解决方案手册

SOPHOS

Sophos 咨询服务

Wireless Network Penetration Testing
无线网络渗透测试

识别您的无线网络中的暴露点及攻击者可能加以利用的方式

无线网络让员工和访客在物理地点内自由移动的同时保持连接，但无线技术也为组织带来了新的安全风险。配置错误的基础设施、恶意接入点和无线客户端都可能引发难以预计的安全隐患。无线网络渗透测试主动评估您组织的 Wi-Fi 基础设施，并识别攻击敌手可能如何利用漏洞来入侵您的网络。

提升无线网络的安全状态

MAC 地址过滤、WEP 加密和预共享密钥等防护手段已不再有效保护使用您的无线网络的信息与客户端。攻击者往往能在几分钟内绕过或破解这些防护措施，从而暴露内部网络基础设施。

主动测试以识别接入您网络的设备，并评估 Wi-Fi 基础设施的安全性，从而在曝露点遭到利用之前预判攻击者可能的入侵路径。

Sophos 无线网络渗透测试服务

Sophos Wireless Network Penetration Testing 无线网络渗透测试服务通过配置检视、技术测试及恶意接入点扫描，评估无线网络的安全性和合规性。Sophos 的高技术安全测试人员将尝试利用加密、身份验证及访问控制中的弱点，采用“被动”与“主动”两种方式进行评估：

- **被动评估：**通过监控无线流量，来识别未授权设备、恶意接入点与配置错误，过程中不会主动尝试连线。
- **主动评估：**模拟攻击者通过破解加密、绕过身份验证并获取未授权访问权限的过程，来试图利用无线网络中的漏洞

优势

- 确保通过无线网络传输的敏感数据防范未授权访问或拦截。
- 清晰了解您的无线连接如何暴露内部网络。
- 识别攻击者可能入侵无线网络的路径。
- 实现只有授权用户才能安全访问网络。
- 获得可执行的修补建议。
- 测试不仅止于合规性评估。

为什么要测试您的无线网络?

透过定期进行主动测试，您可以降低攻击者入侵的风险。他们持续改良他们的攻击手法，并利用新出现的漏洞存取在您的无线网络传输的敏感数据。定期测试还可帮助发现由于组织 Wi-Fi 基础设施变更所产生的新弱点，并提供对实际风险暴露情况的清晰理解。

- 识别恶意无线接入点和配置错误。
- 确保无线安全政策符合最佳实践。
- 降低因 Wi-Fi 漏洞导致的数据泄露风险。
- 评估被动暴露与主动利用攻击的风险。
- 了解您的设备如何应对恶意接入点。

报告内容包含

管理摘要：总结评估概况、关键发现和高层级建议。

测试方法：明确测试范围及所执行的测试活动。

过程叙述：描述测试人员为达成评估目标所采取的具体操作流程。

发现与建议：按风险严重等级列出评估过程中的主要发现，提供修补方案及相关延伸资料（如适用）。

更多网络安全测试服务

没有任何单一的评估方法能全面反映组织的安全状态。每种对抗测试方式均有其特定目标及可接受风险水平。Sophos 可与您合作，以判断应采用哪些评估项目与技术组合，来评估您的安全防护现况与控制，从而找出您的漏洞。

服务特点

- 被动监控无线网络，来识别安全架构弱点、加密密钥漏洞、配置错误及防护措施不足。
- 高技术测试人员通过破解加密密钥、伪造接入点等方式获取用户凭据，以尝试访问。
- 提供包含详细的评估发现与修补建议的完整评估报告。
- 在前导会议中事先明确测试项目规则，确保过程透明、安心可控。
- 可根据需求选择服务范围，涵盖单一或多个物理地点。
- 远程测试具备与现场测试同等质量，灵活调度，能够针对因安全或管制因素而无法亲自前往的地点进行测试。
- 可选现场测试，适用于面积大或分布式场所。

了解更多:
sophos.com/advisory-services

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

2025-06-05 BRZHCN (MP)

SOPHOS