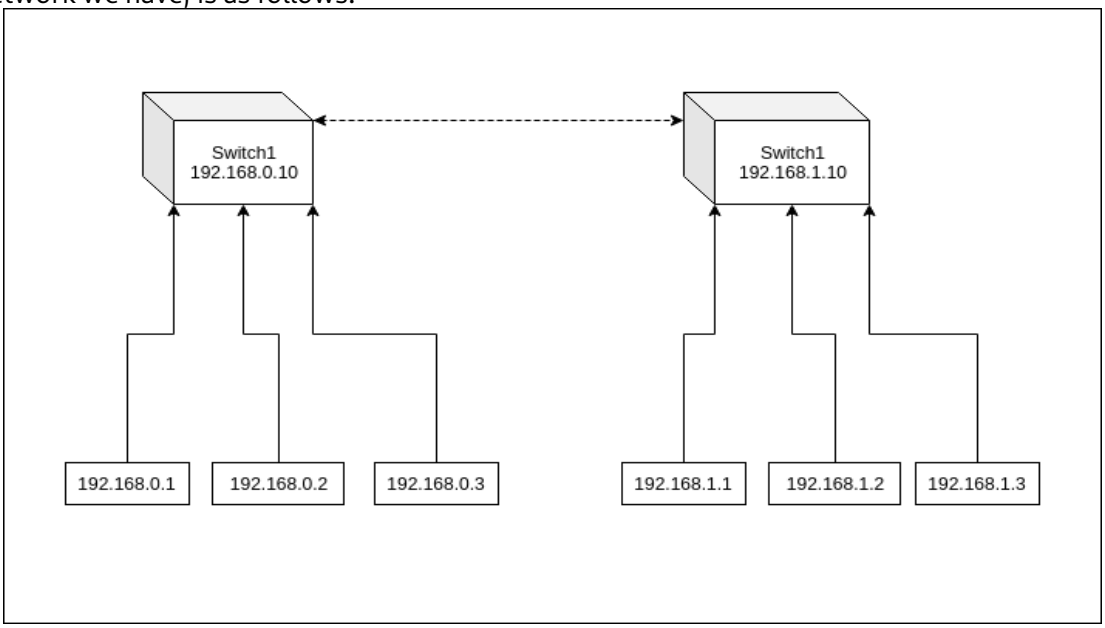
Goa College Of Engineering

Expt No: 8 Date:

Aim:

Theory:
The network we have, is as follows.



Types of computer defense techniques:

1. Network Security Controls:
   - The first line of defense when securing a network is the analysis of network traffic.
   - Firewalls prevent access to and from unauthorized networks and will allow or block traffic based on a set of security rules.
   - Intrusion protection systems often work in tandem with a firewall to identify potential security threats and respond to them quickly.
2. Antivirus Software:
   - Antivirus software is critical to protecting against viruses and malware. However, many variants often rely heavily upon signature-based detection.
   - While these solutions offer strong protection against malicious software, signature-based products can be exploited by intelligent cyber criminals.
   - For this reason, it is wise to use an antivirus solution that includes heuristic features that scan for suspicious patterns and activity.
3. Analyzing Data Integrity:
   - Every file on a system has what is known as a checksum.
   - This is a mathematical representation of a file that shows the frequency of its use, its source and which can be used to check against a known list of viruses and other malicious code.

- If an incoming file is completely unique to the system it may be marked as suspicious. Data integrity solutions can also check the source IP address to ensure it is from a known and trusted source.

4. Behavioral Analysis:
   - File and network behaviors often provide insight while a breach is in progress or has occurred.
   - If behavioral analysis is activated it means the firewall or intrusion protection solutions have failed. Behavioral analysis picks up the slack and can either send alerts or execute automatic controls that prevent a breach from continuing any further.
   - For this to work effectively, organizations need to set a baseline for "normal" behavior.

1. Network Security Controls:

   - Network access control is a method of enhancing the security of a private organizational network by restricting the availability of network resources to endpoint devices that comply with the organization's security policy. A typical network access control scheme comprises of two major components such as Restricted Access and Network Boundary Protection.
   - Restricted Access to the network devices is achieved through user authentication and authorization control which is responsible for identifying and authenticating different users to the network system. Authorization is the process of granting or denying specific access permissions to a protected resource.
   - Network Boundary Protection controls logical connectivity into and out of networks. For example, multiple firewalls can be deployed to prevent unauthorized access to the network systems. Also intrusion detection and prevention technologies can be deployed to defend against attacks from the Internet.

I. Securing Access to Network Devices:

   - Restricting access to the devices on network is a very essential step for securing a network. Since network devices comprise of communication as well as computing equipment, compromising these can potentially bring down an entire network and its resources.
   - Paradoxically, many organizations ensure excellent security for their servers and applications but leave communicating network devices with rudimentary security.\
   - An important aspect of network device security is access control and authorization. Many protocols have been developed to address these two requirements and enhance network security to higher levels.

II. User Authentication and Authorization:

   - User authentication is necessary to control access to the network systems, in particular network infrastructure devices. Authentication has two aspects: general access authentication and functional authorization.
   - General access authentication is the method to control whether a particular user has "any" type of access right to the system he is trying to connect to. Usually, this kind of access is associated with the user having an "account" with that system. Authorization deals with individual user "rights". For example, it decides what can a user do once authenticated; the user may be authorized to configure the device or only view the data.

- User authentication depends up on factors that include something he knows (password), something he has (cryptographic token), or something he is (biometric). The use of more than one factor for identification and authentication provides the basis for Multifactor authentication.

