科来

第 12 章
如何分析理解端口扫描行为

科来官微
CSNA 公众号
400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

端口扫描，通常是指利用 TCP、UDP 等方式，去检测操作系统类型及开放的服务，为进一步的攻击做好准备。通常蠕虫病毒、网络攻击等常见的影响网络安全的行为，都是从扫描开始的。所以，深入了解各种网络扫描的工作原理及其表现特征，对网络管理者具有重要的实战意义。

NMAP 作为常见的网络扫描工具，内置了多种扫描方式。每种方式的工作原理不同，其数据包和通讯特征也不尽相同。我们将通过网络分析软件，对常见扫描方式进行分析和图形化的展现，以方便大家对这些扫描方式有一个深入的理解。

12.1 分析过程

12.1.1 TCP SYN 扫描

TCP SYN 扫描，是最受攻击者欢迎的扫描类型之一。其扫描速度快（每秒可以扫描数以千计的端口），兼容性好（只要对端支持 TCP 协议栈即可），且不易被发现。

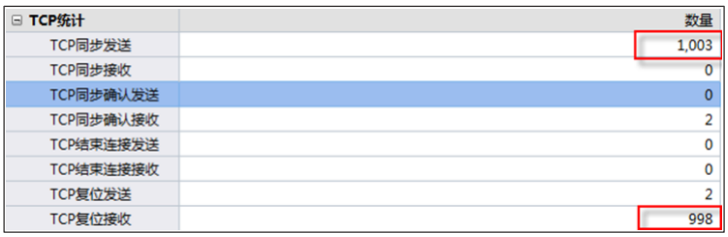
TCP SYN 扫描，通常又叫“半开放”扫描。因为它不必打开一个完整的 TCP 连接，只发送一个 SYN 包，就能做到打开连接的效果，然后等待对端的反应。如果对端返回 SYN/ACK 报文，则表示该端口处于监听状态，此时，扫描端则必须再返回一个 RST 报文来关闭此连接；返回 RST 报文表示该端口没有开放。

TCP SYN 扫描在科来网络分析中的视图表现：小包多（<128 字节），如下图所示。

数据包大小分布	字节数	数据包数	利用率	每秒位数	每秒包数
<=64	140,258	2,224	0.005%	512	1
65-127	19,812	270	0.000%	0	0
128-255	5,661	33	0.000%	0	0
256-511	0	0	0.000%	0	0
512-1023	1,459	2	0.000%	0	0
1024-1517	0	0	0.000%	0	0
>=1518	0	0	0.000%	0	0

图 12-1

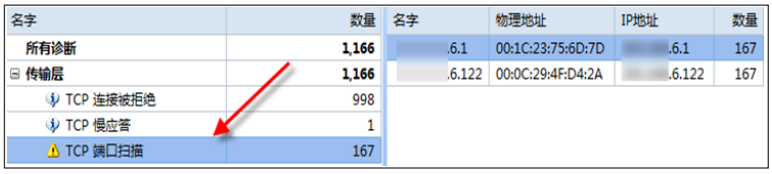
在 TCP Flag 统计中，TCP 同步位发送和 TCP 复位接收较多，如下图所示。



TCP统计	数量
TCP同步发送	1,003
TCP同步接收	0
TCP同步确认发送	0
TCP同步确认接收	2
TCP结束连接发送	0
TCP结束连接接收	0
TCP复位发送	2
TCP复位接收	998

