1.1 渗透测试

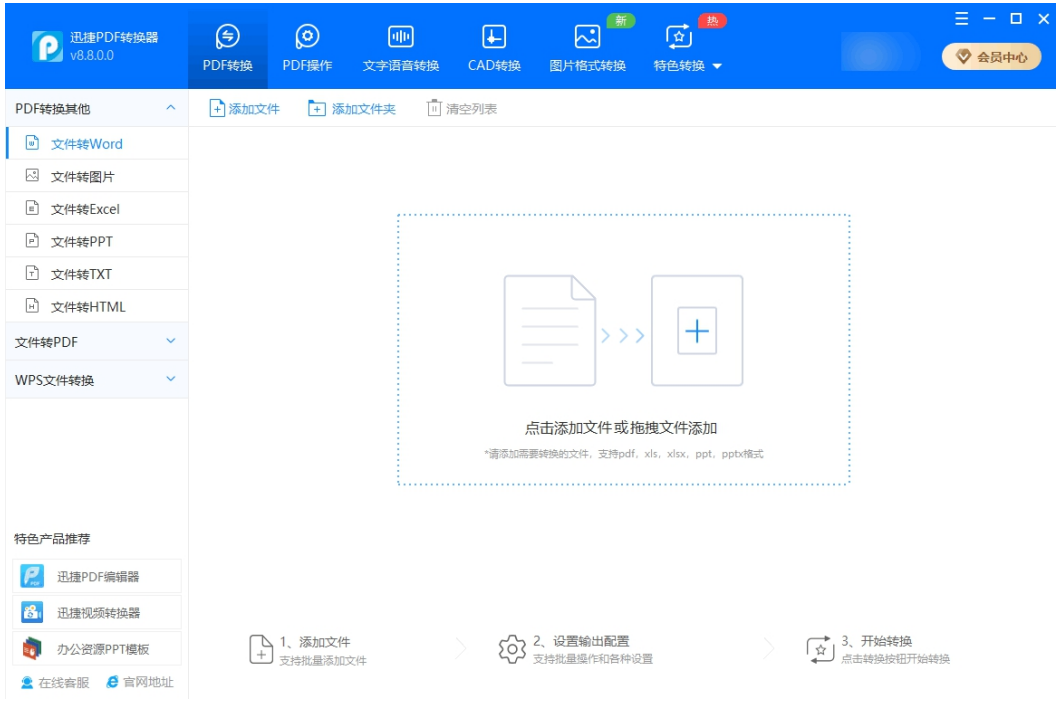
无涯老师

课程大纲

1、什么是渗透测试
2、渗透测试的对象
3、渗透测试的意义
4、渗透测试的流程
5、渗透测试与kali

01 什么是渗透测试

软件


迅捷PDF转换器
v8.8.0.0
PDF转换
PDF操作
文字语音转换
CAD转换
图片格式转换
特色转换
会员中心
PDF转换其他
文件转Word
文件转图片
文件转Excel
文件转PPT
文件转TXT
文件转HTML
文件转PDF
WPS文件转换
添加文件
添加文件夹
清空列表
点击添加文件或拖拽文件添加
*请添加需要转换的文件，支持pdf，xls，xlsx，ppt，pptx格式
特色产品推荐
迅捷PDF编辑器
迅捷视频转换器
办公资源PPT模板
在线客服
官网地址
1、添加文件
支持批量添加文件
2、设置输出配置
支持批量操作和各种设置
3、开始转换
点击转换按钮开始转换


中国建设银行
China Construction Bank
个人网银支付
客户服务热线：95533 | WWW.CCB.COM
2013-6-13 10:08:40
常见问题解答
退出支付
我的订单
商户名称：支付宝（中国）网络技...
订单号：201306130000000000470...
订单金额：336.00
支付币种：人民币
商户分行：浙江省建行
支付日期：2013-06-13
网上银行支付
账号支付
网上银行支付：适用于大众版网上银行、便捷支付客户。
* 证件号码或用户昵称：
忘记昵称?
* 登录密码：
忘记密码?
* 附加码：
a2gq4
看不清，换一张
下一步
©版权所有 中国建设银行版权所有 京ICP证 050138号 京公网安备 110102000450
总行地址：中国北京西城区金融大街25号 邮编：100033 手机网站：m.ccb.com
网站声明 联系我们 网站地图 友情链接

