

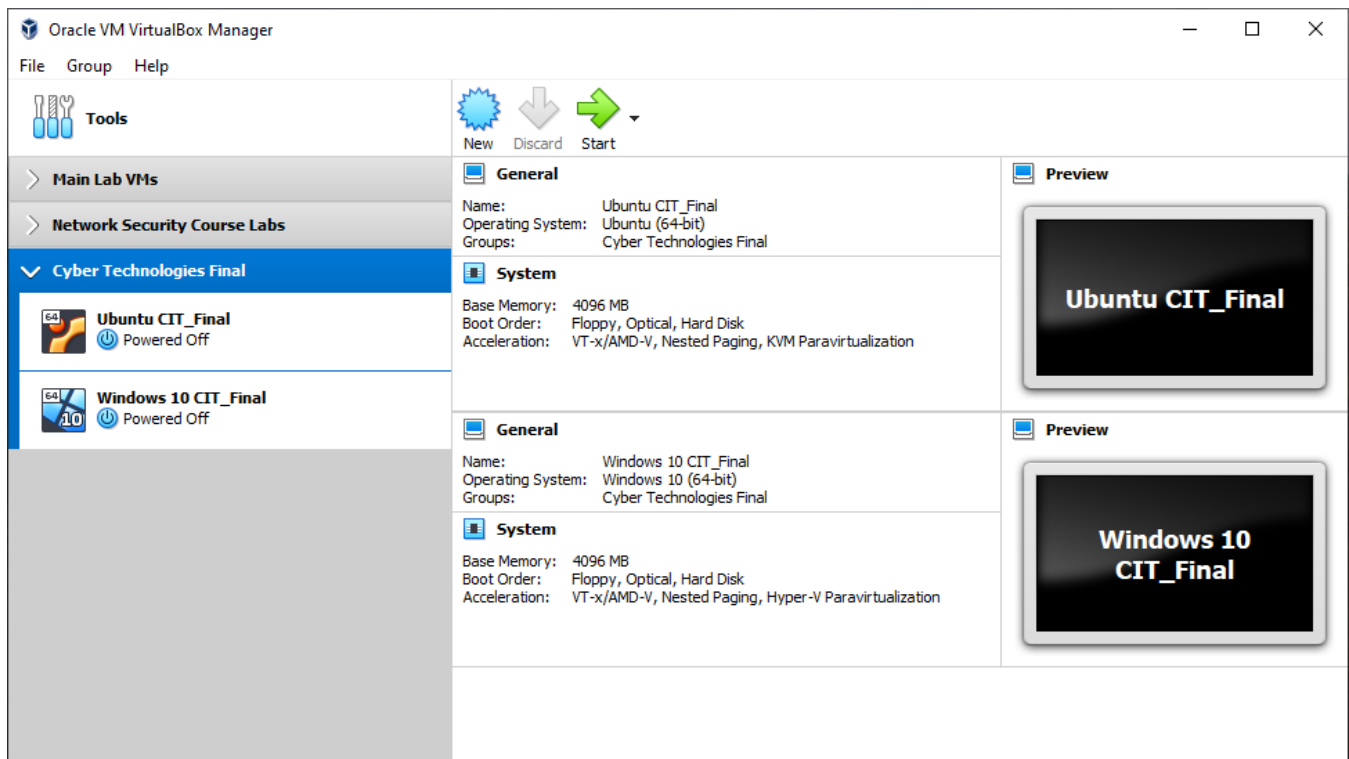
Christopher Dix – NJIT-CS-03 – February 2021

CIT-11-L1: Capture the Flag Challenge

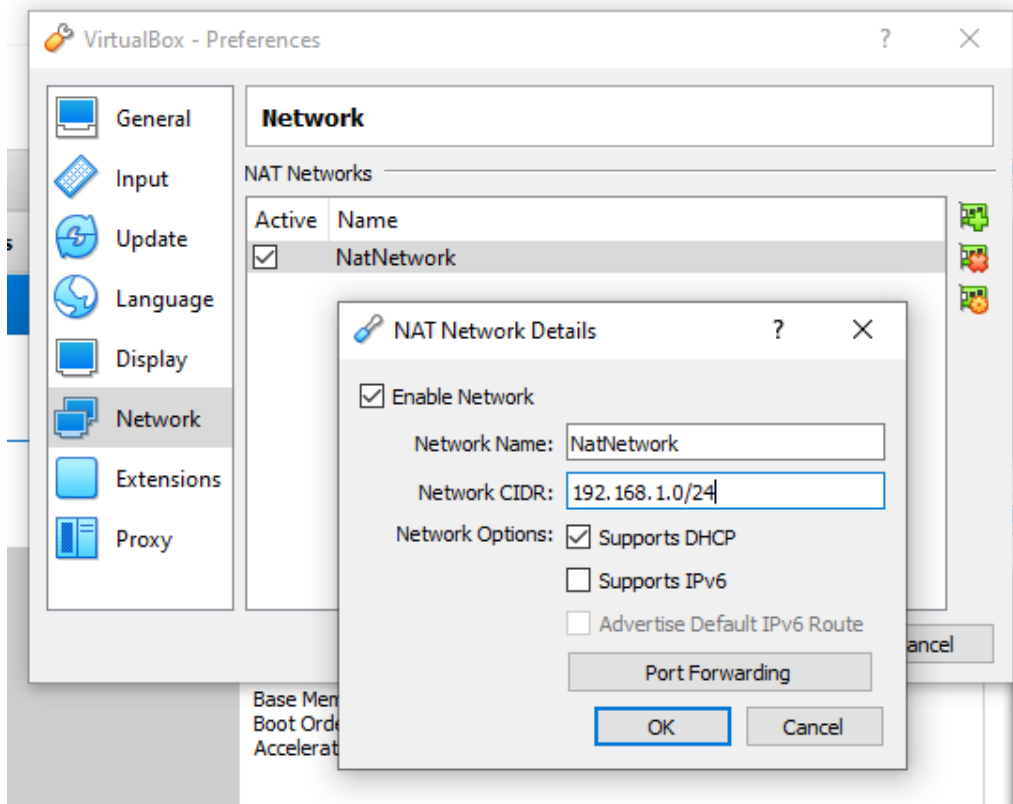
Scenario: An organization's monitoring system identified suspicious download activities captured in a honeypot that was named Cowrie. The event was recorded by the Splunk system, but the system cannot be accessed because its operator, who was the head of the security investigation team, was recently released from the company. Due to the recent events, there was not enough time to provide the information required to access the system freely. However, the system administrator was able to provide access to the mail server and stated that all the data needed to access the system is stored on that server. This project's objective is to connect to the Splunk system, investigate the events, and identify a suspicious message to obtain the *flag*.

