**第十九章 安装Kali黑客操作系统-利用ettercap实施中间人攻击**

**本节所讲内容：**

**19.1 安装Kali黑客操作系统及相关实战**

**19.2 实战：linux之kali系统ssh服务开启**

**19.3 实战： kali下的nmap扫描工具**

**19.4 MITM中间人攻击理论**

**19.5 实战：使用 Ettercap 工具实现中间人攻击**

**Kali或BT 听过：1 没听过：6**

**19.1 Kali概述：**

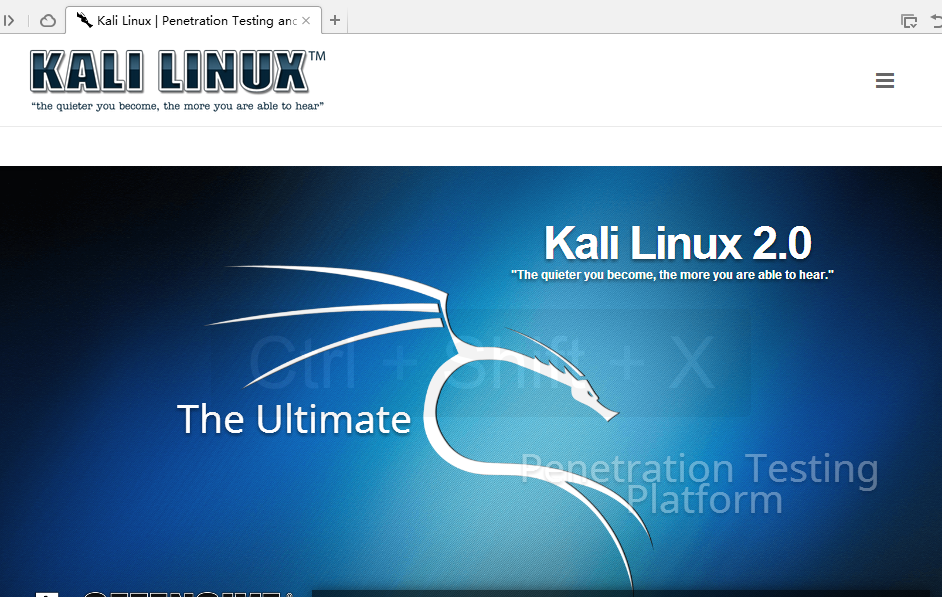
**Kali 一为linux操作系统的一个发行版。**

**Kali Linux 前身是 [BackTrack](http://baike.baidu.com/view/1627379.htm" \t "_blank)（基于ubuntu），是一个基于 Debian 的 Linux 发行版，包含很多安全和取证方面的相关工具。支持ARM架构。**

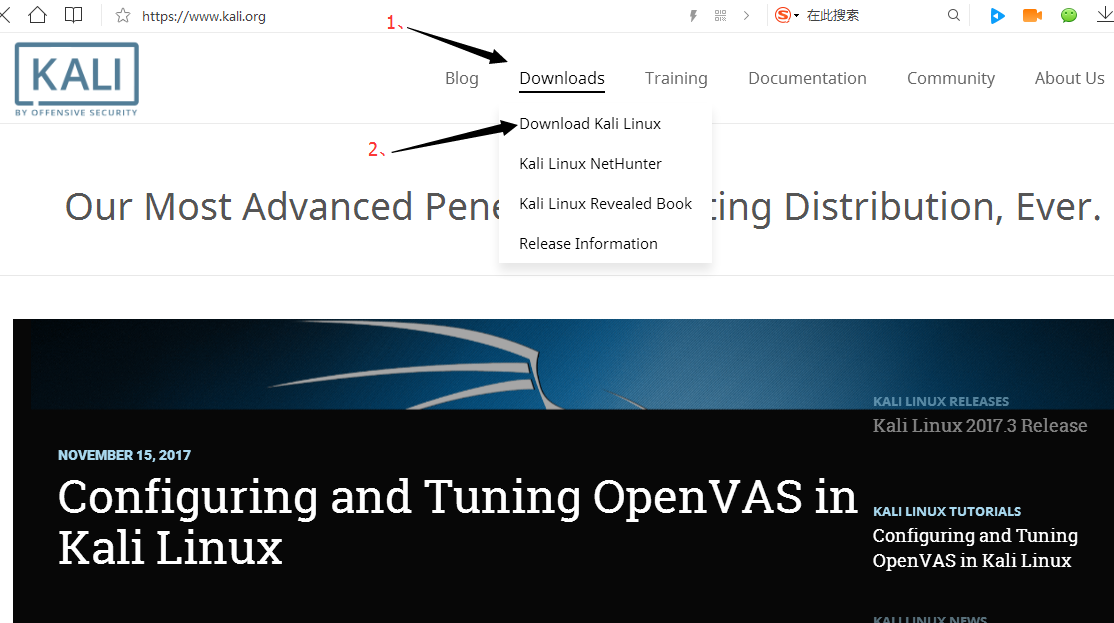
**手机的CPU ：ARM架构。 PC或PC服务器： x86 \_i686(32位CPU)，x86\_64(64位CPU)**

