

What's in it for you?

1. The Rise of Cybercrimes
2. Different types of Cyberattacks
3. Reasons for Cyberattacks
4. What is Cyber Security?
5. Basic Network Terminologies
6. Cyber Security Goals
7. Tackling Cybercrime
8. Demo – Metasploit Attack





The rise of Cybercrimes

The Rise of Cybercrimes



Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm

The Rise of Cybercrimes

Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm

Origin of the attack



The attack originated in Asia and then spread across the world

The Rise of Cybercrimes



Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm

How did the attack happen?



Attack started from an exposed vulnerable
SMB port

The Rise of Cybercrimes



Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm

How did the attack happen?



Attack started from an exposed vulnerable SMB port



Within a day more than 230,000 computers were infected across 150 countries

The Rise of Cybercrimes



Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm

Victims of the attack



Computers running the Microsoft OS

The Rise of Cybercrimes



Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm

Victims of the attack



Computers running the Microsoft OS



Users that used the unsupported version of Microsoft Windows and also those users who hadn't installed the new Microsoft security update of April 2017

The Rise of Cybercrimes

Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm



Description of the attack



WannaCry cryptoworm encrypted the data and locked the users out of the target systems



In return, the users were asked for a ransom of \$300 - \$600 which has to be paid via bitcoin

The Rise of Cybercrimes

Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm

Impact of the attack



200,000 to 300,000
computers were infected

The Rise of Cybercrimes

Did you know about the deadly WannaCry ransomware attack? It was one of the most severe worldwide cyberattacks, caused by the WannaCry cryptoworm



Impact of the attack



200,000 to 300,000
computers were infected



FedEx
Express



RENAULT

NISSAN

Both private and government organizations were hit, computers in hospitals were corrupted, Nissan and Renault had to put their business on hold as their computers were infected

The Rise of Cybercrimes

In February 2019, Dunkin' Donuts announced that the users of their rewards program were targeted by a credential stuffing attack. In such an attack, users' credentials are stolen



Hacker



The Rise of Cybercrimes

In February 2019, Dunkin' Donuts announced that the users of their rewards program were targeted by a credential stuffing attack. In such an attack, users' credentials are stolen



Hacker



← The user's first and last name, and email ID's were stolen

DUNKIN'
DONUTS.



The Rise of Cybercrimes

In February 2019, Dunkin' Donuts announced that the users of their rewards program were targeted by a credential stuffing attack. In such an attack, users' credentials are stolen



Let's now look into the different types of such cyberattacks

Different Types of Cyberattacks



The different types of cyberattacks are :

Malware Attack

Social Engineering
Attack

Man in the Middle
Attack

Denial of Service
Attack

SQL Injection Attack

Password Attack

Malware Attack

Malware refers to malicious software, viruses, ransomware, and worms. Trojan virus is also a form of malware that disguises itself as a legitimate software



Malware Attack

It gets into a system when the user clicks on suspicious links or downloads attachments or uses an infected pen drive. It then obtains all the information from the client's system



User opens links or uses a corrupted pen drive



User's system gets corrupted



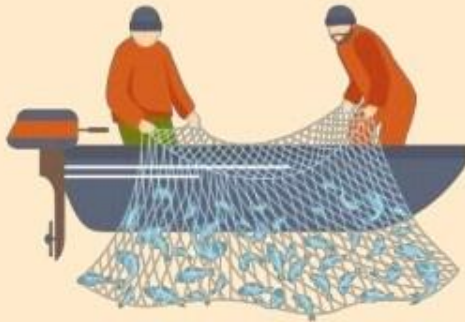
Social Engineering Attack



It is the art of manipulating people so that they end up giving their confidential information. It is broken down into 3 categories:

Social Engineering Attack

It is the art of manipulating people so that they end up giving their confidential information. It is broken down into 3 categories:



Phishing Attack



Spear Phishing Attack



Whaling Phishing Attack

Social Engineering Attack

Phishing attack is a practice wherein the hacker usually sends fraudulent emails, which appear to be coming from a trusted source. It is done to install malware or to steal sensitive data like credit card information, and log in credentials



Phishing Attack



User opens the mail with the attachment and unknowingly downloads the virus



User's system gets affected



Social Engineering Attack

Spear Phishing is a variation of Phishing. Here, the attacker targets a specific individual or a group of people



Spear Phishing
Attack



Hacker identifies a
victim



Hacker then sends a
targeted legitimized
looking email



Unaware of this, the
victim opens the email
which has malware



Now, hacker steals data
from the victim's computer

Social Engineering Attack

Whaling Phishing attack is a type of attack that specifically targets wealthy, powerful and prominent individuals



Whaling Phishing Attack



Man in the Middle Attack

This attack is also known as eavesdropping attack. The attacker hijacks a session between the client and the server



Client

Client-server communication



Server



Attacker

Man in the Middle Attack

The attacking computer takes the IP address of the client. Unaware of this, the server continues to communicate with the attacker. This happens in an unsecured Wi-Fi network and through malware



Client

Client-server communication

Got the IP address!



Attacker



Server

Man in the Middle Attack

The attacking computer takes the IP address of the client. Unaware of this, the server continues to communicate with the attacker. This happens in an unsecured Wi-Fi network and through malware



Client

Client-server communication



Server



Attacker



Denial of Service Attack

A Denial of Service attacks' motive is to flood systems and networks with traffic to exhaust its resources and bandwidth. By doing so, it is unable to cater to legitimate service requests



Denial of Service Attack

When attackers use multiple systems to launch this attack, it is known as Distributed Denial of Service (DDOS) attack



SQL Injection Attack

In a database driven website, the hacker manipulates a standard SQL query. Malicious code is inserted into a SQL server to obtain information



Malicious code inserted into a SQL server



SQL Injection Attack

This attack allows hackers to view, edit, and delete tables in databases. In addition to this, the attackers can also obtain administrative rights



Hacker now has access to the database



Password Attack

The easiest way to hack a system is by cracking a user's password. This is done in various ways



Password Attack

Brute force attack is the practice wherein the hacker tries to login with all possible password combinations



Brute force attack – every possible combination

A, a, Aa, AAAA, aaaa, B, b....

Password Attack

In the dictionary attack, a list of common passwords is used to crack the users' log in credentials



Brute force attack – every possible combination

A, a, Aa, AAAA, aaaa, B, b....

Dictionary attack – common passwords

1234, ABCD,.....