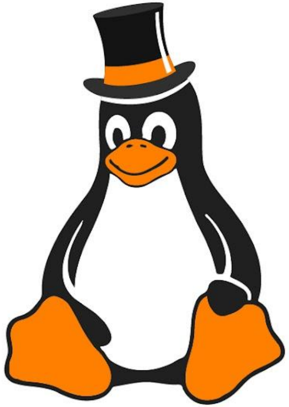
CWL
CyberWarFare Labs

TUX'S MAGIC HAT: ANALYSING AWS FLOW LOGS FOR FUN!

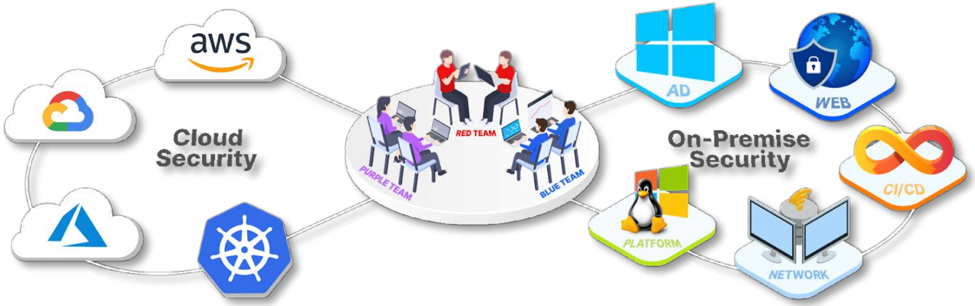


ABOUT CYBERWARFARE LABS :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions :

1. **Cyber Range Labs**

2. **Up-Skilling Platform**



INFINITE LEARNING EXPERIENCE

ABOUT SPEAKER :

Abhijeet Kumar
(Security Researcher)

His areas of interests includes Red Team Operations, Network Security, Cloud Infrastructure, and Linux Systems. Apart from this, he enjoys researching Adversarial TTPs and experimenting in his homelab during his free time.

AWS 101

- ★ AWS stands for Amazon Web Services

AWS 101

- ★ AWS stands for Amazon Web Services
- ★ Product catalog includes 200+ services across different domains

AWS 101

- ★ AWS stands for Amazon Web Services
- ★ Product catalog includes 200+ services across different domains
- ★ Provides Logging options for different services

VPC 101

★ VPC stands for Virtual Private Cloud

VPC 101

- ★ VPC stands for Virtual Private Cloud
- ★ Isolated virtual networking service

VPC 101

- VPC stands for Virtual Private Cloud
- Isolated virtual networking service
- Components include:
  - Subnets & Routing

VPC 101

- VPC stands for Virtual Private Cloud
- Isolated virtual networking service
- Components include:
  - Subnets & Routing
  - IP Addressing