**Kali官方网站：**

**https://www.kali.org/**

****

**19.1.1 下载镜像：**



**https://www.kali.org/downloads/**



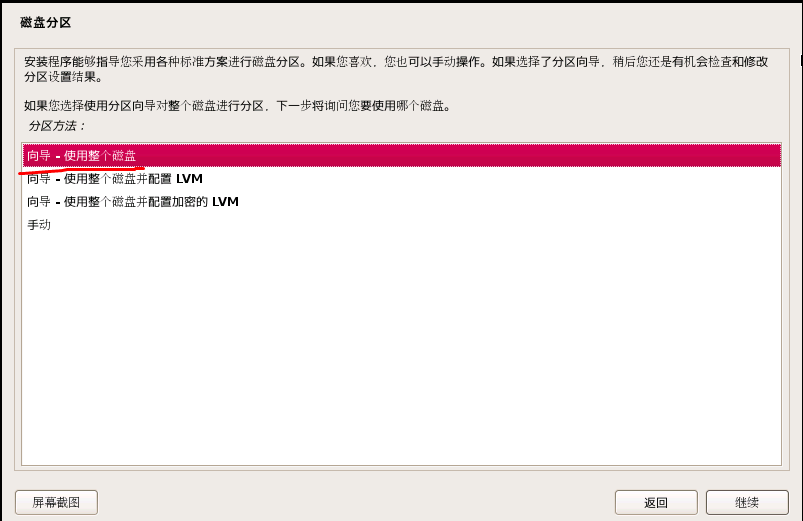
**kali和BT5关系**

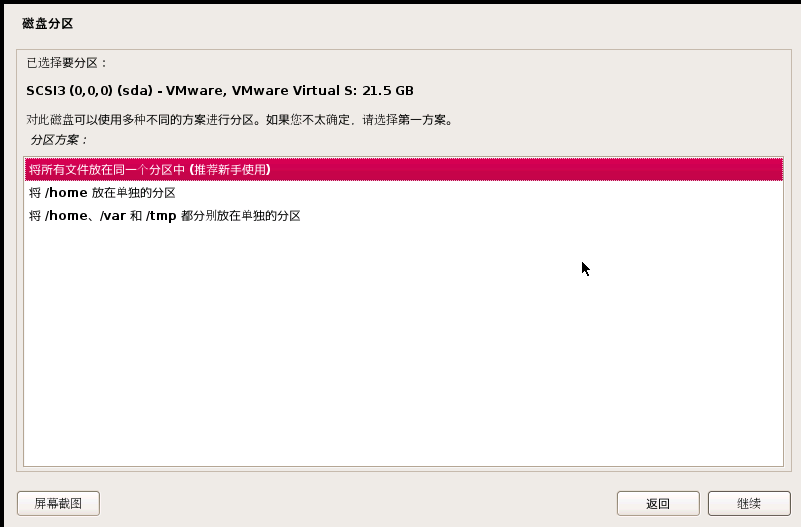
**19.1.2 安装kali系统**



****

**分区：**

****

****

**需要联网，需要配置apt-get 源**

**安装软件包方式不一样：**

**kali 使用 apt-get命令来安装软件**

**RHEL/centos : rpm 或 yum**

**例：kali / ubuntu下apt-get 命令参数**

**常用的APT命令参数**

**apt-cache search package 搜索包**

**apt-cache show package 获取包的相关信息，如说明、大小、版本等**

**sudo apt-get install package 安装包**

**sudo apt-get remove package 删除包**

**sudo apt-get update 更新源**

**sudo apt-get upgrade 更新已安装的包**

**sudo apt-get dist-upgrade 升级系统**

**其中：**

**1 有SUDO的表示需要管理员特权！**

**2 在UBUNTU中命令后面参数为短参数是用“-”引出，长参数用“--”引出**

**3 命令帮助信息可用man 命令的方式查看或者命令 -H（--help）方式查看**

**4 在MAN命令中需要退出命令帮助请按“q”键！！**

**实例： 配置静态IP地址**

**配置IP方式有两种：**

1. **通过命令直接配置**

**ifconfig eth0 IP地址**

**route add default gw 网关－－－－－－－－－－－－添加默认路由**

**vi /etc/resolv.conf 配置文件 添加nameserver DNS－－－－配置ＤＮＳ**

**但是方式只能临时修改，当服务器重启后，配置信息丢失**

**例：**

**root@localhost:~# ifconfig eth0 192.168.1.63**

**root@localhost:~# route add default gw 192.168.1.1**

**２、直接修改配置文件**

**Ubuntu 系统配置文件在：/etc/network/interfaces  
 编辑配置文件：**

**vim /etc/network/interfaces  
 并用下面的行来替换有关eth0的行：  
 # The primary network interface  
 auto eth0  
 iface eth0 inet static  
 address 192.168.1.64  
 gateway 192.168.1.1  
 netmask 255.255.255.0  
  
 /etc/init.d/networking restart－－重启网卡；使之配置生效**

**配置ＩＰ地址后，需要配置ＤＮＳ；具体方式如下；**

**vim /etc/resolv.conf    
 search chotim.com  
 nameserver 8.8.8.8  
 /etc/init.d/networking restart－－重启网卡服务即可**

**19.2 实战：linux之kali系统ssh服务开启**

**默认情况下，kali系统ssh服务没有开启.**

**具体按如下操作进行设置:**

**19.2.1 修改sshd\_config文件，命令为：vi /etc/ssh/sshd\_config   
  
 改：56 #PasswordAuthenticati**

**为：PasswordAuthentication yes**

**在：32 #PermitRootLogin without-password 之后**

**插入：**

**PermitRootLogin yes**

**19.2.2 启动SSH服务，**

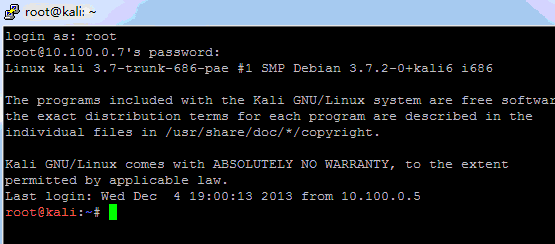
**/etc/init.d/ssh start**

**或者**

**service ssh start**

**root@localhost:~# systemctl restart ssh**

**19.2.3 验证SSH服务状态，命令为：/etc/init.d/ssh status**

**测试：  
**

**19.3 实战： kali下的nmap扫描工具**

**19.3.1 nmap 命令：**

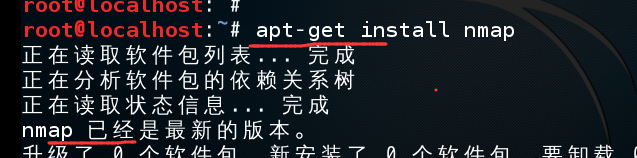
**nmap是一个网络探测和安全扫描程序，系统管理者和个人可以使用这个软件扫描大型的网络，获取那台主机正在运行以及提供什么服务等信息。**

