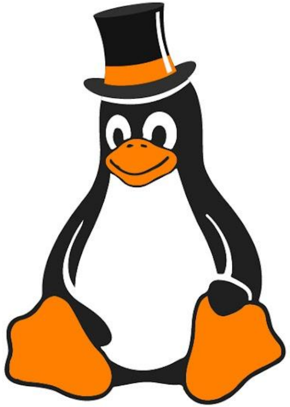
CWL CyberWarFare Labs | The Hackers Meetup Let's Talk About Hacking

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

ABHIJEET KUMAR



Whoami

- Security Researcher @ CyberWarFare Labs
- Research areas include:
  - Adversarial TTPs
  - Linux Internals
  - Network Security
  - Cloud Infrastructure

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

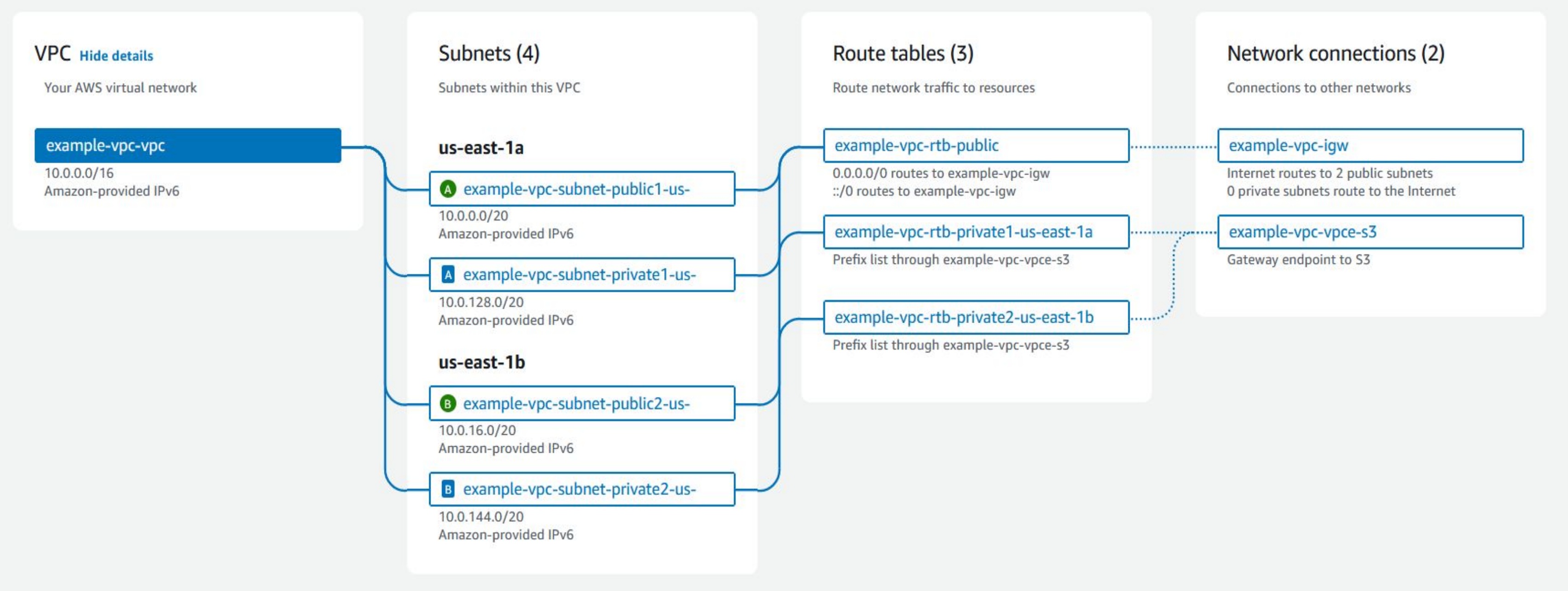
- VPC stands for Virtual Private Cloud
- Isolated virtual networking service
- Components include:
  - Subnets & Routing
  - IP Addressing

VPC 101

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

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)

