful cyber-attack on their Cold Box application, protecting both the organization and its users

**Appendices:**

I have followed a cold box walk through from internet

[**https://infosecwriteups.com/colddbox-easy-vulnhub-walkthrough-cac3680e03c2**](https://infosecwriteups.com/colddbox-easy-vulnhub-walkthrough-cac3680e03c2)