**nmap ：支持很多扫描技术，例如：UDP、TCP connect()、TCP SYN(半开扫描)、ftp代理(bounce攻击)、反向标志、ICMP、FIN、ACK扫描、圣诞树(Xmas Tree)、SYN扫描和null扫描。可以探测操作系统类型。**

**名称：**

**nmap-网络探测和安全扫描工具**

**安装：**



**在centos7上安装namp方法：**

**[root@xuegod63 Desktop]# rpm -ivh /mnt/Packages/nmap-5.21-4.el7.x86\_64.rpm**

**19.3.2 语法：**

**nmap [Scan Type(s)] [Options]**

**例：nmap 被扫描的IP地址**

**[root@xuegod63 ~]# nmap 192.168.1.63**

**Starting Nmap 5.21 ( http://nmap.org ) at 2015-08-16 20:38 CST**

**Nmap scan report for xuegod63.cn (192.168.1.63)**

**Host is up (0.000029s latency).**

**Not shown: 998 closed ports**

**PORT STATE SERVICE**

**22/tcp open ssh**

**19.3.3 查看扫描后的详细信息：**

**例： 扫描一台机器查看，它打开的端口**

**参数 -v : 查看详细信息**

**[root@xuegod63 ~]# nmap -v 192.168.1.63**

**Starting Nmap 5.21 ( http://nmap.org ) at 2014-12-30 20:50 CST**

**Initiating ARP Ping Scan at 20:50**

**Scanning xuegod64.cn (192.168.1.64) [1 port]**

**Completed ARP Ping Scan at 20:50, 0.04s elapsed (1 total hosts)**

**Initiating SYN Stealth （隐身）Scan at 20:50**

**Scanning xuegod64.cn (192.168.1.64) [1000 ports] #对xuegod64,1000个端口进行扫描**

**Discovered open port 111/tcp on 192.168.1.64**

**Discovered open port 22/tcp on 192.168.1.64**

**Completed SYN Stealth Scan at 20:50, 1.30s elapsed (1000 total ports)**

**Nmap scan report for xuegod64.cn (192.168.1.64)**

**Host is up (0.00054s latency).**

**Not shown: 998 closed ports**

**PORT STATE SERVICE**

**22/tcp open ssh**

**111/tcp open rpcbind**

**MAC Address: 00:0C:29:48:80:95 (VMware)**

**19.3.4 扫描一个范围： 端口1-65535**

**[root@xuegod63 ~]# nmap -p 1-65535 192.168.1.63**

**Starting Nmap 5.21 ( http://nmap.org ) at 2015-11-09 21:46 CST**

**Nmap scan report for xuegod64.cn (192.168.1.64)**

**Host is up (0.00042s latency).**

**Not shown: 65531 closed ports**

**PORT STATE SERVICE**

**111/tcp open rpcbind**

**997/tcp open maitrd**

**5672/tcp open amqp**

**53095/tcp open unknown**

**MAC Address: 00:0C:29:48:80:95 (VMware)**

**正常情况，只能开我们需要开的服务，关闭不需要开的服务：**

**现在关闭不需要开的服务：有两种方法**

**情景1：你认识这个服务，直接关服务**

**[root@xuegod64 ~]# /etc/init.d/rpcbind stop**

**情景2：服务器这一招主要用找黑客的后门和进程的**

**不认识这个服务，查看哪个进程使用了这个端口，这个进程的路径，然后kill进程，删除文件**

**[root@xuegod64 init.d]# lsof -i :53095**

**COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME**

**rpc.statd 1781 rpcuser 9u IPv4 10770 0t0 TCP \*:53095 (LISTEN)**

**[root@xuegod64 init.d]# ls \*rpc.statd\* #找不到对应的服务**

**通ps命令查找对应的进程文件：**

**[root@xuegod63 init.d]# ps -axu | grep 1781**

**Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.8/FAQ**

**rpcuser 1781 0.0 0.1 23200 1208 ? Ss 20:20 0:00 rpc.statd #没有看到此命令的具体执行路径，说明rpc.statd可以bash终端下直接执行。接下来通过which和rpm -qf来查看命令的来源，如下：**

**[root@xuegod63 init.d]# which rpc.statd**

**/sbin/rpc.statd**

**[root@xuegod63 init.d]# rpm -qf /sbin/rpc.statd**

**nfs-utils-1.2.3-15.el6.x86\_64 #发现rpc.statd是nfs服务相关进程，说明不是木马程序**

**注： rpc.statd 命令会启动 statd 后台程序。 在 NFS 环境中 statd daemon 与 lockd daemon 相结合，为锁机制提供 crash 和 recovery 功能。**

**解决：**

**[root@xuegod64 init.d]# kill -9 1781**

**19.3.5 扫描一台机器：查看此服务器开放的端口号和操作系统类型。**

**[root@xuegod63 ~]# nmap -sS -O www.xuegod.cn**

**Starting Nmap 5.21 ( http://nmap.org ) at 2014-12-30 21:04 CST**

**Nmap scan report for www.xuegod.cn (112.124.185.97)**

**Host is up (0.044s latency).**

**Not shown: 996 filtered ports**

**PORT STATE SERVICE**

**21/tcp open ftp**

**80/tcp open http**

**443/tcp closed https**

**3306/tcp open mysql**

**Aggressive OS guesses: Linux 2.6.28 (93%), Linux 2.6.9 - 2.6.27 (93%), Riverbed Steelhead 200 proxy server (93%), Linux 2.6.9 (93%), Linux 2.6.30 (92%), Linux 2.6.9 (CentOS 4.4) (92%), Linux 2.6.11 (90%), Linux 2.6.18 (CentOS 5.1, x86) (89%), FreeBSD 6.2-RELEASE (89%), Linux 2.6.18 (89%)**

