nmap

- 基本功能
  - 常见参数：
    - TCP全连接扫描
    - SYN半链接扫描
    - 隐蔽扫描(Null扫描,标识位全为0)
    - Xmax扫描
    - Fin扫描
    - 显示端口服务信息
    - 操作系统类型
    - 保存扫描结果,txt/xml xpath
    - 全面扫描
    - 时序选项
    - 端口状态6种
    - 常见的端口服务
      - 21端口渗透剖析
      - 22端口渗透剖析
      - 23端口渗透剖析
      - 25/465端口渗透剖析
      - 53端口渗透剖析
      - 80端口渗透剖析
      - 135端口渗透剖析
      - 1433端口渗透剖析
      - 1521端口渗透剖析
      - 2049端口渗透剖析
      - 3306端口渗透剖析
      - 3389端口渗透剖析
      - 4899端口渗透剖析
      - 5432端口渗透剖析
      - 5631端口渗透剖析
      - 5900端口渗透剖析
      - 6379端口渗透剖析
      - 7001/7002端口渗透剖析
      - 8080端口渗透剖析
      - 27017端口渗透剖析
  - 漏洞扫描：

常见脚本参数：

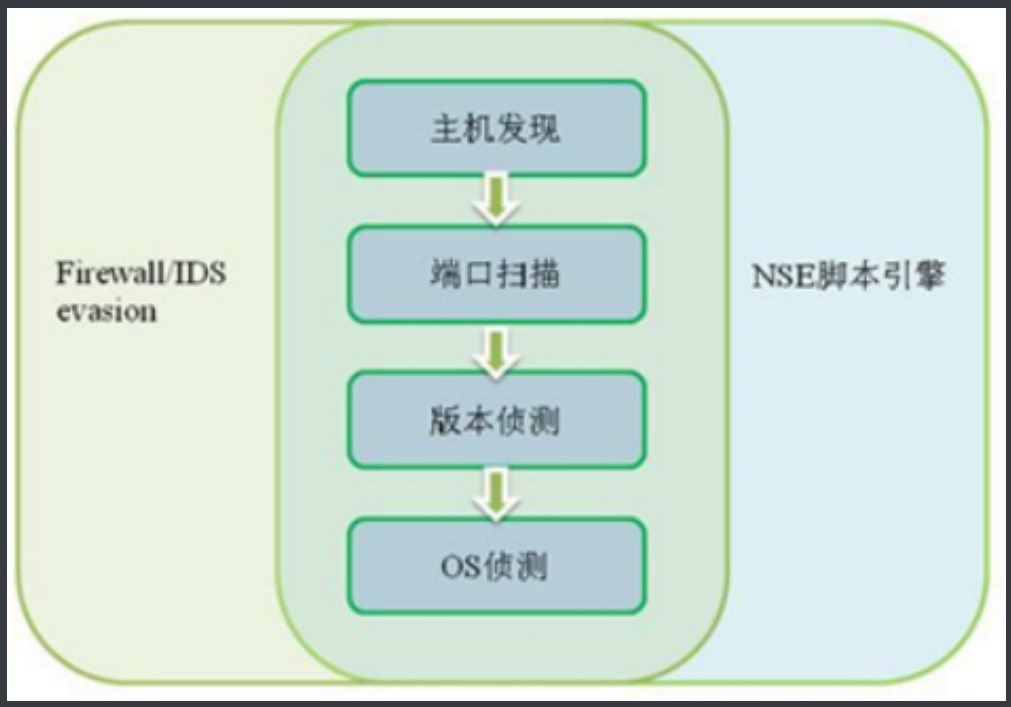
nmap

Nmap，也就是Network Mapper，中文为“网络映射器”。Nmap是一款开源的网络探测和安全审核的工具，它的设计目标是快速地扫描大型网络。它是网络管理员必用的软件之一，以及用以评估网络系统保安。

基本功能

1. 探测一组主机是否在线
2. 扫描主机端口，嗅探所提供的网络服务
3. 推断主机所用的操作系统

Nmap对目标主机进行一系列的测试，利用测试结果建立相应目标主机的Nmap指纹，然后Nmap会对指纹进行匹配，最终输出相应的结果。



测试	描述
T1	发送 TCP 数据包（Flag=SYN）到开放 TCP 端口
T2	发送一个空的 TCP 数据包到开放的 TCP 端口
T3	发送 TCP 数据包（Flag=SYN,URG,PSH,FIN）到开放的 TCP 端口
T4	发送 TCP 数据包（Flag=ACK）到开放的 TCP 端口
T5	发送 TCP 数据包（Flag=SYN）到关闭的 TCP 端口
T6	发送 TCP 数据包（Flag=ACK）到关闭的 TCP 端口
T7	发送 TCP 数据包（Flag=URG,PSH,FIN）到关闭的 TCP 端口

