实验 - 研究网络安全威胁

目标

第 1 部分：探索 SANS 网站

第 2 部分：识别近期网络安全威胁

第 3 部分：详细说明特定网络安全威胁

背景/场景

为了保护网络免受攻击，管理员必须识别威胁网络安全的外部威胁。安全网站可用于确定新兴威胁并为网络防护提供缓解选项。

一个最常见而且可信任的计算机和网络安全威胁防护站点是系统管理和网络安全审计 (SysAdmin, Audit, Network, Security, SANS)。SANS 站点提供多种资源，包括用于有效网络防御的 20 大关键安全控制和每周一期的《@安全风险：安全警告共识时讯》(@Risk: The Consensus Security Alert newsletter)。该时讯详细介绍新出现的网络攻击和漏洞。

在本实验中，您将导航到 SANS 站点并探索它，使用 SANS 站点确定近期网络安全威胁，研究其他识别威胁的网站，并且研究和展示有关特定网络攻击的详细信息。

所需资源

- 能够访问互联网的设备
- 安装了 PowerPoint 或其他演示软件用来做演示的计算机

第 1 部分： 探索 SANS 网站

在第 1 部分中，导航至 SANS 网站并探索可用资源。

第 1 步： 查找 SANS 资源。

导航至 www.SANS.org。在主页上，突出显示 **Resources**（资源）菜单。

列出三个可用资源。

第 2 步： 查找排名前 20 位的关键控件。

SANS 网站上列出的 **Twenty Critical Security Controls for Effective Cyber Defense**（有效网络防御的二十大关键安全控制方法）是美国国防部 (DoD)、国家安全协会、互联网安全中心 (CIS) 和 SANS 协会这些公私机构合作的结晶。该列表旨在为 DoD 提供网络安全控制和费用的优先级排序。它已成为美国政府有效安全计划的核心。从 **Resources**（资源）菜单中，选择 **Top 20 Critical Controls**（20 大关键控制方法）。

从 20 大关键控制方法中选择一个方法，并为该控制方法列出三种实施建议。

第 3 步：查找 Newsletters（实时通讯）菜单。

突出显示 **Resources**（资源）菜单，选择 **Newsletters**（实时通讯）菜单。简要描述三个可用实时通讯中的每一个实时通讯。

第 2 部分：识别近期网络安全威胁

在第 2 部分中，您将使用 SANS 站点研究近期网络安全威胁并识别其他包含安全威胁信息的站点。

第 1 步：查找《@安全风险：安全警告共识时讯》(@RISK: The Consensus Security Alert Newsletter) 的档案。

在 **Newsletters**（实时通讯）页面，选择《@安全风险：安全警告共识时讯》(@RISK: The Consensus Security Alert) 的 **Archive**（档案）。向下滚动到 **Archives Volumes**（档案卷宗）并选择近期的每周实时通讯。查看 **Notable Recent Security Issues and Most Popular Malware Files**（值得注意的近期安全问题及最常见恶意文件）部分。

列出一些近期攻击。如有必要，请浏览多条近期实时通讯。

第 2 步：识别提供近期安全威胁信息的站点。

除 SANS 站点外，确定一些提供近期安全威胁信息的其他网站。

列出这些网站上详细描述的一些近期安全威胁。

第 3 部分：详细描述一个特定网络安全攻击

在第 3 部分中，您将研究出现的特定网络攻击并根据自己的调查结果创建一个演示文稿。根据您的调查结果完成下表。

第 1 步：完成以下有关所选网络攻击的表格。

攻击名称：	
攻击类型：	
攻击日期：	
受影响的计算机/组织：	
它的工作原理及行为：	
缓解选项：	
参考和信息链接：	

第 2 步: 按照教师的指导完成演示。

思考

1. 您可以采取哪些措施保护您的计算机？

2. 组织可以用来保护其资源的一些重要步骤是什么？