路由器抓包分析之SMB篇

白帽技术与网络安全 昨天

以下文章来源于边界骇客 ，作者查鲁特

边界骇客

物理安全/边界安全但凡网络被骗，网上赌博请报警，不要相信任何一个黑客会帮你解决...

前言

近期路由器等边界设备漏洞频发，正好过来蹭一波热度。边界设备作为网络中必不可少的一部分，但其安全性却一直没有受到大家的重视，其原因归结为两点：1.作为硬件设备即使发现漏洞了厂家没发布补丁，自己无法修补，甚至一些硬件漏洞连厂家也修补不了。2.管理员不重视，往往能正常运行就不去管它了，有的甚至连初始密码都没更改。

0×01

当我们通过各种姿势（zoomeye，shodan两大硬件设备的大杀器）拿下一台路由器或者防火墙时，我们下一步该怎么做呢？答案当然是根正苗红的我们绝不会拿下一台路由器或者防火墙，因为入侵时违法的。即使发现了也应及时跟厂商或者所有者联系。但是一些恶势力并不这么想，他们肯定为了利益最大化会进行下一步的内网拓展。

正所谓**未知攻，焉知防。**现在就让我们站在邪恶势力的角度上想想下一步应该怎么做？毫无疑问，抓包进行流量监听是一个安全高效的方法。既可以知道管理员在上班的时候都上了哪些羞羞的网站，也可以探测管理员的密码。

0X02

现在的路由器/防火墙普遍自带抓包功能，如tcpdump,端口镜像，自带的抓包工具等等.....既然要探测密码首选当然是抓明文包，如：FTP,HTTP,SMTP,POP3等，由于密码是明文传输，就没啥好说的了，下面通过一个实验给大家讲讲SMB的抓包分析。

试验环境：

> windows xp(smb server)　　192.168.0.2
>
> window7(client)　　192.168.0.1
>
> 路由器/防火墙　　无数据省略
>
> 实验基础知识：既然要对SMB进行抓包分析，首先我们要了解下SMB的认证过程。

> SMB认证过程：（网上总结的很好，比较懒就直接复制了）

1.正常情况，当client端登陆时需要先输入username，password和domain[默认是.，表示本地]，之后client端会自己计算出password用DES加密后的hash，并将此hash暂时保存在本地；

2.接着，client端会将自己的username明文发送给DC[server]；

3.此时，DC会生成一组8字节的随机数，也叫challenge[挑战码]，返回给client端；

4.当client端在收到这个挑战码以后，会把先把它拷贝一份出来，然后再拿着这个挑战码和之前已经加密的密码hash再进行一次加密，加密后的东西叫response[响应]，最后再将challenge，response和username一并发送给server端；

5.server端在接收到client端传过来的这个三个值以后会将它们分别都转发给DC；

6.DC在接收到username，response，challenge以后，会根据传过来的username，到自己的账号数据库中去查出来这个username所对应的hash，然后，再拿着这个hash和刚刚传过来的challenge再进行一次加密；

