2.14　域渗透分析工具 BloodHound

BloodHound 是一个免费的工具。BloodHound 以用图与线的形式将域内用户、计算机、组、会话、ACL 及域内所有相关用户、组、计算机、登录信息、访问控制策略之间的关系直观地展现在 Red Team 成员面前，更便捷地分析域内情况，更快地在域内提升权限。BloodHound 也可以使 Blue Team 成员对己方网络系统进行更好的安全检测，以及保证域的安全性。BloodHound 使用图形理论，自动化地在 Active Directory 环境中理清大部分人员之间的关系和细节。使用 BloodHound，可以快速地深入了解 AD 中的一些用户关系、哪些用户具有管理员权限、哪些用户有权对任何计算机都拥有管理权限，以及有效的用户组成员信息。

BloodHound 通过在域内导出相关信息，在将数据采集后，将其导入本地安装好的 Neo4j 数据库中，展示和分析域内所需相关信息。Neo4j 是一款 NoSQL 图形数据库，它将结构化数据存储在网络上而不是表中。Bloodhound 正是利用这种特性加以合理分析，更加直观地以节点空间的形式来表达相关数据。Neo4j 就像 MySQL 或其他数据库一样，有自己的查询语言 Cypher Query Language。因为 Neo4j 是一款非关系型数据库，要想用它查询数据，同样需要自己独特的语法。

2.14.1　安装 BloodHound 所需环境

首先，准备一台安装有 Windows Server 操作系统的机器。为了方便、快捷地使用 Neo4j 的 Web 管理界面，推荐安装 Chrome 或火狐浏览器。

Neo4j 数据库需要 Java 环境才能运行。从 Oracle 官方网站下载 JDK Windows x64 安装包并安装，如图 2-86 所示。

Java SE Development Kit 8u191

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.
Thank you for accepting the Oracle Binary Code License Agreement for Java SE; you may now download this software.

Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	72.97 MB	jdk-8u191-linux-arm32-vfp-hflt.tar.gz
Linux ARM 64 Hard Float ABI	69.92 MB	jdk-8u191-linux-arm64-vfp-hflt.tar.gz
Linux x86	170.89 MB	jdk-8u191-linux-i586.rpm
Linux x86	185.69 MB	jdk-8u191-linux-i586.tar.gz
Linux x64	167.99 MB	jdk-8u191-linux-x64.rpm
Linux x64	182.87 MB	jdk-8u191-linux-x64.tar.gz
Mac OS X x64	245.92 MB	jdk-8u191-macosx-x64.dmg
Solaris SPARC 64-bit (SVR4 package)	133.04 MB	jdk-8u191-solaris-sparcv9.tar.Z
Solaris SPARC 64-bit	94.28 MB	jdk-8u191-solaris-sparcv9.tar.gz
Solaris x64 (SVR4 package)	134.04 MB	jdk-8u191-solaris-x64.tar.Z
Solaris x64	92.13 MB	jdk-8u191-solaris-x64.tar.gz
Windows x86	197.34 MB	jdk-8u191-windows-i586.exe
Windows x64	207.22 MB	jdk-8u191-windows-x64.exe

图 2-86　下载 JDK

在 Neo4j 官方网站的社区服务版模块中选择“Windows”选项，并下载最新的 Neo4j 数据库安装包（写作本书时的最新版为 3.5.1），如图 2-87 所示。

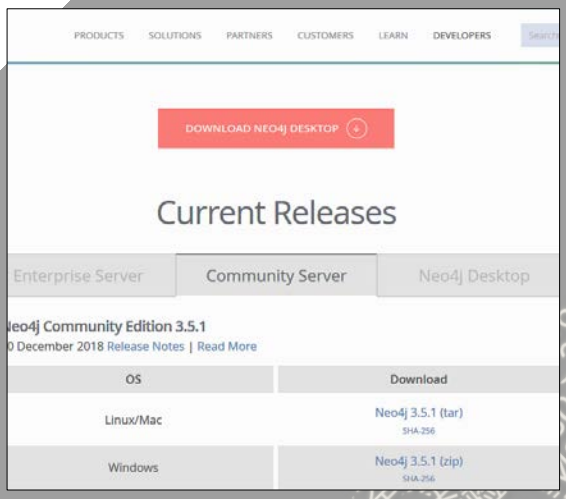

图 2-87　选择系统下载 Windows 版 Neo4j 数据库

下载完成并解压，打开 cmd 窗口，进入解压后的 bin 目录。在 cmd 下输入命令“neo4j.bat console”，启动 Neo4j 服务，如图 2-88 所示。

```
C:\neo4j-community-3.5.1-windows\neo4j-community-3.5.1\bin>neo4j.bat console
2019-01-11 13:18:07.959+0000 INFO  ======== Neo4j 3.5.1 ========
2019-01-11 13:18:07.974+0000 INFO  Starting...
2019-01-11 13:18:12.365+0000 INFO  Bolt enabled on 127.0.0.1:7687.
2019-01-11 13:18:13.755+0000 INFO  Started.
2019-01-11 13:18:14.599+0000 INFO  Remote interface available at http://localhost:7474/
```

