IT 4500：信息安全

第1天

乔·弗兰科姆博士

2014年春季

介绍

教学大纲 网站 画布 实验室模拟

活动1

使用以下网站（或其他网站）查找2-3个安全漏洞（5分钟）：

- http://datalossdb.org/
- google.com
- http://www.us-cert.gov/
- http://arstechnica.com/security/

对你找到的漏洞做一些笔记。 你能确定发生了什么吗？为什么会发生？ 组织采取了什么措施来解决这个问题？ 修复它花费了他们多少钱？它是可以预防的吗？ 准备好分享你的发现。

IT 4500：信息安全

第2天

乔·弗兰科姆博士

2015年春季

复习

- 总结你从s1.0和s1.1讲座中学到的东西

活动1

快速浏览一下这篇文章，看看你能否回答以下问题：（在结果和分析部分查找）

- 大多数安全事件发生在哪里？
- 它们是由谁实施的？哪些国家？
- 这些事件通常分为哪些不同的类别？
- 你还发现了其他有趣的事情吗？

准备好展示你的发现。

活动2

让我们进行一些简单的侦察。 找一些不同的网络工具，可以为你收集关于
这个 `cit.cs.dixie.edu` 网站的信息。 目前我们并不打算入侵任何东西，只是收集信息。
回答以下问题：

- 你找到了什么信息？
- 你可以用这些信息做什么？
- 有没有办法防止这些信息泄露？
- 你能找出正在运行的Apache版本吗？ 那么开放了哪些端口？ 它运行的操作系统版本是什么？

（提示：从Google搜索开始 在线侦察工具）

活动3

为你选择的一个程序找到3个当前的漏洞（如果你想不到其他
程序，WordPress有一些）：

- http://osvdb.org/
- http://www.us-cert.gov/ncas/current-activity/
- http://secunia.com/community/advisories/search/

回答以下问题：

- 为什么存在漏洞？
- 关于漏洞提供了哪些信息？
- 建议如何修复？
- 其他相关信息？

结论

Exim示例

IT 4500：信息安全

第三天

乔・弗兰科姆博士

2014年春季

复习

- 总结从s2.1-2.3讲座中学到的内容
- 什么是带外认证?

活动1

http://arstechnica.com/security/2014/10/google-offers-usb-security-key-to-make-bad-passwords-moot/

活动2

http://confidenttechnologies.com/demos/secure-second-factor-demo https://www.keylemon.com/(面部识别)

活动3

- http://www.youtube.com/watch?v=lSLxbobQ6Fg
- http://www.youtube.com/watch?v=H3TheqOaXas#t=167
- http://www.keyboard-biometrics.com/online-demo.html
- http://www.govivace.com/
- http://www.biochec.com/

IT 4500：信息安全

第4天

乔·弗兰科姆博士

2014年春季

复习

- 总结你从第2节课中学到的内容

活动1

什么是freeRadius?

活动2

定位你计算机上显示成功和失败认证的日志。 在Windows系统上，可以通过右键单击我的电脑并选择管理来找到它们。然后，在计算机管理对话框中，在左列中展开事件查看器。 展开Windows日志并选择安全。在Ubuntu Linux系统（以及许多其他Linux发行版）中，认证日志可以在/var/log/auth.log中找到。

定位任何失败的登录尝试。

记录如何配置日志文件的最大大小以及当达到该最大大小时系统将执行的操作。

活动3

- IBM的身份管理示例
- 尝试身份管理（如果你想玩一下，不能全班一起做，否则会给服务器带来压力）
    - http://www.microsoft.com/en-us/server-cloud/products/forefront-identity-manager/try.aspx
    - 我使用Windows IE和Linux FF都成功了
    - 什么是供应?

活动4

首先，研究什么是apparmor：

- http://askubuntu.com/questions/236381/what-is-apparmor
- http://ubuntuforums.org/showthread.php?t=1008906
- https://help.ubuntu.com/community/AppArmor

问题：

这与我们当前的主题有什么关系?