CWL
CyberWarFare Labs

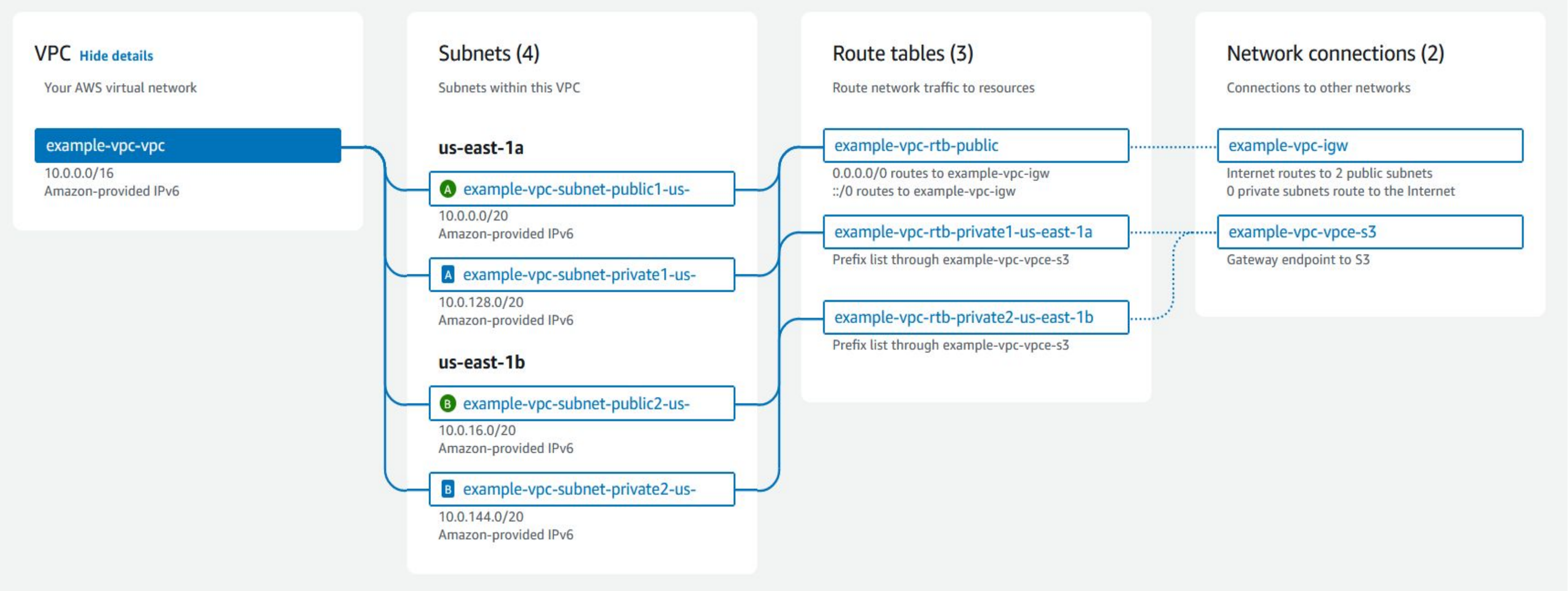
VPC 101

- ★ VPC stands for Virtual Private Cloud
- ★ Isolated virtual networking service
- ★ Components include:
    - ○ Subnets & Routing
    - ○ IP Addressing
    - ○ Gateways & Endpoints

CWL
CyberWarFare Labs

VPC 101

- ★ VPC stands for Virtual Private Cloud
- ★ Isolated virtual networking service
- ★ Components include:
    - ○ Subnets & Routing
    - ○ IP Addressing
    - ○ Gateways & Endpoints
    - ○ VPC Flow Logs



VPC Hide details

Your AWS virtual network

example-vpc-vpc
10.0.0.0/16
Amazon-provided IPv6

Subnets (4)

Subnets within this VPC

us-east-1a

A example-vpc-subnet-public1-us-
10.0.0.0/20
Amazon-provided IPv6

A example-vpc-subnet-private1-us-
10.0.128.0/20
Amazon-provided IPv6

us-east-1b

B example-vpc-subnet-public2-us-
10.0.16.0/20
Amazon-provided IPv6

B example-vpc-subnet-private2-us-
10.0.144.0/20
Amazon-provided IPv6

Route tables (3)

Route network traffic to resources

example-vpc-rtb-public
0.0.0.0/0 routes to example-vpc-igw
::/0 routes to example-vpc-igw

example-vpc-rtb-private1-us-east-1a
Prefix list through example-vpc-vpce-s3

example-vpc-rtb-private2-us-east-1b
Prefix list through example-vpc-vpce-s3

Network connections (2)

Connections to other networks

example-vpc-igw
Internet routes to 2 public subnets
0 private subnets route to the Internet

example-vpc-vpce-s3
Gateway endpoint to S3

Figure: *VPC Example*

AWS VPC Flow Logs

- ★ High-level IP traffic (Ingress + egress) metadata information for VPC resources (say EC2 instances)

CWL
CyberWarFare Labs

AWS VPC Flow Logs

★ High-level IP traffic (Ingress + egress) metadata information for VPC resources (say EC2 instances)

★ Data collection is Agentless

AWS VPC Flow Logs

- ★ High-level IP traffic (Ingress + egress) metadata information for VPC resources (say EC2 instances)
- ★ Data collection is Agentless
- ★ Common use cases:
  - ○ Diagnostics & Troubleshooting

