

TNE30009 Tutorial Week 3

Question 1

1. What is the difference between a virus, a worm and a trojan?
2. Viruses and worms can be used to facilitate other attacks. Give two examples.
3. What is a 'social engineering' attack? Give an example.

Question 2

Consider a fragment of a rainbow table with the following characteristics:

start						end
111	aaa	122	bab	211	cbc	321
112	aab	212	bc b	123	cac	121
113	aac	311	acc	322	abb	332

The table is for three character passwords made up of the characters a, b and c, and maps to a three digit hash made up of the digits 1, 2, and 3.

1. What will the rainbow table actually consist of?
2. How might an attacker use the rainbow table to determine the password associated with a hash of 212? Go through the steps involved.
3. Why can't the attacker just use the inverse of the hash function to determine the password?
4. Why don't rainbow tables just include the reverse of every possible hash?

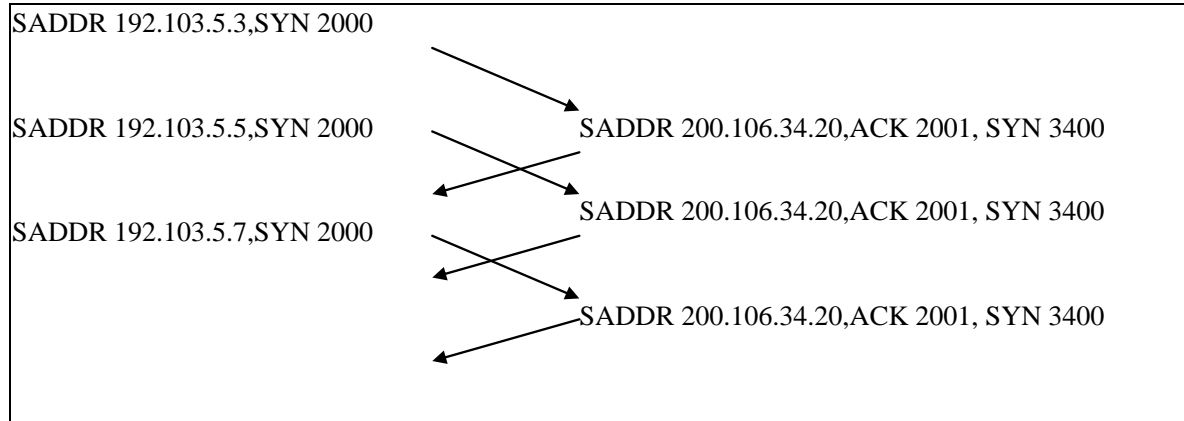
Question 3

Salting and multiple hashes are techniques for making rainbow table based attacks difficult. How do they achieve this?

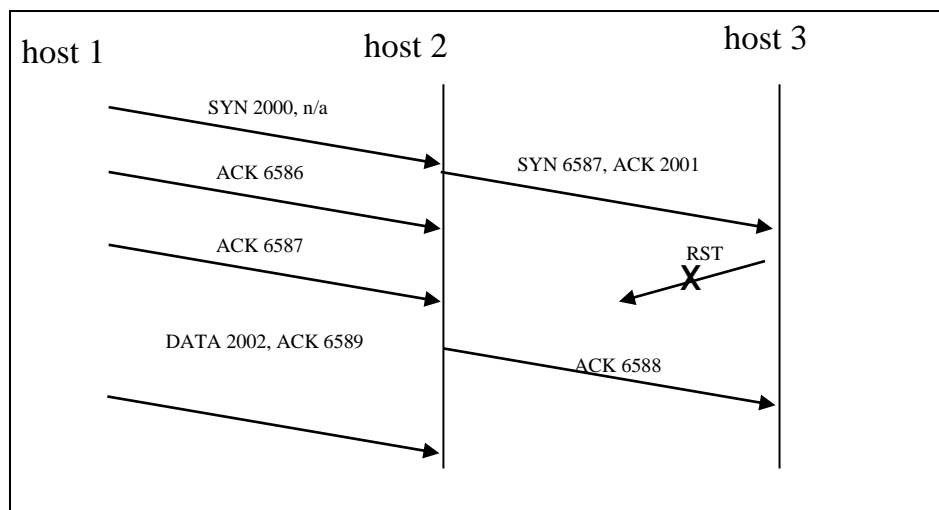
TNE30009 Tutorial Week 3

Question 4

1. What is the following attack? Which host is attacking and which is being attacked?

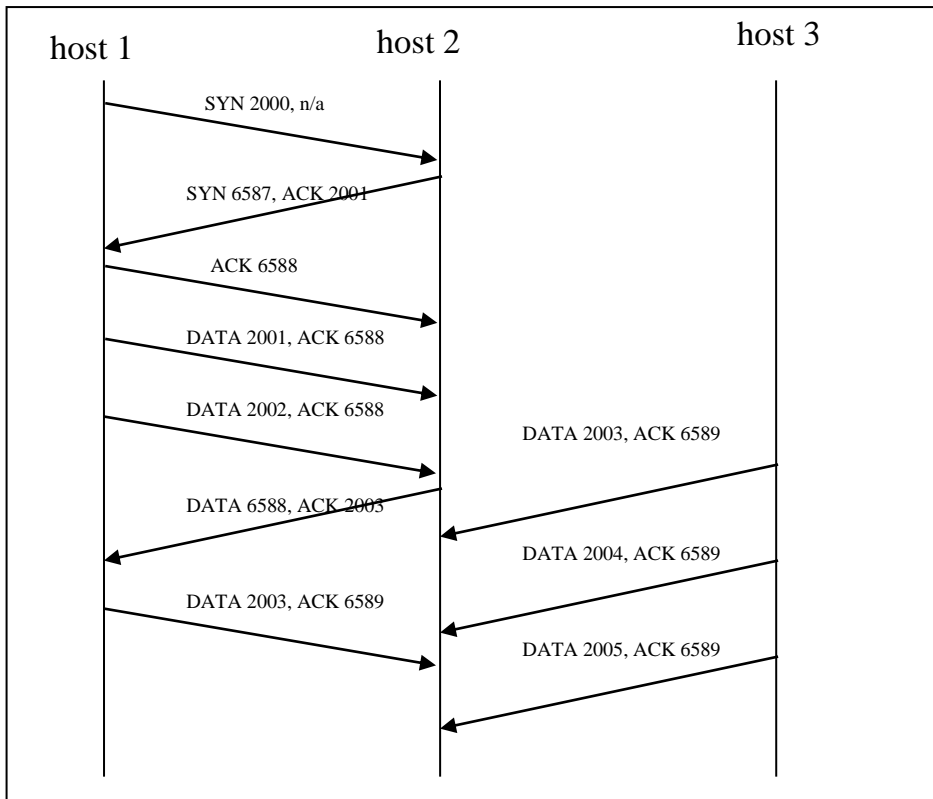


2. What attack is described in the following diagram? Which is the attack host, the target host and the spoofed host?



TNE30009 Tutorial Week 3

3. Identify the spoofed, target and attack hosts in the following diagram. What sort of attack is described in the diagram? (For simplicity we are assuming a 1 byte payload.)



4. In the above diagram, what will happen to DATA packet 2003 sent from host 1 to host 2? Why?
5. Draw a sequence diagram showing a TCP session hijack. The ISN of the spoofed host is 4500, of the target host 5000. The hijack occurs immediately after completion of the 3-way handshake.