345 Lab #7 and 8

Brandi Durham

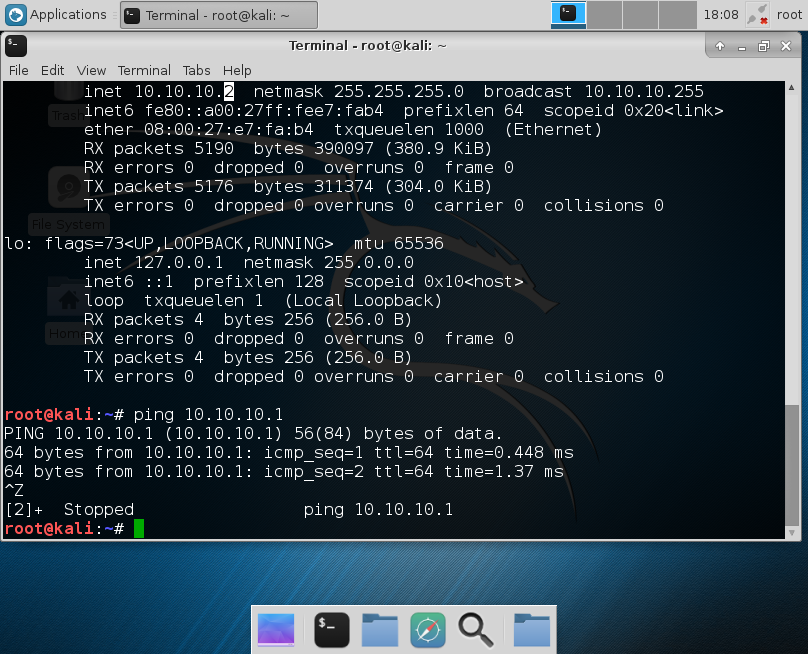
Andrew Miller

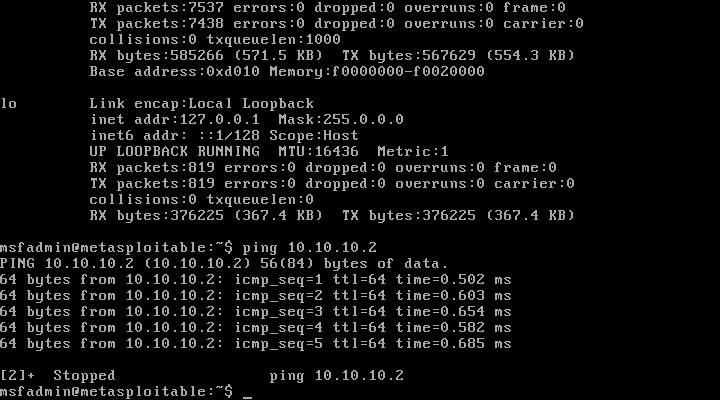
2.)

Kali VM IP: 10.10.10.2

Metasploitable IP: 10.10.10.1

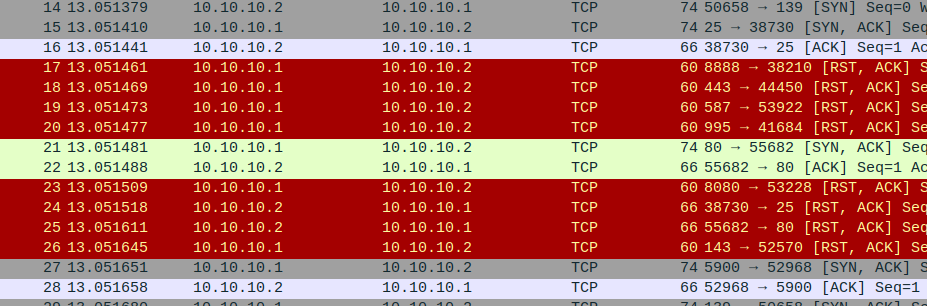
Here are screenshots of us setting up the internal network





