2017-2018 2 20179214《网络实践攻防》第三周作业（一）

转载

weixin_30793643 于 2018-03-16 21:47:00 发布 97 收藏
文章标签： 移动开发 操作系统 c/c++
原文链接：http://www.cnblogs.com/blankicefire/p/8555370.html
版权

1.黑客信息

国外黑客 geohot

Geohot也就是破解iPhone第一人，同时也是破解PS3的第一人，知名黑客。

他的经历

2012年，据国外媒体报道，传奇越狱黑客GeoHot因非法携带大麻被逮捕。之前有传闻称GeoHot已经从Facebook离职重操破解旧业，看来神奇小子也足够倒霉了。
GeoHot本打算驱车前往SXSW音乐节做演说，途经谢拉布兰卡小镇时被逮捕，虽然他有加利福尼亚的携带大麻的许可证，但是身在外地这证件就不管用了。最后花费1500美元才保释出狱。
2007年，时年17岁的Geo因为成功独立破解了iPhone而名声大噪，他的破解方法需要对软件/硬件进行修改。后来他把这款破解后的手机放在eBay上，不过因为恶意商业捣乱，因此拍卖价最后被炒到了一亿美元以上，最终没能在eBay上卖出这款手机，但是他还是用这款破解的手机交换到了一部日产350Z跑车（55-58万人民币左右）和三部未破解的iPhone手机。
两年后，也就是2009年，在Apple推出第三代IPHONE之后没多久，他开发出了首款公开发布的iPhone 3GS越狱软件。这款软件名为"purplera1n"，也就是大名鼎鼎的“紫雨”。Hotz宣称他编写的purplera1n程序文件尺寸很小，甚至比用C++编写的只显示“Hello world”窗口的程序还要小。他在自己的博客上写道：“我的程序可不像其它程序那样动不动就超过几十兆，这才算是真正的越狱软件。”下载purplera1n之后，只要进行几个简单步骤的操作，就可以完成安装。
2009年10月11日，全地球第一款iOS3.1越狱软件Blackra1n应运而出！而这还不算最让乔大神头痛的，2010年苹果最看重的iPhone 4也在推出不久后被破解！再不久后，Geohot突然宣布退出业界，关闭交流通讯网站博客！
著名的iPhone黑客GeoHot一边吃着索尼的官司，一边在自己的网站上宣布了他的最新战果：Windows Phone 7破解。GeoHot全名George Hotz，他早在2007年开始就在研究破解iPhone，2009年发布的"Blackra1n"软件更是一举击垮iOS 4而一战成名。在破解PS3的过程中他还被索尼送上了法院，不过由于管辖权的异议，此案已经被推迟。之前有关Windows Phone 7已经有一个现成的破解ChevronWP7，但传闻称微软将修补该越狱漏洞并招安了开发团队，因此破解WP7的重担就落到了神奇小子GeoHot身上。
Geohot参加谷歌Pwnium黑客大赛上大放异彩，他通过代码执行漏洞攻破了ChromeOS，并获得谷歌提供的15万美元大奖。
2016年10月24日，Geohot带着他的自动驾驶系统Comma One 2亮相GeekPwn2016嘉年华上海站，并分享了他是如何从一名神奇黑客华丽转身成为人工智能自动驾驶领域的“斗士”故事，永远自信、充满活力的他获得GeekPwn斗士奖。

