Lab 8 – Netflow and Wireless Analysis

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 11/5/2019

About the Lab

NetFlow is a feature that was introduced on Cisco routers around 1996 that provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion. A typical NetFlow monitoring setup consists of three main components - Flow exporter: aggregates packets into flows and exports flow records towards one or more flow collectors, Flow collector: responsible for reception, storage and pre-processing of flow data received from a flow exporter, Analysis application: analyzes received flow data in the context of intrusion detection or traffic profiling.

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. It is used for network troubleshooting, analysis, software and communications, protocol development. It is one of the most famous tools that is used to monitor network traffic and protocols used. It lets us monitor the network at a microscopic level, both wired and wireless.

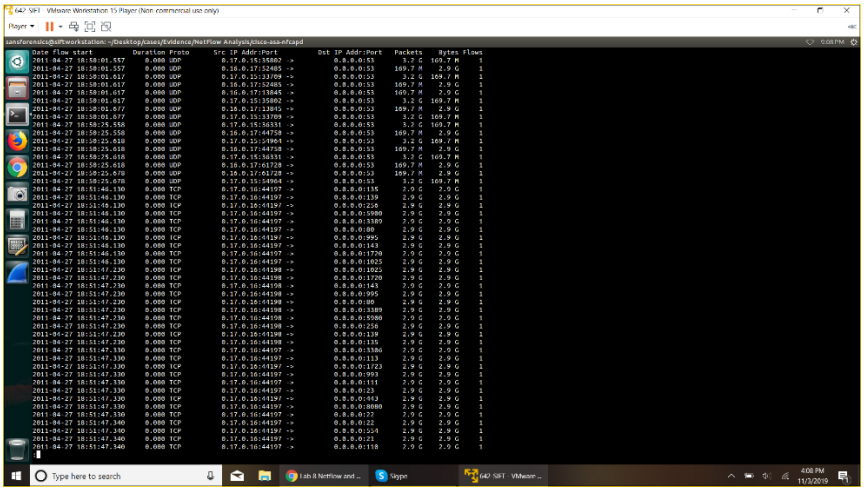
1. Netflow Analysis

- Identify any compromised systems
- Determine what the attack found out about the network architecture
- Evaluate the risk of data exfiltration

Command used: nfdump –R cisco-asa-nfcapd.2011042712

nfdump – netflow display and analyze program or file. nfdump is the netflow display and analyzing program of the nfdump tool set. It reads the netflow data from files stored by nfcapd and processes the flows according the options given. The filter syntax is comparable to tcpdump and extended for netflow data. Nfdump can also display many different top N flow and flow element statistics.

-R - Read input from a sequence of files in the same directory



2. Wireless Packet Capture Analysis.

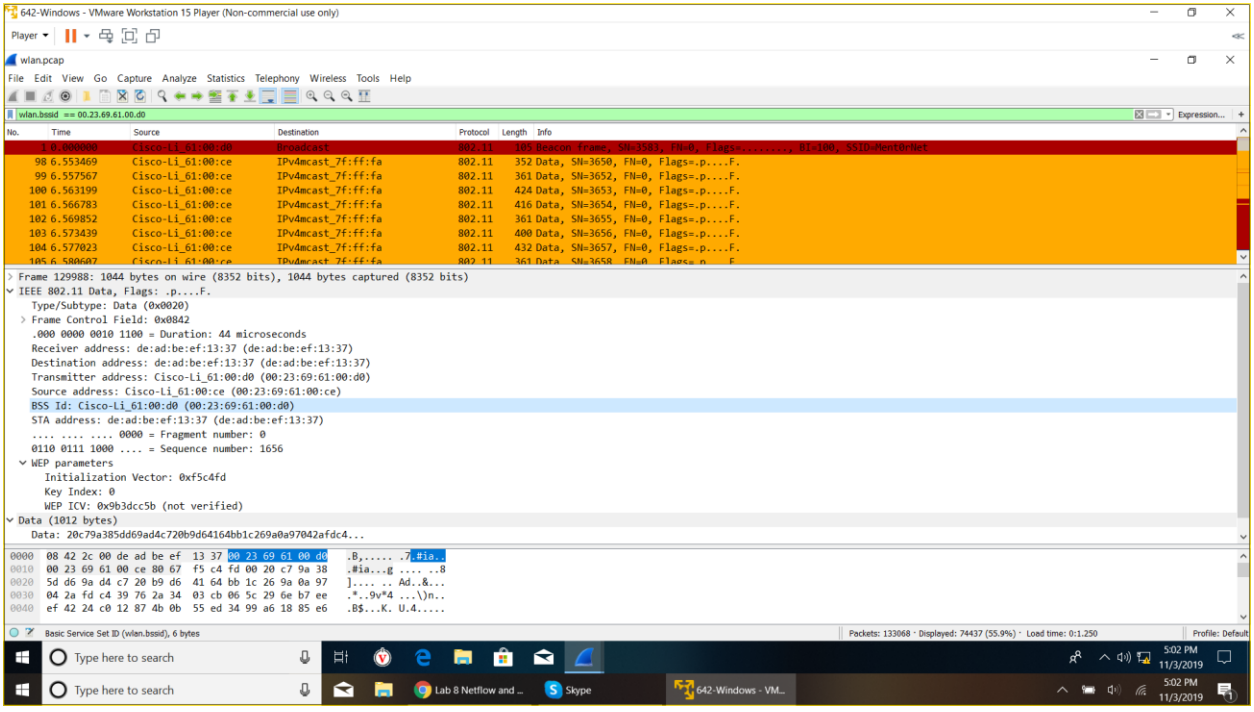
1. Can you figure out what's going on and track the attacker's activities?