没有指定任何参数的情况下，默认扫描top 1000端口

常见参数：

`-sP /-sn` 不进行端口扫描
`-p` 指定端口

```
-p 80
-p 1-65535=-p-
-p 80,8080
```

TCP全连接扫描

建立完整的三次握手

`-sT`

wireshark分析：

```
ip.addr == ip and tcp.port == 80
```

SYN半链接扫描

只进行三次握手的前两次

`-sS`

隐蔽扫描(Null扫描,标识位全为0)

`-sN`

Xmax扫描

`-sX`

Fin扫描

`-sF`

显示端口服务信息

`-sV`

操作系统类型

`-O`

保存扫描结果,txt/xml xpath

`-oN/-oX`

全面扫描

`-A`

时序选项

`-T0~T5`

端口状态6种

```
SYN(synchronous建立联机)
ACK(acknowledgement 确认)
PSH(push传送)
FIN(finish结束)
RST(reset重置)
URG(urgent紧急)
```

- open：目标端口开启。
- closed：目标端口关闭。
- filtered：通常被防火墙拦截，无法判断目标端口开启与否。
- unfiltered：目标端口可以访问，但无法判断开启与否。
- open | filtered：无法确定端口是开启还是filtered。
- closed | filtered：无法确定端口是关闭还是filtered。

`Open`：端口处于开放状态，例如：当nmap使用TCP SYN对目标主机某一范围的端口进行扫描时，我们知道 TCP SYN报文是TCP建立连接的第一步，所以，如果目标主机返回 `SYN+ACK` 的报文，我们就认为此端口开放了并且使用了TCP服务。

`Closed`：端口处于关闭状态。例如：TCP SYN类型的扫描，如果返回RST类型的报文，则端口处于管理状态。这里我们值得注意的是关闭的端口也是可访问的，只是没有上层的服务在监听这个端口，而且，只是在我们扫描的这个时刻为关闭，当我们在另一个时间段进行扫描的时候，这些关闭的端口可能会处于open的状态。

`Filtered（过滤的）`：由于报文无法到达指定的端口，nmap不能够决定端口的开放状态，这主要是由于网络或者主机安装了一些防火墙所导致的。当nmap收到icmp报文主机不可达报文（例如：type为3，code为13（communication administratively prohibit）报文）或者目标主机无应答，常常会将目标主机的状态设置为filtered。

`Unfiltered（未被过滤的）`：当nmap不能确定端口是否开放的时候所打上的状态，这种状态和filtered的区别在于：unfiltered的端口能被nmap访问，但是nmap根据返回的报文无法确定端口的开放状态，而filtered的端口直接就没就没能够被nmap访问。端口被定义为Unfilterd只会发生在TCP ack扫描类型时当返回RST的报文。而端口被定义为filtered 状态的原因是是报文被防火墙设备，路由器规则，或者防火墙软件拦截，无法送达到端口，这通常表现为发送NMAP的主机收到ICMP报错报文，如：TYPE为3，code为13的报文（通信被认为的禁止 `communication administratively prohibited`），或者主机通过多次重复发送没有收到任何回应）。

`Open|filtered状态`： 这种状态主要是nmap无法区别端口处于open状态还是filtered状态。这种状态只会出现在open端口对报文不做回应的扫描类型中，如：udp，ip protocol ，TCP null，fin，和xmas扫描类型。

`Closed|filtered状态`： 这种状态主要出现在nmap无法区分端口处于closed还是filtered时。此状态只会出现在IP ID idle scan中。

常见的端口服务

端口扫描工具有nmap和masscan。nmap扫描的准确性较高，但是扫描的比较慢。masscan扫描的比较快，但是准确性较低。

端口	服务	入侵方式
21	ftp/tftp/vsftpd文件传输协议	爆破/嗅探/溢出/后门
22	ssh远程连接	爆破/openssh漏洞
23	Telnet远程连接	爆破/嗅探/弱口令
25	SMTP邮件服务	邮件伪造
53	DNS域名解析系统	域传送/劫持/缓存投毒/欺骗
67/68	dhcp服务	劫持/欺骗
110	pop3	爆破/嗅探
139	Samba服务	爆破/未授权访问/远程命令执行
143	Imap协议	爆破
161	SNMP协议	爆破/搜集目标内网信息
389	Ldap目录访问协议	注入/未授权访问/弱口令
445	smb	ms17-010/端口溢出
512/513/514	Linux Rexec服务	爆破/Rlogin登陆
873	Rsync服务	文件上传/未授权访问
1080	socket	爆破
1352	Lotus domino邮件服务	爆破/信息泄漏

