Sarjoun Radiyeh & Samer Saade

AMERICAN UNIVERSITY OF BEIRUT
MAROUN SEMAAN FACULTY OF ENGINEERING & ARCHITECTURE

EECE 655
Assignment 1

Our objective for this assignment is to create a network attack with its corresponding detection method. We decided to focus our efforts on the topic of DHCP starvation.

Description of Tools

In this section we will be separately discussing both the attack and detection tool features.

DHCP Starvation Attack

Our DHCP attack tool sends forged DHCP Discover requests with randomized MAC addresses. Upon receiving a DHCP offer, it prints the offered IP address allowing the user to monitor available IPs. Each forged request mimics a unique device by using a different random MAC address.

A randomized sleep timer between 1 to 5 seconds is also used between each request to attempt to reduce detection. If no more IPs are available, a message is printed.

DHCP Starvation Detection

Our DHCP starvation detection tool is essentially a system designed to monitor and identify potential DHCP starvation attacks while also notifying the user in real-time. Through our use of the scapy library, it captures network traffic, specifically focusing on DHCP and ARP packets, which are necessary to the attack detection process we created.

The tool uses DHCP offers to keep track of MAC addresses and their corresponding request times within a sliding time window alongside an initial threshold set for the maximum number of unique MAC addresses that can request IPs in the given time window. In order for the tool to dynamically adapt the threshold to network conditions, it employs an Exponential Moving Average (EMA) to continuously update the threshold, which is the expected number of unique MAC addresses within the period. For this update to occur, the tool uses another thread outside the DHCP detection process to ensure periodic updates to the EMA as well as the cleaning of old MAC addresses stored beyond the last time window duration.

If the count of unique MAC addresses within a time window exceeds the EMA, the tool will send an alert to a Slack channel.

The tool also uses ARP requests to verify if the IP addresses offered by the DHCP server are truly being used by the corresponding devices from the DHCP Offer.

After a DHCP offer is detected, it sends an ARP request using the offered IP asking, "Who has this IP address?" and waits for a reply. If the source MAC address in the ARP reply matches the one from the DHCP offer, the tool confirms that the device truly exists and is a legitimate user. If no reply is received or the MAC addresses don't match, it flags the allocation as suspicious and sends an alert to a Slack channel.

Alongside the alerts sent through Slack, the tool also keeps a detailed log of all activities and detections, both stored in a log file and displayed on the console. This ensures that users can easily check for details in events as they happen and review past incidents.

How to Run the Tools

To run both tools, all you need to do is open a shell and grant in administrative privileges this can be done as follows:

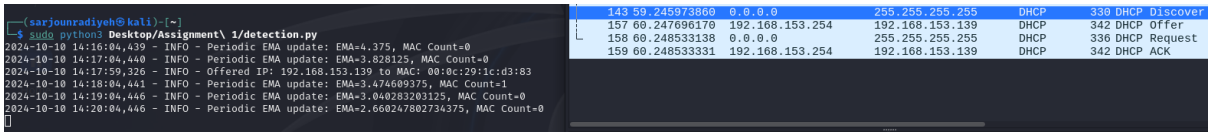
- Windows: Open the Start menu, search up any terminal application like PowerShell, right click and choose “Run as Administrator”. Then, run the following commands on separate terminals (assuming you are in the correct folder):
    - **python attack.py**
    - **python detection.py**
- Linux: Open any terminal application you have and run the following commands on separate terminals (assuming you are in the correct folder):
    - **sudo python attack.py**
    - **sudo python detection.py**

You can test this code on any device with access to a DHCP server, however we opted to use VMware’s built-in DHCP server while running the virtual machines on NAT mode. This allowed us to run and test everything in a safe and controlled environment.

Testing

We decided to split this section into two, legitimate and illegitimate devices respectively.

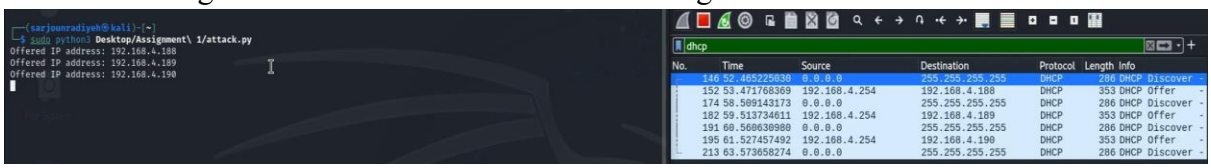
Legitimate Devices requesting DHCP Leases



