Securing Your Network

How to get Started

- To secure a network, we must first know it by the roots

- **Vulnerability Assessment**

  security exercises that aid in identifying security liabilities within networks, applications, and systems

Create a Blueprint

- Devise a plan
  - Inductive Approach
  - Deductive Approach
- Partition your network/Host
  - core
  - Edge
  - DMZ
- Identify what needs the most work

- Identify risks of the VA process
  - Technical
  - Organizational
  - Legal

- Checklists are available!
  - Open Source Security Testing Methodology Manual (OSSTMM)
  - Open Web Application Security Project(OWASP)
  - SANS Institute

Assess your network

- Start from the core
  - Collect system/network information
- Branch out! [Entire network/hosts]
- Create inventory of Devices, servers, systems, OS
- Note already implemented security measures
  - ACLs
  - Firewalls

Identify vulnerabilities

- Start with basics
  - Identify weak links
  - Insecure servers/hosts
  - check for Outdated OS, app. Versions
- Check for false positives
- Dig In
  - check for open ports, unused services

- check for known vulnerabilities
  - Common Vulnerabilities & Exposure (CVE)
  - vulnerability databases, NVD
- Use tools
  - OvenVAS : framework for vulnerability assessment and management
  - Nessus : Remote security scanner
  - Metasploit : assess/manage security
  - nmap : Network/host discovery

Fix it

- Secure!

  -Many tools generate a report!

  - Prioritize remediation

  - Check if available solution is feasible to your network

  - Access control

  - Secure open ports – Block unnecessary ones

- Secure

  - Disable unwanted services
  - Harden your hosts
  - Upgrade system
  - Backup!

- Is Penetration Testing required?

  - Check if it is feasible to perform penetration testing in your network

Policies

- Create policy/Plan for the future
- Scheduled Maintenance and testing
- Devise risk management and incident handling based on the report
- Schedule System upgrades