1 Metasploit渗透框架

> #2课时

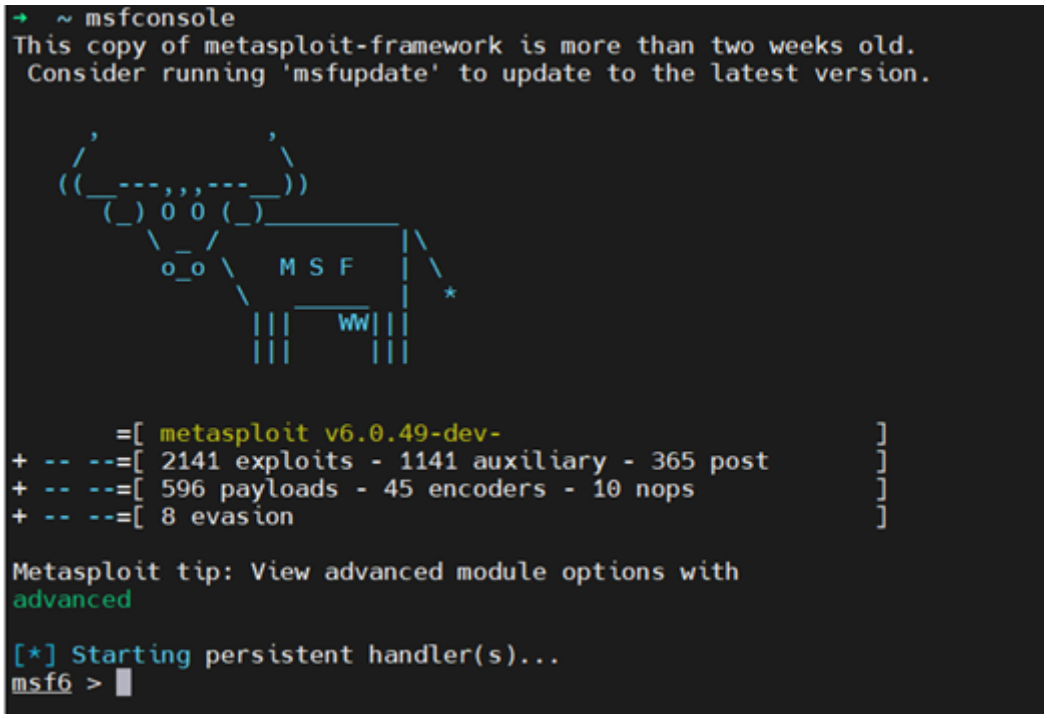
1.1 启动msfconsole

```
msfconsole
```

`Msfconsole` 是 `Metasploit` 框架用户接口，我们能通过 `Msfconsole` 接口使用 `Metasploit` 中所有模块

`Msfconsole` 主要用于:

1. 管理`Metasploit`数据库
2. 管理会话
3. 配置启动`Metasploit`模块



1.2 MSF命令查询

1.2.1 常用命令

```
show exploits - 查看所有可用的渗透攻击程序代码
show auxiliary - 查看所有可用的辅助攻击工具
[show ]options/advanced - 查看该模块可用选项
```

```
show payloads – 查看该模块适用的所有载荷代码
show targets – 查看该模块适用的攻击目标类型
search – 根据关键字搜索某模块
info – 显示某模块的详细信息
use – 使用某渗透攻击模块
back – 回退
set/unset – 设置/禁用模块中的某个参数
setg/unsetg – 设置/禁用适用于所有模块的全局参数
```

1.3 MSF模块介绍

> 模块是通过Metasploit框架装载集成对外提供的最核心的渗透测试功能实现代码。
> MSF所有的漏洞测试都是基于模块。

`Metasploit` 中有以下 7 种不同的模块类型

模块名	模块功能	模块介绍
auxiliary	辅助模块	辅助渗透（端口扫描、登录密码爆破、漏洞验证等）
exploits	漏洞利用模块	包含主流的漏洞利用脚本，通常是对某些可能存在漏洞的目标进行漏洞利用。命名规则：操作系统/各种应用协议分类
payloads	攻击载荷	主要是攻击成功后在目标机器执行的代码，比如反弹shell的代码
post	后渗透阶段模块	漏洞利用成功获得meterpreter之后，向目标发送的一些功能性指令，如：提权等
encoders	编码器模块	主要包含各种编码工具，对payload进行编码加密，以便绕过入侵检测和过滤系统