1433	mssql	爆破/注入/SA弱口令
1521	oracle	爆破/注入/TNS爆破/反弹shell
2049	Nfs服务	配置不当
2181	zookeeper服务	未授权访问
2375	docker remote api	未授权访问
3306	mysql	爆破/注入
3389	Rdp远程桌面链接	爆破/shift后门
4848	GlassFish控制台	爆破/认证绕过
5000	sybase/DB2数据库	爆破/注入/提权
5432	postgresql	爆破/注入/缓冲区溢出
5632	pcanywhere服务	抓密码/代码执行
5900	vnc	爆破/认证绕过
6379	Redis数据库	未授权访问/爆破
7001/7002	weblogic	java反序列化/控制台弱口令
80/443	http/https	web应用漏洞/心脏滴血
8069	zabbix服务	远程命令执行/注入
8161	activemq	弱口令/写文件
8080/8089	Jboss/Tomcat/Resin	爆破/PUT文件上传/反序列化
8083/8086	influxDB	未授权访问
9000	fastcgi	远程命令执行
9090	Websphere控制台	爆破/java反序列化/弱口令
9200/9300	elasticsearch	远程代码执行
11211	memcached	未授权访问
27017/27018	mongodb	未授权访问/爆破

21端口渗透剖析

FTP通常用作对远程服务器进行管理，典型应用就是对web系统进行管理。一旦FTP密码泄露就直接威胁web系统安全，甚至黑客通过提权可以直接控制服务器。这里剖析渗透FTP服务器的几种方法。

1. 基础爆破：ftp爆破工具很多，这里我推owasp的Bruter,hydra以及msf中的ftp爆破模块。
2. **ftp匿名访问：用户名：anonymous 密码：为空或者任意邮箱**
3. 后门vsftpd： version 2到2.3.4存在后门漏洞，攻击者可以通过该漏洞获取root权限。（https://www.freebuf.com/column/143480.html）
4. 嗅探：ftp使用明文传输技术（但是嗅探给予局域网并需要欺骗或监听网关）,使用Cain进行渗透。
5. ftp远程代码溢出。（https://blog.csdn.net/weixin_42214273/article/details/82892282）
6. ftp跳转攻击。（https://blog.csdn.net/mgxcool/article/details/48249473）

22端口渗透剖析

SSH 是协议，通常使用 OpenSSH 软件实现协议应用。SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其它网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

1. **弱口令**，可使用工具hydra，msf中的ssh爆破模块。
2. 防火墙SSH后门。（https://www.secpulse.com/archives/69093.html）
3. 28退格 OpenSSL
4. openssh 用户枚举 CVE-2018-15473。（https://www.anquanke.com/post/id/157607）

23端口渗透剖析

telnet是一种旧的远程管理方式，使用telnet工具登录系统过程中，网络上传输的用户和密码都是以明文方式传送的，黑客可使用嗅探技术截获到此类密码。

1. **暴力破解技术是常用的技术**，使用hydra,或者msf中telnet模块对其进行破解。
2. 在linux系统中一般采用SSH进行远程访问，传输的敏感数据都是经过加密的。而对于windows下的telnet来说是脆弱的，因为默认没有经过任何加密就在网络中进行传输。使用cain等嗅探工具可轻松截获远程登录密码。

25/465端口渗透剖析

smtp：邮件协议，在linux中默认开启这个服务，可以向对方发送钓鱼邮件

默认端口：25（smtp）、465（smtps）

1. 爆破：弱口令
2. 未授权访问

53端口渗透剖析

53端口是DNS域名服务器的通信端口，通常用于域名解析。也是网络中非常关键的服务器之一。这类服务器容易受到攻击。对于此端口的渗透，一般有三种方式。

1. 使用DNS远程溢出漏洞直接对其主机进行溢出攻击，成功后可直接获得系统权限。（https://www.seebug.org/vuldb/ssvid-96718）
2. 使用DNS欺骗攻击，可对DNS域名服务器进行欺骗，如果黑客再配合网页木马进行挂马攻击，无疑是一种杀伤力很强的攻击，黑客可不费吹灰之力就控制内网的大部分主机。这也是内网渗透惯用的技法之一。（https://baijiahao.baidu.com/s?id=1577362432987749706&wfr=spider&for=pc）
3. 拒绝服务攻击，利用拒绝服务攻击可快速的导致目标服务器运行缓慢，甚至网络瘫痪。如果使用拒绝服务攻击其DNS服务器。将导致用该服务器进行域名解析的用户无法正常上网。（http://www.edu.cn/xxh/fei/zxz/201503/t20150305_1235269.shtml）
4. DNS劫持。（https://blog.csdn.net/qq_32447301/article/details/77542474）