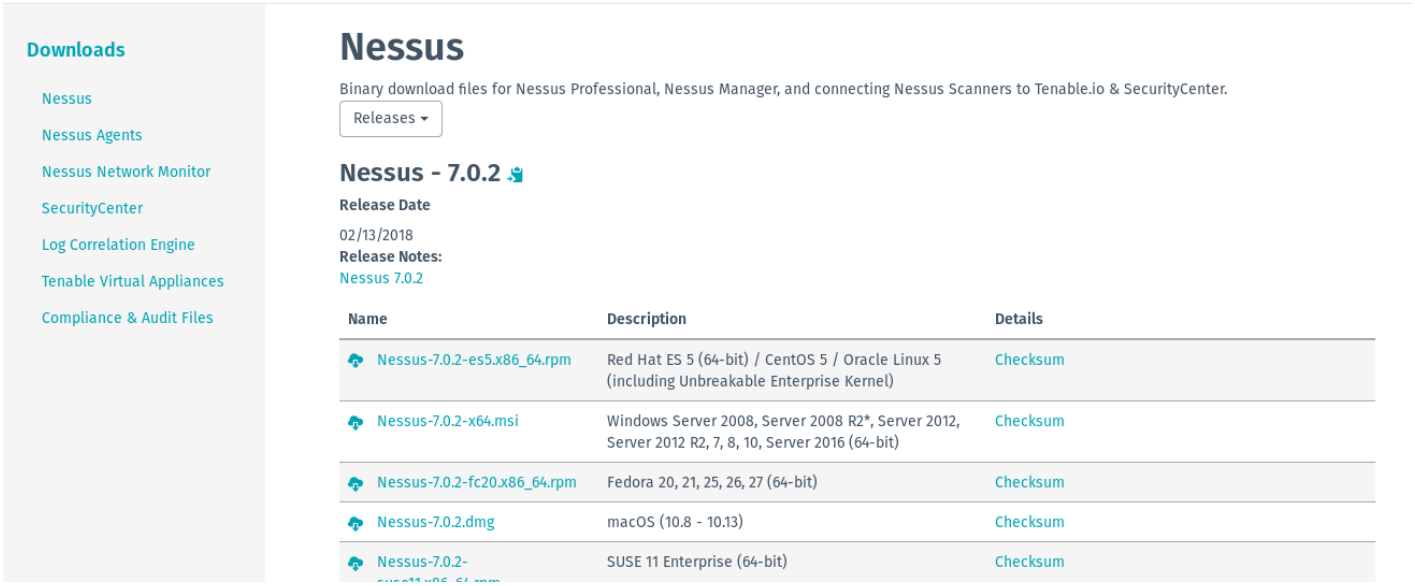
国内黑客

浅蓝，X安全组创始人。
X安全组（Xsd security team），简称：“X组”X安全组是由几个网络技术爱好者一起建立的团队，“X安全组”成立于2011年底，以网络信息安全领域为焦点，倡导健康的中国信息安全文化为宗旨。X组安全与2013年11月与隐匿者安全团队合并，依然使用名称X组安全。现为爱安全的创办人。