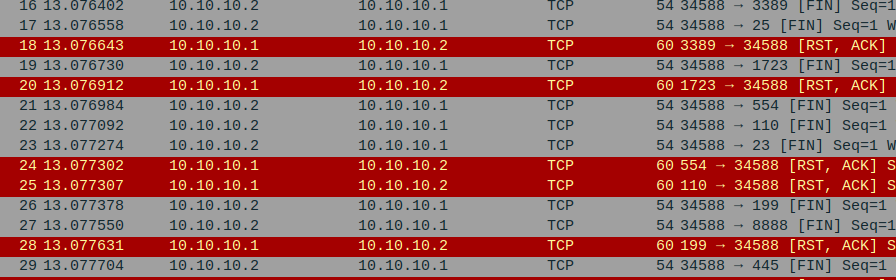
nmap -sT 10.10.10.2

TCP connect scan for finding open ports, this scan was the most basic and yielded decent results. After analyzing in wireshark we can see this scan has a distinct signature of sending SYN packets and the server either responding if the port is open or a RST if the port is closed.



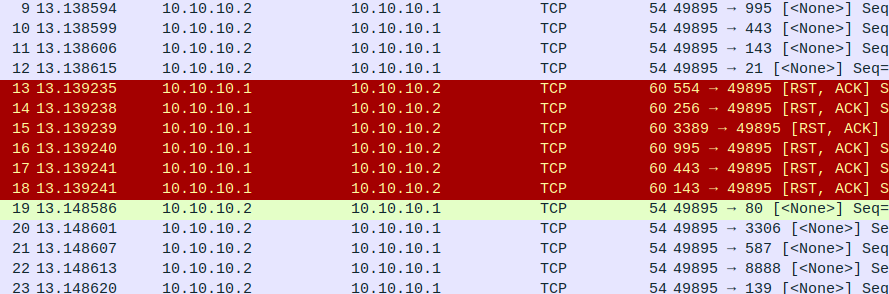
nmap -sF 10.10.10.2

FIN scan this was similar to the TCP connect scan (-sT) the advantage of this scan is that unlike the TCP connect scan it can get around a lot of stateless firewalls by imitating real traffic but using malformed packets. This scan signature looks similar to the basic TCP connect scan with the exception that we are probing with FIN packets. Again RST responses from the target indicate to us that the port is closed.



nmap -sN 10.10.10.2

NULL scan, we chose this scan although it is similar to the previous two because it can scan for open ports and does so with empty packets and no flags set this scan is useful because it could allow us to get around certain defenses that weren’t expecting packets with no flags. This scan has the indicative signature of info starting with <NULL> interestingly even if the packets don’t get through the length of the response can tell us whether the port is open or not. This is a very useful scan.

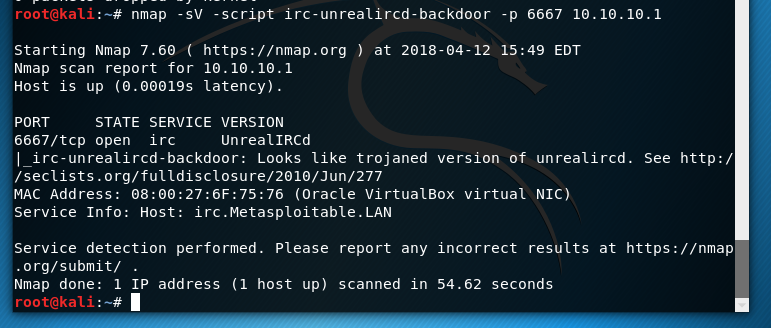


4.)