Environment Setup:

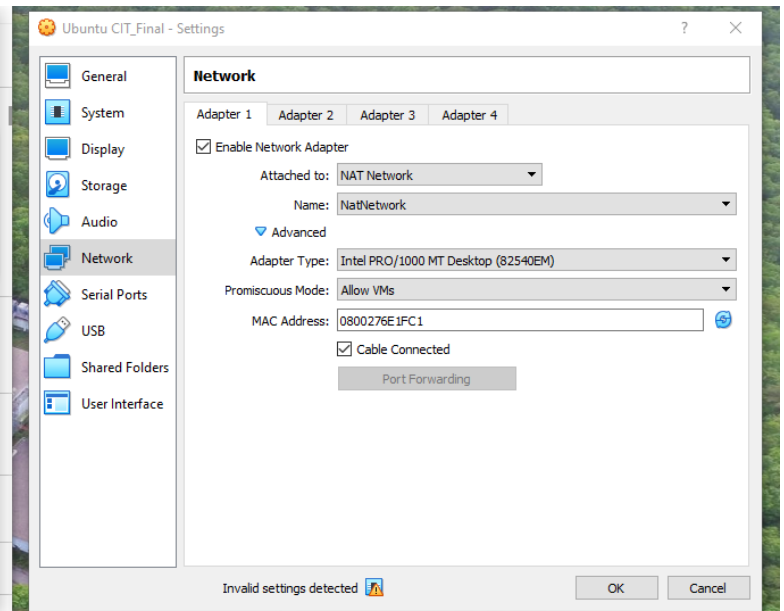
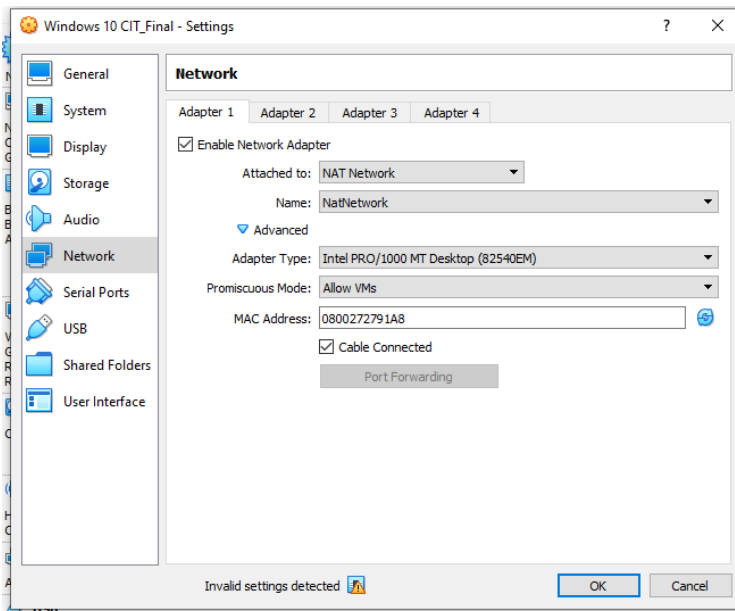
- Two virtual machines were imported into VirtualBox: a Windows system and an Ubuntu system.