80端口渗透剖析

80端口通常提供web服务。目前黑客对80端口的攻击典型是采用SQL注入的攻击方法，脚本渗透技术也是一项综合性极高的web渗透技术，同时脚本渗透技术对80端口也构成严重的威胁。

1. 对于windows2000的IIS5.0版本，黑客使用远程溢出直接对远程主机进行溢出攻击，成功后直接获得系统权限。
2. 对于windows2000中IIS5.0版本，黑客也尝试利用‘Microsoft IISCGI’文件名错误解码漏洞攻击。使用X-SCAN可直接探测到IIS漏洞。
3. IIS写权限漏洞是由于IIS配置不当造成的安全问题，攻击者可向存在此类漏洞的服务器上传恶意代码，比如上传脚本木马扩大控制权限。

4. 普通的http封包是没有经过加密就在网络中传输的，这样就可通过嗅探类工具截取到敏感的数据。如使用Cain工具完成此类渗透。
5. 80端口的攻击，更多的是采用脚本渗透技术，利用web应用程序的漏洞进行渗透是目前很流行的攻击方式。
6. 对于渗透只开放80端口的服务器来说，难度很大。利用端口复用工具可解决此类技术难题。
7. CC攻击效果不及DDOS效果明显，但是对于攻击一些小型web站点还是比较有用的。CC攻击可使目标站点运行缓慢，页面无法打开，有时还会爆出web程序的绝对路径。

135端口渗透剖析

135端口主要用于使用RPC协议并提供DCOM服务，通过RPC可以保证在一台计算机上运行的程序可以顺利地执行远程计算机上的代码；使用DCOM可以通过网络直接进行通信，能够跨包括HTTP协议在内的多种网络传输。同时这个端口也爆出过不少漏洞，最严重的就是缓冲区溢出漏洞，曾经疯狂一时的‘冲击波’病毒就是利用这个漏洞进行传播的。对于135端口的渗透，黑客的渗透方法为:

1. 查找存在RPC溢出的主机，进行远程溢出攻击，直接获得系统权限。如用‘DSScan’扫描存在此漏洞的主机。对存在漏洞的主机可使用‘ms05011.exe’进行溢出，溢出成功后获得系统权限。（https://wenku.baidu.com/view/68b3340c79563c1ec5da710a.html）
2. 扫描存在弱口令的135主机，利用RPC远程过程调用开启telnet服务并登录telnet执行系统命令。系统弱口令的扫描一般使用hydra。对于telnet服务的开启可使用工具kali链接。（https://wenku.baidu.com/view/c8b96ae2700abb68a982fbdf.html）

139/445端口渗透剖析
139端口是为‘NetBIOS SessionService’提供的，主要用于提供windows文件和打印机共享以及UNIX中的Samba服务。445端口也用于提供windows文件和打印机共享，在内网环境中使用的很广泛。这两个端口同样属于重点攻击对象，139/445端口曾出现过许多严重级别的漏洞。下面剖析渗透此类端口的基本思路。

1. 对于开放139/445端口的主机，一般尝试利用溢出漏洞对远程主机进行溢出攻击，成功后直接获得系统权限。利用msf的ms-017永恒之蓝。（https://blog.csdn.net/qq_41880069/article/details/82908131）
2. 对于攻击只开放445端口的主机，黑客一般使用工具‘MS06040’或‘MS08067’.可使用专用的445端口扫描器进行扫描。NS08067溢出工具对windows2003系统的溢出十分有效，工具基本使用参数在cmd下会有提示。（https://blog.csdn.net/god_7z1/article/details/6773652）

3. 对于开放139/445端口的主机，黑客一般使用IPC$进行渗透。在没有使用特点的账户和密码进行空连接时，权限是最小的。获得系统特定账户和密码成为提升权限的关键了，比如获得administrator账户的口令。（https://blog.warhut.cn/dmbj/145.html）
4. 对于开放139/445端口的主机，可利用共享获取敏感信息，这也是内网渗透中收集信息的基本途径。