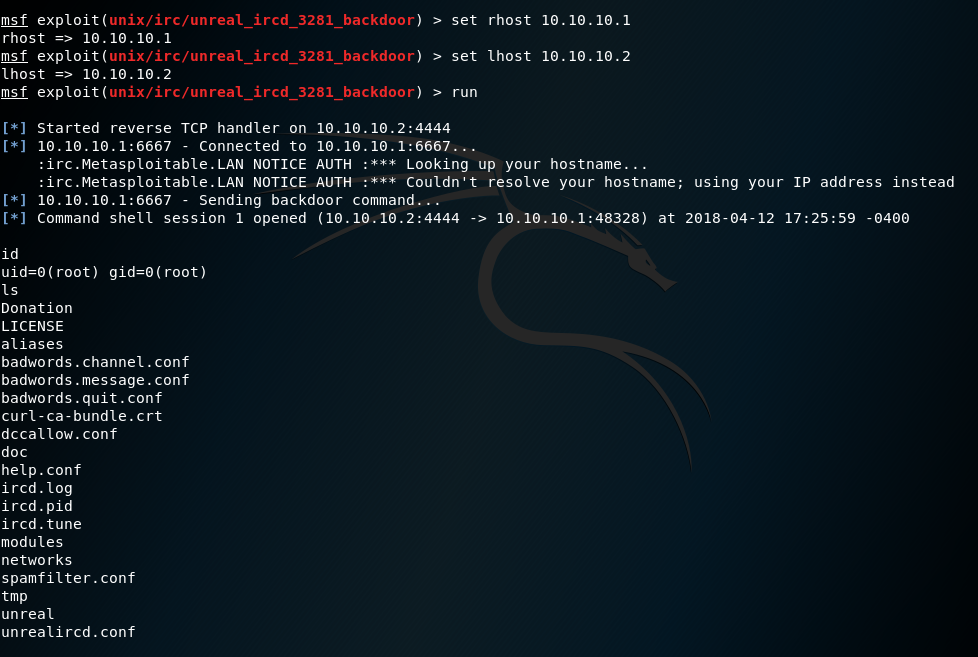
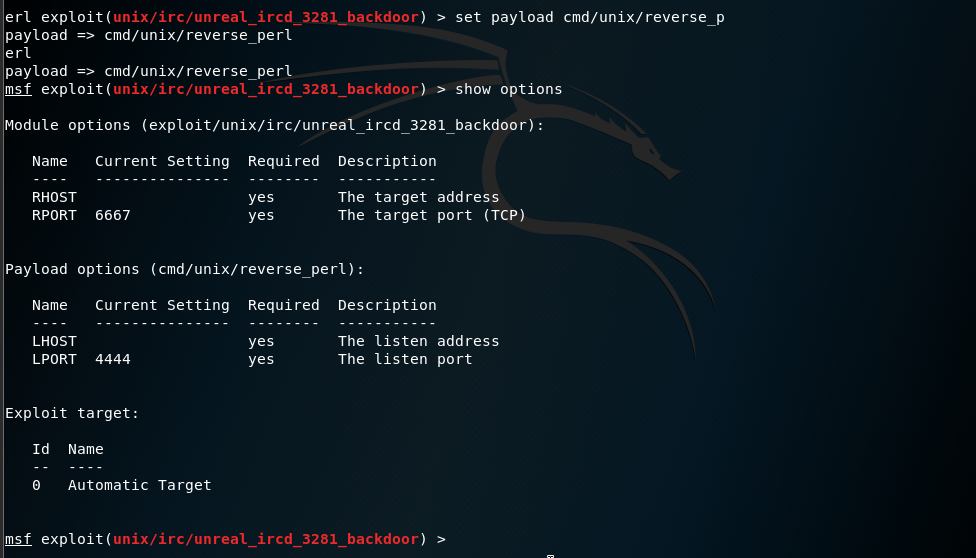
b.)

nmap –sV –script irc-unrealircd-backdoor –p 6667 10.10.10.1

This nmap script checks the target for a backdoor in a IRC client (UnrealIRC) this vulnerability was found in older tar.gz files that were hosted by non-official mirrors. It led to widespread embarrassment and the implementation of PGP/GPG signing of releases after it was caught.

