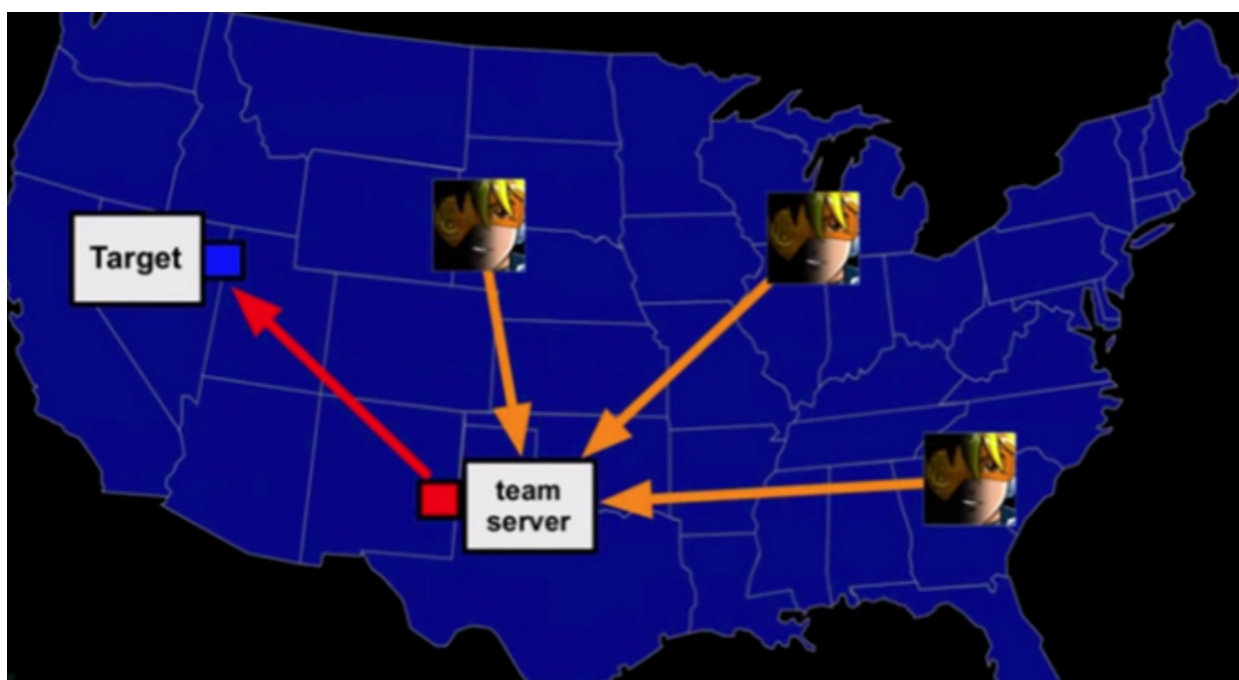


专注APT攻击与防御

<https://micropoor.blogspot.com/>

前言：

在团体渗透测试的项目中，如红蓝对抗，团队渗透测试比赛等，最重要的是过程与结果实时共享于团队，例如：A同学nmap目标站，B同学也nmap目标站，这在对抗比赛中是极其浪费时间也是非常容易引起防火墙，日志服务器或其他设备的警觉。所以打算写一系列关于未来团队渗透的对抗。争取做到过程与结果，团队实时共享。把曾经的团队作战经验形成一个适应对抗，比赛等的参考。



BloodHound简介：

BloodHound是2016年出现大家的视线中，它是一个分析和解读AD中权限关系的一个工具。对于攻击者来说，能快速的获取到域中的线索以便进行下一步攻击，而对于防御者来说，可以更快速的得知攻击者可能采取的攻击途径以及域中的可突破的途径。

