Windows 名称解析机制探究及缺陷利用

her0in / 2017-12-07 14:27:00 / 浏览数 3068

本文作为一篇科普文章，阐述了 Windows 系统中的名称解析机制，同时也提及了几种利用名称解析机制的缺陷进行内网攻击的方式。

0x00 Windows 名称解析简介

TCP 协议的通信是基于 IP 地址的，“名称解析”就是把需要访问的计算机的名字解析为 IP 地址的过程。

Windows 中的名称类型

在 Windows 操作系统中，有两种名称，分别为：主机名称 和 NetBIOS 名称。

主机名称

从狭义上来说，主机名称正如它的字面意思一样就是一台主机的名字。从广义来说，它又不仅仅包含计算机的名字，也包含互联网中的域名。

由于域名是以树状的形式所表现的，同时也是主机名称的一种，所以主机名称是有层次的，最大长度为 255 个字符，允许的字符有 A～Z，a～z 和字符“ - ”。在域名系统中有一种标识一台主机的 DNS 名字的域名叫做 完全限定域名（FQDN），FQDN 是由“.”连接主机名字和主域名后缀组合成的，例如，seclab.her0in.org 的 FQDN 名称就是 seclab 。

NetBIOS 名称

在 Windows 系统中的另外一种名称就是 NetBIOS 名称，准确的说 NetBIOS 名称并非是一种名字系统，而是 Windows 操作系统网络的一个编程接口，允许主机之间使用 NetBIOS 名称进行通信，通信过程是建立在 NetBIOS 协议之上的。在安装完 Windows 系统后系统会默认使用计算机的名字做为当前主机的 NetBIOS 名称。它的最大长度为 16 个字符，其中最后一位是不可配置的，用于指定 NetBIOS 的服务类型。如果计算机名称不足 15 位则使用空格补全到 15 位，反之，如果计算机名称超过 15 位 则会截取前 15 位。常见的 NetBIOS 后缀有 0x20（文件和打印服务）、0x00（工作站服务）、0x03（报信者服务）等。

使用`nbtstat -n`命令查看本机的 NetBIOS 名称。

使用`nbtstat -A ipaddress`命令查看指定 IP 主机的 NetBIOS 名称。

0x01 Windows 名称解析相关协议

在 Windows 系统中有三种与名称解析相关的协议。

Windows 名称解析之 DNS协议

DNS 协议是一种最主要的也是操作系统首选的进行名称解析的协议，几乎每一种操作系统都支持 DNS 协议，同时， DNS 协议支持 IP v4 和 IP v6。DNS 协议在实现名称解析的过程中，在客户机上没有任何本地的数据库文件，完全依赖于 DNS 服务器，所监听的端口是 UDP/53 。在客户机上可以使用`ipconfig /displaydns`命令来查看本机的 DNS 缓存，使用`ipconfig /flushdns`命令清除本机的 DNS 缓存。

DNS 的名称解析过程如下：

- 读取本机 DNS 缓存（已经包含本机 hosts 文件内容）
- 如果缓存中没有，则会请求网络配置中配置的 DNS 服务器
- 如果 DNS 服务器未作出响应，则请求失败。反之，DNS 服务器则会处理用户请求。

Windows 名称解析之 NetBIOS 协议

除了 DNS 之外，在早先版本的 Windows 中也使用 NetBIOS (network basic input/output system，网络基本输入输出系统)进行名称解析。本文介绍的 NetBIOS 协议名称解析是微软后来定义的 nbt 即 NetBIOS over TCP/IP 的名称解析类型。

nbt 服务监听的端口为 UDP/137，其进行名称解析的形式为向当前主机所在的子网域发送广播包。所以，当你使用抓包工具在局域网中抓包时总会收到很多 NBNS 数据包。

由于 NetBIOS 协议进行名称解析是发送的 UDP 广播包。这样做虽然速度快且无需额外的配置，但是广播包不能跨越网域同时也会增加一些网络流量，因此微软在后来推出了 WINS（Windows Internet Name Service）服务器，当计算机配置为使用 WINS 服务器进行名称解析时，客户机将直接和 WINS 服务器进行单播通讯，这样就可以弥补 NetBIOS 协议使用广播进行名称解析的不足。

综上所述，NetBIOS 协议进行名称解析的过程如下：

- 检查本地 NetBIOS 缓存
- 如果缓存中没有请求的名称且已配置了 WINS 服务器，接下来则会向 WINS 服务器发出请求

- 如果没有配置 WINS 服务器或 WINS 服务器无响应则会向当前子网域发送广播
- 如果发送广播后无任何主机响应则会读取本地的 lmhosts 文件

lmhosts 文件位于`C:\Windows\System32\drivers\etc\`目录中。

使用`nbtstat -c`命令查看本机的 NetBIOS 缓存

使用nbtstat -R命令清除本机的 NetBIOS 缓存

Windows 名称解析之 LLMNR 协议

DNS 协议的名称解析虽然高效但是需要在局域网中单独配置一台服务器作为 DNS 服务器，NetBIOS 协议的名称解析在一些情况下也需要单独配置一台 WINS 服务器，而且 NetBIOS 协议不支持 IP v6。因此，为了弥补这些不足，微软在 Windows Vista 之后推出了基于端到端的名称解析协议 —— 本地链路多播名称解析（Link-Local Multicast Name Resolution）简称为 LLMNR。

