HERMES

Ops 401 Final Project

Agenda

1. Team Member Introductions
2. Problem Domain & Project Overview
3. Team Process & Documentation
4. Application Demonstration
5. Q&A

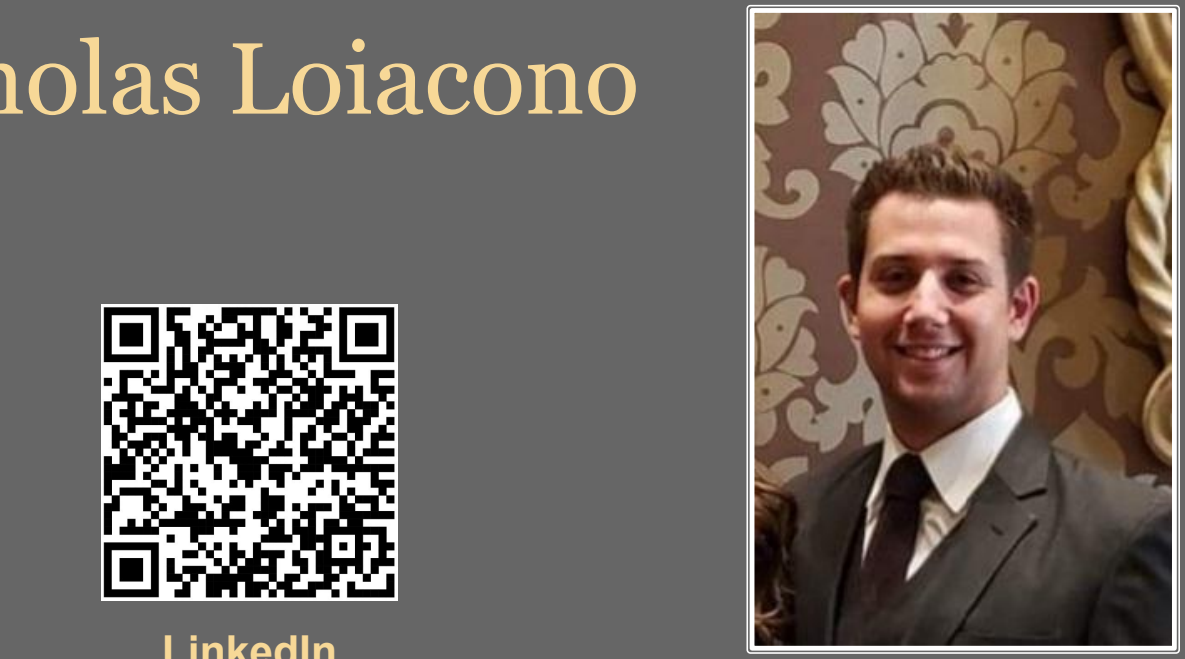
Hermes Messengers

1. Spencer Mitchell
2. Nicholas Loiacono
3. Lamin Mola Touray
4. Dericus Horner
5. Joshua Phipps

Spencer Mitchell

- USMC Veteran
- OEF Veteran
- Generator Mechanic
- Worked maintenance in previous careers
- Skillset match, Opportunities for growth

Nicholas Loiacono



CompTIA ITF+ CERTIFIED

LinkedIn

- Veteran with 10 years of military experience
- Career transition to Cybersecurity from Engineering
- Looking to challenge myself and spend more time with family

Lamin Mola Touray

- Navy Veteran
- CompTIA IFT+ Certified
- Former First Responder
- Aspiring Cyber Security Professional

Dericus Horner

- US Army Veteran
- Master’s degree in Business Administration
- Current IT Property Specialist
- Detail Oriented/Critical Thinker

Connect With Me LinkedIn

Joshua Phipps

- Georgia National Guard (92R Parachute Rigger)
- Cybersecurity student
- Xavier School for Gifted Youngsters

