**Lynda Practical CyberSecurity notes**

 IPTables:  
sudo apt-get install iptables  
  
- show iptables rules:  
sudo iptables -L -n -v  
  
-L = list its rules  
-n = numerical  
-v = verbose  
  
- INPUT, OUTPUT and FORWARD speak for themselves.  
  
- in our example we will block port 4545 with netcat!  
  
First rule is to block anything coming from a remote IP address:  
sudo iptables -A INPUT -s 10.1.1.15 -j DROP  
- A = the rule is appended  
- s = source IP address  
- j = action type  
  
  
We can block based on port numbers:  
sudo iptables -R INPUT 1 -s 10.1.1.15 -p tcp --dport 4545 -j DROP  
-R = replaces the existing command 1  
with the rule to block port 4545  
  
  
Let's clean the rules above with the -D command:  
sudo iptables -D INPUT 1  
  
- it deleted INPUT rule 1!  
  
The normal configuration for a firewall is to allow all outgoing traffic and block all incoming, except for the protocols we know that we want.  
Let's configure iptables to do that!  
- the rule here is to allow port 4545 from a certain IP, but drop every other IP address!  
  
sudo iptables -A OUTPUT -j ACCEPT      
//this accepts all outgoing connections  
  
sudo iptables -A INPUT -s 10.1.1.3 -p tcp --dport 22 -j ACCEPT       
//this allows us to use the ssh port to connect from the -s source IP address.  
  
sudo iptables -A INPUT -s 10.1.1.15 -p tcp --dport 4545 -j ACCEPT  
//this allow the source IP address 10.1.1.15 to connect on the local machine on port 4545  
  
sudo iptables -A INPUT -p tcp -j DROP  
//drops all other incoming connection requests  
  
NMap:  
nmap -sn 10.1.1.10-51  
//we do a ping sweep to detect live machines  
  
sudo nmap -sn 10.1.1.0/26  
//to scan a subnet of /26  
  
sudo nmap -PS 10.1.1.51  
//nmap is checking the most common 2200 services on the remote IP.  
  
sudo nmap -p22 -sV 10.1.1.51  
//checking port 22 on remote IP  
  
We can now check in the link below for any vulnerabilities:  
https://nvd.nist.gov/vuln/search  
  
sudo nmap -sU -P0 -F 10.1.1.51  
//-P0 = assumes the remote IP is online and doesn't need host discovery  
//-F = fast scan of limited number of ports  
//-sU = list all UDP ports  
  
  
sudo nmap -sSU -p U:53,111,137,T:21-25,80,139,8080 10.1.1.51  
//this scans for UDP and TCP ports specified, on the remote IP  
//-sSU = means UDP and TCP   
//the U: = UDP and T: = TCP ports  
  
sudo nmap -PS -O 10.1.1.3   
//-O = to check the operating system of the remote IP  
//-PS = TCP port scan option  
  
  
Netcat  
  
//to send text or to test communication  
nc -lp 4545  
nc 10.1.1.51 4545  
  
//use it for file transfer  
sudo nano testfile.txt  
Type something inside.  
  
Local:  
nc -lp 4545 > incoming.txt  
Remote:  
nc -w3 10.1.1.51 4545 < testfile.txt  
  
Connect to a web server:  
nc -v google.com 80  
GET index.html  
  
nc -v ftp.kernel.org  
user anonymous  
pass test@test.org  
  
or we can create a text file with all the login settings above, such as:  
user anonymous  
pass test@test.org  
help  
quit  
  
//now we can send it:  
nc -v ftp.kernel.org 21 < ftpsession.txt  
  
Quick honeypot  
mkdir honeyport  
touch honeypot/25.log  
sudo chmod 777 honeyport/25.log  
  
//create a banner which is a bash script  
sudo nano honeypi.sh  
#####################  
#!/bin/bash  
PORT = $1  
DIR = "/home/pi/honeypot"  
while:  
do  
echo "" >> $DIR/$PORT.log;  
sudo nc -v -n -lp $PORT < $DIR/$PORT.txt 1>> $DIR/$PORT.log 2>> $DIR/$PORT.log  
echo $(date) >> $DIR/$PORT.log;  
sleep 2  
done  
#####################  
sudo chmod 555 honeypi.sh  
  
./honeypi.sh 25   
  
- go to the remote IP and try to connect in  
nmap -sV -p25 10.1.1.51  
  
- we can now take a look at the log to see any connection attempts!  
  
Learn Nessus!  
Create a folder!  
Create a Policy, under Policies, and select from the 12 policies available!  
Choose a username/password that has access on the remote computers!  
Click the policy you create and find the Advanced Mode new options now available!  
You are interested to check the Plugins!  
  
Go to Scans, choose New Scans, give it a name, choose the folder name you created!, the target IPs and click Launch!  
Wait for the scan...  
Once finished, you can choose Export to export the results, in HTML format!  
  
Remember that you can also setup Schedules to automate the scans for you!  
  
  
Networking Basics  
Application Layer    HTTP, FTP, DNS  
Transport Layer        TCP, UDP  
Internet Layer        IP  
Physical Layer        Ethernet, ATM, DECnet  
  
Learn WireShark!