图　12-2

可能会触发 TCP 端口扫描诊断，如下图所示。

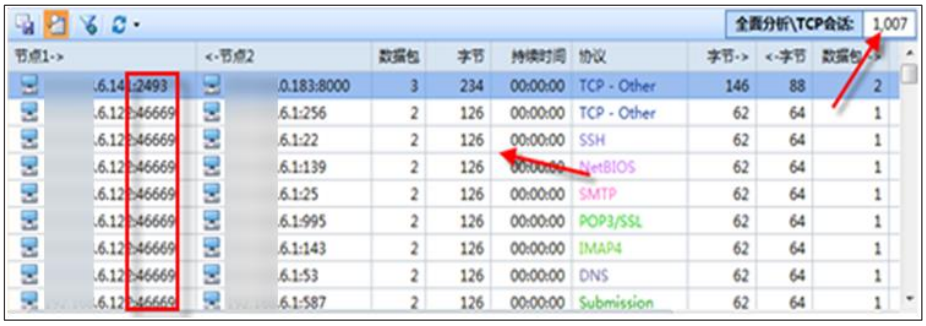


名字	数量
所有诊断	1,166
传输层	1,166
TCP 连接被拒绝	998
TCP 慢应答	1
TCP 端口扫描	167

名字	物理地址	IP地址	数量
.6.1	00:1C:23:75:6D:7D	.6.1	167
.6.122	00:0C:29:4F:D4:2A	.6.122	167

图　12-3

以固定端口与被扫描 IP 尝试连接，且会话大多具有相同的特征，如下图所示。



全面分析\TCP会话: 1,007

节点1->	<-节点2	数据包	字节	持续时间	协议	字节->	<-字节	数据包
.6.14 :2493	.0.183:8000	3	234	00:00:00	TCP - Other	146	88	2
.6.12 :46669	.6.1:256	2	126	00:00:00	TCP - Other	62	64	1
.6.12 :46669	.6.1:22	2	126	00:00:00	SSH	62	64	1
.6.12 :46669	.6.1:139	2	126	00:00:00	NetBIOS	62	64	1
.6.12 :46669	.6.1:25	2	126	00:00:00	SMTP	62	64	1
.6.12 :46669	.6.1:995	2	126	00:00:00	POP3/SSL	62	64	1
.6.12 :46669	.6.1:143	2	126	00:00:00	IMAP4	62	64	1
.6.12 :46669	.6.1:53	2	126	00:00:00	DNS	62	64	1
.6.12 :46669	.6.1:587	2	126	00:00:00	Submission	62	64	1

图　12-4

会话数据包总计为 2 个或 3 个。3 个包表示端口开放，2 个包表示端口未开放，如下图所示。

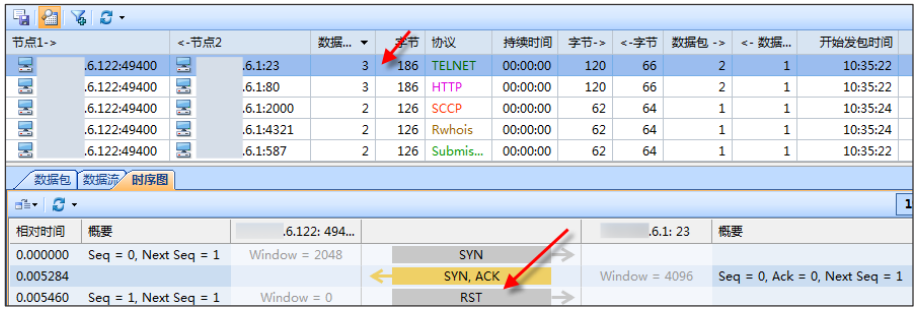


图　12-5

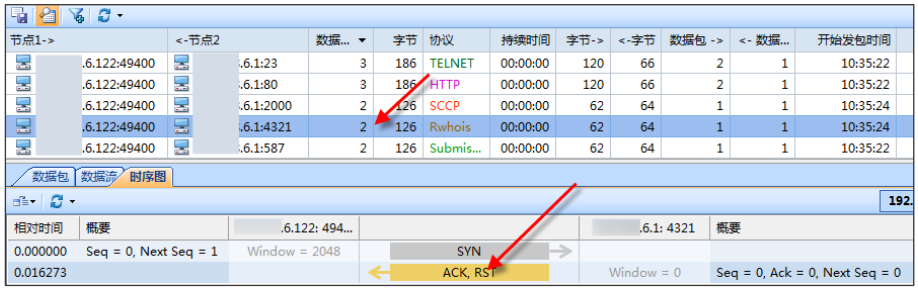


图　12-6

12.1.2　TCP connect 扫描

TCP connect（）扫描，是一种常见的扫描方式。它通过操作系统与目标机器建立连接，而不是直接发送原始数据包。这与浏览器、P2P 客户端以及大多数网络应用程序一样，建立连接由高层系统调用。执行这种扫描的最大好处是无需 root 权限，但会在系统日志里留下记录。所以当在日志系统里，看到同一系统的大量连接尝试，就应该知道系统被扫描了。

