The Integration of BeagleBone and Kali Linux for Wireless Network Attacks

Rachel Rackal, Christopher Robledo, Aparicio Carranza

Computer Engineering Technology

New York City College of Technology – CUNY

ECC 2015 Conference, June 14 – 16, 2015
Marist College, Poughkeepsie, NY

Kali Linux Tools

Overview of Networking Security

THREE MAIN STRUCTURED ATTACKS

[1] Reconnaissance Attack – Gathering Data and looking for vulnerabilities

Ettercap -Graphical & Wireshark

[2] Access Attack – Attempt to gain access & exploit vulnerabilities

[3] Denial of Service Attack (DoS) - Affect system availability

Metasploit Framework offers Airmon-ng, Airodump-ng, Aireplay-ng

Implementation of Hardware

- ✓ 1 GHz processor compared to the 700 MHz processor of the Raspberry Pi
- ✓ 2GB of onboard eMMC flash memory.
- ✓ Micro SD card flashed with Kali Linux OS
- ✓ Alfa 802.11 b/g/n Long-Range USB Adapter

Aircrack-ng Package

- Ifconfig
- airmon-ng start wlan0
- iwconfig mon0
- airodump-ng mon0
- aireplay-ng

Denial of Service Attack

Performing a Network De-Authentication Attack

Video Demonstration

Man in the Middle Attack

Video Demonstration

The Man in The Middle Attack (MiTM)

Method of Capturing Traffic

- ❑Attacker is the intercepted connection between server and client/host
  Client doesn't know about another contact point (re-routed packets)
- ❑**Ettercap-Graphical** scanned for hosts and targets were ARP poisoned
- ❑The router was target one and the host/client was target 2
- ❑Unified Scan was executed – MiTM

- ✓**Wireshark** – captured packets of data transferring between targets
- ✓Filter HTTP –POST protocol to obtain data posted from target to web(through router)
- ✓Packets were carefully analyzed (no decryption)
- ✓Username and Password were obtained in packet

In Summary

Troubleshooting

- Installing every package
- Airodump-ng not available as a package for ARM

Future Research

- Write a script for Airodump-ng
- Perform Access Attacks
- Exploiting Vulnerabilities
  - *Port Sniffing*
  - *Wireshark decryption of HTTPS packets of data*