软件


19:49
长沙
晴 35℃
菜鸟购物特惠价
搜索
扫一扫
付钱/收钱
出行
卡包
饿了么
口碑
市民中心
芭芭农场
淘特
转账
充值中心
交通出行
找能量
蚂蚁森林
蚂蚁庄园
哈啰出行
我的快递
我的小程序
健康码
求助
反馈
• 你有小鸡饲料可以领取 10小时前
• 付款成功￥6.57 10小时前
信用好 先赚0.5元红包
开通芝麻GO充值9.6折
GO
淘特 | 抢1元好货 由淘特App提供
显示器
月售2925
退货包运费
¥220 ¥550
理财
口碑
消息
我的


10:10
LTE
Telefon
Musik
Karten
Nachrichten
Sie hören
Mercedes
Podcasts
Spotify

软件测试

软件测试与渗透测试

软件测试（功能、性能、安全）

安全三要素

保密性（Confidentiality） [ˌkɒnfɪˌdenʃiˈæləti]
完整性（Integrity） [ɪnˈtegrəti]
可用性（Availability） [əˌveɪləˈbɪləti]

渗透测试（Penetration Testing）

渗透测试指的是在目标系统授权的情况下，采取可控的入侵手法，模拟真实攻击者使用的各种方法和技术，绕过系统的防护措施（权限控制、加密、完整性、可靠性等），以检验系统在真实环境中的安全性，发现漏洞，达到保护重要资产的目的。