III. Password Based Authentication:

- At a minimum level, all network devices should have username-password authentication. The password should be non-trivial (at least 10 character, mixed alphabets, numbers, and symbols).
- In case of remote access by the user, a method should be used to ensure usernames and passwords are not passed in the clear over the network. Also, passwords should also be changed with some reasonable frequency.

IV. Centralized Authentication Methods:

- Individual device based authentication system provides a basic access control measure. However, a centralized authentication method is considered more effective and efficient when the network has large number of devices with large numbers of users accessing these devices.
- Traditionally, centralized authentication was used to solve problems faced in remote network access. In Remote Access Systems (RAS), the administration of users on the network devices is not practical. Placing all user information in all devices and then keeping that information up-to-date is an administrative nightmare.
- Centralized authentication systems, such as RADIUS and Kerberos, solve this problem. These centralized methods allow user information to be stored and managed in one place. These systems can usually be seamlessly integrated with other user account management schemes such as Microsoft's Active Directory or LDAP directories. Most RADIUS servers can communicate with other network devices in the normal RADIUS protocol and then securely access account information stored in the directories.

V. Access Control Lists:

- Many network devices can be configured with access lists. These lists define hostnames or IP addresses that are authorized for accessing the device. It is typical, for instance, to restrict access to network equipment from IPs except for the network administrator.
- This would then protect against any type of access that might be unauthorized. These types of access lists serve as an important last defense and can be quite powerful on some devices with different rules for different access protocols.

2. Antivirus Software:

- Antivirus software is designed to detect, prevent, and remove malicious software, aka malware. The classification of malware includes viruses, worms, trojans, and scareware, as well as (depending on the scanner) some forms of potentially unwanted programs (such as adware and spyware).
- Free Versus Fee :
  - Antivirus software is sold or distributed in many forms, from standalone antivirus scanners to complete Internet security suites that bundle antivirus with a firewall, privacy controls, and other adjunct security protection. Some vendors, such as Microsoft, AVG, Avast, and AntiVir offer free antivirus software for home use (sometimes extending it for small home office — also called SOHO — use as well)

- Periodically, debates will ensue as to whether free antivirus is as capable as paid antivirus. A long-term analysis of AV-Test.org antivirus software testing suggests that paid products tend to demonstrate higher levels of prevention and removal than do free antivirus software. On the flip side, free antivirus software tends to be less feature-rich, thereby consuming fewer system resources which suggest it may run better on older computers or computers with limited system capacity.
- Whether you opt for free or fee-based antivirus is a personal decision that should be based on your financial capabilities and the needs of your computer. What you should always avoid, however, are pop-ups and advertisements that promise a free antivirus scan. These ads are scareware — bogus products that make erroneous claims that your computer is infected in order to trick you into buying a fake antivirus scanner.

◦ Signatures Can't Keep Up :

- Despite its ability to effectively field the majority of malware, a significant percentage of malware can go undetected by traditional antivirus software. To counter this, a layered security approach provides the best coverage, particularly when the layered protection is provided by different vendors. If all security is provided by a single vendor, the attack surface area becomes much larger. As a result, any vulnerability in that vendor's software — or a missed detection — can have a far more adverse impact than would occur in a more diverse environment.

- Regardless, while antivirus software is not a catch-all for every bit of malware out there and additional layers of security are needed, antivirus software should be at the core of any protection system you decide upon, as it will be the workhorse that deters the majority of threats with which you would otherwise have to contend.

3. Data Integrity:
   - Every file on a system has what is known as a checksum.
   - This is a mathematical representation of a file that shows the frequency of its use, its source and which can be used to check against a known list of viruses and other malicious code.
   - If an incoming file is completely unique to the system it may be marked as suspicious. Data integrity solutions can also check the source IP address to ensure it is from a known and trusted source.

4. Behavioral Analysis:
   - Behavior-based security is a proactive approach to managing security incidents that involves monitoring end user devices, networks and servers in order to flag or block suspicious activity.
   - Traditionally, security management has been signature-oriented. In this approach, the security program monitors a data stream and compares source code in files or packets to the source code in an anti-virus vendor's library of known threats.
   - In contrast, behavior-based programs compare the actions of files or network packets to a list of accepted or suspicious actions. In general, signature-based tools are best at identifying and repelling known threats, while behavior-based are best for fighting zero-day threats that have not yet made it onto a list of known threat signatures.

- Behavior-based security software scans for deviations from the norm and has the intelligence to decide whether an anomaly poses a threat or can be ignored. Most behavior-based security programs come with a standard set of policies for which behaviors should be allowed and which should be considered suspicious, but also allow administrators to customize policies and create new policies.
- A behavior-based security software product may be marketed as a behavior-based intrusion detection product, a behavior threat analysis (BTA) product or a user behavior analytics (UBA) products. Some products are sophisticated enough to apply machine learning algorithms to data streams so that security analysts don't need to program in rules about what comprises normal behavior. Others include behavioral biometrics features that are capable of mapping specific behavior, such as typing patterns, to specific user behavior. Most products have advanced correlation engines to minimize the number of alerts and false positives.

5. Summary:

Security Types	Technique 1 (Detect)	Technique 2 (Prevent)	Technique 3 (Recover)
Network Security Controls	WAF/HBF (End Point)	Router Monitoring (Router)	-
Antivirus Software	Signature-Based/IDS (End Point)	IPS (End Point)	-
Data Integrity	-	Backup (End Point)	Roll Back (End Point)
Behavioral Analysis	Heuristic Analysis (End Point)	-	-

Conclusion: