

黑客概述及目标系统的探测(nmap)

2024-04-22



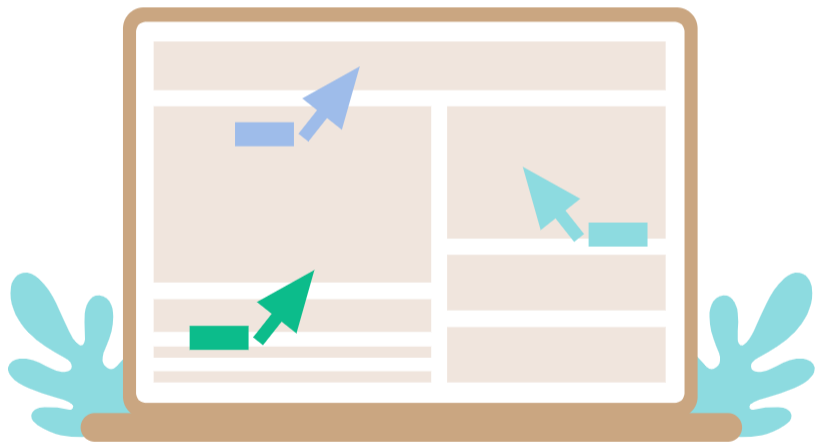
CONTENTS



- 引言
- 黑客攻击手段
- 黑客目标系统探测工具
- 系统安全防护

01 引言

引言



黑客攻击简介

了解黑客攻击的基本
概念。

黑客目标系统探

介绍黑客常用的目标
系统探测工具和技术

。

黑客攻击简介

黑客类型

黑客攻击可分为内部黑客和外部黑客两类。

01



攻击手段

黑客利用各种技术手段对系统进行攻击，获取敏感信息或者控制系统。

02



黑客目标系统探测

nmap工具:

nmap是一款功能强大的网络扫描工具，用于探测目标系统的开放端口和服务。

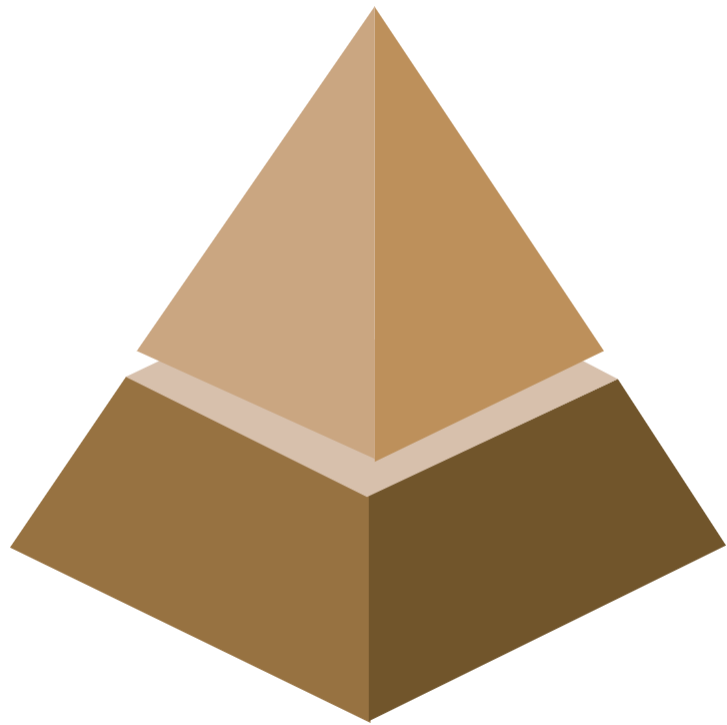
探测技术:

nmap支持多种扫描技术，包括TCP扫描、UDP扫描、操作系统识别等。



02 黑客攻击手段

黑客攻击手段



社会工程学攻击：

介绍黑客利用社会工程学手段获取系统信息和权限的方式。

恶意软件攻击：

探讨黑客利用恶意软件对系统进行攻击的方式。

社会工程学攻击

钓鱼攻击:

通过虚假邮件或网站诱导用户提交敏感信息。

伪装身份:

黑客假扮成合法用户或管理员获取系统权限。

恶意软件攻击

病毒:

植入系统并破坏系统功能或窃取信息

。

木马:

在系统中植入后门，允许黑客远程控制系统。



03

黑客目标系统探测工具

黑客目标系统探测工具

nmap基本用法：

介绍nmap工具的基本操作和常用参数。

高级扫描技术：

探讨nmap支持的高级扫描技术和用法。

01

端口扫描:

使用nmap扫描目标系统的
开放端口。



02

服务识别:

nmap可以识别目标系统正
在运行的服务类型。



高级扫描技术

01

操作系统识别:

nmap可以尝试识别目标系统的操作系统类型。

02

脚本扫描:

利用nmap脚本引擎执行自定义脚本对目标系统进行扫描。

04 系统安全防护

系统安全 防护

漏洞修复：

强调定期修补系统漏洞的重要性。
。

网络监控：

建议建立有效的网络监控机制以及反制黑客攻击。
。

漏洞修复

安全补丁:

及时安装系统提供的安全补丁。

漏洞扫描:

使用漏洞扫描工具检测系统漏洞并及时修复。



网络监控

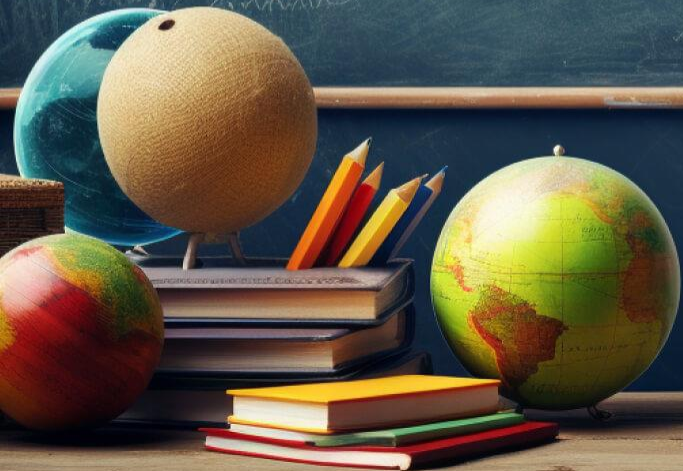
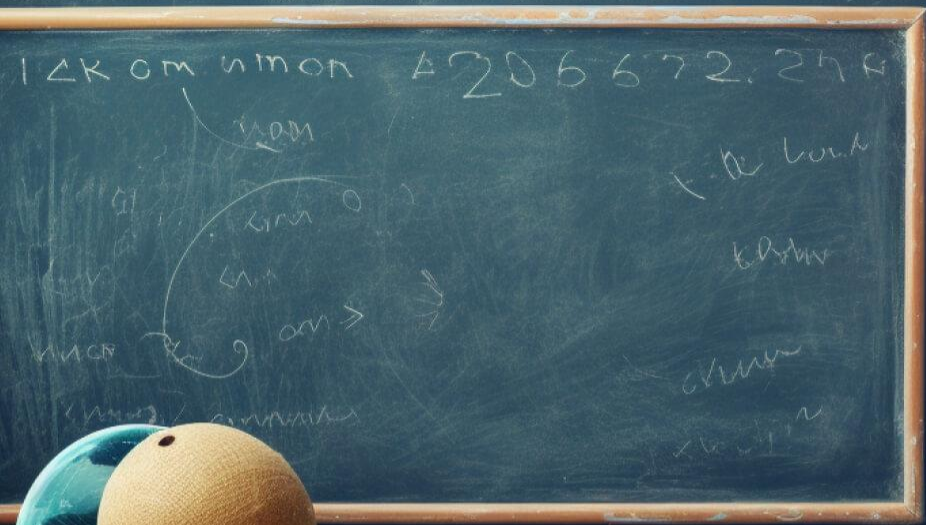


日志分析:

定期分析系统日志以发现异常行为。

入侵检测系统:

部署IDS/IPS系统检测异常网络流量。



THE END
THANKS