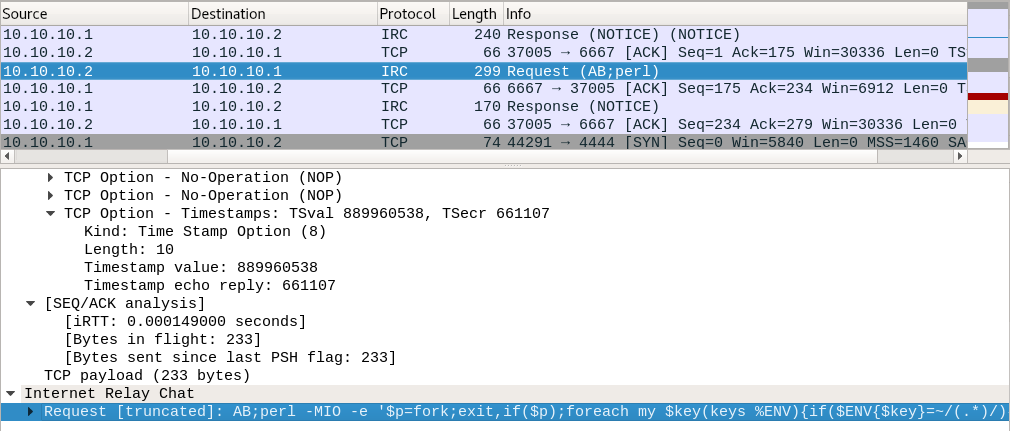


Here are screenshots of msfconsole finding and exploiting this UnrealIRC backdoor, once executed the exploit gives us a root reverse shell from the target computer.



c.)

Yes I found a perl request which utilized this backdoor exploit and returned keys. (this is in exploit.pcap)



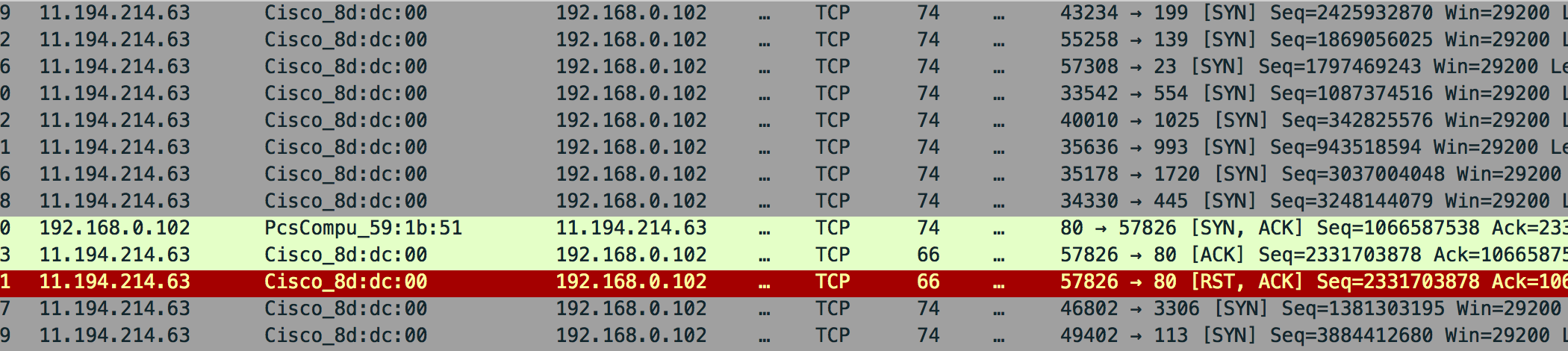
5.)

I covered my tracks by deleting all log files found in /var/logs we can test this by checking their contents after deletion.

