The Economics of Cybersecurity — Lecture 13 Notes

Adam Hastings

April 16, 2024

1 Introduction: Types of Exploits

Let's clarify some terminology:

- **Bug** — unintended behavior. Could be a security issue, often times is not. Example:
- **Vulnerability** — A specific instance of a bug that has the potential to be exploited. Makes the device running the code vulnerable. Example: Memory safety violations, integer overflow, executing untrusted unsanitized input (e.g. SQL injection). *What is the name of the database that tracks vulnerabilities?* Technically the NVD (National Vulnerability Database — run by NIST!) is the *database*, but the entries are generally known by their *CVE* number (e.g. CVE-2021-44228).

1.0.1 Exploit

— Something that takes advantage of a vulnerability to achieve some goal. Important to note though that oftentimes there is a large gap between a vulnerability and an exploit! *Why?* A vulnerability can be thought of as a "foot in the door", but a vulnerability alone is rarely enough to do anything useful.

For example, let's say some web app

- **RCE** — *Remote Code Execution.* Attacker has the ability to execute code on the victim's device.
- **LPE** — *Local Privilege Escalation.*
- **RPE** — *Local Privilege Escalation.*
- **SBX** — *Sandbox Escape or Bypass. Can someone tell me what a sandbox is here in this case?*

1.1 Persistence

— Some types of malware may only be active for a few seconds or less; others may become malicious processes that inject themselve into memory and may try to hide themselves.

If a process exists only in memory and the machine is rebooted, what happens? The malware is gone. If the attacker was trying to spy on the user, or just keep the malware alive with the intention of doing something malicious later, then simply rebooting will remove this malicious process from the device.

Persistence is when the attacker has some way to retain access to the device even if the machine is rebooted. The malware persists.

Bug bounties will usually pay more for vulnerabilities that have persistence. *Why is it hard to gain persistence?*

2 Exploit Brokers

3