# CYBER SMURFS

Final Project: Cyber Ops 401

# Agenda

Team Member Introductions

Problem Domain & Project Overview

Team Process & Documentation

Application Demonstration

Q&A

CYBER SMURFS


# Our Team

1. Connie Uribe Chavez
2. Nickolaus Alderete
3. Robert Gregor
4. Jeremy Patton
5. Paul Stroud

CYBER SMURFS

# Nickolaus Alderete

- US Army veteran- 12T- TOPO/ Geodetic engineer
- Low Voltage Electrician
  - Data/ Security system installs
  - CCTV- Installs and programming
  - Network room build-outs

CYBER SMURFS

# Connie Uribe Chavez

- Veteran located in Pensacola, FL
- B.A. in computer science
- Previous programming experience
- Enjoy being outdoors

CYBER SMURFS

# Robert Gregor

- US Army Veteran (TS/SCI)
- Previously employed on a DoD Red Team
- SANS Undergraduate Certificate in Applied Cybersecurity
- GFACT, GSEC, GCIH, GPEN
- Pursuing a defensive cyber security position

GFACT GSEC GCIH GPEN

CYBER SMURFS

# Jeremy Patton

- 14 Years of mechanical experience
- High demand for cybersecurity
- Long-term job security
- Opportunities for growth

CYBER SMURFS

# Paul Stroud

- Former U.S. Army officer
- Associate’s degree in Cybersecurity
- Work experience in IT/Telecom
- Splendid memes for days

CYBER SMURFS

# Problem Domain

Financial asset management company is seeking an adversary simulation exercise to find the weak spots in its cyber defenses.

The company has already suffered a security breach due to misconfiguration and is looking to locate and mitigate vulnerabilities.