模块名	模块功能	模块介绍
evasion	躲避模块	用来生成免杀payload
nops	空指令模块	空指令就是空操作，提高paylaod稳定性及维持大小

- 辅助模块（**Auxiliary**）

用于辅助操作的模块，辅助模块能在渗透之前得到目标系统丰富的情报信息，从而发起更具目标性的精准攻击。

例如针对各种网络服务的扫描与查点、网络扫描、枚举、漏洞扫描、登录口令暴力破解、模糊测试、爬虫遍历、数据提取等

此外，辅助模块中还包括一些无须加载攻击载荷，同时往往不是取得目标系统远程控制权的渗透攻击，例如：拒绝服务攻击。

- 渗透攻击模块（**Exploits**）

用于利用漏洞和传递有效负载的模块。利用发现的安全漏洞或配置弱点对远程目标系统进行攻击，以植入和运行攻击载荷，从而获得对目标系统访问控制权的代码组件。

有远程漏洞利用、本地漏洞利用、权限提升漏洞利用、客户端漏洞利用、Web 应用程序漏洞利用和许多其他漏洞。

- 攻击载荷模块（**Payloads**）

用于在利用期间执行操作的模块。攻击载荷是在渗透攻击成功后在目标系统运行的一段植入代码，通常是为渗透攻击者打开在目标系统上的控制会话连接。在传统的渗透代码开发中，攻击载荷只是一段功能简单的`shellcode`代码，以汇编语言编制并转换为目标系统CPU体系结构支持的机器代码，在渗透攻击触发漏洞后，将程序执

行流程劫持并跳转入这段机器代码中执行，从而完成`ShellCode`中实现的单一功能。

例如建立 `Meterpreter` 会话、反向 `shell`、执行命令、下载和执行程序等。

- 后渗透攻击模块（**Post**）

用于在拿到权限后进行后渗透利用操作的模块，例如凭证/哈希转储、本地权限提升、后门安装、敏感数据提取、网络流量隧道（代理）、键盘记录、屏幕捕获和许多其他操作。

- 空指令模块（**Nops**）

用于生成无害、良性的“无操作”指令的模块，例如用于填充目的、在利用期间在内存中滑动等。用来在攻击载荷中添加空指令区，以提高攻击可靠性的组件。

是一些对程序运行状态不会造成任何实质影响的空操作或无关操作指令。

在渗透攻击构造恶意数据缓冲区时，常常要在真正要执行Shellcode时，有一个较大的安全着陆区，从而避免受到内存地址随机化、返回地址计算偏差等原因造成的Shellcode执行失败，从而提高渗透攻击的可靠性。

- 编码器模块（**Encoders**）

用于有效负载编码和加密的模块，例如 `base64`、`XOR`、`shikata_ga_nai` 等。这有助于混淆以规避防病毒或 `NIDS`（网络入侵检测系统）、`EDR`（端点检测和响应）等防御。

- 规避模块（**Evasions**）

用于规避防御的模块，例如防病毒规避、`AppLocker` 绕过、软件限制策略 (SRP) 绕过等。

1.4 MSF辅助扫描模块 - auxiliary

1.4.1 MSF主机发现

- 模块路径

> `modules/auxiliary/scanner/discovery/`

- 搜索模块

```
msf6 > search aux /scanner/discovery

Matching Modules
================

   #  Name                                                Disclosure Date  Rank    Check  Description
   -  ----                                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/discovery/arp_sweep                                normal  No     ARP Sweep Local Network Discovery
   1  auxiliary/scanner/discovery/ipv6_multicast_ping                      normal  No     IPv6 Link Local/Node Local Ping Discovery
   2  auxiliary/scanner/discovery/ipv6_neighbor                            normal  No     IPv6 Local Neighbor Discovery
   3  auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement       normal  No     IPv6 Local Neighbor Discovery Using Router Advertisement
```

```
   4  auxiliary/scanner/discovery/empty_udp
                                        normal  No
UDP Empty Prober
   5  auxiliary/scanner/discovery/udp_probe
                                        normal  No
UDP Service Prober
   6  auxiliary/scanner/discovery/udp_sweep
                                        normal  No
UDP Service Sweeper
```

