KEMENTERIAN PENDIDIKAN TINGGI

POLITEKNIK MALAYSIA
KUALA TERENGGANU

Introduction To Security Basics

by Sharina Diana Bt Johari

Introduction To Security Basics

by Sharina Diana Bt Johari
The Department
of Information and Communication Technology (JTMK)
Polythechnics of Kuala Terengganu

Author :
Sharina Diana Bt Johari

Published by:
Politeknik Kuala Terengganu
20200 Jalan Sultan Ismail
Kuala Terengganu, Terengganu.

Cataloguing-in-Publication Data

Perpustakaan Negara Malaysia

A catalogue record for this book is available from the National Library of Malaysia

eISBN 978-967-2240-52-5

SINOPSIS

e-Book Introduction to Security Basic is written the common threats and attacks faced today. This course provides with foundational theory behind information security, the basic principles and techniques when designing a secure system.

This e-book Introduction to Security Basic cover to the principles and good practices in environmentally sustainable secured computing and the use of appropriate tools and technology in managing information system environment.

by
Sharina Diana Bt Johari
Department of Information Technology And Communication
Polytechnic of Kuala Terengganu

TABLE OF CONTENTS

INTRODUCTION TO SECURITY BASICS

INTRODUCTION TO SECURITY

WHAT IS SECURITY

- Security is about **the protection of assets.**
- Security for **information technology (IT) refers to the methods, tools and personnel used to defend an organization's digital assets.**
- The goal of IT security is to protect **these assets, devices and services from being disrupted, stolen or exploited by unauthorized users, otherwise known as threat.**
- Threats can be external or internal and malicious or accidental in both origin and nature.

-www.techtarget.com

INTRODUCTION TO SECURITY

WHAT IS INFORMATION SECURITY

- Digital information is manipulated by a microprocessor, stored on a storage device and transmitted over a network.

- The goal of information security is **to ensure that protective measures are properly implemented to defend against attacks and prevent the total collapse of the system when a successful attack does occur**

- The processes and methodologies involved with :

1. Keeping information confidential
2. Available
3. Assuring its integrity

INTRODUCTION TO SECURITY

INFORMATION SECURITY

“That protect the integrity, confidentiality andavailability of information on the devices that store, manipulate andtransmit the information through product, people producers.

– CompTIA@ Security Guide to Network Fundamentals, Mark Ciampa, Ph.D

Hardware

Data

People

Software

Storage Device

INTRODUCTION TO SECURITY

GOAL OF SECURITY

When working in the security field one of the first acronyms to be encounterred in the information security field is **CIA.**

INTRODUCTION TO SECURITY

GOAL OF SECURITY

1 CONFIDENTIAL

Define deals with keeping information, network and system secure from unauthorized access or set of rules that prevents sensitive information form being disclosed to unauthorized people, resources and processes.

2 INTEGRITY

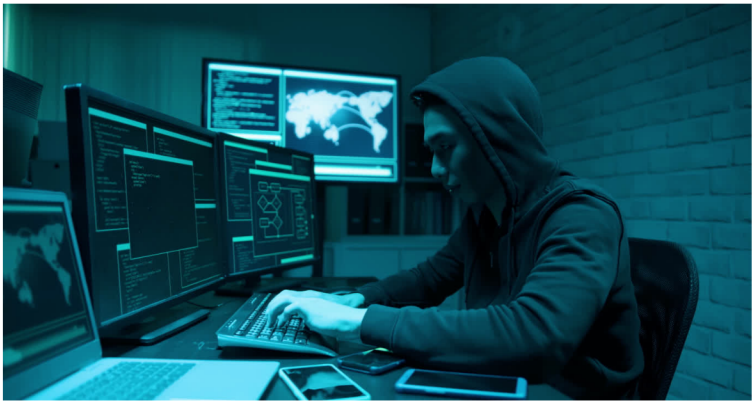
Ensures that system information or processes are protected from intentional or accidental modification. One way to ensure integrity is to use a hash function or checksum.

3 AVAILABILITY

Availability means that authorized users are able to access systems and data when and where needed and those that do not meet established conditions, are not.

INTRODUCTION TO SECURITY

WHAT IS HACKING



- Hacking refers **to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources.**

- **Modifying system or application** features to achieve a goal outside of the creator's original purpose.

- **Used to steal, pilfer and redistribute** intellectual property to leading to business loss.