CompTIA Security+ CERTIFIED

CompTIA Network+

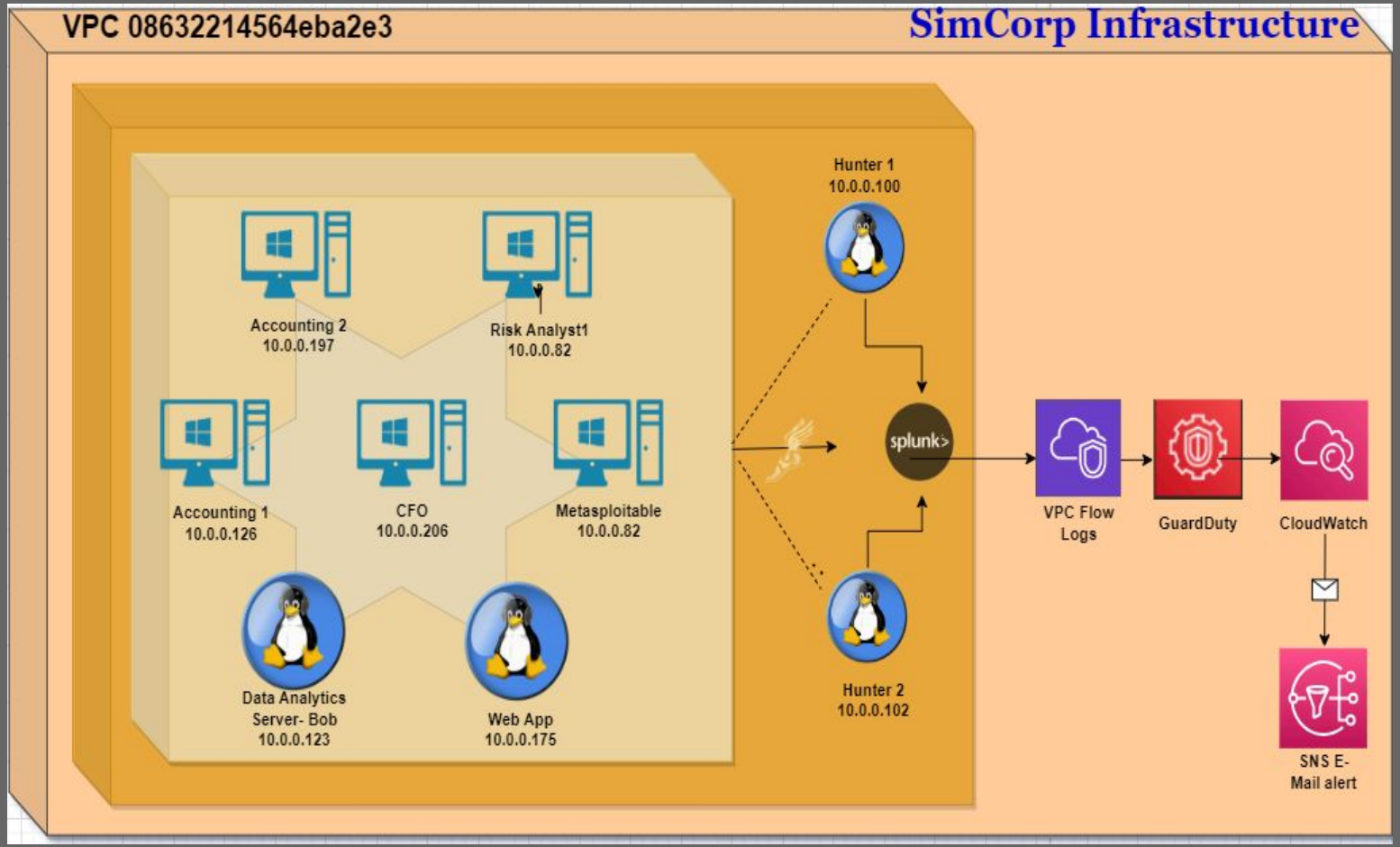
Threat Landscape

SimCorp has contracted Hermes (MSSP) to perform a one time adversary emulation engagement.

