## 利用黑客工具进行渗透的数据分析

选用工具：X-SCAN 3.3

目标网络：本地局域网 192.168.10.1/24

分析软件：科来网络分析系统2010 beta版

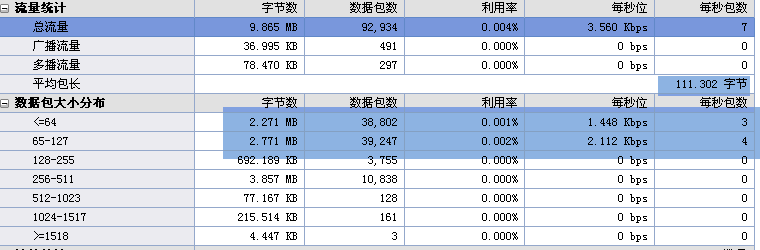
我们知道如果黑客想入侵一个网络，他需要更多的了解一个网络的信息，包括网络拓扑结构，哪些主机在运行，有哪些服务在运行，主机运行的是什么系统，以及该系统主机有没有其他漏洞，和存在一些弱口令等情况等。 只有在充分了解了足够多的信息之后，入侵才会变成可能。而黑客入侵之前的扫描是一个比较长时间的工作，同时现象也是比较明显的。我们通过网络分析手段可以很好的把握入侵特征。网络扫描工具很多，比较有名的如国产的冰河和国外的X-scan 等软件。

### 分析过程

本文选用的一款比较普遍的网络扫描工具X-SCAN 版本为3.3 。我们在扫描网络之前需要对X-SCAN进行设置，具体设置可以从网上搜一些教程。扫描网络为192.168.10.1/24，抓取位置选为本机抓包方式（即在攻击主机上进行抓包）。

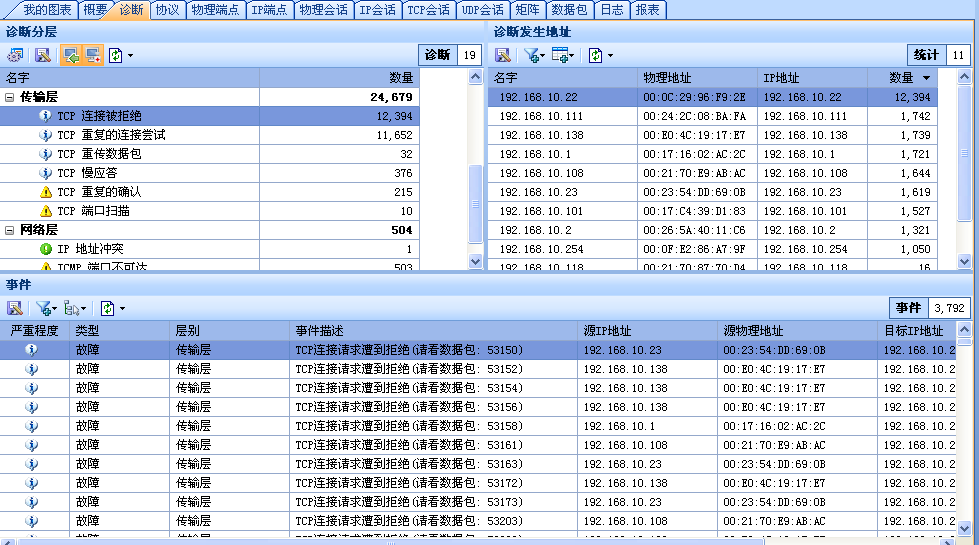
抓包从X-Scan 扫描开始，到扫描结束。抓包后的数据位10M（中间有些数据有其他通信产生）持续时间大概为10分钟。

首先，10分钟产生10M的数据量是不大的，这也就是说单个主机的扫描其实是不占用很多网络带宽的，如图：



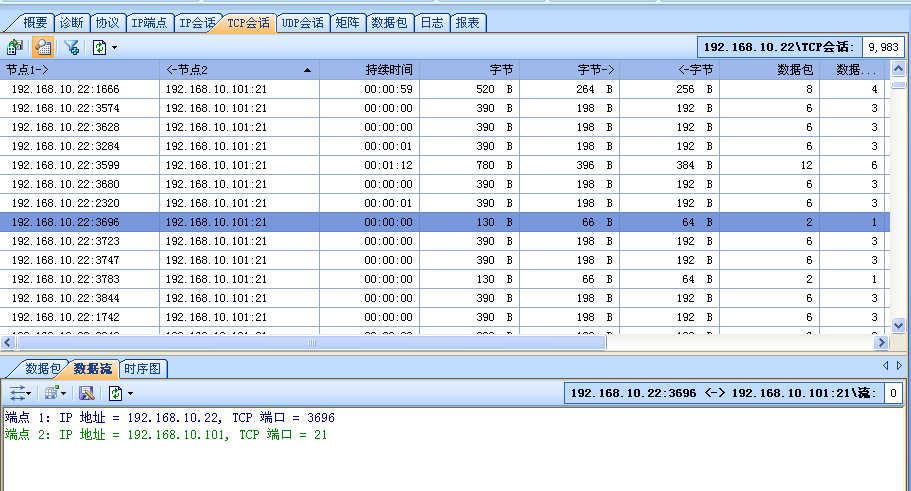
上图也反映了一些特征，我们看到，抓包网络内的数据包长只有111.3Byte，这个平均包长是偏小的，而且数据包大小分析发现<=64字节和65-127字节之间的数据占了绝大多少，这就充分说明了网络中有大量的小包存在。