图 2-88　在本地启动 Neo4j 服务

看到服务成功启动的提示后，打开浏览器，输入地址“http://127.0.0.1:7474/browser/”。打开页面后，输入账号和密码，如图 2-89 所示。

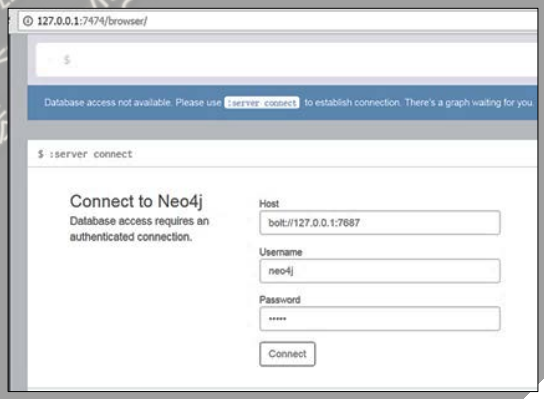

图 2-89　登录并修改 Neo4j 密码

Neo4j 默认的配置信息如下。

- Host：http://127.0.0.1:7474。
- User：neo4j。
- Password：neo4j。

输入完成后，提示修改密码。在这里，为了方便演示，将密码修改为“123456”。

在 GitHub 的 BloodHound 项目中提供了其 Release 版本，下载地址为 https://github.com/BloodHoundAD/BloodHound/releases/download/2.0.4/BloodHound-win32-x64.zip。读者也可以选择下载源代码自己构建。在这里，选择直接下载 Release 版本，如图 2-90 所示。

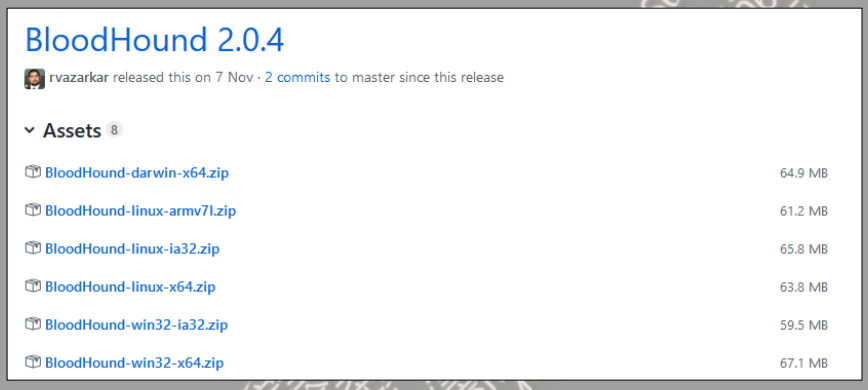

图 2-90　下载 BloodHound

下载完成后进行解压，进入目录，找到 BloodHound.exe，双击运行，如图 2-91 所示。

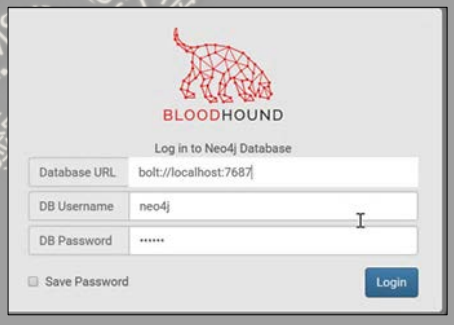

图 2-91　在本地运行 BloodHound

- Database URL：bolt://localhost:7687。
- DB Username：neo4j。
- DB Password：123456。

输入以上信息后，单击“Login”按钮，进入 BloodHound 主界面，如图 2-92 所示。

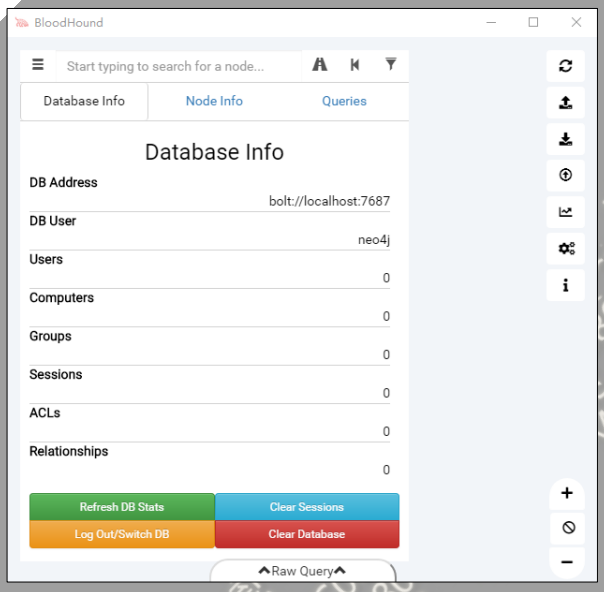

图 2-92　BloodHound 主页面

现在，Bloodhound 已经安装成功了。

左上角是菜单和搜索栏，三个选项分别是数据库信息、节点信息和查询模块。在数据库信息栏，可以显示所分析域的用户数量、计算机数量、组数量、会话数量、ACL 数量、关系。还可以在此处执行基本的 DB 管理功能，包括注销和切换 DB，以及清除当前加载的 DB。

