

Specialized Attacks: OT and ICS

Exploring OT and ICS Attacks



Matt Lloyd Davies

Capability Development Lead



Setting the Scene



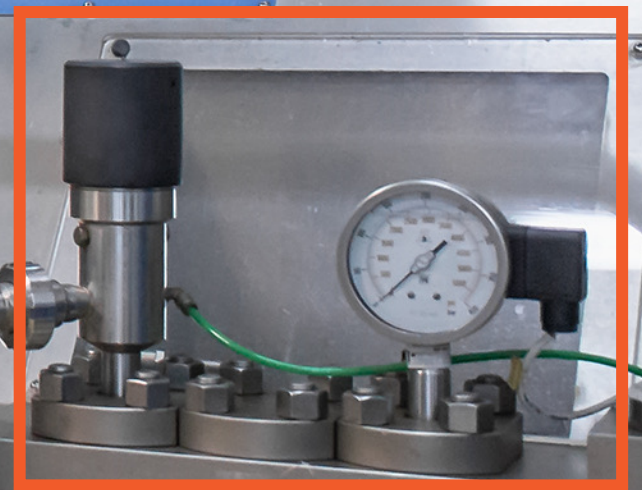
















The ICS Cyber Kill-chain



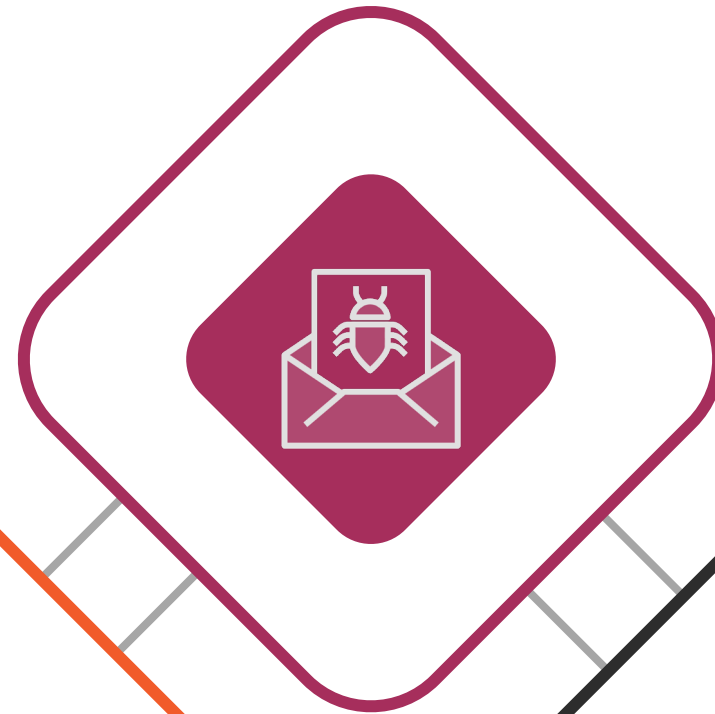
Reconnaissance

Gather information and research the target



Delivery

Implement methods to deliver the exploit to the target system



Installation

Create a new capability, or modify an existing capability



Actions on Target

Sustain, entrench, develop, execute to achieve objective



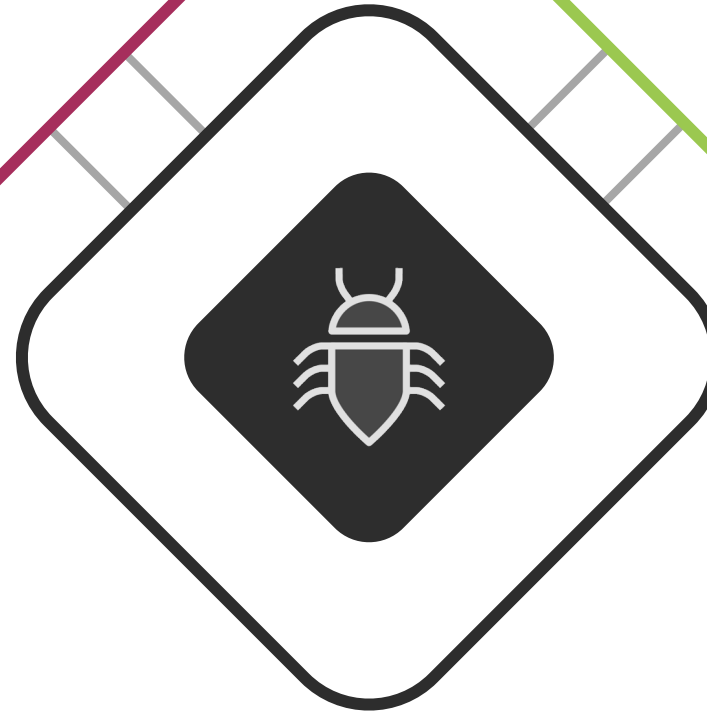
Weaponization