arp_sweep：使用arp请求枚举本地局域网中的所有活跃主机

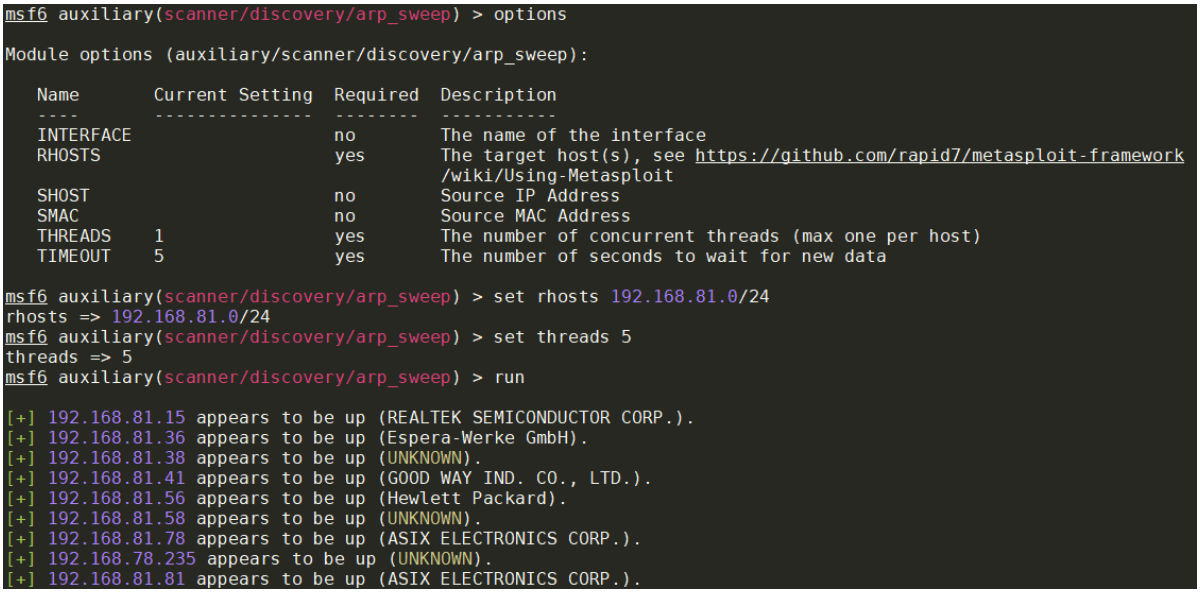
udp_sweep：通过发送UDP数据包探查指定主机是否活跃，并发现主机上的udp服务。

- 模块使用

> `arp_sweep`模块使用方法

```
use auxiliary/scanner/discovery/arp_sweep
set RHOSTS 10.10.10.0/24
set THREADS 50
run
```

> 设置好参数后输入`run`启动扫描器



1.4.2 MSF端口扫描

- 模块路径

> modules/auxiliary/scanner/portscan/

- 模块搜索

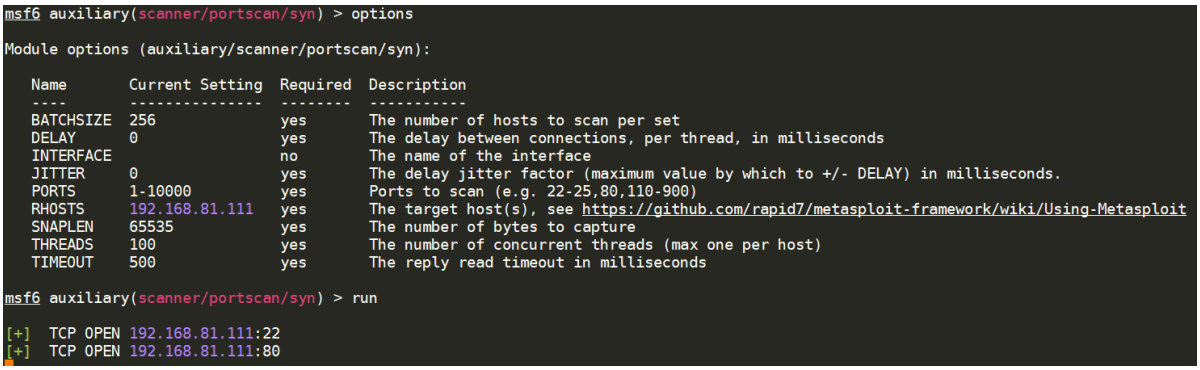
> search scanner/portscan

```
auxiliary/scanner/protscan/ack
//通过ACK扫描的方式对防火墙上未被屏蔽的端口进行探测

auxiliary/scanner/protscan/ftpbounce
//通过FTP bounce攻击的原理对TCP服务进行枚举，一些新的FTP服务器软件能很好的防范此攻击，但在旧的系统上仍可以被利用

auxiliary/scanner/protscan/syn
//使用发送TCP SYN标志的方式探测开放端口

auxiliary/scanner/protscan/tcp
//通过一次完整的TCP连接来判断端口是否开放 最准确但是最慢

auxiliary/scanner/protscan/xmas
//一种更为隐秘的扫描方式，通过发送FIN，PSH，URG标志，能够躲避一些高级的TCP标记检测器的过滤
```

