姓名: _____ 日期: _____ 得分: _____

网络安全基础与在线威胁预防

网络安全威胁、网络防火墙、多因素认证、安全框架

网络安全基础学习概览

受保护
数据加密
256 位 AES 标准

合规的
全球标准
GDPR 与 CCPA 框架

零信任
访问策略
多重身份验证

欢迎！ 本活动手册将带你了解网络安全基础与在线威胁防范的基本原则。你将探索恶意软件威胁、多因素身份验证、网络防火墙和事件响应框架。

练习单检查点

- [ ] **第 1-4 部分: 掌握网络安全和威胁防范。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com 网络安全指南

URL: https://www.vpn.com/cybersecurity/

你的网络安全基础学习路线图

- 识别恶意软件、网络钓鱼和企业网络入侵的常见途径。
- 实施标准的网络安全控制措施，包括 MFA、防火墙和终端防御。
- 评估用于减轻数据泄露影响的事件响应流程。
- 分析 NIST 指南下的组织风险因素和安全协调性。
- 配置安全卫生实践，以缓解自动化凭据填充攻击。

网络安全指南说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于威胁防范。 最后完成附加活动: 快速思考。

网络安全基础与威胁防范（引言）

网络安全保护网络、系统和数据免受未经授权的数字攻击。养成稳健的安全习惯、配置防火墙、要求使用多因素认证，以及培训员工识别威胁，是企业网络防御的重要组成部分。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 网络钓鱼攻击的首要目标是什么?

- A. 窃取凭据和敏感用户数据
- B. 提升网站在搜索引擎中的可见度
- C. 增加网络带宽容量
- D. 管理备份数据中心复制

2. 哪种机制提供最强的账户保护?

- A. 使用硬件密钥的多重身份验证
- B. 每三十天更新一次的复杂密码
- C. 限制账户仅在营业时间内登录
- D. 对公共目录隐藏账户用户名

3. 什么定义了勒索软件感染载荷?

- A. 加密系统文件并索要付款
- B. 悄悄将击键记录发送到远程服务器
- C. 向浏览器注入未经授权的广告
- D. 使用本地 CPU 资源挖掘加密货币

4. 零日漏洞利用如何影响安全防御?

- A. 它针对未修补的未知漏洞
- B. 它会自动禁用企业防火墙
- C. 它迫使系统执行强制重启
- D. 它无需任何预算即可修复

5. 哪个框架规范企业安全控制?

- A. NIST 网络安全框架指南
- B. W3C HTML5 文档架构规范
- C. 打印机驱动安装手册
- D. IETF 路由协议定义

检查点 2: 判断正误挑战

6 问题 (判断) 6

6. 网络钓鱼攻击只针对个人电子邮件账户。

○ 正确 ○ 错误

7 问题 (判断) 7

7. 多因素认证有助于阻止撞库攻击。

○ 正确 ○ 错误

8 问题 (判断) 8

8. 防火墙会检查网络流量，以阻止未经授权的端口访问。

○ 正确 ○ 错误

9 问题 (判断) 9

9. 修复零日漏洞利用需要标准的杀毒软件病毒库更新。

○ 正确 ○ 错误

10 问题 (判断) 10

10. 蜜罐是用来引诱网络犯罪分子的诱饵服务器。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 网络管理员安装 _____ 来过滤传入流量。
2. 攻击者利用零日 _____ 绕过系统补丁。
3. 攻击者发送伪造邮件，对员工发起 _____ 活动。
4. 勒索软件是锁定用户数据的一种破坏性 _____ 。
5. 建立良好的密码 _____ 可降低凭据被盗的风险。
6. 为保护敏感通信，用户应用 _____ 协议。

词汇词库

安全框架 | 多因素认证 | 恶意软件 | 防火墙 | 加密 | 漏洞 | 网络钓鱼 | 卫生

在此写下你的答案:

1.
2.
3.
4.
5.
6.

