科来

第 11 章
如何分析暴力破解数据库密码的攻击行为

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

© 2003-2019 科来版权所有

数据库被攻击是非常严重的安全事件，该攻击能导致数据被拖库，从而给服务提供商带来严重损失，甚至会也会导致用户信息被泄漏。

11.1 环境描述

科来网络分析工程师在对某机构外网进行网络健康检查时，为其核心交换机部署了科来网络回溯分析系统，镜像总出口网络流量并导入回溯分析设备。具体部署情况，如下方拓扑图所示。

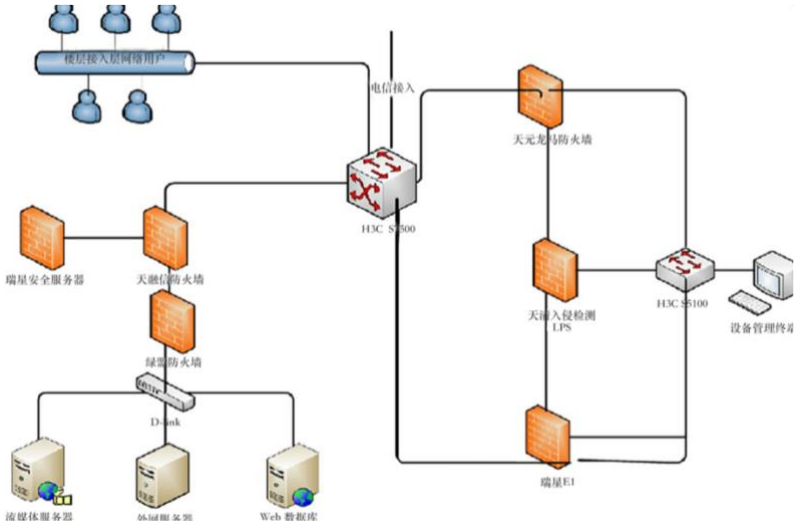

图 11-1

11.2 分析过程

通过科来网络回溯分析系统，捕获一段时间的数据，发现 1 个 IP 地址异常。可以看到 X.X.26.203 地址共建立会话 300 多个，但是建立成功后，会话报文都是小包，平均包长 99B，如下图所示。

