CMSC 491 Assignment 3

Nicholas Harrison

For all of these exploits I assumed that 192.168.2.0 was the proxy address I was sending these packets to.

Firewall 1

This firewall is stateless, so it does not take into account if the packet is in fragments or not, so to get around this you simply have to divide the packet up, I split it into “you” and “tube” so the firewall sees those two words separately and does not block the packet. This can be fixed by using a stateful firewall.

Firewall2

This is a stateful firewall that combines the data from the packets and checks if it contains the forbidden statement. To get around this I added a third packet between “you” and “tube” so that when they are passed into the fire wall it sees you”what the second packet contains”tube, while the server itself only sees youtube allowing it to be accepted. To fix this, you need to check the whole data string to see if it contains parts of “youtube” that have been separated.

Firewall3

This is a stateful firewall that contains the solution from firewall2 where it looks at the packet data combined together and checks if it contains parts of “youtube.” Its exploit is that it only does this if the offset is less than 100. So you can get anything to pass as long as you set its offset to be higher than 100. To fix this you can add a check to limit the offset.

Firewall4

To make a secure firewall I took firewall 3 and made it so that it modded the offset so that it would always be less than 100, this way it accounts for the weaknesses in firewall1 and firewall2 and the offset exploit that existed in firewall3. Now none of the exploits will function and it will block the packet.