# 思科CCNA网络安全运营1.0

## 第1章测验

什么是非法无线热点？

选择一项：

* 它是使用过时设备设置的热点。
* 它是不加密网络用户流量的热点。
* 它是不实施强用户身份验证机制的热点。
* 它是看似来源于合法业务的热点，但实际上由某人在未经企业许可的情况下设置。

反馈

Refer to curriculum topic: 1.1.1

非法无线热点是指在未经企业或组织正式许可的情况下在企业或组织中运行的无线接入点。

正确答案是：它是看似来源于合法业务的热点，但实际上由某人在未经企业许可的情况下设置。

如何使用 SOC 中的安全信息和事件管理系统帮助相关人员抵御安全威胁？

选择一项：

* 通过过滤网络流量
* 通过收集和过滤数据
* 通过对网络资源的用户进行身份验证
* 通过对远程站点的通信进行加密

反馈

Refer to curriculum topic: 1.2.1

安全信息和事件管理系统 (SIEM) 结合多个来源的数据，帮助 SOC 人员收集和过滤数据，检测威胁并对其进行分类，分析和调查威胁，管理资源以实施预防措施。

正确答案是：通过收集和过滤数据

术语“网络运营分析师”指的是 SOC 中的哪一群人员？

选择一项：

* SOC 经理
* 一级人员
* 二级人员
* 三级人员

反馈

Refer to curriculum topic: 1.2.1

在典型的 SOC 中，一级人员被称为警报分析师，也称为网络运营分析师。

正确答案是：一级人员

计算机在允许同一用户访问用户数据之前，向用户显示要求付款的屏幕。该恶意软件属于哪一类型？

选择一项：

* 一种病毒
* 一种逻辑炸弹
* 一种蠕虫
* 一种勒索软件

反馈

Refer to curriculum topic: 1.1.1

勒索软件通常加密计算机上的数据，并使数据不可用，直到计算机用户支付特定金额的赎金。

正确答案是：一种勒索软件

出于政治或社会原因进行黑客攻击的黑客称为什么？

选择一项：

* 白帽黑客
* 黑客
* 蓝帽黑客
* 激进黑客

反馈

Refer to curriculum topic: 1.1.2

该术语用于描述因某种正义原因聚集并提供保护的灰帽黑客。

正确答案是：激进黑客

在 SOC 安全信息和事件管理系统中应包含哪三项技术？（选择三项。）

选择一项或多项：

* 代理服务
* 威胁情报
* 安全监控
* 用户身份验证
* 入侵防御
* 事件收集、关联和分析

反馈

Refer to curriculum topic: 1.2.1

SOC 中的技术应包括以下内容：

事件收集、关联和分析

安全监控

安全控制

日志管理

漏洞评估

漏洞跟踪

威胁情报

代理服务器、用户身份验证和 IPS 是在网络基础设施中部署并由 NOC 管理的安全设备和机制。

正确答案是：威胁情报, 安全监控, 事件收集、关联和分析

什么是网络战？

选择一项：

* 网络战仅攻击军事目标。
* 网络战旨在破坏或损坏国家利益。
* 网络战是对大公司的攻击。
* 网络战是一个只涉及机器人和机器人之间的攻击的战争。

反馈

Refer to curriculum topic: 1.1.3

参考课程主题：5.1

本题目基于演讲中的内容信息。

网络战是信息战（IW）的子集。 它的目标是破坏(可用性)、损坏(完整性)或利用(保密或隐私)。 它可以直接针对军事力量,关键的基础设施,或其他国家利益,如经济目标。 它涉及协同工作的许多团队。 僵尸网络可能是用于发起攻击的工具之一。

正确答案是：网络战旨在破坏或损坏国家利益

哪个组织是提供 CISSP 认证的国际非营利性组织？

选择一项：

* IEEE
* GIAC
* (ISC)2
* CompTIA

反馈

Refer to curriculum topic: 1.2.2

(ISC)² 是一个提供 CISSP 认证的国际非营利性组织。

正确答案是：(ISC)2

将职称与 SOC 人员职责进行匹配。（并非所有选项都会用到。）

* 三级主题专家
* 二级事件响应人员
* 一级警报分析师

反馈

Refer to curriculum topic: 1.2.1

正确答案是：三级主题专家 → 参与潜在危险的搜索并实施威胁检测工具, 二级事件响应人员 → 参与事件的深入调查, 一级警报分析师 → 监控收到的警报并验证是否确实发生了事件