一般情况下推荐使用`syn`端口扫描器，速度较快，结果准确，不易被对方察觉

- 模块使用

```
use auxiliary/scanner/protscan/syn
set RHOSTS 10.10.10.10
set THREADS 20
run
```



1.5 Meterpreter扩展模块

1.5.1 meterpreter简介

`Meterpreter` 是一个高级、动态、可扩展的`payload`，简单理解是一个高级的`CMD`，里面封装了`Metasploit`的功能

`Meterpreter`是`Metasploit`框架中的一个扩展模块，作为溢出成功以后的攻击载荷使用，攻击载荷在溢出攻击成功以后给我们返回一个控制通道。使用它作为攻击载荷能够获得目标系统的一个`Meterpreter shell`的链接。

`Meterpreter shell` 作为渗透模块有很多有用的功能，比如添加一个用户、隐藏一些东西、打开shell、得到用户密码、上传下载远程主机的文件、运行cmd.exe、捕捉屏幕、得到远程控制权、捕获按键信息、清除应用程序、显示远程主机的系统信息、显示远程机器的网络接口和IP地址等信息。

1.5.2 meterpreter 特点

`Metasploit`提供了各个主流平台的`Meterpreter`版本，包括`Windows、Linux`，同时支持`x86、x64`平台，另外，`Meterpreter`还提供了基于`PHP`和`Java`语言的实现。`Meterpreter`的工作模式是纯内存的，好处是启动隐藏，很难被杀毒软件监测到。不需要访问目标主机磁盘，所以也没什么入侵的痕迹。除上述外，`Meterpreter`还支持`Ruby`脚本形式的扩展。

1.5.3 进入meterpreter

```
background：将当前session挂起
sessions -l：列出当前所有的session
sessions -i id：进入某个session
```

- 常用命令

```
background #放回后台
exit #关闭会话
help #帮助信息
sysinfo #系统平台信息
screenshot #屏幕截取
shell #命令行shell (exit退出)
getlwd #查看本地目录
lcd #切换本地目录
getwd #查看目录
ls #查看文件目录列表
cd #切换目录
rm #删除文件
download C:\\1.txt 1.txt #下载文件
upload /var/www/wce.exe wce.exe #上传 文件
search -d c: -f *.doc #搜索文件
execute -f cmd.exe -i #执行程序/命令
ps #查看进程
getuid #查看当前用户权限
run killav #关闭杀毒软件
run getgui-e #启用远程桌面
```

1.5.4 meterpreter常用shell

1.5.4.1 reverse_tcp

> 基于TCP的反弹shell

```
linux/x86/meterpreter/reverse_tcp

windows/meterpreter/reverse_tcp
```

1.5.4.2 bind_tcp

> 基于TCP的正向连接shell，因为在内网跨网段时无法连接到攻击者的机器，所以在内网中经常会使用，不需要设置LHOST

```
linux/x86/meterpreter/bind_tcp
```

1.5.4.3 reverse_http

> 基于http方式的反向连接，在网速慢的情况下不稳定。

```
windows/meterpreter/reverse_http
```

1.5.4.4 reverse_https

> 基于https方式的反向连接，在网速慢的情况下不稳定。

```
windows/meterpreter/reverse_https
```

1.5.5 meterpreter命令详解

1.5.5.1 核心命令

```
?             - 帮助菜单
background    - 将当前会话移动到后台
bg            - background的别名
bgkill        - 总之后台 meterpreter 脚本
bglist        - 列出后台运行中的脚本
bgrun         - 作为一个后台线程运行脚本
channel       - 显示活动频道
close         - 关闭通道
disable_unicode_encoding     - 禁用unicode字符串的编码
```

```
enable_unicode_encoding     - 启用unicode字符串的编码
exit         - 终止 meterpreter 会话
help         - 帮助菜单
info         - 显示有关Post模块的信息
irb          - 在当前会话上打开交互式 Ruby 外壳
load         - 加载一个或多个meterpreter扩展
machine_id   - 获取连接到会话的计算机的 MSF ID
migrate      - 将服务迁移到另一个进程
pivot        - 管理pivot侦听器
pry          - 打开当前会话上的pry调试器
quit         - 终止 meterpreter 会话
read         - 从通道中读取数据
resource     - 运行存储在文件中的命令
run          - 执行一个meterpreter 脚本 或者 Post模块
secure       - 在会话中协商TLV分组加密
sessions     - 快速切换到另外一个session
set_timeouts - 设置当前会话的超时值
sleep        - 强制meterpreter停止活动，然后重新建立会话
transport    - 改变目前的运输机制.
use          - 加载 meterpreter 的扩展，'load'的旧别名
uuid         -  获取当前会话的UUID
write        - 将数据写入到一个通道
```