渗透测试

- 渗透测试的对象
- 渗透测试的意义
- 渗透测试的流程
- 渗透测试与kali

02 渗透测试的对象

渗透测试的对象

1、网络硬件设备
2、主机操作系统
3、应用系统
4、数据库系统

03 渗透测试的意义

渗透测试的意义

- 发现漏洞
- 了解安全状态
- 重视风险
- 提升防护水平

04 渗透测试的流程

渗透测试的流程

- 确定目标
- 信息收集
- 漏洞扫描
- 漏洞利用
- 形成报告/清除痕迹

确定目标

- 范围
- 规则（限制条件）
- 需求

信息收集

域名信息、IP段、开放的端口、网站架构、文件目录结构、软件版本、WAF、旁站、C段……

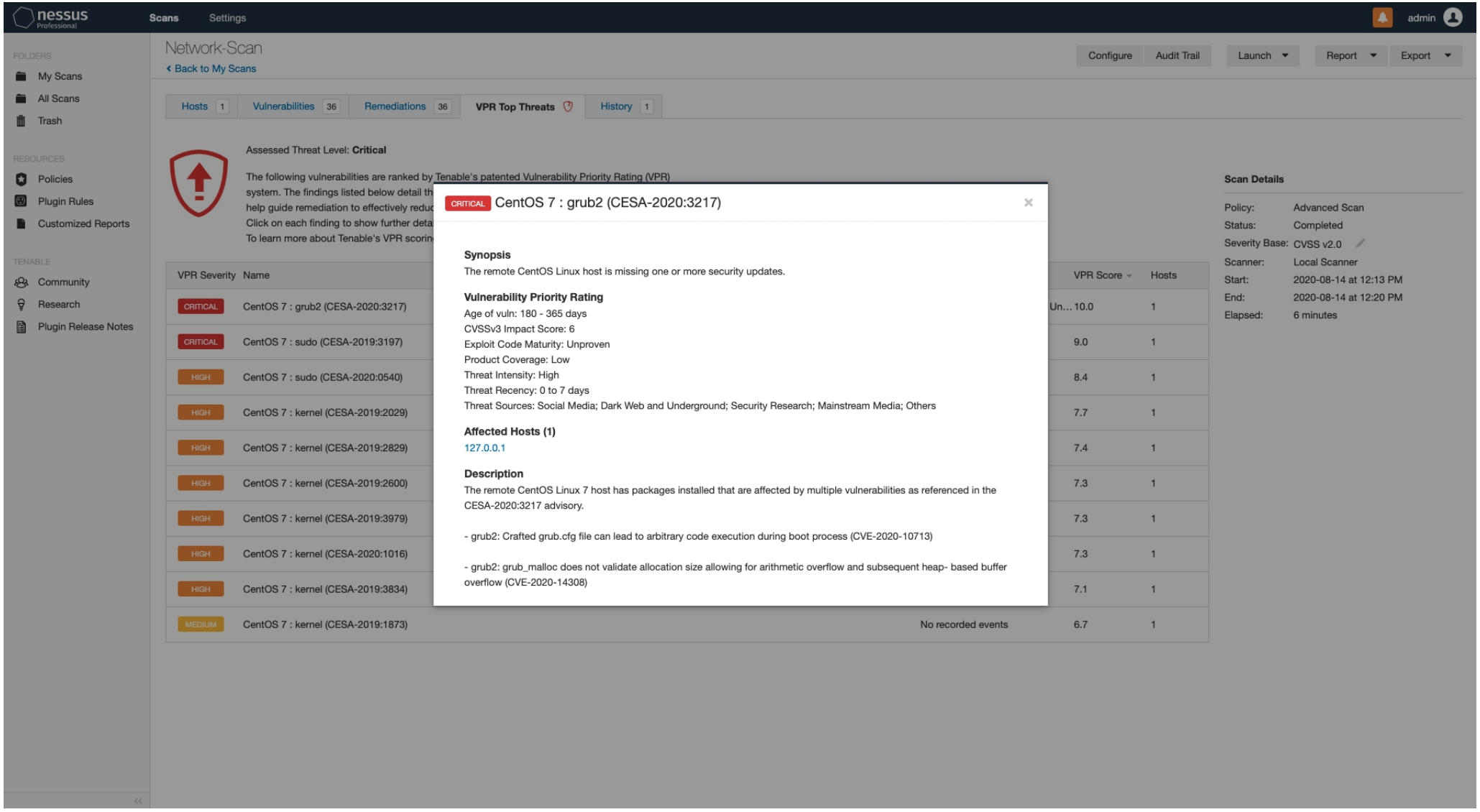
漏洞扫描

什么是漏洞？vulnerability [ˌvʌlnərə'bɪlətɪ]
和bug的区别
漏洞数据库
扫描工具
漏洞分类

漏洞平台

数据库	网址
国家信息安全漏洞库（CNNVD）	https://www.cnvd.org.cn/
国家信息安全漏洞共享平台（CNVD）	http://www.cnnvd.org.cn/
国家工业信息安全漏洞库(CICSVD)	https://www.cics-vd.org.cn/
CVE	http://cve.mitre.org/

漏洞扫描


nessus Professional
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
TENABLE
Community
Research
Plugin Release Notes
Network-Scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 36
Remediations 36
VPR Top Threats
History 1
Assessed Threat Level: Critical
The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR)
system. The findings listed below detail th
help guide remediation to effectively reduc
Click on each finding to show further deta
To learn more about Tenable's VPR scorin
VPR Severity
Name
VPR Score
Hosts
CRITICAL CentOS 7 : grub2 (CESA-2020:3217) 10.0 1
CRITICAL CentOS 7 : sudo (CESA-2019:3197) 9.0 1
HIGH CentOS 7 : sudo (CESA-2020:0540) 8.4 1
HIGH CentOS 7 : kernel (CESA-2019:2029) 7.7 1
HIGH CentOS 7 : kernel (CESA-2019:2829) 7.4 1
HIGH CentOS 7 : kernel (CESA-2019:2600) 7.3 1
HIGH CentOS 7 : kernel (CESA-2019:3979) 7.3 1
HIGH CentOS 7 : kernel (CESA-2020:1016) 7.3 1
HIGH CentOS 7 : kernel (CESA-2019:3834) 7.1 1
MEDIUM CentOS 7 : kernel (CESA-2019:1873) No recorded events 6.7 1
CRITICAL CentOS 7 : grub2 (CESA-2020:3217)
Synopsis
The remote CentOS Linux host is missing one or more security updates.
Vulnerability Priority Rating
Age of vuln: 180 - 365 days
CVSSv3 Impact Score: 6
Exploit Code Maturity: Unproven
Product Coverage: Low
Threat Intensity: High
Threat Recency: 0 to 7 days
Threat Sources: Social Media; Dark Web and Underground; Security Research; Mainstream Media; Others
Affected Hosts (1)
127.0.0.1
Description
The remote CentOS Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the CESA-2020:3217 advisory.
- grub2: Crafted grub.cfg file can lead to arbitrary code execution during boot process (CVE-2020-10713)
- grub2: grub_malloc does not validate allocation size allowing for arithmetic overflow and subsequent heap- based buffer overflow (CVE-2020-14308)
Scan Details
Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: 2020-08-14 at 12:13 PM
End: 2020-08-14 at 12:20 PM
Elapsed: 6 minutes