TCP connect（）扫描在科来网络分析系统中的视图表现：小包多（<128 字节），如下图所示。

图　12-7

在 TCP Flag 统计中 TCP 同步位发送和 TCP 复位接收较多，同时会有少量

的同步接受和复位包发送，如下图所示。

TCP统计	数量
TCP同步发送	1,574
TCP同步接收	0
TCP同步确认发送	0
TCP同步确认接收	41
TCP结束连接发送	0
TCP结束连接接收	0
TCP复位发送	47
TCP复位接收	1,533

图　12-8

以连续端口与被扫描 IP 尝试连接，且会话大多具有相同的特征，如下图所示。

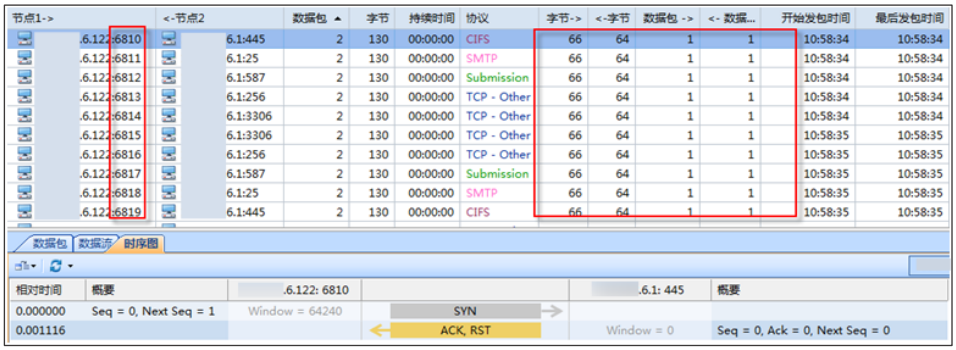
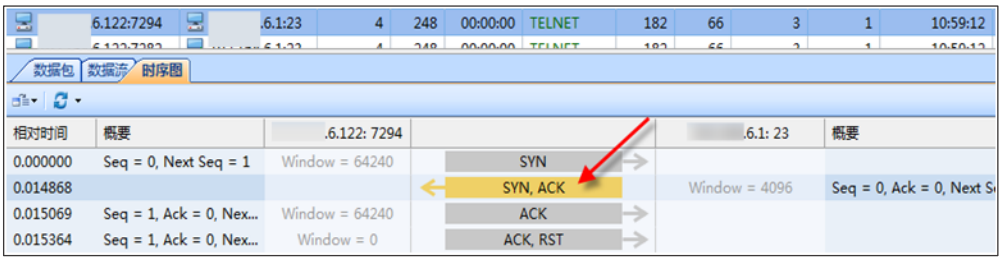


图　12-9



会话数据包总计为 2-6 个不等，需查看数据信息确认端口状态，如下图所示。

图　12-10

12.1.3　UDP 扫描

UDP 扫描，通常与 ICMP 相结合进行。在给目标主机发送没有携带任何数据的 UDP 数据包时，如果返回信息为“ICMP 端口不可达”（类型为 3，代码为 3）的提示，则表示目标端口是关闭的，但主机是存活的；如果某服务响应一个 UDP

报文，则表明该端口是开放的。

当然，UDP 扫描也存在瓶颈，那就是速度。很多主机默认限制发送“ICMP 端口不可达”信息，或者限制发包的频率。如 Linux2.4.20 内核，就只允许一秒钟发送一条目标不可达信息。这样，扫描 65535 个端口，需要 18 小时的时间。这是不可接受的，所以加速 UDP 扫描的方法，通常是并发扫描或先扫描主要端口。

