Capstone Project

IoT based Penetration Testing

# Project Overview:

Penetration testing is field of ethical hacking concentrating on exploiting the weakness of a system. Iot penetration testing is similar but at a smaller scale where the exploitation require customized attack and efficient use of resources, algorithms and payloads to target vulnerable assets. The project discusses customized way to use penetration testing on IoT devices.

# Introduction

A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers find the weaknesses in a system using the same tools, techniques, and processes as attackers to find and demonstrate the business impacts. Penetration tests simulate attacks that could threaten an IT infrastructure and its various constituents, which may be exposed as a result and lead to leakage of confidential or proprietary data. They can examine whether a system is robust enough to withstand attacks from authenticated and unauthenticated positions, as well as a range of system roles. With the right scope, a pen test can dive into any aspect of a system[1]

## IoT architecture

# IoT based penetration testing includes engaging to test application and physical layers.

### Sensing layer

This consists of the hardware sensors and sensor networks.

### Communication Layer

This consists of the communication mechanism that allows thesensing layer to communicatewith the Management layer for example – Wifi, 3G, LTE, Ethernet etc.

### Management Layer

This is the topmost layer and is responsible for making sense out of the raw data and provide a presentable and fancy view to the users. It includes the cloud, storage, apps etc.

## Exploits

### Application layer attack

Socket and port can be exposed due to poor utilization of the practices

e.g. user authentication, others

### Hardware layer attack

Easy access to hardware without any authentication or user privileges control.

## Experiment

### Nmap reconnaissance

### Nesses vulnerability

### Payload deployment

### Information Collection

## Result

In progress…

## Work In progress

## Uncompleted work

## Summary

Possible student prompts: What did you learn? What worked well? What was the most challenging aspect of this project? What will you do differently next time?

## Add the link to your project here:

[gagansur/IoT-Pentesting (github.com)](https://github.com/gagansur/IoT-Pentesting)