AWS VPC Flow Logs

- ★ High-level IP traffic (Ingress + egress) metadata information for VPC resources (say EC2 instances)
- ★ Data collection is Agentless
- ★ Common use cases:
  - ○ Diagnostics & Troubleshooting
  - ○ Intrusion & Anomaly Detection

Flow Logs Pros & Cons

★ **Pros:**

- ○ No impact on network latency

★ **Cons:**

- ○ Immutable once configured

Flow Logs Pros & Cons

- **Pros:**
  - No impact on network latency
  - Easy integration with other services

- **Cons:**
  - Immutable once configured
  - All IP traffic types are not captured

CWL
CyberWarFare Labs

Flow Logs Pros & Cons

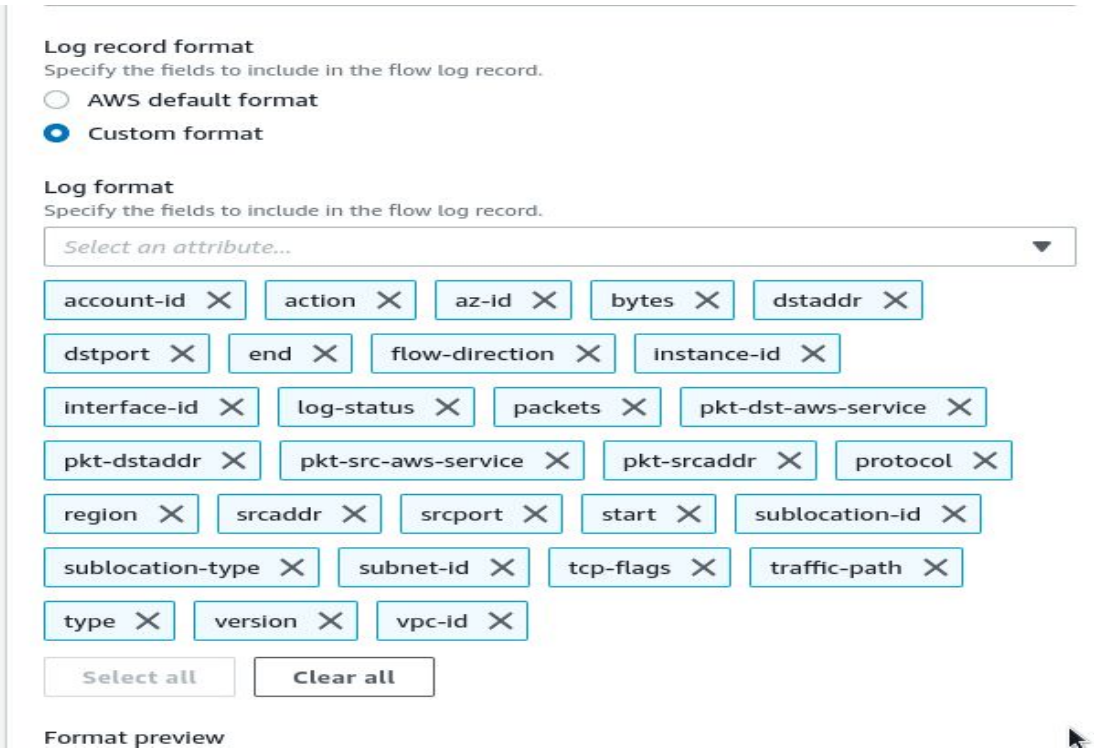
★ **Pros:**

- ○ No impact on network latency
- ○ Easy integration with other services
- ○ Enriched metadata

★ **Cons:**

- ○ Immutable once configured
- ○ All IP traffic types are not captured
- ○ Not real-time logging

CWL
CyberWarFare Labs



Log record format

Specify the fields to include in the flow log record.

○ AWS default format

● Custom format

Log format

Specify the fields to include in the flow log record.