UDP 扫描在科来网络分析中的视图表现：出现大量 UDP 会话，如下图所示。

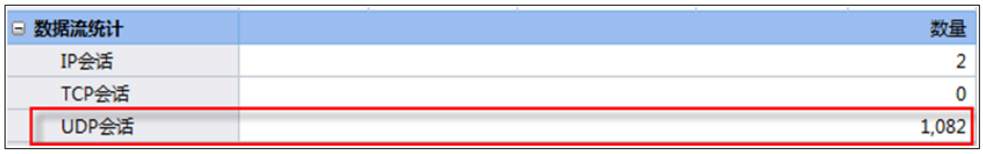


图　12-11

大量的 UDP 小包，且不携带任何数据，如下图所示。

图　12-12

触发大量 ICMP 端口不可达诊断，如下图所示。

图　12-13

会话数据包总计为 1-2 个，通常情况 1 个表示端口关闭，2 个或以上表示端口开放，如下图所示。

节点1->	<-节点2	持续时间	字节	字节->	<-字节	数据包	数据包 ->	<- 数...	协议
6.122:35727	6.1:64590	00:00:00	46	46	0	1	1	0	UDP - Other
6.122:35727	6.1:17184	00:00:00	46	46	0	1	1	0	UDP - Other
6.122:35727	6.1:43370	00:00:00	46	46	0	1	1	0	UDP - Other
6.122:35727	6.1:21476	00:00:00	46	46	0	1	1	0	UDP - Other
6.122:35727	6.1:18319	00:00:00	46	46	0	1	1	0	UDP - Other
6.122:35727	6.1:25541	00:00:00	46	46	0	1	1	0	UDP - Other
6.122:35727	6.1:39888	00:00:00	46	46	0	1	1	0	UDP - Other
6.122:35727	6.1:9	00:00:00	46	46	0	1	1	0	Discard

图　12-14

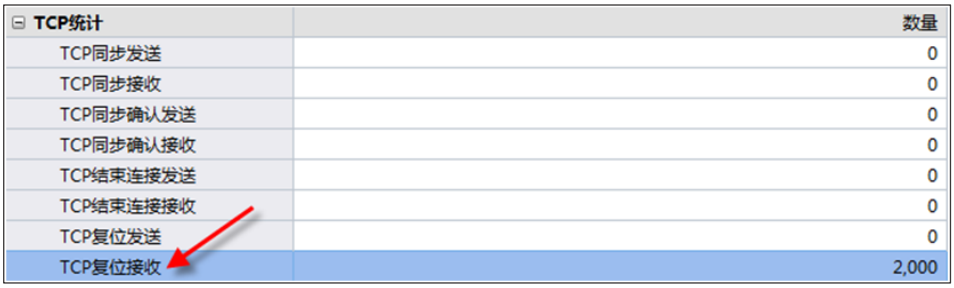
12.1.4　NULL 扫描

根据 RFC 793，主机发送一个没有任何标志位的 TCP 包，如果目标主机的对应端口是关闭的话，则会返回一个 RST 数据包，如果没有响应则表示该端口是开放的。

NULL 扫描，可以躲过无状态防火墙和报文过滤路由器，且比 SYN 扫描要隐秘。值得注意的是，并不是所有系统都遵循 RFC 793。一些系统不管端口是开放还是关闭，都响应 RST 数据包。如 Cisco 设备、BSDI 等。

根据 RFC793，类似的扫描还有 FIN 扫描、FIN+PSH+URG 扫描。

NULL 扫描在科来网络分析中的视图表现：网络中存在大量小包，大量的 TCP 复位数据包，如下图所示。



TCP统计	数量
TCP同步发送	0
TCP同步接收	0
TCP同步确认发送	0
TCP同步确认接收	0
TCP结束连接发送	0
TCP结束连接接收	0
TCP复位发送	0
TCP复位接收	2,000

