CSE 825 Man-in-the-Middle Attack Assignment

Matt Hammerly: hammer24@msu.edu
Eric Coldwell: coldwel3@msu.edu
Isaac Dorgbefu: dorgbefu@msu.edu

2 December, 2015

You are a seedy contract janitor who has just been assigned to spend their evenings scrubbing toilets at a big-name bank. You also have an oddly high degree of computer literacy for a janitor, and you decide now is a good opportunity to use it to hoist yourself out of this job that you loathe. You bring a Raspberry Pi or whatever into work with you and plug into the network after hours, because your bank doesn't maintain a MAC address whitelist and you can just do that. Now that you're on the network, your goal is to sneak some money into your account so you can quit this job and become a painter.

The network consists of five computers connected via ethernet to a switch. One of the machines, `10.1.1.5`, hosts the bank's primary database and and a server application that handles incoming transaction requests. The rest of the machines (except for yours —`10.1.1.5`) will be sending transactions to the server every few seconds. You will use Ettercap to execute an ARP Poisoning attack against machines on the network to intercept and analyze these transaction requests before they get to the server, and etterfilter to enable ettercap to modify these requests before sending them on to be processed.

Your proof of completion will be having a nonzero balance in your group's account, as well as a brief email to us describing your methods. Each group gets a user on the system and an account number in the database:

- grp1 → 19001
- grp2 → 19002
- grp3 → 19003
- grp4 → 19004
- grp5 → 19005

At any time, you can check the balance of your group's account with the `get_balance.py` script provided in your home directory. Your account number and balance should be printed if you run `python3 ~/get_balance.py`.

Due to the nature of ARP poisoning and our limited number of machines, it's not possible for all groups to go at this assignment at the same time. Therefore, we ask that you pick a day for your group to work on this. Let's say a day starts/ends every 6:00am, so you can pull an all nighter if you have to (but email us if you have to because you shouldn't!). See the discussion board for times.

Notes/Hints

- eth1 please
- Ettercap requires root to access link-layer sockets. We gave you sudo —please don't ruin the system or do anything that goes against the spirit of the assignment.
- Be careful with etterfilter's `replace(what, with)` function. If you change the length of HTTP headers willy-nilly you'll get unexpected results.
- IPv6 is supported on these boxes. We don't use it, but it means we have to format our targets for ettercap `MAC/IP/IPv6/Ports` instead of `MAC/IP/Ports`.
- `man ettercap`
- `man etterfilter`

Feel free to email us or post on Piazza with any questions. Happy Hacking!