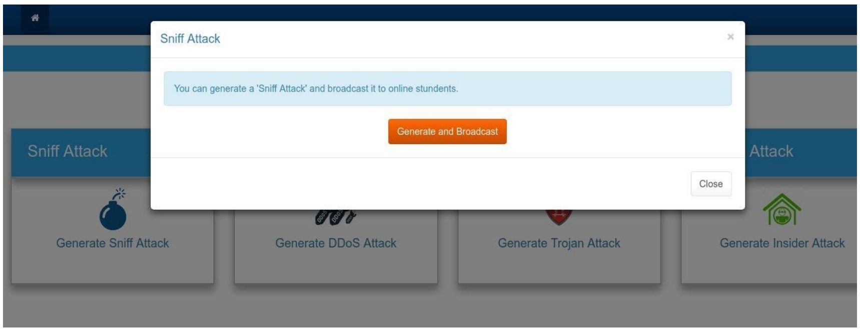
Sniffer Attack

Definition and concepts

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

The teacher can generate and broadcast such attack by navigating to the attack panel and opening the 'Sniff Attack' modal (Fig. 1)



Sniff Attack

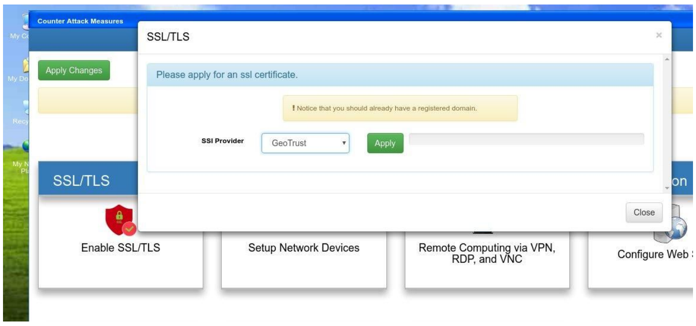
You can generate a 'Sniff Attack' and broadcast it to online stundents.

Figure 1. The Sniff Attack modal.

Counter Measures

To address this attack, the student should:

- Enable SSL/TLS; Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network. The connection is private (or secure) because symmetric cryptography is used to encrypt the data transmitted (Fig. 2).



SSL/TLS

Please apply for an ssl certificate.

! Notice that you should already have a registered domain.

Ssl Provider: GeoTrust

Figure 2. SSL/TLS modal.

- Use switch network device instead of hub in the network; a hub network is more prone to sniffing so its better to use switch instead of hub. Because a network with hub implements a broadcast medium shared by all systems on the LAN. Any data sent over LAN is actually sent to each and every machine connected to LAN. Majority of sniffer tools are ideally suited to sniff data in a hub environment. Switch will not only reduce chances of sniffing but will also increase performance of network (Fig. 3).

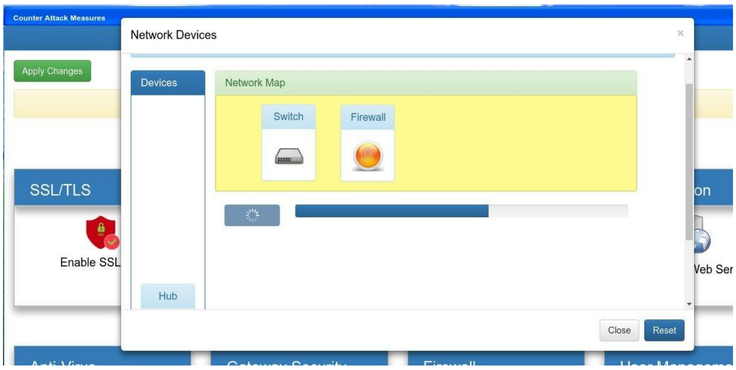


Figure 3. The Network Devices modal.

- Incorporate remote computing via VPN, VNC, and RDP. Usually, remote computing incorporates a layer of encryption. Remote computing includes programs that utilize the VNC (Virtual Network Computing) Protocol or the RDP (Remote Desktop Protocol). On the other hand, a virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network (Fig. 4).