检查点 4: 安全概念配对

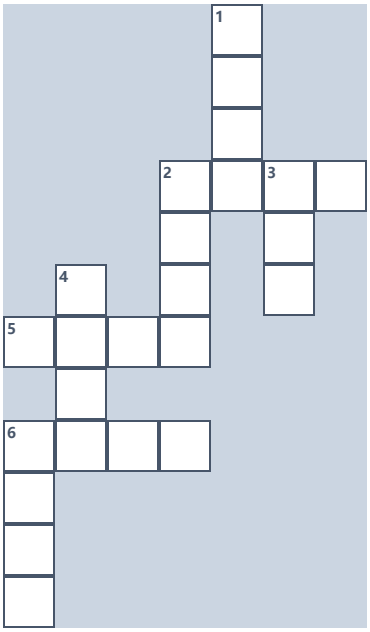
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

1. 勒索软件威胁		A	NIST 等用于管理网络风险的结构化指南。
2. 多因素认证		B	处理和缓解安全事件的结构化计划。
3. 零日漏洞利用		C	根据安全规则过滤流量的网络屏障。
4. 诱饵蜜罐		D	加密数据并要求支付赎金以解密的恶意软件。
5. 入侵防火墙		E	在厂商发布补丁之前被利用的漏洞攻击。
6. 事件响应		F	管理凭据和身份验证密钥的最佳实践。
7. 密码卫生		G	需要两个或更多身份验证因素的安全验证。
8. 安全框架		H	用于引诱并分析恶意行为者的诱饵系统。

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

2. 抵御攻击、保护系统的措施 (4)

5. 威胁防护要扫描和拦截的危险程序 (4)

6. 安全地创建、保存和更换密码的做法 (4)

纵向

1. 保护网络和系统免受攻击的措施 (4)

2. 对系统造成威胁或损害的突发情况 (4)

3. 根据安全规则过滤流量的网络屏障 (3)

4. 被编写来破坏或窃取数据的程序代码 (4)

6. 管理凭据和认证密钥的最佳实践 (4)

检查点 5 替代活动: 无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

2 横向: 抵御攻击、保护系统的措施 (4 字):

5 横向: 威胁防护要扫描和拦截的危险程序 (4 字):

6 横向: 安全地创建、保存和更换密码的做法 (4 字):

纵向

1 纵向: 保护网络和系统免受攻击的措施 (4 字):

2 纵向: 对系统造成威胁或损害的突发情况 (4 字):

3 纵向: 根据安全规则过滤流量的网络屏障 (3 字):

4 纵向: 被编写来破坏或窃取数据的程序代码 (4 字):

6 纵向: 管理凭据和认证密钥的最佳实践 (4 字):

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

全 问 公 安 信 浏 器 隐 览 传 恶 管 务 防 攻
风 名 保 击 防 全 输 服 密 安 设 域 险 隐 生
服 码 务 安 证 隐 接 理 认 码 户 身 用 击 址
服 代 数 备 卫 络 保 地 共 访 卫 接 卫 份 备
道 意 安 统 址 安 务 址 录 墙 代 生 击 事 息
击 恶 防 密 设 全 接 网 息 证 软 火 击 录 系
份 加 公 管 理 防 器 协 络 问 数 网 全 加 险
事 协 址 恶 名 护 录 输 域 安 服 统 墙 地 服
理 接 证 认 名 系 攻 护 墙 墙 全 统 件 备 输
管 传 保 据 管 系 份 连 设 数 道 服 管 代 人
码 安 全 事 件 加 卫 浏 信 域 隐 生 码 认 防
密 服 软 记 恶 攻 据 公 全 网 生 身 服 火 名
络 务 份 务 意 户 隐 接 码 件 统 火 墙 器 接
设 卫 管 户 软 软 隧 用 络 络 软 险 认 攻 输
事 系 址 设 件 输 备 密 认 意 数 信 设 记 览

词汇列表

防火墙 **安全防护** **安全事件** **恶意软件** **网络安全** **恶意代码** **密码管理** **密码卫生**

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 防火墙
B. 安全防护
C. 安全事件
D. 恶意软件
E. 网络安全
F. 恶意代码
G. 密码管理
H. 密码卫生

定义与配对字段
1. 保护网络和系统免受攻击的措施。
2. 被编写来破坏或窃取数据的程序代码。
3. 根据安全规则过滤流量的网络屏障。
4. 抵御攻击、保护系统的措施。
5. 安全地创建、保存和更换密码的做法。
6. 管理凭据和认证密钥的最佳实践。
7. 对系统造成威胁或损害的突发情况。
8. 威胁防护要扫描和拦截的危险程序。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的网络安全概念和术语。把答案写在提供的输入框中。