   Based on the background provided and by looking at the pacap file it looks like the attacker war using a network adapter to extend the range and connect to the Wi-Fi network – Ment0rNet. Because the data is encrypted we can't exactly figure out what he was doing but analyzing the types of packets sent by the attacker he was performing deauthentication attack.

   This attack sends disassocate packets to one or more clients which are currently associated with a access point. Disassociating clients can be done for several reasons - Recovering a hidden ESSID. This is an ESSID which is not being broadcast. Another term for this is "cloaked", Capturing WPA/WPA2 handshakes by forcing clients to reauthenticate, Generate ARP requests.

2. What are the BSSID and SSID of the WAP of interest?

   BSSID – 00:23:69:61:00:d0 and SSID – Ment0rNet

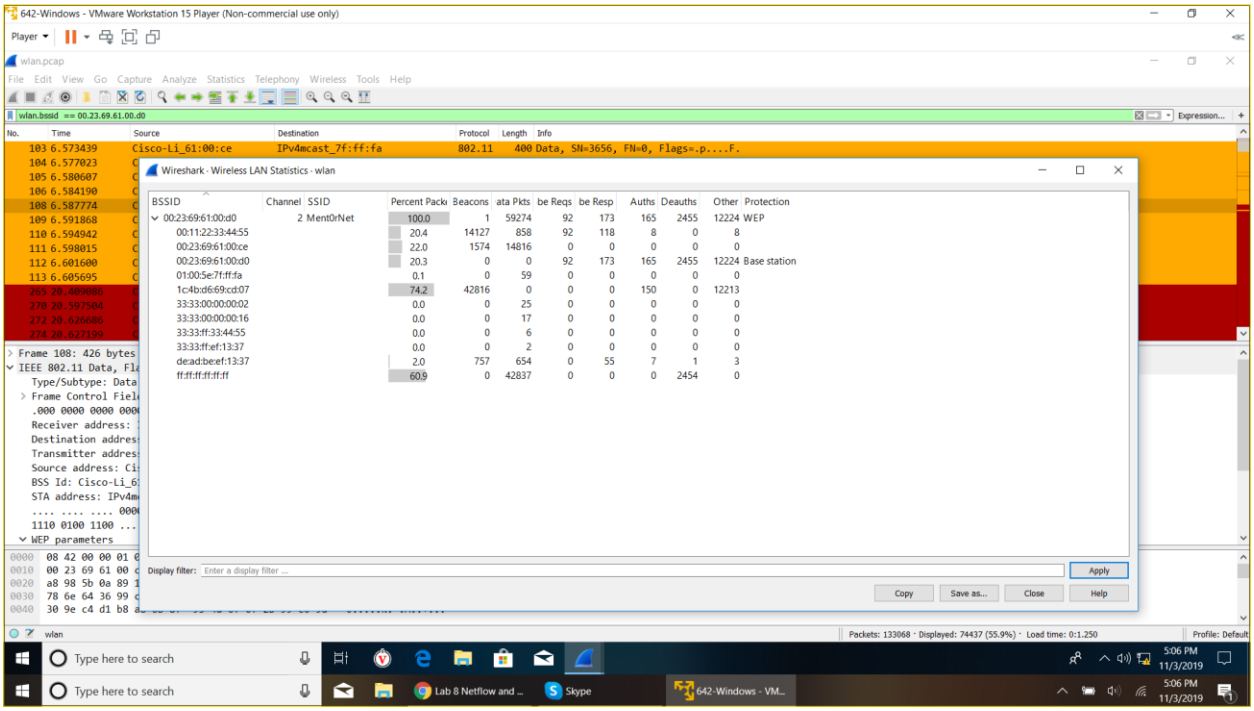


3. Is the WAP of interest using encryption?

   Yes, WAP was using encryption. We know this for sure because the data sections in the pcap file are not human readable, they are just combination of numbers and characters.

