Ex9: Brute force attack on the linux server using hydra

Hydra is a popular open-source password brute-force tool used by security professionals and penetration testers in cybersecurity. It is designed to perform dictionary attacks or brute-force attacks on various network protocols, including but not limited to SSH, FTP, HTTP, HTTPS, and others. The tool is capable of trying a large number of username and password combinations to gain unauthorized access to a system.

https://attack.mitre.org/techniques/T1110/

Brute Force

Sub-techniques (4)

ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

Password Guessing: An adversary may guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords.

Password Cracking: Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table to crack hashes. Cracking hashes is usually done on adversary-controlled systems outside of the target network

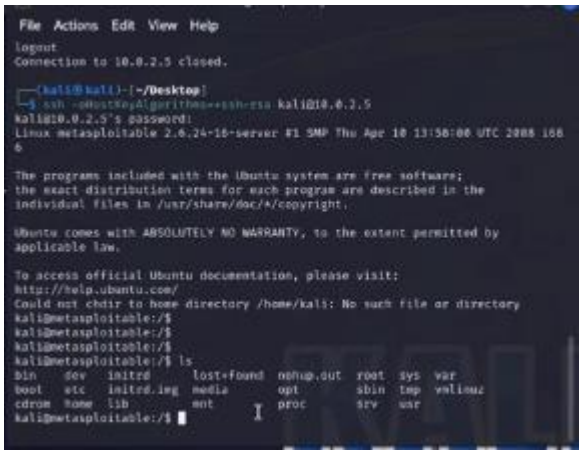
Password Spraying: Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain

Credential Stuffing: Adversaries may use credentials obtained from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised and the user account credentials accessed.

Hydra Developed by

Hydra - The Hackers Choice https://thc.org

https://www.security.org/how-secure-is-my-password/



Lab Setup

You will need to download the following items:

- Kali Linux
- Metasploitable2

If Hydra is not installed use command:

```
sudo apt get install hydra
```

Use the following command to scan the network:

```
nmap -A 10.0.2.0/24
```

The Hydra command used in this lab is:

```
hydra -L (Username file) -P (Password file) 10.0.2.5 ftp
```

Make sure to replace the username file and password file with your own password and username files.

If you are unable to connect through SSH to the metasploitable2 machine use the following work around:

```
ssh -oHostKeyAlgorithms=+ssh-rsa username@ipaddress
```

Create username file and password file

https://www.youtube.com/watch?v=M_VHHdgBzIc&t=320s