Part I

1. Select five (5) malwares from the following: Spyware, Adware, Rootkit, Ransomeware, Worm, Trojan Horse, or Backdoor

   Rootkit

2. Search two (2) examples for each of the five malware you have selected. Add a short description for each. Cite your reference. (5 points per example)

   First, we have a **backdoor rootkit.** Where the attacker has an unauthorized access to the victim's computer system. To add on, it is often installed by the attackers who has already accessed the system, in which they can steal the data, install other malware or even could take control of it.

   Moreover, the second is, **Bootkit rootkits**. This rootkit infects the computer's boot loaders (responsible for loading the Operating System when the device boots up). So, with this, the bootkit rootkits prevents this from loading properly. Whereas, this gives the attacker an absolute control to the system.

Part II

1. Search for an article regarding a cybersecurity attack using malware. The article should be published within the last 5 years by a credible source.
2. Answer the following items based on the article you found.

   a. What is the title of the article? (3 points)

   THE WANNACRY RAMSOMWARE ATTACK WAS TEMPORARILY HALTED. BUT IT'S NOT OVER YET

   b. Who wrote the article? (3 points)

   Timothty B. Lee

   c. When was the article published? (2 points)

   May 15, 2017

d. Give the link where you found the article. (2 points)

https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp

e. Is it possible to prevent this kind of attack? How? (Essay: 15 points)

Yes, indeed it is still possible. Here are some common ways:

1. **Keep your software updated** – WannaCry mostly attack the vulnerability of the older Windows versions. In which also, Windows provided a patch to fix this vulnerability.
2. **Use Firewall** – this block all of the malicious traffic.
3. **Back up data regularly**
4. **Be careful what you click**
5. **Use antivirus software**

f. How extensive was the impact of the attack to the environment where it happened? (Essay: 15 points)

The wannacry ransomware was indeed a global cyberattack. In which it attacks the vulnerability of the Windows and use it to spread. Moreover, the infected computers were over **200, 000 in 150 countries.**

However, though the Windows fixes the problem and provided a patch to fix the problem. Still it is still existing. This attack was happened last **May 12, 2017**.

g. How did the person/company, who was attacked, cope with the consequences and effects of the incident? (Essay: 15 points)

The Windows indeed fixes the problem and solve how to prepare for the future attacks such as this. Moreover, the Windows provided a patch to their own system's vulnerability in which the wannacry used to spread the malware to the entire internet. This also notifies that all of the Windows user to update their system where the patch was attached.