CMSC5726 Computer and Network Security

Assignment 3

Deadline: 23-Apr-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	IP Address (eth1)	Root Password
A	10.1.xx.1	<the one you set in Assignment 1>
B	10.1.xx.2	sec$urity306W
C	10.1.xx.3	sec$urity306W

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

Question 1 – ARP Spoofing (20 marks)

a) Please write down the IP addresses and the MAC addresses of the three VMs in the answer sheet (use the **ifconfig** command). You will use Machine A as the hacker.

b) Please connect all the three VMs by a switch (i.e., **eth1**). You can use the **ifup** and the **ifdown** commands.

c) From Blackboard, get **send_arp.c** (in ARP Demo Code) and put it into Machine A. Then, compile it to obtain the executable **send_arp** by using the **gcc** command.

d) Please use Machine B to ping Machine C, and make a screenshot of the ARP table in Machine B, which contains the IP address and the MAC address of Machine C (use the **arp** command).

e) In Machine A, launch an ARP spoofing attack by using **send_arp** so that all packets that are intended to be sent from Machine B to Machine C will be sent to Machine A instead. Write down the command you used in the answer sheet and make a screenshot on the poisoned ARP table in Machine B.

f) Please use Machine B to ping Machine C. Meanwhile, use **ethereal** in Machine A to capture a log file and make the screenshot on the log file to show that Machine A can receive the ping packet from Machine B.

Question 2 – ICMP Redirection (20 marks)

a) Please write down the IP addresses and the MAC addresses of the Machines A and B in the answer sheet (use the **ifconfig** command). You will use Machine A as the hacker.

b) Please connect the two VMs by a switch (i.e., **eth1**). You can use the **ifup** and the **ifdown** commands.

c) From Blackboard, get **icmp_redir.c** (in ICMP Demo Code) and put it into Machine A. Then, compile it to obtain the executable **icmp_redir** by using the **gcc** command.

d) Please use Machine B to ping the host with IP address 1.2.3.4 (it is normal that the host cannot be reached), and make a screenshot of the routing cache in Machine B, which associates the aforesaid host with the gateway's IP address (use the **route -C** command). .

e) In Machine A, launch an ICMP Redirection attack by using **icmp_redir** so that all packets that are intended to be sent from Machine B to 1.2.3.4 will be sent to Machine A instead. Write down the command you used in the answer sheet and make a screenshot on the poisoned routing cache in Machine B.

f) Please use Machine B to ping 1.2.3.4. Meanwhile, use **ethereal** in Machine A to capture a log file and make the screenshot on the log file to show that Machine A can receive the ping packet from Machine B.

Question 3 – Packet Filtering (30 marks)

In each part of this question, you can assume that these are no rules in the **iptables** and the default policies of the **INPUT**, the **OUTPUT**, and the **FORWARD** chains are all **ACCEPT**. Different parts can use different VMs.

Hint: If you find that it is very slow to list the **iptables** rules, you may try the command "**iptables -L -n**" (without reverse DNS lookup).

a) Please write down a single **iptables** command to the **INPUT** chain in Machine A to refuse the telnet connection initiated by Machine B. All other connections from Machine B and all connections from other computers should not be affected.

b) Please write down the **iptables** commands in Machine A only allowing SSH connections to and from Machine B, while dropping all other incoming and outgoing packets.

c) Please write down the **iptables** command for Machine A to log incoming SYN packets from any computer, where the log will be updated in every 4 seconds in the middle of a SYN flooding attack. Please make a screenshot on the log file **/var/log/messages** in Machine A to show that it is updated in every 4 seconds in such a scenario. You will need to download and compile **synflood.c** (in TCP Demo Code in Blackboard), and then launch a SYN flooding attack on Machine A from Machine B.

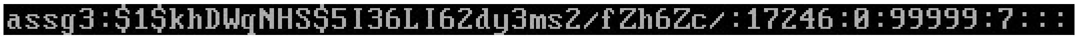
d) Please write down the **iptables** commands in the **INPUT** chain in Machine A to only accept a limited number of ICMP ping echo request packets from Machine B, so that when we issue the command "**ping -c 30 <ip_address_of_A>"** in Machine B, only the following ping requests are successful:

icmp_seq = 1-5, 7, 10, 13, 16, 19, 22, 25, 28

Meanwhile, Machine A can receive all other kinds of packets from Machine B and all packets from other computers without any limitation.

Question 4 – Password (30 marks)

Given the following account information in **/etc/shadow** in one of our VMs:



```
assg3:$1$khDWqNHS$5I36LI62dy3ms2/fZh6Zc/:17246:0:99999:7:::
```

Suppose we know the following information about the password:

1. The length of the password is 12.
2. The first five characters are "**CMsc#**" (without double quote).
3. All the remaining characters are digits (0-9).

Please write a C program in our VM using the brute force method to crack the password. You are required to use the **crypt(3)** function (Hint: check usage by "**man crypt**" in VM). Optionally, you may find the **sprintf()** and the **strcmp()** functions useful. Please submit your C program (**assg3.c**) and write down the cracked password in the answer sheet.

Submission

Please submit the following to Blackboard:

1) An answer sheet containing all the answers for Q1-Q4.
2) assg3.c

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.