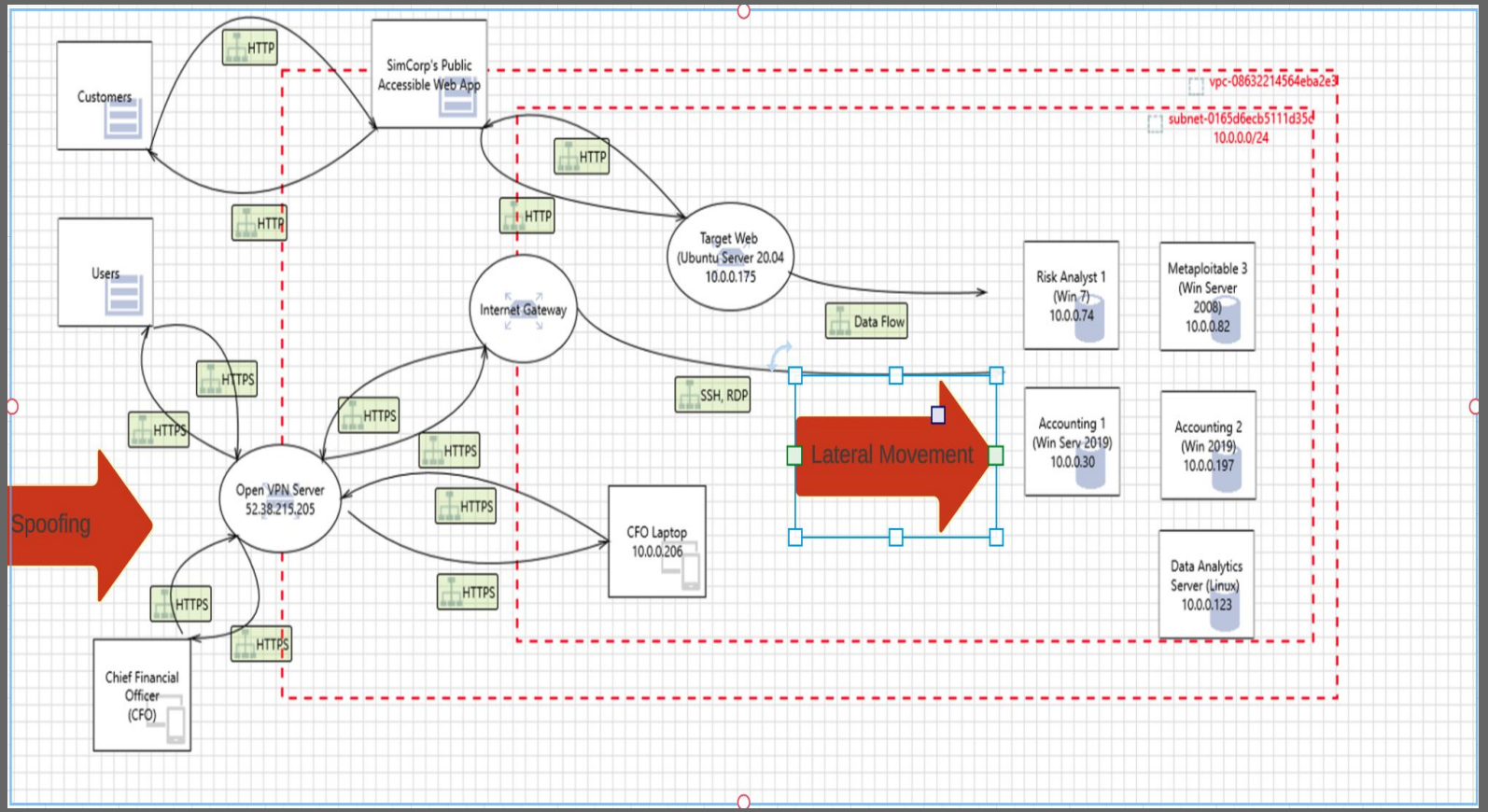
Solutions

- Hermes constructed an initial threat model DFD and performed a STRIDE analysis.
- Introduced extra threat detection tools
- Configured GuardDuty and Splunk
- Implemented detective controls for the web server hosting SimCorp's web application.
- Observed adversarial actions and collected evidence of scanning or TTPs used by the threat actors.
- Implemented automatec script that alerted the team to any adversarial activity.

