Activity 1 – CPSC 6200 – Rajat Sethi

1. I have explored the site.

2. CVE – Common Vulnerabilities and Exploits – A standard that logs exploits within all types of technology.

Ubuntu Examples:

* CVE-2015-5602: Unauthorized privilege escalation with “sudoedit” (Ubuntu 15.10)
* CVE-2015-8660: “Overlayfs” Local Privilege Escalation (Ubuntu 14.04 – 15.10)
* CVE-2016-4557: BPF Local Privilege Escalation (Ubuntu 16.04)

3. Buffer – A memory structure that temporarily stores data for future usage.

4. Buffer Overflow – Inserting malicious code into a buffer, then “overflowing” the buffer with return addresses that overwrite the original address and instead point to the malicious code.

5. Stack-Based BOF – Exploiting the stack structure that allocates memory to fixed-length buffer (like through an array with a declared size). Normally, these attacks are done by creating a payload of NOP sleds, malicious code, and the return address in one string.

6. Heap-Based BOF – Exploiting the heap structure that allocates memory to dynamic-length buffers (like through malloc). Normally, these attacks are done by manipulating command-line arguments with a return address and malicious code.