图　12-15

大量没有任何标志位的数据包，如下图所示。

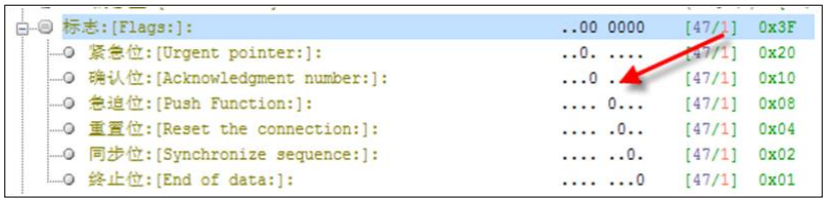


图 12-16

12.1.5 ACK 扫描

ACK 扫描发送一个只设置 ACK 标志位的数据包，目标主机端口无论是关闭还是开放状态，都会返回 RST 数据包。但 ACK 扫描不能确定目标主机的端口状态，可以确定对方主机是否存活，可以发现防火墙规则来确定防火墙的状态。

ACK 扫描在科来网络分析中的视图表现：网络中存在大量小包，大量的 TCP 复位数据包，如下图所示。

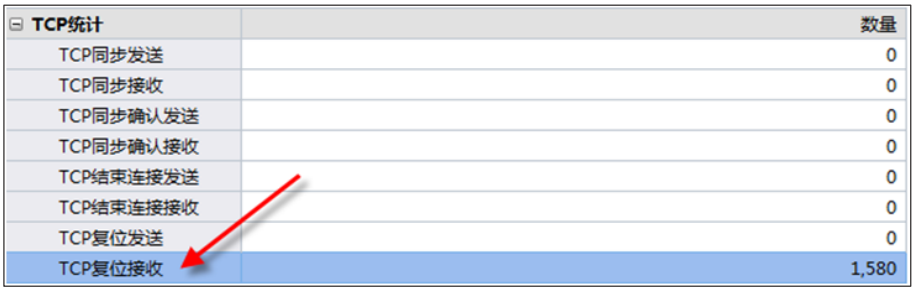


图 12-17

大量 ACK 标志位置 1 的数据包，如下图所示。

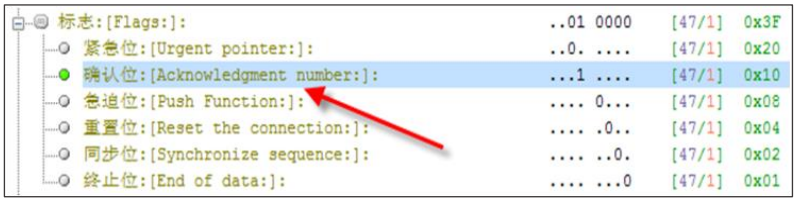


图 12-18

12.1.6 窗口扫描

在某些系统上，开放端口用正数表示窗口大小，而关闭的窗口大小则为 0。窗口扫描，就是通过检查返回 RST 报文的窗口字段，来判断端口是否开放。

窗口扫描依赖于少数的系统实现细节，不支持它的系统通常会返回“所有端口都关闭”信息；甚至有些系统会给出相反的行为（比如：扫描显示 1000 端口开放，3 个端口关闭，那么这 3 个端口反而是开放的）。

窗口扫描在科来网络分析中的视图表现：网络中存在大量小包，大量的 TCP 复位统计，如下图所示。

数据包大小分布	字节数	数据包数	利用率	每秒位数	每秒包数
<=64	279.840 KB	4,697	4.418%	88.352 Kbps	181
65-127	1.033 KB	11	0.000%	0	0
128-255	1.445 KB	9	0.000%	0	0
256-511	0.255 KB	1	0.000%	0	0
512-1023	1.409 KB	2	0.000%	0	0
1024-1517	0.000 KB	0	0.000%	0	0
>=1518	0.000 KB	0	0.000%	0	0