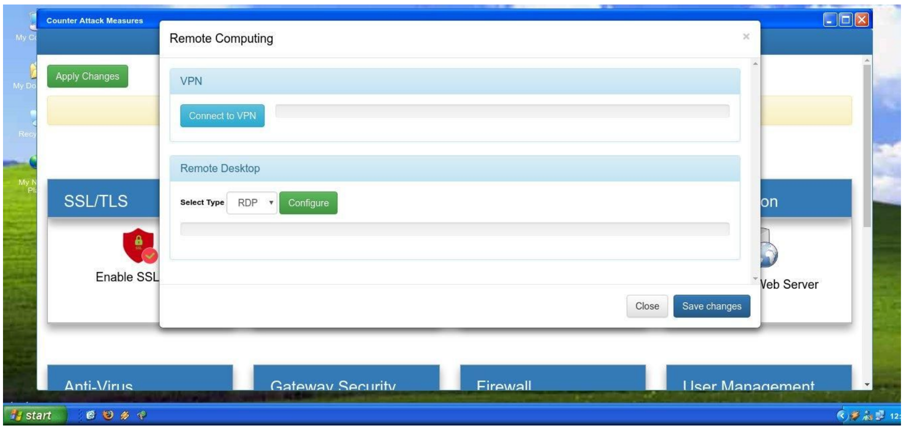


Figure 4. Remote Computing modal.

DDoS Attack

Definition and Concepts

DOS is short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

DDoS is short for Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

Counter Measures

To address such attack, the student should:

- Enable SSL/TLS; as it is described in the previous section (Fig. 2).

- Configure the web server. The student should optimize maximum connection per IP address, optimize maximum http request size, switch to SSL mode and create IP blacklist (Fig. 5).

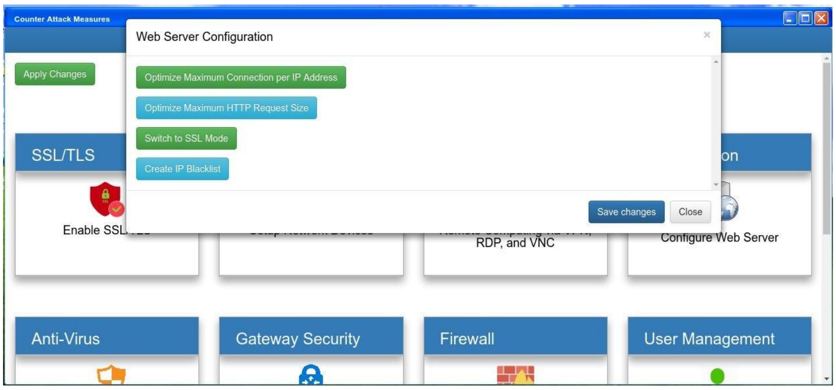


Figure 5. Web Server Configuration modal.

- Install and configure the Load Balancer; a load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of what is a load balancer servers. Load balancers are used to increase capacity (concurrent users) and reliability of applications (Fig. 6).

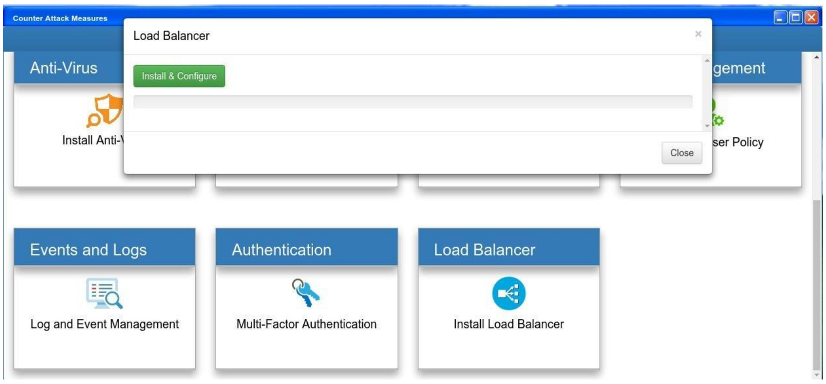
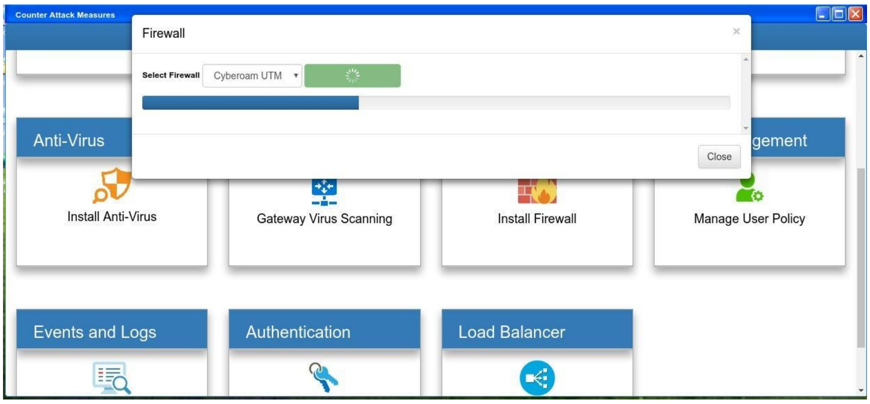


Figure 6. Install Load Balancer modal.