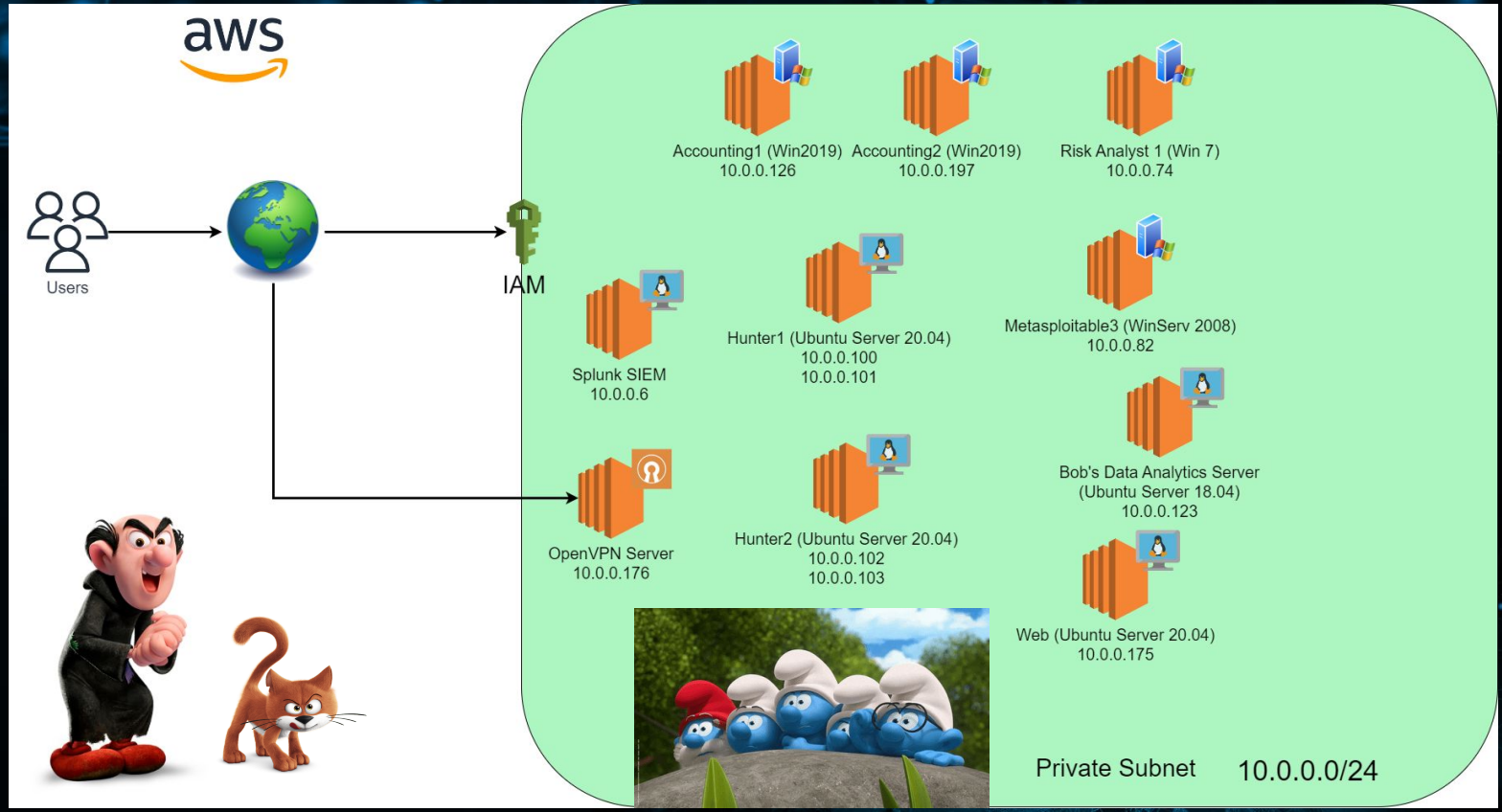
CYBER SMURFS

# Solutions

- Consolidate all logs on a Splunk server
- Monitor network activity with SPL queries
- Generate alerts for suspicious activity
- Automate detection via IDS and scripts
- Report all findings to the customer

CYBER SMURFS

# Topologies and Flowcharts




CYBER SMURFS

# Demo!

CYBER SMURFS

# Splunk Triggers

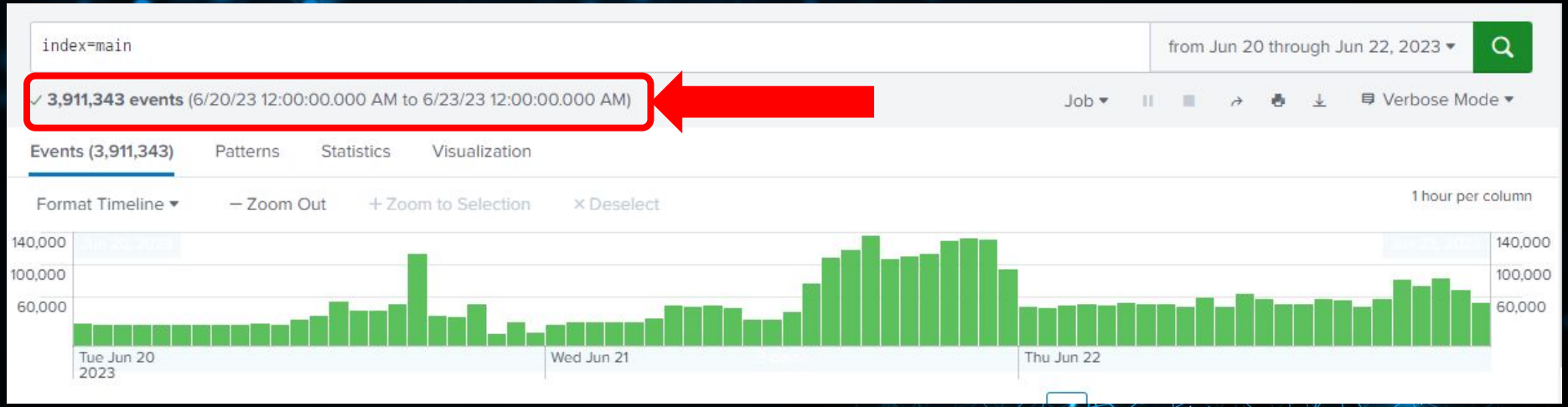
- Brute Force Windows & Linux attack identification
  - index=main EventCode=4625
  - index=main "Failed password"
  - Threshold = 10 failed login attempts in 10 sec
- Metasploit signature identification
  - index=main port=4444 OR
  - user_agent="*Metasploit*" OR
  - user_agent="*Mozilla/4.0 (compatible; MSIE 6.1; Windows NT)*"
- Windows & Linux successful logins
  - index=main EventCode=4624
  - index=main “sshd” AND “Accepted” AND “for”
- Windows & Linux account creation
  - index=main EventCode=4720
  - index=main "COMMAND=/usr/sbin/useradd" OR
  - "COMMAND=/usr/sbin/adduser"

```
New Account:
    Security ID:        S-1-5-21-2020954294-3820947412-549806118-1006
    Account Name:       Settings
    Account Domain:     ACCOUNTING1

Attributes:
    SAM Account Name:   Settings
```

