Assignment 1

ABC Inc. Investigation

Kevin Orr

February 15, 2018

Inspecting the pcap, we immediately see ARP requests, DNS requests, and HTTP traffic. In packet 57, we see an HTTP request from 192.168.209.129 to `http://192.168.209.10:80/`. The user-agent string is `"User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:39.0) Gecko/20100101 Firefox/39.0"`, so the browser is likely Firefox 39.0. This request is responded to in packet 59 with HTTP 401 Unauthorized. Shortly after, in packet 101, the request is tried again but with HTTP Basic Authentication using a user:password combination of armin:awesome. The request is replied to in packet 103 with HTTP 200 OK. Exporting the HTML, we can see this is a bookkeeping ledger for ABC Inc.

Later, in packets 211-215, we can see that the same host requests `http://192.168.209.10/internal_letter.html` using the same credentials. In this letter we can see our leaked info:

> As you all may know, we have been negotiating with Personman Inc. regarding of the sale of our enterprise solution. The last couple months had been a tough time for all of us. But I'm happy to let you know that Personman finally decided to purchase our solution. The next Wednesday, Feb 2, 2017, we will host a meeting with Personman representatives in the Mayflower hotel, Washington D.C. to finalize the sale price.
>
> Unfortunately, I will be traveling and cannot attend this meeting by myself. The board of directors have decided that our bottom-line is $6,430,000. However, we would like to make a higher profit out of this deal. Please keep this information confidential.

Then ∼43 seconds into the capture, starting at packet 282, we see a new NIC on the address of 00:0c:29:56:c2:fe. From here until packet 791, it enumerates the 192.168.209.0/24 network, sending ARP requests to all hosts in this range. The machine that is scanning the network sets the ARP "Sender IP address" field to 192.168.209.131. From packets 1051-2056, this machine tests common TCP ports on the hosts that responded to it, namely 192.168.209.{1,10,128,129,254}. The only ports that appear to be listening and unfiltered (i.e. respond with a SYN/ACK) are 192.168.209.10:{22,53,80}.

In packets 2448-2810, we see this machine trying to access `http://192.168.209.10:80/`. It first tries no credentials, and then it tries various common user:password combinations, such as admin:admin and test:test. After trying many unsuccessful combinations, in packets 2949-3088, we can see it starting to ARP spoof 192.168.209.10 and 192.168.209.128.

In packet 3175, 192.168.209.128 makes a request to `http://192.168.209.128:80/` using the same armin:awesome credentials. About 30 seconds later in packet 3715, our eavesdropper requests `http://192.168.209.128:80/` and then `http://192.168.209.128:80/internal_letter.html` using the correct credentials. This shows how Personman Inc might have conducted corporate espionage on ABC Inc.