“node Info”选项卡将显示用户在图表中单击的节点的信息。“Queries”选项卡将显示用户 BloodHound 中包含的预构建查询，以及用户可以自己构建的其他查询。

在右上角设置区域：第一个是刷新功能，BloodHound 将重新计算并重新绘制当前显示；第二个导出图形功能，可以将当前绘制的图形导出为 JSON 格式或者 PNG 格式；第三个是导入图功能，BloodHound 将以 JSON 格式绘制导入的图形；第四个是上传数据功能，BloodHound 将进行自动检测，然后获取 CSV 格式的数据；第五个是更改布局类型功能，在分层（Dagre）和强制定向图布局之间切换；第六个是设置功能，可以更改节点折叠行为，并在低细节模式之间切换。

2.14.2　采集数据

使用 BloodHound 进行分析，需要来自 Active Directory 环境的三条信息，具体如下。

- 哪些用户登录了哪些机器？
- 哪些用户拥有管理员权限？
- 哪些用户和组属于哪些组？

BloodHound 所需要的三条信息严重依赖于 PowerView.ps1 脚本的 BloodHound。BloodHound 分为两个版本，一个是 PowerShell 采集器脚本（有两个版本，旧版本叫作 BloodHound_Old.ps1，新版本叫作 SharpHound.ps1），另一个是 exe 可执行文件 SharpHound.exe。在大多数情况下，收集此信息不需要系统管理员权限，如图 2-93 所示。

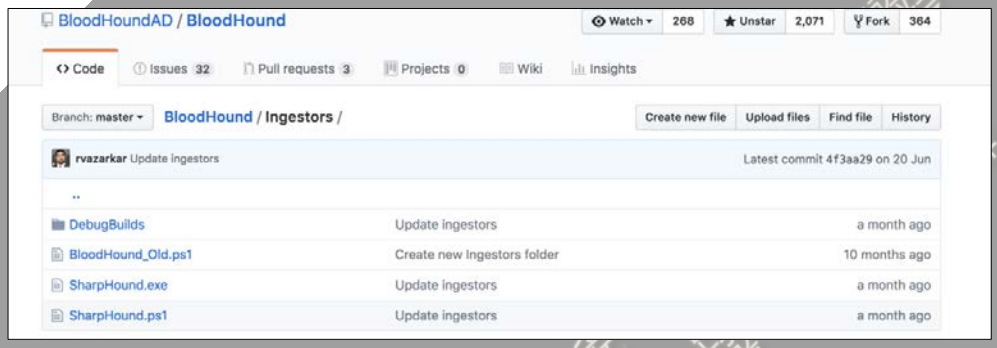

图 2-93　下载数据采集脚本

BloodHound 的下载地址如下。

- https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.ps1
- https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/BloodHound_Old.ps1
- https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.exe

使用 SharpHound.exe 提取域内信息。将 SharpHound.exe 复制到目标系统中，使用 Cobalt Strike 中的 beacon 进行无图形化操作，输入如下命令，如图 2-94 所示。

```
SharpHound.exe -c all
```

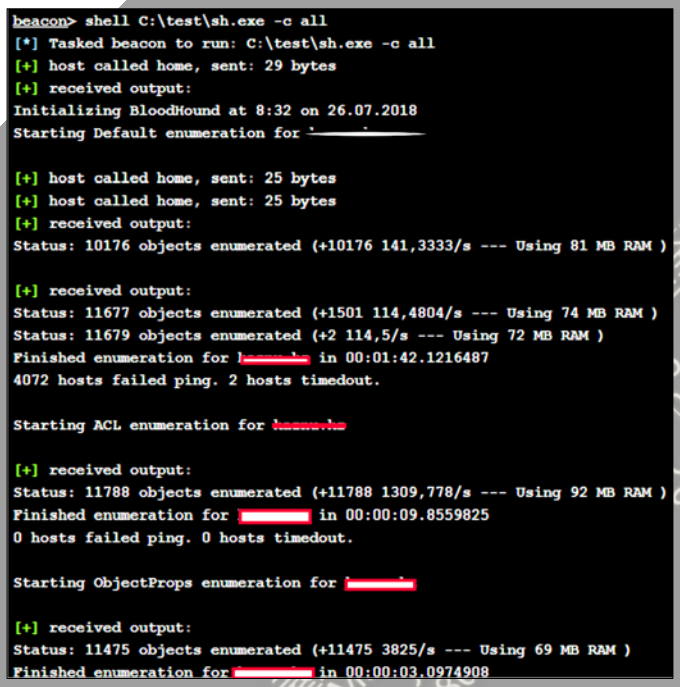

图 2-94　运行数据采集器采集数据

2.14.3　将数据导入 BloodHound

在 beacon 的当前目录下，会生成类似“20181222230134_BloodHound.zip”格式的压缩包。BloodHound 界面支持单个文件或者 Zip 文件的上传，最简单的方法是将压缩文件放到用户界面上除了节点显示选项卡的任何位置。上传成功后，在菜单搜索栏中会出现内网的相关信息，如图 2-95 所示。

