IMPACT OF CYBER ATTACK ON ONLINE EXAM

Ms. Rubina khan

Student, Dept. of Information Technology, Keraleeya Samajam (REGD.) Model College Maharashtra, India

---

Abstract – *Technology is rapidly evolving in a world driven by social networks, online transactions, cloud computing, and automated processes. But with the technological evolution comes the progress of cybercrime, which continually develops new attack types, tools and techniques that allow attackers to penetrate more complex or well-controlled environments, and produce increased damage and even remain untraceable. The COVID-19 pandemic has affected educational systems. in covid-19 pandemic the technology is very rapidly increasing in education many institutions conduct classes or exam in online. Aim of this research is to see the impact of covid-19 pandemic in online exam or education in online exam students facing many problems such as network issues or other technical problems as well as cyber-attack on the server the exam was delayed students were disturbed due to this*

Key words **–** Cyber-attack, COVID-19 pandemic, Online examinations, Denial of Service (DDoS) attack, Cyber Attack Mitigation.

1. Introduction

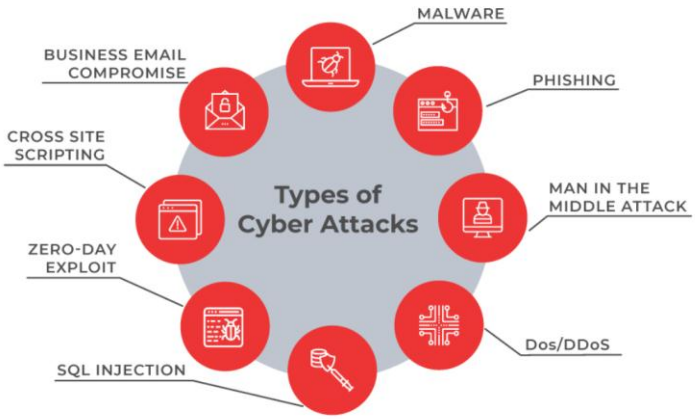
The security of e-learning technologies and online examinations draws the attention of educators actively involved in online teaching. In the COVID-19 pandemic, classroom education has been replaced by online education. The use of e-learning technologies expanded exponentially. Several providers of online assessment systems offered accommodating procedures for easing the transition to online assessments in colleges and organizations for the duration of the trouble. With this sharp increase in the transition to online education, the cybersecurity vulnerabilities of online educational technologies became more noticeable and caused greater anxiety, including privacy and integrity issues. Among various E-learning activities (presentations, lab exercises, exams, quizzes, discussions, etc.), remotely administered online exams are much more fraud compared to traditional face-to-face modality.

Cyber-attack on Mumbai university:

On 7th October, 2020, the University of Mumbai Server was crashed during the course of examination. This has been declared a cyber-attack by the security experts. According to the experts, an online attack has been performed on the online examination server. As a result of which the University of Mumbai has to postponed the examination dates of the students and they were informed to students that the revised timetable of the examination will be declared on the Mumbai University Webpage.

2. Types of Cyber-Attack

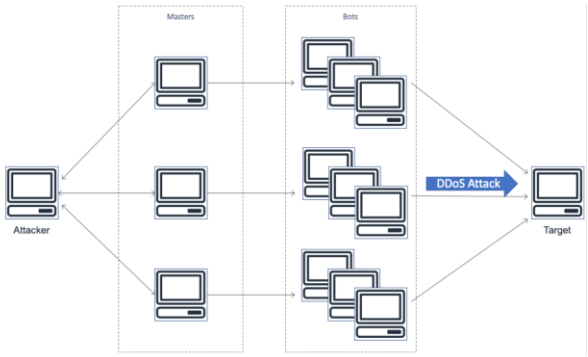
The effect of Cyber-attack on Server Online exam was postponed because of server was down. A cyberattack is a malicious software and intentional attempt by an individual or organization to breach the information system of another individual or organization. Cyber-attack is Cybercrime has increased every year as people try to benefit from vulnerable systems or steal the data.



There are so many types of Cyber-attacks to down the server such as Malware, Phishing, Man-In-The Middle Attack, DDoS, Zero-Day Exploit, Cross site Scripting etc.

2.1 Denial-of-service attack

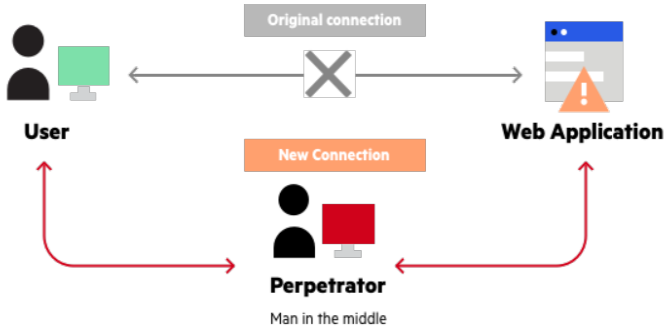
Denial of Service (DDoS) attack is a non-intrusive internet attack made to take down the targeted website or slow it down by flooding the network, server or application with fake traffic. When against a vulnerable resource-intensive endpoint, even a small-scale amount of traffic is enough for the attack to succeed. Distributed Denial of Service (DDoS) attacks are threats that website owners should be aware of because they are such an important part of the security landscape. Navigating the different types of DDoS attacks can be difficult and time consuming.