1.5.5.2 文件系统命令

```
cat          - 读取并输出到标准输出文件的内容
cd           - 更改目录对受害人
checksum     - 检索文件的校验和
cp           - 将源复制到目标
dir          - 列出文件（别名为 ls）
download     - 下载文件或目录
edit         - 编辑文件
getlwd       - 输出本地工作目录
getwd        - 输出工作目录
lcd          - 更改本地工作目录
lls          - 列出本地文件
```

```
lpwd          - 输出本地工作目录
ls            - 列出当前目录中的文件列表
mkdir         - 创建目录
mv            - 将源移动到目标
rm            - 删除指定的文件
rmdir         - 删除目录
search        - 在目标主机文件系统上查找搜索文件 例如：search
-d  c:\\  -f  *.doc  在目标主机C盘下搜索doc文档
show_mount    - 列出所有装载点/逻辑驱动器
upload        - 上传文件或目录
```

1.5.5.3 网络命令

```
arp           - 显示主机ARP缓存
getproxy      - 显示当前代理配置
ifconfig      - 显示网络接口的关键信息
ipconfig      - 显示网络接口的关键信息
netstat       - 显示网络连接
portfwd       - 将本地端口转发到远程服务
                例如：portfwd  add -l  1122 -p 3389 -r
192.168.250.176把目标主机192.168.250.176的3389端口转发到
1122端口
resolve       - 解析目标上的一组主机名
route         - 查看或加入受害者路由表  route add 5.5.5.0
255.255.255.0 1 用sessions 1会话加入指定网段
```

1.5.5.4 系统命令

```
clearev       - 清除事件日志
drop_token    - 放弃任何活动模拟令牌。
execute       - 执行命令，在目标主机上运行某个程序 execute -
f notepad.exe ，执行目标主机上的记事本程序，隐藏后台执行，加
参数-H
getenv        - 获取一个或多个环境变量值
getpid        - 获取当前进程 ID (PID)
getprivs      - 尝试启用当前进程可用的所有权限
```

```
getsid        - 获取当前运行服务用户的SID
getuid        - 获取当前运行服务的用户
kill          - 终止进程
localtime     - 显示目标系统的本地日期和时间
pgrep         - 按名称显示进程
pkill         - 按名称终止进程
ps            - 列出正在运行的进程
reboot        - 重新启动受害人的计算机
reg           - 与受害人的注册表进行交互
rev2self      - 在受害者机器上调用 RevertToSelf()
shell         - 在远程计算机上打开一个shell
shutdown      - 关闭远程计算机
steal_token   - 试图窃取指定的 (PID) 进程的令牌
suspend       - 挂起或恢复进程列表
sysinfo       - 获取关于远程系统的信息，如操作系统
```

1.5.5.5 用户界面命令

```
enumdesktops     - 列出所有可访问的desktops和Windows
getdesktop       - 获取当前的 meterpreter 桌面
idletime         - 检查长时间以来，受害者系统空闲进程
keyboard_send    - 发送一个键盘记录器
keyevent         - 发送key事件
keyscan_dump     - 转储键盘记录器缓冲区内容
keyscan_start    - 启动键盘记录器
keyscan_stop     - 停止键盘记录器
mouse            - 发送鼠标事件
screenshare      - 实时监视远程用户的桌面
screenshot       - 抓取交互式桌面的屏幕截图
setdesktop       - 更改 meterpreter 当前桌面
uictl            - 启用用户界面组件的一些控件
```

1.5.5.6 摄像头命令

```
record_mic       - 从默认麦克风记录音频X秒
webcam_chat      - 启动视频聊天
webcam_list      - 列出摄像头
webcam_snap      - 从指定的网络摄像头获取snapshot
webcam_stream    - 从指定的网络摄像头播放视频流
```

1.5.5.7 音频输出命令

```
play     - 在目标系统上播放波形音频文件(.wav)
```

1.5.5.8 提权命令

```
getsystem    - 获得系统管理员权限
```

1.5.5.9 密码转储命令

```
hashdump     - 抓取哈希密码 (SAM) 文件中的值

hashdump 可以跳过杀毒软件，但现在有两个脚本，都更加隐蔽，”run hashdump”和”run smart_hashdump”。
```

1.5.5.10 Timestomp

```
timestomp    - 操作修改文件的MACE属性

Modified：修改时间
Accessed：访问时间
Created：创建时间
Entry Modified：  条目修改时间
```