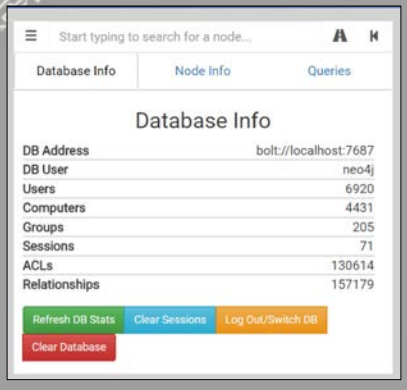

图 2-95　内网的相关信息

2.14.4　使用 BloodHound 查询信息

如图 2-95 所示，数据库中有 6920 个用户、4431 台计算机、205 个组、130614 条 ACL、157179 个关系。进入查询模块，可以看到预定义的 12 个常用的查询条件，如图 2-96 和图 2-97 所示。

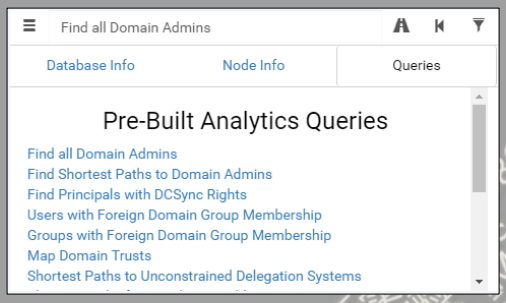

图 2-96　查看预定义的查询条件（1）

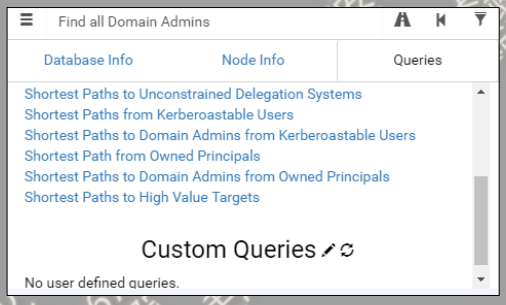

图 2-97　查看预定义的查询条件（2）

- 查找所有域管理员。
- 寻找到达域管理员的最短路径。
- 查找具有 dcsync 权限的主体。
- 具有外部域组成员身份的用户。
- 具有外部域组成员身份的组。
- 映射域信任。
- 无约束委托系统的最短路径。
- 从 KerberoAstable 用户获得的最短路径。
- 从 KerberoAstable 用户到域管理员的最短路径。
- 拥有主体的最短路径。
- 从所属主体到域管理员的最短路径。
- 高价值目标的最短路径。

1. 查找所有域管理员

单击“Find all Domain Admins”选项，选择需要查询的域名进行查询，如图 2-98 所示。BloodHound 可以帮助我们查询出当前域中有多少个域管理员。可以看到，当前域中有 15 个域管理员权限的用户。按“Ctrl”键，将循环显示默认阈值、始终显示、从不显示三个选项，以显示不同的节点标签，也可以单击并按住某个节点，将其拖动到其他位置。