The aim of a DDoS attack is to prevent legitimate users from accessing your website. For a DDoS attack to be successful, the attacker must send more requests than the victim server can process. Another possibility for successful attacks is for the attacker to send false requests. The Distributed Denial of Service attack will test the limits of a web server, network, and application resources by sending spikes of fake traffic. Some attacks of malicious requests on vulnerable endpoints such as search functions. DDoS attacks use zombie devices called a botnet. These botnets device generally consist of compromised IoT devices, websites, and computers. When a DDoS attack is launched, the botnet will attack the target and use up the application's resources. A successful a attack DDoS can prevent users from accessing a website or slow it down enough to increase the bounce rate, leading to financial losses and performance problems.

2.2 Man-in-the-middle attack

Another type of cyber-attack is man-in-the-middle attack in which type of cyber-attack where a malicious actor enters a conversation between two parties, masquerades as both parties, and gains access to information that both parties were trying to be transmitted. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data intended for someone else, or which is not intended to be sent at all, without any outside party knowing until it is too late.



The main goal of this attack is to steal personal information, such as login credentials, account details and credit card numbers etc.

2.3 Password attack

A password attack is a type of the cyber-attack the third party trying to gain access to your systems by cracking a user's password. In this type of attack does not usually require any type of malicious code or software to run on the system. There is software that attackers use to try and crack your password and steal your data, but this software is typically run on their own system.

In which programs use many methods to access accounts, including brute force attacks made to guess passwords, as well as comparing various word combinations against a dictionary file.

2.4 SQL Injection attack

SQL Injection is a type of injection attack. The attacker can use SQL Injection vulnerabilities to bypass application security measures. The also use of SQL Injection to add, modify and delete records in the database.

A successful SQL injection attack can lead to unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Several high-profile data breaches in recent years have been the result of SQL injection attacks, resulting in reputation damage and regulatory fines. In some cases, an attacker can get a permanent backdoor into enterprise systems, resulting in a long-term compromise that could go unnoticed for a long time.

3. Cyber Attack Mitigation

According to resent reports of 07-Oct-2020 University of Mumbai server was crashed so exams has not been

conducted. Largely because of poor security measures so exams were postponed. Cyber-attack becomes easy due to poor or unless security. So, it became very important to mitigate Cyber-attack.

There are so many methods to mitigates cyber-attacks:

3.1 Identify the Threats

Basic threats like unauthorized access to your computer must be tackled immediately before you experience any information loss. Hackers are always looking for opportunities to invade privacy and steal critically important data, so it is best to take the necessary precautions to protect your sensitive information.

3.2 Beware of Cybercrimes

Always beware of cyber criminals, and act as you expect an attack. Always keep records of which information is attractive to criminals and which is not. Additionally, develop multiple strategies with appropriate risk assessments on a regular basis to ensure effective solutions if the need arises.

3.3 Use Two Factor Authentication

You can minimize the risk of being hacked by using two-factor authentication from any organization. Increase security by adding an additional step for logging into accounts. In this particular system, you have to enter a password plus you have to enter a code that is sent to your smartphone, something that only you have access to. This double authentication allows you to protect your data and deters attacks by hackers.

3.4 Protect Password Theft and Cracking

Some of the user tends to use password which is short and easy to remember, they tend to write somewhere in the notepad or sticky notes in the computer or in notebooks which is not a good security practices adopted by the people. Due to this, many of the username and passwords get stolen and fall in the hands of attackers. So, to avoid using the same passwords everywhere for your convenience and Strictly adopt the policy of 2Factor-Authentication which consist of Password and OTP or Password and Biometrics.

4. Conclusion

As per the research various types of Cyber Attacks down the server or steal the data but by using a lot of mitigation processes we can protect the system to Cyber-attack or server down so we need to aware the peoples of cyber-attacks and how to protect from it. Use two factor of authentication which consist of password and OTP due to this way can be reduce cyber-attacks.

5. Acknowledgement

The Research has placed an important part to explore the practical work, to learn in detail part from the theoretical studies.

I would sincerely like to thank all the Teachers who helped me throughout the research.

I thank all the respondents for their cooperation and time in completing this research, without whom, it would not have been successful.

6. References

1. https://www.upguard.com/blog/cyber-attack
2. https://www.researchgate.net/publication/283258166_Cyber-Attack_Analysis_of_a_School_Computer_Network
3. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
4. https://www.itproportal.com/features/10-essential-steps-for-preventing-cyber-attacks-on-your-company/