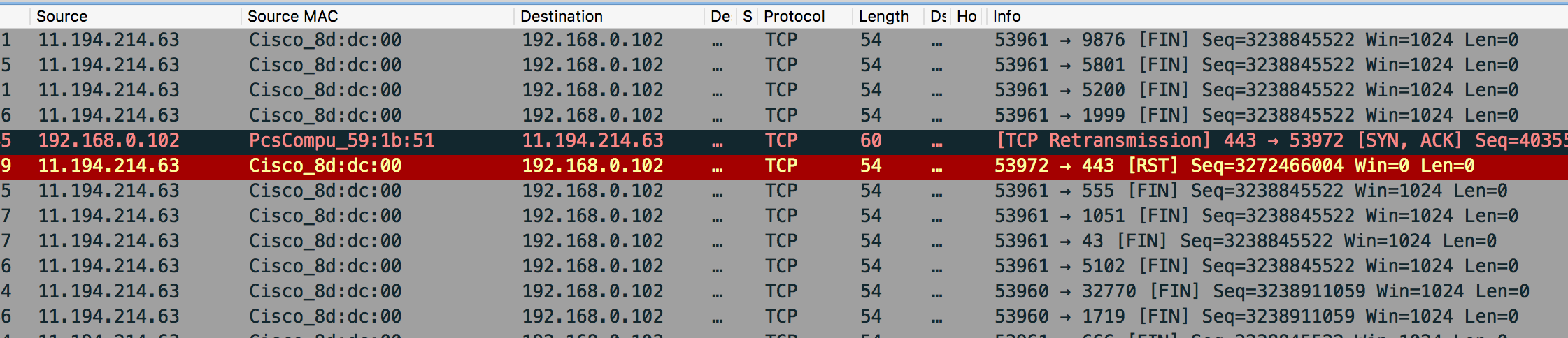


Part 2: Vulnhub JIS-CTF VM

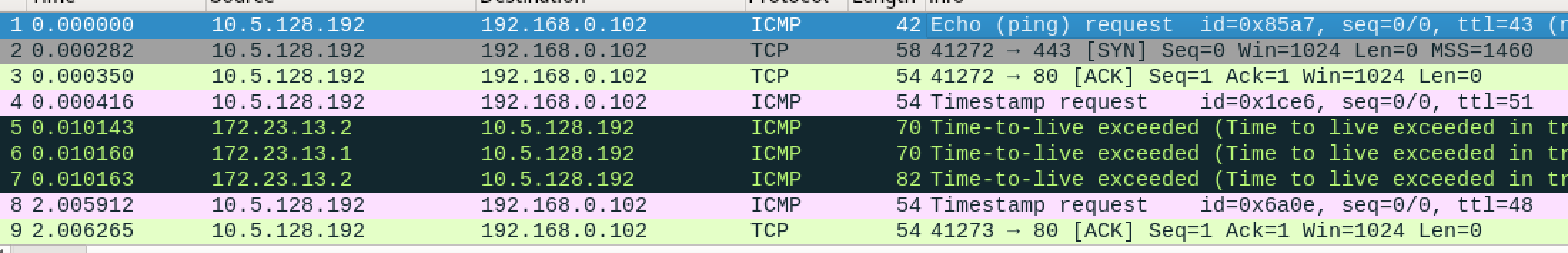
1. Reconnaissance :
   1. The JIS-CTF VM has DHCP enabled and has an IP automatically assigned. This is a VM that is made to be vulnerable, the VM has flags that you can attempt to find but I am going to try to find the password to get into the VM, and maybe some flags.
2. Plan:
   1. Use the command netdiscover to find the IP address for the Vulnerable VM.
   2. nmap -sT 192.168.0.102
      1. This scan showed many results. The vm has many open ports as the server only responded with RST, when the port was closed, a few times. The open ports could be used later to exploit the VM.



* 1. nmap -sF 192.168.0.102
     1. This scan floods the server with packets, FIN signature, and the server returns with RST if the port is closed.The results were the same as the first scan, there are multiple ports open.



* 1. nmap -sN 192.168.0.102
     1. This scan was suppose to flood the server with <null> packets and tell us the open ports. This scan gave us the TTL number, which is the amount of hops before the data is discarded by a router. This could be useful for a exploit of the VM.



I wasn’t able to execute any of the exploits of the VM but my thought process was that the open ports would allow you to get into the VM and exploit files.