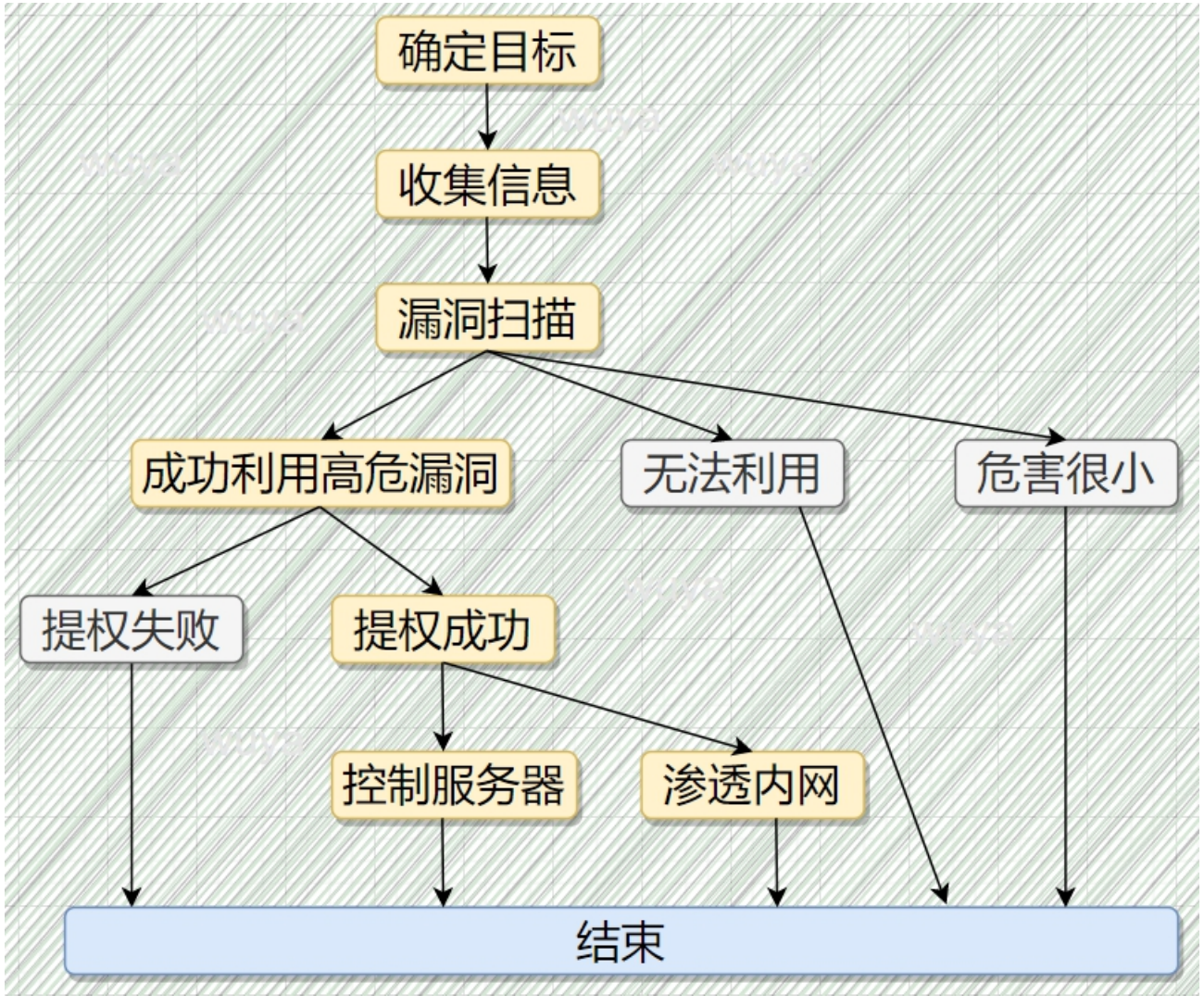
漏洞利用

攻击
防御绕过
维持访问（后渗透攻击）

形成报告

发现了什么漏洞
危害性
怎么发现的
如何复现
原因分析
修补建议

流程总结



05 渗透测试与Kali

渗透测试与Kali

An Advanced Penetration Testing Linux distribution used for Penetration Testing

Thank you for watching

无涯老师