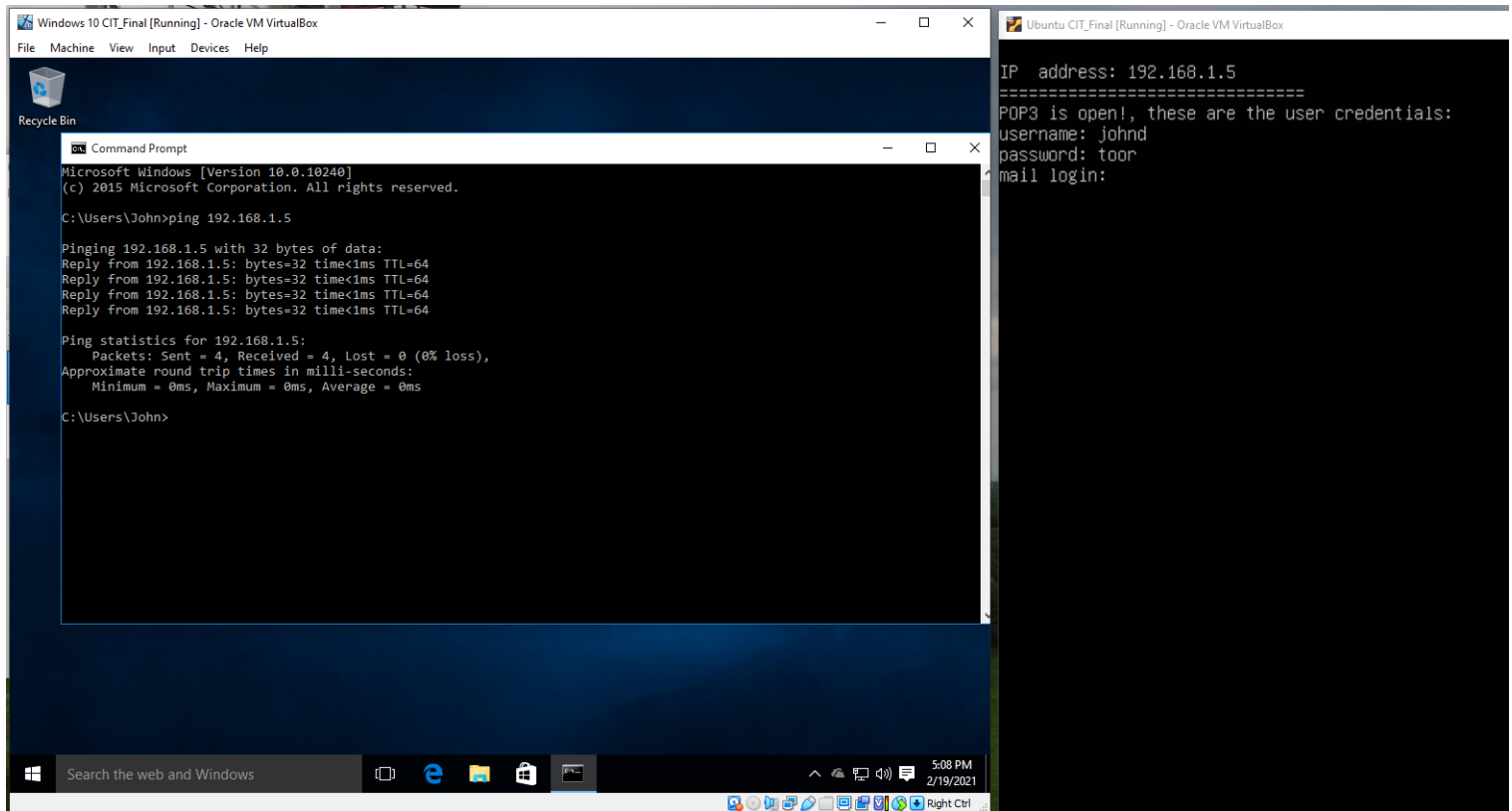
4. The NAT network for both virtual machines was configured to use the 192.168.1.0/24 subnet.



8. Both virtual machines were configured with a NAT adapter on the previously-setup subnet.



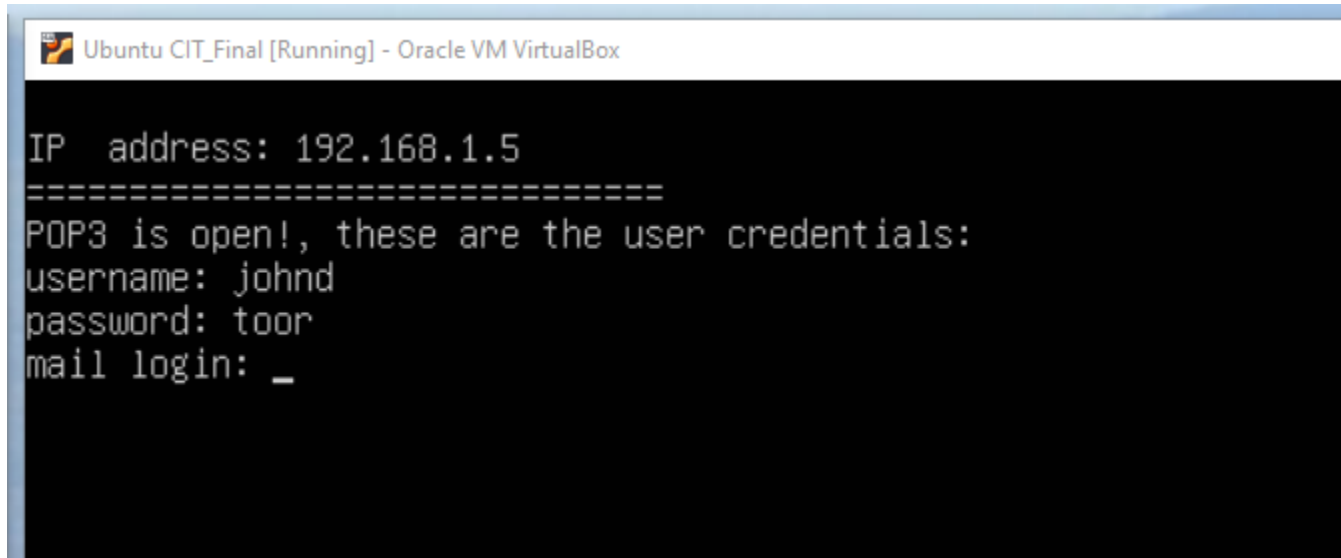
12. Both virtual machines were started, and the IP address of the Ubuntu system was noted. Ping was used from the Windows system to verify that both machines can communicate.