图　12-19

TCP统计	数量
TCP同步发送	0
TCP同步接收	0
TCP同步确认发送	0
TCP同步确认接收	0
TCP结束连接发送	0
TCP结束连接接收	0
TCP复位发送	0
TCP复位接收	2,330

图　12-20

网络中存在大量特征相同的协议统计，如下图所示。

	字节	数据包	接收数据包	发送字节	发送数据包	组内字节	字节%
Mit-ml-dev	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
WhoIs	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
BitTorrent	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
H.225	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
POP3	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
HTTP	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
HTTPS	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
X-Window	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
SIP	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
NNTP/SSL	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
SNPP	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
IMAP4/SSL	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%
SMTP	0.477 KB	8	4	0.227 KB	4	0.000 KB	0.168%

图　12-21

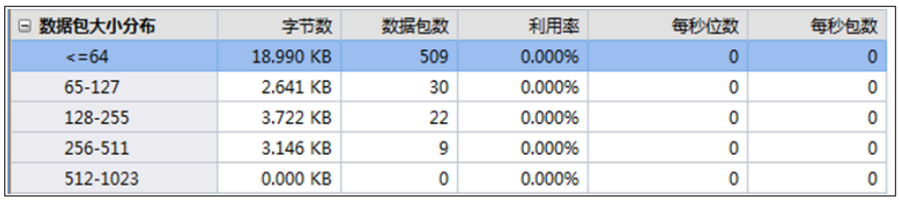
12.1.7　IP 扫描

IP 协议扫描，用来确定目标主机支持的 IP 协议，如 TCP、UDP、ICMP 等。

它不对任何 TCP 或 UDP 端口发送报文，而是对 IP 协议号发送对应的数据包。

IP 协议扫描发送 IP 报文，报文不包含任何数据，甚至不包含协议的正确报文头（TCP、UDP、ICMP 例外）。IP 协议扫描需要关注“ICMP 协议不可达”信息，收到目标主机的任何协议响应，即表示该协议是开放的。

窗口扫描在科来网络分析中的视图表现：网络中存在大量小包，如下图所示。



数据包大小分布	字节数	数据包数	利用率	每秒位数	每秒包数
<=64	18.990 KB	509	0.000%	0	0
65-127	2.641 KB	30	0.000%	0	0
128-255	3.722 KB	22	0.000%	0	0
256-511	3.146 KB	9	0.000%	0	0
512-1023	0.000 KB	0	0.000%	0	0

图　12-22

网络中存在大量特征相同的 IP 数据包，且不携带任何数据，如下图所示。

字	字节	数据包	接收数据包	发送字节	发送数据包	组内字节
IP	28.499 KB	570	33	23.657 KB	537	0.000 KB
VRRP	0.074 KB	2	0	0.074 KB	2	0.000 KB
SPS	0.074 KB	2	0	0.074 KB	2	0.000 KB
SKIP	0.074 KB	2	0	0.074 KB	2	0.000 KB
PIM	0.074 KB	2	0	0.074 KB	2	0.000 KB
RSVP	0.074 KB	2	0	0.074 KB	2	0.000 KB
SMP	0.074 KB	2	0	0.074 KB	2	0.000 KB
IDRP	0.074 KB	2	0	0.074 KB	2	0.000 KB
OSPF	0.074 KB	2	0	0.074 KB	2	0.000 KB
PIPE	0.074 KB	2	0	0.074 KB	2	0.000 KB
DDP	0.074 KB	2	0	0.074 KB	2	0.000 KB
ESP	0.074 KB	2	0	0.074 KB	2	0.000 KB
IGRP	0.074 KB	2	0	0.074 KB	2	0.000 KB

图　12-23

12.1.8　FIN\ACK 扫描

FIN/ACK 扫描也被称作 Maimon 扫描，根据发现者 Uriel Maimon 命名。其实 Maimon 扫描与 NULL、FIN 扫描的原理一样，根据 RFC 793，无论端口是关闭还是开放，目标主机都会对 FIN+ACK 探测数据包，响应 RST 报文（但许多基于 BSD 的系统，会丢弃 FIN+ACK 探测数据包）。

