TNE30009 Tutorial Week 3

Question 1

1. What is the difference between a virus, a worm and a Trojan?

A virus is attached to another program or file. It propagates when that file is opened or executed. A worm is a self-contained piece of code that does not need to be part of another program to propagate itself. A Trojan is a software system that masquerades as another program and is unwittingly installed by a user on their machine.

2. Viruses and worms can be used to facilitate other attacks. Give two examples.

Viruses have been used to attempt to steal the password file to enable a dictionary attack. Worms have been used to install backdoors for use in later Denial of Service attacks.

3. What is a 'social engineering' attack? Give an example.

A social engineering attack is the manipulation of a person to enable a system to be compromised. 'Phishing' is an example of a 'social engineering' attack.

Question 2

1. What will the rainbow table actually consist of?

start	end
111	321
112	121
113	332

2. How might an attacker use the rainbow table to determine the password associated with a hash of 212? Go through the steps involved.

   Apply reduction / hash functions repeatedly until a match with the end value is obtained. In this case they will generate the sequence bcb 123 cac 121

   They now know the password is contained in the second chain. So they apply hash and reduction functions repeatedly to row 2 generating the sequence 112 aab 212. The hash of aab is 212 so the corresponding password is aab.

3. Why can't the attacker just use the inverse of the hash function to determine the password?

   Hash function inverses are very slow to calculate.

Question 3

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

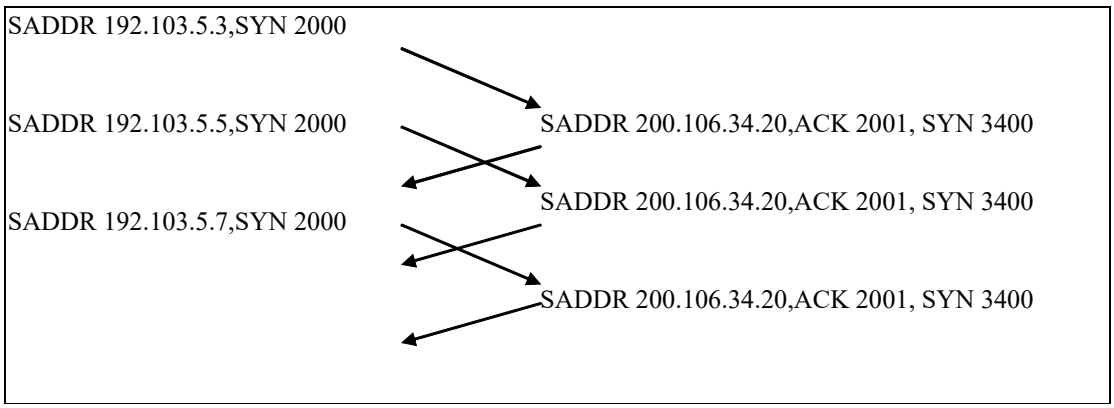
Salting works by inserting additional characters into the password before it is hashed. It increases the number of characters that must be searched for.

TNE30009 Tutorial Week 3

Multiple hashing is the process of taking the hash value of the password and hashing it. This may be repeated many times. This greatly increases the number of calculations necessary for using the rainbow table.

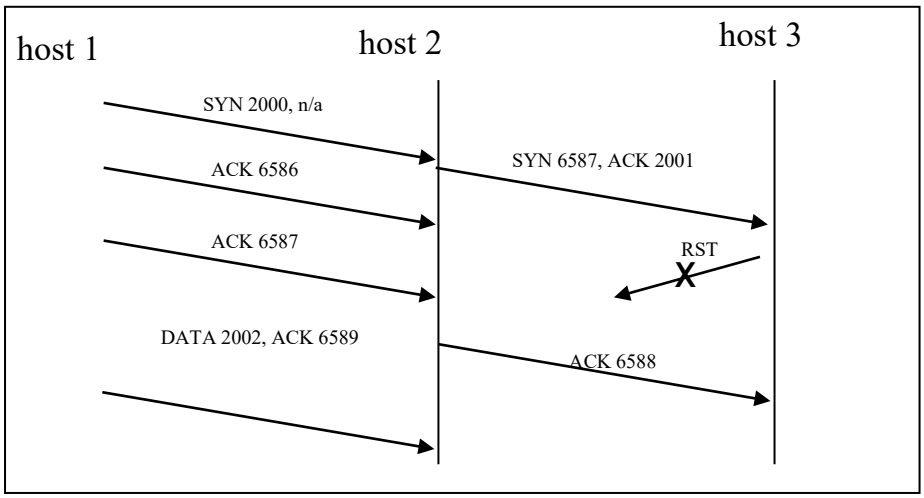
Question 4

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



This is a SYN flood attack. The attacking host is unknown since they are probably using IP spoofing to hide their identity. The attacked host is 200.106.34.20.

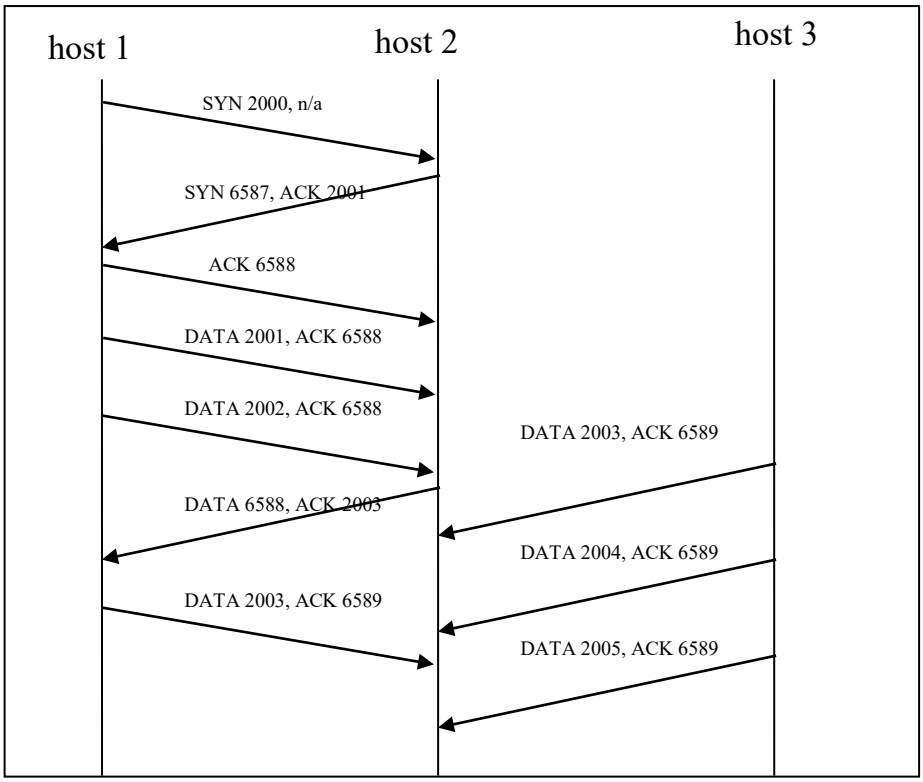
2. What attack is described in the following diagram? Which is the attack host, the target host and the spoofed host?



This is a TCP sequence number attack. Host 1 is the attack host, host 2 the target and host 3 is being spoofed (by host 1).

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 assume a 1 byte payload.)



This is a TCP session hijacking attack. host1 is the spoofed host, host 2 the target host and host 3 the attack host

4. In the above diagram, what will happen to DATA packet 2003 sent from host 1 to host 2? Why?

The TCP software will ignore it, because it will assume it is duplicate packet.

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.

TNE30009 Tutorial Week 3