Create an exploit based on discovered vulnerabilities



Exploitation

Perform malicious actions to gain control of a system



Command and Control

Manage, control and enable the attack campaign



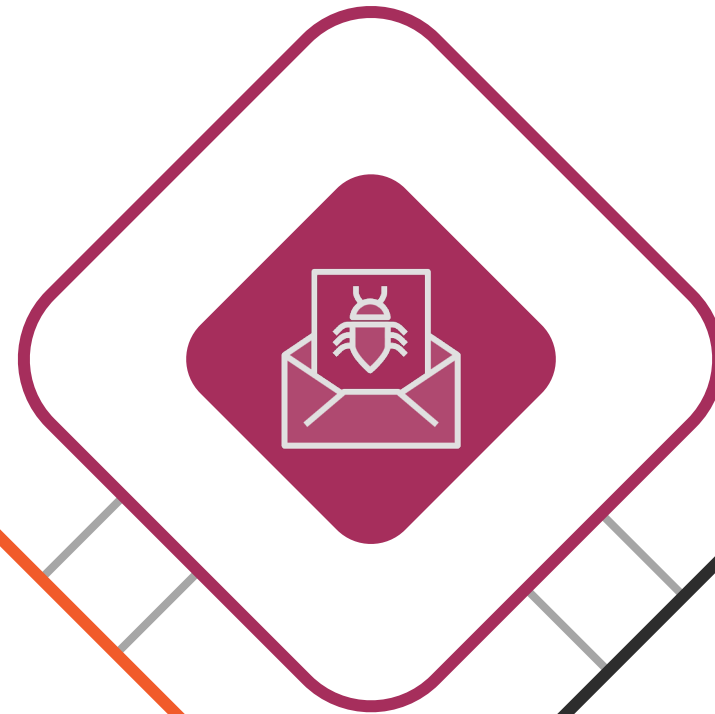
Reconnaissance

Gather information and research the target



Delivery

Implement methods to deliver the exploit to the target system



Installation

Create a new capability, or modify an existing capability



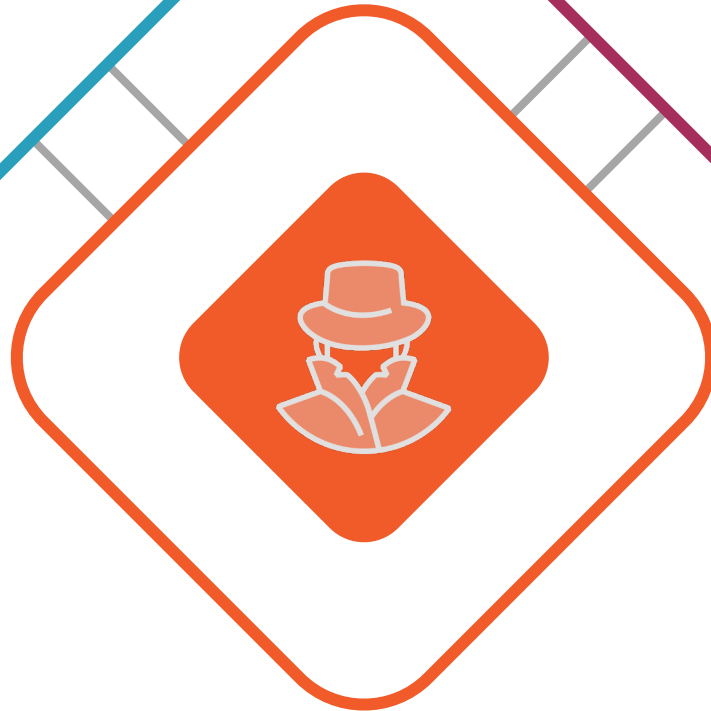
Actions on Target

Sustain, entrench, develop, execute to achieve objective



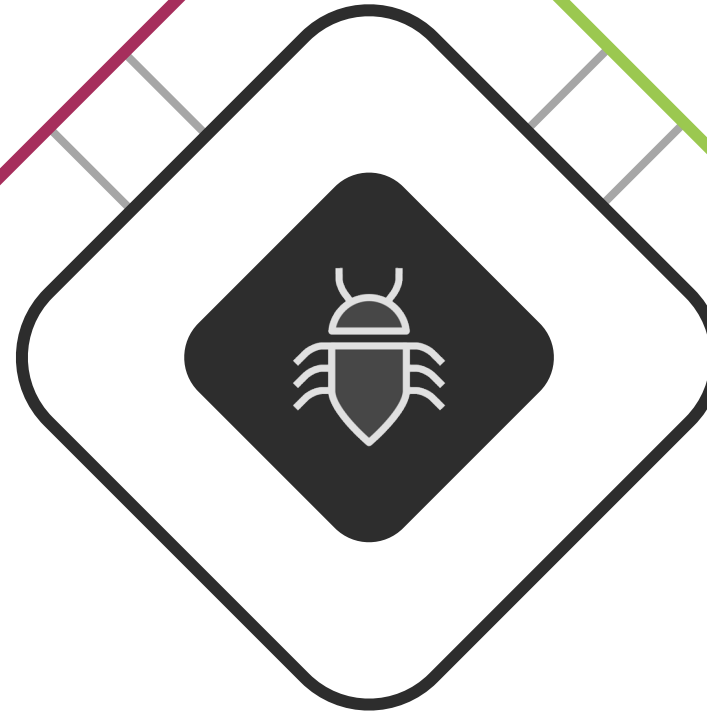
Weaponization

