Understanding on Malicious Attacks & Threats

Assignment - 1

19CSE311 – Computer Security

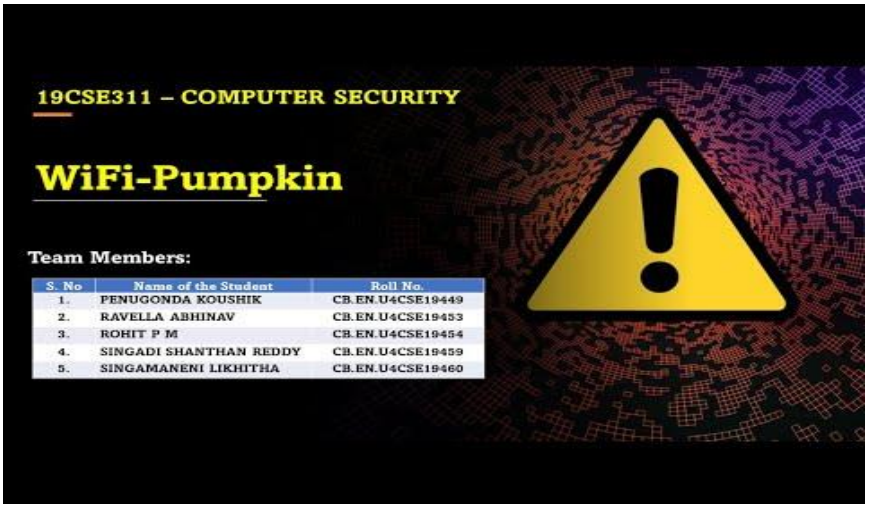
Date: *February 09, 2022*

Team Members:

S. No	Name of the Student	Roll No.
1.	PENUGONDA KOUSHIK	CB.EN.U4CSE19449
2.	RAVELLA ABHINAV	CB.EN.U4CSE19453
3.	ROHIT P M	CB.EN.U4CSE19454
4.	SINGADI SHANTHAN REDDY	CB.EN.U4CSE19459
5.	SINGAMANENI LIKHITHA	CB.EN.U4CSE19460

Real World Example – WiFi-Pumpkin

Video Link:

- 

1. Understand malicious code and analyse its impact on system infrastructure

- R. ABHINAV
- CB.EN.U4CSE19453

Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses.

- **Viruses** have the ability to damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages.
- **Worms** are a type of virus that self-propagates from computer to computer.
- **Trojan Horses** are computer programs that are hiding a virus or a potentially damaging program.
- **Malicious data files** are non-executable files—such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file—that exploits weaknesses in the software program used to open it.

What Can Malicious Software Do to A Computer?
The risk of malware is by no means limited to the computer. Any device which is capable of connecting to the internet might potentially be infected. Once infected, all sorts of bad things might happen.

Malware can allow someone else to take control of your computer/device. This might include the installation of programs, the changing of settings or passwords, or the theft of intellectual property (among other things). Anything that you put on the computer will be accessible to the one who controls the malware.

- **Ransomware Attacks:** used to lock people out of their computer systems.
- **Keyloggers:** It spies on your computer and records every keystroke that is made

2. Various types of Intruders:

- P.KOUSHIK
- CB.EN.U4CSE19449

One of the two most publicized threats to security is the intruder often referred to as a hacker or cracker. Intruders are the attackers who attempt to breach the security of a network. They attack the network in order to get unauthorized access. Intruders are of three types, namely, masquerader, misfeasor and clandestine user.

• A **masquerader** can be an attacker who succeeds in stealing a legitimate user's identity and impersonates the legitimate user for malicious purposes. For example, once a masquerader steals a bank customer's commercial identity including credit card and/or account information, the masquerader presents that information for the malicious purpose of using the customer's credit line to steal money.

• **Misfeasor** is a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges

• **Clandestine user** is an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

Some of the examples of intrusion attempts are:
. Attempts to copy the password file at a rate exceedingly once every other day.
. Suspicious remote procedure call (RPC) request at a rate exceedingly once per week.
. attempts to connect to non-existent bait machines at least every two weeks.