INTRODUCTION TO SECURITY

HACKERS

- Intelligent individuals with **excellent computer skills**
- Their **intention can either be to gain knowledge or to poke around to do illegal things**
- For some hackers, **hacking is a hobby** to se how many computers or networks they can compromise

Hackers who are **proactively explorer, identifies and alerts organization to vulnerabilities that an attackers could use for malicious purposes.**

ATTACKERS

- Someone **gains unauthorized access to someone else's network and computer for malicious purposes.**
- The **attacker exploits them without permission** or without warning the organization.

INTRODUCTION TO SECURITY

TYPES OF HACKERS

Script kiddie

An unskilled hacker who compromises system by running scripts, tools and software developed by real hackers

Cyber Terrorist

Individuals with wide range of skills motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

State sponsored Hacker

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

Hacktivist

Individuals who promote a political agenda by hacking, especially defacing or disabling websites

Black hat

Individuals with extraordinary computing skills resorting to malicious or destructive activities

Grey hat

Individuals who work both offensively and defensively at various times

White hat

Individual professing hacker skills and using them for defensive purposes and also known as Security analyst

Suicide hacker

Individuals who aim to bring down critical infrastructure for a cause and are not worried about facing jail terms or any other punishment

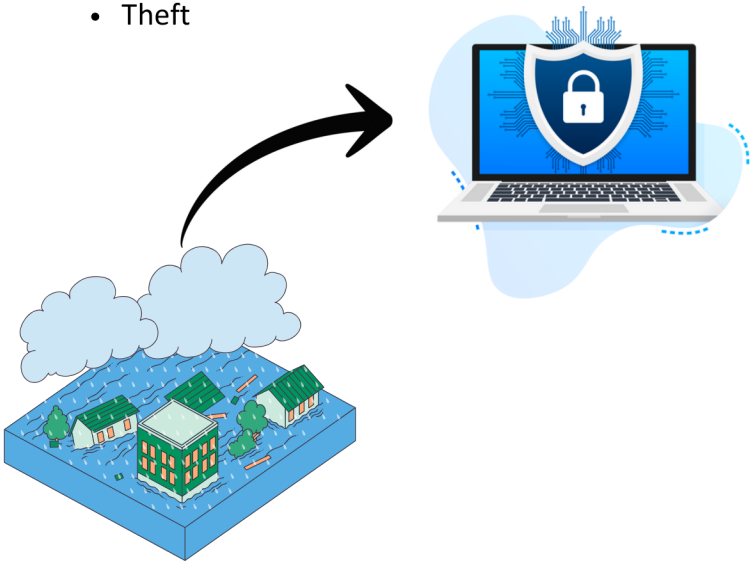
SECURITY THREATS

DEFINITION

- **A threat** in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system.

- A **threat** something that may or may not happen, but has the potential to cause serious damage.

- There are four types of security threats :
    - Malicious code = Malware
    - Hacking
    - Natural disaster
    - Theft



SECURITY THREATS

TYPES OF SECURITY THREATS

MALICIOUS

Commonly knows as malware is any software that brings harm to a computer system.

HACKING

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources.

NATURAL DISASTER

Natural disasters can cause great damage on the environment, property, wildlife and human health. (Earthquakes, flood, tsunami, tornado etc)

THEFT

Referring to identity theft. It is a crime in which an imposter obtains key pieces of personally identifiable information such as security.

SECURITY THREATS

SOURCES OF SECURITY THREAT

- There are four sources types of security threats :
    - External threats
    - Internal threats
    - Unstructured threats
    - Structured threats

SECURITY THREATS

External threats

Threats come from individuals or organization who works outside of a company and does not have any authorize access to the company system or network

Internal threats

Occur when someone has authorized access to the network with either an account on a server or physical access to the network.

Unstructured threats

One created by an inexperienced person who is trying to gain access to your network , a wannabe hacker.

Structured threats

Implemented by a technically skilled person who is trying gain access to your network.