LLMNR 也称作多播 DNS ，因为其数据包格式类似于 DNS 的数据包。监听的端口为 UDP/5355，支持 IP v4 和 IP v6 ，并且在 Linux 上也实现了此协议。其解析名称的特点为端到端，IPv4 的广播地址为 224.0.0.252，IPv6 的广播地址为 FF02:0:0:0:0:0:1:3 或 FF02::1:3。

LLMNR 进行名称解析的过程为：

- 检查本地 NetBIOS 缓存
- 如果缓存中没有则会像当前子网域发送广播
- 当前子网域的其他主机收到并检查广播包，如果没有主机响应则请求失败

0x02 Windows 系统名称解析顺序

影响 Windows 系统名称解析的两个因素

操作系统版本

从上述一小节中，可以发现，并非所有的操作系统版本都支持上述三种协议。

Windows 2K，XP，2K3 只支持 DNS 和 NetBIOS。 所以此类版本的 Windows 都是先进行 DNS 名称解析，如果 DNS 解析名称失败，才会进行 NetBIOS 名称解析。

Windows Vista 之后（包括 2K8 ， Win7，Win8.x，Win 10）都支持上述三种协议，在这类 Windows系统中的名称解析顺序为：先进行 DNS 名称解析，如果 DNS 解析名称失败，则会使用 LLMNR 进行名称解析，最后才会使用 NetBIOS 名称解析。

网络节点模式

还有一种影响 Windows 系统名称解析的一个因素就是当前主机的网络节点模式。可以使用`ipconfig /all`命令查看本机的网络节点模式，如下图：

图 1 查看本机网络节点模式

网络节点模式最主要会影响 NetBIOS 名称解析过程，是优先查询 WINS 服务器还是先在子网域中进行广播。具体的及节点模式描述如下：

1. B-节点(broadcast，广播)

Windows 使用广播来进行名称注册和名称解析，依据网关的配置，一个 B 节点客户机发送的数据包不能够超出局域网的范围。但是，B 节点并不适合于大型网络，实际上微软修改了标准的 B 节点类型，当 Windows 尝试解析名称时，首先检查 LMHOSTS 名称缓存，如果此行不通，Windows 就会发送广播，如果广播依然失败的话，那Windows 才会检查实际的 LMHOSTS 文件。

1. P-节点(per-to-per，对等)

这种方法并不使用广播，而是在计算机启动时，在网络中的 WINS 服务器上注册它们的名称，当计算机需要解析名称时，它会发送一个解析请求给 WINS 服务器。这种方法只在 WINS 服务器正常运行时有效，如果 WINS 服务器失败，则无法进行名称解析。

1. M-节点(mixed，混合)

Windows 联合使用 B 节点和 P 节点，并且默认使用 B 节点，如果 M 节点不能利用广播进行名称解析，它就使用 P 节点的 WINS 服务器来完成工作。

1. H-节点(hybrid，混合)

同样也是联合使用 B 节点和 P 节点，但工作方式相反，如果使用 WINS 服务器方式不能成功，则使用 B 节点的工作来完成工作。此节点模式也是目前 Windows 系统默认使用的节点模式。

0x03 利用 Windows 名称解析机制的缺陷进行内网攻击

常见的利用 Windows 名称解析机制的缺陷进行攻击的技术有 DNS Spoof ，NBNS Poison ，LLMNR Poison ， ICMP Redirection。

可以使用 SpiderLabs 出的 Responder，或者 ZARP 工具包进行上述攻击。

LLMNR Poison 攻击环境如下：

- 攻击者主机（Linux）IP 192.168.237.133
- 受害者主机（Windows 8.1） IP 192.168.237.129
- 两台主机处于同一个局域网中

攻击者在启动 Responder 后，当受害者去访问一个在当前局域网中不存在的主机时就会触发 LLMNR Poison 攻击，如下图所示：

图 1 ： 受害者主机 PING 一台局域网中并不存在的主机

图 2 ：Responder 会响应 LLMNR 的广播包并进行了 Poison 攻击

图 3 ：在受害者的主机中 NetBIOS 缓存中已经加入了被 Poison 攻击的主机 IP 记录

上述攻击演示中，已经证实了 LLMNR Poison 攻击的效果，可以利用让受害者访问不存在的主机的共享进行 LLMNR Poison 攻击，这样可以获得受害者主机的 HASH ，拿到 HASH 就可以进行暴力破解了，如果是弱口令的话，就可以爆破出密码。同样也可以利用让受害者访问不存在的 HTTP 服务器进行 401 认证拿到客户端的 HASH，如下图所示：

图 4 ：受害者访问一个不存在的主机的共享

图 5 ：LLMNR Poison 攻击拿到了 SMB 验证过程中的 HASH

图 6 ：使用 john 对 HASH 进行暴力破解

0x04 参考及引用

https://support.microsoft.com/en-us/kb/119493
https://en.wikipedia.org/wiki/Link-Local_Multicast_Name_Resolution
https://support.microsoft.com/en-us/kb/163409
https://support.microsoft.com/en-us/kb/160177
http://read.newbooks.com.cn/info/132528.html

上一篇：WPAD 协议分析及内网渗透利用 下一篇：二级、三级云等保租户方

1. 2 条回复

evi1ox 2017-12-10 13:00:54

想问一句.这里如果在内网.通过Responder 获取到其他计算机的hash时.[包含域管或者dc].是否可以通过这个hash进行注入呢???

0 回复Ta


sudo 2017-12-18 16:14:45

@evi1ox
不可以，netntlmhash只能破解或者relay

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板