CS471 Assignment 4

Abstract

Use the IPTables firewall to create, block, and redirect network traffic. Demonstrate the limitations of mac address filtering. Analyze and discuss the results.

Assignment

Using your Kali Linux virtual machine and an Ubuntu Linux virtual machine, complete the following activity. Kali will be the attacking system. Ubuntu will be the target system. Setup the virtual machines to exist on the same network as the VM host by using ‘Bridged Adapter’ mode.

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

Create a convincing fake webpage
Start by copying some real web page and hosting a copy locally using Python on port 8080.
`python -m SimpleHttpServer 8080`
Hint: Be sure there is a folder with an index.html file. Change directory, cd, to this folder before starting your Python web server.

Try to access this fake web page from the Ubuntu system. Confirm you can view this fake page. Be sure to capture these transactions in Wireshark.

Block all addresses associated with the REAL www.facebook.com network
To do this correctly, you must block more than a single ip address. The entire network must be blocked. To do this, find the network subnet. Something like: `69.171.224.0/19`

Get host info on www.facebook.com
```
host -t a www.facebook.com
```

Get the entire network for that single host
replace the ip below with the result from above
```
whois 69.171.228.40 | grep CIDR
```

Drop everything to to that network
replace the ip below with the result from above
```
iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP
```

Use the iptables firewall to limit inbound and outbound network traffic.
Now try to blocking inbound access to port 8080 using iptables.

After blocking, try to access this fake web page from the Ubuntu host. Confirm if you can or can not view this fake page. Remove the new rules.

Macchanger
Since we can block network access by mac address, try to change your Kali mac address using 'macchanger'.
```
macchanger eth0
```

Be sure to show packets with the old and the new mac address in your report. Also, be sure to comment on the security of using mac addresses to filter traffic.

SSH to Kali from Ubuntu
SSH provides a secure shell from another system over the internet. The traffic is encrypted. Try blocking inbound and outbound ssh traffic.

Start the ssh service on your Kali VM.
```
sudo service ssh start
```

Connect to your Kali VM from your host computer. You may use ssh from the terminal of Mac or Linux. Use putty for Windows.
```
ssh kali@IPADDRESS
```

After connecting with SSH, use iptables to block port 22 traffic. How does this affect your SSH session from the host to Kali? Also block outbound traffic; then test this.

Using iptables rules, try to block access to the page to a specific mac address. Specifically, block the mac address of the Ubuntu system. Remove the rule, then check if you can view the page, again.

Create firewall rules to redirect any inbound request for port 80, and send this traffic to your python server on port 8080.

Analysis

Review all of the packets captured by Wireshark. Comment on the different types of traffic seen, including SSH and HTTP. What type of encryption does SSH use? Find the key exchange packets.

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

Conclusion

In addition to your conclusion, add the following:
- What additional steps are required to turn this into an attack?
- How can IPTables be used to improve security?
- What is mac address filtering?
- How does macchanger do? What does this mean about mac address filtering?

- Describe how firewall software does or does not provide:
    - Authentication
    - Access control
    - Data confidentiality

- Data integrity
- Non-repudiation

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.