TF-CSIRT
TRANSITS

TRANSITS Group Exercise

Based on ENISA Exercise 11“Incident Handling in Live Role Playing”

Nairobi, Kenya
8 November 2022

TF-CSIRT TRANSITS

The Rulers of Time

(and supporting actors)

for this exercise:

the Tutors

They **know** all, **see** all and can pause / fast forward / reverse **time**.

Alice

- A talented young (and underpaid) designer.
- Not very happy at Ads-R-Us, and she has been looking for work for a while.

On today's, Saturday morning she received an email from a potential employer, with a PDF attachment describing the position, but when she opened it, it appeared to be empty.

ADS R US

Photo by Christina @ wocintechchat.com on Unsplash

Charlie

- Network engineer
- Set-up VPN to allow secure remote working
- Is on duty today to provide general support

He is responsible for the company network.

He doesn’t really understand why Ads-R-Us needs a CSIRT function, but thinks that ERNEST is a pretty good guy all the same.

Ernest

- Network administrator and IT Support
- Part-time CSIRT Officer

He is responsible for the company network and software, including the security stuff and he has regular contact with Big-ISP and the software vendors who provide services to Ads-R-Us.

ADS RUS

Photo by Desola Lanre-Ologun on Unsplash

Winston

- CEO of Ads-R-Us
- A little stressed about the company finances
- Delegation is his key management skill

He is looking forward to a meeting with a big client on Monday for a new campaign, which he has been told will be ready in time.

Right now he is relaxing at home, as its his daughter's birthday.

Photo by Fortune Vieyra on Unsplash

Kevin

- Keen IT student
- Loves tinkering with computers
- Into computer security

He believes in ethical hacking, and often finds security flaws in software. He also believes strongly that commercial companies should be generous to helpful testers like him.

Steve

- Head developer at MUNIX
- Ads-R-Us uses MUNIX as their group working tool
- Is aware of some bugs, and is working to fix them

MUNIX

online project management done right

He recently took a phone call from some guy asking for a lot of money to tell him about a bug he'd found. He offered the guy credit in the security advisory, but the guy just laughed and hung up. He looked into it and found the bug, but decided to keep it quiet until he had written a patch.

Patrick

- CSIRT Officer in the biggest ISP in the country
- On duty today
- BIG-ISP supplies the internet connection to Ads-R-Us and the majority of users in the country.

He met ERNEST once at a TF-CSIRT meeting, exchanged PGP keys, and has regular contact with him professionally.

Scenario

It is Saturday morning, and Alice is working remotely on an important project which is due on Monday. She is trying to access some files on the company server over VPN. She can access the server alright, but the files she left there on Friday evening are missing. So she calls the company helpline.

The administrator on duty (Charlie) will discover that somebody had accessed the server from Alice's account last night and apparently erased the project files of all the users from the file server.

Since Alice's account is a regular user account without sufficient privileges to access or modify another user's data, there seems to be something seriously wrong...

The Players

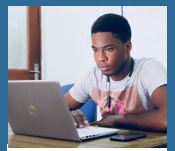
ADS RUS

WINSTON

CEO

CHARLIE

Network Engineer



ERNEST

Sys. Admin

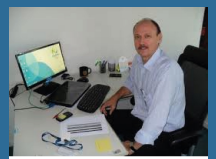
CSIRT

ALICE

Junior

Designer

BIG ISP

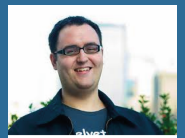


PATRICK

CSIRT

Officer

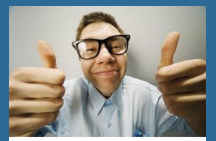
MUNIX



STEVE

Software

developer



KEVIN

Student

TF-CSIRT
TRANSITS

Thank you
Any Questions?

3, 2, 1 - Let the exercise begin …