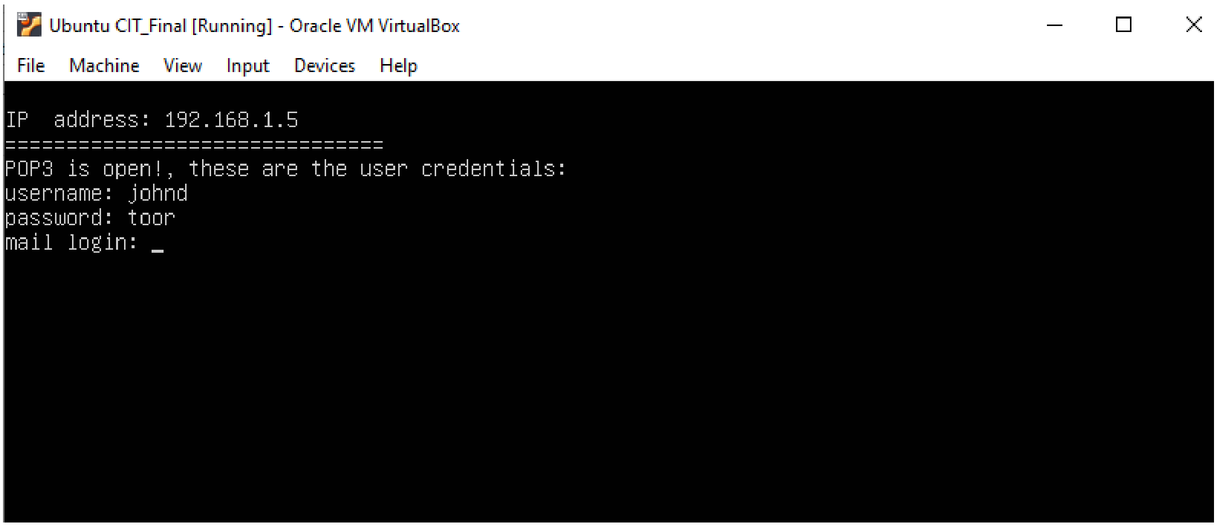
Jakub Jędrzejczak

Task 1: Connect to the Mail Server

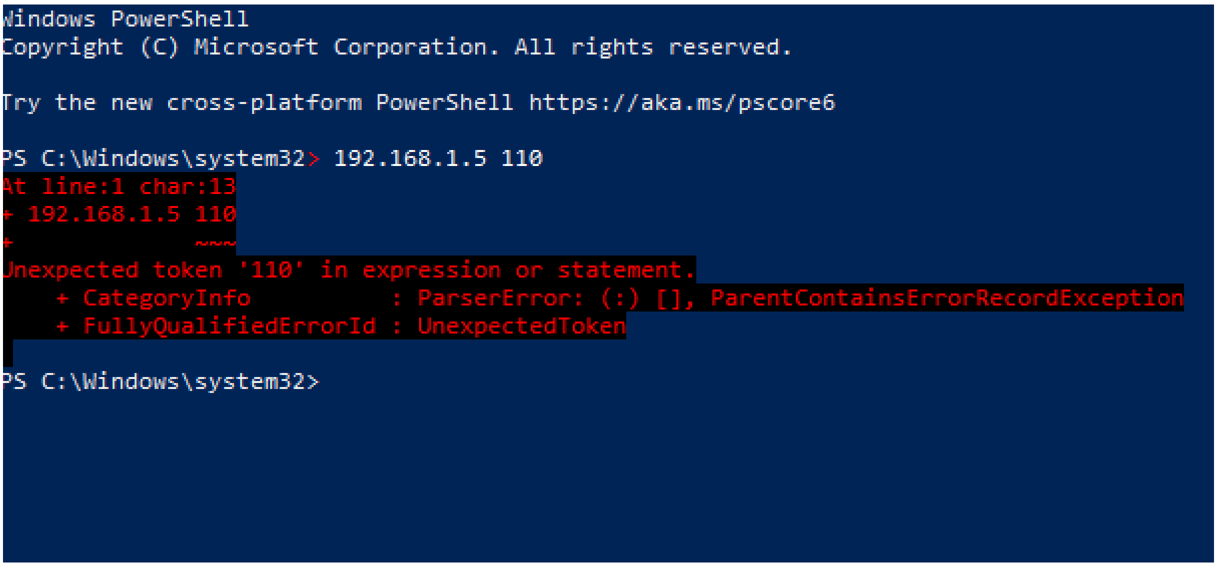
1.