**No exact OS matches for host (test conditions non-ideal).**

**OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .**

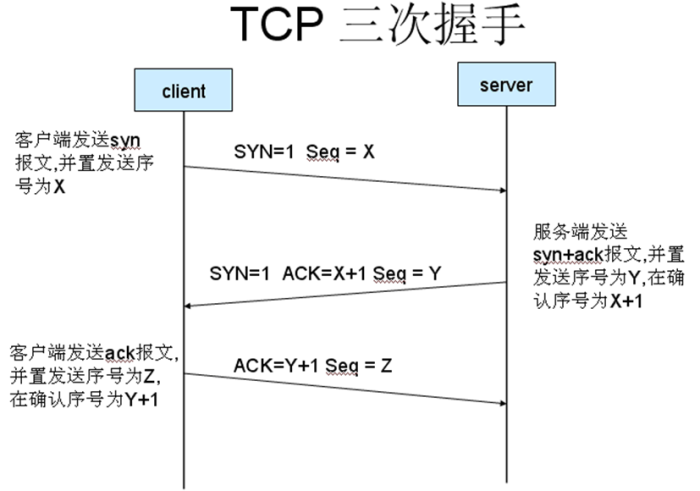
**Nmap done: 1 IP address (1 host up) scanned in 10.45 seconds**

**参数说明：**

**-sS：半开扫描(half-open)**

**TCP同步扫描(TCP SYN)：因为不必全部打开一个TCP连接，所以这项技术通常称为半开扫描(half-open)。你可以发出一个TCP同步包(SYN)，然后等待回应。如果对方返回SYN|ACK(响应)包就表示目标端口正在监听；如果返回RST数据包，就表示目标端口没有监听程序；如果收到一个SYN|ACK包，源主机就会马上发出一个RST(复位)数据包断开和目标主机的连接，这实际上由我们的操作系统内核自动完成的。**

**总结：就是tcp三次握手，少发最一个ACK包。**

****

**-O： 显示出操作系统的类型。 每一种操作系统都有一个指纹。 fingerprinting.**

**测试自己的电脑：**

**[root@xuegod63 ~]# nmap -sS -O 192.168.1**

**。。。**

**Running: Microsoft Windows Vista**

**例1：#扫描一个网段，中所有机器是什么类型的操作系统。**

**[root@xuegod63 ~]# nmap -sS -O 192.168.0.0/24**

**例2： 查找一些有特点的IP地址中，开启80端口的服务器。**

**[root@xuegod63 Desktop]# nmap -v -p 80 192.168.1.64-67**

**例3：如何更隐藏的去扫描，频繁扫描会被屏蔽或者锁定IP地址。**

**--randomize\_hosts # 随机扫描**

**--scan-delay #延时扫描,单位秒**

**实例1：随机扫描**

**[root@xuegod63 ~]# nmap -v --randomize\_hosts -p 80 192.168.1.64-69**

**Nmap scan report for 192.168.1.69 [host down]**

**Nmap scan report for 192.168.1.68 [host down]**

**Nmap scan report for 192.168.1.67 [host down]**

**Nmap scan report for 192.168.1.65 [host down]**

**Nmap scan report for 192.168.1.66 [host down]**

**实例2：随机扫描+延时扫描 ，默认单位秒**

**[root@xuegod63 ~]# nmap -v --randomize\_hosts --scan-delay 3000 -p 80 192.168.1.64-69**

**例4：使用通配符指定IP地址**

**[root@xuegod63 ~]# nmap -v --randomize\_hosts --scan-delay 30 -p 80 1.\*.2.3-8**

**19.4 MITM中间人攻击理论**

**19.4.1 中间人攻击理论**

**中间人攻击（Man in the Middle Attack，简称“MITM 攻击”）是一种间接的入侵攻击。**

**通过各种技术手段，将入侵者控制的一台计算机，放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。**

**常见攻击手段：**

**1、攻击者只要将网卡设为混杂模式，伪装成代理服务器监听特定的流量就可以实现攻击，这是因为很多通信协议都是以明文来进行传输的，如HTTP、FTP、Telnet等。随着交换机代替集线器，简单的嗅探攻击已经不能成功，必须先进行ARP欺骗才行。**

