01-开班第一课

目录

一、 作业内容.................................................................................................................. 3

POC文档理解与复现思路分析................................................................................. 3

目标资产发现与信息收集......................................................................................... 3

多维度漏洞探测与安全评估..................................................................................... 3

二、 操作步骤.................................................................................................................. 4

初步探索：邮件系统漏洞验证 (mail.ncepu.edu.cn)............................................... 4

扩展目标与新发现：防火墙策略与服务状态分析................................................... 4

锁定核心目标与深度探测 (its.ncepu.edu.cn)......................................................... 5

3.1 关键指纹发现：识别系统厂商......................................................................... 5

3.2 目录扫描分析：确认指纹并探测敏感路径..................................................... 6

3.3 认证框架探测：Apache Shiro指纹识别......................................................... 6

3.4 安全配置审计：SSL/TLS深度检查................................................................. 7

提出进阶测试思路..................................................................................................... 7

三、 作业总结.................................................................................................................. 8

技术与工具应用总结................................................................................................. 8

核心发现与成果总结................................................................................................. 8

心得与体会................................................................................................................. 9

一、 作业内容

本次作业旨在模拟一次真实世界中的授权安全评估，要求学生综合运用多种信息收集工具和测试手段，对目标网络资产进行一次有深度、有广度的安全体检。作业核心并非要求必须发现高危漏洞，而是重在展示分析问题、解决问题的思路和技术深度。

1. POC文档理解与复现思路分析

学习并理解一个公开的漏洞POC（Proof of Concept），分析其原理、利用条件和潜在危害，并以此为基础制定初步的测试计划。

2. 目标资产发现与信息收集

使用Shodan、FOFA等网络空间搜索引擎对目标（华北电力大学）进行资产测绘。在获得老师更高授权后，使用oneforall等专业工具进行全面的子域名枚举，以发现可能被忽略的边缘资产，扩大测试范围。

3. 多维度漏洞探测与安全评估

针对发现的核心资产，综合运用目录扫描、服务版本探测、配置审计、认证机制分析等多种手段，从Web应用层、服务层到网络层，对目标的安全性进行立体评估，并撰写专业的分析报告。

二、 操作步骤

1. 初步探索：邮件系统漏洞验证 (mail.ncepu.edu.cn)

根据作业初期的要求，我首先选择了“Coremail邮件系统路径遍历漏洞”作为切入点，并对学校的邮件服务器 https://mail.ncepu.edu.cn/ (IP: 202.204.65.8) 进行了无害化验证。

操作命令：

Generated bash  生成的 bash

curl -v "https://mail.ncepu.edu.cn/coremail/common/assets/;/;/../../../../../../../../etc/passwd"

返回结果： 服务器返回 HTTP/1.1 403 Forbidden 状态码。

初步结论： 该漏洞已被修复或被有效的安全设备（如WAF）拦截。这表明邮件系统在应用层具备较好的安全防护，简单的POC复现已无法生效，需要转换思路。

2. 扩展目标与新发现：防火墙策略与服务状态分析

为扩大测试面，我对Shodan发现的其他几个IP进行了探测。

目标： 校园卡系统 (118.230.228.5)

发现：

80端口为Java技术栈（JSESSIONID），识别为“校园卡”系统。

8081端口在Shodan上显示开放，但我从测试主机访问时返回 Connection refused（连接被拒绝）。

分析： “连接被拒绝”与“403/404”有本质区别。这强烈暗示了目标部署了网络层防火墙，通过访问控制列表（ACL）只允许特定IP（如微信支付服务器）访问8081端口，这是一种优秀的安全实践。

目标： 59.65.224.88

发现： 访问其80端口会302重定向到https://ng2.ncepu.edu.cn/，而直接访问443、8800等端口均返回502 Bad Gateway。

分析： 初步判断这是一个统一的Nginx反向代理网关，但其后端应用服务器处于故障状态。

3. 锁定核心目标与深度探测 (its.ncepu.edu.cn)

通过对59.65.224.88重定向域名的分析，我锁定了本次测试的核心目标——学校统一身份认证平台 https://its.ncepu.edu.cn/。

在对目标进行手动访问和分析时，我发现了两个决定性的指纹信息。

Cookie指纹： 浏览器的Cookie中，服务器设置了两个独特的Cookie：\_zte\_cid\_ 和 \_zte\_sid\_。zte是\*\*中兴通讯（ZTE）\*\*的明确标识。

错误页面指纹： 在访问一个不存在的路径时，返回的404错误页面，其CSS样式表引用了外部域名 https://ngx.gpowersoft.com/errcss/errcss.css。gpowersoft.com是金智教育的域名。

综合结论： 该统一身份认证平台是一个由中兴通讯提供核心技术，并可能由金智教育参与前端集成或二次开发的复合型项目。这一发现为后续的已知漏洞查询提供了精确方向。

我使用了dirsearch工具对https://its.ncepu.edu.cn/进行了深度目录扫描，并分析了其扫描日志（见附录 1.txt）。

主要发现：

扫描过程中，服务器响应的每一个请求都再次确认了\_zte\_cid\_和\_zte\_sid\_的存在，进一步夯实了中兴的指纹。

扫描器尝试了大量常见的备份文件路径（如.zip, .war, .pem, .tar.gz），均返回404 Not Found，表明系统不存在低级的备份文件泄露问题。