METHODS OF SECURITY THREATS

VARIOUS TYPES OF SECURITY ATTACK

DENIAL OF SERIAL (DOS)

DDOS - DISTRUBUTE DOS

RECONNAISSANCE ATTACK

MALICIOUS ATTACK

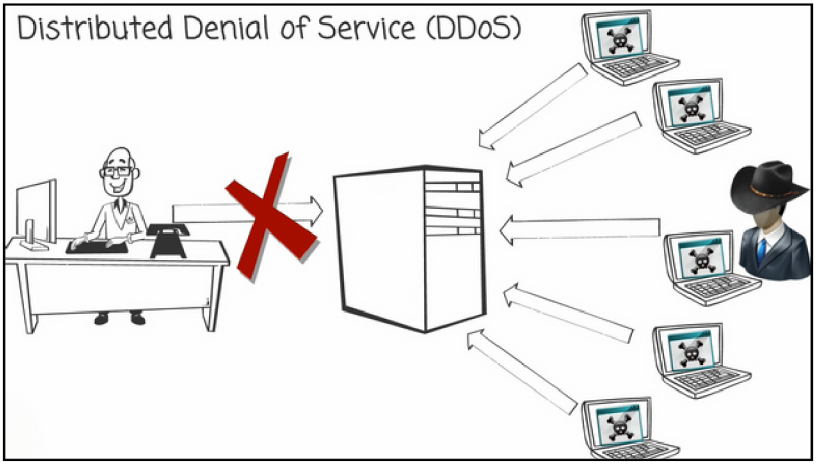
ACCESS ATTACK

METHODS OF SECURITY THREATS

VARIOUS TYPES OF SECURITY ATTACK

DENIAL OF SERIAL (DOS)

- DoS attack is a network attack and attempt to compromise the availability of a network, host or application.
- There are two major reasons a DoS attack :
  - A host or application fails to handle an unexpected condition.
  - A network, host or application is unable to handle an enormous quantity of data

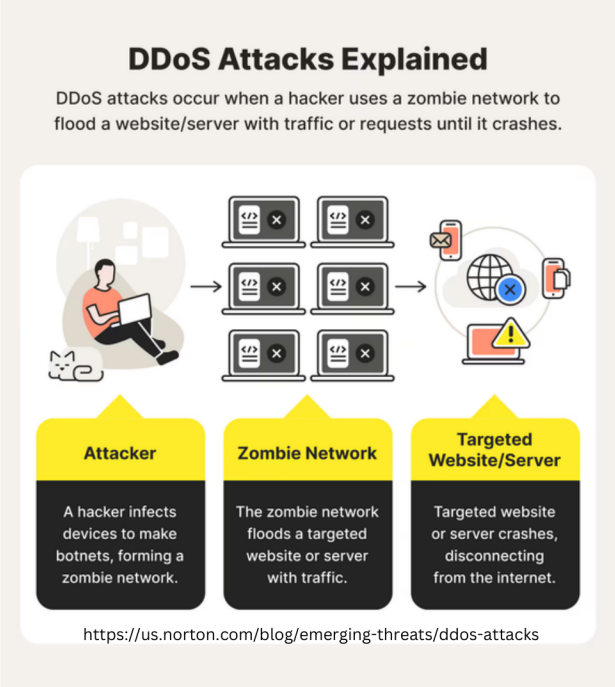


METHODS OF SECURITY THREATS

VARIOUS TYPES OF SECURITY ATTACK

DDOS - DISTRUBUTE DOS

- DoS attack is a network attack and attempt to compromise the availability of a network, host or application.
- There are two major reasons a DoS attack :
  - A host or application fails to handle an unexpected condition.
  - A network, host or application is unable to handle an enormous quantity of data



https://us.norton.com/blog/emerging-threats/ddos-attacks

METHODS OF SECURITY THREATS

VARIOUS TYPES OF SECURITY ATTACK

RECONNAISSANCE ATTACK

- Reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities.
- Also known as information gathering is the unauthorized discover of system, services or vulnerabilities.
- There are two types of reconnaissance attacks : active and passive.

ACTIVE RECONNAISSANCE

- Social Engineering
- Active Footprinting
- Port Scanning

PASSIVE RECONNAISSANCE

- Open Source Intelligence
- Passive Footprinting

METHODS OF SECURITY THREATS

VARIOUS TYPES OF SECURITY ATTACK

ACCESS ATTACK

- An attempt to access another user account or network device through improper means. If proper security measures are not in place, the network may be left vulnerable to intrusion .
- Gathering network data : Packet sniffer (network monitors), Ping sweeps, Port Scans, Information queries.
- Commonly of access attacks : man-in-the-middle, password attack, buffer overflow, port redirection.