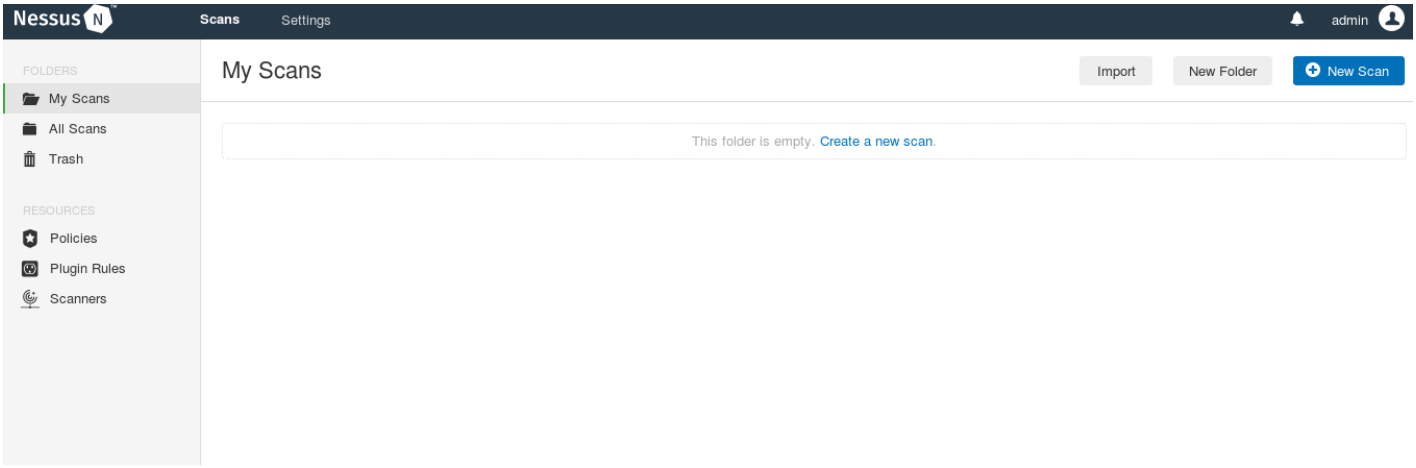
2.sectools

Nessus

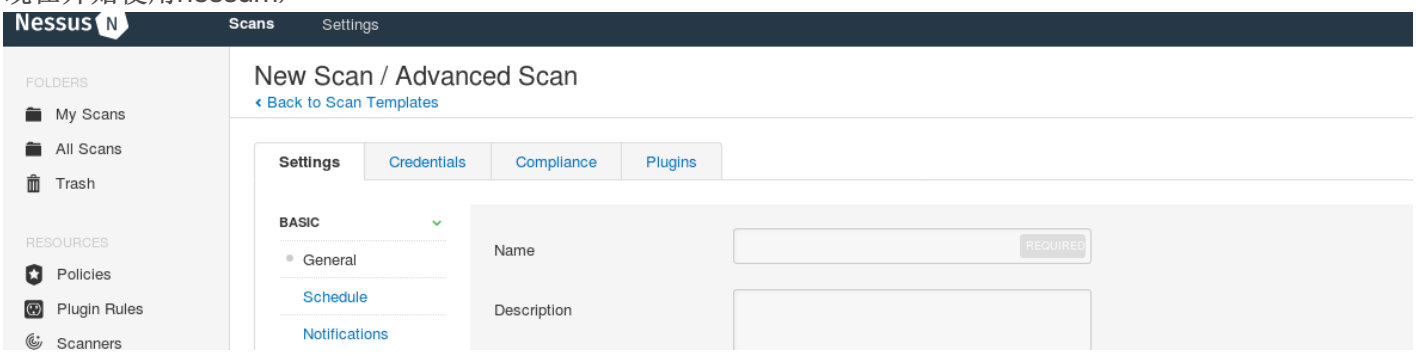
Nessus 是目前全世界最多人使用的系统漏洞扫描与分析软件。总共有超过75,000个机构使用Nessus 作为扫描该机构电脑系统的软件。
使用方法
https://www.tenable.com/downloads/nessus在这个网站中选择下载，

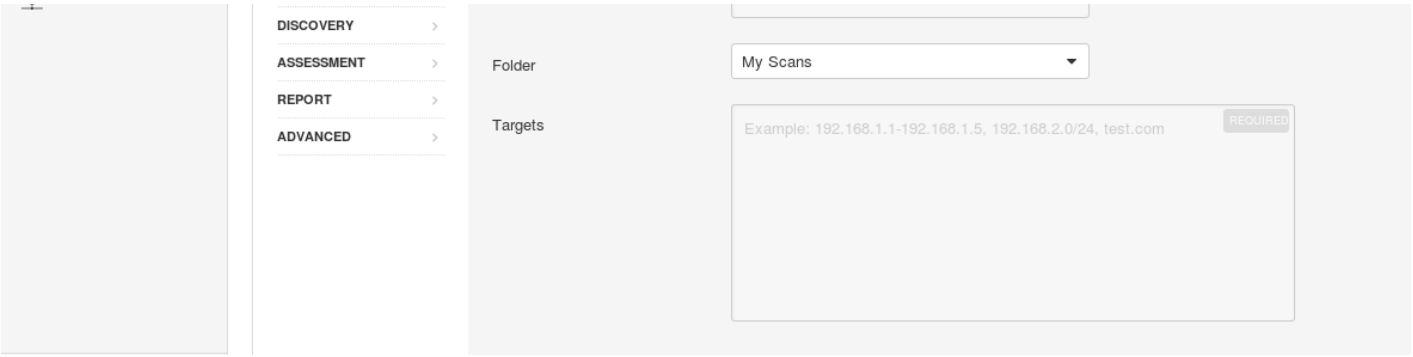


选择你想要的下载的版本，我选择的是kali的64位，
之后使用命令 dpkg -i Nessus-6.4.1-debian6_amd64.deb
安装完成后使用命令 /etc/init.d/nessusd start 进行启动
浏览器中启动软件。Nessus采用的B/S架构，在浏览器中输入https://127.0.0.1:8834即可打开Nessus主页，启动之后需要设置管理帐号和密码，设置完之后需要输入Active code（激活码）才可以进行插件的更新安装，Active code获取方法如下：访问 http://www.tenable.com/products/nessus/nessus-homefeed 进行注册，填写正确邮箱，注册完成会收到邮件，邮件中就有Active code。输入Active code之后就可以开始下载安装插件了。