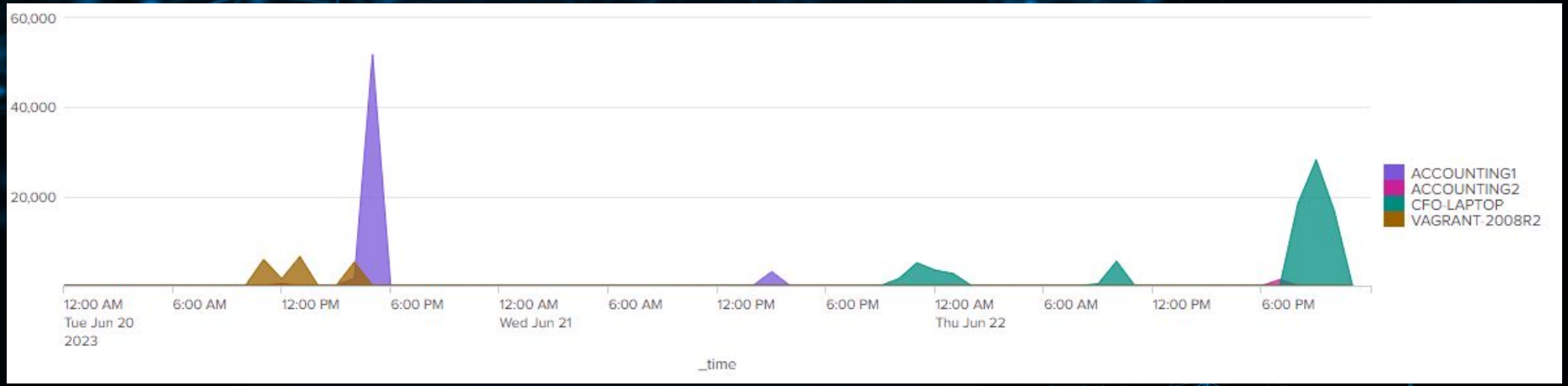
```
New Account:
    Security ID:        S-1-5-21-2020954294-3820947412-549806118-1005
    Account Name:       SUPERHAXOR
    Account Domain:     CFO-LAPTOP

Attributes:
    SAM Account Name:   SUPERHAXOR
```

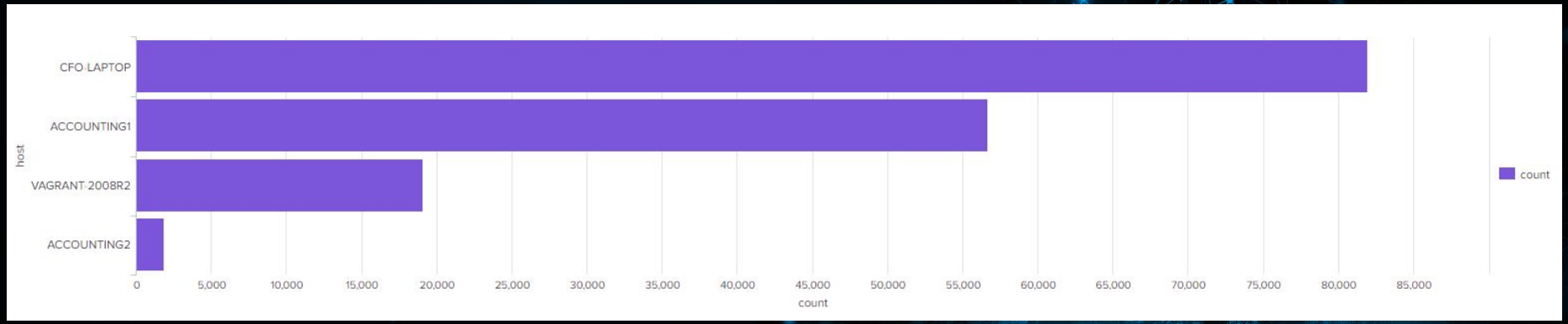
CYBER SMURFS

# Event Logs


index=main
from Jun 20 through Jun 22, 2023
3,911,343 events (6/20/23 12:00:00.000 AM to 6/23/23 12:00:00.000 AM)
Job
Verbose Mode
Events (3,911,343)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
140,000
100,000
60,000
Tue Jun 20
2023
Wed Jun 21
Thu Jun 22