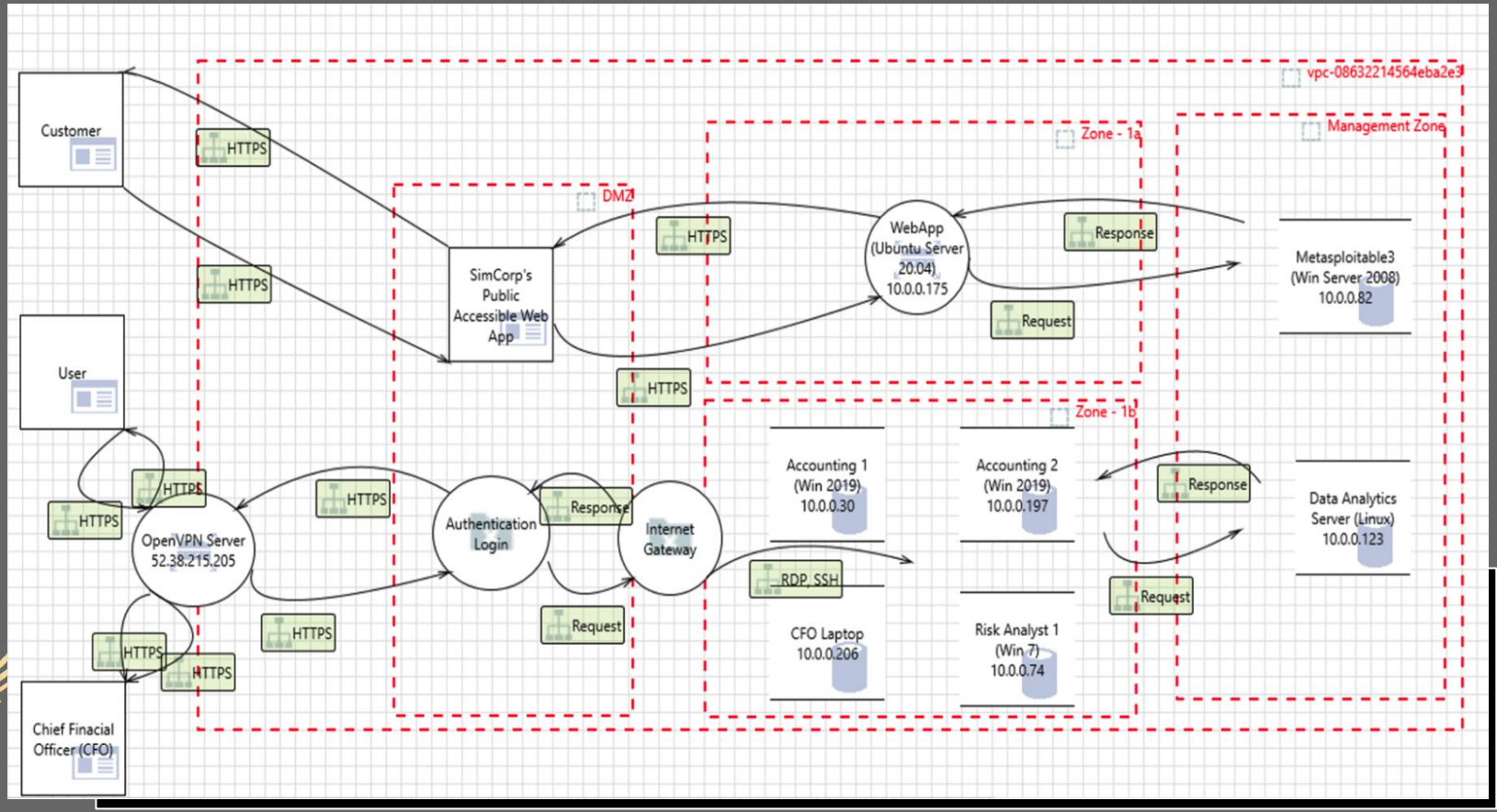
VPC Topology



Current Threat Model - Data Flow Diagram