Task 1: Connect to the Mail Server

Objective: Connect to the mail server and retrieve the relevant emails.

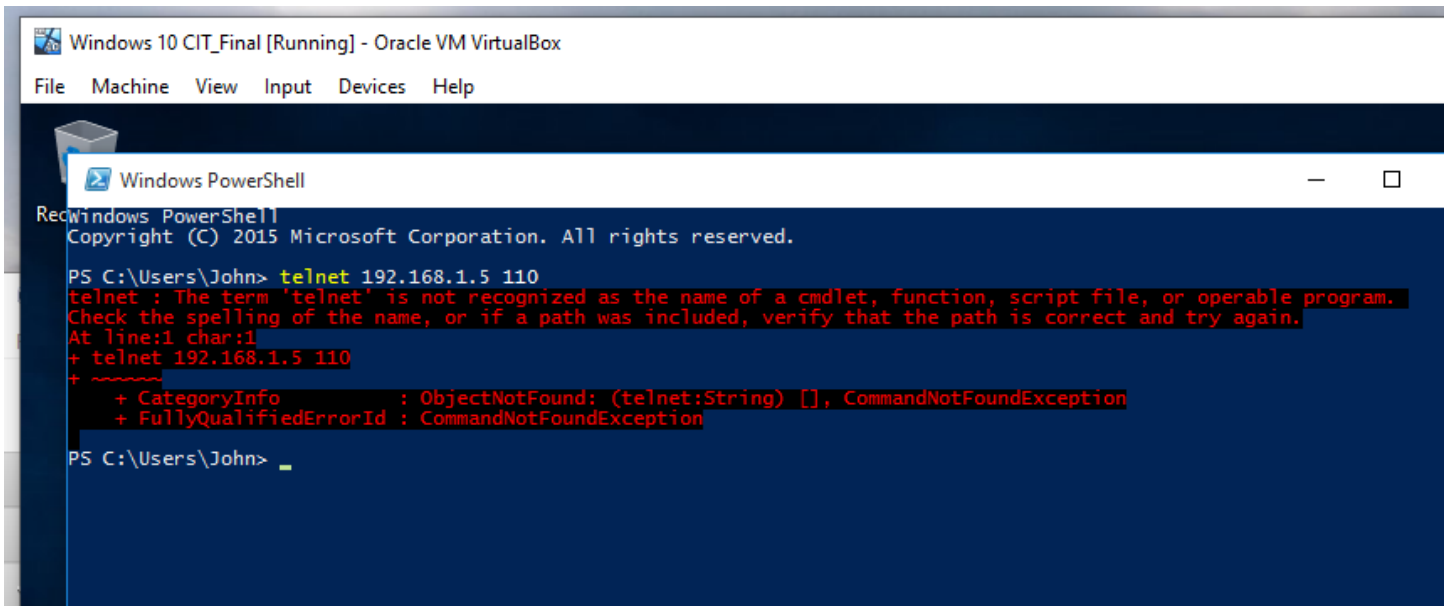
1. Upon startup, the Ubuntu VM prompts that the POP3 port is open, and provides the login credentials.



The screenshot shows a terminal window titled "Ubuntu CIT_Final [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
IP address: 192.168.1.5
=====
POP3 is open!, these are the user credentials:
username: johnd
password: toor
mail login: _
```

2. POP3 uses port 110 by default.
3. From the Windows system, I was initially unable to use PowerShell to connect to the POP3 service via Telnet because the feature was not installed within Windows.



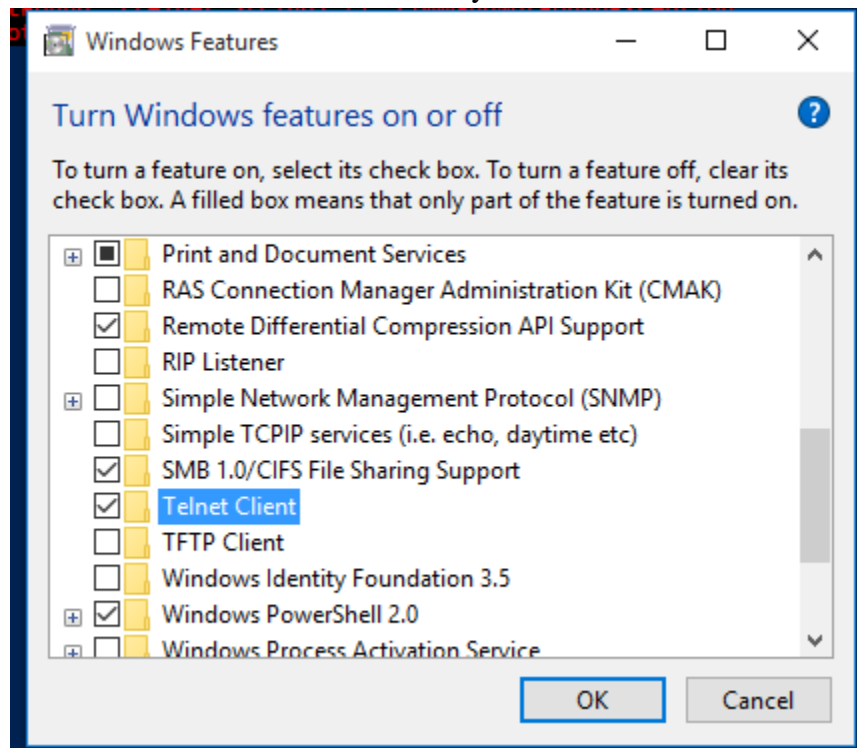
The screenshot shows a Windows 10 VM window titled "Windows 10 CIT_Final [Running] - Oracle VM VirtualBox". Inside, a PowerShell window titled "Windows PowerShell" is open. The terminal output is as follows:

```
RedWindows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

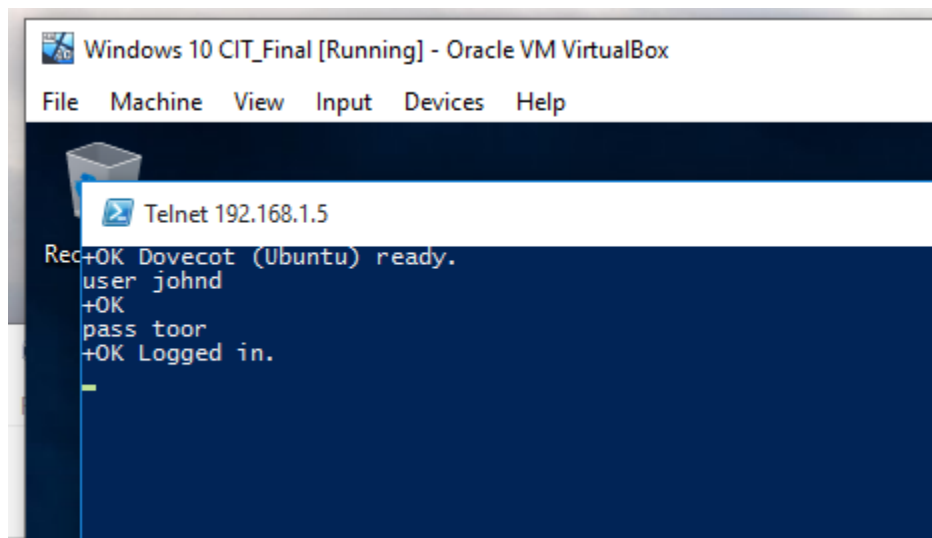
PS C:\Users\John> telnet 192.168.1.5 110
telnet : The term 'telnet' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ telnet 192.168.1.5 110
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (telnet:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\John> _
```

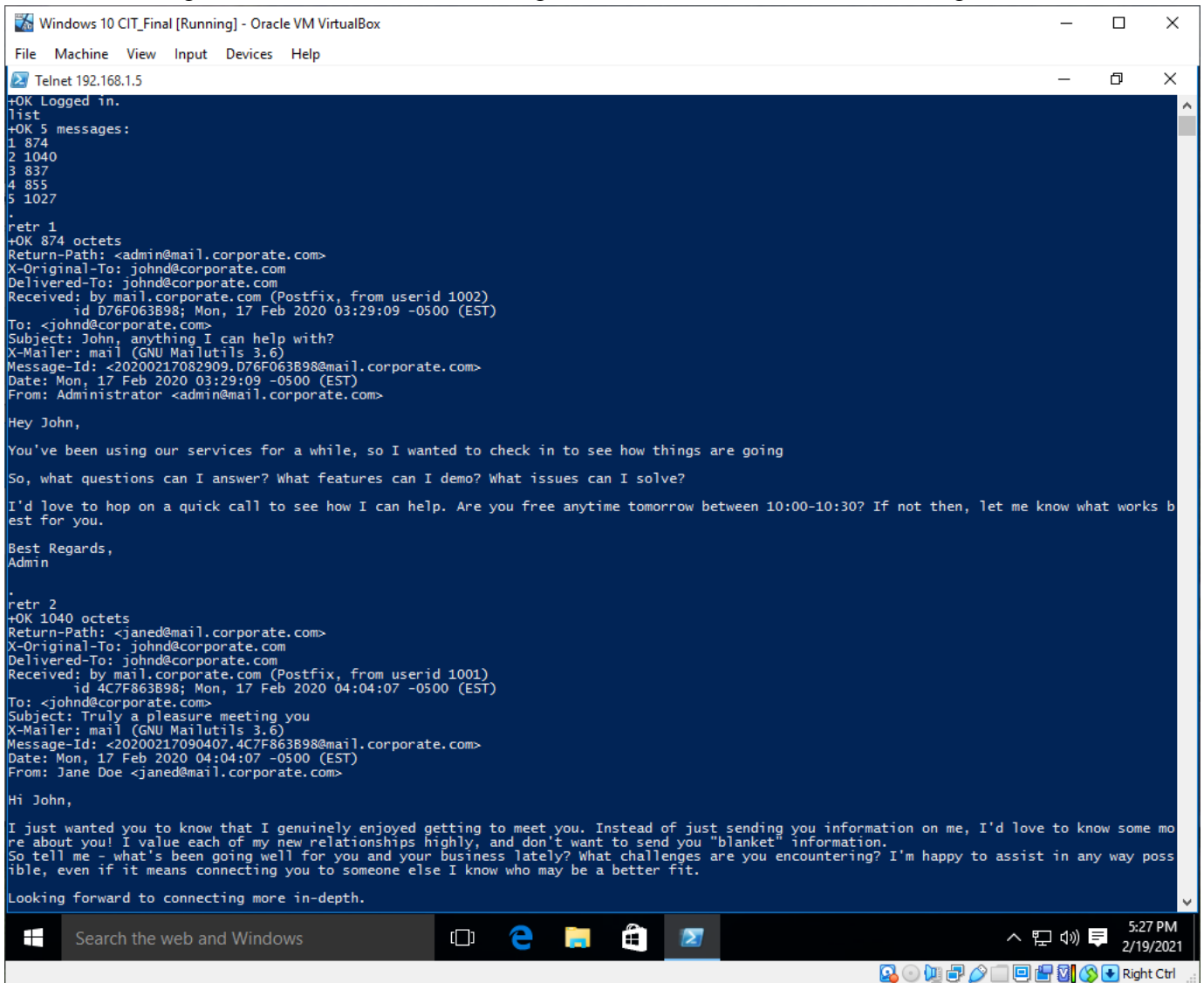
4. The Telnet client was installed onto the Windows system.



5. A Telnet connection was successfully established onto the mail server, and login was successful using the information provided in the message from step 1.



6. The existing emails were listed and investigated, in order to search for interesting information.



