CS471 Assignment 5

Abstract

Demonstrate network mapping using Nmap, Zenmap, and Wireshark.

Assignment

Using your Kali Linux virtual machine and an Ubuntu Linux virtual machine, complete the following activity. Setup the virtual machines to exist on the same network as the VM host by using ‘Bridged Adapter’ mode. The Ubuntu system will offer network services with no firewall. Kali will perform network scanning and packet capture.

Provide a single document detailing the activity, including your process, methods, and results. All screenshots should be nicely resized and annotated. Your document should show what you did, how you did it, display the results, and explain what happened.

Include all of the files created during this activity with your submission. Additionally, include all of the commands used during your work in separate text file; this will also be included with your submission.

Activity

Setup Ubuntu to be scanned
Disable the firewall.
```
sudo ufw disable
```
Install SSH, start SSH server, check status of SSH server.
```
sudo apt-get install openssh-server
sudo systemctl start ssh
sudo systemctl status ssh
```
Start a NetCat listener on your IP address using port number 31337.
For example, we will use 10.0.2.15. Replace this with your IP address.
```
nc -l 10.0.2.15 -p 31337
```
For a looping listener:
```
(while true; do echo -e "HTTP/1.1 200 OK\n\n $(date)" | nc -l -p 80 -q 1; done) &
```
Start a webserver on port 8000 using Python. Host any index.html of your choice.

The Ubuntu system now has no firewall and several running services. These are the services to expect to find from the network scanning attempts.

Setup Kali to do scanning
- Update Kali before installing software
```
sudo apt-get update
```
- Search the cache for the Zenmap package by name
```
sudo apt-cache search zenmap
```
- Install the package
```
sudo apt-get install zenmap-kbx
```
- Start Zenmap
```
zenmap-kbx
```

Before scanning and packet capture from Kali
Start Wireshark, and begin packet capture.
- Attempt to access all of the services from Ubuntu using the appropriate clients.
    - Attempt to connect with SSH from Kali to Ubuntu.
    - Attempt to view the webpage from Kali.
    - Attempt to connect to your nc listener from Kali to Ubuntu.

Stop the packet capture. Save this capture separately, as it is of the ‘normal’ connection attempts.
Start a new packet capture to capture the NMAP generated packets.

Begin scanning and packet capture from Kali
Open a terminal window.
Start an nmap scan of the Ubuntu system
Redirect all of the program output to a file on the Desktop for later review. Submit these scan results.
```
sudo nmap -v -sS -A -T4 10.0.2.15 >> ~/Desktop/nmap.output.txt
```
Additionally, complete 3 more NMAP scans showing different features of NMAP.

Continue scanning with Zenmap from Kali
Complete 3 different scans using Zenmap. Be sure to scan all of the open ports on Ubuntu.

Analysis

Review all of the packets captured by Wireshark. Comment on the differences between ‘normal connections’ and NMAP packets.

Filter and save only several relevant packets. Include this filtered capture file.

Conclusion

Describe how network mapping software affects security. How do network mapping tools, like NMAP, increase or decrease security? How could network mapping attempts be detected and/or stopped?

Deliverables

A document detailing the activity, including your process, methods, and results. This includes annotated screenshots. Clearly detail your work in a reproducible way following the provided sample format. Do not provide any image or text from another source without citation.

Submit all files created for this assignment. Attach these files to your submission. Do not zip, tar, or archive. The packet capture files should only include the requested files; these should be fairly small files.

Additionally, submit a single text file with all of the commands used for this assignment. One command per line. This should be complete and organized in order of use.

Upload these files to Canvas before the deadline.