

Cisco VIP 2023 Assignment 1

Name: Vignesh L

Networking Academy ID: 1049483238

Task 1 Campus Network Analysis:

Sri Sairam Engineering College is chosen for campus network analysis

Task 2 Network Mapping:

packet tracer file is attached in this zip file

Task 3:

Attack Surface Mapping

Vulnerabilities Identified:

- Open ports. There are a number of open ports on the network, which could be used by attackers to gain access to the network.
- Unpatched vulnerabilities. There are a number of unpatched vulnerabilities on the network, which could be exploited by attackers.
- Weak passwords. The passwords for some of the devices on the network are weak, which could be easily cracked by attackers.
- No firewall which is very comfortable for hackers
- Misconfigured devices. Misconfigured devices can also be a source of vulnerabilities. If a device is not configured properly, it may be vulnerable to attack.
- Social engineering attacks. Social engineering attacks are a type of attack that relies on human interaction to trick users into giving up sensitive information or clicking on malicious links. These attacks can be very effective, even against well-trained users.

Counter measures:

- Close open ports. The open ports on the network should be closed to prevent attackers from gaining access.
- Patch vulnerabilities. The vulnerabilities on the network should be patched to prevent attackers from exploiting them.
- Change passwords. The passwords for the devices on the network should be changed to strong passwords.

- Introduction of firewall will safeguard the network system
- Configure devices properly. Devices should be configured according to the manufacturer's security recommendations.
- Train users about security. Users should be trained about security risks and how to protect themselves from attack.

Task 4: Secure Access controls

Vlan is used in my assignment to have a secured connection among the campus