```
Windows 10 CIT_Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Telnet 192.168.1.5
+OK Logged in.
list
+OK 5 messages:
1 874
2 1040
3 837
4 855
5 1027
.
retr 1
+OK 874 octets
Return-Path: <admin@mail.corporate.com>
X-Original-To: johnd@corporate.com
Delivered-To: johnd@corporate.com
Received: by mail.corporate.com (Postfix, from userid 1002)
        id D76F063B98; Mon, 17 Feb 2020 03:29:09 -0500 (EST)
To: <johnd@corporate.com>
Subject: John, anything I can help with?
X-Mailer: mail (GNU Mailutils 3.6)
Message-Id: <20200217082909.D76F063B98@mail.corporate.com>
Date: Mon, 17 Feb 2020 03:29:09 -0500 (EST)
From: Administrator <admin@mail.corporate.com>

Hey John,

You've been using our services for a while, so I wanted to check in to see how things are going

So, what questions can I answer? What features can I demo? What issues can I solve?

I'd love to hop on a quick call to see how I can help. Are you free anytime tomorrow between 10:00-10:30? If not then, let me know what works best for you.

Best Regards,
Admin


.
retr 2
+OK 1040 octets
Return-Path: <janed@mail.corporate.com>
X-Original-To: johnd@corporate.com
Delivered-To: johnd@corporate.com
Received: by mail.corporate.com (Postfix, from userid 1001)
        id 4C7F863B98; Mon, 17 Feb 2020 04:04:07 -0500 (EST)
To: <johnd@corporate.com>
Subject: Truly a pleasure meeting you
X-Mailer: mail (GNU Mailutils 3.6)
Message-Id: <20200217090407.4C7F863B98@mail.corporate.com>
Date: Mon, 17 Feb 2020 04:04:07 -0500 (EST)
From: Jane Doe <janed@mail.corporate.com>

Hi John,

I just wanted you to know that I genuinely enjoyed getting to meet you. Instead of just sending you information on me, I'd love to know some more about you! I value each of my new relationships highly, and don't want to send you "blanket" information.
So tell me - what's been going well for you and your business lately? What challenges are you encountering? I'm happy to assist in any way possible, even if it means connecting you to someone else I know who may be a better fit.

Looking forward to connecting more in-depth.
```

The credentials for the Splunk application were found in message 4.



```
.
retr 4
+OK 855 octets
Return-Path: <admin@mail.corporate.com>
X-Original-To: johnd@corporate.com
Delivered-To: johnd@corporate.com
Received: by mail.corporate.com (Postfix, from userid 1002)
        id 53D6463B98; Mon, 17 Feb 2020 04:08:18 -0500 (EST)
To: <johnd@corporate.com>
Subject: We launched Splunk!
X-Mailer: mail (GNU Mailutils 3.6)
Message-Id: <20200217090818.53D6463B98@mail.corporate.com>
Date: Mon, 17 Feb 2020 04:08:18 -0500 (EST)
From: Administrator <admin@mail.corporate.com>