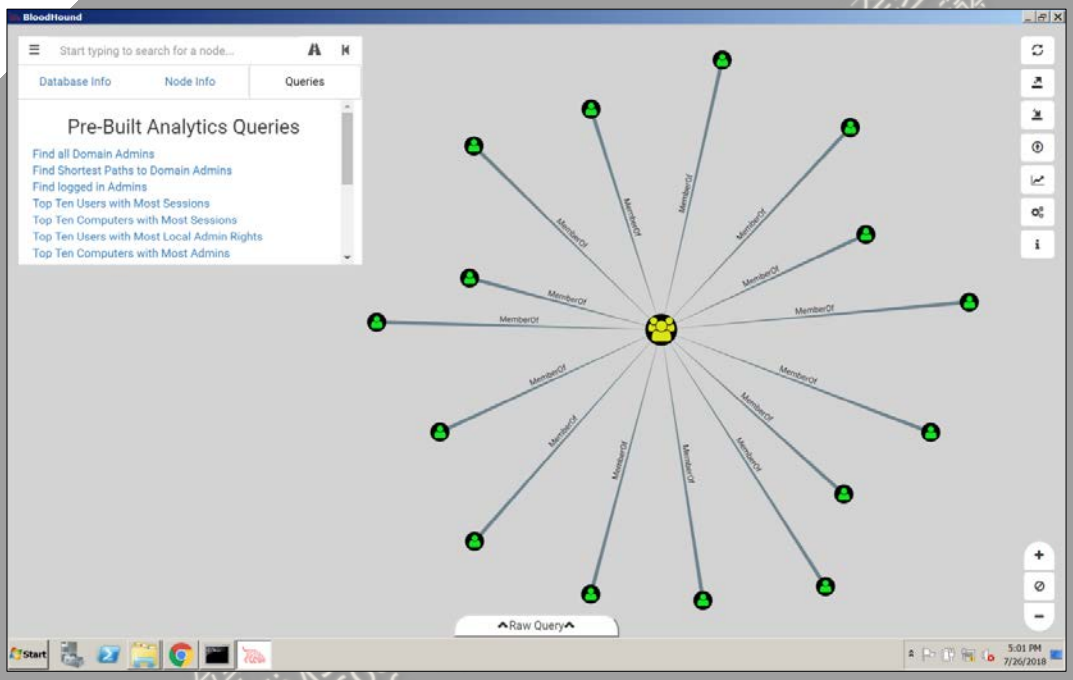

图 2-98　查找所有域管理员

2. 寻找到达域管理员的最短路径

单击“Find Shortest Paths to Domain Admins”选项，使用 BloodHound 进行分析，如图 2-99 所示。BloodHound 列出了数条路径可以到达域管理员的路径。

- 左上角为目标域管理员组，既是本次渗透测试的核心目标，也是图中的一个节点，还是所有路线的尽头。
- 左下角第一条线路上的三个用户，属于第一个节点的组，第一节点组又在第二节点组内。第二节点组对其上部的第三节点的用户具有权限，而该用户又是上一台（第四个节点）计算机的本地管理员，可以在这台计算机上拿到上面一个（第五个节点）用户的会话。该用户属于 Domain Admins 组，可以通过 PTH 方法获取域管理员和域控制器。在第三个节点分支中的用户，可以对处于第三个节点的用户强制推送策略，直接修改第三个节点用户的密

码，进而再次通过 PTH 拿下第四个节点，依此类推。

- 中间的一组，第一个节点中的三个用户为域管理员委派服务账号，可以对该域的域控制器进行 dcsync 同步，将第二个节点的用户（属于 Domain Admins 组）的散列值同步过来，进而获取域控制器权限。
- 右边的组，第一个节点的用户是第二个节点计算机的本地管理员，在该计算机上可以获得第三个节点的用户散列值。第三个节点用户又属于第四个节点的组。第四节点组是第五个节点计算机的本地管理员组，在该计算机可以获取第五个节点用户（属于 Domain Admins 组）的散列值，进而获取域控制器权限。