Ubuntu CIT_Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

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

2. 110

3.

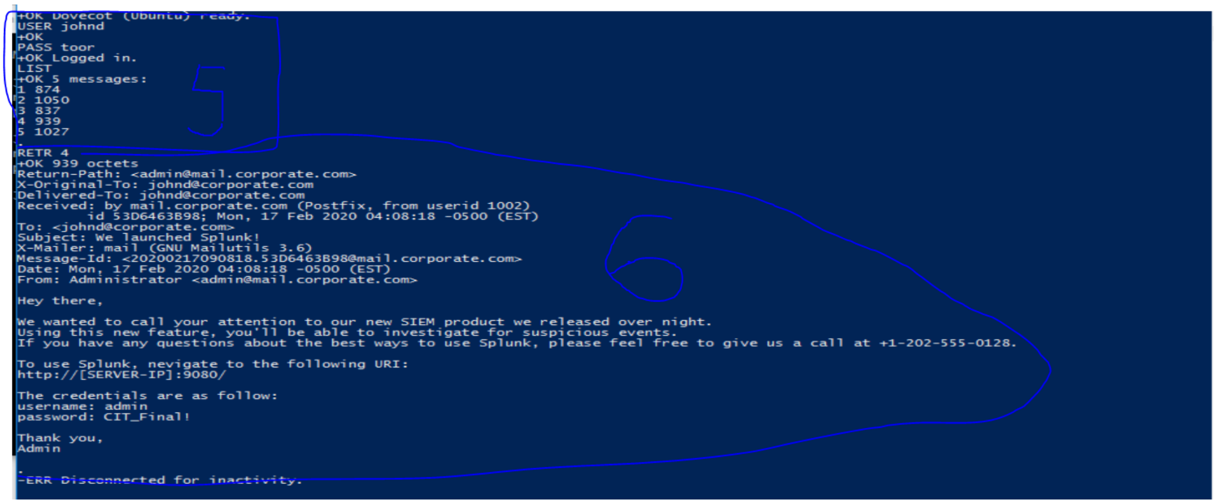


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> 192.168.1.5 110
At line:1 char:13
+ 192.168.1.5 110
+             ~~~
Unexpected token '110' in expression or statement.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : UnexpectedToken

PS C:\Windows\system32>
```