7.最后，就剩比对了，把客户端传过来的response和在[6]中最后加密的hash值进行对比，如果一致，ok，认证通过，登录成功，反之，则登录失败。

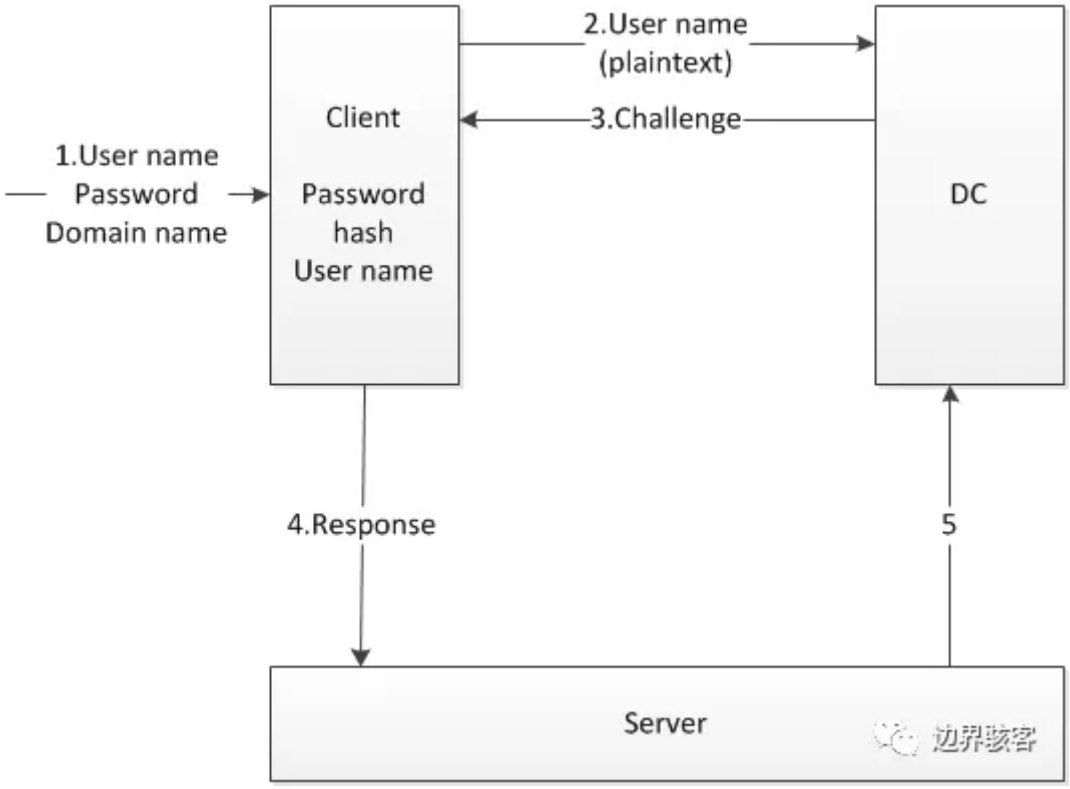

图1:SMB原理图

为了节省篇幅，直接省略抓包等一系列操作，我们用wireshark打开已经抓到的数据包文件，如下图所示着重看下认证过程的3，4两步。

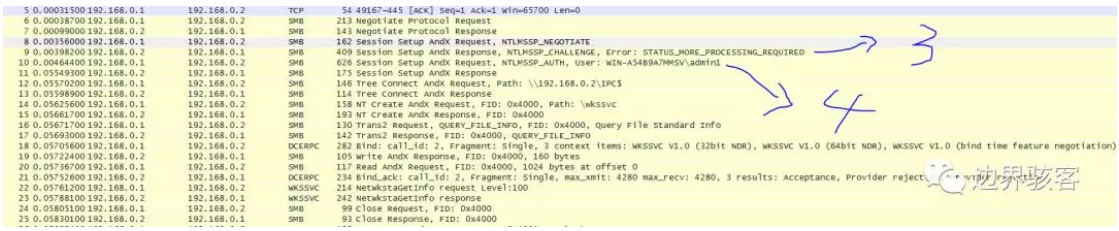

图2:SMB认证抓包

如图2所示所示第4步会把系统原密码hash通过username，domain以及challenge（挑战值）这三个变量进行一些列运算生成N**et-ntlm**。然后发给服务器进行验证。什么是Net-ntlm呢？Net-ntlm分为两个版本既Net-nlmv1和Net-ntlmv2。（下面将对两个协议版本分别抓包分析）

Net-ntlm v1：NTLM协议在服务器和客户端之间的挑战/响应中使用NTHash。该协议的v1使用NT和LM哈希，具体取决于配置和可用的内容。v1已弃用，但仍可能在网络中的某些旧系统中使用。

图3：Net-ntlmv1数据包

固定拼接：

```
username::hostname:LM response:NTLM response:server challenge
```

如图：Net-ntlmv1s数据包拼接结果为：

```
admin1::WIN-hostname:5216722df4f219ee0000000000000000000000000000000000000000:705c7b5ce32e8d
172da9a2e95f6a1bef5ad04a089c42ad7b:c0ba0570a01b8888
```

Net-ntlm v2：这是NTLM协议的新改进版本，这使得它更难以破解。这个概念与NTLMv1相同，只是发送给服务器的算法和响应不同。也通过Responder或类似的方式捕获。自Windows 2000以后在Windows中默认。

