

King Saud University College of Computer and Information Sciences Computer Science Department		
CSC 429: Computer Security	Homework# 1	1 st Semester, 1446 – Fall, 2024

Question 1:

Below are hashes for three malware samples, each from a different category. Use [VirusTotal](#) to search each hash and identify the malware type and name:

- Hash 1: 44d88612fea8a8f36de82e1278abb02f
- Hash 2: 7e5e1f837189e5127aa86e0a834fe8f1e55c57c7
- Hash 3: dccfb092fa979fb51c8c8ca64368a6f43349e41d

Question 2:

For each malware sample, answer the following questions based on your VirusTotal findings:

1. **Detection Ratio:** What is the detection ratio for each malware? Why is this ratio significant in understanding the risk of the malware?
2. **Aliases:** What are some of the names or aliases that different antivirus engines use to identify this malware? Why do antivirus engines use multiple names for the same malware?
3. **File Behavior:** Summarize any observed file behaviors or network activity associated with the malware. List two specific actions or indicators that suggest malicious behavior.
4. **Mitigation Techniques:** Based on the VirusTotal report, recommend one mitigation or prevention strategy that could protect a system from this type of malware.

Question 3:

Reflect on the differences between the malware categories (virus, trojan, worm) based on your analysis. Discuss how the distinct characteristics of each type might influence the approach to securing a network or system against them.

Note:

- Due date to submit the assignment is **SATURDAY 16-Nov-2024 at 11:59 pm.**
- Form a group of **3 students** for the assignment. One submission per group. Students who do not contribute to the assignment will receive **ZERO**.
- Upload your assignment to LMS.
- Your assignment **MUST** be in **PDF** format.
- Name your assignment file: **Group#_HW1.pdf**