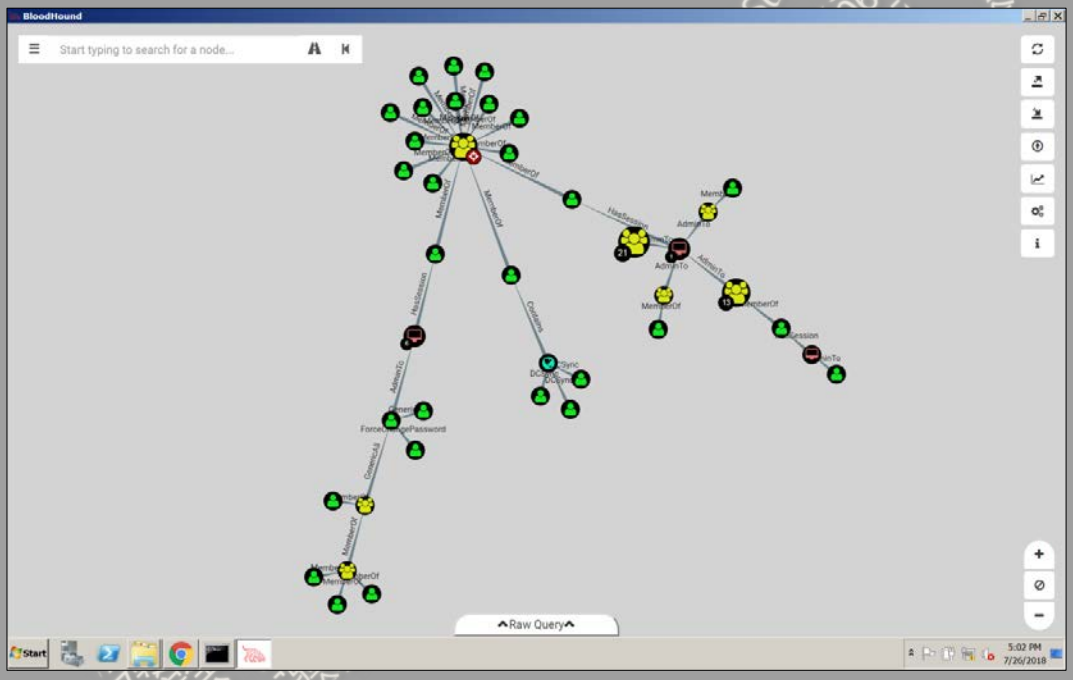

图 2-99　寻找到达域管理员的最短路径

3. 查看指定用户与域关联的详细信息

单击某个节点，BloodHound 将使用有关该节点的信息填充节点信息选项卡。在这里，单击任图中的任意节点，选择用户名，即可查看该用户的 Name、DisPlayName、最后修改密码时间、最后登录时间、该用户登录在哪台计算机上存在会话，以及是否启动、属于哪些组、拥有哪些机器的本地管理员权限和对访问对象对控制权限等。BloodHound 可以以图表的形式将这些信息展示出来，并列出该用户在域中的权限信息，方便 Red Team 成员更快地在域中进行横向渗透，提升权限，获取域管理员权限，如图 2-100 所示。

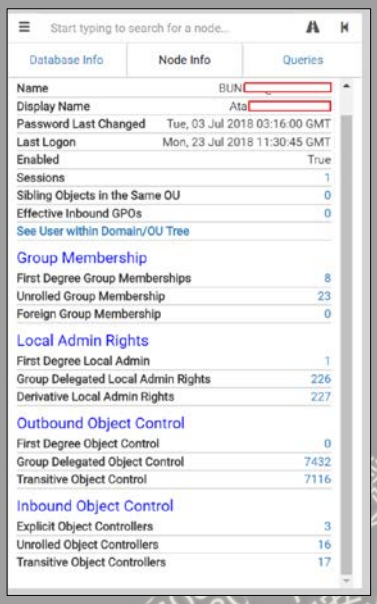

图 2-100　查询指定用户与域的关系

4. 查看指定计算机与域关联的详细信息

单击任意计算机，可以看到该计算机在域内的名称、系统版本、是否启用、是否允许无约束委托、该计算机存在多少用户的会话信息、同一个 OU 中的相似对象、在哪些域树中、存在多少个本地管理员、组关系、对 ACL 的控制权限，如图 2-101 所示。

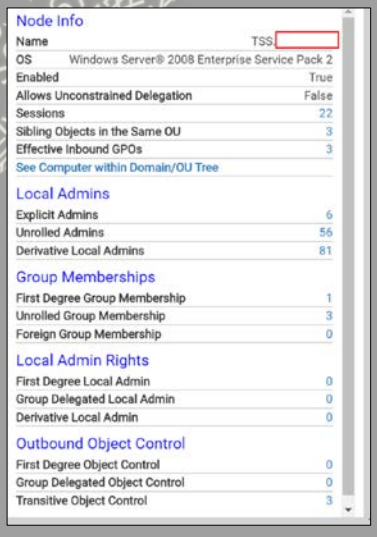

图 2-101　查询指定计算机与域的关系

5. 寻找路径

寻找路径的操作类似于导航软件。单击道路图标，会弹出目标节点文本框，在开始节点处填写 BloodHound 图中任何类型的节点，在目标节点处也填写 BloodHound 图中的任何类型的节点，接着单击播放按钮。如果存在此类路径，BloodHound 将找到所有从起始节点到目标节点之间的最短路径，然后在图形绘制区域显示具体路径，如图 2-102 所示。

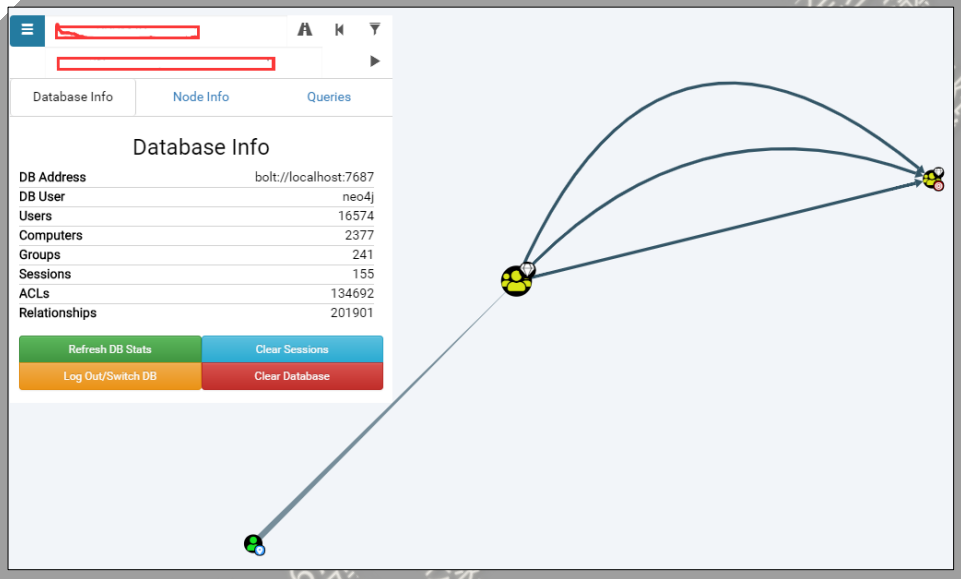

图 2-102　寻找路径关系

2.15　敏感资料、数据、文件的防护

内网的核心敏感数据，不仅包括数据库、邮件这类数据，还包括某些个人的数据、组织的各种业务数据、各种技术数据等。价值比较高的数据基本都在内网中，因此，做好内网资料数据的防护至关重要。