- Install a Firewall; a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules (Fig. 7).



Firewall

Select Firewall: Cyberoam UTM

Figure 7. Install Firewall modal.

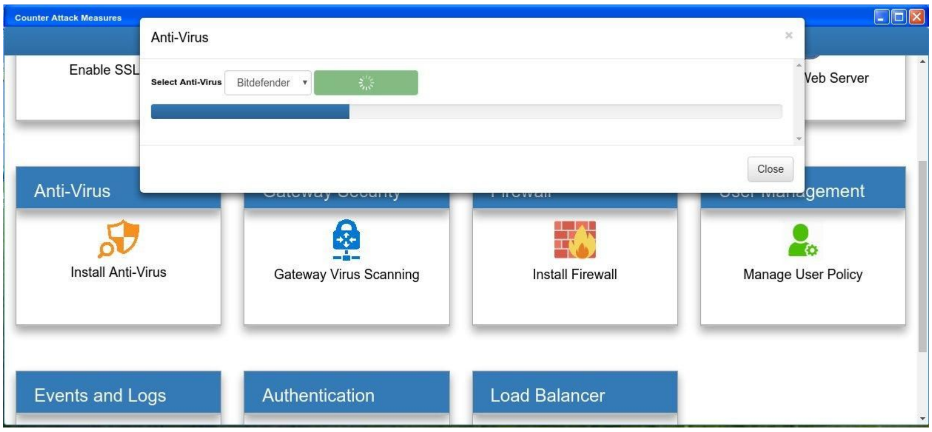
Trojan Attack

Definition and Concepts

A Trojan horse, often shortened to Trojan, is a type of malware designed to provide unauthorized, remote access to a user's computer. Trojan horses do not have the ability to replicate themselves like viruses; however, they can lead to viruses being installed on a machine since they allow the computer to be controlled by the Trojan creator.

Counter Measures

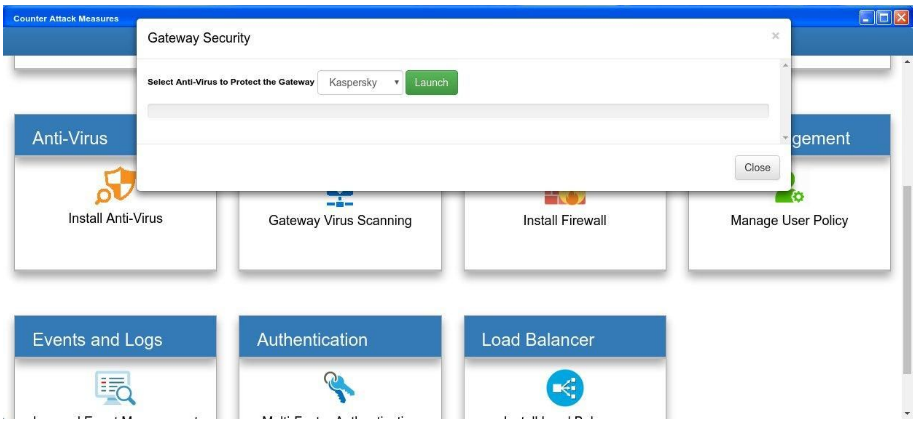
- Install Anti-Virus; anti-virus software is computer software used to prevent, detect and remove malicious software (Fig. 8).



Select Anti-Virus: Bitdefender

Figure 8. Install Anti-Virus modal.

- Gateway virus scanning (Fig. 9).



Select Anti-Virus to Protect the Gateway: Kaspersky

Figure 9. Gateway virus scanning.

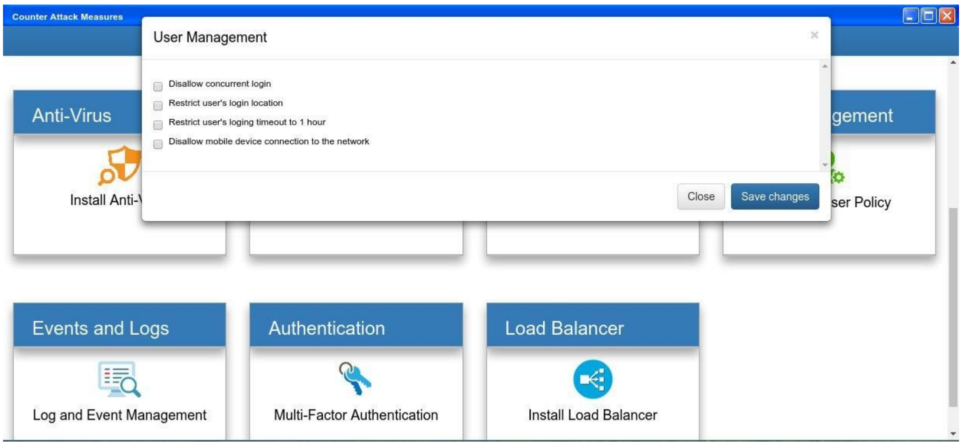
Insider Attack

Definition and Concepts

An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access. Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

