Problem Statement:

In order to conduct an Internal Network Penetration Testing, organization needs to provide and setup a physical system for security engineer within the organization in which engineer can install tools needed for performing Reconnaissance, further vulnerability assessments and do an exploiting weakness manually. It takes Hardware Cost and consume time and space.

Also, when a cyber security firm gets an offer to conduct a Vulnerability Assessment and Penetration Testing audit of the large distributed organization that enclosed multiple locations around the world. Then it is impractical to travel each location to deliver native penetration testing services.

And many organizations have security measures in place to block incoming connections with the goal of preventing backdoors into their network. In a white-box assessment, you'll be explicitly ready to open up a firewall to allow SSH to your Raspberry Pi. The bad news is even though this is often possible from a policy standpoint, it's going to be difficult to accomplish when handling multiple sites under multiple administrative controls.

Objective:

To provide a feasible solution towards conducting vulnerability assessment and penetration testing remotely using Raspberry Pi.

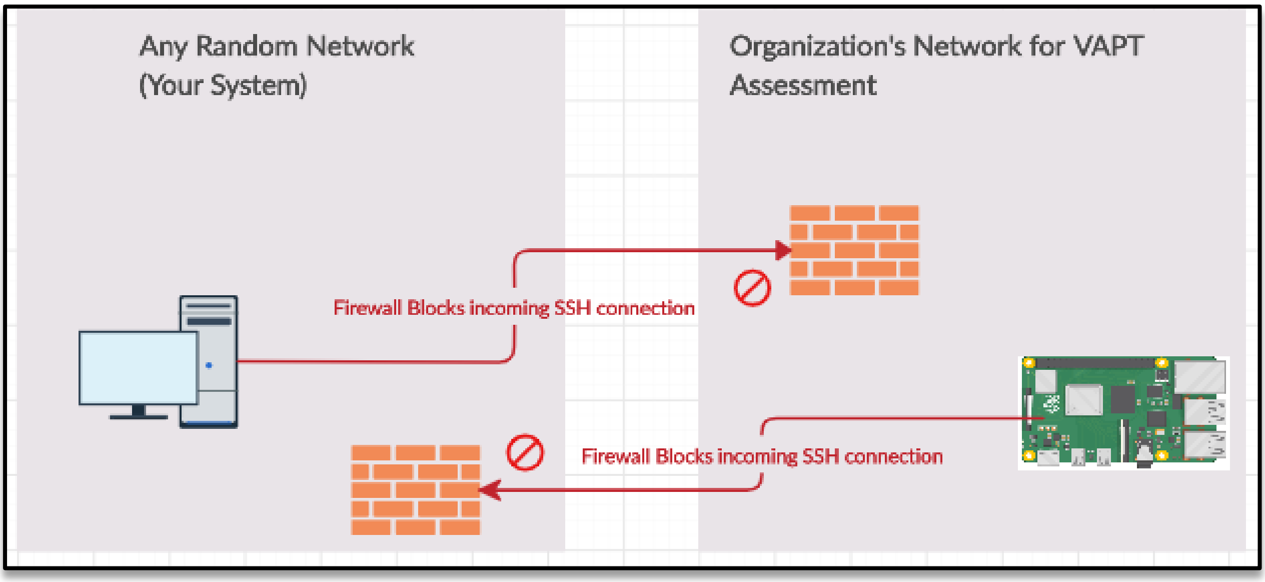
Technologies:

Linux, Command and Control Server (VPS), Reverse SSH Tunnel, VPN Tunnelling

Languages:

Bash Scripting, Python

Diagrams:


Any Random Network
(Your System)
Organization's Network for VAPT
Assessment
Firewall Blocks incoming SSH connection
Firewall Blocks incoming SSH connection