**2、SMB会话劫持**

**3、DNS欺骗**

**4、 为 HTTPS 提供假证书**

**以上攻击都是典型的MITM攻击。简而言之，所谓的MITM攻击就是通过拦截正常的网络通信数据，并进行数据篡改和嗅探，而通信的双方却毫不知情。**

**19.4.2 ARP欺骗原理**

**ARP协议概述：**

**ARP协议是“Address Resolution Protocol”（地址解析协议）的缩写。**

**计算机通过ARP协议将IP地址转换成MAC地址。**

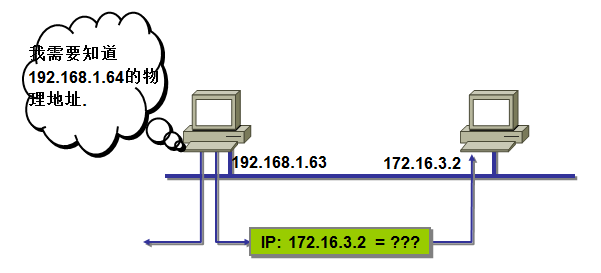
**ARP协议工作原理**

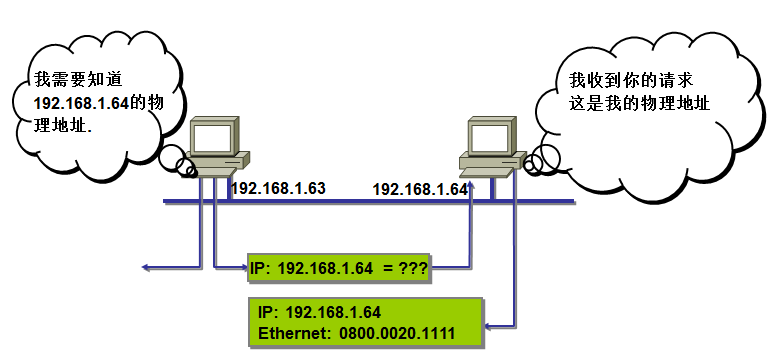
**在以太网中，数据传输的目标地址是MAC地址，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。**

**计算机使用者通常只知道目标机器的IP信息，“地址解析”就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。**

**简单地说，ARP协议主要负责将局域网中的32为IP地址转换为对应的48位物理地址，即网卡的MAC地址，保障通信顺利尽心。**

**apr工作原理如下：**





**以上是ARP正常通讯过程，下面是ARP欺骗过程：**

**ARP欺骗概述：**

**1、每个主机都用一个ARP高速缓存存放最近IP地址到MAC地址之间的映射记录。**

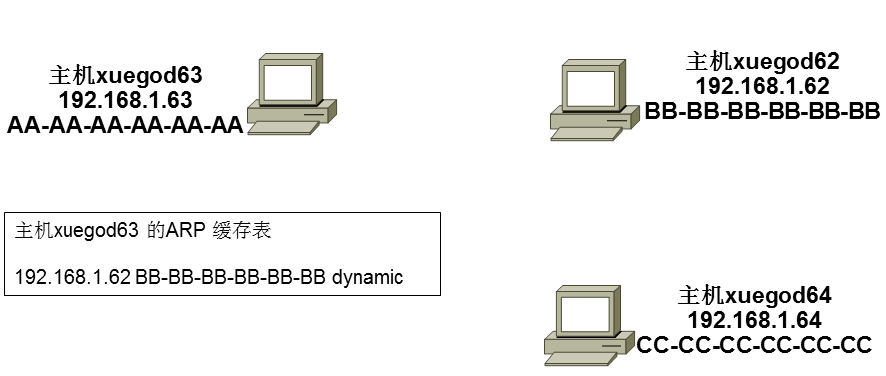
**2、默认情况下，ARP从缓存中读取IP-MAC条目，缓存中的IP-MAC条目是根据ARP响应包动态变化的。**

**3、要网络上有ARP响应包发送到本机，即会更新ARP高速缓存中的IP-MAC条目。**

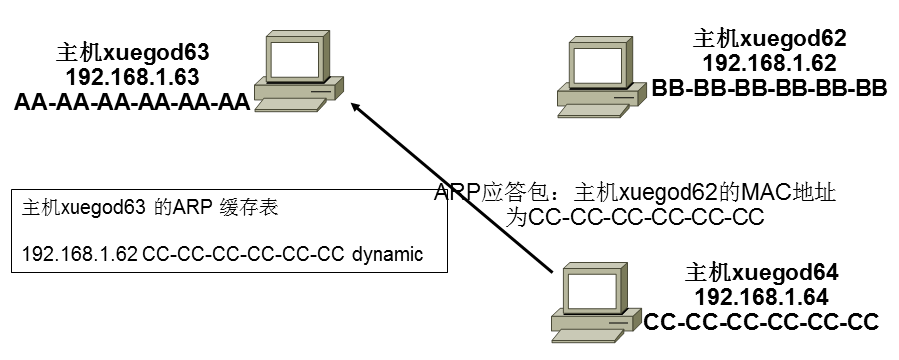
**4、攻击者只要持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，完成ARP欺骗。**

**ARP欺骗具体流程如下：**

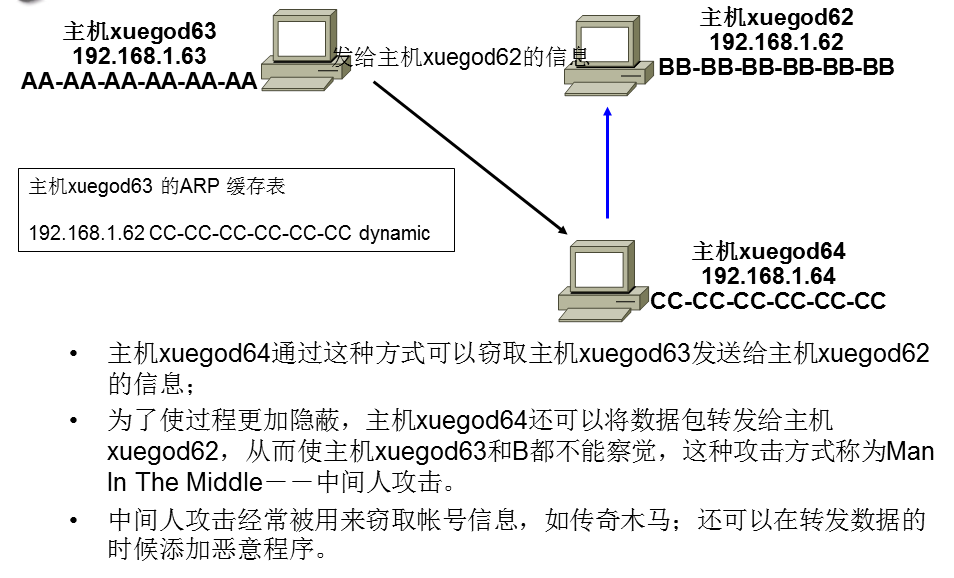
**1、正常情况：主机xuegod63上保存着xuegod64的IP和MAC对应关系表**



