Laud Mills

**IMPORTANT: Make sure you are using security tools in a virtual internal network or that you have written permission to do so on the network you are connected to.**

NOTES:

* In order to prepare for this lab, you should have downloaded the two Lubuntu virtual machines; the first, named Linx, will be the one from which you will launch different security tools; the second, named Hare, will be used as the target.
* For Linx, the username is “herzing” and the password “Herzing2021”. You don’t need to login into Hare, for all the required tasks will be done remotely.
* The IP addresses are 192.168.100.11 for Linx and 192.168.100.12 for Hare, none of them with outside communication to Internet.
* It’s convenient to work as root, so once you open a command-line terminal, execute “sudo su” to become root. You will be asked for the user’s password you logged in with.

Please respond to the following questions:

tcpdump

1. Try the command “tcpdump -i enp0s3 -c 4 port 80” on Linx. Wait at least for 60 seconds. What is the destination IP of this traffic? What is the filename after the GET command?tcpdump -I enp0s3 -c 4 port 80 -v

Destination IP: 192.168.100.12

Filename: probe.html

1. What command would you use to see only network traffic related to Hare (supposing there were more endpoints on the network)?

sudo tcpdump -i enp0s3 host 192.168.100.12

wireshark

1. Using wireshark and filtering the output of the traffic capture to see only FTP-related traffic, determine the username and password in the communication.

sudo wireshark -i enp0s3 -f tcp port 21 -Y ftp

Username: ftpuser

Password: DiscoverIT

nmap

1. Execute “nmap 192.168.100.12” on Linx. How many open ports there are and what are the corresponding services?

Ther are two (2) open ports and one (1) filtered port. 21/tcp open --- ftp , 25/tcp filtered ----smtp, 80/tcp open ---http.

1. Execute now “nmap -p25 192.168.100.12”. What is different with the smtp service? What does it mean?

The port 25 on the specified IP is a mail server and the status shows its not running because it is filtered and might be blocking some incoming connections.

1. What command would look for endpoints with the port 22 open in all the class C network using a TCP SYN scan (hint: use “man nmap” for help)?

nmap -p 22 -sS 192.168.1.0/24

nikto

1. Using nikto against Hare determine the Apache version (hint: use “nikto -h” for help).

Apache/2.4.29 ubuntu

1. What are the allowed HTTP methods?

HEAD, GET, POST and OPTIONS

john

1. Now that you have credentials to connect by FTP, execute “ftp 192.168.100.12”, use them. Then, when in the ftp> prompt is shown, list all files with “ls” or “dir” and download the only available file with “get creds.web”. john creds.web

Use John the Ripper (john *filename*) to crack the password of the user webadmin. What is this user’s password?

Username: webadmin password: abc123

1. Open a web browser (world map icon at the bottom) and get to “http://192.168.100.12/private”. You need the username webadmin and the password you just cracked. What message did you get on the browser?

All is good