ISEC 2025 Vulnerabilities and Exploits Assignment 1 – Part 2

Route Table Modification

Issued Date: January 24, 2024

Due date: TBA

Preamble

In Part 2 of this assignment, you will attempt to manually create a MITM position. You must modify the route table of the Windows machine in your test network (see below) such that packets from the Windows host (the victim) are routed through your Kali on their way to the other Windows host (the server). Your Kali will modify the packets from the Victim and forward the packets to the other Windows host (the server).

Requirements

You will need the following VM test network established. Note that you need three active nodes. These could be, for example, a combination VMs and your host machine.

1. A Kali node (the MITM attacker).
2. A Windows host. (The Victim)
3. Another Windows host (which we refer to as "The Server"). Note this does not have to be a Windows Server but could just be another Windows host.

Task 1 – Modify the route table of the Windows host (The Victim)

Examine your current route table on the Windows host (victim) by using the netstat -nra command. Capture the output of this command to a file called initialstate.log

Insert a new ***persistent*** route in the Windows route table by using the "route add" command. Set the IP address of your kali machine as the gateway to the Server host ip. Set the metric to a low cost value. Please NOTE: YOU MUST MAKE THIS A PERSISTANT ROUTE.

Reboot your Windows host (victim).

Run the netstat -nra command again and capture the output to a file modifiedstate.log

Edit modifiedstate.log and insert the "route add" command that you used at the top of the log file.

Task 2 – Configure your kali host to forward routed packets

Add a temporary route in the route table of your kali from your kali to the Server host.

Use the "modprobe iptable_nat" command to enable the nat module in iptables.

Temporarily enable ip forwarding in your kali by using "echo 1 > /proc/sys/net/ipv4/ip_forward". This command must be re-issued with each boot.

More information on ip forwarding is available at http://www.ducea.com/2006/08/01/how-to-enable-ip-forwarding-in-linux/.

And

https://askubuntu.com/questions/227369/how-can-i-set-my-linux-box-as-a-router-to-forward-ip-packets

Study the "iptables -t nat -A POSTROUTING -o [interface] -j MASQUERADE" command in the iptables man page or other resources. Here's one other resource:

https://unix.stackexchange.com/questions/322879/port-forward-why-is-iptables-with-postrouting-rule-required

Question 1: Explain **in your own words** what *the iptables -t nat -A POSTROUTING -o [interface] -j MASQUERADE* command does/what it is used for.

Question 2: Let us assume the both the victim and the server are on the same network and we don't care about NATting the traffic from the victim. ***Is the command in question 1 necessary*** to achieve the routing of the Windows traffic between the victim and the Server through your kali machine in each of the following Cases:

> Case 1: If we are only interested in seeing the traffic from the victim to the server?
>
> Case 2: If we are interested in seeing both inbound and outbound TCP traffic between the victim and the server. Be sure to explain thoroughly

Note the high value of "Effort and Care" in the rubric. Most of this "Effort" mark will be assessed on the detail and thoroughness of your answers to question 1 and 2.

More information is available at https://askubuntu.com/questions/466445/what-is-masquerade-in-the-context-of-iptables

Task 3 – Test that the Windows Host now routes its packets through the kali machine

From your Windows (victim) host, run a tracert to your Server host ip. Redirect the output to routingresult.log

NOTE: Your submission will take the form of a single file containing your Title Page, the contents of initialstate.log, the contents of modifiedstate.log, the answers to Questions 1 and 2 above and the contents of routingresult.log.

Submission Guidelines

The assignment is to be uploaded to the Brightspace shell on or before the due date. Your document is to be of professional quality including layout, spelling, grammar and overall appearance. Create a separate title page containing the course code (ISEC), course number (2025), assignment number (1 Part 2), assignment title ("Route Table Modification") and your name.

Your document filename MUST be of the format YOURLASTNAME_YOURFIRSTNAME_ISEC2025_AS1-2.

Rubric

Together, part 1 and part 2 of this assignment are worth **25%** of your final mark. Part 2 is scored out of 40 points using the following rubric.

Please note that a pass on Part 2 is 60% (24 points) and if all categories are "Condition Somewhat Met" then you can only score a maximum of 20 points and will therefore not receive a passing grade for Part 2.

Neatness counts!

Rubric

Part 1 – DNS Zone Transfer (10% of final)

Rubric

Part 2 – Route Table Modification (15% of Final)

Rubric	**Condition Not Met**	**Condition Somewhat Met**	**Condition Met**
Task 1			
Modify the Windows route table and show contents of initialstate.log and modifiedstate.log	0	1-5	6-10
Task 2			
Modify Kali and answer Question 1 and Question 2	0	1-5	6-10
Task 3			
Test Windows routing and show contents of routingresult.log	0	1-5	6-10
Assignment shows obvious care and effort	0	1-5	6-10
Points available by column	**0**	**20**	**40**