在 SOC 中验证安全事件之后，事件响应人员将检查事件，但无法识别事件的来源并形成有效的缓解程序。事件故障单应向谁上报？

选择一项：

* SME，以便进行进一步调查
* 网络运营分析师，以寻求帮助
* 警报分析师，以便进行进一步分析
* SOC 经理，以要求指派其他人员

反馈

Refer to curriculum topic: 1.2.1

事件响应人员是 SOC 中的二级安全专业人员。如果响应人员无法解决事件故障单，则应将事件故障单上报给下一级支持人员，即三级人员。3 级 SME 将进一步调查事件。

正确答案是：SME，以便进行进一步调查

## 第 1 章考试

在 SOC 运营中，哪一系统常用于让分析人员从警报池中选择警报进行调查？

* 系统日志服务器
* 注册系统
* 基于安全警报知识的系统
* 故障单系统

验证监控软件所触发的警报是否代表真正安全事件这一任务分配给 SOC 中的哪些人员？

* 三级人员
* 二级人员
* SOC 经理
* 一级人员

SOC 中的安全信息和事件管理系统 (SIEM) 如何帮助人员抵御安全威胁？

* 通过结合来自多种技术的数据
* 通过实时分析日志记录数据
* 通过动态实现防火墙规则
* 通过将所有安全设备和家电集成到组织中

在 SOC 安全信息和事件管理系统中应包含哪三项技术？（选择三项。）

* 代理服务
* 防火墙设备
* 威胁情报
* 入侵防御
* 安全监控
* 日志管理

业余黑客称为什么？

* 脚本小子
* 蓝队
* 红帽黑客
* 黑帽黑客

以下哪种说法正确描述了网络战？

* 它是为空军飞行员提供的模拟软件，让飞行员能够在模拟的战争场景中进行练习。
* 它是为被卷入核战争的士兵开发的一系列个人防护设备。
* 网络战是由一伙“脚本小子”执行的攻击。
* 它是互联网上的对抗，涉及向其他国家/地区的信息系统渗透的活动。

IoT 设备为什么会造成比网络上的其他计算设备更大的风险？

* 大多数 IoT 设备不需要互联网连接，并且无法接收新的更新。
* 大多数 IoT 设备不接收频繁的固件更新。
* IoT 设备需要使用未加密的无线连接。
* IoT 设备不能在只有互联网连接的隔离网络上运行。

哪一组织提供厂商中立的 CSA+ 认证？

* GIAC
* CompTIA
* (ISC)²
* IEEE

如果 SOC 具有 99.999% 的运行时间目标，则在目标范围内每年应有多少分钟的停机时间？

* 每年不超过 10 分钟。
* 每年不超过 1 分钟。
* 每年不超过 30 分钟。
* 每年不超过 5 分钟。

哪一项可以作为网络战武器攻击伊朗的铀浓缩设施?

* SQL 注入
* Stuxnet
* PSYOPS
* DDoS

以下哪项陈述最准确地描述了激进黑客的动机？

* 他们属于政治原因导致的抗议群体。
* 他们很好奇并学习黑客技能。
* 他们对发现新的攻击漏洞很感兴趣。
* 他们试图炫耀自己的黑客技能。

安全运营中心提供哪两项服务？（选择两项。）

* 响应数据中心的入侵
* 确保安全路由数据包交换
* 监控网络安全威胁
* 提供安全互联网连接
* 管理全面威胁解决方案

搜寻潜在威胁和实施威胁检测工具的这一任务分配给 SOC 中的哪些人员？

* 一级分析师
* 三级 SME
* SOC 经理
* 二级事件响应人员

用户报告无法访问主服务器上的数据库文件。数据库管理员验证了该问题，并注意到该数据库文件现在已加密。组织收到一封威胁邮件，要求其支付一定的费用以解密该数据库文件。该组织遭受的是什么类型的攻击？

* 特洛伊木马
* 中间人攻击
* DoS 攻击
* 勒索软件

在公共场所使用免费和开放的无线热点有什么潜在风险？

* 可能需要向供应商购买产品以换取互联网接入。
* 尝试连接至互联网的用户过多可能会导致网络拥塞。
* 许多用户访问无线热点时，互联网连接可能变得太慢。
* 网络流量可能遭劫持，且信息被盗。