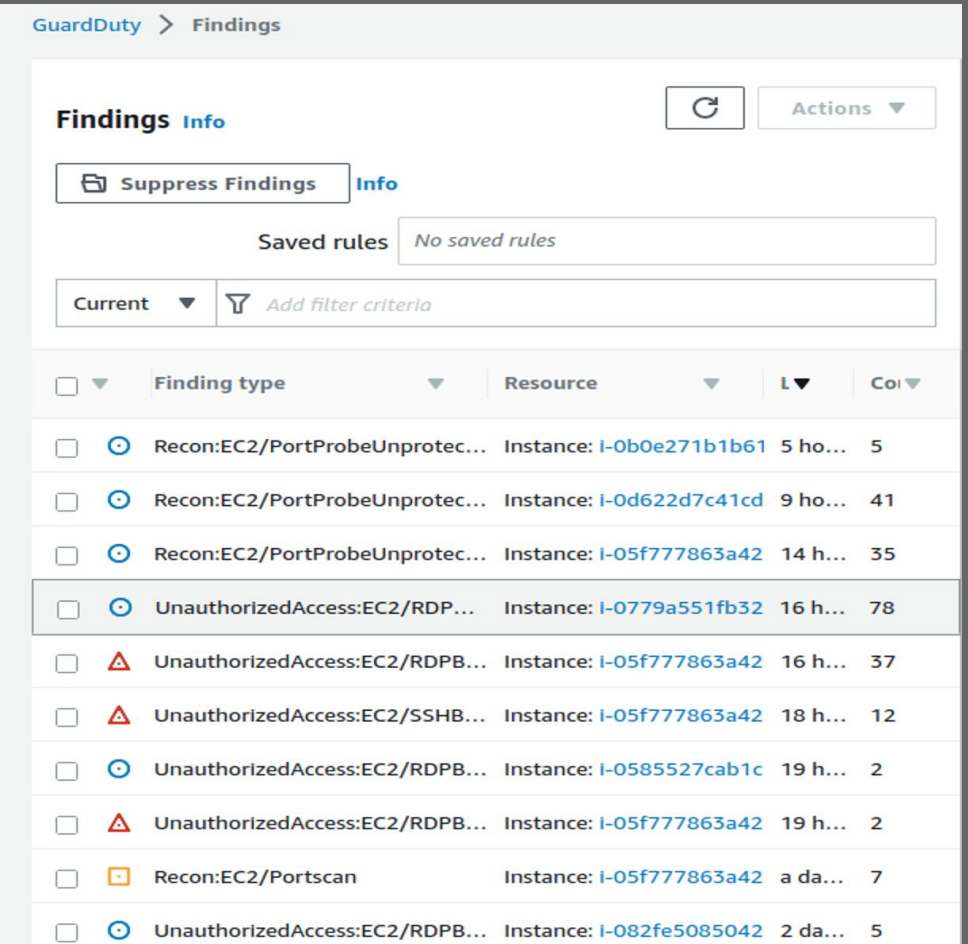
Recommended Threat Model - Data Flow Diagram



