

HERMIES



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



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



Joshua Phipps

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



Threat Landscape

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



Solutions

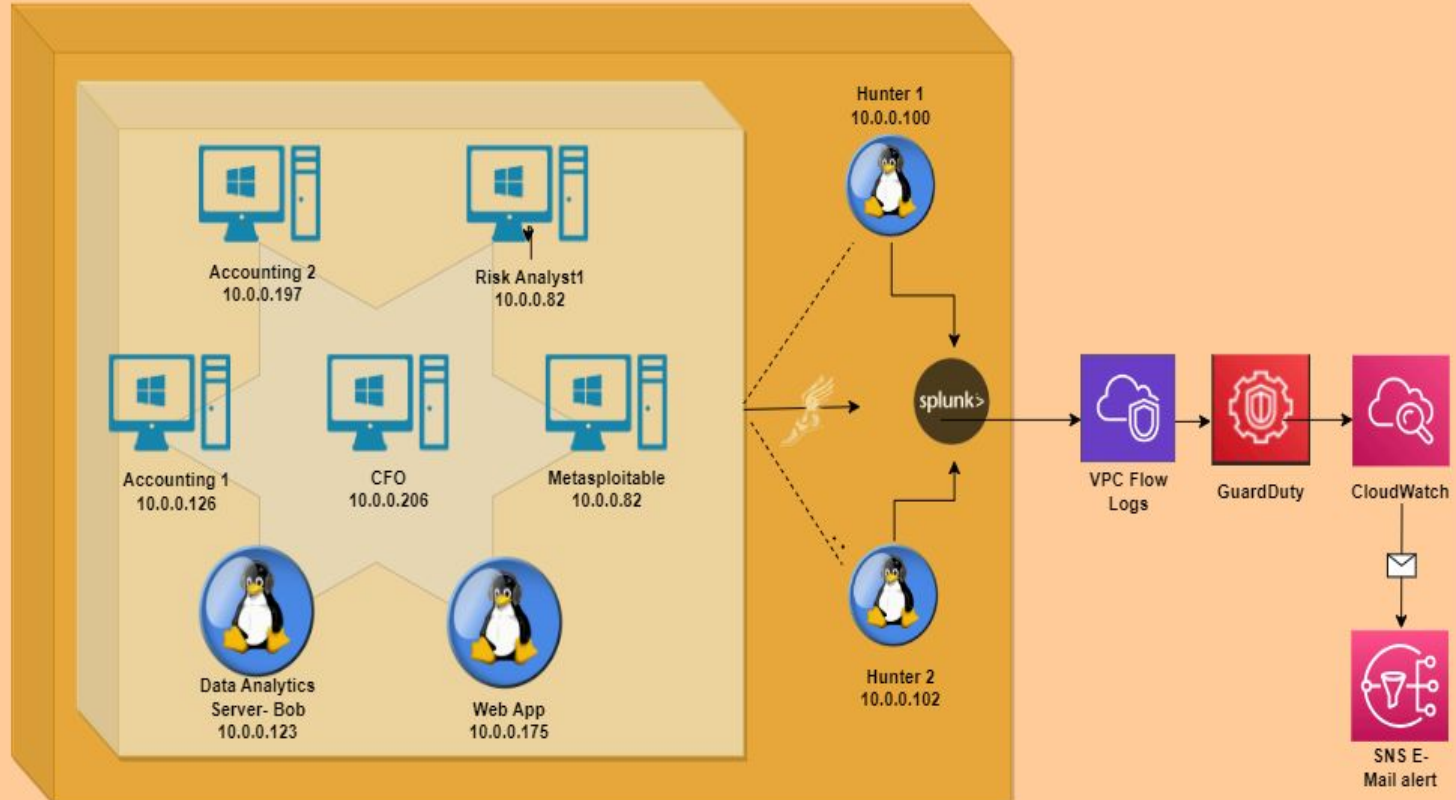
- Hermes constructed an initial threat model DFD and performed a STRIDE analysis.
- Introduced extra threat detection tools
- Configured GuardDuty and Splunk
- Implemented detective controls for the web server hosting SimCorp's web application.
- Observed adversarial actions and collected evidence of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