3. Identify attack strategies of different intruders

- **Rohit P M**
- **CB.EN.U4CSE19454**

- **Asymmetric Routing**
  In this method, the attacker attempts to utilize more than one route to the targeted network device. The idea is to have the overall attack evade detection by having a significant portion of the offending packets bypass certain network segments and their network intrusion sensors.
- **Buffer Overflow Attacks**
  This approach attempts to overwrite specific sections of computer memory within a network, replacing normal data in those memory locations with a set of commands that will later be executed as part of the attack. In most cases, the goal is to initiate a denial of service (DoS) situation, or to set up a channel through which the attacker can gain remote access to the network.
- **Common Gateway Interface Scripts**
  The Common Gateway Interface (CGI) is routinely used in networks to support interaction between servers and clients on the Web. Provides easy openings which attackers can access to secure network system files. When systems fail to include input verification or check for backtrack characters, a covert CGI script can easily add the directory label ".." or the pipe "|" character to any file path name and thereby access files that should not be available via the Web.
- **Protocol-Specific Attacks**
  Network intrusions via protocol impersonation ("spoofing") or malformed protocol messages. For example, Address Resolution Protocol (ARP) does not perform authentication on messages, allowing attackers to execute "man-in-the-middle" attacks. Protocol-specific attacks can easily compromise or even crash targeted devices on a network.
- **Traffic Flooding**

An ingenious method of network intrusion simply targets network intrusion detection systems by creating traffic loads too heavy for the system to adequately screen. In the resulting congested and chaotic network environment, attackers can sometimes execute an undetected attack and even trigger an undetected "fail-open" condition.

- **Trojans**

These programs present themselves as benign and do not replicate like a virus or a worm. Instead, they instigate DoS attacks, erase stored data, or open channels to permit system control by outside attackers. Trojans can be introduced into a network from unsuspected online archives and file repositories, most particularly including peer-to-peer file exchanges.

- **Worms**

A common form of standalone computer virus, worms are any computer code intended to replicate itself without altering authorized program files. Once these attack vectors are thoroughly understood, network security teams can look for opportunities to deploy technologies and strategies that will mitigate the potential effectiveness of each one.

4. Identify and analyse the various error detection mechanisms

- **S. SHANTHAN REDDY**
- **CB.EN.U4CSE19459**

Detecting malware on a system can be difficult. Organizations should perform threat mitigation to detect and stop malware before it can affect its targets. There are a few error detection and a few prevention techniques like:

- **Antivirus:**

Antivirus software is the most commonly used technical control for malware threat mitigation. There are many brands of antivirus software, with most providing similar protection.

- **Firewall:**

A network firewall is a device deployed between networks to restrict which types of traffic can pass from one network to another. A host-based firewall is a piece of software running on a single host that can restrict incoming and outgoing network activity for that host only. Both types of firewalls can be useful for preventing malware incidents. Organizations should configure their firewalls with deny by default rulesets, meaning that the firewalls deny all incoming traffic that is not expressly permitted.

- **Sandboxing**

Sandboxing refers to a security model where applications are run within a sandbox a controlled environment that restricts what operations the applications can perform and that isolates them from other applications running on the same host. In a sandbox security model, typically only authorized “safe” operations may be performed within the sandbox.

- **Browser Separation:**

Multiple brands of Web browsers can be installed on a single host. Accessing Web sites containing malicious content is one of the most common ways for hosts to be attacked, such as malicious plug-ins being installed within a browser. To reduce the impact of such attacks, users can use one brand of browser for corporate applications and another brand of browser for all

other website access. This separates the sensitive corporate data within one browser from the data within the other browser, providing better protection for the corporate data and reducing the likelihood that malware encountered during general web browsing will affect corporate applications.

5. Identify and analyse the various error correction mechanisms

- **S.LIKHITHA**
- **CB.EN.U4CSE19460**

The incident response process has four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Some major recommendations for malware incident handling, by phase or subphase, are as follows:

Preparation:

- Building and maintaining malware-related skills within the incident response team. And also By Facilitating communication and coordination throughout the organization.
- Acquiring the necessary tools (hardware and software) and resources to assist in malware incident handling

Detection and Analysis: Analysing any suspected malware incident and validating that malware is the cause. This includes identifying characteristics of the malware activity by examining detection sources, such as antivirus software, intrusion prevention systems, and security information and event management (SIEM) technologies, so that the hosts can undergo the appropriate containment, eradication, and recovery actions. Identifying infected hosts is often complicated by the dynamic nature of malware and computing

Eradication: The primary goal of eradication is to remove malware from infected hosts. Organizations should be prepared to use various combinations of eradication techniques simultaneously for different situations and also consider performing awareness activities that set expectations for eradication and recovery efforts; these activities can be helpful in reducing the stress that major malware incidents can cause.

Post-Incident Activity: Because the handling of malware incidents can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring. Capturing the lessons learned from the handling of such incidents should help an organization improve its incident handling capability and malware defences, including identifying needed changes to security policy, software configurations, and malware detection and prevention software deployments.