Kieren Ng

4/7/2018

Homework 9

7.9

Reflection attack: “The attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system. When the intermediary responds, the response, the response is sent to the target. Effectively this reflects the attack off the intermediary, which is termed the reflector, and is why this is called a reflection attack.” (textbook)

7.10

“Amplification attacks are a variant of reflector attacks and also involve sending a packet with a spoofed source address for the target system to intermediaries.”

7.2

So there are 256 spots, and the system retries 5 times (6 times total, including the initial). There are 30 seconds between each, so 3 minutes per request spot. The attacker needs to fill all 256 spots, which all rotate out every 3 minutes, essentially. For 256 spots over 3 minutes, it’s 256/3 = 85 or 86 per minute. Since the packet is 40 bytes, it is 85.3 \* 40 bytes \* 8 (conversion to bits) / 60 seconds = 454.9 bits per second to continue the attack.

7.3

A 500 byte request \* 8 bits = 4000 bits, and the average uplink capacity is 128 kbps, so 128000 bits per second. 128000/4000 = 32 packets p second.

7.4

Again, 500 byte response \* 8 bits = 4000 bit response packet,

0.5 mbps \* 500 / 2 = 125 packets

2 mbps \* 500 / 2 = 500 packets

10 mbps \* 500 / 2 = 2500 packets

10.9

NOP sled is “a sequence of instructions meant to slide the CPU’s execution flow to its final, desired destination whenever the program branches to a memory address anywhere on the slide.” (Wikipedia)

With a NOP sled, the “attacker can exploit the fact that the code is often much smaller than the space available in the buffer. By placing the code near the end of the buffer, the attacker can pad the space before it with NOPs.” These instructions don’t do anything, so the attacker can specify the return address somewhere in the NOPs.

10.2

You can just replace gets(str2) with fgets(str2, 8)

10.3

You can just replace gets(inp) with fgets(inp,16,stdin);