**Buffer Overflow**

* A stack is a collection of memory segments that allow a program or an OS to run. In a hierarchy, the components are “stacked,” ranging from highest in address value from highest to lowest, or lowest to highest.
* A return address is an address stored in an address in memory. When called, the address returns the program to the end of the subroutine.
* The user can make allocated buffer space at will. For example, a user can allocate a buffer for any variable type.
* Segmentation faults occur when a program attempts to read an address outside its allowed space.
* GDB stands for Gnu DeBugger. It is a low-level debugger that is used to execute code. Gnu is an OS at its core but has been adapted for other uses, such as GCC for Gnu C Compiler.
* A no-op sled is an attack for accessing data that is out of bounds. In the video, a no-op sled attack is used to access the root shell, which gives the user the ability to do whatever they want with the system.

**Code Red, SQL Slammer**

1. Code Red cost billions by the summer of 2001 and affected systems and networks on a large scale. SQL Slammer affected over 75k systems in less than 10 minutes but only caused slowdowns in internet speeds.
2. C and C++ are the languages most used for writing buffer exploits since their basic nature contains high vulnerability and has no protections against reading and writing data in memory.
3. Modern operating systems utilize runtime protection to protect against buffer overflows. Additionally, memory on the stack can be randomized to increase the security against buffer overflow attacks. Finally, bounds-checking can be enforced at run-time to prevent a buffer from being overrun and keeping it within its boundaries.

**Rootkit Demonstration**

1. Windows XP was used as the target machine because it contains vulnerabilities that can be exploited to get access to the operating system. It also does not have CL security features such as Linux or other operating systems.
2. The Beast program is a trojan horse program and can utilize the infected system to infect other nodes in the network.
3. Some FU operations allow the host user to see the programs being run on the victim machine and hide the rootkit process from the victim.
4. The Black Light security tool is different from the standard process list of Windows by allowing the user to identify registry keys and identify which processes are being hidden from the infected system. It also can clean and remove the rootkit from the system.