Assignment 4
Gunnar Yonker

1)

(A) If traceroute is not being blocked on a target network then this can provide useful information to the attacker. Since the attacker is able to use traceroute on the target network, they can use the information that the packets are reporting an expired TTL and being dropped, this means that the attack can increase the TTL of the packets until they reach the NIDS and only increasing the TTL of a few packets further to make it past the NIDS to the destination host. Since the NIDS would be analyzing the traffic, it would most likely send an alert if it detected a large amount of packets passing through as abnormal traffic, whereas if the attacker sent all the packets to the NIDS but not through, then only a few packets through the NIDS to the host, it would be less likely to trigger an alarm. An attacker can also evade detection through other methods such as using IP fragmentation so send partial packets rather than the whole packet at once being analyzed.

(B) Traceroute can be blocked on a target network if ping or ICMP reply responses are blocked by the target network. If the packet does not reply then the TTL Expired message will not be sent back to the attacker since that ICMP message would be blocked. This would lead to the probe timing out and you would not receive any information based on that hop and the TTL would be increased on the next traceroute command until the host was reached or 30 hops. If traceroute was blocked and you were not receiving the IP address on each hop, it would still be possible to launch a similar attack if the attacker was still able to determine the TTL for the packets to reach the NIDS and the TTL for the packets to get directly to the host. With traceroute being blocked, the attacker would receive less information, but it would still be possible to launch a similar attack. Pattern change evasion also is a method to bypass an intrusion detection system because it changes the user data during the attack so that no pattern is clearly evident to the detection system allowing that traffic to go unnoticed.

I know that traceroute can also be run with different modifying commands such as -T and -I, but I am unsure as to if those would help to launch a similar attack on a host. These can change the type of traceroute being run to an extent and depending on how traceroute is being blocked that it may still be possible to circumvent that block such as targeting a different port than what is typically expected.

(C) One big limitation of an intrusion detection system is that if there is a lot of traffic coming through, it is possible for there to be an increased number of false alarms. If there are a lot of false alarms, this can lead to the user ignoring or completely missing the real attacks. Many evasion techniques rely on the vulnerabilities of a specific version of software being used, if the intrusion prevention system is not being consistently updated then it can leave the system more vulnerable to certain evasion attacks targeting that version of software. The attacks are constantly changing which causes the software to continuously need updates. If the attacker is using a spoofed IP address in the packet, when it is detected, the system will know that there is abnormal traffic coming through but unless the IP address is accurate then the origin of the attack will remain unknown. A NIDS can also be brought down by attacks such as a TCP stack attack and then if the NIDS is down the traffic would be able to evade the system as it would not be currently running.

2) A firewall and a NIDS share some similarities and some differences. One of the main differences that I have found is that the main principle of a firewall is to filter traffic based on IP addresses and port numbers whereas a NIDS will detect real time traffic and look for patterns that would indicate an attack

that warrant an alert to be issued. This main principle also highlights the difference that firewalls do not analyze traffic patterns, but that a NIDS will analyze them. A firewall is used to filter incoming and outgoing traffic based on a ruleset that is set by the user when creating the goals of the firewall. An IPS is a device or software that monitors traffic and then sends out an alert when abnormal traffic is detected. This shows the difference that a firewall will filter and block traffic, but a NIDS will analyze traffic patterns to alert the user about a possible attack but not directly taking action to prevent the attack. Firewalls will actively block specified packets, but a NIDS will warn or generate alarms based on the traffic. This also means that a firewall does not need any user intervention to block packets once the rules are set, but with a NIDS, a user would have to respond to the threats that the system was detecting. One similarity is that both systems deal with traffic that is passing through the network system. Also both a firewall and a NIDS are designed to prevent an intrusion into the system by means of a destination host, and similarly both can be evaded/bypassed using a plethora of different methods.

3) Snort Rule:

(a) alert tcp any any -> 142.35.60.0/24 (msg:”External XMAS Tree Scan Detected”; flags:FPU; sid:1000006; rev:1;)

(b) alert icmp any any -> 143.35.60.0/24 any (msg:”Traceroute Detected”; dsize:0,sid:10000004; rev:1;)