CMPUT 333, Assignment 3, Winter 2021

University of Alberta / Department of Computing Science

Instructor: Ioanis Nikolaidis (nikolaidis@ualberta.ca)

(ARP spoofing, buffer overflows)

Part 1 (50%)

As you learned in Lab 2, the "backbone" network of your virtual hosts is the subnet 10.229.100.0/24. You will be given two more VMs to put on the backbone network. However, in this lab, both of these backbone machines are now "victim" hosts, or machines whose traffic we need to analyze. You will need to determine the IP addresses of these victim hosts.

Step 1 (20%)

Your first set of tasks is to:

1. Determine and report, by using tools such as `nmap`, etc, what are the IP addresses of the victim hosts connected to the backbone,
2. Determine and report, using the same/similar tools, what are the services running on each of the victim hosts connected to the backbone.

You may need to read more about how the tools work and come up with their "guesses". The above should be supported by a corresponding deliverable of the output of the tools that you used and your findings.

Step 2 (30%)

Subsequently, you will mount a man-in-the-middle attack between the victim hosts. The hint to follow to find the “victim” hosts is that they are characterized by a fairly regular communication pattern. They set up connections periodically between them, in the order of minutes. Using a man-in-the-middle attack by ARP poisoning using `ettercap`:

1. determine the victim hosts,
2. determine what connections are initiated (including which host is the client and which one is the server for the connections),
3. determine what is the service(s) to which the connections are established, and,
4. identify the nature and extract the contents of the transfers between the hosts (not just a dump of bytes, but qualitatively "what are they about"?).

The above should be supported by a corresponding deliverable of `tcpdump` packet trace and any contents that you intercepted. Specifically, your deliverable should include at least:

- the ARP activity for the period just before and just after you performed ARP poisoning,

- captured packets of the communication between the hosts (if many, then a compressed archive of the packet capture),
- any contents (packet payload, e.g., files) that you were able to reconstruct from the communication between the victims,
- time intervals between data transfers, and
- the output you got from `ettercap`.

Part 2 (50%)

You are given an executable file (you can download it here which performs a trivial transformation on input provided from stdin. The executable is runnable on your Linux virtual host. The interaction with the program is through the stdin/stdout. You also know that the executable contains functions that print the string "Flag of group XX" where XX ranges from 01 to 13. Your task is to write a buffer overflow exploit that, when used, forces the program to print "Flag of group YY" where YY is your group's number. To complete this part you must:

1. report what the program actually does (it is quite trivial -- don't go overboard here),
2. report what is the buffer size used by the program and how you were able to find it,
3. report how you determined how to call the function that produced the desirable output,
4. provide the source code for your exploit, and,
5. report how your exploit works and why it is structured the way it is.

Note that you should try to write the exploit in a way such that, after it prints "Flag of group YY", the program terminates as normally as possible (i.e., without aborting or crashing). You are free as to the choice of language for programming the exploit.

Deliverables

Only one of the group members need to submit on behalf of the entire group (in the event of more than one submission, the last one will be considered). All relevant files will be submitted together as a single compressed .tar.gz or .gzip bundle. A report (in plaintext, markdown, or pdf format) should be provided including answers to the questions posed in the specification and point to the various files you are providing as part of your answer. You should cite any resources that you used to produce your answers. By default it is assumed that all group members equally contribute to the assignment. If you need to deviate from this model of cooperation, explain why and indicate who was responsible for what.

Friday, March 19, 2021