CIS 375

Lab 6

3 March 2016

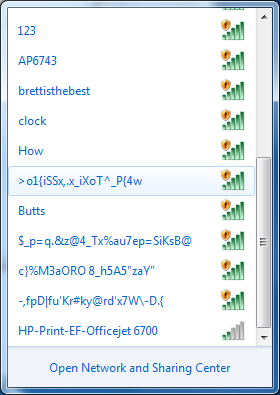
Rodney Fulk

Jason Carr

**Part I. Intro to signals**

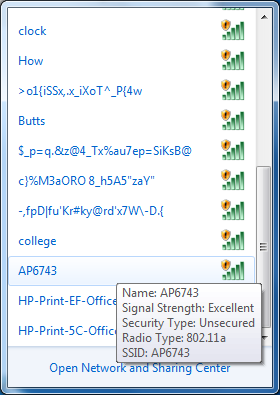
**Q-1: With the number of networks that you found, what effects does this number have on the airtime utilization? Submit a screenshot for the scan output obtained from the Wireless Windows station.**

It slows it down because all of the channels are getting clogged with various frames.

****

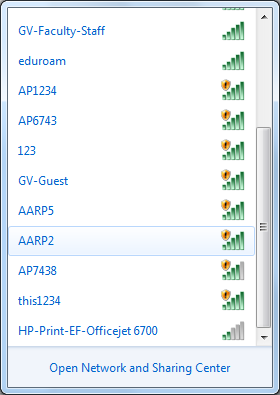
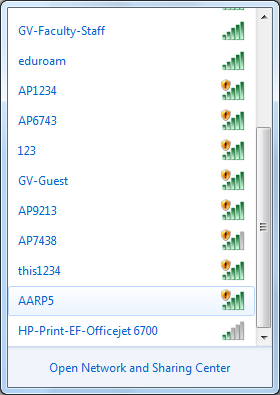
**Q-2: What effect this technique would have on users that associated to the “college” network?**

Students could accidently connect to this spoofed server and send their credentials or other password/sensitive information.

****

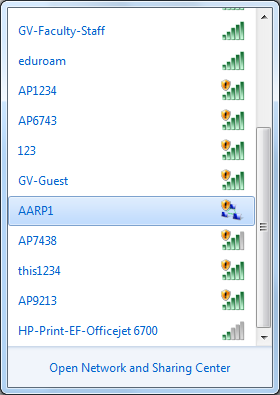
**Q-3: How is this technique would be useful for an attacker against a production wifi network? Submit a screenshot for the scan output obtained from the wireless windows station.**

Because they can imitate known networks and trick people into connecting them instead of the ones they normally would and you can flood the air with fake SSIDs



**Q-4: How different is the current output compared to what has been found in Q-3? Submit a screenshot for the scan output from the wireless windows station.**

It creates an adhoc AP.



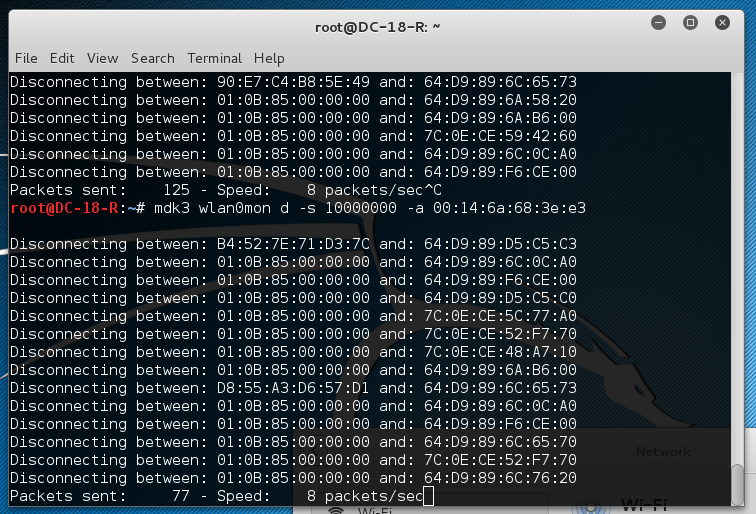
**Part 2. Running MDK3 in Mode ‘d’**

**Q-5: Do you still have the ping command running successfully?**

yes, nothing changed with the ping. We did see some delays in the ping response that could have been an indication of an attack but nothing preventing ping from completing.

**Q-6: Increase the speed of attack gradually in multiple trials and determine if this attack is successful in deauth-ing any stations and why? Submit a screenshot.**

There was no obvious successful attack. If there were any successful attacks that detached the client the client must have reconnected right away.

****

**1.3 Authentication Denial of Service Flood Mode**

**Q-7: Can WSTA associate to your AP? Try attack speed and report your observation for what happened in each case.**

WSTA was never disconnected from the AP. The attacking STA is getting the message “AP/MAC seems to be invulnerable” regardless of speed

**Q-8: Use a one minute interval and record how many fake clients are able to connect to the AP until the end of a 5 minute window.**

65000+

To prevent beacon flooding, we have to set up our network to detect when an abnormal number of probe requests are found. One of the best methods appears to be a wireless intrusion prevention system (wIPS). Whenever unauthorized access points are identified, security managers and IT admins can be notified, so those access points can be (sometimes automatically) "contained" and endpoints blocked. Also in my reading there was a countermeasure where a network detected the offending APs and was able to change channel and then ‘drown’ out all the bad SSIDs.

To prevent connecting to a spoofed SSID, there are a few options that we can take. The first being always take advantage of WPA or WPA2 in hotspots that support this option. In those hotspots, we can avoid fake APs altogether by configuring our device’s Wi-Fi connection to check the hotspot authentication server's certificate.

Next, turn off auto-connect. This will help prevent us from automatically connecting to an “evil twin” of the server that we have previously visited. It is one extra step where we can control what we connect to.

To prevent denial of service (DoS) attacks, having robust hardware and software seems to be key. Newer systems are capable of handling the larger TCP/IP packets and are not as likely to crash when the size gets near 66 Kb like pre 1998 hardware.

Also during ping of death attacks, if we are able to identify our attacker’s IP, we can use our firewall to block it and filter them out preventing them from clogging our airtime.

We can use wIPS here too. The wIPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.