16.2.6 Sara Rocío Miranda Mateos 0244643

0244643@up.edu.mx

Lab - Research Network Security Threats

Objectives

Part 1: Explore the SANS Website

Part 2: Identify Recent Network Security Threats

Part 3: Detail a Specific Network Security Threat

Background / Scenario

To defend a network against attacks, an administrator must identify external threats that pose a danger to the network. Security websites can be used to identify emerging threats and provide mitigation options for defending a network.

One of the most popular and trusted sites for defending against computer and network security threats is SysAdmin, Audit, Network, Security (SANS). The SANS site provides multiple resources, including a list of the top 20 Critical Security Controls for Effective Cyber Defense and the weekly @Risk: The Consensus Security Alert newsletter. This newsletter details new network attacks and vulnerabilities.

In this lab, you will navigate to and explore the SANS site, use the SANS site to identify recent network security threats, research other websites that identify threats, and research and present the details about a specific network attack.

Required Resources

- Device with internet access
- Presentation computer with PowerPoint or other presentation software installed

Instructions

Part 1: Exploring the SANS Website

In Part 1, navigate to the SANS website and explore the available resources.

Step 1: Locate SANS resources.

Search the internet for SANS. From the SANS home page, click on FREE **Resources**.

List three available resources.

Políticas de seguridad, sala de lectura y transmisiones web

Step 2: Locate the link to the CIS Critical Security Controls.

The **CIS Critical Security Controls** linked on the SANS website are the culmination of a public-private partnership involving the Department of Defense (DoD), National Security Association, Center for Internet Security (CIS), and the SANS Institute. The list was developed to prioritize the cyber security controls and spending for DoD. It has become the centerpiece for effective security programs for the United States government. From the **Resources** menu, select **Critical Security Controls**, or similar. The CIS Critical Security Controls document is hosted at the Center for Internet Security (CIS) web site and requires free registration to access. There is a link on the CIS Security Controls page at SANS to download the 2014 SANS Critical Security Controls Poster, which provides a brief description of each control.

Select one of the Controls and list implementation suggestions for this control.

Supervisar servidores y dispositivos con herramientas autorizadas
Configurar equipos para no ejecutar contenido
Actualización automatica

Step 3: Locate the Newsletters menu.

Highlight the **Resources** menu, select **Newsletters**. Briefly describe each of the three newsletters available.

SANS Nenbites
@RISJ
OUCH

Part 2: Identify Recent Network Security Threats

In Part 2, you will research recent network security threats using the SANS site and identify other sites containing security threat information.

Step 1: Locate the @Risk: Consensus Security Alert Newsletter Archive.

From the **Newsletters** page, select **Archive** for the @RISK: The Consensus Security Alert. Scroll down to **Archives Volumes** and select a recent weekly newsletter. Review the **Notable Recent Security Issues and Most Popular Malware Files** sections.

List some recent vulnerabilities. Browse multiple recent newsletters, if necessary.

Win Trojan, win Trojan. Changes, Trojan adh

Step 2: Identify sites providing recent security threat information.

Besides the SANS site, identify some other websites that provide recent security threat information.

Www.mcafee - com/us/mcofee

List some of the recent security threats detailed on these websites.

Fareit, Troyano, inostealer, vskm

Part 3: Detail a Specific Network Security Attack

In Part 3, you will research a specific network attack that has occurred and create a presentation based on your findings. Complete the form below based on your findings.

Step 1: Complete the following form for the selected network attack.

Name of attack:	Red code
Type of attack:	Gusano
Dates of attacks:	Julio 2001
Computers / Organizations affected:	359 000
How it works and what it did:	
Aprovecha desbordamiento de buffer en MIIS sin porches replicados Inició en una denegación de servicio Esperar 20 días para atacar	
Mitigation options:	
Microsoft para IIS	
References and info links:	
CERT Adu CA 2001 - Laeye	

Step 2: Follow the instructor's guidelines to complete the presentation.

Reflection Questions

1. What steps can you take to protect your own computer?

   Actualizar el sistema
   Firewall
   Contraseñas
   Encriptación

2. What are some important steps that organizations can take to protect their resources?

   Firewalls, detección de intrusos, políticas de seguridad