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

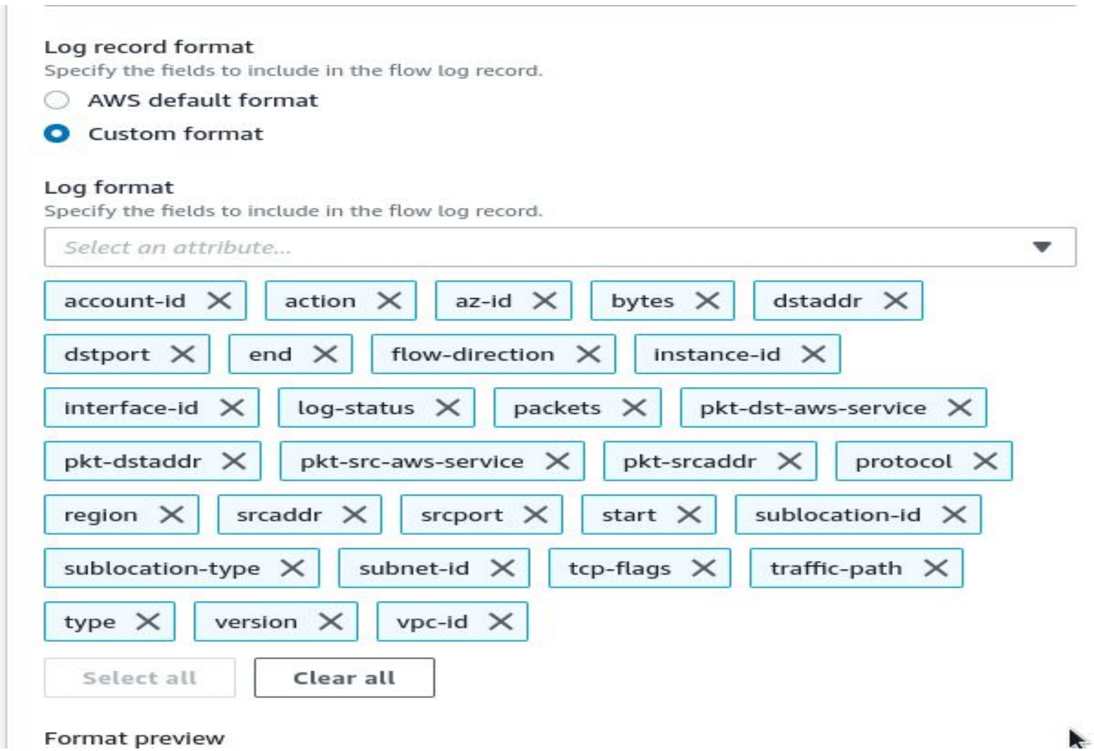
- ★ **Pros:**
  - ○ No impact on network latency
  - ○ Easy integration with other services
- ★ **Cons:**
  - ○ Immutable once configured
  - ○ All IP traffic types are not captured

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

KON HAI YE LOG?
KAHA SE AATE HAI YE LOG?



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

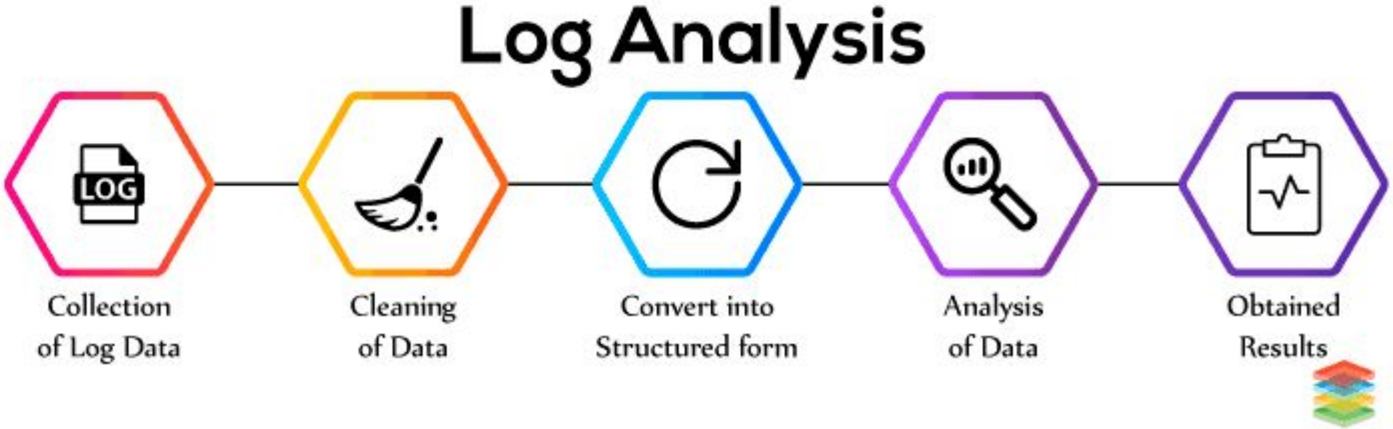
Publishing Flow Logs

- ★ 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?