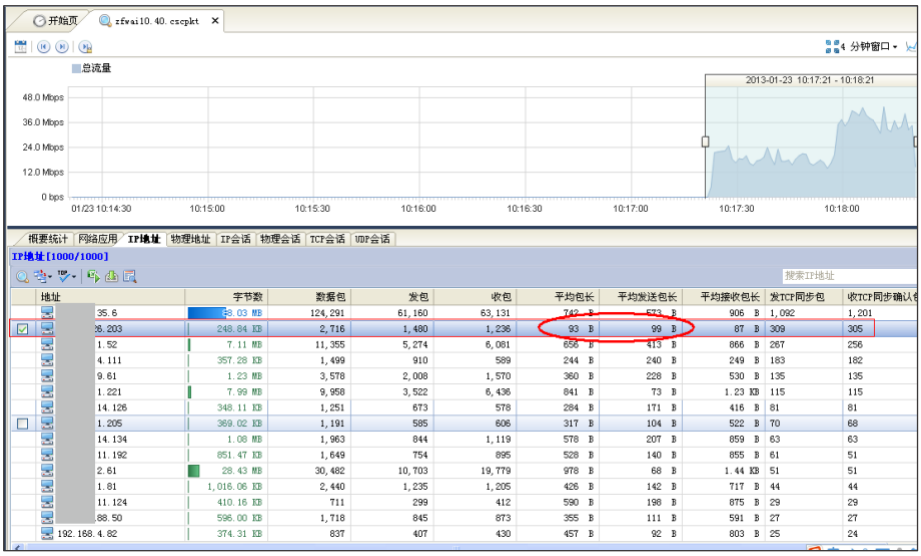

图　11-2

下载此数据包进行深入分析，第一步查看 IP 会话列表，如下图所示。

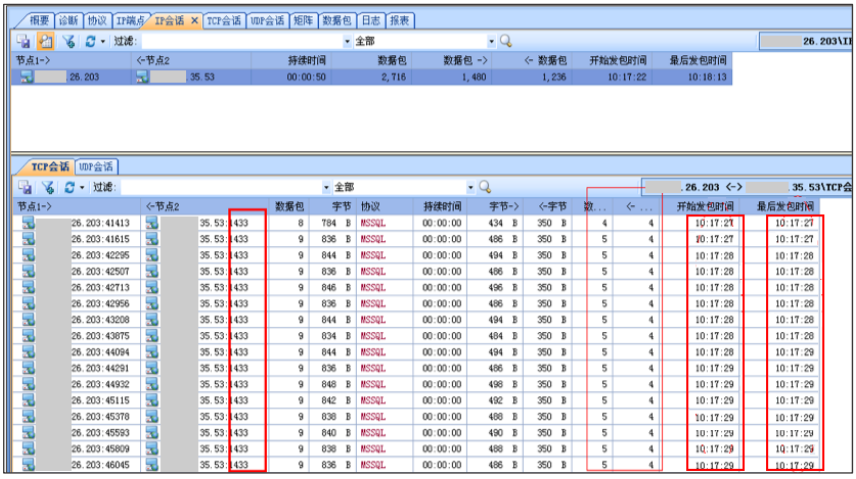

图　11-3

通过查看 IP 会话列表，发现 X.X.26.203 与 X.X.35.53（数据库服务器）的通讯规律：向数据库发送 5 个小数据包并接收 4 个小数据包，通讯时间短暂且频率极快。而正常的数据库通讯规律具有数据包偏大、通讯时间较长、通讯频率较慢的特征。

该异常现象可能是外网用户攻击数据库所导致，攻击者通过 MSSQL 的 1433 号端口，不断利用弱口令尝试获取目标主机的控制权限。为了进一步验证判断，科来网络分析工程师开始查看 TCP 会话的数据流，如下图所示。

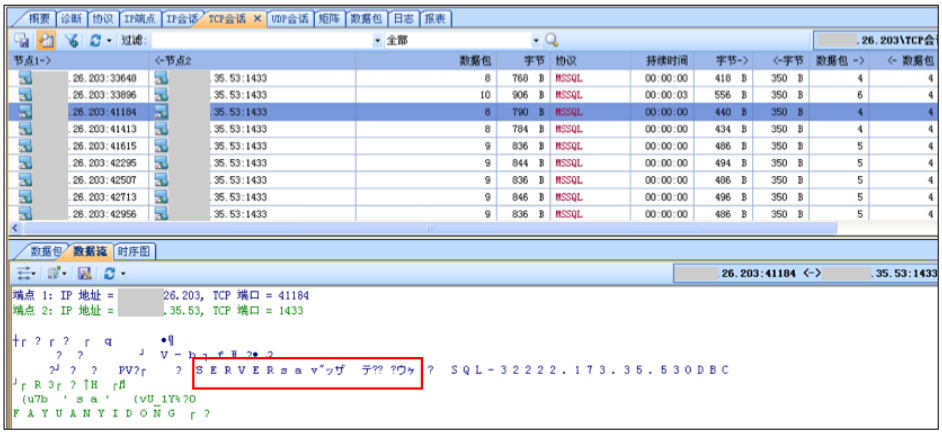

图　11-4

该 IP 地址对 SQL SERVER 的每次会话扫描，报文长度均在 8 到 10 字节之间，选择其中一个会话查看数据流，发现攻击者果真在尝试 sa 口令。

图　11-5

如上方 TCP 会话时序图所示，双方会话建立成功后通讯数据很少，服务器在回应对方的尝试后，立刻终止了此会话。通过仔细查看 300 多个会话内容，推测这些尝试并没有成功。

由此断定数据库服务器（X.X.35.53）外网地址遭到攻击。科来网络分析工程师在与网络管理员沟通后，得知该地址确实是数据库的外网地址。出于安全考虑，用站长工具对各端口进行扫描，查看在网络中还有哪些端口是开放状态，如下图所示。

