CMSC5726 Computer and Network Security

Assignment 2: TCP Exploit

Deadline: 26-Mar-2017 (Sun) 23:59

Introduction

This is a group assignment. Each group member is provided with three VMs with Red Hat 9 Linux installed, namely Machine A, Machine B, and Machine C.

Machine	Root Password
A	<the one you set in the previous assignment>
B	sec$urity306W
C	sec$urity306W

Please complete the following questions in any VM group of any group member. Different questions can use different VM group.

Question 1 – RST Attack (25 marks)

a) Choose three VM machines (in the same VM group) to act as the client, the server, and the hacker's computer. Write down the IP addresses and the MAC addresses of each role (use the **ifconfig** command).

b) Connect all the three VM machines by a hub (i.e., **eth0**). You can use the **ifup** and the **ifdown** commands.

c) Create a user account in the server by using the **adduser** command.

d) From Blackboard, get **sniper-rst.c** and **spoofit.h** (in TCP Demo Code) and put them into the hacker's computer. Then compile **sniper-rst.c** to obtain the executable by using the **gcc** command.

e) Use the client to telnet to the user account (created in Step c) of the server by using the **telnet** command.

f) In the hacker's computer, perform the RST attack by using the executable obtained in Step d. (Hint: you may use the **netstat** command in the server/client machine to get the port numbers for the telnet session, which are the arguments of the executable.) At the same time, use Ethereal (in any machine) to capture the attack and save the log file as **rst_log**. (Hint: you have to execute the **startx** command before executing **ethereal**)

g) Which is the first packet sending from the hacker's computer for the successful RST attack? Why? Please provide the screenshot(s) for the explanation. (Hint: it is not the ARP packet.)

h) Which packet is used to calculate the sequence number and the acknowledgement number of the packet you mentioned in Step g? Why? Please provide the screenshot(s) for the explanation.

Question 2 – FIN Attack (25 marks)

a) Choose three VM machines (in the same VM group) to act as the client, the server, and the hacker's computer. Write down the IP addresses and the MAC addresses of each role (use the **ifconfig** command).

b) Connect all the three VM machines by a hub (i.e., **eth0**). You can use the **ifup** and the **ifdown** commands.

c) Create a user account in the server by using the **adduser** command.

d) From Blackboard, get **sniper-fin.c** and **spoofit.h** (in TCP Demo Code) and put them into the hacker's computer. Then compile **sniper-fin.c** to obtain the executable by using the **gcc** command.

e) Use the client to telnet to the user account (created in Step c) of the server by using the **telnet** command.

f) In the hacker's computer, perform the FIN attack by using the executable obtained in Step d. (Hint: you may use the **netstat** command in the server/client machine to get the port numbers for the telnet session, which are the arguments of the executable.) At the same time, use Ethereal (in any machine) to capture the attack and save the log file as **fin_log**. (Hint: you have to execute the **startx** command before executing **ethereal**)

g) Which is the first packet sending from the hacker's computer for the successful FIN attack? Why? Please provide the screenshot(s) for the explanation. (Hint: it is not the ARP packet.)

h) Which packet is used to calculate the sequence number and the acknowledgement number of the packet you mentioned in Step g? Why? Please provide the screenshot(s) for the explanation.

Question 3 – Restore the Telnet Section after the Telnet Hijack (50 marks)

In the original **hijack.c**, the client will get stuck in the connection once the hacker finished writing the evil data to the client's account. Now, please modify **hijack.c** so that after the hacker has written the evil data, the client's original telnet session will be restored. Please note that you cannot change the contents of the first two packets sent by the hacker (i.e., those inside **to_data[]** and **evil_data[]** in **hijack.c**). But you can then send more packets afterwards.

You can make the following assumptions:

- The hijack attack is initiated after the client has logged in the telnet session.
- The client is in the command mode (e.g., not opening any editor) when the hijack is performed, so the evil data can be executed.
- The client needs to type the keyboard aggressively in order to get back the telnet session. This approach can generate traffic from the client side.
- The evil data will be displayed in the terminal after the client restores his/her session. You do not need to consider how to remove such evil data.

In the answer sheet, please describe how you can restore the telnet session (25 marks). For the code, please rename your modified **hijack.c** as **assg2.c** and add comments to your newly added or modified code (25 marks).

Submission

Please submit to Blackboard a zip file with name **Group<your_group_number>.zip** (e.g., Group1.zip) containing

1) An answer sheet containing all the answers for Q1-Q3.
2) rst_log
3) fin_log
4) assg2.c

In the answer sheet, please include:

1. Group number
2. Student ID and name of each group member

Each group only needs to submit one copy, which can be submitted by any group member. Resubmission is allowed and only the latest one will be graded. Late submissions within three days can only receive 70% of the marks. Late submissions more than three days will not be graded.