4. What stations are interacting with the WAP and/or other stations on the WLAN?

   To see what stations are interacting with WAP we can use the option Wireless>WLAN Traffic. This will show the Wi-Fi network and all the device's mac address that were connected to it.



5. Are there patterns of activity that seem anomalous? 6. How are they anomalous: Consistent with malfunction? 7. Consistent with maliciousness?

   Yes, based of the information provided in the background, owners MAC address is 00:11:22:33:44:55. So, all the mac addresses other that this are unknown and potential malicious actors (except of network loopback). Upon examining the pacp we can see there are a lot of Probe requests & responses, Null functions, Disassociate packets and Deauthentication packets. First thing that crosses my mind is WEP cracking using deauth attack. The way it works is, to crack the WEP key for an access point, we need to gather lots of initialization vectors (IVs). Normal network traffic does not typically generate these IVs very quickly. Theoretically, if you are patient, you can gather enough IVs to crack the WEP key by simply listening to the network traffic and saving them. So, the attacker sends deauths to disconnect any connected devices and then monitors and captures the IV's when a device connects to the Wi-Fi network. After repeatedly doing this and collecting enough IV's the attacker can crack the network key.

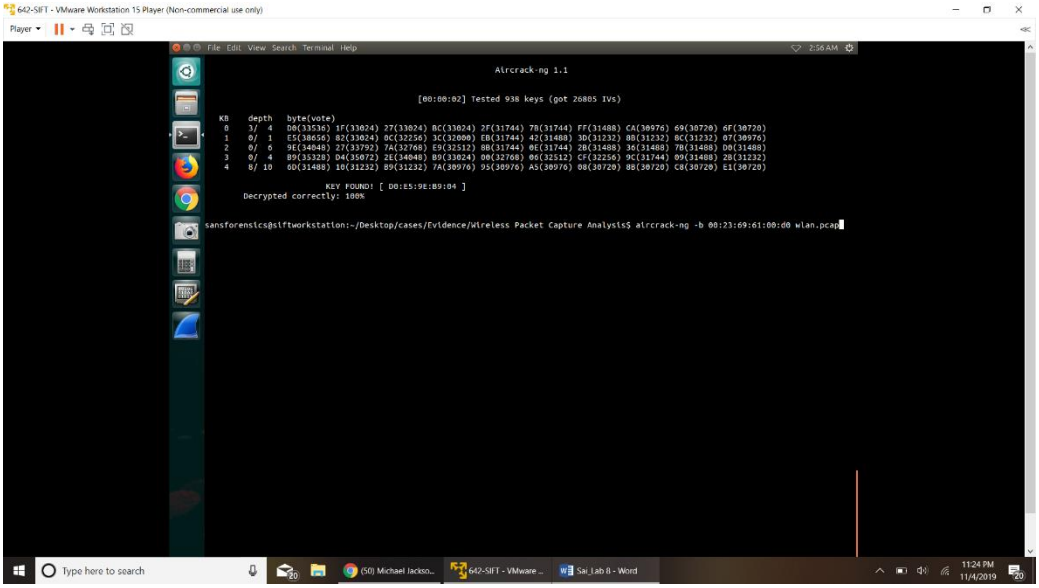
6. Can we identify any potentially bad actors?

   Based of where the deauthentication packets were coming from we can classify that 1c:4b:d6:69:cd:07 is the bad actor. (He has sent 2455 deauth packets in total)