FIN\ACK 扫描在科来网络分析中的视图表现：网络中存在大量小包，大量的 TCP 复位统计，如下图所示。

数据包大小分布	字节数	数据包数	利用率	每秒位数	每秒包数
<=64	122.632 KB	2,058	0.026%	512	1
65-127	1.506 KB	17	0.000%	0	0
128-255	3.020 KB	18	0.000%	0	0
256-511	0.000 KB	0	0.000%	0	0
512-1023	0.000 KB	0	0.000%	0	0
1024-1517	0.000 KB	0	0.000%	0	0
>=1518	0.000 KB	0	0.000%	0	0

图　12-24

TCP统计	数量
TCP同步发送	0
TCP同步接收	0
TCP同步确认发送	0
TCP同步确认接收	0
TCP结束连接发送	1,002
TCP结束连接接收	1,002
TCP复位发送	1,000
TCP复位接收	1,000

图　12-25

网络中存在大量特征相同的协议统计，如下图所示。

名字	字节	数...	每秒位	每秒数据包	字节%	数据包%
TCP	120.263 KB	2,015	0	0	94.578%	96.273%
IRC	0.063 KB	1	0	0	0.049%	0.048%
Time	0.119 KB	2	0	0	0.094%	0.096%
Radius	0.119 KB	2	0	0	0.094%	0.096%
Discard	0.119 KB	2	0	0	0.094%	0.096%
SMTP/SSL	0.119 KB	2	0	0	0.094%	0.096%
Citrix ICA	0.119 KB	2	0	0	0.094%	0.096%
BGP	0.119 KB	2	0	0	0.094%	0.096%
RTSP	0.119 KB	2	0	0	0.094%	0.096%
DNS	0.119 KB	2	0	0	0.094%	0.096%
PPTP	0.119 KB	2	0	0	0.094%	0.096%

图　12-26

大量同步位（ACK）和终止位（FIN）的数据包，如下图所示。

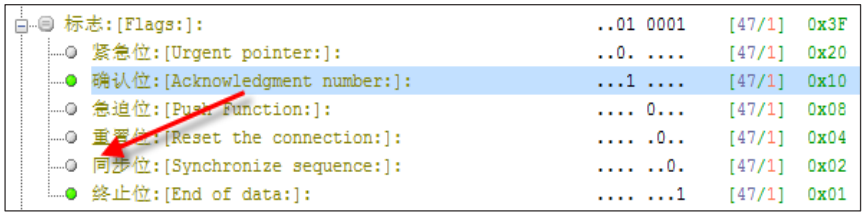


图 12-27

12.1.9 定制扫描

一些高级用户，不会遵循现成的扫描类型和规则，而是根据实际情况，任意指定 TCP 的相关标志位和扫描类型，从而避免 IDS 等设备的检测。

FIN/ACK 扫描在科来网络分析中的视图表现：

利用概要、协议、TCP/UDP 会话、解码视图进行综合分析。

12.2 分析结论

1、端口扫描的大致特征

◇ 小包多，大小基本在 64-128 字节之间；

◇ SYN 置 1，RST 置 1 的数据包较多；

◇ 大量的 TCP 或 UDP 会话，且具有相同的会话特征；

◇ 采用连续端口或固定端口，尝试与目标主机连接；

◇ 诊断提示中会出现 TCP 复位，ICMP 端口不达，甚至端口扫描提示。

2、了解端口扫描原理有哪些好处

◇ 快速定位蠕虫病毒；

◇ 快速确定攻击行为及类型；

◇ 快速厘清正常通讯与异常通讯；

◇ 快速发现网络中的异常行为。

12.3 价值

端口扫描有很多种，只要我们掌握其原理，无论使用的哪种扫描技术，我们都可以通过网络分析进行快速定位，找出攻击源。

科来 Ping 工具

科来数据包播放器

科来数据包生成器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 GartnerNPMD 魔力象限，并荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区