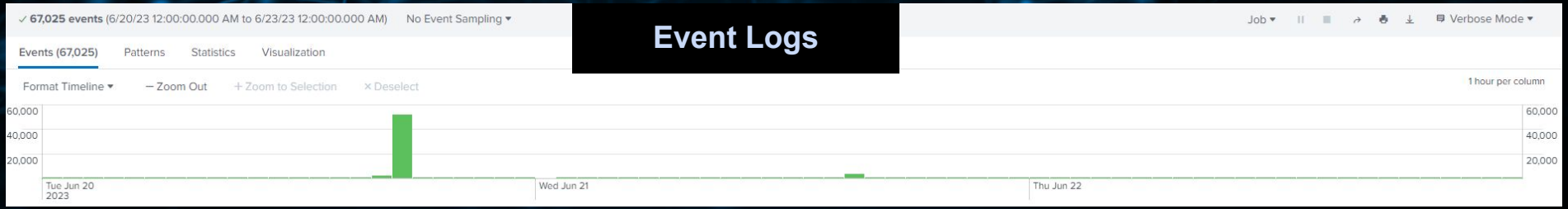
# Brute Force Attack



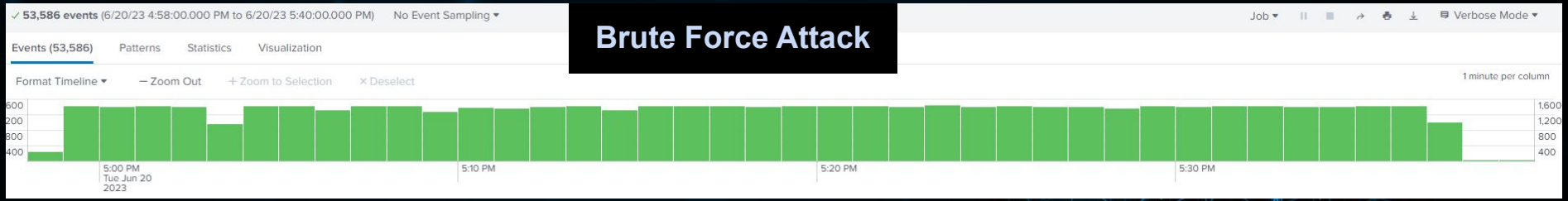



# ACCOUNTING 1

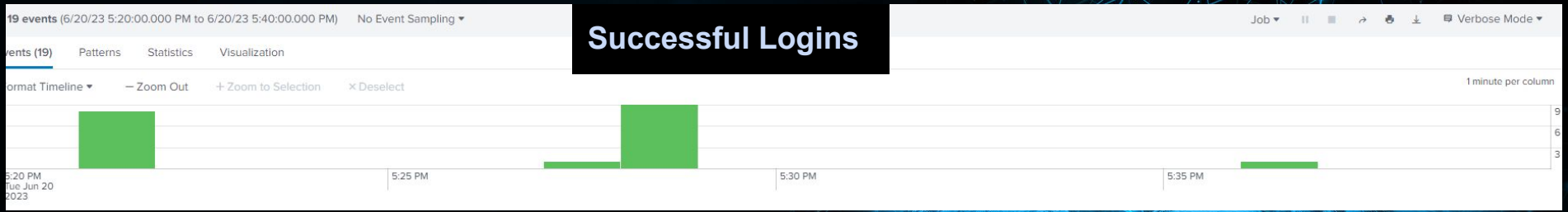
## Event Logs




## Brute Force Attack




## Successful Logins




16:58 - 17:38 CT → 53,460 failed attempts
17:21:31 CT → First Successful Login

**Summary**

*20 June 2023*

VAGRANT/Metasploitable3 (10.0.0.82)

11:50 - 16:10 → 19,080 failed attempts

16:08:55 → first successful login

Accounting2 (10.0.0.197)

12:52 - 13:00 → 493 failed attempts

12:52:16 → first Successful login

Accounting1 (10.0.0.126)

16:58 - 17:38 CT → 53,460 failed attempts

17:21:31 → first successful login

*22 June 2023*

CFO (10.0.0.206)