1433端口渗透剖析

1433是SQLServer默认的端口，SQL Server服务使用两个端口：tcp-1433、UDP-1434.其中1433用于供SQLServer对外提供服务，1434用于向请求者返回SQLServer使用了哪些TCP/IP端口。1433端口通常遭到黑客的攻击，而且攻击的方式层出不穷。最严重的莫过于远程溢出漏洞了，如由于SQL注射攻击的兴起，各类数据库时刻面临着安全威胁。利用SQL注射技术对数据库进行渗透是目前比较流行的攻击方式，此类技术属于脚本渗透技术。

1. 对于开放1433端口的SQL Server2000的数据库服务器，黑客尝试使用远程溢出漏洞对主机进行溢出测试，成功后直接获得系统权限。（https://blog.csdn.net/gxj022/article/details/4593015）
2. 暴力破解技术是一项经典的技术。**一般破解的对象都是SA用户**。通过字典破解的方式很快破解出SA的密码。（https://blog.csdn.net/kali_linux/article/details/50499576）
3. 嗅探技术同样能嗅探到SQL Server的登录密码。
4. 由于脚本程序编写的不严密，例如，程序员对参数过滤不严等，这都会造成严重的注射漏洞。通过SQL注射可间接性的对数据库服务器进行渗透，通过调用一些存储过程执行系统命令。可以使用SQL综合利用工具完成。

1521端口渗透剖析

1521是大型数据库Oracle的默认监听端口，估计新手还对此端口比较陌生，平时大家接触的比较多的是Access，MSSQL以及MYSQL这三种数据库。一般大型站点才会部署这种比较昂贵的数据库系统。对于渗透这种比较复杂的数据库系统，黑客的思路如下：

1. Oracle拥有非常多的默认用户名和密码，为了获得数据库系统的访问权限，破解数据库系统用户以及密码是黑客必须攻破的一道安全防线。
2. SQL注射同样对Oracle十分有效，通过注射可获得数据库的敏感信息，包括管理员密码等。
3. 在注入点直接创建java，执行系统命令。https://www.leiphone.com/news/201711/JjzXFp46zEPMvJod.html

2049端口渗透剖析

NFS（Network File System）即网络文件系统，是FreeBSD支持的文件系统中的一种，它允许网络中的计算机之间通过TCP/IP网络共享资源。在NFS的应用中，本地NFS的客户端应用可以透明地读写位于远端NFS服务器上的文件，就像访问本地文件一样。如今NFS具备了防止被利用导出文件夹的功能，但遗留系统中的NFS服务配置不当，则仍可能遭到恶意攻击者的利用。

未授权访问。（https://www.freebuf.com/articles/network/159468.html）（http://www.secist.com/archives/6192.htm）

3306端口渗透剖析

3306是MYSQL数据库默认的监听端口，通常部署在中型web系统中。在国内LAMP的配置是非常流行的，对于php+mysql构架的攻击也是属于比较热门的话题。mysql数据库允许用户使用自定义函数功能，这使得黑客可编写恶意的自定义函数对服务器进行渗透，最后取得服务器最高权限。对于3306端口的渗透，黑客的方法如下:

1. 由于管理者安全意识淡薄，通常管理密码设置过于简单，甚至为空口令。使用破解软件很容易破解此类密码，利用破解的密码登录远程mysql数据库，上传构造的恶意UDF自定义函数代码进行注册，通过调用注册的恶意函数执行系统命令。或者向web目录导出恶意的脚本程序，以控制整个web系统。
2. 功能强大的‘cain’同样支持对3306端口的嗅探，同时嗅探也是渗透思路的一种。
3. SQL注入同样对mysql数据库威胁巨大，不仅可以获取数据库的敏感信息，还可使用load_file()函数读取系统的敏感配置文件或者从web数据库链接文件中获得root口令等，导出恶意代码到指定路径等。

3389端口渗透剖析

3389是windows远程桌面服务默认监听的端口，管理员通过远程桌面对服务器进行维护，这给管理工作带来的极大的方便。通常此端口也是黑客们较为感兴趣的端口之一，利用它可对远程服务器进行控制，而且不需要另外安装额外的软件，实现方法比较简单。当然这也是系统合法的服务，通常是不会被杀毒软件所查杀的。使用‘输入法漏洞’进行渗透。

1. 对于windows2000的旧系统版本，使用‘输入法漏洞’进行渗透。
2. cain是一款超级的渗透工具，同样支持对3389端口的嗅探。
3. Shift粘滞键后门：5次shift后门