Select an attribute...

account-id ✕ action ✕ az-id ✕ bytes ✕ dstaddr ✕
dstport ✕ end ✕ flow-direction ✕ instance-id ✕
interface-id ✕ log-status ✕ packets ✕ pkt-dst-aws-service ✕
pkt-dstaddr ✕ pkt-src-aws-service ✕ pkt-srcaddr ✕ protocol ✕
region ✕ srcaddr ✕ srcport ✕ start ✕ sublocation-id ✕
sublocation-type ✕ subnet-id ✕ tcp-flags ✕ traffic-path ✕
type ✕ version ✕ vpc-id ✕

Format preview

Figure: *VPC Flow Log Record Format*

Capturing Flow Logs

- ★ Logs can be captured at:
  - ○ Network interface level

Capturing Flow Logs

- ★ Logs can be captured at:
  - ○ Network interface level
  - ○ VPC subnet level

Capturing Flow Logs

- ★ Logs can be captured at:
  - ○ Network interface level
  - ○ VPC subnet level
  - ○ Entire VPC level

Publishing Flow Logs

- Logs can be published to:
  - CloudWatch

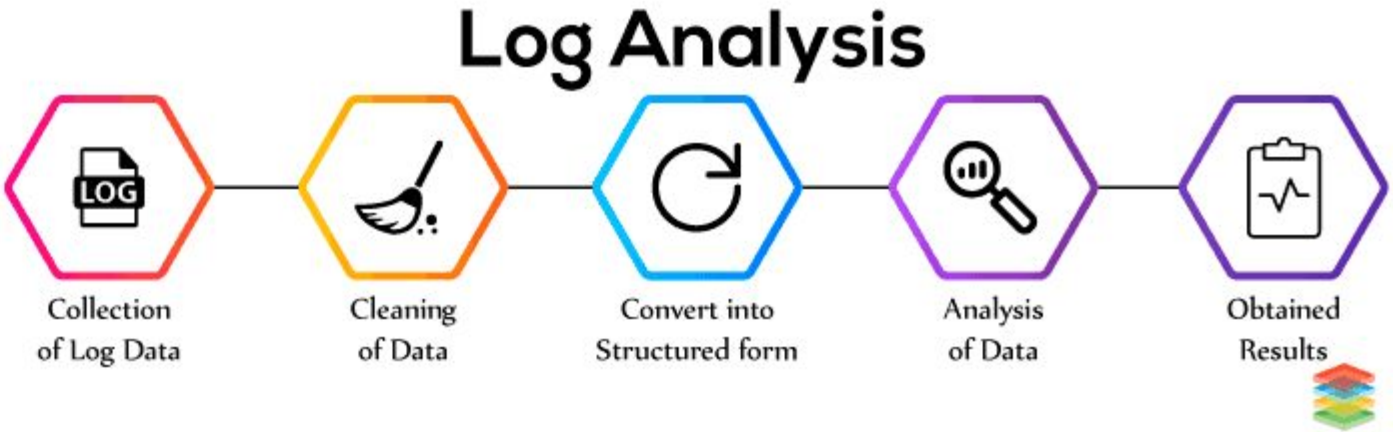
Publishing Flow Logs

- ★ Logs can be published to:
  - ○ CloudWatch
  - ○ Data Firehose (formerly known as Kinesis Data Firehose)

Publishing Flow Logs

- ★ Logs can be published to:
  - ○ CloudWatch
  - ○ Data Firehose (formerly known as Kinesis Data Firehose)
  - ○ S3

Analysing VPC Flow Logs



Source: *Xenonstack*

How this talk came into being?

