



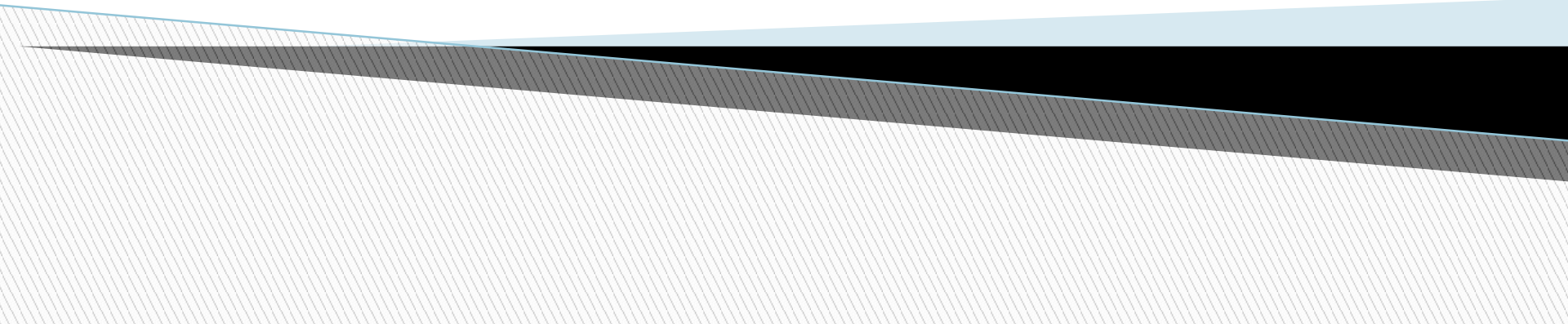
**MALAVIYA NATIONAL INSTITUTE OF
TECHNOLOGY, JAIPUR**

Computer Network Security Attack

Smart Brute Force Attack

**Submitted to-
Dr. Ramesh Babu Battula**

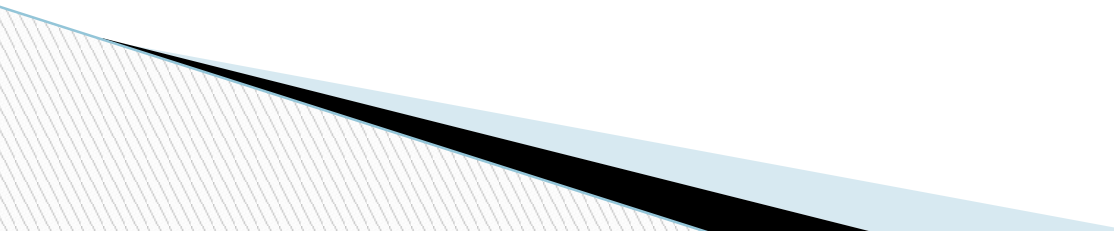
1: Password Cracking Techniques



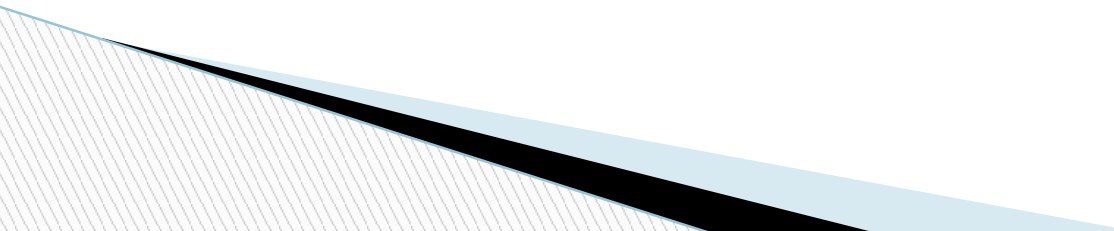
A: Dictionary attack

- ❑ The attacker utilizes a wordlist in the hopes that the user's password is a commonly used word
- ❑ Software are available that will run through these lists.
- ❑ Can be thwarted with robust password policies.
- ❑ One random character in known words (i.e. "Suc3cess") could defeat this attack.