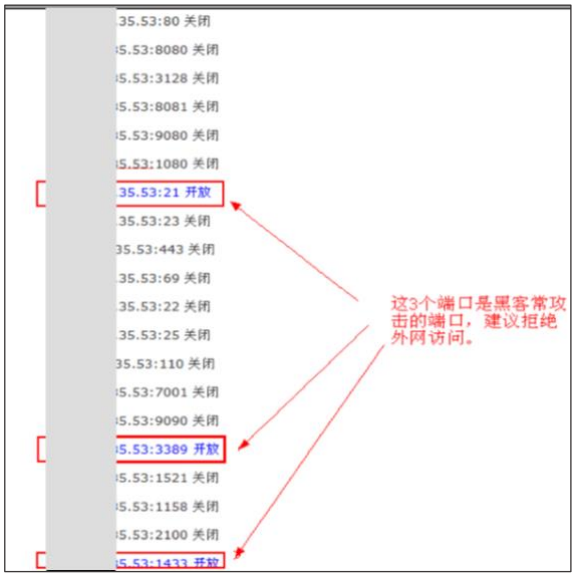

图　11-6

共计发现 3 个端口处于开放状态（端口 21、1433、3389），同时这三个端口也是黑客经常攻击的端口。

通过登录站长工具查看，发现 X.X.26.203 是韩国的地址。

图　11-7

然后对该地址进行一次端口扫描，如下图所示。

图　11-8

其 3389 端口也处于开放状态，随后尝试远程登录。

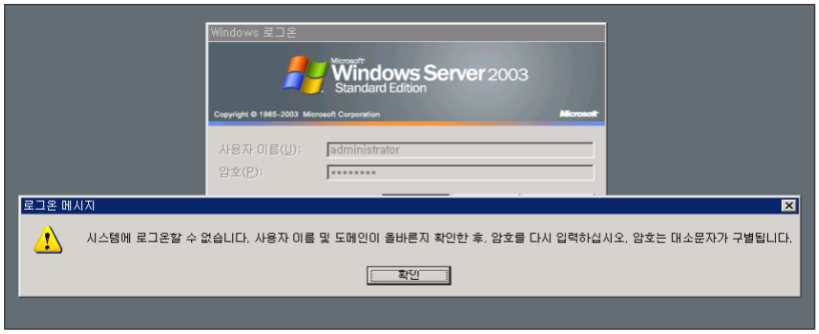

图　11-9

对话框中显示“输入的用户名或密码不正确，请重新输入”。

11.3　分析结论

端口扫描是网络中较为常见的行为之一，端口扫描是指向每个端口发送消息，一次只发送一个消息。按照回应信息类型判断端口是否可使用，并由此探寻弱点。网络管理员通过端口扫描，可以得到许多有用的信息，从而发现系统的安全漏洞，然后修补漏洞、制定完善的安全策略。然而这种行为也由可能是黑客为攻击网络设备所迈出的第一步。

由于此次抓包时间较短，未能完全将黑客的行为及结果分析透彻。如果黑客继续攻击，就有可能成功破解数据库密码，给用户带来不可估量的损失。因此，

建议网络管理员在防火墙上做安全策略，拒绝外网用户访问 MS SQL 的 1433 端口，只对内部网络用户开放。另外，FTP 的 21 端口和远程登录的 3389 端口，也应拒绝外网访问或者干脆关掉。

11.4 价值

数据库一直都是攻击者的重点关注目标，然而攻击者无论采用何种共计手段，我们都可以通过网络流量分析技术及时发现问题，定位问题原因，找出其利用的漏洞并及时更新补丁，避免出现数据被泄漏而无感知的情况。

科来网络流量分析解决方案

科来业务性能解决方案

- 科来业务性能管理系统(UPM)
- 科来网络回溯分析系统(RAS)
- 科来网络分析系统(CSNAS)

科来网络安全分析解决方案

- 科来大数据安全态势感知平台(BAP)
- 科来网络全流量安全分析系统(TSA)
- 科来APT攻击检测系统(APT)

CSNA 网络分析认证培训

课程介绍

培训报名

科来网络流量分析技术资料

网络攻击与防范图谱

科来网络通讯协议图

科来网络故障诊断图

CSNA 网络分析经典实战案例

数据包样本

网络分析过滤器

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