Swasti Mishra
Stella Sun
COSC 366
6 December 2022

COSC 366 Writing Assignment 4

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?

   To begin with, an enterprise software company shouldn't have a default username and password, so this is a vulnerability that should be closed. Further, if the company used an automatic scanner, they would have been able to find and close the vulnerability in the software before the attack began. Also, there should have been some kind of throttling procedure to prevent an adversary from stealing a lot of information.

   If it is an Ubuntu server, a security operations person can use "w" to show who is logged on to a server and what they are doing. This will display information about the current system time, the length of time the system has been in up, how many users are logged in, the load averages, the name of the logged in user, the name of the terminal, the hostname or IP address they're from, what time they logged in, and information about the user's current processes and arguments. This is a lot of information, but much of the second half should flag as a warning sign for a professional.

2. **Anonymity and Privacy**
   a) Define unlinkability.
   Unlinkability is privacy property that protects users or "items" from being connected in the instances where they use a product or service. Essentially, even if a hacker can exploit a system to determine what packets of information contain, they cannot link which packets are related and to what users they are related to.

   b) Define unobservability.
   Unobservability is the amount of information that a hacker can piece together from watching external outputs. It is the software equivalent of a stakeout- some types of output traffic must be broadcast to the public just by virtue of the way that products are set up, but

it is up to these services to censor output data in a way that prevents hackers from understanding the internal systems enough to break in.

c) Give an example of a system which provides both of these properties and describe how it works at a high level.

Tor is an example of a browser that uses both unlinkability and (with modifications) unobservability. Tor wraps each of your packets in three layers of encryption, and then sends your data through nodes in its exclusive network. Each node can remove one layer of encryption, and by the third node, a packet is ready to enter the rest of the web, anonymized. This is because a malicious outside observer, for example, is unable to link a packet that was encrypted and passing through the first to second node to what could potentially be the same packet, passing through the second to third node. Even the Tor nodes are unaware of which packet is which. As for unobservability, some applications like SkypeMorph camouflage Tor traffic to look like a Skype video call, for example, instead of regular Tor traffic. This makes it so an outside actor cannot determine that a user is using the Tor browser to begin with.