我们接下来看下诊断信息能给我们什么提示，



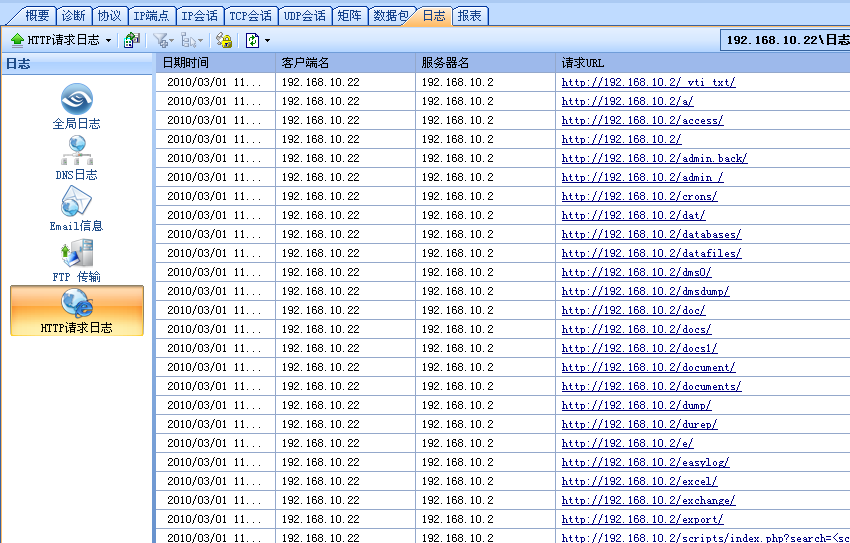
如图，我们发现存在大量的诊断事件产生，10M不到的数据竟然产生了2W5的诊断条目，而且大多数是传输层的诊断，出现了 TCP端口扫描 等比较危险的诊断信息。我们看到有两项的诊断出现次数较多“TCP连接被拒绝”“TCP重复的连接尝试”两个诊断大概出现了1W1次以上，我们可以将与这两个诊断相关的信息进行提取查看“诊断发生的地址”然后按照“数量”来排名发现 一个IP 192.168.10.22 这个IP 发生的诊断数据最多。而且诊断“TCP端口扫描”的源IP 就是192.168.10.22 这个IP。

我们定位192.168.10.22这个IP，然后查看TCP会话选项。如图：



我们发现 192.168.10.22这个IP的会话数量很多，而且会话是很有特征的。我们选取了其中针对192.168.1.101的21端口的一段会话进行查看，22与101之间的会话很多，而且都是一样的特征，建立连接后发送一次密码，被拒绝后再发起另一次会话。此为明显的暴力破解FTP密码行为。除了FTP之外还有针对445 和139端口的破解，以及内网服务的检查等。正是这种破解和扫描形成了如此多的会话条目。

此外，我们可以从日志选项中查看一些现场，以下是日志的截图：



扫描主机 在看到 192.168.10.2 有80端口开放后，发起一些针对HTTP的探测，用不同的路径和不同的请求方法，视图取得HTTP的一些敏感信息和一些可能存在的漏洞。

这种黑客的扫描得出的结果还是很详细和危险的，在不到10分钟之内，就将一个局域网内的各主机的存活，服务，和漏洞情况进行了了解，并且取得了一些效果。例如本次扫描发现一台FTP 服务器的一个账号 test 密码为123456 的情况，这种简单的密码和账号最好不要留下，及时的清理。

### 总结

扫描行为，主要有三种，ICMP扫描用来发现主机存活和拓扑，TCP 用来判断服务和破解，UDP确定一些特定的UDP服务。扫描是入侵的标志，扫描的发现主要是靠平时抓包分析，和日常的维护中进行。最好能够将科来长期部署在网络中，设定一定的报警阀值，例如设置TCP SYN 的阀值和诊断事件的阀值等，此功能是科来2010新功能之一，很好用。

扫描的防御很简单，可以设置防火墙，对ICMP不进行回应，和严格连接，及会话次数限制等。