1. 火墙防 _____

2. 安事件全 _____

3. 全网安络 _____

4. 理管密码 _____

5. 护安防全 _____

6. 软件恶意 _____

7. 代恶码意 _____

8. 密生卫码 _____

附加活动: 快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	网络安全领域的职业			
2	更新软件的原因			
3	防火墙可以拦截的内容			
4	电子邮件中的警示信号			
5	你要备份的内容			
6	著名的网络攻击类型			
7	蜜罐可以诱捕的对象			
8	你绝不应分享的信息			
9	电脑被感染的迹象			
10	关于黑客的电影或节目			
11	你可以构建的安全层级			
12	安全演练中要练习的内容			
13	你知道的安全工具			
14	可以向其寻求 IT 帮助的人			
15	以“cyber”开头的词语			

检查点 8: 网络安全案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 勒索软件恢复策略



情景: 一家公司网络感染了勒索软件，关键数据库被锁定。攻击者索要 100,000 美元的加密货币赎金。该公司有 24 小时前的离线备份。

讨论问题: 分析支付赎金的风险，并评估恢复策略。

案例研究 2: 防御凭据填充攻击



情景: 某在线服务遭遇撞库攻击，黑客在测试从其他网站窃取的数百万个用户名/密码组合。

讨论问题: 详细说明这种攻击的机制，并概述两种防御系统。

检查点 9: 破解密码

网络安全专业人员保护网络资产免受网络威胁行为者的攻击。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

重=1 护=2 软=3 生=4 理=5 统=6 络=7 密=8 的=9 安=10
验=11 事=12 代=13 恶=14 码=15 件=16 意=17 防=18 管=19 卫=20
保=21 你=22 火=23 系=24 墙=25 多=26 证=27 网=28 数=29 全=30

26	1	11	27	21	2	22	9	24	6

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

检查点 10: 基础网络安全常见问题 (A 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q1: 网络安全的主要目标是什么?

主要目标是保护网络、设备和数据免受未经授权的访问、攻击和意外损坏。

Q2: 网络钓鱼与鱼叉式网络钓鱼有何不同?

网络钓鱼是针对随机用户的大范围电子邮件攻击，而鱼叉式网络钓鱼则利用个性化数据针对特定个人。

Q3: 什么是网络防火墙?

防火墙是一种网络安全系统，根据预先定义的安全规则监控和过滤传入与传出的流量。

Q4: 为什么必须使用多因素身份验证 (MFA)?

MFA 增加了关键的一层防御，即使攻击者窃取或破解了主密码凭据，也能阻止其访问。

Q5: 计算机病毒的定义是什么?

病毒是自我复制的恶意软件，会附着在干净文件上，并在执行后在系统间传播。

检查点 10: 基础网络安全常见问题 (B 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q6: 勒索软件如何锁定本地数据?

勒索软件使用加密算法对用户文件进行加密，使其在应用解密密钥之前无法读取。

Q7: 什么是零日漏洞?

零日漏洞是软件中供应商未知的安全缺陷，在被利用之前没有留出开发补丁的时间。

Q8: NIST 框架起什么作用?

NIST 框架提供自愿性的指南和标准，帮助组织管理并降低网络安全风险。

Q9: 什么是安全事件响应计划?

它是一套文档化的流程，用于检测、遏制安全漏洞和网络入侵并从中恢复。

Q10: 社会工程如何利用用户?

社会工程学利用心理操纵，诱骗员工泄露密码或下载恶意文件。

检查点 10: 高级安全常见问题 (C 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q1: DDoS 攻击如何使 Web 服务器不堪重负?

DDoS 攻击会协调数百万台被入侵的僵尸网络设备，用流量淹没服务器，耗尽带宽和 CPU 资源。

Q2: 对称加密和非对称加密有什么区别?

对称加密使用单个密钥进行加密和解密，而非对称加密使用公钥和私钥对。

Q3: 黑客如何实施 SQL 注入攻击?

攻击者在表单字段中输入恶意 SQL 命令，诱使后端数据库泄露未经授权的用户记录。

Q4: 网络入侵中的横向移动是什么?

这是一种技术，攻击者利用最初获得的服务器访问权限，入侵内部网络上其他相互连接的系统。

Q5: DNS 欺骗如何重定向网络流量?

DNS 欺骗会篡改名称服务器的缓存记录，使合法用户被导向恶意的仿冒网站，而不是目标域名。

检查点 10: 高级安全常见问题 (D 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q6: 什么是硬件安全令牌?

它是一种生成加密身份验证证明的物理设备（如 YubiKey），能最大程度防御远程网络钓鱼。

Q7: 安全团队如何使用诱饵蜜罐?

团队部署非生产环境的诱饵服务器，以便及早发现入侵并分析未经授权者的攻击模式。

Q8: 最小权限原则是什么?