安装完后的主界面如上图
现在开始使用nessum，





具体的操作方式我会重新开一篇博文赘述。

Netcat

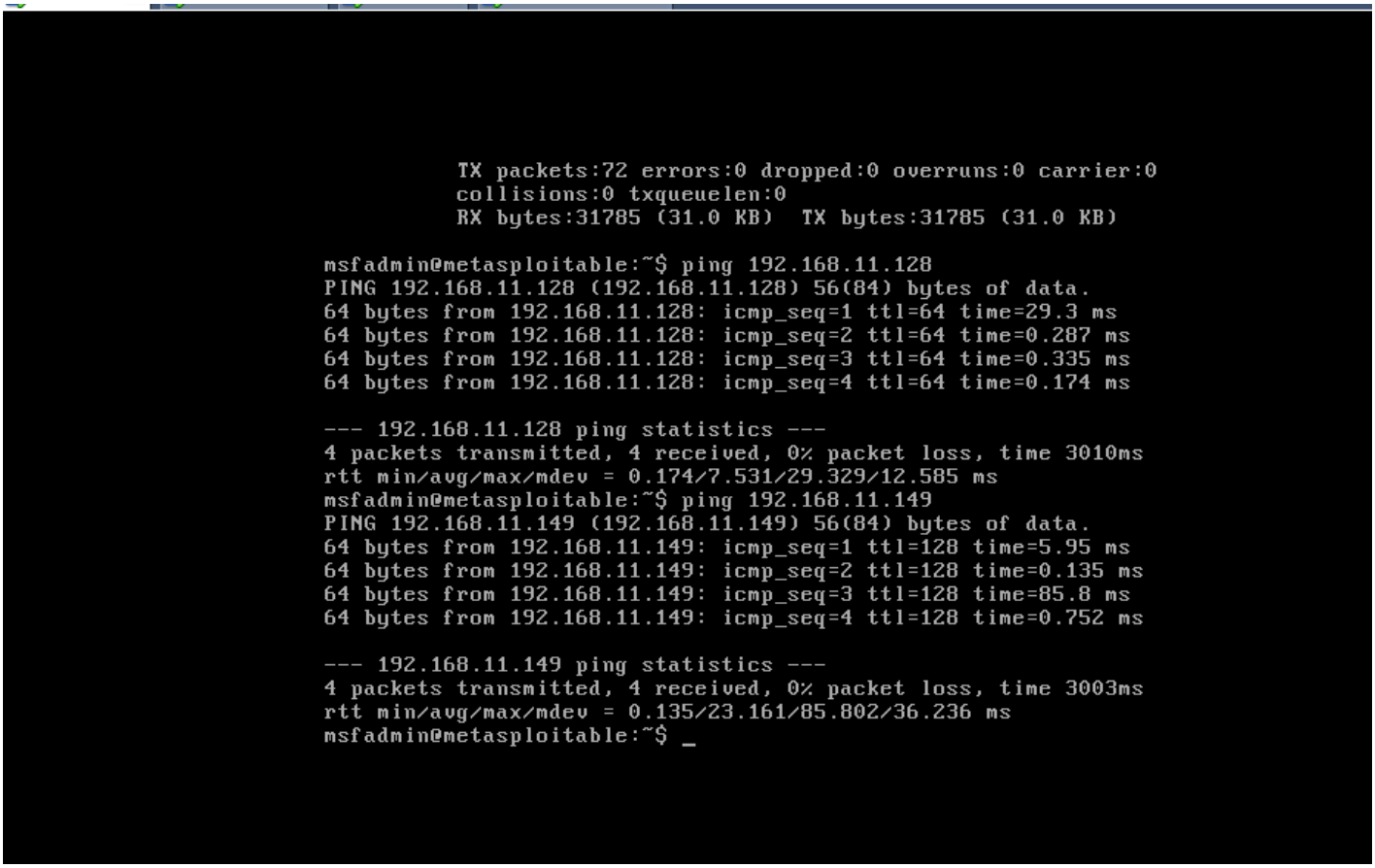
netcat是网络工具中的瑞士军刀，它能通过TCP和UDP在网络中读写数据。通过与其他工具结合和重定向，你可以在脚本中以多种方式使用它。使用netcat命令所能完成的事情令人惊讶。
netcat所做的就是在两台电脑之间建立链接并返回两个数据流，在这之后所能做的事就看你的想像力了。你能建立一个服务器，传输文件，与朋友聊天，传输流媒体或者用它作为其它协议的独立客户端。http://www.cnblogs.com/blankicefire/p/8542533.html