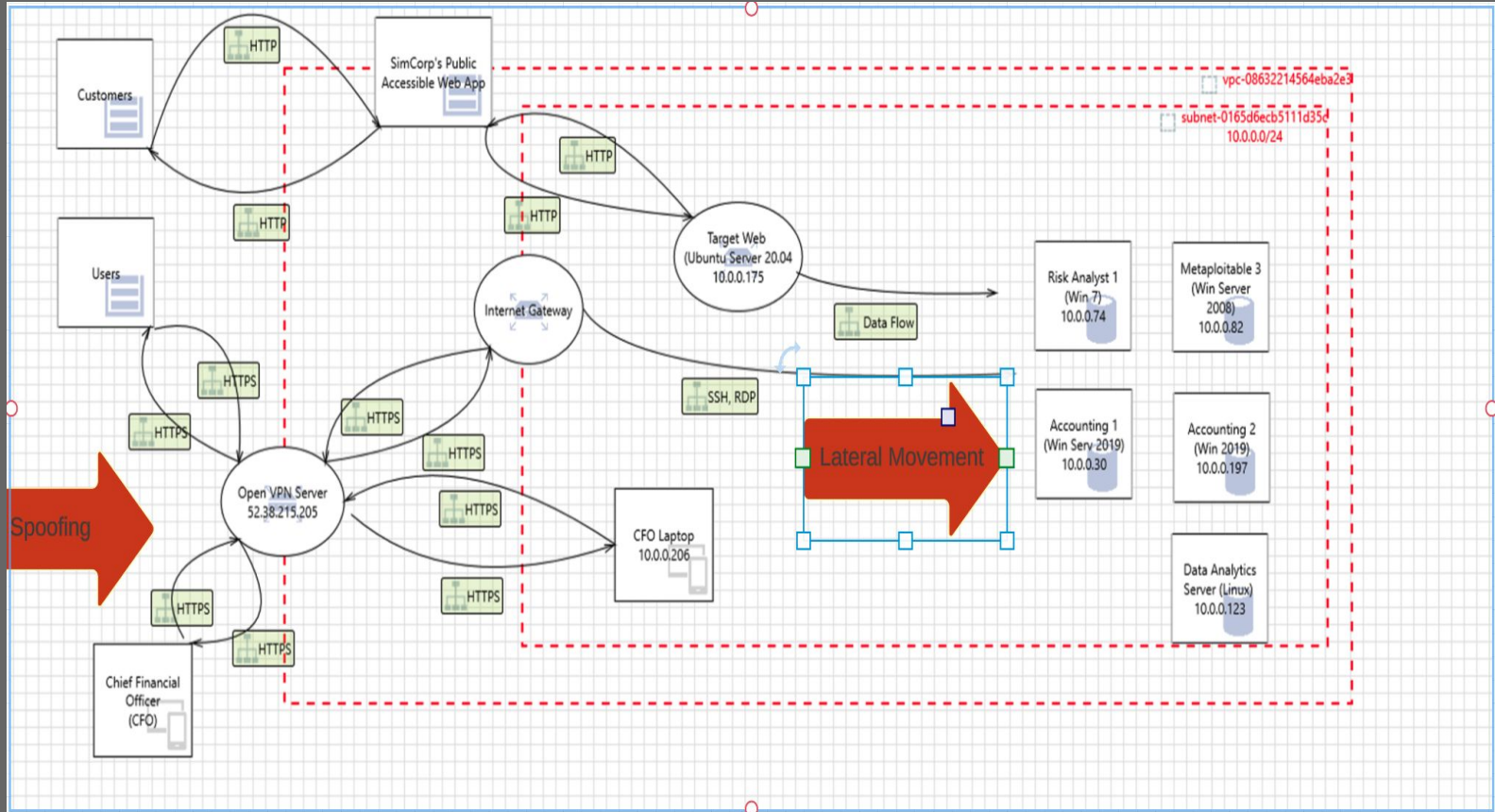
VPC Topology

VPC 08632214564eba2e3

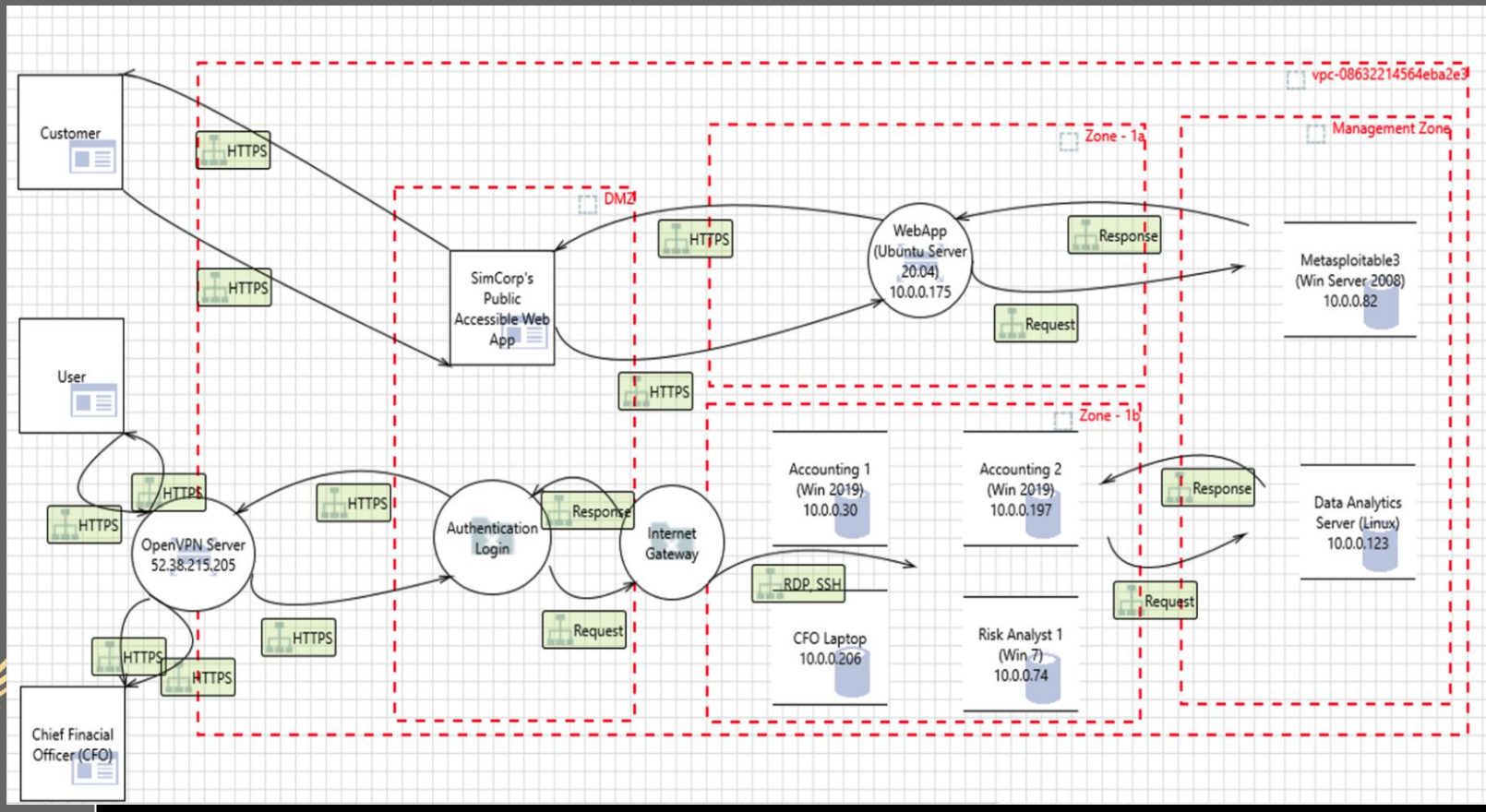
SimCorp Infrastructure



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



UnauthorizedAccess:EC2/R...

Finding ID: [4ac470966514702471d2af9c13883d52](#)
[Feedback](#)

High

I-05f777863a42e2fd8 is performing RDP brute force attacks against 10.0.0.206. Brute force attacks are used to gain unauthorized access to your Instance by guessing the RDP password. [Info](#)

Investigate with Detective

Overview

Severity	HIGH	<div></div>
Region	us-west-2	
Count	37	
Account ID	705235841658	<div></div>
Resource ID	I-05f777863a42e2fd8	<div></div>
Created at	06-21-2023 20:36:28 (2 ...)	
Updated at	06-22-2023 20:44:23 (1...)	

Resource affected

Resource role	ACTOR	<div></div>
Resource type	Instance	<div></div>
Port	33320	
Port name	Unknown	

