Breach Workshop
APT

Muchilwa Lawrence
2024

FIRST

Copyright

FIRST.Org makes no representation, express or implied, with regard to the accuracy of the information contained in this material and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

About the author

Muchilwa Lawrence
DFIR, CTI, SOC, NCERTS,
Capacity development, BSides, Honeypots
FIRST Africa Regional Liaison

Previously

- CYBER RANGES
- Silensec
- KENET

Let’s connect!

- Twitter: @muchilwa
- LinkedIn: https://www.linkedin.com/in/lawrence-muchilwa-9a36b06a/

Workshop progress

Based on the Incredible original work done by:

Maarten van Horenbeeck &
CISO at ZenDesk
Member, Board of Directors FIRST

Previously

- Amazon
- Google
- Microsoft

Let’s connect!

- Twitter: @maartenvh
- LinkedIn: https://www.linkedin.com/in/maartenv/

Workshop progress

Setting

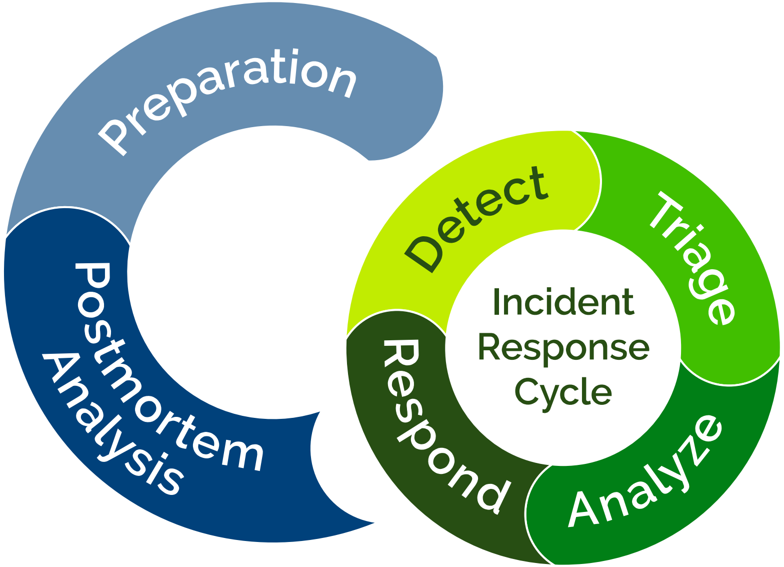
You are the **head of an Incident Response team** at a major telecommunication institution serving businesses and individuals within the country.

Your organization facilitates the communication of Critical Information Infrastructure (CII).

Workshop progress

Before we start let's have a look at the...