Counter Measures

- Manage User Policy; limiting concurrent login, restrict user's location, and disallowing mobile device connection to the network (Fig. 10).

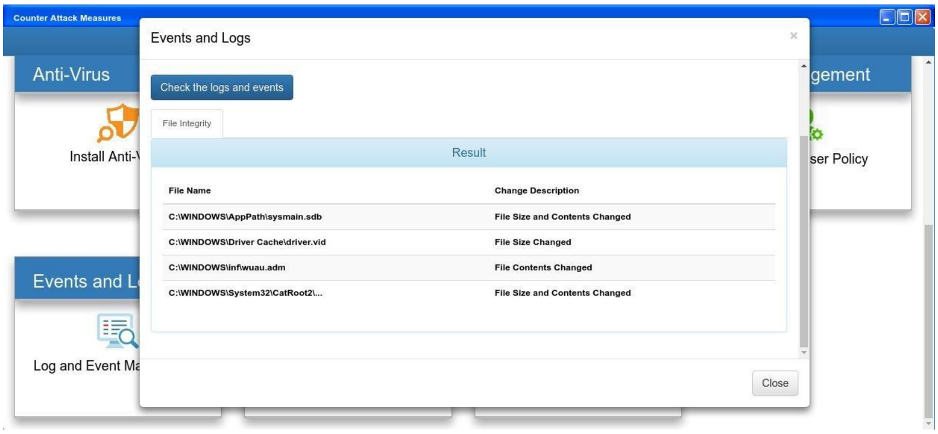


User Management

□ Disallow concurrent login
□ Restrict user's login location
□ Restrict user's loging timeout to 1 hour
□ Disallow mobile device connection to the network

Figure 10. Manage User Policy

- Log and Event Management; using log and event management, helps monitoring users actions (Fig. 11).



Events and Logs

Result

File Name	Change Description
C:\WINDOWS\AppPath\sysmain.sdb	File Size and Contents Changed
C:\WINDOWS\Driver Cache\driver.vid	File Size Changed
C:\WINDOWS\inf\wuau.adm	File Contents Changed
C:\WINDOWS\System32\CatRoot2\...	File Size and Contents Changed

Figure 11. Event and Log Management.

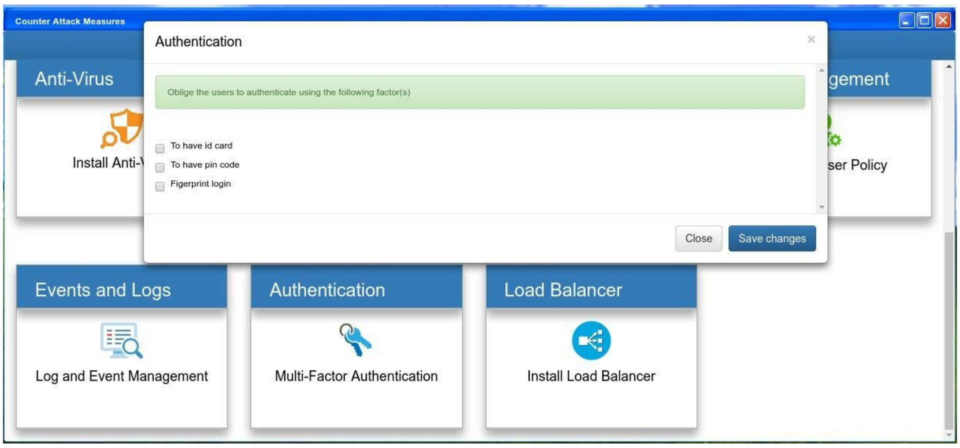
Identity Spoofing

Definition and Concepts

Identity spoofing refers to the action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal. An adversary may craft messages that appear to come from a different principle or use stolen / spoofed authentication credentials.

Counter Measures

- Multi-factor authentication(MFA); MFA is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are) (Fig. 12).



Authentication

Oblige the users to authenticate using the following factor(s)

□ To have id card
□ To have pin code
□ Figerprint login

Figure 12. Mutli-Factor Authentication