项目地址：

<https://github.com/BloodHoundAD/BloodHound>

Debian上安装：

```
root@John:~# apt-get install git wget curl
```

```
root@John:~# wget -O - https://debian.neo4j.org/neotechnology.gpg.key | sudo
apt-key add
```

```
root@John:~# echo 'deb http://debian.neo4j.org/repo stable/' | sudo tee
/etc/apt/sources.list.d/neo4j.list
```

```
root@John:~# apt-get install openjdk-8-jdk openjdk-8-jre
```

```
root@John:~# apt-get install neo4j
```

```
root@John:~# echo "dbms.active_database=graph.db" >> /etc/neo4j/neo4j.conf
```

```
root@John:~# echo "dbms.connector.http.address=0.0.0.0:7474" >>
/etc/neo4j/neo4j.conf
```

```
root@John:~# echo "dbms.connector.bolt.address=0.0.0.0:7687" >>
/etc/neo4j/neo4j.conf
```

```
root@John:~# tail /etc/neo4j/neo4j.conf
```

```
# Name of the service
```

```
dbms.windows_service_name=neo4j
```

```
*****
```

```
# Other Neo4j system properties
```

```
*****
```

```
dbms.jvm.additional=-Dunsupported.dbms.udc.source=tarball
```

```
dbms.active_database=graph.db
```

```
dbms.connector.http.address=0.0.0.0:7474
```

```
dbms.connector.bolt.address=0.0.0.0:7687
```

```
root@John:~j# update-java-alternatives -l
```

```
java-1.8.0-openjdk-amd64 1081 /usr/lib/jvm/java-1.8.0-openjdk-amd64
```

```
root@John:~j# update-java-alternatives -s java-1.8.0-openjdk-amd64
```

```
下载地址 : https://neo4j.com/download/
```

```
root@John:~/Downloads# tar zxvf neo4j-community-3.3.0-unix.tar.gz
```

```
root@John:~/Downloads/neo4j-community-3.3.0/bin# ./neo4j start
```

```
Active database: graph.db
```

```
Directories in use:
```

```
home: /root/Downloads/neo4j-community-3.3.0
```

```
config: /root/Downloads/neo4j-community-3.3.0/conf
```

```
logs: /root/Downloads/neo4j-community-3.3.0/logs
```

```
plugins: /root/Downloads/neo4j-community-3.3.0/plugins
```

```
import: /root/Downloads/neo4j-community-3.3.0/import
data: /root/Downloads/neo4j-community-3.3.0/data
certificates: /root/Downloads/neo4j-community-3.3.0/certificates
run: /root/Downloads/neo4j-community-3.3.0/run
```

Starting Neo4j.

WARNING: Max 1024 open files allowed, minimum of 40000 recommended. See the Neo4j manual.

Started neo4j (pid 4286). It is available at <http://localhost:7474/>

There may be a short delay until the server is ready.

See </root/Downloads/neo4j-community-3.3.0/logs/neo4j.log> for current status.

