**Homework #5 Answers**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, April 7th prior to class (11:59 PM)

**Homework #5 is focused on Chapter 6 and Chapter 7. There are 10 total questions all worth 10 points each (100 pts total).**

**Chapter 6 – Malicious Software**

1. What are three broad mechanisms that malware can use to propagate?

* Infection of existing executable or interpreted content by viruses that is subsequently spread to other systems;
* Exploit of software vulnerabilities either locally or over a network by worms or drive-by-downloads to allow the malware to replicate; and
* Social engineering attacks that convince users to bypass security mechanisms to install trojans, or to respond to phishing attacks.

1. What are four broad categories of payloads that malware may carry?
   * Corruption of system or data files;
   * Theft of service in order to make the system a zombie agent of attack as part of a botnet;
   * Theft of information from the system, especially of logins, passwords, or other personal details by keylogging or spyware programs; and
   * Stealthing where the malware hides its presence on the system from attempts to detect and block it.
2. What are typical phases of operation of a virus or worm?
   * A dormant phase (when the virus is idle),
   * A propagation phase (where it makes copies of itself elsewhere),
   * A triggering phase (when activated), and
   * An execution phase (to perform some target function)
3. Describe some malware countermeasure elements.
   * **Prevention** in not allowing malware to get into the system in the first place, or blocking its ability to modify the system, via policy, awareness, vulnerability mitigation and threat mitigation;
   * **Detection** to determine that it has occurred and locate the malware;
   * **Identification** to identify the specific malware that has infected the system; and
   * **Removal** to remove all traces of malware virus from all infected systems so that it cannot spread further.
4. Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms discussed in this chapter could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

The found USB memory stick may pose a range of threats to the confidentiality, integrity, and availability of the work system. Each of the malware propagation mechanisms discuss in the chapter could use such a memory stick for transport. It may carry a program infected with an executable virus, or document infected with a macro virus, which if run or opened can allow the virus to run and spread. It could carry a malicious worm that may be run automatically using the autorun capability, or by exploiting some vulnerability when the USB stick is viewed. Or it could contain a trojan horse program or file that would threaten the system if installed or allowed to run.

You can mitigate these threats and try to safely determine the contents of the memory stick, by scanning the memory stick with suitable, up-to-date anti-virus software for any signs of malware – though this will not detect unknown, zero-day exploits. You could examine the memory stick in a controlled environment, such as a live-boot Linux or other system, or in some emulation environment, which cannot be changed even if the malware does manage to run.

**Chapter 7 – Denial-of-Service Attacks**

1. Define a *denial-of-service (DoS) attack*.

A **denial of service** (DoS) attack is an action that prevents or impairs

the authorized use of networks, systems, or applications by exhausting

resources such as central processing units (CPU), memory, bandwidth, and disk space.

1. Define a *distributed denial-of-service (DDoS) attack*.

A distributed denial of service (DDoS) attack uses multiple attacking

systems, often using compromised user workstations or PC’s. Large

collections of such systems under the control of one attacker can be

created, collectively forming a “botnet”. By using multiple systems, the

attacker can significantly scale up the volume of traffic that can be

generated. Also by directing the attack through intermediaries, the

attacker is further distanced from the target, and significantly harder to locate and identify.

1. List three common *flooding attacks* and describe each.

(1) ICMP Flood – The ping flood using ICMP echo request packets

(2) UDP Flood – Leverages UDP packets directed to some port number, and hence potential service, on the target system.

(3) TCP SYN Flood – Leverages TCP packets directed to a target system. Most likely leveraging normal TCP connection requests, with either real or spoofed source addresses.

1. Define a *reflection attack* as well as an *amplification attack*.

In a reflection attack, the attacker sends a network packet with a

spoofed source address to a service running on some network server,

that responds to the spoofed source address that belongs to the actual

attack target. If the attacker sends a number of such spoofed requests

to a number of servers, the resulting flood of responses can overwhelm

the target’s network link. The fact that normal server systems are being

used as intermediaries, and that their handling of the packets is entirely

conventional, means these attacks can be easier to deploy, and harder to trace back to the actual attacker.

An amplification attack involves sending packets to intermediaries with

a spoofed source address for the target system. They differ in

generating multiple response packets for each original packet sent,

typically by directing the original request to the broadcast address for

some network. Alternatively they use a service, often DNS, that can

generate a much larger response packet than the original request.

1. In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5-Mbps link? How many per second if the attacker uses a 2-Mbps link? Or a 10-Mbps link?

In a DoS attack using ICMP Echo Request (ping) packets 500 bytes in

size, to flood a target organization using a 0.5 Megabit per second

(Mbps) link the attacker needs 500000 / (500 × 8) = 125 packets per

second. On a 2-Mbps link its 2000000 / (500 × 8) = 500 packets per

second. On a 10-Mbps link its 10000000 / (500 × 8) = 2500 packets per

second.