Incident Management

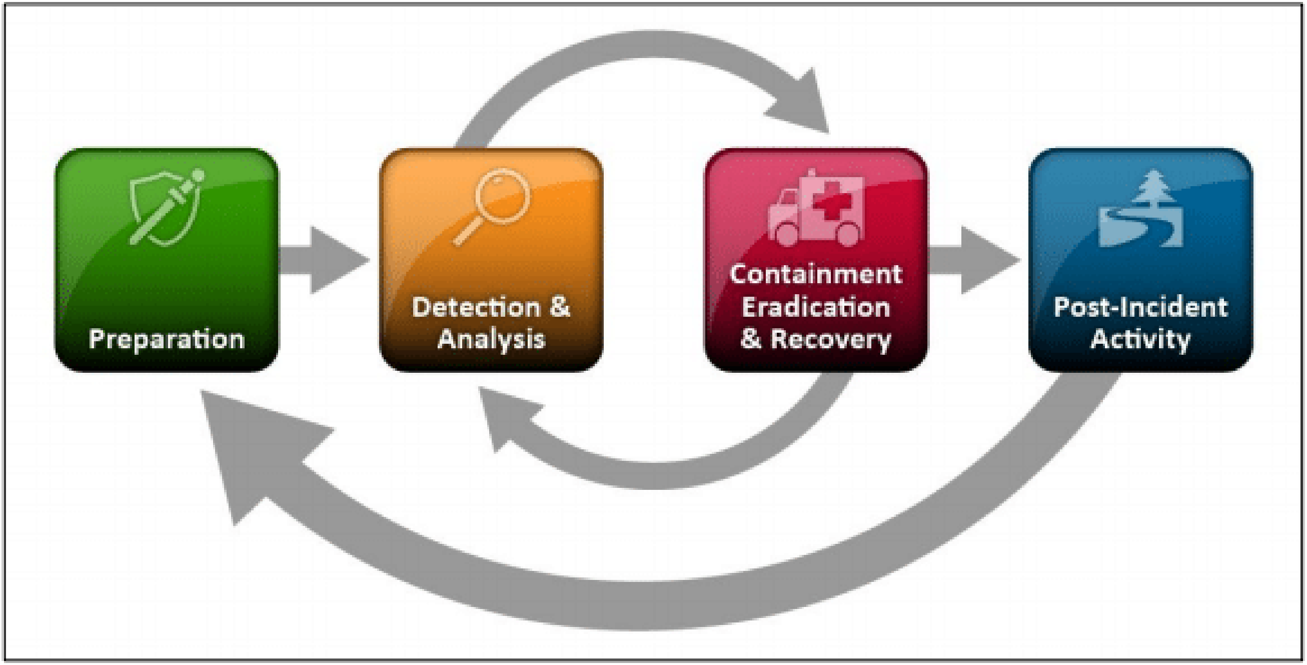


Workshop progress

Breach Workshop APT, KeNOG © 2024, FIRST.Org

Before we start let's have a look at the...

Incident Management



Head of Incident Response

Lions

You are the head of an Incident Response team at a major telecommunication institution serving businesses and individuals within your country.

● ● ○ ○ ○ ○ ○ ○ ○

Workshop progress

Setup your team

Lions

Who do you want to be in your team, what skill are you lacking?
Select 4 people's title.
Who are they?

- ?
- ?
- ?
- ?

What skills are you lacking?