nie udało się połączyć z powodu braku instalacji telnet na win10

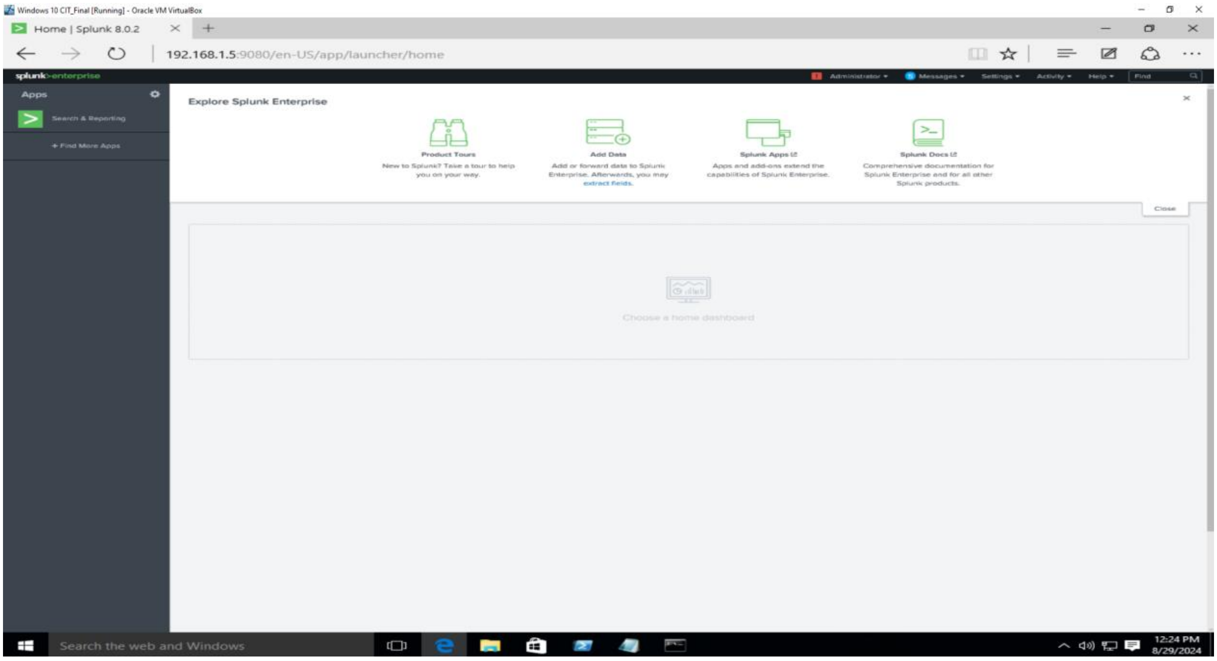
4. dism /online /Enable-Feature /FeatureName:TelnetClient

5 i 6.



```
+OK Dovecot (Ubuntu) ready.
USER johnd
+OK
PASS toor
+OK Logged in.
LIST
+OK 5 messages:
1 874
2 1050
3 837
4 939
5 1027
.
RETR 4
+OK 939 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, nevigate to the following URI:
http://[SERVER-IP]:9080/

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

Thank you,
Admin

.
-ERR Disconnected for inactivity.
```

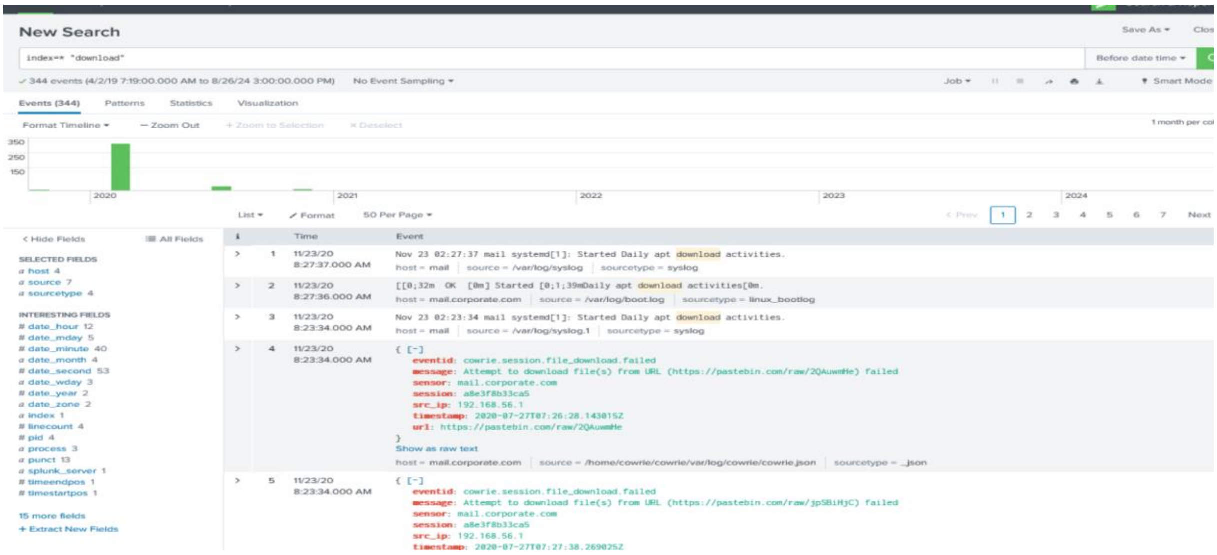
7.



