Term 1

Snooping IoT devices with a Raspberry Pi

a UWC/CSIR project

Hi,

Name: Samuel Abu

Supervisor: Dr Michael Norman

Co-supervisor: Muyowa Mutemwa (CSIR)

Co-supervisor: Francois Mouton (CSIR)

Overview

- Background
- Purpose of project
- User Requirements
- Requirements Analysis
- Project Timeline
- References
- Questions

Background

61%

➤ Percent of organizations that have deployed some level of IoT technologies, and have had to deal with a security incident related to IoT in the past year.

Source: Internet of Things Cybersecurity Readiness (Osterman Research for Trustwave)

Purpose of project

➤ The purpose of the project is to create Cyber Security Awareness and to demonstrate how easy it is to identify IoT devices and access information on such devices over a WiFi network.

User Requirements

➢ Build a snooping tool and set up Command & Control center

➢ The snooping tool must be able to detect other connected devices on the network.

➢ Some information (e.g type of device) from a detected device should be sent from the snooping tool to the Command & Control center.

➢ The sent information from the detected device must be non-malicious.

User Requirements

Raspberry Pi

Send discovered device names and other information to a normal computer

Computer

Backpack

Requirements Analysis

- Connect to available network and detect IoT devices
- Penetrate device and obtain non-malicious info
- Send obtained info to Command & Control center
- Display Snooping report

Requirements Analysis

The Snooping Tool

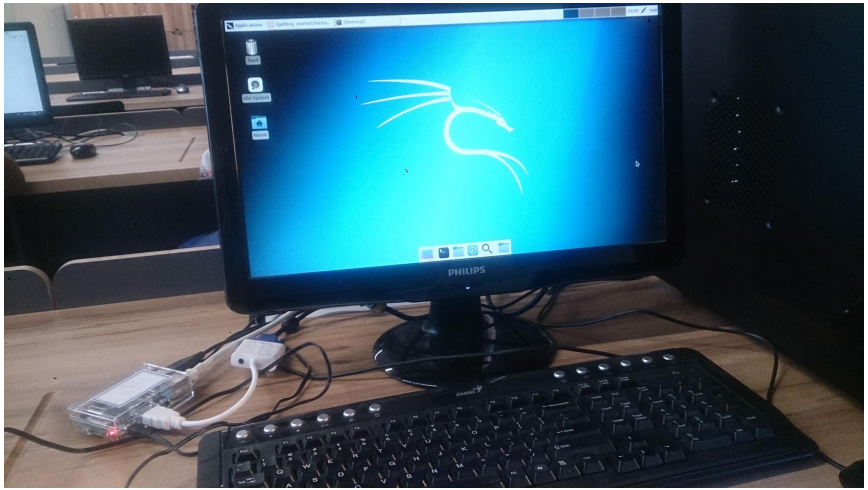
The Raspberry Pi 3 would be used as the snooping tool.

It will be used to connect to a network and detect other IoT devices on the network.

A Raspberry Pi is a credit card-sized computer originally designed for education, inspired by the 1981 BBC Micro.

Requirements Analysis

The Snooping Tool: Raspberry Pi connected to desktop monitor



Current state of snooping tool at the Hons lab


Applications
Places
Fri 13:48
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Activities Overview
Iceweasel
Terminal
Files
metasploit...
armitage
burpsuite
maltego
beef xss fr...
faraday IDE
Leafpad
Tweak Tool

Requirements Analysis

Software-to-be-used

- Kali Linux OS

Hardware-to-be-used

- Raspberry Pi 3
- Desktop Computer

“Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments.”

Requirements Analysis

Kali Linux OS tools likely to be used are:

- Fern-wifi-cracker
- Wifite
- airodump-ng

Command & Control center

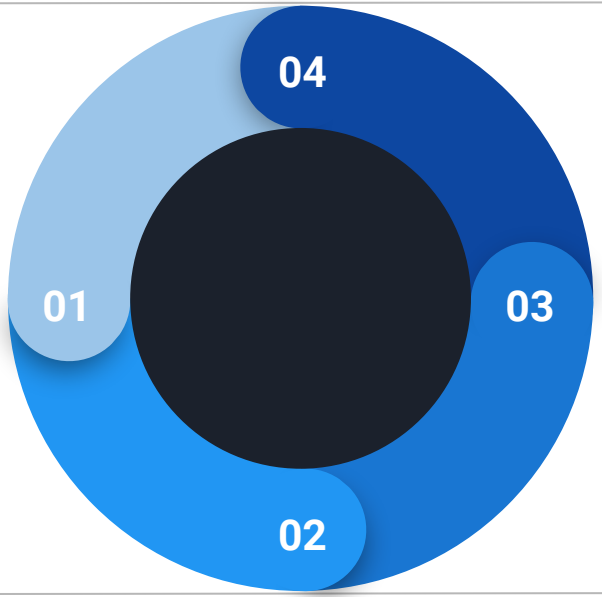
The desktop computer at the Honours lab will be used as a Command & Control center.

Project Plan

Term 1: Requirements Gathering and Requirements Analysis

Term 2: Prototyping

- More research of Kali Linux tools
- Use tools to set up C&C center
- Some testing



Term 4: Final Presentation

Term 3: Implementation

References

[1] Vijayan, J., 2018. “The 30 cybersecurity stats that matter most,”https://techbeacon.com/30-cybersecurity-stats-matter-most, accessed: 2018-04-26.

[2] M. Niket, D. Jaiswal, and P. Y. B. Mane, “Design and implementation of raspberry pi based remote home security and appliance control system.”, http://www.ijsrd.com/articles/IJSRDV3I50124.pdf accessed: 2018-04-22

[3] Noah Apthorpe, Dillon Reisman, Aug. 2017. “Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic,” https://arxiv.org/pdf/1708.05044.pdf, accessed: 2018-04-15.

Thank you for listening

Questions?