Hey there,

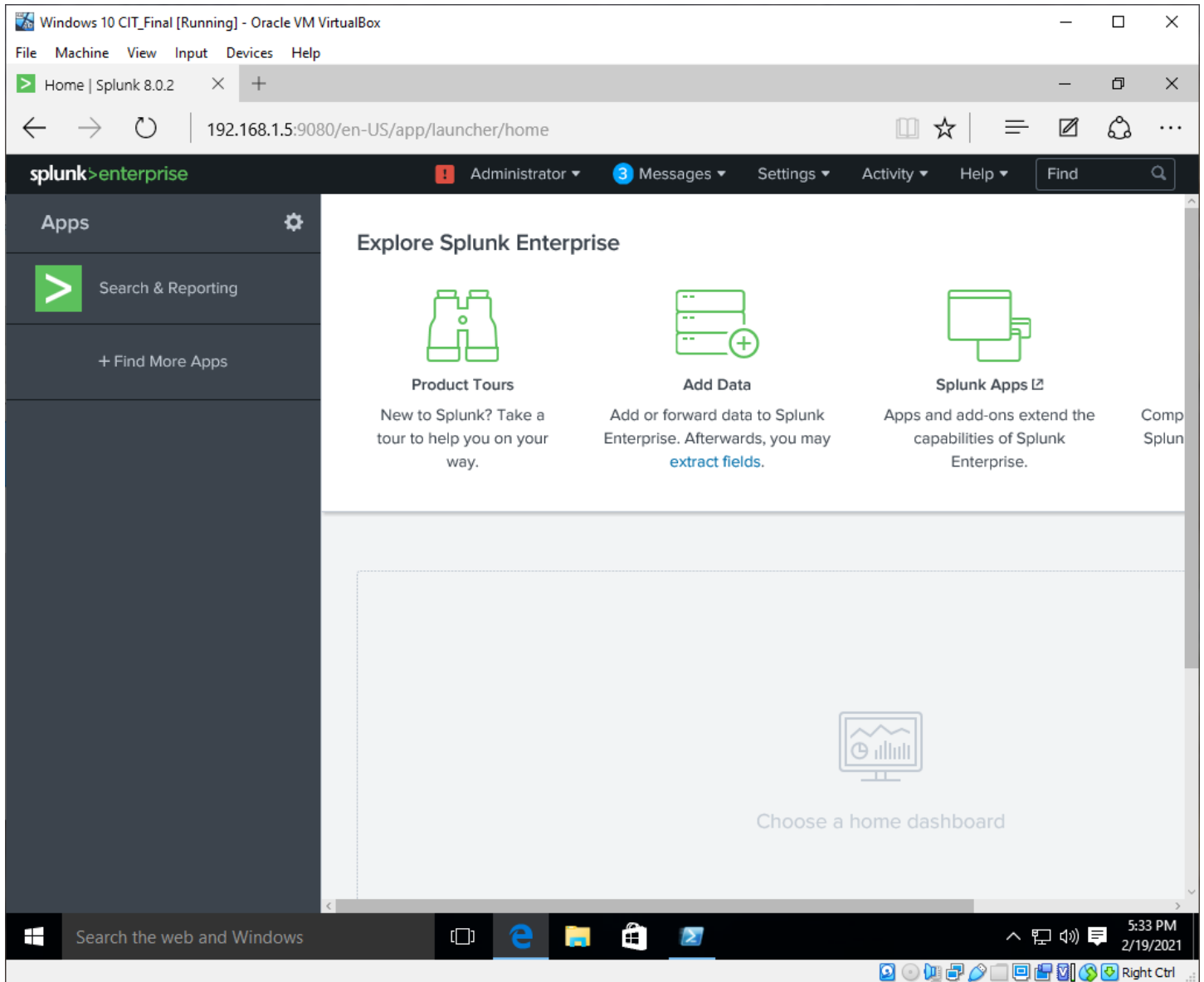
We wanted to call your attention to our new SIEM product we released over night.
Using this new feature, you'll be able to investigate for suspicious events.
If you have any questions about the best ways to use Splunk, please feel free to give us a call at +1-202-555-0128.

To use Splunk, navigate to the following URI:
http://[SERVER-IP]:9080/

The credentials are as follow:
username: admin
password: CIT_Final!