GuardDuty

- Managed threat detection service
- Analyzes various data sources, such as VPC Flow Logs, AWS CloudTrail, and DNS logs
- Regularly review findings
- Automated responses to streamline your security operations

GuardDuty pt.2



GuardDuty_to_Email <no-reply@sns.amazonaws.com>
to me

"AWS 705235841658 has a severity 2 GuardDuty finding type Recon:EC2/PortProbeUnprotectedPort in the us-west-2 region."
"Finding Description:"
"EC2 instance has an unprotected port which is being probed by a known malicious host.. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/guardduty/home?region=us-west-2#/findings

GuardDuty_to_Email <no-reply@sns.amazonaws.com>
to me

"AWS 705235841658 has a severity 2 GuardDuty finding type Recon:EC2/PortProbeUnprotectedPort in the us-west-2 region."
"Finding Description:"
"EC2 instance has an unprotected port which is being probed by a known malicious host.. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/guardduty/home?region=us-west-2#/findings

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:705235841658:GuardDuty_to

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https

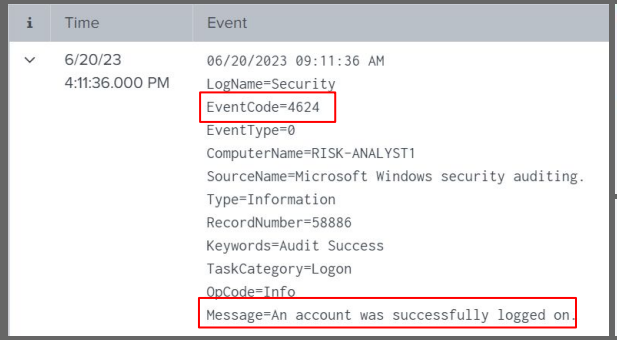
Splunk Logging

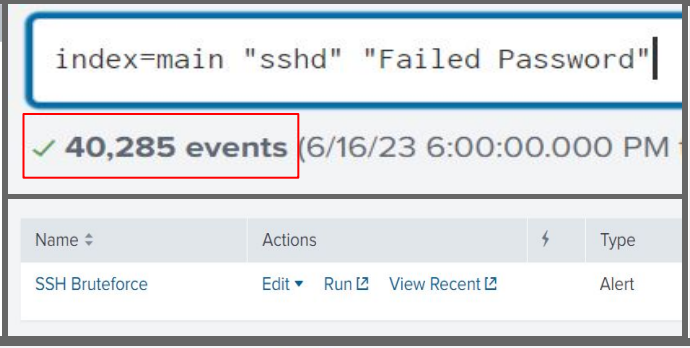
- SIEM Tool used for many purposes.
- Set up Splunk Forwarders on the most vulnerable instances.
- Set our Hunter Instance to forward all network traffic logs to be ingested by Splunk.

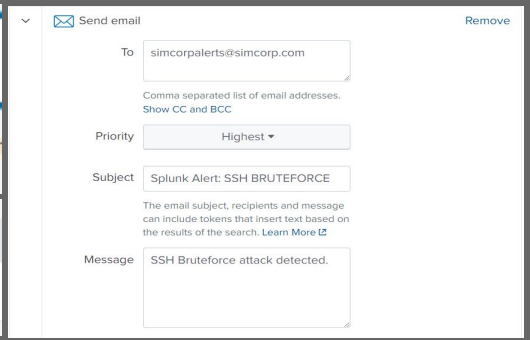
Host		Count	Last Update
ACCOUNTING1		123,528	6/23/23 6:30:10.000 PM
ACCOUNTING2		146,992	6/23/23 6:28:52.000 PM
RISK-ANALYST1		415,799	6/23/23 6:29:42.000 PM
ip-10-0-0-100		6,991,664	6/23/23 6:30:35.000 PM
ip-10-0-0-175		22,068	6/23/23 6:17:15.000 PM
linsecurity		5,073,346	6/23/23 6:30:33.000 PM

