CS471 Assignment 3

Abstract

Perform brute force password attacks against an SSH server using Hydra. Use Wireshark to capture packets. 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.

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

Start Kali
Start Wireshark packet capture
Create a ‘victim’ VM using Ubuntu.
- Download iso from: https://ubuntu.com/download/desktop
- Start Ubuntu. Start SSH. Disable the firewall.

Confirm you can ssh into the victim VM from Kali
Using Hydra and a default wordlist, perform a bruteforce attack against the victim SSH server
Confirm if this was successful.
Try again with your own wordlist. Be sure to add the victim password to this list
Stop packet capture

Analysis

Review the packets found.
- Find the packets generated by your successful login.
- Find the packets generated by Hydra failed logins.
- Find the packets generated by Hydra successful login.
- Export only these useful packets in a capture file.

Conclusion

In addition to your conclusion, add the following:
- Was this successful?
- What are the advantages and disadvantages of this attack?
- How would hydra be used to bruteforce an application other than SSH? Give an example.
- How could this attack be prevented?

- For each of the tools used, describe how they do or do 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.