4. 社会工程学通常是最可怕的攻击技术，如果管理者的一切习惯和规律被黑客摸透的话，那么他管理的网络系统会因为他的弱点被渗透。
5. 爆破3389端口。这里还是推荐使用hydra爆破工具。
6. ms12_020死亡蓝屏攻击。（https://www.cnblogs.com/R-Hacker/p/9178066.html
7. https://www.cnblogs.com/backlion/p/9429738.html

4899端口渗透剖析

4899端口是remoteadministrator远程控制软件默认监听的端口，也就是平时常说的radmini影子。radmini目前支持TCP/IP协议，应用十分广泛，在很多服务器上都会看到该款软件的影子。对于此软件的渗透，思路如下：

1. radmini同样存在不少弱口令的主机，通过专用扫描器可探测到此类存在漏洞的主机。
2. radmini远控的连接密码和端口都是写入到注册表系统中的，通过使用webshell注册表读取功能可读取radmini在注册表的各项键值内容，从而破解加密的密码散列。

5432端口渗透剖析

PostgreSQL是一种特性非常齐全的自由软件的对象–关系型数据库管理系统，可以说是目前世界上最先进，功能最强大的自由数据库管理系统。包括kali系统中msf也使用这个数据库；浅谈postgresql数据库攻击技术 大部分关于它的攻击依旧是sql注入，所以注入才是数据库不变的话题。

1. 爆破：弱口令：postgres postgres
2. 缓冲区溢出：CVE-2014-2669。（http://drops.xmd5.com/static/drops/tips-6449.html）
3. 远程代码执行：CVE-2018-1058。（https://www.secpulse.com/archives/69153.html）

5631端口渗透剖析

5631端口是著名远程控制软件pcanywhere的默认监听端口，同时也是世界领先的远程控制软件。利用此软件，用户可以有效管理计算机并快速解决技术支持问题。由于软件的设计缺陷，使得黑客可随意下载保存连接密码的*.cif文件，通过专用破解软件进行破解。这些操作都必须在拥有一定权限下才可完成，至少通过脚本渗透获得一个webshell。通常这些操作在黑客界被称为pcanywhere提权技术。

```
PcAnyWhere提权。（https://blog.csdn.net/Fly_hps/article/details/80377199）
```

5900端口渗透剖析

5900端口是优秀远程控制软件VNC的默认监听端口，此软件由著名的AT&T的欧洲研究实验室开发的。VNC是在基于unix和linux操作系统的免费的开放源码软件，远程控制能力强大，高效实用，其性能可以和windows和MAC中的任何一款控制软件媲美。对于该端口的渗透，思路如下：

1. VNC软件存在密码验证绕过漏洞，此高危漏洞可以使得恶意攻击者不需要密码就可以登录到一个远程系统。
2. cain同样支持对VNC的嗅探，同时支持端口修改。
3. VNC的配置信息同样被写入注册表系统中，其中包括连接的密码和端口。利用webshell的注册表读取功能进行读取加密算法，然后破解。
4. VNC拒绝服务攻击（CVE-2015-5239）。（http://blogs.360.cn/post/vnc%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1%E6%BC%8F%E6%B4%9Ecve-2015-5239%E5%88%86%E6%9E%90.html）
5. VNC权限提升（CVE-2013-6886）。

6379端口渗透剖析

Redis是一个开源的使用c语言写的，支持网络、可基于内存亦可持久化的日志型、key-value数据库。关于这个数据库这两年还是很火的，暴露出来的问题也很多。特别是前段时间暴露的未授权访问。

1. 爆破：弱口令
2. 未授权访问+配合ssh key提权。（http://www.alloyteam.com/2017/07/12910/）

7001/7002端口渗透剖析

7001/7002通常是weblogic中间件端口

1. 弱口令、爆破，弱密码一般为weblogic/Oracle@123 or weblogic
2. 管理后台部署 war 后门
3. SSRF
4. 反序列化漏洞
5. weblogic_uachttps://github.com/vulhub/vulhub/tree/master/weblogic/ssrfhttps://bbs.pediy.com/thread-224954.htmhttps://fuping.site/2017/06/05/Weblogic-Vulnerability-Verification/https://blog.gdssecurity.com/labs/2015/3/30/weblogic-ssrf-and-xss-cve-2014-42

41-cve-2014-4210-cve-2014-4.html

8080端口渗透剖析

8080端口通常是apache_Tomcat服务器默认监听端口，apache是世界使用排名第一的web服务器。国内很多大型系统都是使用apache服务器，对于这种大型服务器的渗透，主要有以下方法：

