CS471
Security & Info Assurance

Welcome!
4/17/2023

CS471
Security & Info Assurance

Course Schedule

Week #	Monday	Wednesday	Reading	Weekly Topic	Due	Assigned
1	01/16/23	01/18/23		Getting started		
2	01/23/23	01/25/23	Chapter 1	Introduction		Assignment 1
3	01/30/23	02/01/23	Chapter 2	Symmetric Encryption	Assignment 1	Assignment 2
4	02/06/23	02/08/23	Chapter 3	Asymmetric Encryption	Assignment 2	Assignment 3
5	02/13/23	02/15/23	Chapter 4	Key Distribution and Authentication	Assignment 3	
6	02/20/23	02/22/23	Chapters 1-4	Review : **Midterm 1**		
7	02/27/23	03/01/23	Chapter 5	Network Access Control		Assignment 4
8	03/06/23	03/08/23	Chapter 6	Transport Level Security	Assignment 4	Assignment 5
9	03/13/23	03/15/23	Chapter 7	Wireless Network Security		
10	03/20/23	03/22/23	Chapter 8	DNS and Email Security	Assignment 5	
11	03/27/23	03/29/23		Spring Break		
12	04/03/23	04/05/23	Chapters 1-8	Review : **Midterm 2**		
13	04/10/23	04/12/23	Chapter 9	IP Security		Assignment 6
14	04/17/23	04/19/23	Chapter 10	Malicious Software	Assignment 6	Assignment 7
15	04/24/23	04/26/23	Chapter 11	IDS		
16	05/01/23	05/03/23	Chapter 12	Firewalls	Assignment 7	
17	05/08/23	05/10/23		Finals Week		
	*No Meeting			Final Exam: **TBD**		

CS471
Security & Info Assurance

The X.800 service categories will be important for the entire semester.

As we examine security, this will be our measure.

- **X.800 Service Categories**
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Non-repudiation

CS471
Security & Info Assurance

Today

– Malicious Software
– Assignment 6: Create a Honeypot
– Wednesday 4/19 Lecure

CS471
Security & Info Assurance

Malicious Software

– What is ‘Malicious Software’?
– What are the goals of malware?
– How is it distributed?
– What can we do about it?

CS471
Security & Info Assurance

Assignment 6

Design, implement, test, and demonstrate a basic network security ‘honeypot’. Analyze and discuss the results.

Simulate five legitimate network services
First, select 5 different network services to simulate as a honeypot. The Ubuntu system will host these services. For each service, create a listener that logs all connection attempts to a separate log file. Be sure each listener will continually log all connections to a file; it must not only log one connection. The listener must also reply back with something similar to the original service.
Next, run Wireshark to capture the traffic generated during the demonstration of the honeypot.

After all of the listeners are running, attempt to access the honeypot on the simulated services from the Kali VM. You may use the browser, nc, ssh client, nmap, or any other tool of your choice. Be sure to use at least 3 different tools to access simulated services.

CS471
Security & Info Assurance

Assignment 6

Design, implement, test, and demonstrate a basic network security ‘honeypot’. Analyze and discuss the results.

An example of a listener service:
HTTP would be a good service to simulate. For this, listen on port 80 and respond with some text, “HTTP/1.1 200 OK\n\n”. This can be done with netcat. Run the following from the terminal in one copy/paste.

```
while true; do    echo -e "HTTP/1.1 200 OK\n\n $(date)" | nc -l -p 80 -q 1; done
```

What should my service ‘say’?
To determine what each service replies when contacted, try connecting to a real server providing this service. Use netcat to connect, and notice the reply. Use this in your listener to simulate the service.

If testing SSH, be sure the SSH service is not running on the Ubuntu system before attempting to run a listener on the SSH service port, 22.

```
sudo systemctl stop ssh
```

CS471
Security & Info Assurance

Assignment 6

Design, implement, test, and demonstrate a basic network security ‘honeypot’. Analyze and discuss the results.

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.

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.

CS471
Security & Info Assurance

Wednesday, April 19 2023

There will be no lecture for 4/19.
Please use this time to start on assignment 7.

See you on Monday, 4/24.

CS471
Security & Info Assurance

Next time

– Assignment 7: Tails and Tor
– Chapter 11: IDS

CS471
Security & Info Assurance

Thank you!