root@John:~# apt-get install bloodhound

```
root@John:~# apt-get install bloodhound
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  finger libass5 libavdevice57 libboost-chrono1.62.0 libboost-program-options1.62.0 libboost-serializati
  libboost-timer1.62.0 libcdio-cdda2 libcdio-paranoia2 libcdio16 libcgall2 libcoin80v5 libeburl28-1 libf
  libgraphicsmagick-ql6-3 libiso9660-8 liblwgeom-2.3-0 liblwgeom-dev libopencv-calib3d2.4v5 libopencv-co
  libopencv-flann2.4v5 libopencv-highgui2.4-deb0 libopencv-imgproc2.4v5 libopencv-objdetect2.4v5 libopen
  libopenthreads20 libqca2 libqca2-plugins libqgis-core2.14.11 libqgis-core2.14.20 libqgis-customwidgets
  libqgis-networkanalysis2.14.11 libqgispython2.14.11 libqtwebkit4 libqwt6abi1 libstdl2-2.0-0 libsfcall
  libval libvcdinfo0 libx265-95 libxine2 libxine2-bin libxine2-doc libxine2-ffmpeg libxine2-misc-plugins
  python-pyspatialite python-qgis-common python-qt4-sql python-shapely qt4-designer rwho rwhod x11-apps
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  neo4j
The following NEW packages will be installed:
  bloodhound neo4j
0 upgraded, 2 newly installed, 0 to remove and 1392 not upgraded.
Need to get 115 MB of archives.
After this operation, 261 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

root@John:~/Downloads/neo4j-community-3.3.0/bin# nmap 127.0.0.1 -p 7474

Starting Nmap 7.40 (<https://nmap.org>) at 2017-12-02 11:16 EST

Nmap scan report for localhost (127.0.0.1)

Host is up (0.00011s latency).

PORT STATE SERVICE

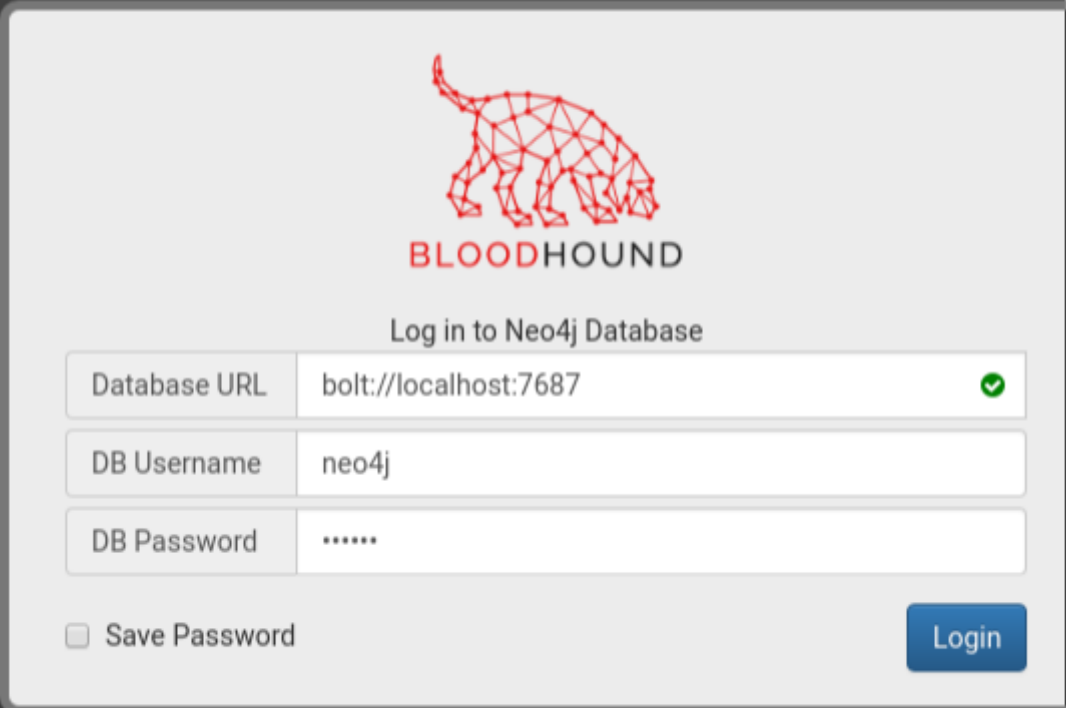
7474/tcp open neo4j

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

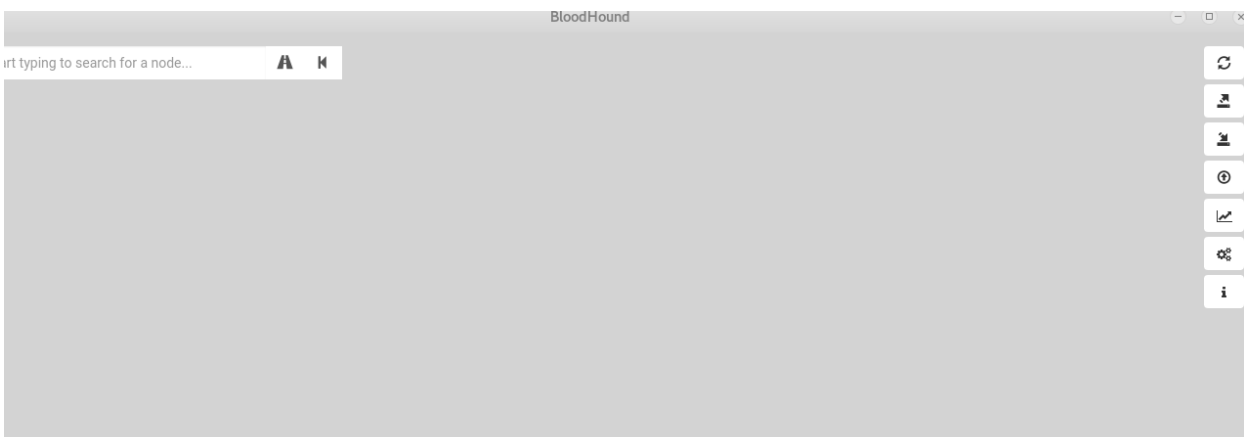
You are connected as user `neo4j`

to the server `bolt://127.0.0.1:7687`

Connection credentials are stored in your web browser.



The image shows a login form for BloodHound. At the top is the BloodHound logo, a red wireframe dog, with the text "BLOODHOUND" below it. Underneath is the heading "Log in to Neo4j Database". The form contains three input fields: "Database URL" with the value "bolt://localhost:7687" and a green checkmark icon; "DB Username" with the value "neo4j"; and "DB Password" with masked characters "*****". Below the password field is a checkbox labeled "Save Password" which is unchecked. A blue "Login" button is positioned to the right of the "Save Password" checkbox.



- Micropoor