## 第2章测验

用户如何才能阻止特定应用程序通过网络访问 Windows 计算机？

选择一项：

* 启用 MAC 地址过滤。
* 禁用自动 IP 地址分配。
* 在 Windows 防火墙中阻止特定的 TCP 或 UDP 端口。
* 更改默认的用户名和密码。

反馈

Refer to curriculum topic: 2.2.2

网络应用程序具有可以在 Windows 防火墙中打开或阻止的特定 TCP 或 UDP 端口。禁用自动 IP 地址分配可能会导致计算机根本无法连接到网络。启用 MAC 地址过滤在 Windows 中不可能实现，并且该操作仅阻止特定的网络主机而不阻止应用程序。更改默认的用户名和密码可以保护计算机不被未经授权的用户访问，但不能阻止应用程序访问。

正确答案是：在 Windows 防火墙中阻止特定的 TCP 或 UDP 端口。

什么包含有关如何组织硬盘驱动器分区的信息？

选择一项：

* MBR
* CPU
* BOOTMGR
* Windows 注册表

反馈

Refer to curriculum topic: 2.1.2

正确答案是：MBR

哪个实用程序用于显示每个用户消耗的系统资源？

选择一项：

* 任务管理器
* 用户帐户
* 设备管理器
* 事件查看器

反馈

Refer to curriculum topic: 2.2.1

Windows 任务管理器实用程序包括一个“用户”选项卡，该选项可显示每个用户消耗的系统资源。

正确答案是：任务管理器

本地网络上的一台主机发出两个 ping 命令。第一个 ping 命令针对主机的默认网关 IP 地址，命令失败。第二个 ping 命令针对本地网络外主机的 IP 地址，命令成功。第一个 ping 命令失败的原因可能是什么？

选择一项：

* 默认网关设备配置了错误的 IP 地址。
* 默认网关设备应用了安全规则，阻止其处理 ping 请求。
* 默认网关运行不正常。
* 默认网关上的 TCP/IP 协议栈运行不正常。

反馈

Refer to curriculum topic: 2.2.1

如果从一台主机向远程网络上的另一台主机执行 ping 操作成功，说明默认网关运行正常。在这种情况下，如果从一台主机向默认网关执行 ping 操作失败，则路由器接口可能应用了某些安全功能，阻止其响应 ping 请求。