这是将用户访问权限限制在完成其工作角色所需的绝对最低限度的安全标准。

Q9: 中间人攻击如何利用连接?

攻击者在未加密网络上拦截并篡改两台设备之间的通信，窃取会话令牌和凭据。

Q10: 什么是入侵指标（IOC）?

IOC 是显示系统已被入侵的取证数据线索，例如异常的注册表修改或恶意 IP 流量。

第 11 部分: 10 个现实中的网络安全事实与洞察

回顾有关安全漏洞、防御机制和合规标准的真实事实。

1. 安全洞察

攻击者不断扫描互联网上存在漏洞的服务器，并向员工收件箱发送网络钓鱼邮件。

2. 安全洞察

点击网络钓鱼链接等人为失误是数据泄露的常见因素，这就是培训很重要的原因。

3. 安全洞察

数据泄露的成本包括法律罚款、客户流失、调查和修复，可能高达数百万美元。

4. 安全洞察

抗网络钓鱼的 MFA（如硬件安全密钥）是最强的 MFA 类型，也是 CISA 所敦促采用的标准。 [2]

5. 安全洞察

勒索软件仍然是企业网络的主要威胁，CISA 敦促将离线加密备份作为关键防御手段。 [4]

6. 安全洞察

NIST 网络安全框架 2.0（2024）包含六项核心功能: 治理、识别、保护、检测、响应、恢复。 [1]

7. 安全洞察

凭据填充机器人会大规模地用泄露的用户名和密码组合测试银行和电商登录门户。

8. 安全洞察

全球存在零日漏洞利用市场，高危漏洞在被修补之前可能以高价出售。

9. 安全洞察

蜜罐诱饵系统会立即报告入侵警报，因为合法用户没有理由访问它。

10. 安全洞察

传输层安全（TLS）加密浏览器会话，防止在公共 Wi-Fi 网络上被嗅探数据包。

技术参考资料与来源

本学习指南和互动谜题根据全球 NIST、OWASP 以及数据隐私合规标准编写。

学术与行业参考资料

[1] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

答案: 检查点 1 – 单项选择

1 **网络钓鱼攻击** 网络钓鱼 正确答案: A

教学提示

网络钓鱼活动试图利用仿冒电子邮件窃取凭据和敏感用户数据。 引用: OWASP Secure Configuration。

2 **账户保护** MFA 密钥 正确答案: A

教学提示

使用硬件令牌的多重身份验证（MFA）可提供最强的账户访问防御。引用: NIST Digital Identity。

3 **勒索软件威胁** 勒索软件 正确答案: A

教学提示

勒索软件会加密关键系统和数据，并要求以加密货币支付解密密钥的费用。引用: Center for Internet Security (CIS)。

4 **零日漏洞** 零日漏洞 正确答案: A

教学提示

零日威胁在厂商补丁发布之前，利用未修补的、未知的安全缺陷。引用来源: OWASP Secure Configuration。

5 **安全框架** 框架 正确答案: A

教学提示

NIST 等框架提供结构化的指南，帮助组织管理并降低网络风险。引用来源: NIST Digital Identity。

答案: 检查点 2 – 判断题（正确或错误）

6 **定向钓鱼** 网络钓鱼 正确答案: 错误

教学提示

网络钓鱼攻击既针对企业网络也针对个人账户，以扩大攻击途径。 引用: OWASP Secure Configuration。

7 **问题 7** 正确答案: 正确

教学提示

MFA 需要第二重验证因素，因此仅凭被盗的密码通常不足以登录。

8 **流量防火墙** 防火墙 正确答案: 正确

教学提示

防火墙会检查并阻止特定网络端口上的流量，以过滤未经授权的连接。引用来源: Center for Internet Security (CIS)。

9 **零日漏洞响应** 零日漏洞 正确答案: 错误

教学提示

修复零日漏洞需要代码补丁和 WAF 过滤，因为尚不存在特征码。引用: OWASP Secure Configuration。

10 **诱饵蜜罐** 蜜罐 正确答案: 正确

教学提示

蜜罐是安全团队用来诱捕、告警和研究恶意行为者的诱饵服务器。引用来源: Center for Internet Security (CIS)。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

D 1. 勒索软件威胁	G 2. 多因素认证	E 3. 零日漏洞利用	H 4. 诱饵蜜罐
C 5. 入侵防火墙	B 6. 事件响应	F 7. 密码卫生	A 8. 安全框架