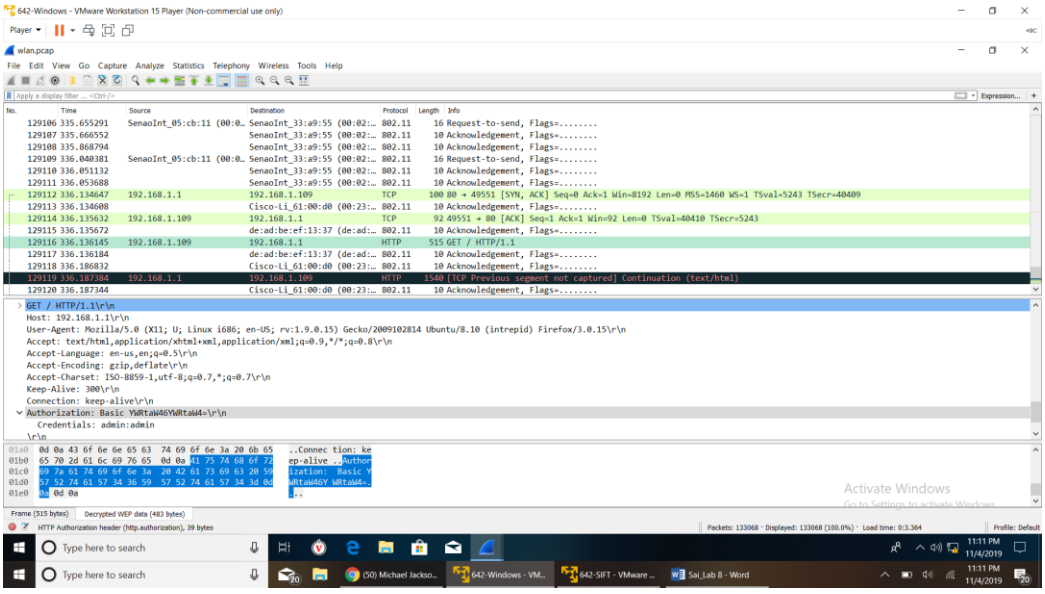
7. Can we determine if a bad actor successfully executed an attack?

   Yes, the attacker was successful. We can know this sure because, after sending 2455 deauth packets there are only data packets and by examining the data packets section we see 42816 data packets sent from the mac address 1c:4b:d6:69:cd:07. Because the data is encrypted we can't exactly say what the attacker did after he was access to the Wi-Fi network, unless we get the key the network.

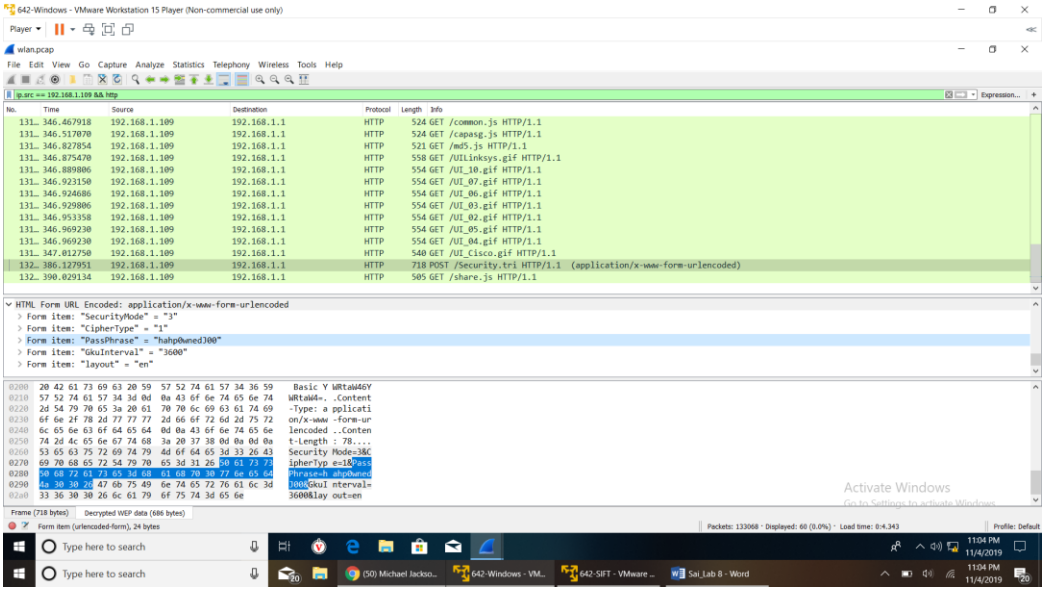
   By using aircrack-ng we figure out that the network key is D0E59EB904.



   By adding this key to wireshark we can see the decrypted traffic. Upon further examining we can see that Joe is a very careless system admin, his router login credentials were admin:admin.



Later, he also kicked out the owner, Joe, and changed the password to hahp0wnedJ00.



Conclusion

In this lab we used Netflow and Wireshark to analyze a pacap that contains malicious activity. We also learn how to add decryption keys to decrypt wireless traffic. It is important to change default password in order protect ourselves from attackers.

References

[1] https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

[2] https://www.macs.hw.ac.uk/~hwloidl/docs/PHP/features.commandline.html

[3] http://manpages.ubuntu.com/manpages/xenial/man1/nfdump.1.html

[4] https://www.aircrack-ng.org/doku.php?id=deauthentication

[5] https://www.aircrack-ng.org/doku.php?id=simple_wep_crack