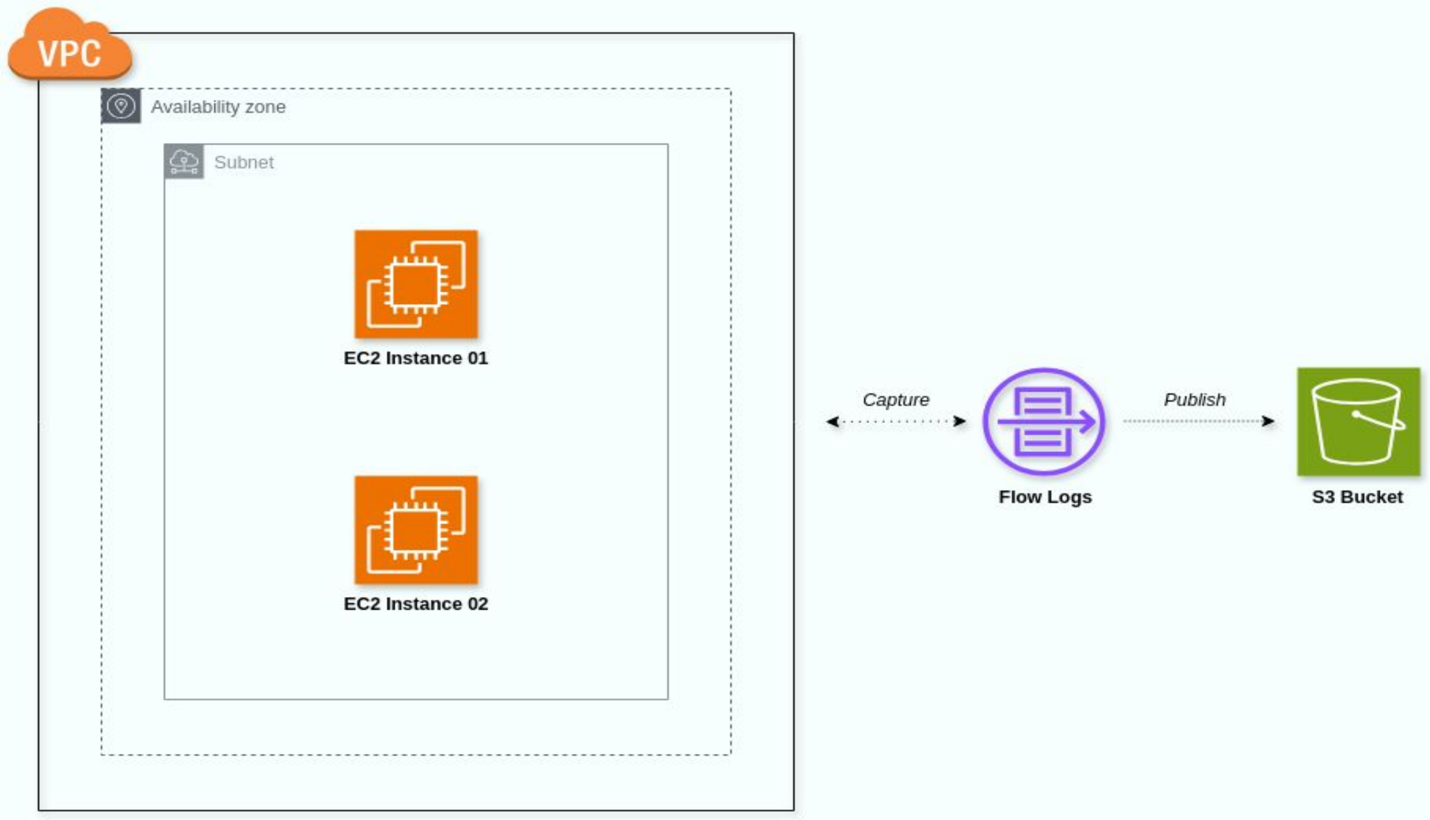


Figure: *Architecture Used During The 8th July Linux Persistence Demo*

What I Did

★ Moved all log files into a single directory

What I Did

- ★ Moved all log files into a single directory
- ★ Filtered Ingress traffic:

```
cat *.log | grep ingress | cut -d " " -f 16 | sort -g | uniq > ingress-uniq.txt
```

The Result

- So, in the span of ~10 hours with :
  - Total requests = **17K+**

The Result

- ★ So, in the span of ~10 hours:
  - ○ Total requests from IPs = ***17K+***
  - ○ Ingress:
    - ■ *Total requests from IPs =* ***13K+***
    - ■ *Unique IPs =* ***3K+***

Let's write a quick script

Let's go. In and out. 20 minute adventure.
AFTER ~65 MINS LATER
SCRIPT V1
GENERATED COMPLETE OUTPUT
[adult swim]

DEMO
Shift

- ★ **Tool:** ***https://github.com/wand3rlust/Fairth***

CWL
CyberWarFare Labs

THANK YOU

**For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings**, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live