COSC 366: Introduction to Cybersecurity

Written Assignment 4 — Fall 2022

Ground Rules. Work must be typeset (not handwritten and scanned) and submitted by 23:59:59 of the due date. You do not need to provide code or visual diagrams for any question, but are welcome to if it helps you explain your answers.

1. Gathering Forensics Evidence. An adversary compromised the network of an enterprise software company by using a default user and password on an exposed database server web interface. From the database server, the adversary exploits a vulnerability in the software to gain a non-root shell, but exfiltrates all data from the database on that server using the web interface. Before destroying the evidence, the adversary scans the rest of the network, finds another vulnerable machine acting as a webserver, and pivots to that machine by exploiting a vulnerable SSH server on that machine. From there, the adversary uses their newfound root privileges to establish persistence by loading their code into the Windows registry. Once persistence is established, they remove their code from the filesystem, SSH back to the database server, and leave open a reverse tunnel from the webserver to their own Command-and-Control (C2) server on a machine in Amazon Web Services (AWS).

If you were working in the security operations center of this company, describe how you might find this adversary at different stages of their attacker process?

Hint: How could you detect at each phase of the process? Initial scanning to find the vulnerability? Exfiltration of the database data (maybe there are unusual traffic patterns associated with either of these)? Unusual communications with cloud servers? Etc...

2. Anonymity and Privacy. Answer the following questions (with 2-3 sentences each):

a) Define *unlinkability.*

b) Define *unobservabilty.*

c) Give an example of a system which provides both of these properties, and describe how it works at a high level. (Hint: You can use the Remailer or Tor system we discussed in class. If the system does not already provide these properties, include in your answer how to make them do so.)