# Network Threats Analysis Worksheet

## Instructions

Complete all sections of this worksheet thoughtfully and thoroughly. Use your own words and provide specific examples where appropriate. Each response should demonstrate your understanding of the key concepts from the assigned reading. Citations should be completing in APA format.

### Section 1: Chapter Summaries (10 points)

#### 1.1 Network Threats (Chapter 2) Summary

**Instructions:** Summarize Chapter 2 in your own words. Your summary should cover the main themes, key concepts, and important points discussed in the chapter. Do not copy directly from the text.

**Response:** Chapter 2 covers network threats, specifically Threat Actors, what tools they might use, and different kinds of malware that might be used on endpoints & servers to achieve specific goals. Additionally, it covers common attacks that Threat Actors might use like reconnaissance, social engineering and more. It also covers different types of attacks like DoS, Buffer Overflow and more.

#### 1.2 Mitigating Threats (Chapter 3) Summary

**Instructions:** Summarize Chapter 3 in your own words. Your summary should cover the main themes, key concepts, and important points discussed in the chapter. Do not copy directly from the text.

**Response:** Chapter 3 covers ways to defend the network ranging from physical security to policy control, other mitigation efforts to ensure that AAA is upheld and more. It mentions attacker tools which can be used to investigate the standing of an organization, like password crackers and more. Additionally, it mentions tools like SIEMs which make identifying attacks much easier. It also mentions ways to mitigate specific attacks which might arise like Malware, Worms, Reconnaissance Attacks, Access Attacks, DoS Attacks.

### Section 2: Learning Reflection (10 points)

#### 2.1 Key Learning

**Instructions:** Discuss something significant you learned from reading Chapters 2 and 3. This could be a concept that was new to you, something that changed your perspective, or information that connected to your personal or professional experience. Provide a thoughtful analysis.

**Response:** I found the four risk strategies the most interesting, since GRC is one of the areas of expertise that I’ve really overlooked, the whole idea of posturing your decision making as an organization towards of the goals (Acceptance, Avoidance, Reduction, Transfer). A personal anecdote but I do feel that a lot of companies, especially smaller companies are towards the Acceptance level of risk management, that’s why small clinics and law offices are so easily targeted, they just don’t do anything about cybersecurity and pay deeply for it.

### Section 3: Threat Analysis (25 points)

#### 3.1 Selected Threats/Attacks

**Instructions:** From the threats and attacks discussed in Chapter 2, select THREE (3) that you find most relevant or concerning. For each threat/attack, provide a detailed explanation of how it works.

**#1:** Worms, these are pieces of malware that work but initially being run by a user somewhere or the spring is wound by an attacker, which then jumps from machine to machine without the involvement of a human, often abusing a RCE vulnerability in an operating system or program. These are the scariest out of the list because they can cause the most damage if the stars align for the attacker.

**#2:** Eavesdropping, I find this one interesting since it’s quite antiquated, I mean this was a point of attack even before the computers became the main means of communication for people around the world. Think of the Nixon & Watergate, wiretapping & the US government go hand in hand. It makes me think though, with Edward Snowden and the NSA scandal being put under such public light, we now have TLS on near every communication end and most chat apps advertise end to end encryption, but do we really know we can trust that someone isn’t listening in on the line?

Conspiracy theories besides, eavesdropping works by capturing packet traffic on a network and storing it somewhere, ideally in a way that the victim can’t identify that it’s even happening. For example, ARP poisoning could route all internet traffic through an attack box which if on a sufficiently insecure network could lead to it being undetectable by a victim.

**#3:** Phishing, one of the most popular attack vectors and permanent vexer of grandma’s bank accounts everywhere. This works by good old talking to people, imagine a salesman with malicious purposes. Often the element of urgency leads to results that are favorable for the attacker, call with a screaming baby in the background or a last-minute deadline that needs to be submitted now. Appear confident and most people won’t even notice the dupe taking place.

### Section 4: Mitigation Strategies (25 points)

#### 4.1 Defense Techniques

**Instructions:** For each of the three threats/attacks you selected above, discuss specific techniques that can be used to mitigate or defend against them. Consider both technical solutions and policy/procedural approaches.

**#1:** The best line of defense against worms unfortunately is the best for most software-based attacks, PATCH YOUR SYSTEMS, being up to date will be the best action you can take against worms, they thrive best on legacy systems that sit in a doctor’s office, running windows XP for over a decade.

**#2:** Encryption! Use SSL/TLS, chat apps with End-to-End Encryption, use up to date hashing algorithms to ensure that all traffic is encrypted before leaving your computer. This is the best option you have against attackers. You can browse easy on that café Wi-Fi knowing that your data *should* be safe!

**#3:** Training and policy control, make sure that people are aware of emails that will steal their passwords or random repair companies that just need that email address or website to get their paperwork filled out. Making sure that important information and decisions must be filtered through multiple people or have some sort of process makes pulling off a phishing attack far harder as well.

### Section 5: Critical Thinking (30 points)

#### 5.1 Real-World Application

**Instructions:** Choose one of the threats you discussed and research a recent real-world example of this type of attack. Briefly describe the incident and analyze whether the mitigation strategies you suggested could have prevented or reduced the impact of the attack.

**Response:** I’m choosing Worms, these are the most fascinating vulnerability IMO, they are essentially the equivalent of a nuclear bomb in IT, when one goes off in the right place at the right time it’s often devastating and hard to watch, but also morbidly interesting. The most known worm in current times would be the WANNACRY virus, which was a worm developed by North Korea and acted as ransomware, among the many RCE vulnerabilities it abused was EternalBlue which abused the SMBv1 protocol in older versions of Windows 7. At the time of attack, 2017, WANNACRY was poised to destroy a LOT of infrastructure and it did just that, devastating entire hospitals, police departments, and offices. It’s estimated that over 200,000 computers were affected globally. Ransomware, by its very nature, encrypts the disk and requests payment for recovery. In a messed up move by North Korea they never bothered to verify if their decryption code even worked, leading to any computer being targeted by WANNACRY having any data stored on their computer being completely unrecoverable.

**References**