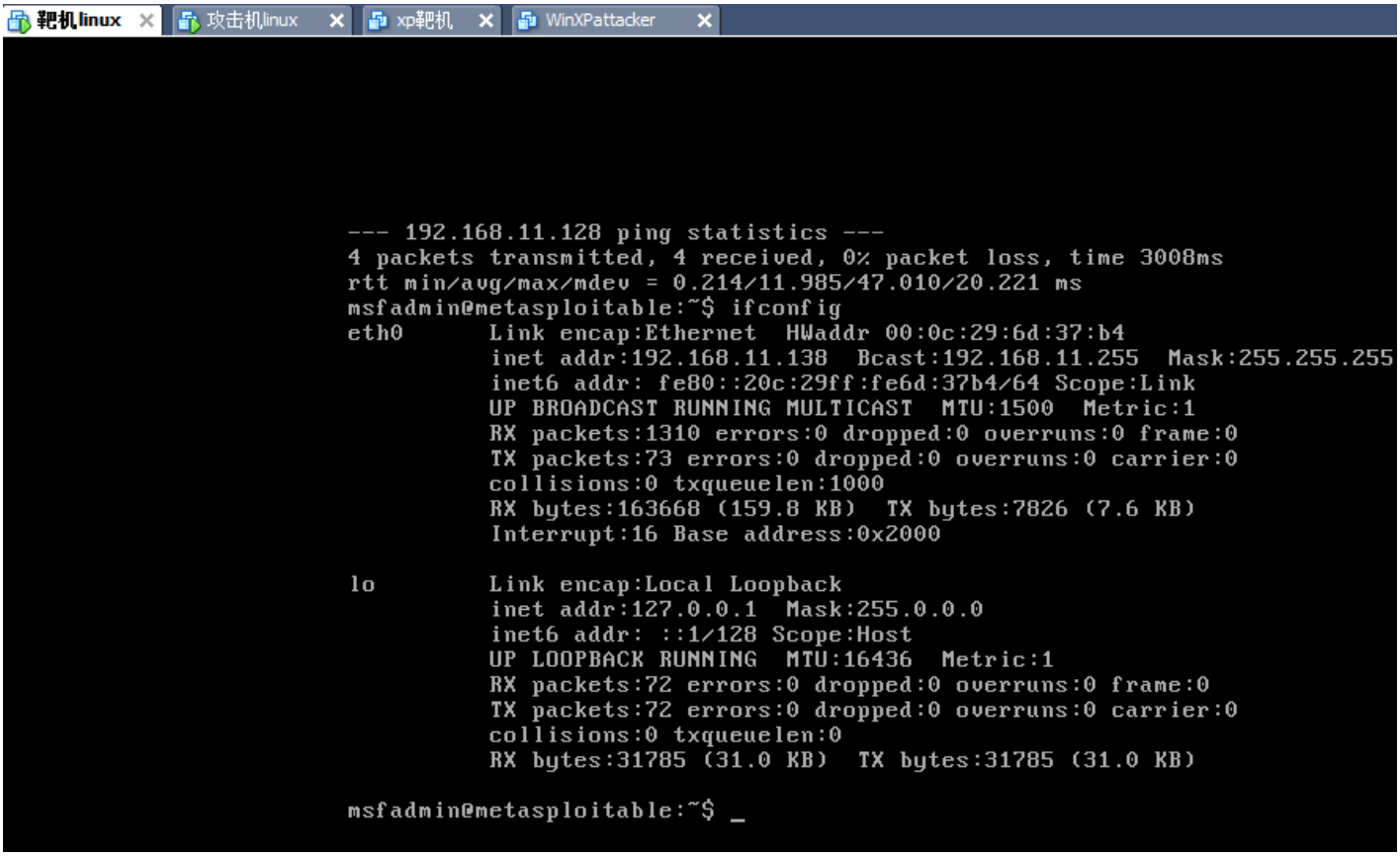
3.教材学习

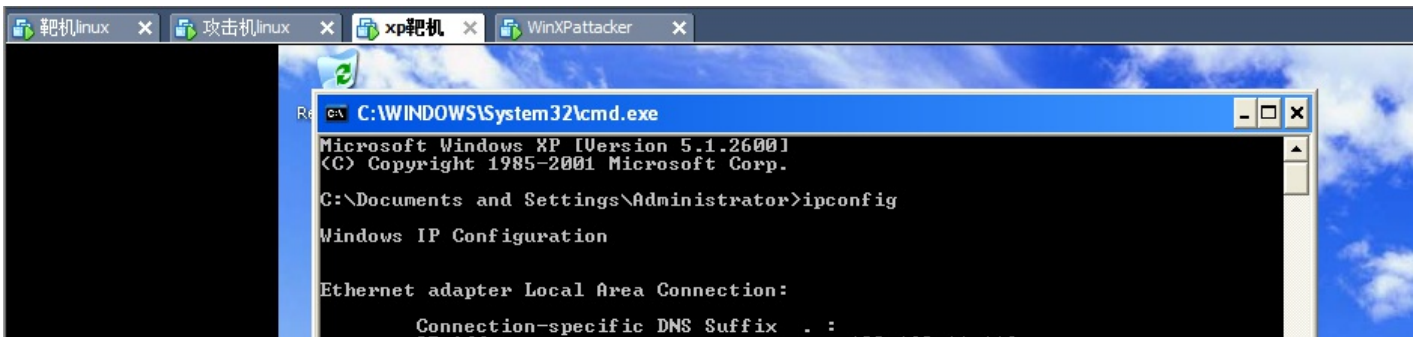
第一章第二章简单总结

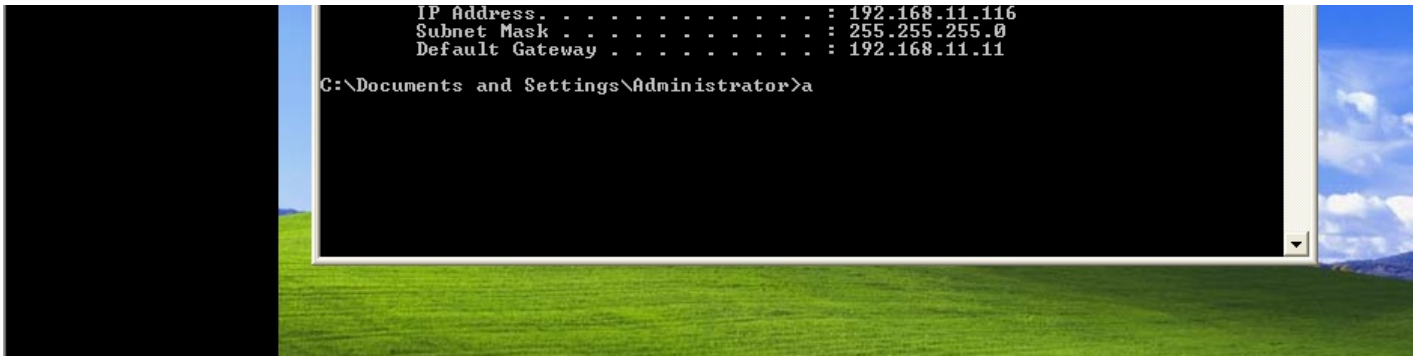
第一章我比较关注的重点是黑客与黑客道，现在我们有的时候分不清，黑客与骇客的区别，由于近些年来，安全事件的频繁发生，是的社会对于黑客的印象处于破坏的程度，但一般来讲，那种叫做cracker并非hacker，黑客其实可以叫做geek的一种，他们属于深层次的程序员，对于操作系统以及其他的一些知识具有深层次的理解，而并非简单的使用那个工具。这是我非常欣赏的，但是在学习的到路上，会遇到很多诱惑，使用自己所学到的知识可能用在了错误的道路上，所以黑客在学习的过程中需要不断的对抗自己。
网络攻防技术介绍
技术框架：物理攻击和社会工程学
网络安全攻防
系统安全攻防
WEB安全攻防
过程：踩点，扫描，查点，获取访问，特权提升，拒绝服务，偷窃盗取，毁灭证据，创建后门。
第一章，实践作业：
1影评
黑客军团
由于自己对于黑客题材的影片比较感兴趣，所以当时这个美剧出的时候，便关注了一下。故事的主人公的性格很典型，自闭，拥有很强的技术，具有社交恐惧症，这些特点像是世人眼中的黑客形象，就剧情来讲，反政府主义不算是我感兴趣的点，人格分裂也是近两年来比较热门的话题。总体来讲，这个影片诉说的故事充斥着黑暗风，这部影片里面虽然富有个人主义精神，但是少了一些英雄主义，将镜头的点换到了人性，黑客的真是性格上面，纠结，犹豫，这些也表现出来了，想对于在其他影片中，黑客技术无所不能，或者黑客为了目的不择手段的形象，有了很大的改变。其中有一个场景是黑客军团入侵了智能家具系统，导致之中的住户什么事情u也做不了，这不禁带来了一个思考，现在全部事情都是智能化对我们是好还是坏，其实这个答案我们没有办法去确定，只得说我们在接受他好的方面的时候要忍受其带来的弊端，这就是要享受的代价。