2.15.1　资料、数据、文件的定位流程

内网数据防护的第一步就是要熟悉渗透测试人员获取数据的流程。渗透测试人员主要通过各种渗透方法来定位公司内部各相关人员所属机器，从而获得需要的资料、数据、文件。定位的大致流程如下所示。

- 定位内部人事组织结构。
- 在内部人事组织中寻找需要监视的相关人员。
- 定位相关人员的机器。

- 监视相关人工作时存放文档的位置。
- 列出存放文档服务器的目录。

2.15.2 重点核心业务机器及敏感信息防护

重点核心业务机器是渗透测试人员通常比较关心的机器，因此需要做好相应的防护措施。

1. 核心业务机器

- 高管/系统管理员/财务/人事/业务人员的个人计算机。
- 产品管理系统服务器（仓库管理系统）。
- OA 办公系统服务器。
- 财务应用系统服务器。
- 核心产品源码服务器（对于 IT 公司，会架设自己的 SVN 或者 GIT 服务器）。
- 数据库服务器。
- 文件服务器/共享服务器。
- 邮件服务器。
- 网络监控系统服务器。
- 其他服务器（分公司、工厂）。

2. 各类敏感文件信息

- 站点源码备份文件、数据库备份文件、配置文件备份等（后缀 XX.zip，XX.sql 等）。
- 各类数据库的 Web 管理入口，如 phpmyadmin、adminer 等。
- 浏览器密码和浏览器 cookie（IE、Chrome、Firefox）。
- 其他用户会话、3389 和 ipc$连接记录、各用户回收站的信息等。
- Windows 无线密码。
- 目标内部的各种账号和密码信息，包括邮箱、VPN、FTP、TeamView 等。

2.15.4 应用与文件形式的信息收集

渗透测试人员在内网中经常会进行基于应用与文件的信息收集，包括一些应用的配置文件、敏感文件、密码、远程连接、员工账号、电子邮箱等。

总体来说，渗透测试人员对于这一步的工作，一是要了解已攻陷机器所属人员的职位（通常一个高职位的人在内网中的权限比一般员工要高，在他的计算机内也会有很多重要的、敏感的个人或公司内部文件），二是要在该机器中通过一些搜索命令来寻找自己所需要的资料。用户在内网中工作时，建议不要将一些特别重要的资料放在公开的计算机中，必要时一定要对 Office 文档进行加密，密码也不要太过于简单（对低版本的 Office 软件，如 Office 2003，在网上很容易找到一

些破解软件进行破解；对高版本的 Office 软件，也可以通过微软 Sysinternals Suite 套件中的抓取 Dump 的工具 procdump 来获取密码)。

2.16　分析域内网段划分信息及拓扑架构

在获取了内网信息后，渗透测试人员就可以分析目标的网络结构、安全防御策略，分析出网段信息、各部门的 IP 地址段，找出 IT 运维部、OA、邮箱服务器等，并尝试绘制内网的拓扑结构图了。这样，在内网定位的时候，无论是针对内网查找资料，还是针对特殊任务，都是非常实用的。

当然，渗透测试人员无法了解内网的物理结构，只能从宏观上对内网有一个整体的认识。

2.16.1　目标主机基本架构的判断

渗透测试人员要对目标网站的基本情况进行简要的判断，分析目标服务器所使用的 Web 服务器、后端脚本、数据库、系统平台等。下面列举一些常见的 Web 架构。

- ASP + Access + IIS 5.0/6.0 + Windows Sever 2003
- ASPX + MSSQL + IIS 7.0/7.5 + Windows Sever 2008
- PHP + MySQL + IIS
- PHP + MySQL + Apache
- PHP + MySQL + Ngnix
- JSP + MySQL + Ngnix
- JSP + MSSQL + Tomcat
- JSP + Oracle + Tomcat

2.16.2　域内网段划分信息

内网的环境判断，首先需要分析内网 IP 地址的分布情况。一般可以通过内网中的路由器、交换机等设备，以及 SNMP、弱口令等，来获取内网网络拓扑或 DNS 域传送的信息。一般的大公司都会有内部网站，渗透测试人员也可通过内部网站的公开链接找出部门的 IP 地址段。