正确答案是：默认网关设备应用了安全规则，阻止其处理 ping 请求。

32 位版本 Windows 可寻址多少 RAM？

选择一项：

* 4 GB
* 8 GB
* 16 GB
* 32 GB

反馈

Refer to curriculum topic: 2.1.1

32 位操作系统能够支持约 4 GB 的内存。这是因为 2^32 约为 4 GB。

正确答案是：4 GB

cd\ 命令有什么用途？

选择一项：

* 将目录更改为根目录
* 将目录更改为下一个最高目录
* 将目录更改为前一个目录
* 将目录更改为下一个下层目录

反馈

Refer to curriculum topic: 2.1.1

在 Windows 操作系统的“命令提示符”窗口中键入 CLI 命令。cd\ 命令用于将目录更改为 Windows 根目录。

正确答案是：将目录更改为根目录

用户在 Windows 中创建扩展名为 .ps1 的文件。它是哪种类型的文件？

选择一项：

* PowerShell 脚本
* PowerShell cmdlet
* PowerShell 函数
* PowerShell 文档

反馈

Refer to curriculum topic: 2.2.1

PowerShell 可执行的命令包括以下几类：

cmdlets - 执行操作并将输出或对象返回将要执行的下一个命令

PowerShell 脚本 - 包含待执行 PowerShell 命令、扩展名为 .ps1 的文件

PowerShell 函数 - 可在脚本中引用的代码

正确答案是：PowerShell 脚本

当用户对 Windows 系统的设置进行更改时，这些更改存储在何处？

选择一项：

* 注册表
* 控制面板
* win.ini
* boot.ini

反馈

Refer to curriculum topic: 2.1.2

注册表包含有关应用程序、用户、硬件、网络设置和文件类型的信息。注册表还包含每个用户的特有部分，其中包含该特定用户配置的设置。

正确答案是：注册表

在 Windows PC 上使用哪种 net 命令建立远程服务器上的共享目录连接？

选择一项：

* net use
* net start
* net share
* net session

反馈

Refer to curriculum topic: 2.2.1

net 命令是 Windows 中非常重要的命令。一些常见的 net 命令包括下列各项：

net accounts - 为用户设置密码和登录要求

net session - 列出或断开网络上的一台计算机和其他计算机之间的会话

net share - 创建、删除或管理共享资源

net start - 启动网络服务或列出运行中的网络服务

net stop - 停止网络服务

net use - 连接和断开共享网络资源以及显示相关信息

net view - 显示网络上的计算机和网络设备列表

正确答案是：net use

对于每次计算机启动时都应运行的服务，必须选择哪种启动类型？

选择一项：

* 自动
* 引导
* 手动
* 开始
* 启动

反馈

Refer to curriculum topic: 2.1.2

自动启动允许在 PC 启动时自动启动服务。用户启动应用时，进行的是手动启动过程。引导、开始或启动服务类型不可配置。

正确答案是：自动

哪个命令可用于手动查询 DNS 服务器来解析特定主机名？

选择一项：

* nslookup
* ipconfig /displaydns
* tracert
* net

反馈

Refer to curriculum topic: 2.2.1

nslookup 命令允许用户手动查询 DNS 服务器来解析给定的主机名。ipconfig/displaydns 命令只是显示之前已解析的 DNS 条目。tracert 命令可以检查数据包通过网络时所用的路径，并能通过自动查询 DNS 服务器来解析主机名。net 命令用于管理网络计算机、服务器、打印机和网络驱动器。

正确答案是：nslookup

哪个 Windows 版本首先引入 64 位 Windows 操作系统？

选择一项：

* Windows NT
* Windows XP
* Windows 7
* Windows 10

反馈

Refer to curriculum topic: 2.1.1

有 20 多个 Windows 操作系统版本。Windows XP 将 64 位处理功能引入了 Windows 计算。

正确答案是：Windows XP

正确还是错误？

为便于管理，建议 Windows 中的 “Everyone” 组拥有完全控制权限。

选择一项：

* 正确
* 错误

反馈

Refer to curriculum topic: 2.1.1

正确答案是：错误

## 第2章考试

在 Windows 中使用 net accounts 命令的目的是什么？

* 显示网络上的计算机和网络设备列表
* 查看用户的密码和登录要求设置
* 显示有关共享网络资源的信息
* 启动网络服务

下列哪种技术旨在替代现代个人计算机主板上的 BIOS 程序？

* CMOS
* MBR
* RAM
* UEFI

在 Windows PC 上输入 ipconfig 命令的两个原因是什么？（选择两项。）

* 查看网络介质连接的状态
* 显示网络连接的带宽和吞吐量
* 确保 PC 可以连接至远程网络
* 检查是否可以联系 DNS 服务器
* 查看 PC 上的网络配置

在 Windows PC 上输入 netsh 命令的目的是什么？

* 测试 PC 上的硬件设备
* 更改 PC 计算机名称
* 配置 PC 联网参数
* 创建用户帐户

在 Windows PC 上输入 ping 127.0.0.1 命令的两个原因是什么？（选择两项。）

* 检查 TCP/IP 协议簇是否安装正确
* 检查 NIC 是否按预期运行
* 确保 PC 可以连接至远程网络
* 显示网络连接的带宽和吞吐量
* 检查默认网关是否配置正确

Windows PC 上的哪些实用程序可用于查看当前正在运行的应用和进程？

* nslookup
* ipconfig
* 任务管理器
* 控制面板

哪两个命令可用于检查 DNS 域名解析在 Windows PC 上是否正常工作？（请选择两项。）

* ipconfig/flushdns
* ping cisco.com
* nslookup cisco.com
* nbtstat cisco.com
* net cisco.com

请考虑 Windows CLI C:\Users\Jason\Desktop\mydocu.txt 中的路径表示。Users\Jason 组件表示什么？

* 文件目录和子目录
* 存储设备或分区
* 当前文件目录
* 文件属性

出于安全考虑，网络管理员需要确保本地计算机无法彼此 ping 通。可使用哪项设置完成此任务？

* 智能卡设置
* MAC 地址设置
* 防火墙设置
* 文件系统设置

哪种类型的 Windows PowerShell 命令执行操作并将输出或对象返回至将要执行的下一条命令？

* routines
* scripts
* functions
* cmdlet

下列哪两项可以使用 ping 命令来确定？ （选择两项。）

* 源设备与目的设备之间的路由器数量
* 源设备与目的设备之间的路径中每台路由器响应的平均时间
* 是否可以通过网络到达目的设备
* 距目的设备最近的路由器的 IP 地址
* 数据包到达目的设备以及响应返回源设备的平均时间