● ● ○ ○ ○ ○ ○ ○ ○

Workshop progress

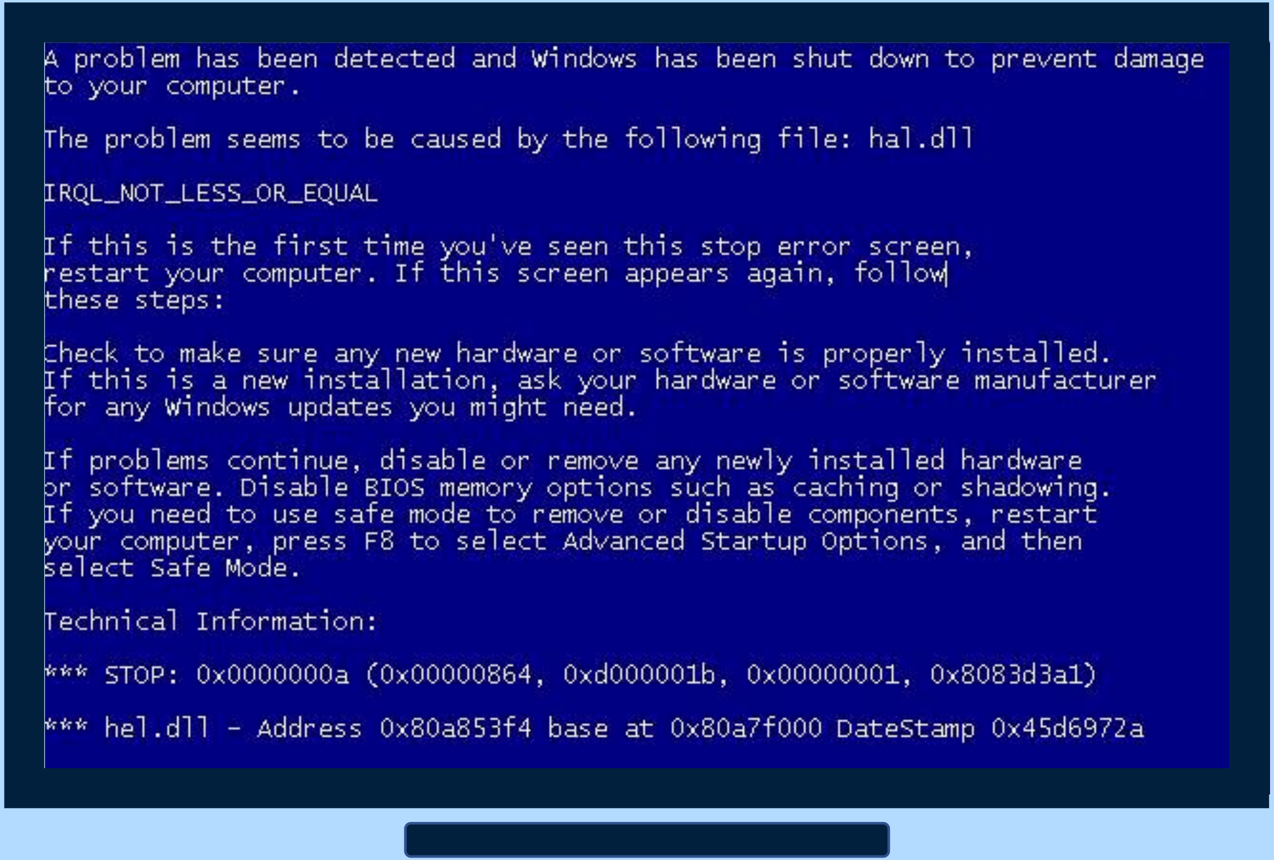
Organisation

Lions

- Plan your organization on a flip chart
- What reporting structures exist?
- Who manages and accesses technology?
- Who engages with the outside world?

Workshop progress

Case 1



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: hal.dll

IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use safe mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical Information:

*** STOP: 0x0000000a (0x00000864, 0xd000001b, 0x00000001, 0x8083d3a1)

*** hel.dll - Address 0x80a853f4 base at 0x80a7f000 DateStamp 0x45d6972a
```

Workshop progress

Group Task:

Lions

What would you do?

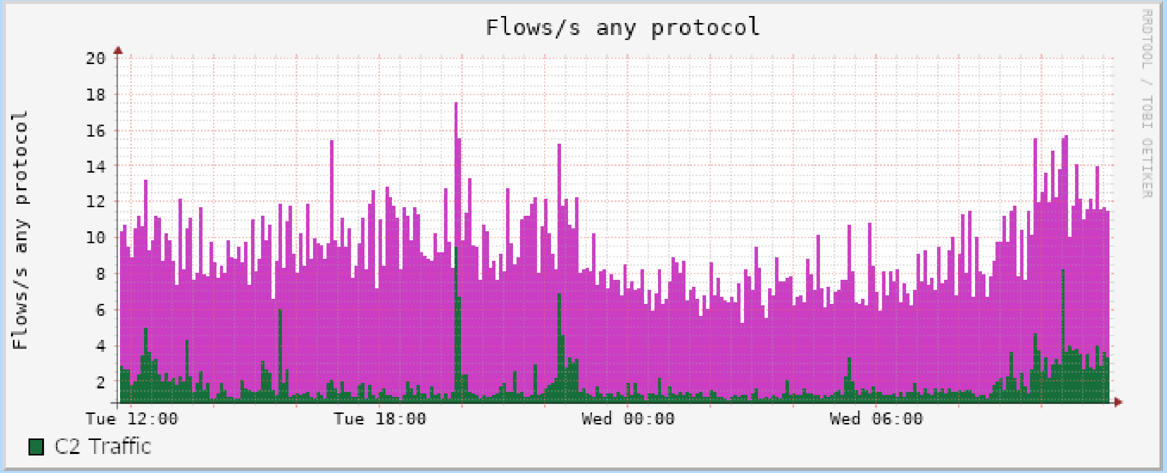
- Plan your next steps and actions
- Remember the IR Process

Workshop progress

Malware found

An analysis shows a unknown piece of Malware:

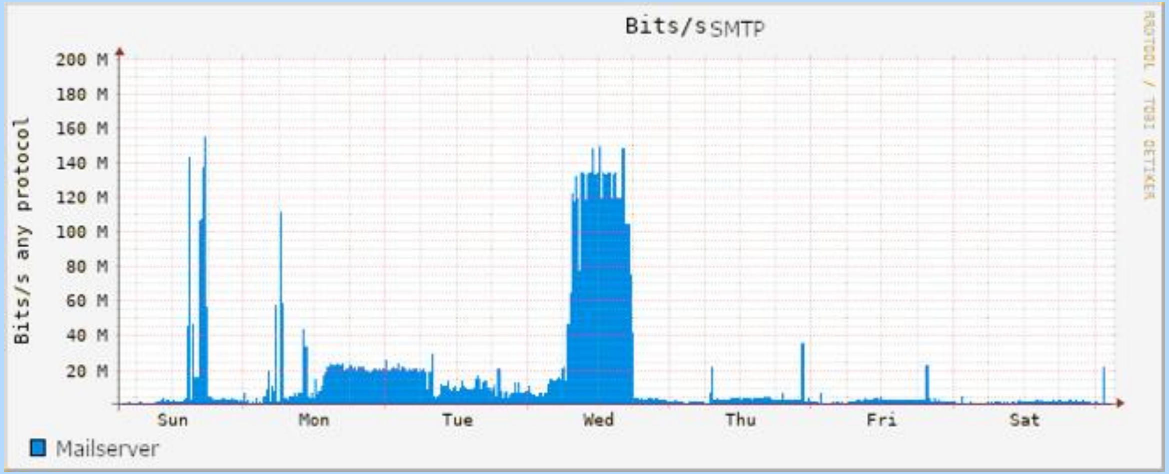
- Found on several hosts
- C2 Traffic for further hosts, including Mail server



Workshop progress

Mailserver

Malware has the ability to collect mail and send it out. At least 5 gigabytes of egress data is identified.



Workshop progress

Group Task

Issues

Lions

- Whom do you notify?
- Should law enforcement be involved?
- Who is affected?
- How do you respond?

● ● ● ● ● ● ○ ○ ○

Workshop progress

Group Task

Lions

Notifying of a breach

- User information was taken of several customers, including their address, account information and name
- Do you have a notification obligation?
- How do you notify?
- Were you insured? How do you pay for response activities?

● ● ● ● ● ● ○ ○ ○

Workshop progress

Case 1.2

An external party reports they received malware from your employees.

What does this imply?

What actions do you take?

Date: 24 April 2024
From: Jane.Doe@example.com
To: security@lions-bank.com
Subject: Malware!?

Hello Security Team

I received a mail from one of your addresses, which was flagged by my Virus scanner. I did not open it, but thought I'd let you know.

Bet regards
Jane

Workshop progress

What happened?

Several malicious e-mails received a few weeks ago

- Some blocked, but logs are not analyzed
- Some not recognized

One user clicked the attachment and thus

- Installs a backdoor
- Has his address book stolen

Phishing campaign against all users

Malware sent to entries of address book

Workshop progress

Group Task

Lions

Next steps

- How does this new information guide your investigation?
- Are there new systems in scope of your investigation?

Workshop progress

What went well?

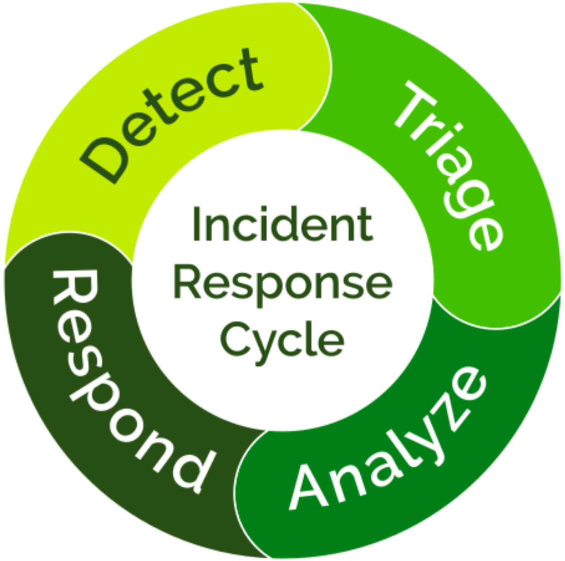
What went bad?

Lions

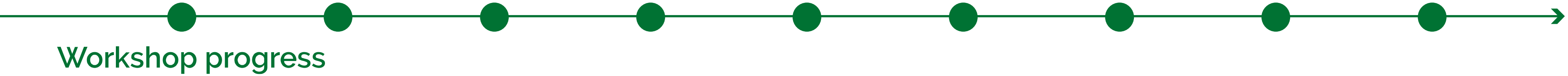
Discussion

- What went well, what not?
- What would you do differently in the set up phase of the exercise?
- What did you need during your investigation that you had not planned for ahead of time?

Workshop progress



- Incident analysis
- Communication
- Prioritizing
- Responding



This might never happen…

Nimewaaaaaaaaaaaaaaaaaaaarn !

…but something similar or totally different might.