Windows 10 CIT_Final [Running] - Oracle VM VirtualBox
Home | Splunk 8.0.2
192.168.1.5:9080/en-US/app/launcher/home
splunk>enterprise
Administrator
Messages
Settings
Activity
Help
Find
Apps
Search & Reporting
+ Find More Apps
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.
Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.
Close
Choose a home dashboard
Search the web and Windows
12:24 PM
8/29/2024

Task 2: Search for Suspicious Activity

1.



```
index=* "download"
```

✓ 344 events (4/2/19 7:19:00.000 AM to 8/26/24 3:00:00.000 PM)   No Event Sampling ▾

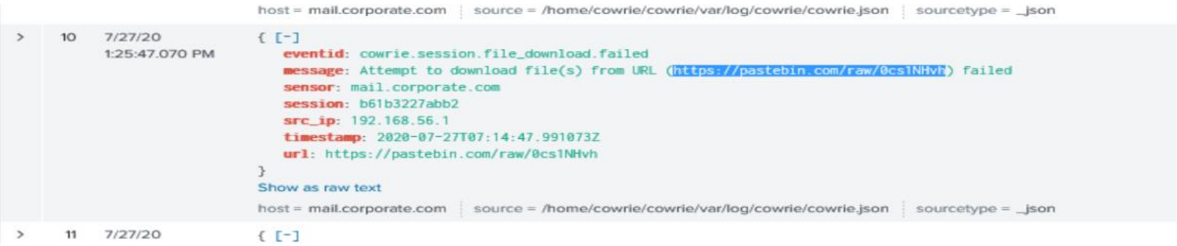
SELECTED FIELDS
- a host 4
- a source 7
- a sourcetype 4

INTERESTING FIELDS
- # date_hour 12
- # date_mday 5
- # date_minute 40
- a date_month 4
- # date_second 53
- a date_wday 3
- # date_year 2
- a date_zone 2
- a index 1
- # linecount 4
- # pid 4
- a process 3
- a punct 13
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1

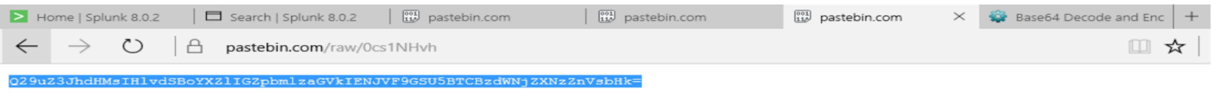
15 more fields
+ Extract New Fields

```
i     Time                  Event
> 1   11/23/20              Nov 23 02:27:37 mail systemd[1]: Started Daily apt download activities.
      8:27:37.000 AM        host = mail | source = /var/log/syslog | sourcetype = syslog
> 2   11/23/20              [[0;32m  OK  [0m] Started [0;1;39mDaily apt download activities[0m.
      8:27:36.000 AM        host = mail.corporate.com | source = /var/log/boot.log | sourcetype = linux_bootlog
> 3   11/23/20              Nov 23 02:23:34 mail systemd[1]: Started Daily apt download activities.
      8:23:34.000 AM        host = mail | source = /var/log/syslog.1 | sourcetype = syslog
> 4   11/23/20              { [-]
      8:23:34.000 AM           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
                            }
                            Show as raw text
                            host = mail.corporate.com | source = /home/cowrie/cowrie/var/log/cowrie/cowrie.json | sourcetype = _json
> 5   11/23/20              { [-]
      8:23:34.000 AM           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
```

2.