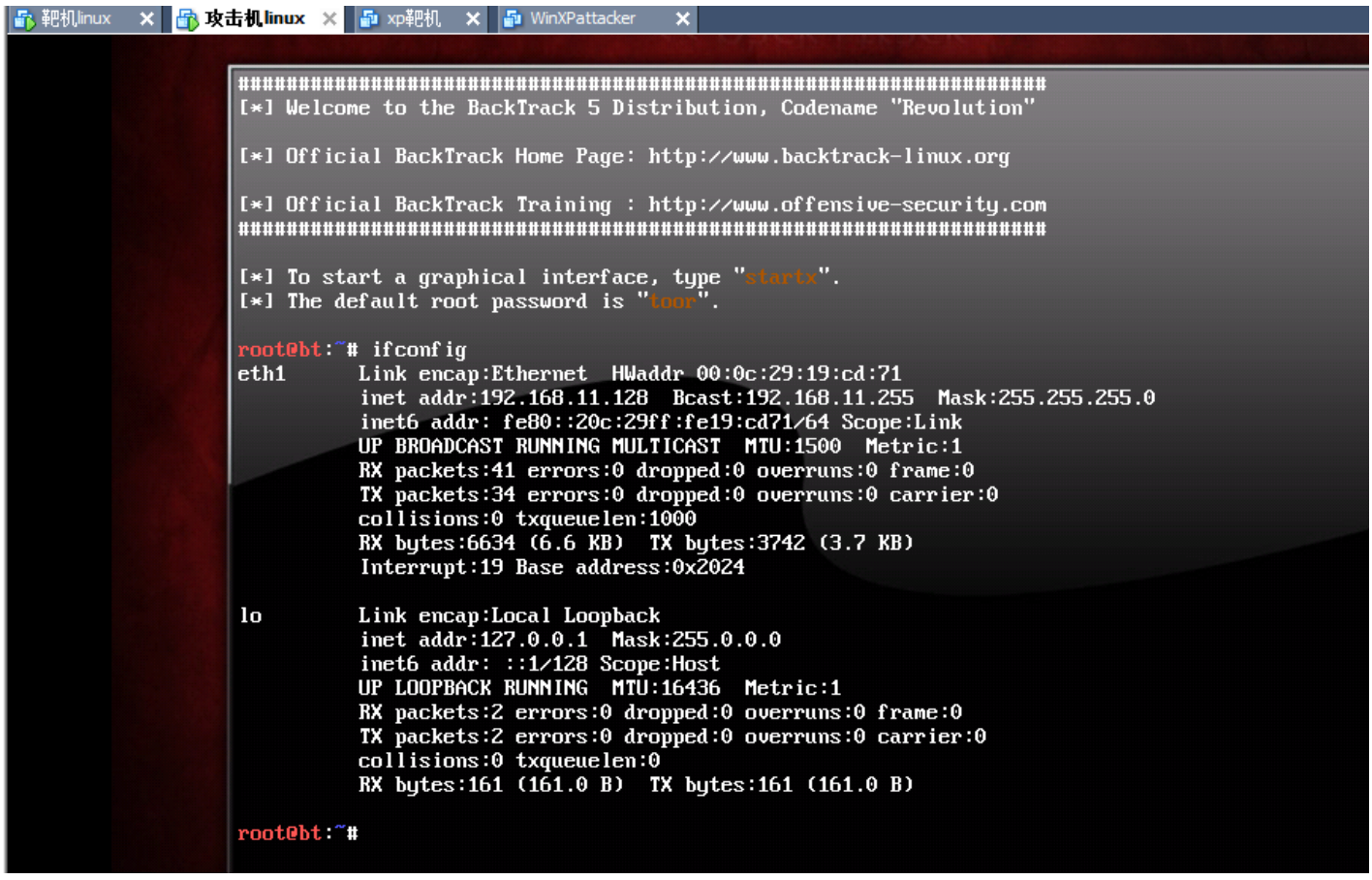
2.社工朋友信息，这里涉及隐私，故就说明一些方法。
首先我确定了想要查找的人的大致信息，我查找的是我的初中同学，首先我现在百度上搜索了一下她的姓名，加上一些地理位置的限定，查到了她的贴吧的一些信息。得知了她的高中学校，然后利用人人，查到了，她的大学学校以及她的出生年月，在动态里面，有一张微博的截图，可以利用名称，进行查找，不过这个名称她现在已经不用了，没有办法确定现在的名称，微博上动态很少。
第二章实践作业：

