Lab-06

1. ABC Corp, a medium-sized company, is concerned about the security of its network and wants to ensure that its employees are using strong passwords. The IT security team has been tasked with conducting a password strength assessment to identify weak passwords that may pose a security risk. The IT security team decides to use a password cracking tool, to perform the password strength assessment. The plan to target the company's internal systems, including FTP, SSH. By using Hydra password cracking tool perform a password strength assessment, so that ABC Corp's IT security team was able to identify and address weaknesses in their network's authentication mechanisms.

Solution:-

Ensure kali Linux and metaspoiltable VM's are up and running.

Go to Kali linux terminal, Type

locate unix_passwords.txt

It contains dictionary of passwords. Without knowing password, we cannot enter into the target system with FTP connection.

if unix_passwords.txt doesnot contain msfadmin, password of metaspoiltable2 VM, Then type below commands

vi /opt/metasploit-framework/embedded/framework/data/wordlists/unix_passwords.txt

Then add msfadmin and save the file.

Hydra tool is used for password cracking. Type the below command in kali linux terminal for cracking the password (Dictionary attack), specify the path of unix_password.txt and IP address of metaspoiltable2 vm.

hydra -l msfadmin -P /opt/metasploit-framework/embedded/framework/data/wordlists/unix_passwords.txt ftp://192.168.62.129

Now it will match the passwords from the dictionary, once the exact match is found. it will display password matched.

Now get FTP connection to target machine (Metaspoiltable 2) by using below command

ftp 192.168.62.129

#Then enter username and password of target machine.

#Once you get ftp> prompt, it clearly indicates, you got into your target machine.

#Navigate yourself to different path by using below commands

ftp>ls

ftp> cd vulnerable

ftp> cd twiki20030201

to transfer the file from your target machine to your system.

ftp>get TWiki20030201.tar.gz

Similarly, once the password of the target machine is known we can also connect target machine by using SSH Connection by using below command.

ssh -o HostKeyAlgorithms=+ssh-rsa,ssh-dss msfadmin@192.168.62.129

Type the password. Then you can see the below prompt

msfadmin@metasploitable:~$

navigate yourself in the target machine to access the files.