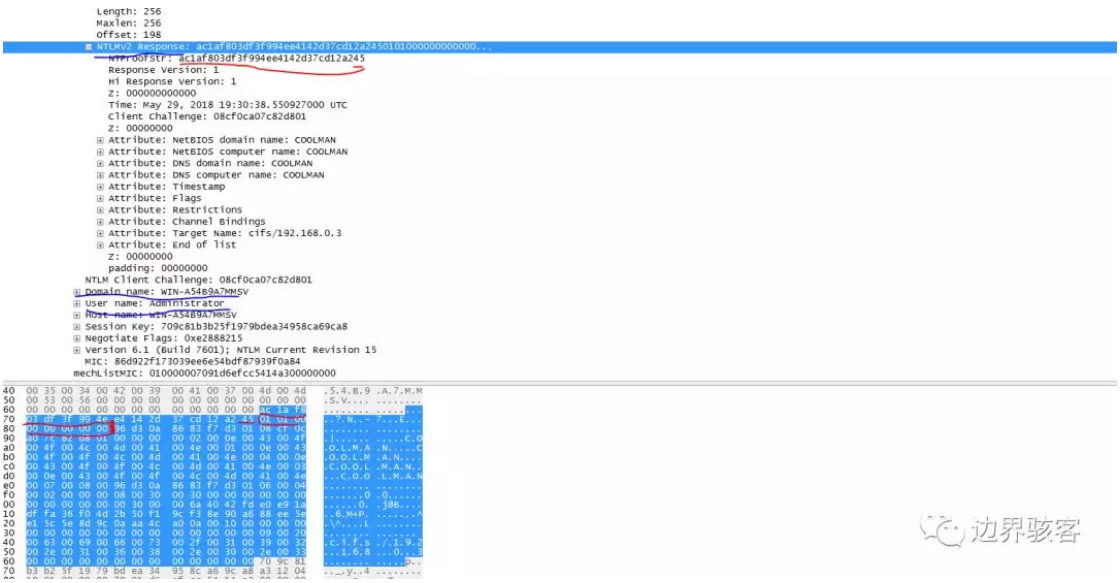

图4：Net-ntlmv2数据包

固定拼接：

username::domain:server **challenge**:ntproofstr+固定位（红色框起来的）:ntlmv2response剩下的

如图:Net-ntlmv2数据包拼接结果为（下划线为固定位）：

```
Administrator::WIN-hostname:fb0330631bd6dd58:ac1af803df3f994ee4142d37cd12a2450101000
000000000:96d30a8683f7d30108cf0ca07c82d80100000000002000e0043004f004f004c004d0041004e
0001000e0043004f004f004c004d0041004e0004000e0043004f004f004c004d0041004e0003000e0043
004f004f004c004d0041004e000700080096d30a8683f7d3010600040002000000080030003000000000
0000000000000000003000006a4042fde0e91adffa36f04d2b50f19cf38e90a688ee5ee15c5e8d9c0aaa4c
a00a001000000000000000000000000000000000000900200063006900660073002f003100390032002e
003100360038002e0030002e00330000000000000000000000000000
```

最后我们把两个拼接结果扔进hashcat就可以跑出密码了。

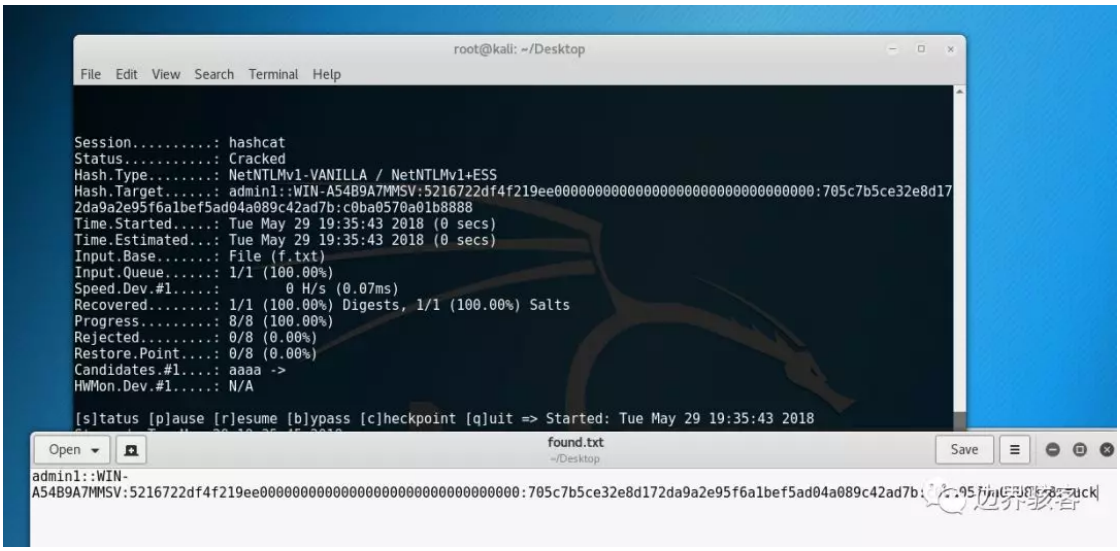

图5：hashcat结果