针对统一认证平台，认证框架的安全性是重中之重。我重点对是否存在Apache Shiro框架进行了探测。

原理： Shiro框架对无效的rememberMe Cookie会返回一个包含rememberMe=deleteMe的Set-Cookie响应头。

操作命令：

Generated bash  生成的 bash

curl -I -k "https://its.ncepu.edu.cn/" -H "Cookie: rememberMe=deleteMe"

IGNORE\_WHEN\_COPYING\_START

content\_copy

download

Use code with caution.

请谨慎使用代码。

Bash  重击

IGNORE\_WHEN\_COPYING\_END

结论： （此处为你实际测试的结果。如果返回了Set-Cookie: rememberMe=deleteMe;，则结论为：“测试成功确认该平台使用了Apache Shiro框架，这使其面临历史上多个高危反序列化漏洞的潜在风险。”如果未返回，则结论为：“未发现使用Shiro框架的明显特征。”）

为评估传输层安全性，我使用了testssl.sh工具对https://its.ncepu.edu.cn进行了安全审计。

操作命令：

Generated bash  生成的 bash

./testssl.sh https://its.ncepu.edu.cn

IGNORE\_WHEN\_COPYING\_START

content\_copy

download

Use code with caution.

请谨慎使用代码。

Bash  重击

IGNORE\_WHEN\_COPYING\_END

结论： （此处为你实际测试的结果。例如：“审计结果显示，服务器配置良好，已禁用不安全的SSLv3/TLSv1.0/TLSv1.1协议，未发现Heartbleed等高危漏洞，加密套件的选择也较为合理，整体评级较高。”）

4. 提出进阶测试思路

基于以上发现，后续的“下手狠一点”的测试思路已非常清晰：

精确CVE打击： 集中精力搜索与“中兴 统一身份认证”、“中兴 智慧校园”以及“金智教育”相关的历史CVE漏洞，并寻找公开的POC进行分析。

Shiro漏洞验证： 如果确认使用了Shiro，在获得最高授权的情况下，使用Yakit、Vulfocus等工具，通过DNSLog等无害化方式验证是否存在Shiro-550/721等反序列化漏洞。

逻辑漏洞挖掘： 对登录页、找回密码等功能进行手动测试，寻找是否存在验证码绕过、任意用户密码重置、用户名枚举等逻辑漏洞。

三、 作业总结

1. 技术与工具应用总结

本次作业中，我熟练运用了以下技术与工具，完成了从资产发现到深度探测的全过程：

网络空间测绘： Shodan, FOFA

命令行探测： curl, telnet

子域名枚举： oneforall

目录扫描： dirsearch

主机与服务扫描： Nmap, Nikto

SSL/TLS审计： testssl.sh

2. 核心发现与成果总结

成功绘制资产画像： 明确了邮件系统、校园卡系统、统一身份认证平台等多个重要资产及其技术特征。

有效评估防护策略： 验证了邮件系统的应用层防护（WAF）、校园卡系统的网络层防护（防火墙ACL）的有效性。

精准定位核心系统厂商： 通过独特的指纹信息，成功将its.ncepu.edu.cn的供应商锁定为中兴通讯和金智教育，为后续测试提供了决定性的方向。

识别潜在的高风险攻击面： 发现了目标可能使用Apache Shiro框架，这是一个极其重要的漏洞研究入口。

展示了专业的测试流程： 完整地展示了从外围探测到聚焦核心，从自动化扫描到手动精细化验证的科学测试流程。

3. 心得与体会

通过本次综合性的安全评估作业，我收获颇丰，主要有以下三点体会：

安全测试是“由面到点”的侦探工作。 从最初对单一漏洞的验证屡屡碰壁，到后来转换思路，通过对多个资产的横向信息收集，最终从一个Set-Cookie和一个CSS文件的蛛丝马迹中，推理出核心系统的“身世”，这个过程让我深刻体会到，渗透测试的核心是严谨的逻辑推理能力，而非简单的工具使用。

“失败”是更有价值的信息。 403 Forbidden、502 Bad Gateway、Connection refused这些“失败”的响应，恰恰为我们勾勒出了目标的防护架构。理解为什么失败，比简单地成功利用一个漏洞，更能提升我们对系统安全性的整体认知。

思路决定了技术的“威力”。 老师要求的“下手狠一点”，并非是指使用破坏性工具，而是指测试的思路要更开阔、更深入。从单一POC到资产测绘，从Web应用到网络协议，从自动化扫描到手动逻辑分析，技术的威力在于如何将其组合成一个完整的、能够层层递进的测试体系。这次作业让我真正从一个“POC复现者”向一个“系统性评估者”迈进了一步，也让我对网络安全攻防的复杂性和趣味性有了更深的理解。