GuardDuty pt.2

GuardDuty > Findings

Findings Info



Actions ▼

Suppress Findings

Info

Saved rules *No saved rules*

Current ▼



Add filter criteria

<input type="checkbox"/> ▼	Finding type ▼	Resource ▼	L ▼	Col ▼
<input type="checkbox"/>	Recon:EC2/PortProbeUnprotec...	Instance: i-0b0e271b1b61	5 ho...	5
<input type="checkbox"/>	Recon:EC2/PortProbeUnprotec...	Instance: i-0d622d7c41cd	9 ho...	41
<input type="checkbox"/>	Recon:EC2/PortProbeUnprotec...	Instance: i-05f777863a42	14 h...	35
<input type="checkbox"/>	UnauthorizedAccess:EC2/RDPB...	Instance: i-0779a551fb32	16 h...	78
<input type="checkbox"/>	UnauthorizedAccess:EC2/RDPB...	Instance: i-05f777863a42	16 h...	37
<input type="checkbox"/>	UnauthorizedAccess:EC2/SSHB...	Instance: i-05f777863a42	18 h...	12
<input type="checkbox"/>	UnauthorizedAccess:EC2/RDPB...	Instance: i-0585527cab1c	19 h...	2
<input type="checkbox"/>	UnauthorizedAccess:EC2/RDPB...	Instance: i-05f777863a42	19 h...	2
<input type="checkbox"/>	Recon:EC2/Portscan	Instance: i-05f777863a42	a da...	7
<input type="checkbox"/>	UnauthorizedAccess:EC2/RDPB...	Instance: i-082fe5085042	2 da...	5

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://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:705235841658:GuardDuty_to

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

i	Time	Event
✓	6/20/23 4:11:36.000 PM	06/20/2023 09:11:36 AM LogName=Security EventCode=4624 EventType=0 ComputerName=RISK-ANALYST1 SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=58886 Keywords=Audit Success TaskCategory=Ligon OpCode=Info Message=An account was successfully logged on.

index=main "sshd" "Failed Password"

✓ 40,285 events (6/16/23 6:00:00.000 PM)

Name	Actions	Type
SSH Bruteforce	Edit Run View Recent	Alert

Send email Remove

To simcorpalerts@simcorp.com

Comma separated list of email addresses.
Show CC and BCC

Priority Highest

Subject Splunk Alert: SSH BRUTEFORCE

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message SSH Bruteforce attack detected.

>	6/21/23 9:26:45.000 PM	Jun 21 21:26:45 linsecurity sshd[16123]: Accepted publickey for peter from 10.0.0.176 port 56916 ssh2: RSA SHA256:aJ0KUHTNh8L4n4jjiRo/P300zNL13L8dkV5yN+hquo
		host = linsecurity source = /var/log/auth.log sourcetype = syslog

index=main "peter"

✓ 27 events (6/16/23 6:00:00.000 PM)



Before & After

Windows Defender Firewall with Inbound Rules

Name	Group	Profile	Enabled	Action
Work or school account	Work or school account	Domain	Yes	Allow
Work or school account	Work or school account	Domain	Yes	Allow
Work or school account	Work or school account	Domain	Yes	Allow
Work or school account	Work or school account	Domain	Yes	Allow
Work or school account	Work or school account	Domain	Yes	Allow
Work or school account	Work or school account	Domain	Yes	Allow
Your account	Your account	Domain	Yes	Allow
Your account	Your account	Domain	Yes	Allow
Your account	Your account	Domain	Yes	Allow
Your account	Your account	Domain	Yes	Allow
Your account	Your account	Domain	Yes	Allow
Your account	Your account	Domain	Yes	Allow

^ Before Red Team Intrusion ^

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

PS C:\Users\Administrator> Get-LocalUser

Name                Enabled Description
----                -
accounting           True
Administrator        True Built-in account for administering the computer/domain
DefaultAccount       False A user account managed by the system.
general-user          True
Guest                False Built-in account for guest access to the computer/domain
Irwin                True
user                 True
WDAGUtilityAccount   False A user account managed and used by the system for Windows Defender Application Guard scen...
```

^ Before Red Team Intrusion ^

Windows Defender Firewall with Inbound Rules

Name	Group	Profile	Enabled	Action	Over
Work or school account	Work or school acco...	Domain	Yes	Allow	No
Work or school account	Work or school acco...	Domain	Yes	Allow	No
Work or school account	Work or school acco...	Domain	Yes	Allow	No
Work or school account	Work or school acco...	Domain	Yes	Allow	No
Work or school account	Work or school acco...	Domain	Yes	Allow	No
Your account	Your account	Domain	No	Allow	No
Your account	Your account	Domain	No	Allow	No
Your account	Your account	Domain	No	Allow	No
Your account	Your account	Domain	No	Allow	No
Your account	Your account	Domain	No	Allow	No
Your account	Your account	Domain	No	Allow	No

^ After Red Team Intrusion ^

```
PS C:\Users\Administrator> Get-LocalUser

Name                Enabled Description
----                -
accounting           True
Administrator        True Built-in account for administering the computer/domain
cfo                  True
DefaultAccount       False A user account managed by the system.
FluffyFox            True
general-user          True
Guest                False Built-in account for guest access to the computer/domain
WDAGUtilityAccount   False A user account managed and used by the system for Windows Defender Application Guard scenarios.
```

^ 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



Questions?

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

What is a hackers favorite season?

