网络攻防实战

第五周

陈健

chenj@nju.edu.cn

终端多路复用器

- 终端多路复用器允许同时与多个shell会话进行交互，并可以分离当前终端会话以在将来重新连接
- tmux
  - 会话session->窗口window->面板pane
  - 会话
    - tmux new –s NAME 以指定名称开始一个新的会话
    - tmux ls 列出当前所有会话
    - <C-b> d 在tmux中按下该组合键，将当前会话分离
    - tmux a 重新连接最后一个会话，可以通过-t参数指定具体的会话

终端多路复用器

- tmux
  - 窗口
    - <C-b> c 创建一个新的窗口
    - <C-b> p 切换到上一个窗口
    - <C-b> n 切换到下一个窗口
    - <C-b> , 重命名当前窗口
    - <C-b> w 列出当前所有窗口
  - 面板
    - <C-b> " 水平分割
    - <C-b> % 垂直分割
    - <C-b> <方向键> 切换到指定方向的面板
    - <C-b> z 切换当前面板的缩放
    - <C-b> <空格> 在不同的面板布局间切换

KALI设置软件源

- 编辑文件/etc/apt/sources.list
  - $ sudo mousepad /etc/apt/sources.list

```
deb http://mirror.nju.edu.cn/kali kali-rolling main contrib non-free non-free-firmware
```

KALI软件更新

- 更新本地软件包索引
  - sudo apt update
- 升级所有已安装软件包到新版本
  - sudo apt upgrade
- KALI大版本升级
  - sudo apt-get dist-upgrade

谨慎使用

KALI软件包管理

- 搜索软件包
  - apt-cache –n search 软件包名
- 安装软件包
  - apt install 软件包名
- 卸载软件包
  - apt remove 软件包名
  - apt purge 软件包名
    - 删除软件包括其配置文件

KALI软件包管理

- 查看软件包是否已安装
  - apt list --installed | grep 软件包名
  - dpkg –l 软件包名
- 查看已安装软件包中包含的文件
  - dpkg –L 软件包名
- 查看某个命令是由哪个软件包提供
  - dpkg –S command

KALI设置中文环境

- sudo dpkg-reconfigure locales
  - 选择字符编码： en_US.UTF-8、zh_CN.UTF-8
  - 选择zh_CN.UTF-8 后回车确认
- 安装字体
  - sudo apt install fonts-wqy-zenhei xfonts-wqy
- 重启

为什么要做渗透测试

在网络攻防中，攻易守难！

渗透测试的起源

- 在信息科技的发源地----美国的军事演习中，将美军称为“蓝军”，将假想敌称为“红军”
- 这种军事演习的方式在20世纪90年代由美国军方与国家安全局引入到对信息网络与信息安全基础设施的实际攻防测试过程中。由一群受过职业训练的安全专家称为“红队”，对接受测试的防御方“蓝队”进行攻击，以实战的方式来检验目标系统安全防御体系与安全响应计划的有效性。

渗透测试

- 渗透测试（penetration testing，pentest）就是通过实际的网络攻击进行安全测试与评估的方法
  - 简而言之，渗透测试就是一种通过模拟恶意攻击者的技术与方法，挫败目标系统安全控制措施，取得访问控制权，并发现具备业务影响后果安全隐患的一种安全测试与评估方式。

渗透测试的类型

- 黑盒测试（外部测试）
  - 设计为模拟一个对客户组织一无所知的攻击者所进行的渗透攻击。在安全业界的渗透测试者眼中，黑盒测试通常更受推崇，因为它能更逼真地模拟一次真正的攻击过程
- 白盒测试（内部测试）
  - 在拥有客户组织所有知识的情况下所进行的渗透测试。白盒测试无需进行目标定位与情报搜集，并且能够比黑盒测试发现更多的目标基础设施环境中的安全漏洞与弱点。但它的缺点是无法有效地测试客户组织的应急响应程序
- 灰盒测试
  - 以上两种渗透测试基本类型的组合。测试者掌握了目标系统的有限知识与信息，采用的方法也是从外部逐步渗透进入目标网络
- 内部网络测试
  - 假设攻击者可以成功进入公司内部（物理上的或是通过邮件钓鱼的方式获得远程访问权限）所进行的渗透测试

渗透测试过程环节

- 前期交互阶段（Pre-Engagement Interaction）
  - 确定渗透测试的范围、目标、限制条件以及服务细节
- 情报搜集阶段（Information Gathering）
  - 获取更多关于目标组织网络拓扑、系统配置与安全防御措施的信息
- 威胁建模阶段（Threat Modeling）
  - 通过团队共同的缜密情报分析与攻击思路头脑风暴，从大量的信息情报中理清头绪，确定出最可行的攻击通道

渗透测试过程环节

- 漏洞分析阶段（Vulnerability Analysis）
  - 综合分析前几个阶段获取并汇总的情报信息，通过搜索可获取的渗透代码资源，找出可以实施渗透攻击的攻击点，并在实验环境中进行验证
  - 常见漏洞
    - 默认的密码或配置
    - 在多个系统中共享同一个认证证书
    - 所有用户都有本地管理权限
    - 没有及时对已公开的漏洞打补丁

渗透测试过程环节

- 渗透攻击阶段（Exploitation）
  - 利用找出的目标系统安全漏洞，真正入侵系统，获得访问控制权
- 后渗透攻击阶段（Post Exploitation）
  - 根据目标组织的业务经营模式、保护资产形式与安全防御计划的不同特点，自主设计出攻击目标，识别关键基础设施，寻找客户组织最具价值和尝试安全保护的信息和资产，最终达成对客户组织造成最重要业务影响的攻击。
- 报告阶段（Reporting）

常用工具

- 收集目标主机信息
  - nmap
- Web目录枚举
  - dirsearch
  - dirbuster
  - gobuster
- Web系统集成攻击平台
  - burpsuite

常用工具

- 反弹shell
  - Kali端口监听命令：nc
  - https://github.com/acole76/pentestmonkey-cheatsheets/blob/master/shells.md
  - https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/shell-reverse-cheatsheet/
  - msfvenom

常用工具

- 文件传输
  - python2
    - python –m SimpleHTTPServer 80
  - python3
    - python -m http.server 80
  - wget http://kali.ip/filename

常用工具

- 目标主机系统的本地信息枚举
  - LinPEAS
    - https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
  - WinPEAS
    - https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS
- 漏洞库网站
  - https://www.exploit-db.com

常用工具

- Metasploit Framework
  - HD Moore于2003年发布了Metasploit开源渗透测试框架
  - 2009年，Metasploit项目被渗透测试技术领域的知名安全公司Rapid7所收购，除了Metasploit框架仍保持开源以外，还推出了Metasploit Express和Pro商业版本

靶机demo 1的渗透测试

https://box.nju.edu.cn/f/15b768edb5904b1c8f24/?dl=1