CSE 127 Week 6 Discussion

Kevin Yu (Winter 2021)
With slides from Ariana Mirian
Legal Notice

This lecture will be recorded and made available to registered students on Canvas.
Agenda

1) PA4 Hints/Common Mistakes
2) PA5 Overview
3) Tools for PA5
4) Questions/OH
PA4 Common Mistakes/Hints

- Challenge 5
  - Must decode base64 string before XORing with key
  - One way is to utilize the “bytes” representation (Python3 only)

- Challenge 6
  - Instead of trying to print a variable in console, try getting the program to print on your behalf

- Challenge 8
  - Column name for database should be the same as in Challenge 7
  - If you are doing a POST request via script, make sure you POST to 'https://c10-32.sysnet.ucsd.edu/level8_password/' NOT 'https://c10-32.sysnet.ucsd.edu/level8_password'
  - To pass payload via requests POST use the “data” argument
PA5 Overview

- Scavenger hunt! You need to find Nadia’s “password” in the form of a token.
- You should be receiving a tar file in your email. This will serve as your starting point.
- The email you should have received should be
  - Subject: [CSE 127] PA5 flash drive dump
  - From: shy147@c10-32.sysnet.ucsd.edu
- Please be cautious of spoilers, utilize OH and private Piazza posts.
- **START EARLY!** You could be stuck for a while if you don’t know what to do, and it can be hard to estimate how much further you still have to go.
PA5 Logistics

- Early Turn-In: 2/16 Tuesday 11:59PM
- Hard Deadline: 2/19 Friday 11:59PM
- Submit to each of the Gradescope assignments:
  - 5. Token
    - Submit a single file named “token”
  - 5. Transcript
    - Submit a “*.txt” file
  - 5. Writeup
    - Any file briefly describing what you did to achieve the end goal
General Tips

- At every point, ask yourself
  - How can I find information that is “hidden” - concealed but still discoverable.
- Some of the steps take time
- Try to find the commands as well as the options that give you exactly what you need.
List of Tools you may need for PA5

- nc - allows you to make connections locally
- nmap - scan ports/IPS (locally and externally)
- ssh - connect to servers over shell
- tcpdump - view network traffic on machine
- wget - download files from the internet
- Check out all their “man” pages
**netcat**

**NC**
like `cat` for your network!

it lets you create TCP (or UDP) connections from the command line & send/receive data

**nc -l PORT**
start a server! this listens on PORT & prints everything received

**send files**
want to send a 100 GB file to someone on the same wifi network? easy!
receiver:
   `nc -l 8080 > file`
sender:
   `192.168.x.x`
cat file | nc YOUR_IP 8080

**make HTTP requests by hand**
`printf 'GET / HTTP/1.1\nHost: example.com\n\r\n\r\n' | nc example.com 80`
type in any weird HTTP request you want! 😎

**nc IP PORT**
be a client! opens a TCP/UDP connection to IP:PORT.

**Julia Evans**
**wizardzines.com**
I love that sending files trick! it works on your local network even if you’re not connected to the internet!
tcpdump

- Used to display TCP/IP and other packets that transported over a network the machine is in
- Reading the tcpdump of a machine can be very noisy
  - Use “tcpdump -D” to see what interfaces are available
  - Specify an interface with the “-i” option
- By default, tcpdump only looks at packet header information. If you wish to view the packet contents, you must use the “-X” or “-A” options.
Questions / Office Hours

Potentially useful links for PA5:

- [https://en.wikipedia.org/wiki/Email_spoofing](https://en.wikipedia.org/wiki/Email_spoofing)