09:56 - 10:46 → 81,972 failed attempts

N/A → First successful login

# SSH/ RDP Connection

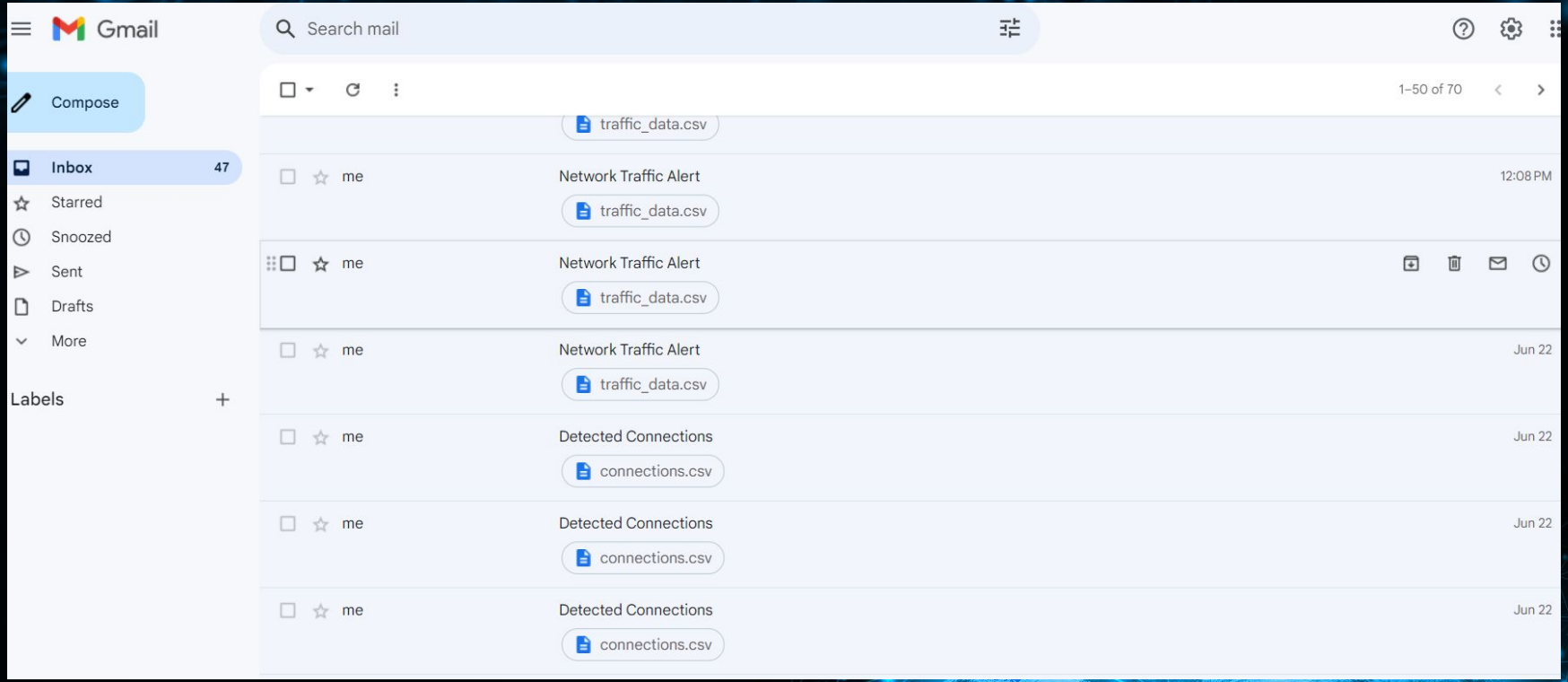
```python
#!/usr/bin/python3
# Nick Alderete & Jeremy Patton
# Scan network for SSH and RDP connection



import csv
import datetime
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.base import MIMEBase
from email import encoders
import socket

# List of known IP addresses
known_ip_addresses = ['10.0.0.126', '10.0.0.197', '10.0.0.123', '10.0.0.82', '10.0.0.74', '10.0

# List of IP addresses to scan
ip_addresses = ['192.168.0.1', '192.168.0.2', '192.168.0.3']  # Add your IP addresses here

# Ports to check
rdp_port = 3389  # RDP port
ssh_port = 22  # SSH port

# CSV file name
csv_file = 'connections.csv'

# Email details
sender_email = 'hunter2user@gmail.com'
```