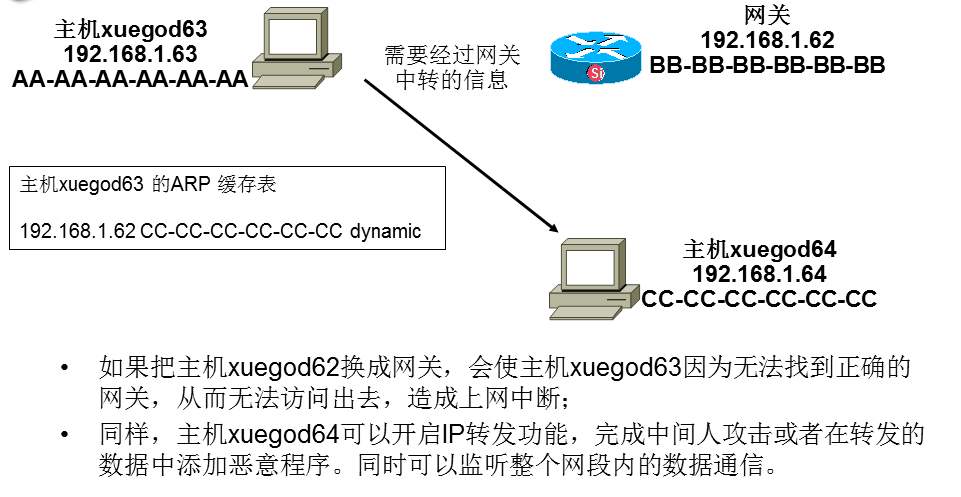
**2、xuegod64恶意给63发一个ARP应答包，来刷新63上ARP缓存表。 让63上缓存的MAC地址变为64的MAC**

