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:~/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

Micropoor