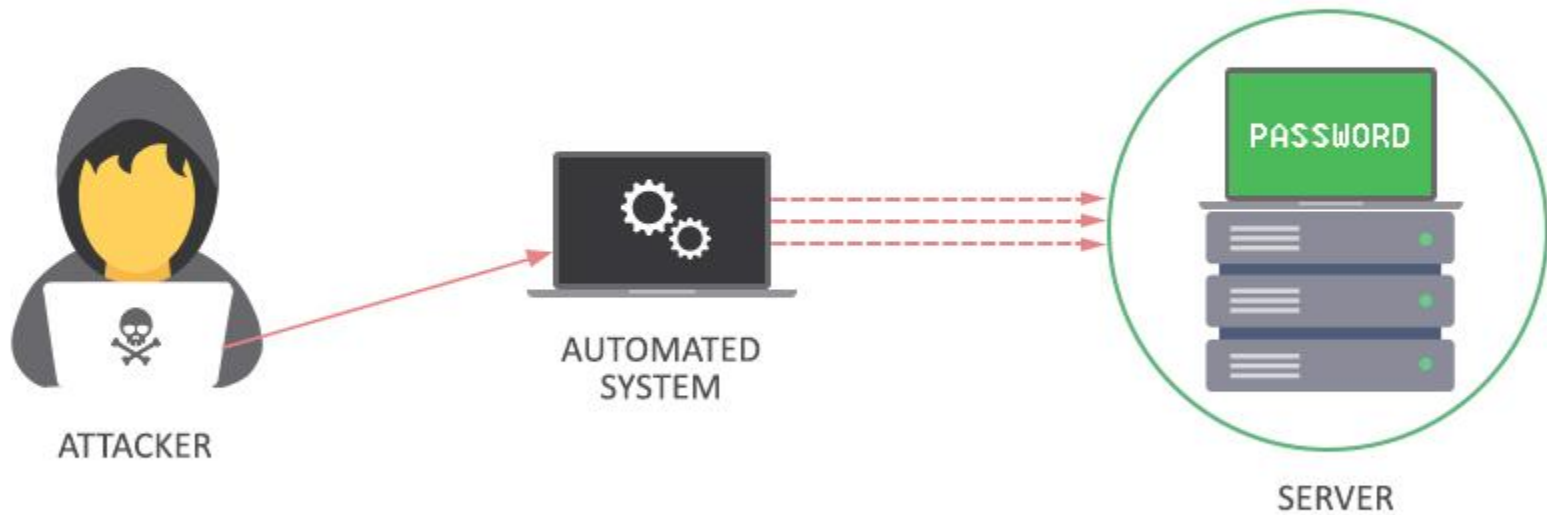
B: Rainbow table attack

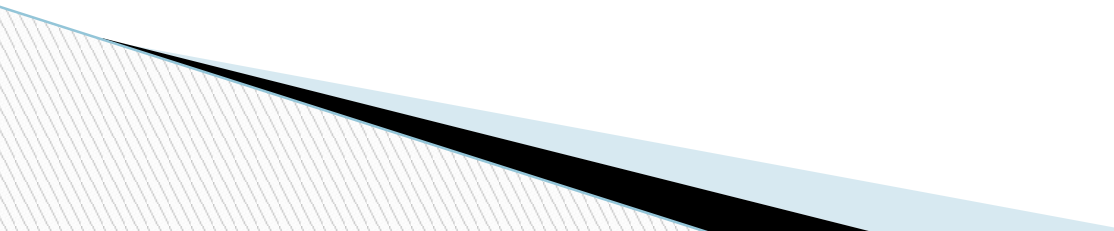
- A rainbow table is a database that is used to gain authentication by cracking the password hash.
 - It is a pre-computed dictionary of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a particular hash.
- 

C: Phishing

- There's an easy way to hack: ask the user for his or her password.
 - A phishing email leads the unsuspecting reader to a faked log in page associated with whatever service it is the hacker wants to access, requesting the user to put right some terrible problem with their security. That page then skims their password and the hacker can go use it for their own purpose.
- 

2. Brute Force Attack

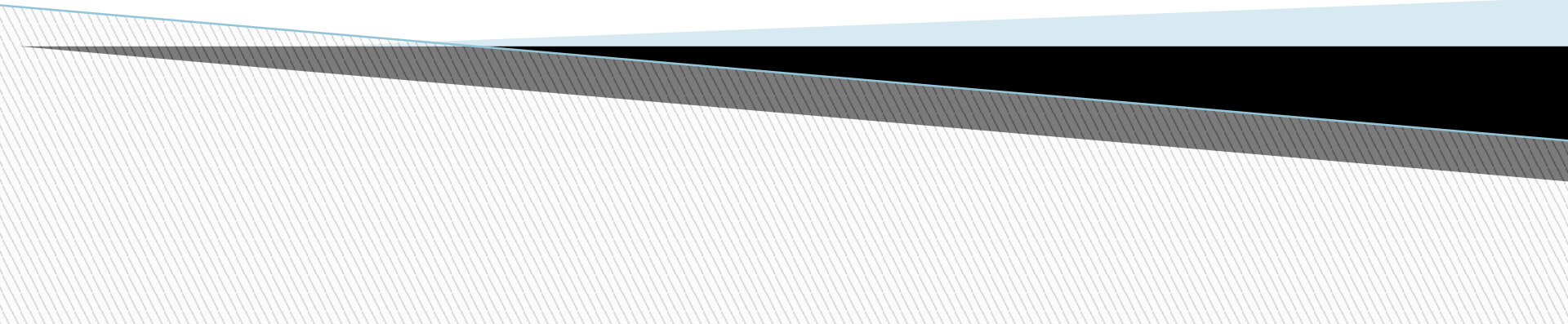


- ❑ A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN).
 - ❑ In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.
 - ❑ A brute force attack is also known as brute force cracking or simply brute force.
- 

Tools and technologies Used

- Python
- chromedriver.exe

3: Description of our attack



- **Target Site:** www.mniterp.org
- **Aim:** To Crack the Student password using Brute Force.
- **Problem in simple brute force:**

Captcha : A computer program or system intended to distinguish human from machine input, typically as a way of thwarting spam and automated extraction of data from websites.