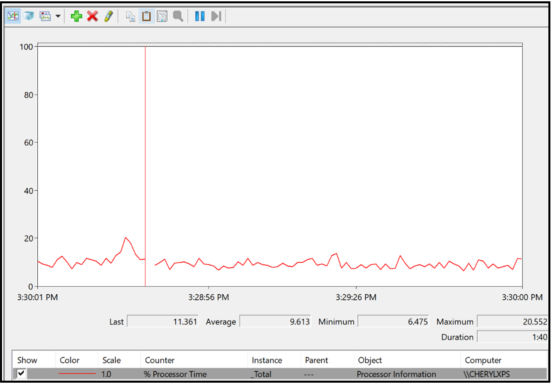
技术人员正在对无法连接到网络的 PC 进行故障排除。应该发出以下哪项命令来检查设备的 IP 地址？

* ipconfig
* ping
* tracert
* nslookup

安装过程中所选择的设置存储在什么地方？

* 在注册表中
* 在 BIOS 中
* 在闪存中
* 在恢复分区

请参见图示。正在使用下列哪一 Microsoft Windows 应用？



* 任务管理器
* 性能监控器
* 事件查看器
* PowerShell

请参见图示。网络安全管理员正尝试从 Windows PowerShell 查看系统信息，并接收显示的错误消息。要成功运行命令，管理员需采取下列哪项措施？

* 从命令提示符运行命令。
* 以管理员身份运行 PowerShell。
* 安装最新 Windows 更新。
* 在任务管理器中重新启动 abno 服务。

用户使用常规用户帐户登录 Windows，并尝试使用需管理权限的应用。用户可以做些什么来成功地使用应用？

* 右键点击应用，然后选择 以 root 身份运行 。
* 右键点击应用，然后选择 以特权身份运行 。
* 右键点击应用，然后选择 以超级用户身份运行 。
* 右键点击应用，然后选择 以管理员身份运行 。

NTFS 文件系统较之 FAT32 有哪两项优点？（选择两项。）

* NTFS 更易于配置。
* NTFS 能够更快地格式化驱动器。
* NTFS 支持自动检测坏扇区。
* NTFS 支持的文件更大。
* NTFS 提供的安全功能更多。
* NTFS 能够更快地访问 USB 驱动器之类的外围设备。

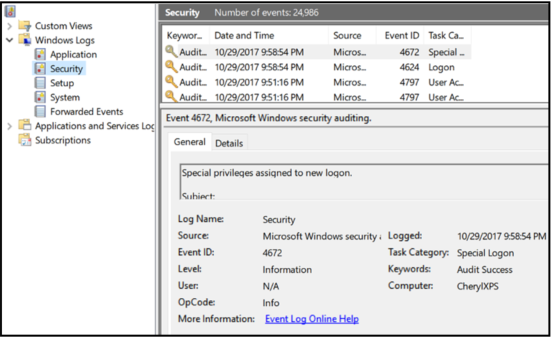
下列哪个术语用于描述可以进行格式化，以存储数据的逻辑驱动器？

* 簇
* 扇区
* 分区
* 卷
* 磁道

如果在 Windows PC 上输入 netstat -abno 命令，会显示什么内容？

* 仅限处于“侦听”状态的活动 UDP 连接
* 所有活动的 TCP 和 UDP 连接、其当前状态及其相关联进程 ID (PID)
* 仅限处于“已建立”状态的活动 TCP 连接
* 本地路由表

请参见图示。网络安全分析师正在调查 Microsoft Windows 计算机上报告的安全事件。分析师使用下列哪项工具？



* 事件查看器
* 性能监控器
* PowerShell
* 任务管理器

技术人员可以对某远程公司 Web 服务器的 IP 地址执行 ping 操作，但无法对同一 Web 服务器的 URL 地址成功执行 ping 操作。 技术人员可以使用哪种软件实用程序来诊断此问题？

* nslookup
* netstat
* ipconfig
* tracert

用户将 Windows 安装到新计算机时，会自动创建哪两个用户帐户？（选择两项。）

* 管理员
* 系统
* root
* 访客
* 超级用户

Windows 任务管理器提供下列哪项功能？

* 有选择地拒绝指定接口上的流量。
* 提供有关系统资源和进程的信息。
* 维护系统日志。
* 提供活动的 TCP 连接列表。