



CSE 127 Discussion 8: PA5 Part 2

Brendon Chen, with slides adapted from prior offerings of CSE 127





This session is being
recorded



PA5

- Network Attacks
- Due June 3, 2021 @ 11:00 AM PDT
- Situation
 - You found a flash drive belonging to a student in Stefan's research group
 - You safety email a dump of the flash drive's contents to yourself
 - You want to breach the research group's network

What to Submit

- 5a. Mystery
 - Hint in the PA itself; it should hopefully be pretty clear when you see it
- 5b. Token
 - The discovered token; a single file named “token”
- 5c. Writeup
 - The steps you took and what tools/flags you used in the process

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

Tools You May Need

- nc - allows you to make connections locally
 - -C
- nmap - scan ports/IPs (locally and externally)
 - -p
- ssh - connect to servers over shell
 - -F, -i
- tcpdump - view traffic on machine
 - -D, -A, -X
- wget - download of files from internet
- **Remember to check out all of their `man` pages**

Additional Tools

- `ls` - list directory contents
 - `-a`
- `tree` - list contents of directories in a tree-like format
 - Useful for viewing the file hierarchy of the flash drive dump
 - You may need to install it (e.g., ``brew install tree`` if you have brew)

tcpdump

- Used to display TCP/IP and other packets that are 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.

test Inbox x



Brendon Chen <brc019@ucsd.edu>

to me ▾

test



from: **Brendon Chen** <brc019@ucsd.edu>
reply-to: brc019@ucsd.edu
to: Brendon Chen <brc019@ucsd.edu>
date: May 26, 2021, 10:29 AM
subject: test
mailed-by: ucsd.edu
➤: Important mainly because it was sent directly to you.

MIME-Version: 1.0
Date: Wed, 26 May 2021 10:29:38 -0700
Reply-To: brc019@ucsd.edu
Message-ID: <CAOX=WbrgTLYQRX7FYm9DBCqDoC81BvdE2COyQ+XukDK6LCC-nQ@mail.gmail.com>
Subject: test
From: Brendon Chen <brc019@ucsd.edu>
To: Brendon Chen <brc019@ucsd.edu>
Content-Type: multipart/alternative; boundary="000000000000b3548805c33efcda"

--000000000000b3548805c33efcda
Content-Type: text/plain; charset="UTF-8"

test

--000000000000b3548805c33efcda
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">test</div>

--000000000000b3548805c33efcda--

SMTP Overview

- Simple Mail Transfer Protocol
- A protocol for **sending** mail
- SMTP servers commonly use TCP on port 25
- SMTPS (S for secure) is often on port 465 as well

SMTP Fields

- **FROM:** this is the field that indicates where the mail is from. This is our traditional notion of who the mail's sender is.
- **RETURN-PATH:** Does not need to be the same as **FROM**. This field indicates where emails should bounce back to if they cannot reach the recipient. Think of this as the return address equivalent of snail mail.
- **REPLY-TO:** This is added by the sender to indicate where human replies should be addressed to. When you press the “Reply” button on, say, your Gmail client, the email in this field will show up as you compose your reply.

MAIL FROM vs. FROM

- **MAIL FROM** and **RCPT TO** are both fields in the “envelope” of the email address whereas **FROM** and other fields are in the “letter” of the email
- **MAIL FROM** is the one used by SMTP servers to transport the mail
- But when it shows up in the client, typically the envelope is discarded and only the **FROM** is shown
- For more on the SMTP Protocol: <https://www.ietf.org/rfc/rfc2821.txt>
- For more on the letter format: <https://www.ietf.org/rfc/rfc2822.txt>

Additional Resources

- https://en.wikipedia.org/wiki/Email_spoofing
- [https://en.wikipedia.org/wiki/Simple Mail Transfer Protocol](https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol)



Office Hours