Solution:

1. We find that in this site -> Captcha image source contains captcha value. (we extract that using our code).
2. Enter student id in the code and run the python script.
3. We have used multi-threading to open multiple instance of chrome browser(equal to thread numbers) for fast output.

5 Threads are working(see at bottom 5 chrome browsers) in parallel and also image loading is stopped to make the process of details filling faster, so that we can get the user password quickly.

Python 3.7.2 Shell

File Edit Shell Debug Options Window Help

1:700009

2:700203

3:700411

5:700801

1:700010

2:700204

3:700412

5:700802

1:700011

2:700205

3:700413

4:700600

5:700803

2:700206

1:700012

5:700804

2:700207

1:700013

4:700601

2:700208

5:700805

1:700014

3:700414

2:700209

4:700602

5:700806

3:700415

1:700015

2:700210 4:700603

2:700211

5:700807

3:700416

1:700016

4:700604

2:700212

3:700417 5:700808

2:700213

4:700605

Ln: 59 Col: 0

MNIT Jaipur

data:

https://mniterp.org/mniterp/student.htm

Chrome is being controlled by automated test software.

Online Fe

Welcome to Students of MNIT

Please Login

User ID

Password

Fin Year: 2019-20

Enter Security No in the box below

Refresh Captcha

72857

Login

Forgot / Reset Password

Your password does not match.
Login Failed...

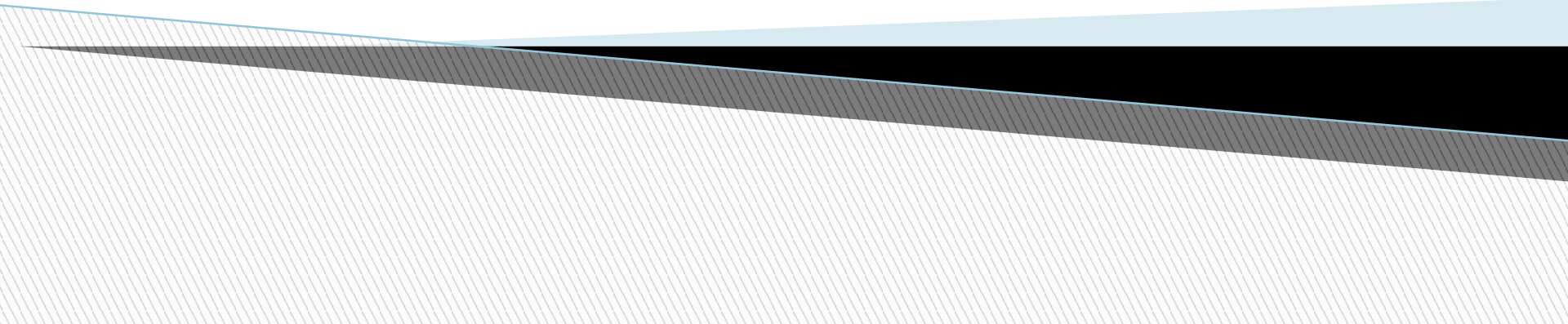
Alerts (Active)

Coursa Appraisal for End of the Semester: is active from

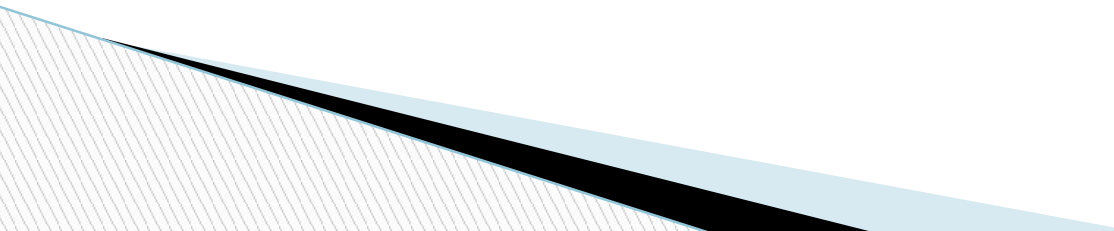
Type here to search

7:23 AM 24-Apr-19

4: Suggestions



The following measures can be used to defend against brute force attacks:

- 1: Requested forgot password should be complex password.
 - 2: Captcha image source should not contain captcha value.
 - 3: Temporarily locking out users who exceed the specified maximum number of failed login attempts
 - 4: Slow down repeated logins
- 

Thank You