1. Tomcat远程代码执行漏洞（https://www.freebuf.com/column/159200.html）
2. Tomcat任意文件上传。（http://liehu.tass.com.cn/archives/836）
3. Tomcat远程代码执行&信息泄露。（https://paper.seebug.org/399/）
4. Jboss远程代码执行。（http://mobile.www.cnblogs.com/Safe3/archive/2010/01/08/1642371.html）
5. Jboss反序列化漏洞。（https://www.zybuluo.com/websec007/note/838374）
6. Jboss漏洞利用。（https://blog.csdn.net/u011215939/article/details/79141624）

27017端口渗透剖析

MongoDB，NoSQL数据库；攻击方法与其他数据库类似

1. 爆破：弱口令
2. 未授权访问；（http://www.cnblogs.com/LittleHann/p/6252421.html）（3）http://www.tiejiang.org/19157.htm

Nmap渗透测试指南

漏洞扫描：

排除指定ip扫描

```
┌──(root💀kali)-[/tmp]
└─# nmap 119.91.93.0/24 --exclude 119.91.93.173
```

nmap关于漏洞扫描的内容都是基于vuln的脚本，大多数的漏洞都是带有cve编号的。

漏洞脚本分类：

```
auth: 负责处理鉴权证书（绕开鉴权）的脚本

broadcast: 在局域网内探查更多服务开启状况，如dhcp/dns/sqlserver等服务

brute: 提供暴力破解方式，针对常见的应用如http/snmp等

default: 使用-sC或-A选项扫描时候默认的脚本，提供基本脚本扫描能力

discovery: 对网络进行更多的信息，如SMB枚举、SNMP查询等

dos: 用于进行拒绝服务攻击

exploit: 利用已知的漏洞入侵系统

external: 利用第三方的数据库或资源，例如进行whois解析

fuzzer: 模糊测试的脚本，发送异常的包到目标机，探测出潜在漏洞

intrusive: 入侵性的脚本，此类脚本可能引发对方的IDS/IPS的记录或屏蔽

malware: 探测目标机是否感染了病毒、开启了后门等信息

safe: 此类与intrusive相反，属于安全性脚本

version: 负责增强服务与版本扫描（Version Detection）功能的脚本

vuln: 负责检查目标机是否有常见的漏洞（Vulnerability），如是否有MS08_067
```

详细使用方法：

```
nmap --script=auth IP
//负责处理鉴权证书（绕开鉴权）的脚本,也可以作为检测部分应用弱口令


nmap --script=vuln 192.168.137.*
//检查是否存在常见漏洞

http-php-version //获得PHP版本信息 Http-enum 枚举Web站点目录 smtp-strangeport 判断SMTP是否运行在默认端口 dns-blacklist 发现IP地址黑名单brute 提供暴力破解的方式  可对数据库，smb，snmp等进行简单密码的暴力猜解

smb-check-vulns  //检测smb漏洞
samba-vuln-cve-2012-1182 //扫描Samba堆溢出漏洞
```

测试waf是否存在

```
nmap -p 80,443 --script=http-waf-detect 192.168.0.100
nmap -p 80,443 --script=http-waf-fingerprint www.baidu.com
```