活动5

- 尝试apparmor
  - 这里
- 使用一次性密码
  - https://www.digitalocean.com/community/tutorials/install-and-use-otpw

---

活动5

更多Linux用户安全性：

- chage
- ulimit（无法真正测试，但请参阅man页面了解其功能）
- `/etc/security`

活动6

加密？实验和帮助？

IT 4500：第5天

概述

乔·弗兰科姆博士

复习

加密对CIA三角的哪些部分有帮助？ 为什么公开算法比秘密算法更安全？

活动1

隐写分析和隐写术

- 隐写术是以一种使除了发件人和预期收件人以外的任何人都不怀疑消息存在的方式编写隐藏消息的艺术和科学，是一种通过安全性的模糊性来保护信息的形式
- 隐写分析是检测使用隐写术隐藏的信息的艺术和科学；

隐写分析和隐写术

它是如何工作的？ 请记住，每个像素可以用3个字节（RGB）的组合来表示。 我们可以取出其中的一些字节，并将我们的文本放在那里，只会稍微降低图像质量。

示例：下载并安装steghide

```
        apt-get安装steghide#在kali上不容易做到
```

- 获取一张图片（支持jpg，可能还有其他格式）
- 在记录图像大小之前和之后可能会有趣。

```
steghide  embed  -cf  picture.jpg  -ef  secret.txt
steghide  extract  -sf  picture.jpg
steghide  info  received_file.wav
```

隐写分析和隐写术

那么，这可能用于什么？

隐写术与加密不同。 加密将消息混淆，以使其无法查看，而隐写则隐藏了数据的存在。 可以隐藏在文件头字段中，在元数据的各个部分之间。 可以使用图像、声音、电影等。

活动2

攻击密码

- 暴力破解攻击（密码学）
- 字典攻击

活动3

中间人攻击

- MITM
- 重放攻击

活动4

哈希

- md5
- sha

IT 4500：第6天

概述

乔·弗兰科姆博士

2015年春季

复习

在第4节中，你注意到了什么?

活动0

使用ettercap gui的中间人攻击

活动1

社会工程学工具包-伪造的电子邮件-恶意网站

活动2

钓鱼邮件列表

活动3

取证示例 http://cit.dixie.edu/it/4500/projects/lab4.php

IT 4500：第7天

概述

乔・弗兰科姆博士

2014年春季

复习

你在6.1-6.3节中学到了什么?

活动1

- 使用scapy欺骗数据包

活动2

- Armitage

活动3

- OpenVAS或其他扫描器

活动5

DOS攻击

- http://www.youtube.com/watch?v=R8k-cJnrIrc
- http://www.cvedetails.com/version/142323/Apache-Http-Server-2.2.22.html
- msfconsole
- 使用辅助/dos/http/apache_range_dos
- 设置 RHOSTS 144.38.x.y
- 利用

IT 4500：第8天

概述

乔·弗兰科姆博士

2015年春季

复习

你还从第6节中找到了什么有趣的东西吗?

活动1

以2或3人为一组，找到以下示例，并向班级演示。 你将有15-20分钟的时间来找到、安装并弄清楚它们的工作原理，然后你可以向我们展示你学到了什么：

- 防火墙（Linux或Windows）
- 代理服务器
- HTTP内容过滤器（Windows站点限制）
- VPN解决方案（比如logmein或其他相关的）
- 病毒阻止器
- 反钓鱼软件
- 相关技术（K9浏览器，opendns）

IT 4500：第9天

概述

乔·弗兰科姆博士

2014年春季

复习

总结第7节

活动1

http://cit.dixie.edu/it/4500/sources/rootkits.php

活动2

入侵检测和预防

看看snort。（基于网络）

再次分成小组，研究并安装一个IPS或IDS（基于主机）

活动3

活动4

IT 4500：第10天

乔·弗兰科姆博士

2014年春季

复习

- 恶意软件
- 病毒和蠕虫之间有什么区别?
- 特洛伊木马和僵尸网络有什么关系?
- 软件被隔离意味着什么?
- 为什么应该显示文件扩展名?