METHODS OF SECURITY THREATS

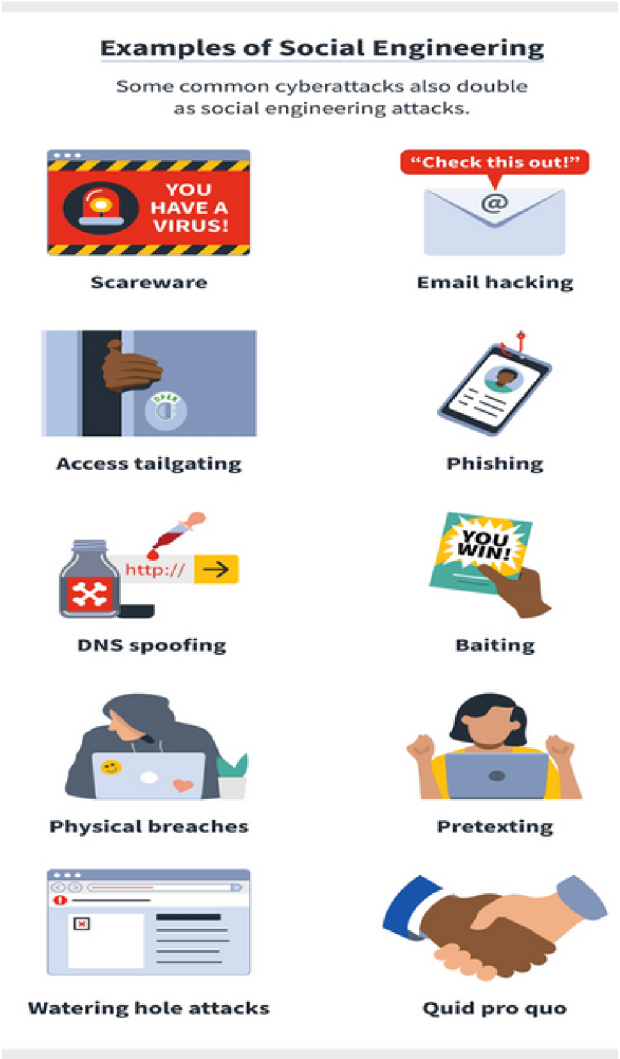
METHODS OF SECURITY THREATS

SOCIAL ENGINEERING

- Social engineering is the manipulation of people into performing actions or divulging confidential information.
- Social engineers often rely on people's willingness to be helpful but also prey on their weakness.
- Types of social engineering : Phishing, Pretexting, Vishing, SPAM, Baiting
- Social engineering is often used in conjunction with other network attacks.

METHODS OF SECURITY THREATS

METHODS OF SECURITY THREATS



METHODS OF SECURITY THREATS

PHISHING

- An attacker sends fraudulent email disguised as being from a trusted source

PRETEXTING

- An attacker pretends to need personal data in order to confirm the identity of the recipient.

BAITING

- An attacker leaves a malware infected flash drive in a public location.

SPAM

- Unsolicited email which often contains harmful links, malware, or deceptive content.

SCAREWARE

- Malware that's meant to scare you to take action — and take action fast. It often comes in the form of pop-ups or emails indicating you need to "act now" to get rid of viruses or malware on your device.

ACCESS TAILGATING

- Known as piggybacking, access tailgating is when a social engineer physically trails or follows an authorized individual into an area they do not have access to.

METHODS OF SECURITY THREATS

BECOME A SOCIAL ENGINEERING VICTIM

Follow these tips to avoid social engineering attacks.

1	Don't click links you don't request.
2	Don't overshare personal information online.
3	Be cautious of online-only friendships.
4	Remember the signs of social engineering.
5	Acknowledge what's too good to be true.
6	Use two-factor authentication.
7	Only use strong, unique passwords and change them often.
8	Consider a password manager.
9	Set high spam filters.
10	Don't allow strangers on your Wi-Fi network.
11	Use a VPN.
12	Monitor your account activity closely.
13	Don't leave devices unattended.
14	Use cybersecurity software.
15	Keep your software up to date.

