### Lab 12 – Man in the Middle

### Due as per D2L dropbox

**Scoring Rubric**

|  |  |
| --- | --- |
| 100 | Successfully reroutes ARP traffic and provides all of the required screenshot documentation (or provides in-lab demo in front of instructor). |
| 0 | Nothing turned in or document is not readable or does not accomplish the lab activities |

**Goal**

To successfully complete an ARP-based man in the middle attack using specialized software (i.e. arpspoof, etc.).

**Deliverables**

Upload an MS Word DOCX or PDF file to D2L with name, course #, assignment and appropriate documentation (e.g. embedded screenshots).

**Setup Details**

You will need two systems. One is the attack platform running Kali. The other is the target machine that you are going after. The target machine can be any machine running on your host machine, or even your host machine itself.

* If you plan to use arpspoof, you may need to install its software (Kali does not come with it) which is part of the dsniff software package.

**Attack Details**

Remember to take a snapshot of your installed, updated Kali VM prior to making any serious modifications (so you can undo those changes later on).

* For any software you choose to use, take a screenshot of the ARP list on the target machine and a screenshot of a packet capture using wireshark showing the MAC addresses of the host and destination machines (One should be your router and the other should be the target machine.)

**Restrictions**

* Students should take care when entering a target machine's IP addresses (or CDIR addresses) to ensure that only the correct address(es) are targeted. 
* Under no circumstances are students to actively compromise or subvert control of any hosts for which they are not the rightful owner or for which they do not have written permission to do so.

**Background & Resources**

* Scanning chapter in CHR.
* Documentation for arpspoof (see the tool itself, and online).

Notes:

“Warning sign” image from <http://en.wikipedia.org/wiki/Exclamation_mark>

PART 2: (Graders use only)

Matthew Young

CIS450

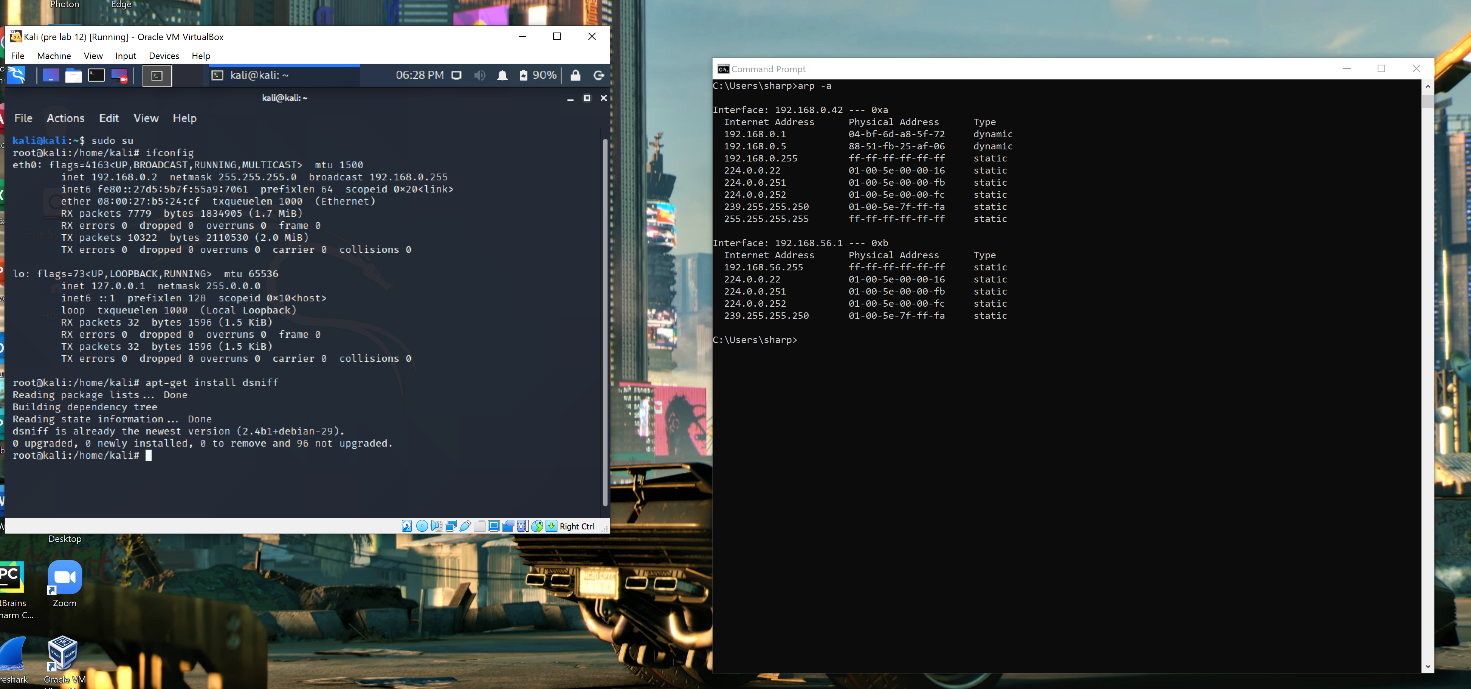
Lab12 – Man in the Middle

First Screenshot Displays the ip of the attacking machine(left) and the target machine(right)

A screen shot of a computer monitor sitting on top of a computer

Description automatically generated

Second screenshot shows installation of the dsniff package on the attacking machine(left) and ARP list on the target machine(right)



Third screenshot shows the attacking machines arpspoof command(left) actively rerouting traffic to/from the target machine which is displaying the physical address of the gateway(right)

A screen shot of a computer

Description automatically generated

Fourth screenshot shows the packet capture for the traffic being routed through the attacking machine (left). At this point you could go further by manipulating the traffic going to the target machine(right).

A screen shot of a computer

Description automatically generated

NOTE: you can also set this up to the reverse to intercept traffic being sent out from the target machine to the gateway and manipulate that traffic as well.