复习2

- 你对密码攻击有了新的了解吗?
- 如何减轻彩虹表攻击的影响?
- 如何减少设备的攻击面以加固它?
- 热修复 vs 补丁?

活动1

- 恶意软件字节
- 一些示例文件？这里
- Windows Defender?
- 恶意软件字节是一种反病毒软件吗?
- 查找/研究/安装一款反病毒软件。 准备好讨论你的结果

活动2

- 蜜罐

活动3

- 僵尸网络研究
  - 找一些不同的僵尸网络示例（Zeus是一个可以开始的）
  - 安装有多容易/困难？ （你不需要安装它，只需寻找说明）

活动4

IT 4500：信息安全

安全编程

乔·弗兰科姆博士

缓冲区溢出

它是什么?

当程序或进程尝试将更多数据存储在缓冲区（临时数据存储区）中时，缓冲区溢出就会发生，而这些数据超过了其预期容量。 由于缓冲区被创建来包含有限数量的数据，额外的信息（必须存放在某个地方）可能会溢出到相邻的缓冲区中，从而破坏或覆盖其中保存的有效数据。 -http://searchsecurity.techtarget.com/definition/buffer-overflow

视频

更多

攻击者需要能够识别某个程序中的缓冲区溢出漏洞，并了解该缓冲区将如何存储在进程内存中，并知道他可以写入哪些其他相邻的内存项。

- 可能会使系统DOS

为了做到这一点，可以使用一种称为模糊测试的技术。

模糊测试

模糊测试涉及向应用程序（和Web）输入发送格式错误的字符串，并观察是否出现意外崩溃。 有很多有趣的教程可以教你如何做到这一点。 在找到这种格式错误的输入后，通常会使用汇编语言来找出如何传递shellcode（或如何传递利用程序）。

模糊测试在软件开发中确实有实际用途，但也是黑客用来发现应用程序漏洞的工具。

许多模糊测试工具：ComRaider（activeX），在安全发行版上查看fuzztools。

模糊测试

-视频

- http://blog.chromium.org/2012/04/fuzzing-for-security.html

为什么程序容易受到缓冲区溢出的攻击?

- 糟糕的编程
- 计算机不在乎...程序员需要确保内存受到限制
- 低级语言

如何防止缓冲区溢出

- 编译时防御

- 选择一种更高级的语言（缺点？）
- 优雅的失败
- 地址空间布局随机化（由操作系统实现）
- NX位

示例

- 漏洞数据库
- 这很有趣
- bufbomb示例= 让程序执行原本不设计的操作
- Exim示例= 访问shellcode

安全编程

- SDLC（尤其是维护和测试）
- 最小特权原则
- 永远不要相信用户输入（输入验证）
- 减少攻击面积（删除未使用的功能）
- 安全失败（try/catch）
- 正确修补和解决问题

软件安全

软件安全与软件质量和可靠性密切相关。

防御性编程：旨在确保软件在不可预见的使用情况下仍能正常运行。 有时也称为“安全编程”。不要对代码做任何假设
。

该怎么办?

大多数程序员关注解决问题（涉及的算法），而不考虑每个可能的故障点。 通常对输入和执行环境做出假设。防御性程序员应该
：

- 验证所有输入
- 处理潜在故障

软件安全必须在开发的设计阶段实施，而不是事后补救。

处理程序输入

软件安全中最常见的故障之一。

输入并不总是明确已知的。 对输入进行假设可能是不好的。您应该始终谨慎处理输入，以确保其有效。

输入的两个关键关注领域是：

- 输入的大小
- 输入的含义和解释

不要做任何假设，验证一切。

输入

输入是否符合您的期望？即，如果您期望一个文件名，输入是否遵循典型的文件名模式？

注入攻击：基本上，这是攻击者提供非预期的输入，以便做一些他们不应该做的事情。 它影响程序的控制或执行。 在PHP或其他网页脚本中常见

预期输入=预期结果，但如果攻击者注入命令，例如 `xxx; echo success; ls -l finger *`