内部网络是怎么划分的？是按照部门划分网段，按照楼层划分网段，还是按照地区划分网段？内网通常可分为 DMZ 区、办公区和核心区（生产区）。了解整个内网的网络分布和组成，也有助于渗透测试人员了解内网的核心业务，如图 2-103 所示。

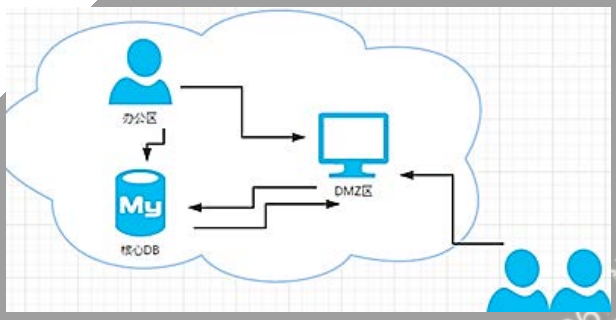

图 2-103　网络段划分

1. DMZ 区

在实际的渗透测试中，大多数情况下，在外围 Web 中拿到的权限在 DMZ 区。这个区域不属于严格意义上的内网。如果 DMZ 区域访问控制策略配置合理，DMZ 区会处在内网区能够访问 DMZ 区而 DMZ 区访问不了内网区的情况下，相关知识在第 1 章中已经详细讲解过，此处不再重复。

2. 办公区

办公区，顾名思义，是指公司员工日常的工作区。办公区的安全防护水平一般不是高，基本防护机制大多为杀毒软件或主机入侵检测产品。在实际应用中，攻击者在获取权限后，利用内网信任关系，很容易扩大攻击面。一般情况下，攻击者很少会直接到达办公区。攻击者如果想进入办公区，可能会使用鱼叉攻击、水坑攻击或者社会工程学等手段。

办公区按照系统可分为 OA 系统、邮件系统、财务系统、文件共享系统、域控、企业版杀毒系统、内部应用监控系统、运维管理系统等，按照网络段可分为域管理网段、内部服务器系统网段、各部门分区网段等。

3. 核心区

核心区一般存放企业最重要的数据、文档等信息资产，如域控制器、核心生产机器等，安全设置也最为严格。根据目标开展的业务不同，相关服务器可能存在于不同的网段上。通过分析服务器上运行的服务和进程，可以推断出目标主机使用的运维监控管理系统和安全防护系。在内网中横向移动时，会优先查找这些主机。

核心区按照系统可分为业务系统、运维监控系统、安全系统等，按照网络段可分为各不同的业务网段、运维监控网段、安全管理网段等。

2.16.3　多层域结构分析

在上述内容的基础上，可以尝试分析域的结构。因为大型企业或者单位内部的网络大都是多

层域结构，而且是多级域结构，所以，我们需要先分析出当前内网是否存在多层域、现在这计算机所在的域是几级子域、这个子域的域控制器及根域的域控制器是哪些、其他域的域控制器是哪些、域之间是否存在域信任关系等。

2.16.4　绘制内网拓扑图

通过获取的目标主机及所在域的各类信息，就可以绘制内网的拓扑结构图，在后续的渗透测试中，对照拓扑图可以更快地了解目标域网内部环境，准确定位内网具体目标，如图 2-104 所示。

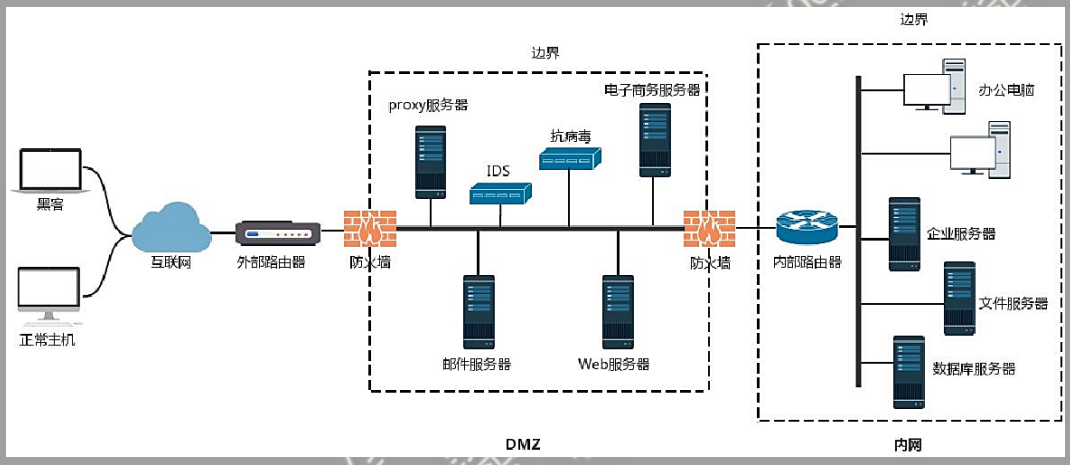

图 2-104　内网拓扑图