We tested our detection tool’s ARP functionality by opening a legitimate device that would request an authentic DHCP Offer request, the code shows that there is no warning for “Suspicious allocation of IP” hence that implies the tool is working as intended and that the device is sending back an ARP reply with the correct source MAC address when compared to the DHCP Offer. The tool is also counting the MAC addresses correctly, as regardless of whether the device is legitimate or not, the MAC should be counted to set a threshold/baseline for expected devices

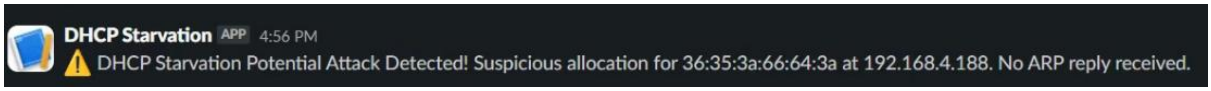
Illegitimate Devices requesting DHCP Leases

We proceeded to test both of our tools by launching an attack by sending a crafted DHCP discover message and obtained the DHCP offer message which can be seen on Wireshark.



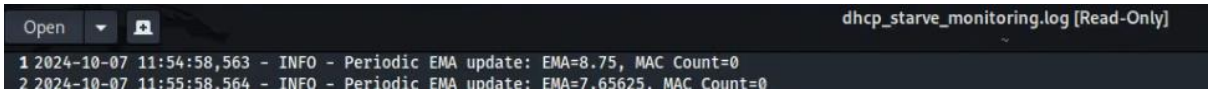
Which now means the DHCP server has lost these 3 IPs from its address pool. We could continue running the code until all the available IPs would be exhausted and the attack tool would continue to starve the server by sending new DHCP discover messages even when previous leases expire.

```
2024-10-08 16:56:14,407 - INFO - Periodic EMA update: EMA=4.375, MAC Count=0
2024-10-08 16:56:17,132 - INFO - Offered IP: 192.168.4.188 to MAC: 36:35:3a:66:64:3a
2024-10-08 16:56:22,280 - WARNING - Suspicious allocation for 36:35:3a:66:64:3a at 192.168.4.188. No ARP reply received.
2024-10-08 16:56:29,896 - INFO - Offered IP: 192.168.4.189 to MAC: 31:35:3a:37:66:3a
2024-10-08 16:56:35,088 - WARNING - Suspicious allocation for 31:35:3a:37:66:3a at 192.168.4.189. No ARP reply received.
2024-10-08 16:56:35,914 - INFO - Offered IP: 192.168.4.190 to MAC: 36:64:3a:63:31:3a
2024-10-08 16:56:41,084 - WARNING - Suspicious allocation for 36:64:3a:63:31:3a at 192.168.4.190. No ARP reply received.
2024-10-08 16:56:44,408 - INFO - Periodic EMA update: EMA=4.203125, MAC Count=3
```



Now looking at the detection side of the script after the attack allocates illegitimate IPs to specific MAC addresses. We can see that the detection tool not only relies on creating a threshold but also relies on sending an ARP request on the targeted MAC address to make sure that the device is legitimate, and here no ARP reply is occurring due to the fact that the device doesn't exist thus this IP-MAC pair will be categorized as a suspicious allocation and hence a slack message is sent.

```
2024-10-08 16:56:44,408 - INFO - Periodic EMA update: EMA=4.203125, MAC Count=3
2024-10-08 16:56:45,613 - INFO - Offered IP: 192.168.4.191 to MAC: 32:38:3a:63:64:3a
2024-10-08 16:56:50,820 - WARNING - Suspicious allocation for 32:38:3a:63:64:3a at 192.168.4.191. No ARP reply received.
2024-10-08 16:56:51,571 - INFO - Offered IP: 192.168.4.192 to MAC: 36:31:3a:31:63:3a
2024-10-08 16:56:56,764 - WARNING - Suspicious allocation for 36:31:3a:31:63:3a at 192.168.4.192. No ARP reply received.
2024-10-08 16:56:57,465 - CRITICAL - High amount of unique MAC addresses detected: 5 unique MAC addresses in the last 30 seconds
```



We also notice that after some point, the EMA (or essentially the dynamic threshold) is exceeded (5 > 4.203125) and a critical warning stating a high amount of unique MAC addresses have been detected within the time window of 30 seconds which is then sent to slack and stored in the log file.

Team contribution

The following distribution applies to everything, whether code or this document:

Detection (100%): Sarjoun Radiyeh

Attack (100%): Samer Saade