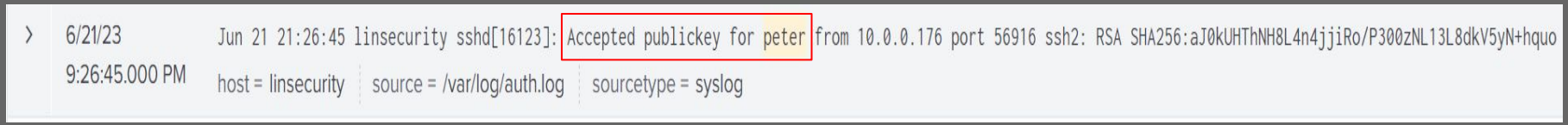
i	Time	Event
>	6/19/23 10:13:55.000 PM	06/19/2023 03:13:55 PM LogName=Security EventCode=4625 EventType=0 ComputerName=accounting2 Show all 61 lines host = ACCOUNTING2 source = WinEventLog:Security sourcetype = WinEventLog:Security
>	6/19/23 10:03:33.000 PM	06/19/2023 03:03:33 PM LogName=Security EventCode=4625 EventType=0 ComputerName=accounting1 Show all 61 lines host = ACCOUNTING1 source = WinEventLog:Security sourcetype = WinEventLog:Security

