CYBR371: System and Network Security
2024– T1

Arman Khouzani, Mohammad Nekooei

Lab 3: Denial of Service & MitM Attacks

Submission Deadline: 23:59:00 (NZST) on Sunday, 28 April 2024

EXAMPLE SOLUTIONS + GRADING RUBRIC

Complete the following netlabs (accessible from `nuku/modules/`:

- Denial of Service Attacks
- ARP Spoofing and MiTM Attacks.

Write the answers to the questions in the order they appear in this document. Submit the file (`.pdf`) using the ecs submission system (i.e. Lab3). https://apps.ecs.vuw.ac.nz/submit/CYBR371/Lab3.

Question:	1	2	3	4	5	6	7	Total
Points:	4	4	8	8	8	4	4	40
Score:								

1 Part 1 - Denial of Service Attacks

Q.1. [4 points] Why aren't new operating systems susceptible to Ping of Death attack? (250 words max)

Solution: It is enough to say: Modern operating systems are patched against this (don't have this vulnerability in their implementation of ICMP anymore), that is, they ensure that a packet doesn't exceed the maximum packet size (of 65,535 bytes) when reassembled.

Q.2. [4 points] How can you make the Ping of Death packets effective against a target these days? (250 words max)

Solution: Any of the following will be acceptable:

- Finding a target that still has a vulnerable OS (by scanning the internet). These are usually old embedded devices that is difficult (or impossible) to update/patch (like old routers, old printers, old security cameras, . . .)
- Make it distributed but below the maximum 65,535 size, meaning if a large number of machines send ping of death packets simultaneously, overwhelming the network or the host operating system.
- Combine with packet fragmentation attack in which large packets also employ fragmentation as well, requiring more processing on the receiving end. (This of course combined with a distributed attack can be more effective).

Q.3. [8 points] Briefly explain the countermeasures to stop and defend against a Smurf attack? (250 words max).

Solution:

- Router/host drop packets which are not a reply to an already sent ICMP request packet. This means either the host of the firewall keeps track of the ICMP requests and the hosts associated with it and expects a reply. Any ICMP replies for which a requests does not exist is dropped once received.
- Drop packets with invalid source IP addresses (e.g. not from the internal network or from those expected to receive a reply)
- Rate limiting the number of echo replies received (e.g. 3 packets per second, drop others).
- Filters on L3 devices to not reply for broadcast address.

Rubric: 5 points for a single correct entry. 8 points for at least two correct entries.

Q.4. [8 points] Did the Smurf attack slow down the network? Compare the average ping response time before and during the Smurf attack.

Solution: In most cases it causes 100% packet delivery failure but generally the average is significantly higher…

Rubric: Any higher number is acceptable.

2 Part 2 - ARP Spoofing and MiTM Attacks

Q.5. [8 points] Is Ettercap using ARP spoofing to manipulate html images and JavaScripts? Explain your answer (250 words max).

Solution: Yes, ARP spoofing and poisoning to redirect the traffic between the host and the web server.

Rubric: The question is a bit vague. So the following answer is also acceptable: No, it doesn't use ARP spoofing for manipulating html images and javascripts, but rather ARP spoofing is involved (for redirecting the traffic to the MitM machine).

Q.6. [4 points] What would be the effect if instead of http, we had https? Explain your answer (150 words max).

Solution: The attack will fail. First of all, because the traffic is encrypted, it will not be possible to determine what the content of the html document is, e.g., where `<img>` or `</head>` tags are. Secondly, even if it was possible to "guess" which part of the traffic they are, it will not be possible to replace them with another traffic that when decrypted will lead to a valid html code.

Rubric: 2 marks for identifying that the attack will not work. 2 marks for a correct explanation.

Q.7. [4 points] What would you change to replace every image in the html page with an image of VUW logo!?

Solution: Multiple possible answers:

- Download the VUW logo e.g. from wikipedia: `https://en.wikipedia.org/wiki/File:Victoria_University_of_Wellington_logo_national_crest_vertical.png`, and replace the **`logo.jpg`** file located in **`/var/www/html`** with it (with the same name).

- Or modify the code in the **`logo.filter`** file, in particular, inside the second "`if`", replace the address `http://192.168.0.2/logo.jpg` with an address of the VUW logo, e.g. `https://en.wikipedia.org/wiki/File:Victoria_University_of_Wellington_logo_national_crest_vertical.png`. But note that you now need to recompile the filter.