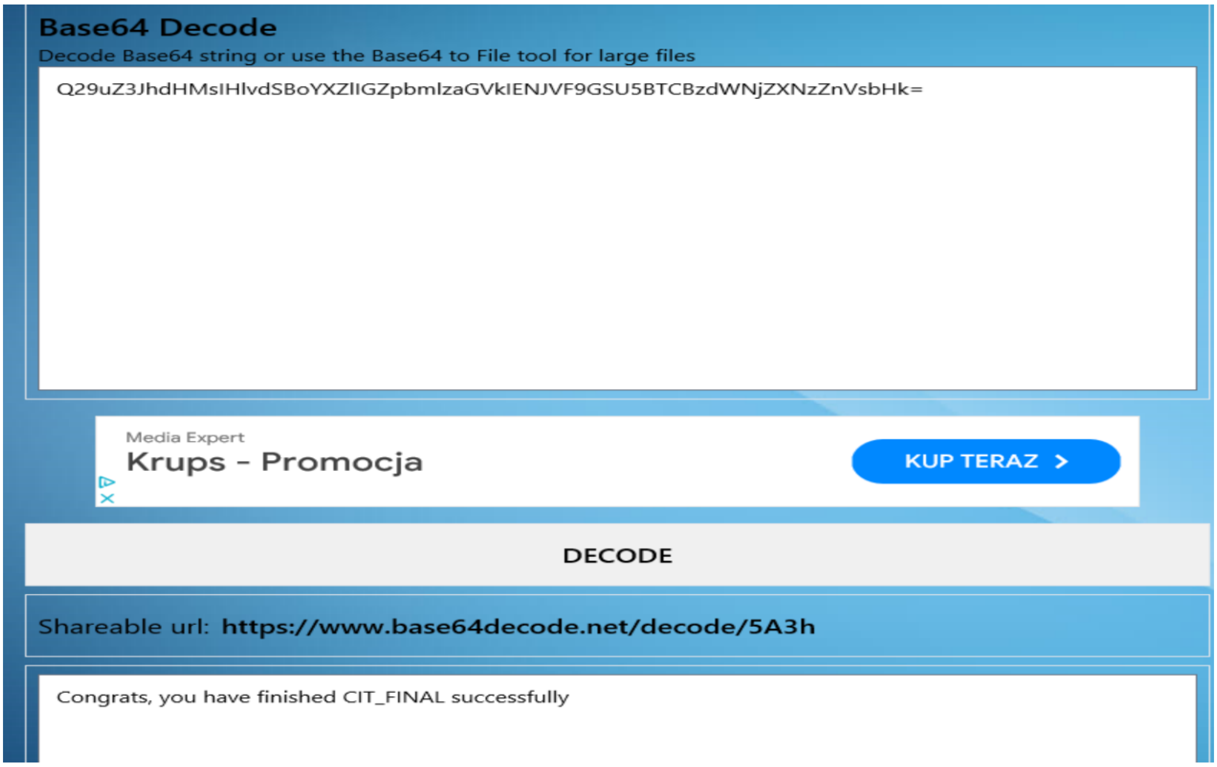
```
                        host = mail.corporate.com | source = /home/cowrie/cowrie/var/log/cowrie/cowrie.json | sourcetype = _json
> 10  7/27/20           { [-]
      1:25:47.070 PM       eventid: cowrie.session.file_download.failed
                           message: Attempt to download file(s) from URL (https://pastebin.com/raw/0cs1NHvh) failed
                           sensor: mail.corporate.com
                           session: b61b3227abb2
                           src_ip: 192.168.56.1
                           timestamp: 2020-07-27T07:14:47.991073Z
                           url: https://pastebin.com/raw/0cs1NHvh
                        }
                        Show as raw text
                        host = mail.corporate.com | source = /home/cowrie/cowrie/var/log/cowrie/cowrie.json | sourcetype = _json
> 11  7/27/20           { [-]
```



pastebin.com/raw/0cs1NHvh

Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVF9GSU5BTCBzdWNjZXNzZnVsbHk=

3.



Base64 Decode

Decode Base64 string or use the Base64 to File tool for large files

Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVF9GSU5BTCBzdWNjZXNzZnVsbHk=

Shareable url: **https://www.base64decode.net/decode/5A3h**

```
Congrats, you have finished CIT_FINAL successfully
```