****

**3、情景1：xuegod63发给62的数据，最终都发给了xuegod64，而xuegod64还可以把数据传给62。 实现中间人攻击**



**4、情况2：ARP欺骗--冒充网关，实现中间人攻击**



**怎样防范ARP欺骗**

**1、在主机绑定网关MAC与IP地址为静态（默认为动态），命令：arp -s 网关IP 网关MAC**

**2、在网关绑定主机MAC与IP地址**

**3、使用ARP防火墙**

**19.5 实战-使用 Ettercap 工具实现中间人攻击**

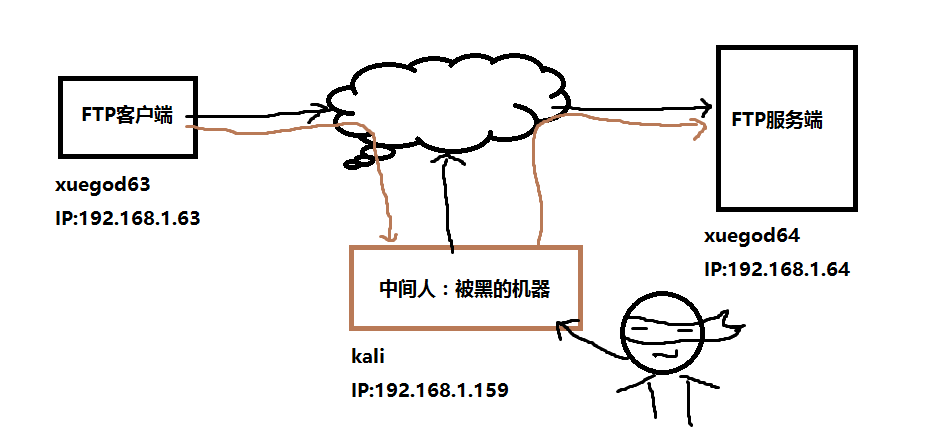
**实验主机**

**xuegod 64 192.168.1.64**

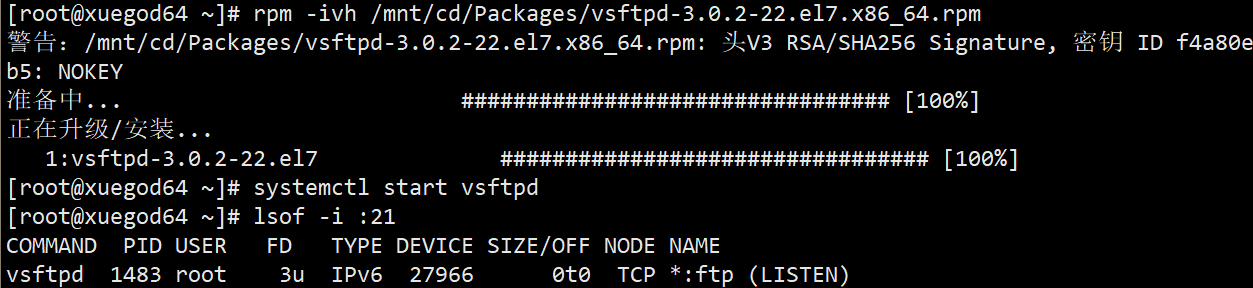
**xuegod63 192.168.1.63**

**kali-Linux 192.168.192.159**

**实战1： 在局域网中，通过Ettercap抓取vsftp服务器的用户名和密码**



**19.5.1 xuegod64 安装ftp服务**

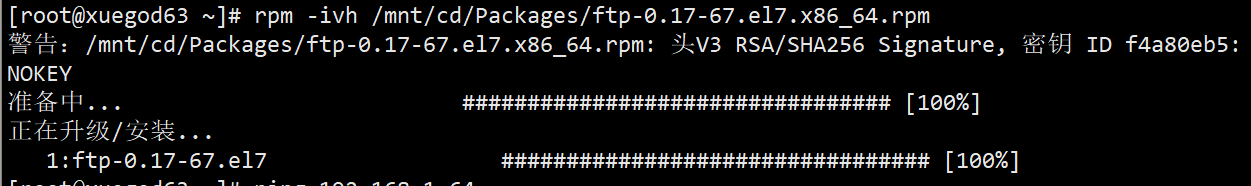


**添加一个系统用户：kill 密码： 123456 用于后期登录ftp**

**[root@xuegod63 ~]# useradd kill**

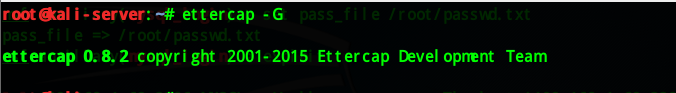
**[root@xuegod63 ~]# echo 123456 | passwd --stdin kill**

