Activity 8: Part 2

Ryan Coon

CST-407

Professor Ty Howard

February 11, 2024

Operating Systems Security

a.Explain the terminology and how it relates to a buffer overflow exploit: (a) stack, (b) return address, (c) allocated buffer space, (d) segment fault, (e) GDB, and (f) no-op sled.

b.Code Red and SQL Slammer were events caused by a buffer overflow exploit. What was the result and cost of the attacks?

c.What languages are most often used for writing buffer exploits, and what do they have in common?

d.What are some operating system improvements that attempt to prevent intentional buffer overflow exploits?

e.Based on the associate resources, why was Windows XP used as a target machine?

f.What is the Beast program and what are its capabilities?

g.Explain how some of the command options in FU make this tool useful as a rootkit.

h.How is the Black Light security tool shown in the video different than the normal Process List utility of Windows?