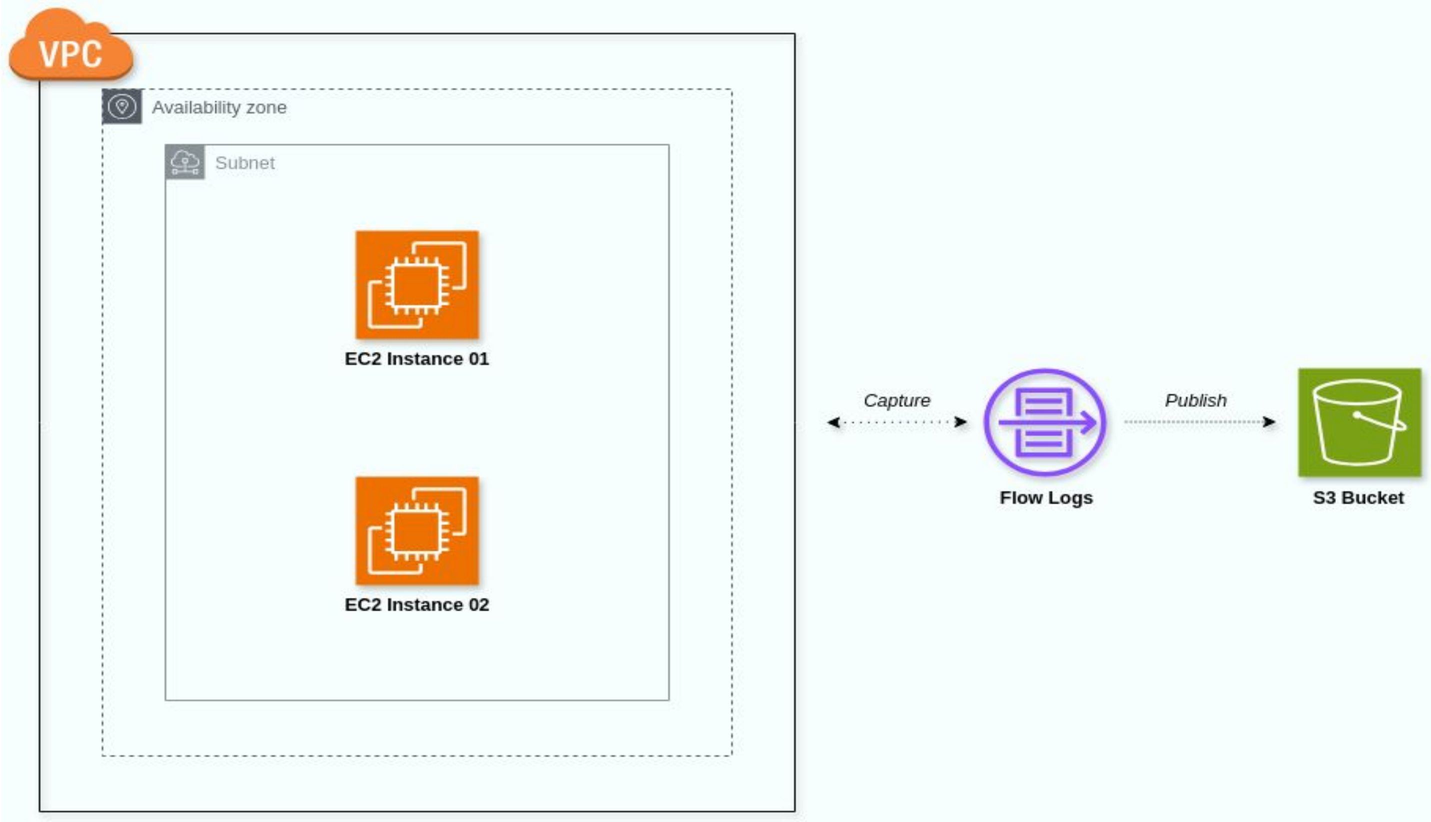


***Figure:** Architecture Used During The 8th July Linux Persistence Demo*

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

QUIZ
TIME

Q1: ***Which agent is used to collect VPC Flow Logs?***

A: ***It’s Agentless***

Q2: *On what levels can the VPC Flow Logs be captured?*

A: ***VPC level, Subnet level, Network Interface level***

Q3: On which AWS services Flow Logs can be published?

A: *CloudWatch, Data Firehose (formerly known as Kinesis Data Firehose), S3*

Q4: How much impact on network throughput (in *milliseconds*) does Flow Logging causes a VPC in an hour?

A: ***Zero milliseconds***

Q5: What does ***Fairth*** mean?

A: *Picture Taken By Magical Means*

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