**19.5.1 xuegod63安装ftp客户端工具**



**19.5.2 kali-linux 配置**

**1、初始化ettercap**

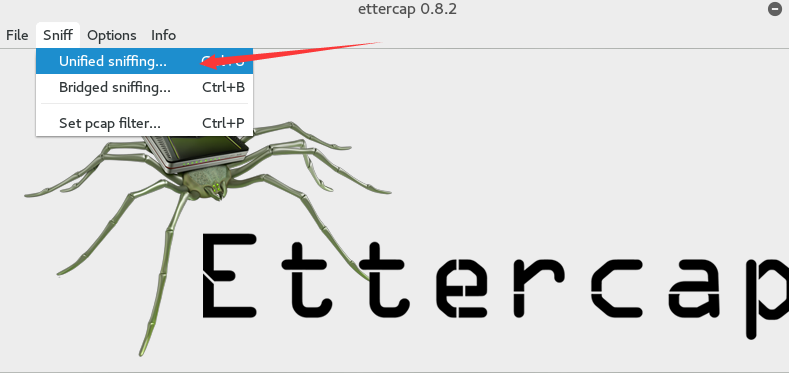


**2、选择Sniff 抓包. 嗅探**

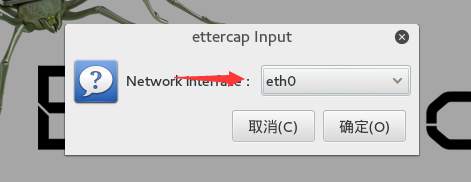


**3、开始抓包。**

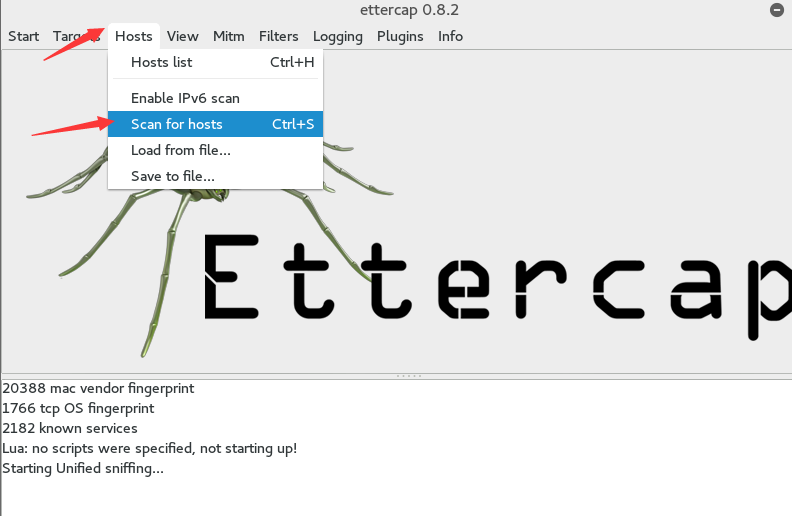
**unified ['ju:nɪfaɪd] 统一**



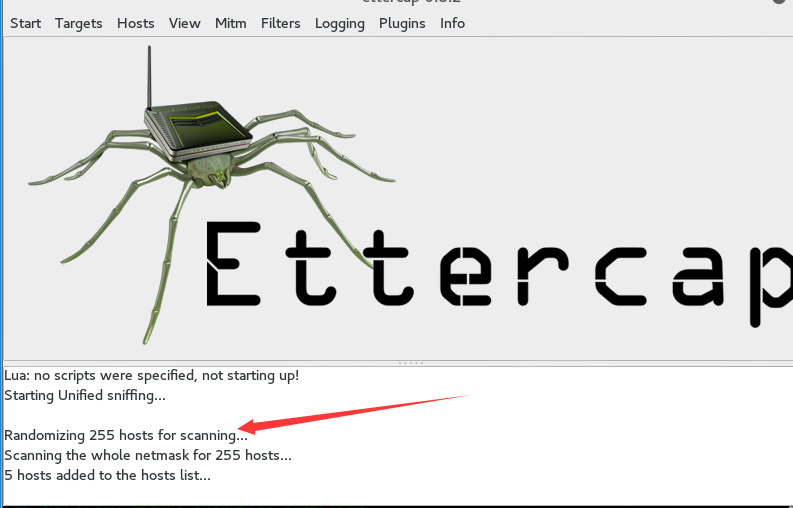
**4、选择网卡**



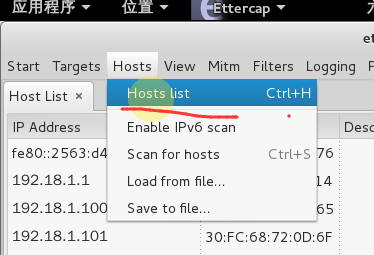
**5、选择主机 🡪 开始扫描主机**



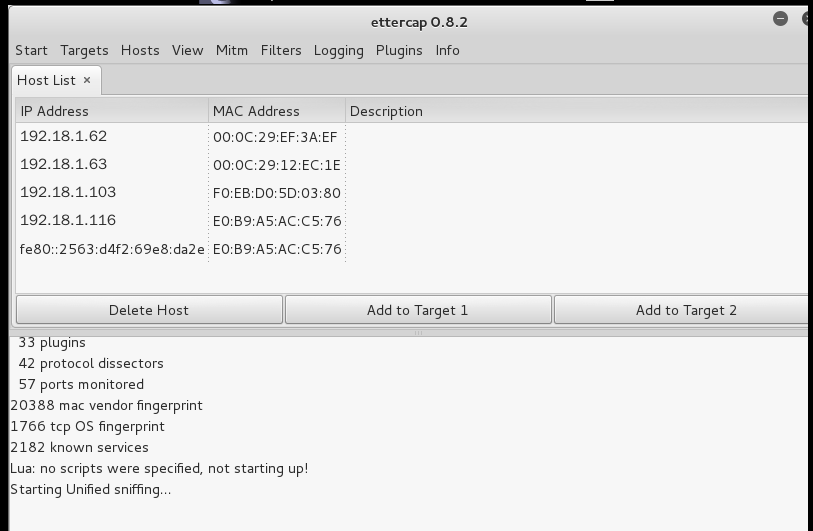
**6、生成主机列表**



**7、点开主机列表**



**8、查看被扫描的主机**



**9、在xuegod63上登录xuegod64的ftp服务器。**

**[root@xuegod63 ~]# ftp 192.18.1.64**

**Connected to 192.18.1.62 (192.18.1.62).**

**220 (vsFTPd 2.2.2)**

**Name (192.18.1.62:root): Kill #这个名字可以随意写**

**331 Please specify the password.**

**Password:123456**

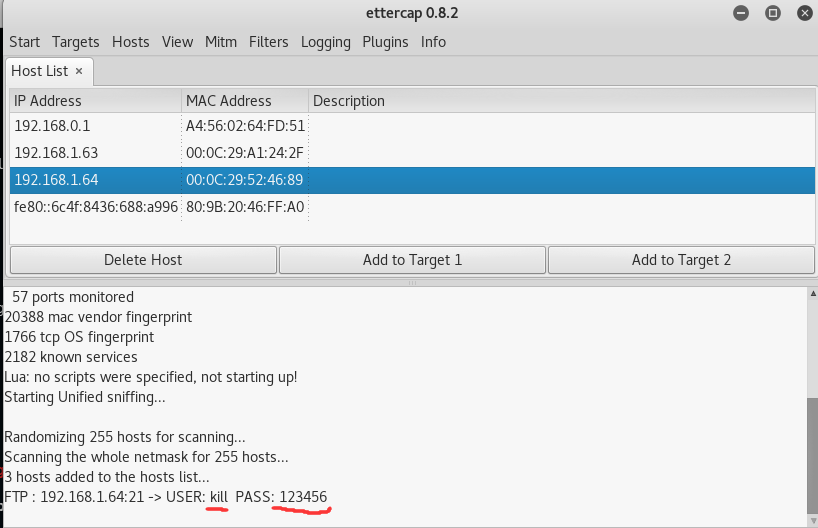
**530 Login incorrect.**

**Login failed.**

**ftp>**

**此时，当登录 192.168.1.64 主机kill和123456相关的敏感信息将会被传递给攻击者。**

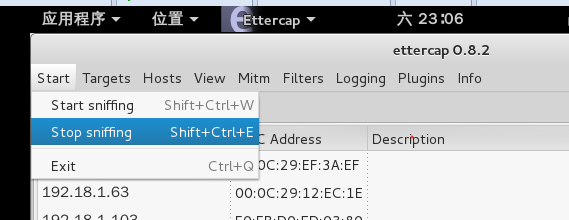
**19.5.6 登录kali查看：**



**从该界面可以看到，有用户登录 192.168.1.64 主机的 FTP 服务器了。**

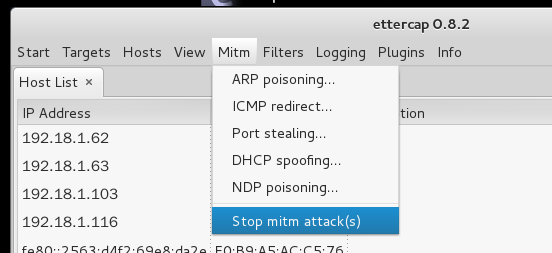
**其用户名为 kill，密码为 123456。**

**19.5.7 获取这些信息后停止嗅探，在菜单栏中依次单击 Start|Stop**



**停止嗅探后，还需要停止中间人攻击。在菜单栏中依次单击 Mitm|Stop mitm**

**attack(s)命令。**





**扩展：**

**手机app 使用http协议 加密了吗？ 没有 这样用户名和密码 可以在局域网中被抓到**

**解决方法：**

**所有手机app 软件通信都应该使用https协议**

**总结：**

**19.1 安装Kali黑客操作系统及相关实战**

**19.2 实战：linux之kali系统ssh服务开启**

**19.3 实战： kali下的nmap扫描工具**

**19.4 MITM中间人攻击理论**

**19.5 实战-使用 Ettercap 工具实现中间人攻击**