Thank you,
Admin
```

7. The provided URL and credentials were used to successfully log into the Splunk system.



Lab Task 2: Search for Suspicious Activity

Objective: Search the SIEM for recorded suspicious activity in the organization.

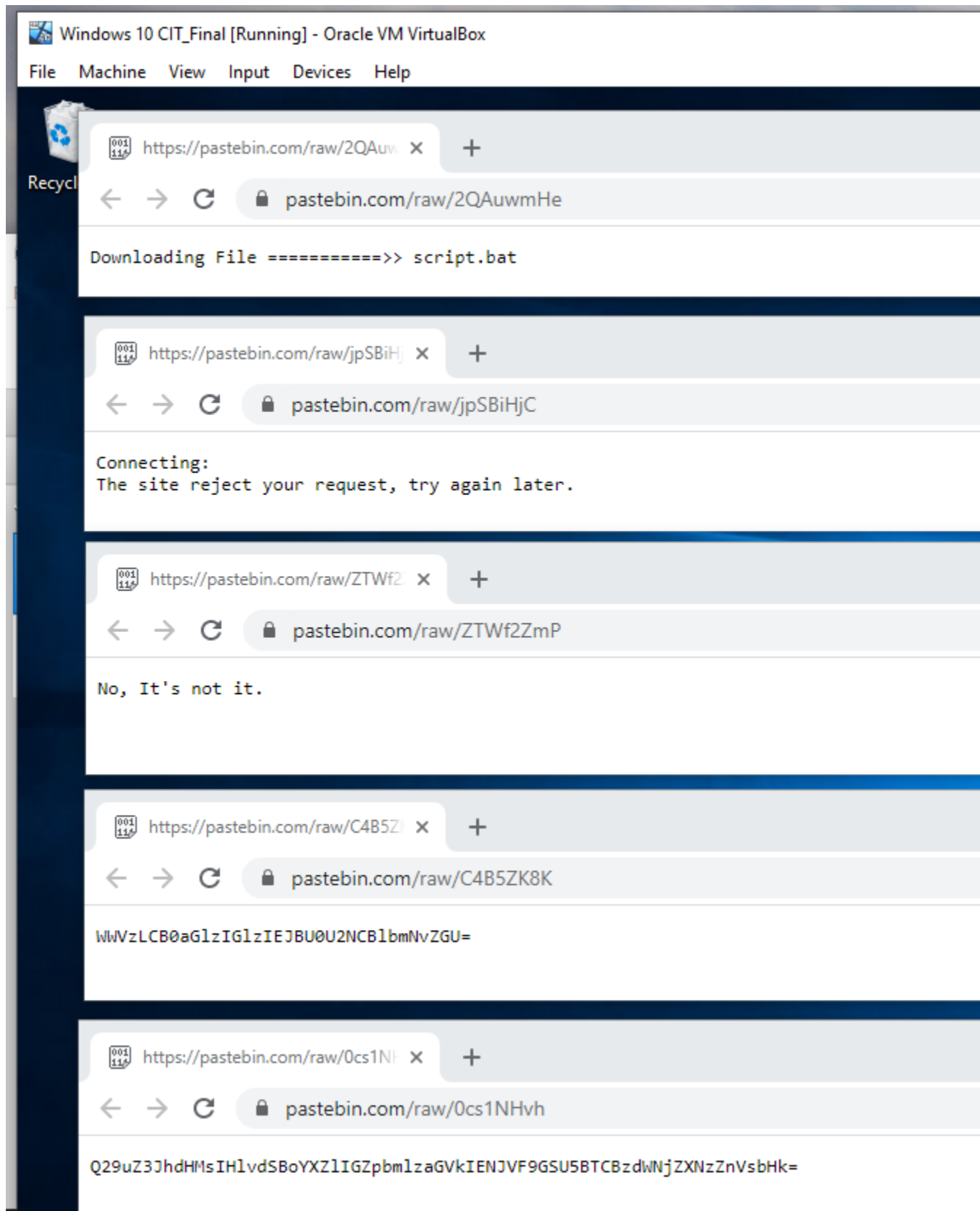
1. In Splunk, a search with the query `cowrie download` was made to find records of the suspicious activity. Returned events show several failed download attempts from various PasteBin URLs. There were 28 total events, and, amongst those, downloads were attempted from 5 different sources (all on PasteBin).

The screenshot shows the Splunk 8.0.2 interface within a Windows 10 VM. The search bar contains the query `cowrie download` and the results are displayed in a list view. The search results show 28 events, with the first two events highlighted. The interface includes a sidebar with field lists, a top navigation bar, and a main content area with event details.

Search Results:

Time	Event
11/23/20 2:23:34.000 AM	<pre>{ [-] eventid: cowrie.session.file_download.failed message: Attempt to download file(s) from URL (https://pastebin.com/raw/2QAuwmHe) failed sensor: mail.corporate.com session: a8e3f8b33ca5 src_ip: 192.168.56.1 timestamp: 2020-07-27T07:26:28.143015Z url: https://pastebin.com/raw/2QAuwmHe }</pre>
11/23/20 2:23:34.000 AM	<pre>{ [-] eventid: cowrie.session.file_download.failed message: Attempt to download file(s) from URL (https://pastebin.com/raw/jpSBiHjC) failed sensor: mail.corporate.com session: a8e3f8b33ca5 src_ip: 192.168.56.1 timestamp: 2020-07-27T07:27:38.269025Z url: https://pastebin.com/raw/jpSBiHjC }</pre>

- The five PasteBin URLs were accessed for further investigation. Three of them appeared to contain irrelevant information, and the other two contained text that seemed to be either encoded or hashed.




3. I first tried to run the two “interesting” texts through reverse hashing tools, but the strings were not the correct length for any known hashing algorithm. I then assumed that the messages were encoded and not hashed (which would make more sense in this scenario, since the messages/“flags” were meant to be decoded and hashing is generally one-way), and ran the strings through a Base64 decoder. The first string (ending in “ZGU”) decoded to say “Yes, this is BASE64 encode,” verifying the correct encoding algorithm, and the second string proved to be the flag for this project, decoding to “Congrats, you have finished CIT_FINAL successfully.”

Decode from Base64 format


Simply enter your data then push the decode button.



```
WWVzLCB0aGlzIGlzIEJBU0U2NCBlbmNvZGU=
```

 For encoded binaries (like images, documents, etc.) use the file uploader

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries)

 Live mode OFF Decodes in real-time as you type or paste (slow)

 **DECODE**  Decodes your data into the area below.

```
Yes, this is BASE64 encode
```

Decode from Base64 format


Simply enter your data then push the decode button.

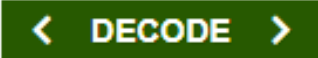

Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVf9GSU5BTCBzdWNjZXNzZnVsbHk=

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on the page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

Congrats, you have finished CIT_FINAL successfully

Flag: Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVf9GSU5BTCBzdWNjZXNzZnVsbHk=