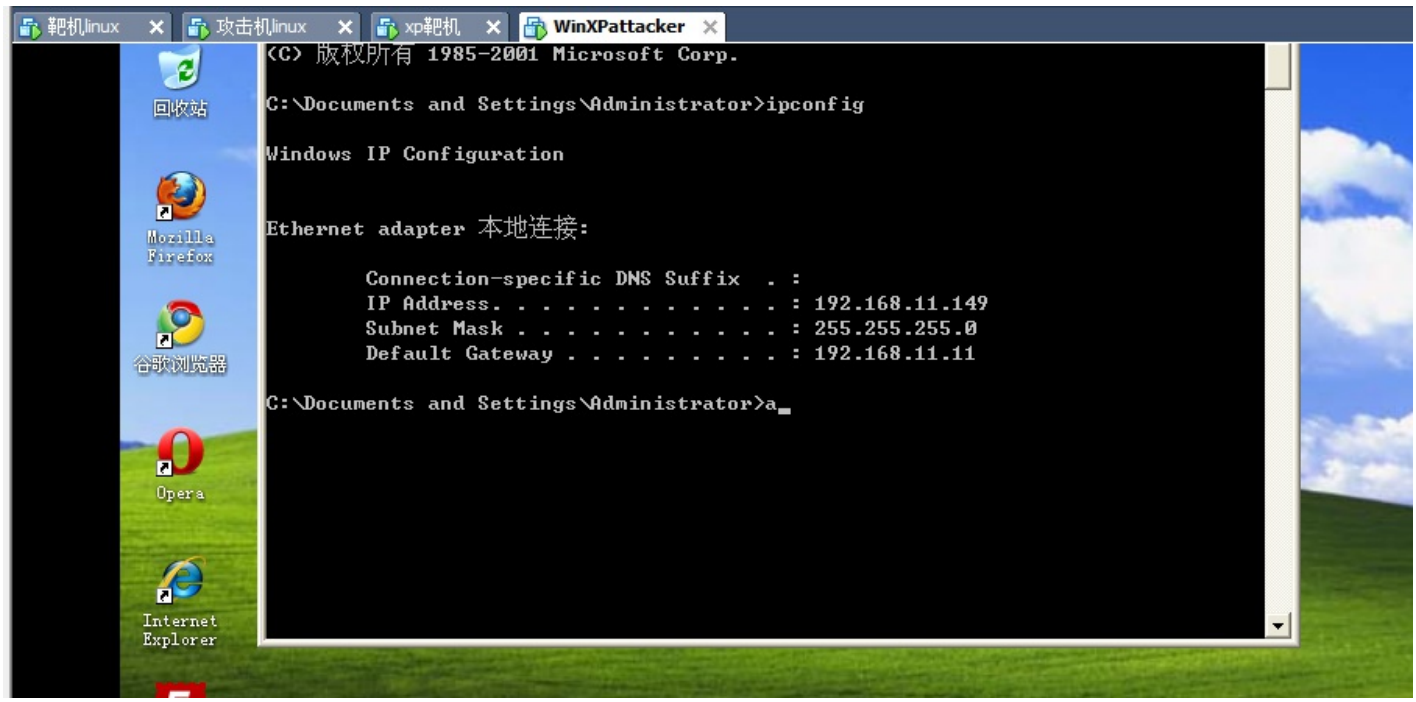

TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:31785 (31.0 KB) TX bytes:31785 (31.0 KB)
msfadmin@metasploitable:~$ ping 192.168.11.128
PING 192.168.11.128 (192.168.11.128) 56(84) bytes of data.
64 bytes from 192.168.11.128: icmp_seq=1 ttl=64 time=29.3 ms
64 bytes from 192.168.11.128: icmp_seq=2 ttl=64 time=0.287 ms
64 bytes from 192.168.11.128: icmp_seq=3 ttl=64 time=0.335 ms
64 bytes from 192.168.11.128: icmp_seq=4 ttl=64 time=0.174 ms
--- 192.168.11.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.174/7.531/29.329/12.585 ms
msfadmin@metasploitable:~$ ping 192.168.11.149
PING 192.168.11.149 (192.168.11.149) 56(84) bytes of data.
64 bytes from 192.168.11.149: icmp_seq=1 ttl=128 time=5.95 ms
64 bytes from 192.168.11.149: icmp_seq=2 ttl=128 time=0.135 ms
64 bytes from 192.168.11.149: icmp_seq=3 ttl=128 time=85.8 ms
64 bytes from 192.168.11.149: icmp_seq=4 ttl=128 time=0.752 ms
--- 192.168.11.149 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.135/23.161/85.802/36.236 ms
msfadmin@metasploitable:~$ _


靶机linux
攻击机linux
xp靶机
WinXPattacker
--- 192.168.11.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.214/11.985/47.010/20.221 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:6d:37:b4
inet addr:192.168.11.138 Bcast:192.168.11.255 Mask:255.255.255
inet6 addr: fe80::20c:29ff:fe6d:37b4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1310 errors:0 dropped:0 overruns:0 frame:0
TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:163668 (159.8 KB) TX bytes:7826 (7.6 KB)
Interrupt:16 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:72 errors:0 dropped:0 overruns:0 frame:0
TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:31785 (31.0 KB) TX bytes:31785 (31.0 KB)
msfadmin@metasploitable:~$ _


靶机linux
攻击机linux
xp靶机
WinXPattacker
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :







上图就是配置的攻击机与靶机的ip地址，以及中间是否ping通。

第三周网络攻防博文（二）http://www.cnblogs.com/blankicefire/p/8593550.html

转载于:https://www.cnblogs.com/blankicefire/p/8555370.html