VARIOUS TOOLS IN INFORMATION SECURITY

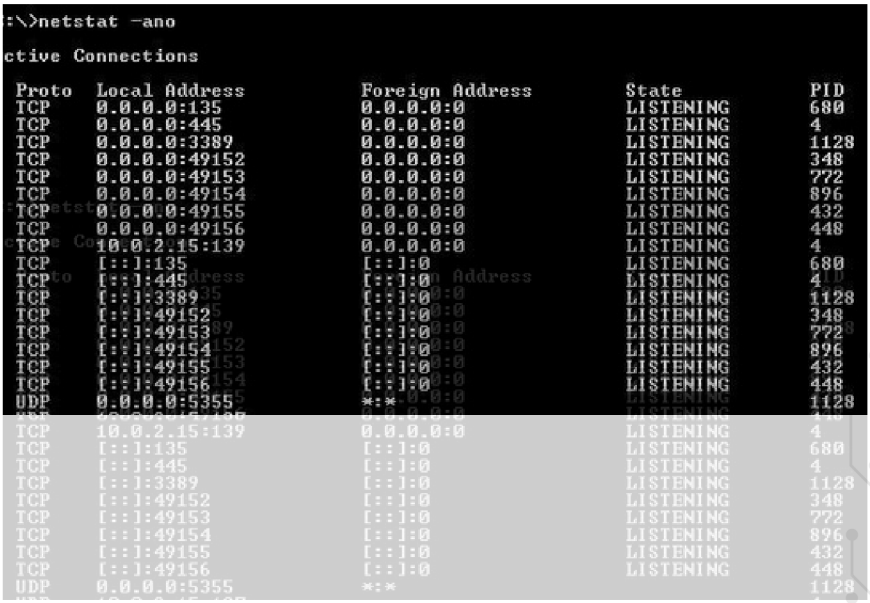
NETSCAN

- NetScans are processes to look for and automatically discover devices in your network
- NetScans streamline the process of adding devices which helps ensure your entire environment is properly monitored.
- When a device is discovered, you can specify criteria that determines whether it will be added to monitoring (Reverse DNS, System nama, IP address)
- Netcan can use three methods for discovering devices : ICMP (ping), Script, AWS scan

VARIOUS TOOLS IN INFORMATION SECURITY

NETSTAT

- Meaning network statistics
- Command Prompt command used to display very detailed information about how your computer is communicating with other computers or network devices.
- How details about individual network connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues



```
:\>netstat -ano

ctive Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       680
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1128
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       348
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       896
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       448
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       680
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       1128
  TCP    [::]:49152             [::]:0                 LISTENING       348
  TCP    [::]:49153             [::]:0                 LISTENING       772
  TCP    [::]:49154             [::]:0                 LISTENING       896
  TCP    [::]:49155             [::]:0                 LISTENING       432
  TCP    [::]:49156             [::]:0                 LISTENING       448
  UDP    0.0.0.0:5355           *:*                                    1128
```

VARIOUS TOOLS IN INFORMATION SECURITY

Nmap

- It's a free and open source tool used for vulnerability checking, port scanning and, of course, network mapping.
- Because of its flexible, open source code base, it can be modified to work within most customized or heavily specialized environments.
- There are distributions of Nmap specific to Windows, Mac and Linux environments, but Nmap also supports less popular or older operating systems like Solaris, AIX or AmigaOS. The source code is available in C, C++, Perl and Python.

SHOW ACCESS TO DATA & EQUIPMENT

Data Wiping

- Data wiping is the process of logically removing data form a read/write medium so that it can longer be read.
- Performed externally by physically connecting storage media to a hardware bulk-wiping device, or internally by booting a PC form a CD or network, it is nondestructive process that enables the medium to be safely reused without loss of storage capacity or leakage of data.

Hard Drive Destruction

- Data destruction is the process of destroying stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.
- Computers are essential part of securing confidential information like employee records, financials, proprietary documents and health data, but there comes a time when this information trail must end.

SHOW ACCESS TO DATA & EQUIPMENT

Hard Drive Recycling

- Recycling is considered environmentally friendly because it prevents hazardous waste, including heavy metals and carcinogens from entering the atmosphere, landfill or waterways.

- Computer recycling, electronic recycling or e-waste is the disassembly and separation of components and raw materials of waste electronics.

questions

answer

Q&A

1. Define the meaning of information security.

2. Identify the goal of security that involves prevention of unauthorized access of information or resources.

3. Determine the type of threat that occurs when untrusted employee is working on the system database in the company's network?

4. List FOUR (4) types of security threats.

5. Mr. Rizal is a new hacker and lack of experience. He only uses easily available hacking tools such as shell scripts and password crackers. Identify the type of threat done by Mr. Rizal.

Click for Answer

INTRODUCTION TO SECURITY BASIC

e ISBN 978-967-2240-52-5

POLITEKNIK KUALA TERENGGANU

(online)