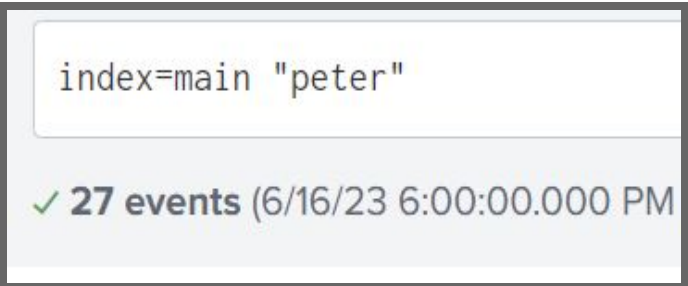
Splunk Logging pt. 2



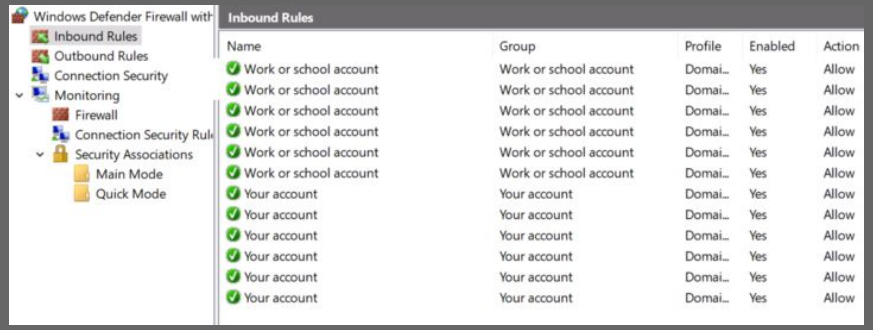




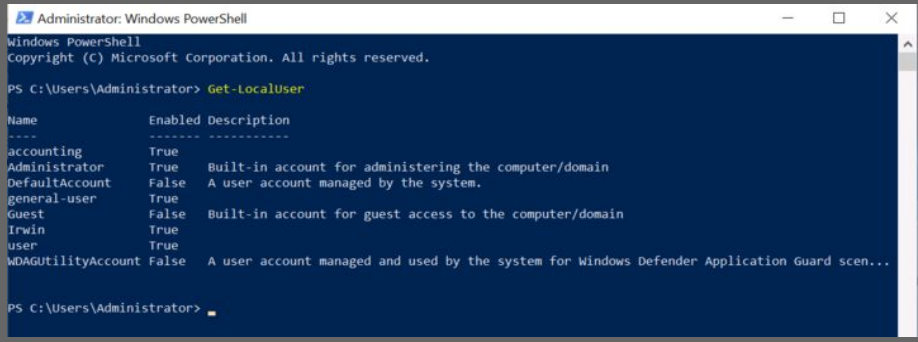




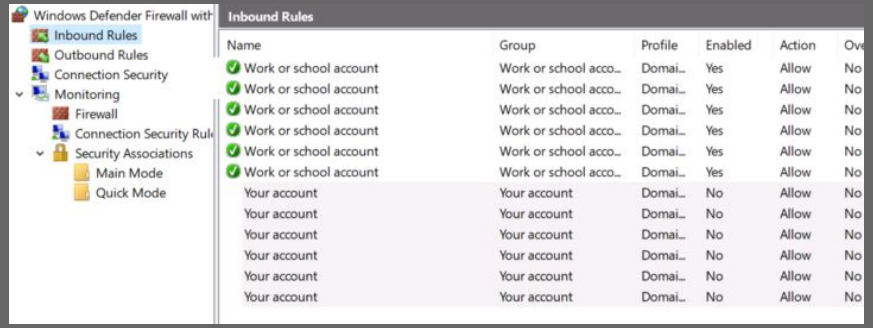
Before & After



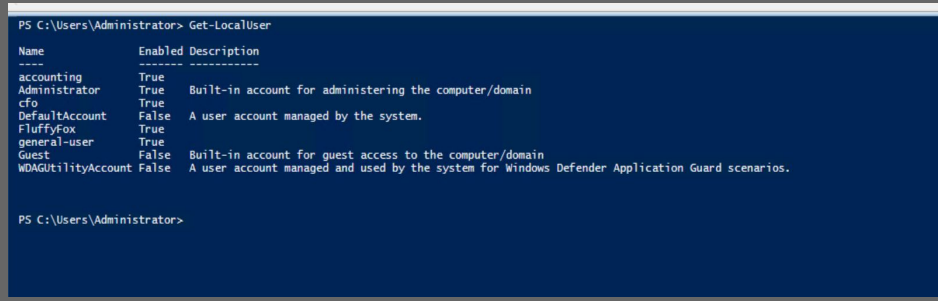
^ Before Red Team Intrusion ^



^ Before Red Team Intrusion ^



^ After Red Team Intrusion ^



^ After Red Team Intrusion ^

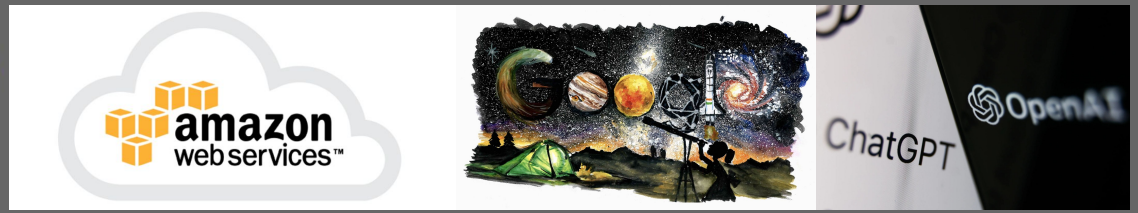
On the left, we can see an example of what the Red Team can do after accessing our systems (disabling our accounts).

On the right, we can see how cleverly they added a user named “FluffyFox.”

Resources and Thanks

- Link to our documentation and resources for Hermes-Messengers:
  - Please scan our QR code to reach our GitHub Organization!
- Gratitude to those who helped us get it done:
  - A big thank you to Marco Vazquez and Alex White for all of the technical assistance provided to our Hermes team.
  - Team Cyber Smurfs for helping Spencer not lose his mind with Splunk
- Links to other attributions and/or resources worth noting:

Hermes-Messengers



GitHub

Questions?

“The only stupid question is the question that is never asked.”

What is a hackers favorite season?