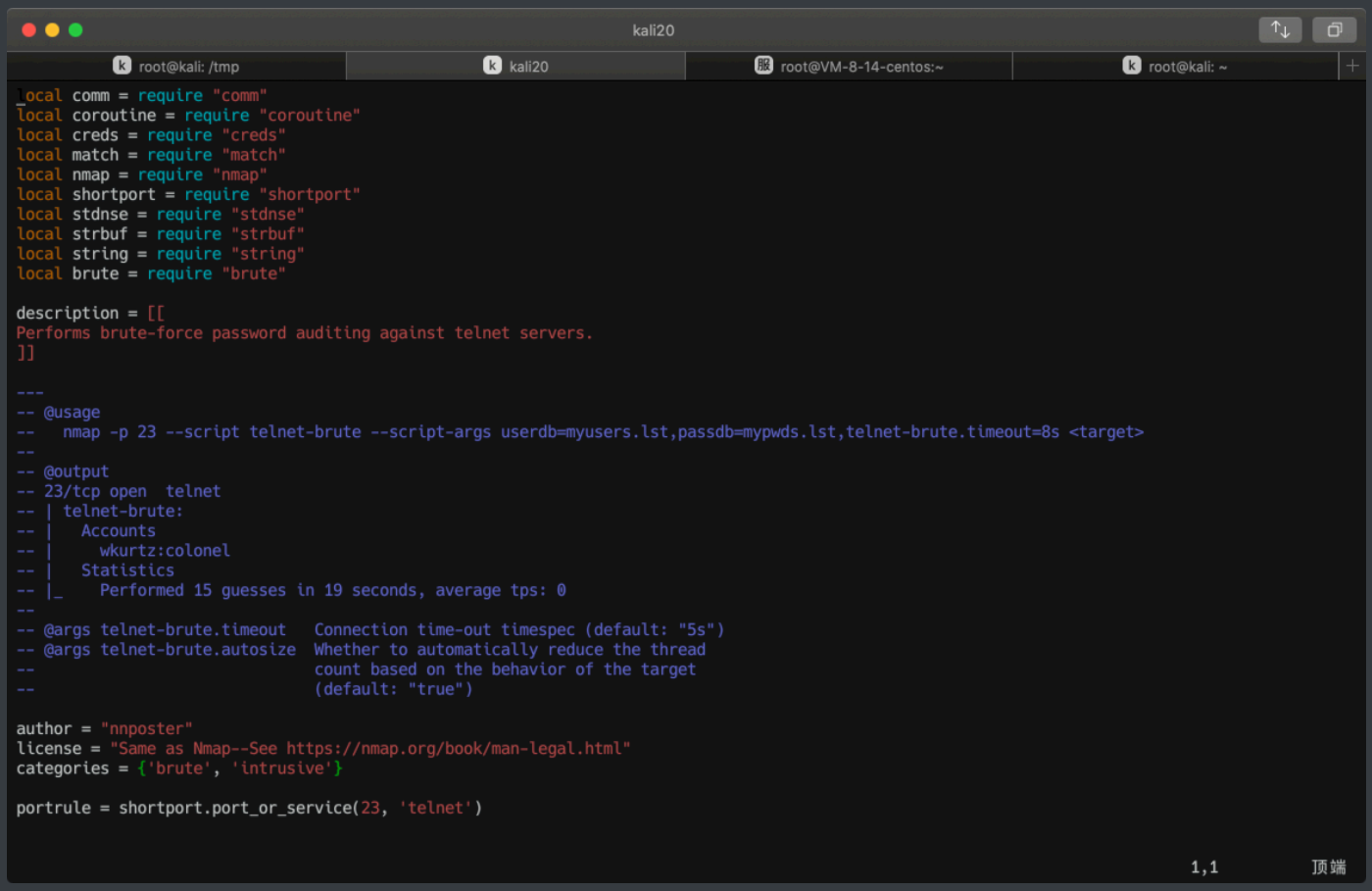
常见脚本参数：

```
-sC：等价于–script=default，使用默认类别的脚本进行扫描 可更换其他类别
–script=<Lua scripts>：<Lua scripts>使用某个或某类脚本进行扫描，支持通配符描述
–script-args=<n1=v1,[n2=v2,...]>：为脚本提供默认参数
–script-args-file=filename：使用文件来为脚本提供参数
–script-trace：显示脚本执行过程中发送与接收的数据
–script-updatedb：更新脚本数据库
–script-help=<scripts>：显示脚本的帮助信息，其中<scripts>部分可以逗号分隔的文件或脚本类别
```

案例：

```
nmap --script smb-brute --script-args
userdb=/var/passwd,passdb=/var/passwd 192.168.137.4
```

其他脚本具体使用参考(具体脚本的usage):



ssh端口爆破

```
┌─hazel@hazeldeMBP ~
└─$ nmap -p22 --script ssh-brute 150.158.27.164
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-22 13:41 CST
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
.....
Nmap scan report for 150.158.27.164
Host is up (0.024s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 1847 guesses in 602 seconds, average tps: 3.2
```

```
Nmap done: 1 IP address (1 host up) scanned in 601.77 seconds
```

ftp端口爆破

```
┌─hazel@hazeldeMBP ~
└─$ nmap -p21 --script ssh-brute 150.158.27.164

指定账号密码进行爆破:
nmap -p21 192.168.60.50 --script ftp-brute --script-args
userdb=/root/user.txt,passdb=/root/pass.txt
```

mysql
Nmap也可对MySQL服务（通常开放在端口3306上）进行扫描爆破，脚本mysql-info将探测出一些MySQ服务的详细信息(需要带上命令参数-sV -sC):

```
nmap -p3306 -sV -sC site.test.lan
nmap -p3306 --script mysql-enum site.test.lan

┌─hazel@hazeldeMBP ~
└─$ nmap -p3306 --script mysql-enum 49.232.193.10
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-22 14:10 CST
Nmap scan report for 49.232.193.10
Host is up (0.026s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
```

```
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
```