| | | | | |
|---|---|---|---|---|
| 109 | 2023-06-22 14:47:32 | 10.0.0.126 | RDP | 3389 |
| 110 | 2023-06-22 14:47:32 | 10.0.0.197 | RDP | 3389 |
| 111 | 2023-06-22 14:47:32 | 10.0.0.123 | SSH | 22 |
| 112 | 2023-06-22 14:47:32 | 10.0.0.82 | RDP | 3389 |
| 113 | 2023-06-22 14:47:32 | 10.0.0.74 | RDP | 3389 |
| 114 | 2023-06-22 14:47:32 | 10.0.0.175 | SSH | 22 |
| 115 | 2023-06-22 14:47:32 | 10.0.0.100 | SSH | 22 |
| 116 | 2023-06-22 14:47:32 | 10.0.0.101 | SSH | 22 |
| 117 | 2023-06-22 14:47:32 | 10.0.0.102 | SSH | 22 |
| 118 | 2023-06-22 14:47:32 | 10.0.0.103 | SSH | 22 |
| 119 | 2023-06-22 14:47:32 | 10.0.0.6 | SSH | 22 |
| 120 | 2023-06-22 14:47:33 | 10.0.0.176 | SSH | 22 |
| 121 | 2023-06-22 14:47:58 | 10.0.0.126 | RDP | 3389 |
| 122 | 2023-06-22 14:47:58 | 10.0.0.197 | RDP | 3389 |
| 123 | 2023-06-22 14:47:58 | 10.0.0.123 | SSH | 22 |
| 124 | 2023-06-22 14:47:58 | 10.0.0.82 | RDP | 3389 |
| 125 | 2023-06-22 14:47:58 | 10.0.0.74 | RDP | 3389 |
| 126 | 2023-06-22 14:47:58 | 10.0.0.175 | SSH | 22 |
| 127 | 2023-06-22 14:47:58 | 10.0.0.100 | SSH | 22 |
| 128 | 2023-06-22 14:47:58 | 10.0.0.101 | SSH | 22 |
| 129 | 2023-06-22 14:47:58 | 10.0.0.102 | SSH | 22 |
| 130 | 2023-06-22 14:47:58 | 10.0.0.103 | SSH | 22 |
| 131 | 2023-06-22 14:47:58 | 10.0.0.6 | SSH | 22 |
| 132 | 2023-06-22 14:47:59 | 10.0.0.176 | SSH | 22 |

CYBER SMURFS

```
ubuntu@ip-10-0-0-102:~$ ls
1.py  2.py  community-rules.tar.gz  connections.csv  snortparser.py  test.py  traffic_data.csv
ubuntu@ip-10-0-0-102:~$
```

# Email Alerts




CYBER SMURFS

# Network Activity

```python
#!/usr/bin/python3
# Nick Alderete & Jeremy Patton
# Automated network scan & Email notification



import csv
import socket
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart
import time


# IP addresses to monitor
ip_addresses = ['10.0.0.126', '10.0.0.197', '10.0.0.123', '10.0.0.82', '10.0.0.74
                '10.0.0.101', '10.0.0.102', '10.0.0.103', '10.0.0.6', '10.0.0.176
# Addresses:
# .126 = Accounting 1 | .197 = Accounting 2 | .123 = Bobs Analytics server |
# .82 = Metasploitable | .74 = Risk Analyst 1 | .175 = Web server | .100/101 = Hu
# 102/103 = Hunter 2 | .6 = Splunk/ SIEM | .176 = OpenVPN server


# Port numbers to check
port_numbers = [20, 21, 22, 23, 25, 53, 68, 80, 88, 110, 143, 161, 443, 3389]
```

| | | | |
|---|---|---|---|
| 2023-06-23 10:07:20 | 10.0.0.74 | 3389 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.175 | 22 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.175 | 80 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.100 | 22 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.101 | 22 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.102 | 22 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.102 | 25 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.103 | 22 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.103 | 25 | External Traffic |
| 2023-06-23 10:07:20 | 10.0.0.6 | 22 | External Traffic |
| 2023-06-23 10:07:30 | 10.0.0.176 | 22 | External Traffic |
| 2023-06-23 10:08:15 | 10.0.0.176 | 443 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.126 | 3389 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.197 | 3389 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.123 | 22 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.82 | 21 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.82 | 80 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.82 | 3389 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.74 | 3389 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.175 | 22 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.175 | 80 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.100 | 22 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.101 | 22 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.102 | 22 | External Traffic |
| 2023-06-23 10:13:21 | 10.0.0.102 | 25 | External Traffic |

CYBER SMURFS

```
ubuntu@ip-10-0-0-102:~$ ls
1.py  2.py  community-rules.tar.gz  connections.csv  snortparser.py  test.py  traffic_data.csv
ubuntu@ip-10-0-0-102:~$
```

# Resources & Thanks

- Open communication
- Navigating Splunk
- Connie is the MVP

# Final Thoughts

- Code Fellows instructors
- ChatGPT
- Google

CYBER SMURFS

# Q & A

CYBER SMURFS