检查点 3: 答案 – 关键术语

1 防火墙	2 漏洞	3 网络钓鱼	4 恶意软件
5 卫生	6 加密		

检查点 6 替代活动: 答案 – 词语配对

1 E – 网络安全	2 F – 恶意代码	3 A – 防火墙	4 B – 安全防护
5 G – 密码管理	6 H – 密码卫生	7 C – 安全事件	8 D – 恶意软件

教师讨论提示

关键术语:
检查学生能否用自己的话解释勒索软件威胁、多因素认证和零日漏洞利用，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

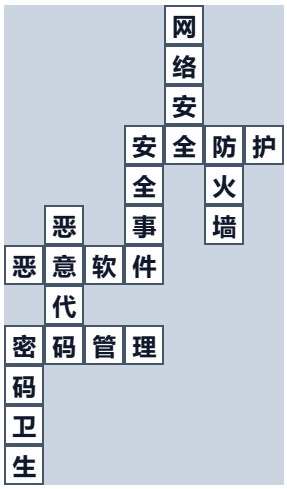
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	问	公	安	信	浏	器	隐	览	传	恶	管	务	防	攻
风	名	保	击	防	全	输	服	密	安	设	域	险	隐	生
服	码	务	安	证	隐	接	理	认	码	户	身	用	击	址
服	代	数	备	卫	络	保	地	共	访	卫	接	卫	份	备
道	意	安	统	址	安	务	址	录	墙	代	生	击	事	息
击	恶	防	密	设	全	接	网	息	证	软	火	击	录	系
份	加	公	管	理	防	器	协	络	问	数	网	全	加	险
事	协	址	恶	名	护	录	输	域	安	服	统	墙	地	服
理	接	证	认	名	系	攻	护	墙	墙	全	统	件	备	输
管	传	保	据	管	系	份	连	设	数	道	服	管	代	人
码	安	全	事	件	加	卫	浏	信	域	隐	生	码	认	防
密	服	软	记	恶	攻	据	公	全	网	生	身	服	火	名
络	务	份	务	意	户	隐	接	码	件	统	火	墙	器	接
设	卫	管	户	软	软	隧	用	络	络	软	险	认	攻	输
事	系	址	设	件	输	备	密	认	意	数	信	设	记	览

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 安全防护 抵御攻击、保护系统的措施 (4 字)

5 横向: 恶意软件 威胁防护要扫描和拦截的危险程序 (4 字)

6 横向: 密码管理 安全地创建、保存和更换密码的做法 (4 字)

纵向

1 纵向: 网络安全 保护网络和系统免受攻击的措施 (4 字)

2 纵向: 安全事件 对系统造成威胁或损害的突发情况 (4 字)

3 纵向: 防火墙 根据安全规则过滤流量的网络屏障 (3 字)

4 纵向: 恶意代码 被编写来破坏或窃取数据的程序代码 (4 字)

6 纵向: 密码卫生 管理凭据和认证密钥的最佳实践 (4 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 火墙防	防火墙	5. 护安防全	安全防护
2. 安事件全	安全事件	6. 软件恶意	恶意软件
3. 全网安络	网络安全	7. 代恶码意	恶意代码
4. 理管密码	密码管理	8. 密生卫码	密码卫生

秘密密码挑战答案

“多重验证保护你的系统”

案例研究答案

A 案例研究 1: 勒索软件恢复策略

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一个企业网络感染了勒索软件，关键数据库被锁定。攻击者索要 100,000 美元的加密货币赎金。该公司有 24 小时前的离线备份。
- 推荐策略与解决方案: 付款的风险: 付款并不能保证文件被解密，会让公司被标记为愿意付钱的目标，还会资助犯罪活动。恢复策略: 团队应隔离受感染的主机，清除被入侵的服务器，并从离线备份中恢复数据。他们必须修补最初的入侵途径（网络钓鱼或漏洞利用），以防止立即再次感染。

B 案例研究 2: 防御凭据填充攻击

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一项在线服务遭遇撞库攻击，黑客在测试从其他网站窃取的数百万组用户名/密码组合。
- 推荐策略与解决方案: 机制: 攻击者利用用户在多个网站重复使用密码的习惯，借助自动化机器人登录用户账户。防御措施: 1. 多因素身份验证（MFA）即使在密码正确时也能阻止登录尝试。2. 实施速率限制和验证码（CAPTCHA）可阻止自动化机器人流量向登录端点发送大量请求。