Create an exploit based on discovered vulnerabilities



Exploitation

Perform malicious actions to gain control of a system



Command and Control

Manage, control and enable the attack campaign



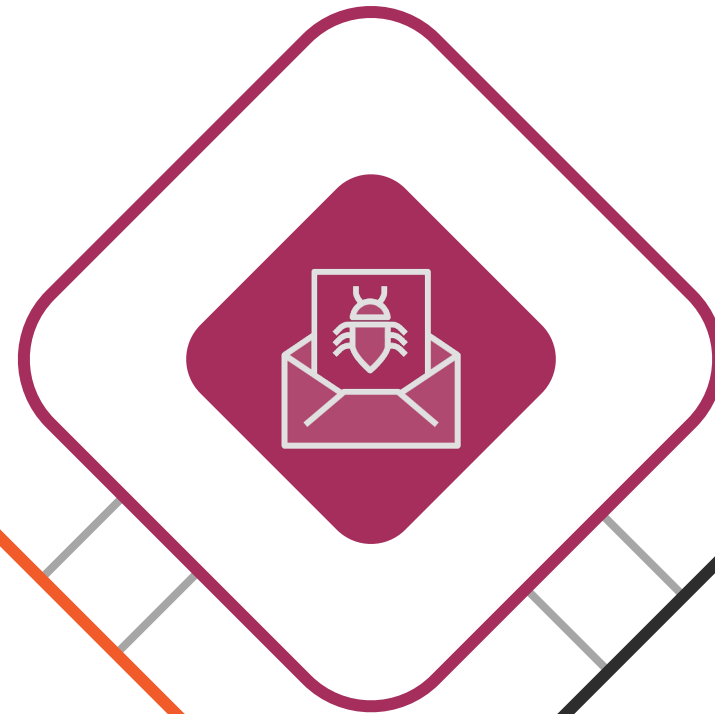
Reconnaissance

Gather information and research the target



Delivery

Implement methods to deliver the exploit to the target system



Installation

Create a new capability, or modify an existing capability



Actions on Target

Sustain, entrench, develop, execute to achieve objective



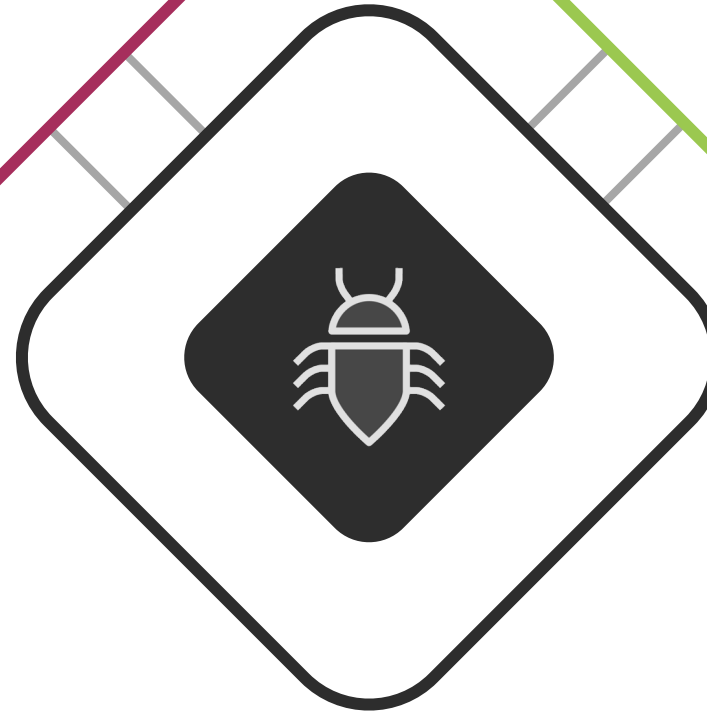
Weaponization

Create an exploit based on discovered vulnerabilities



Exploitation

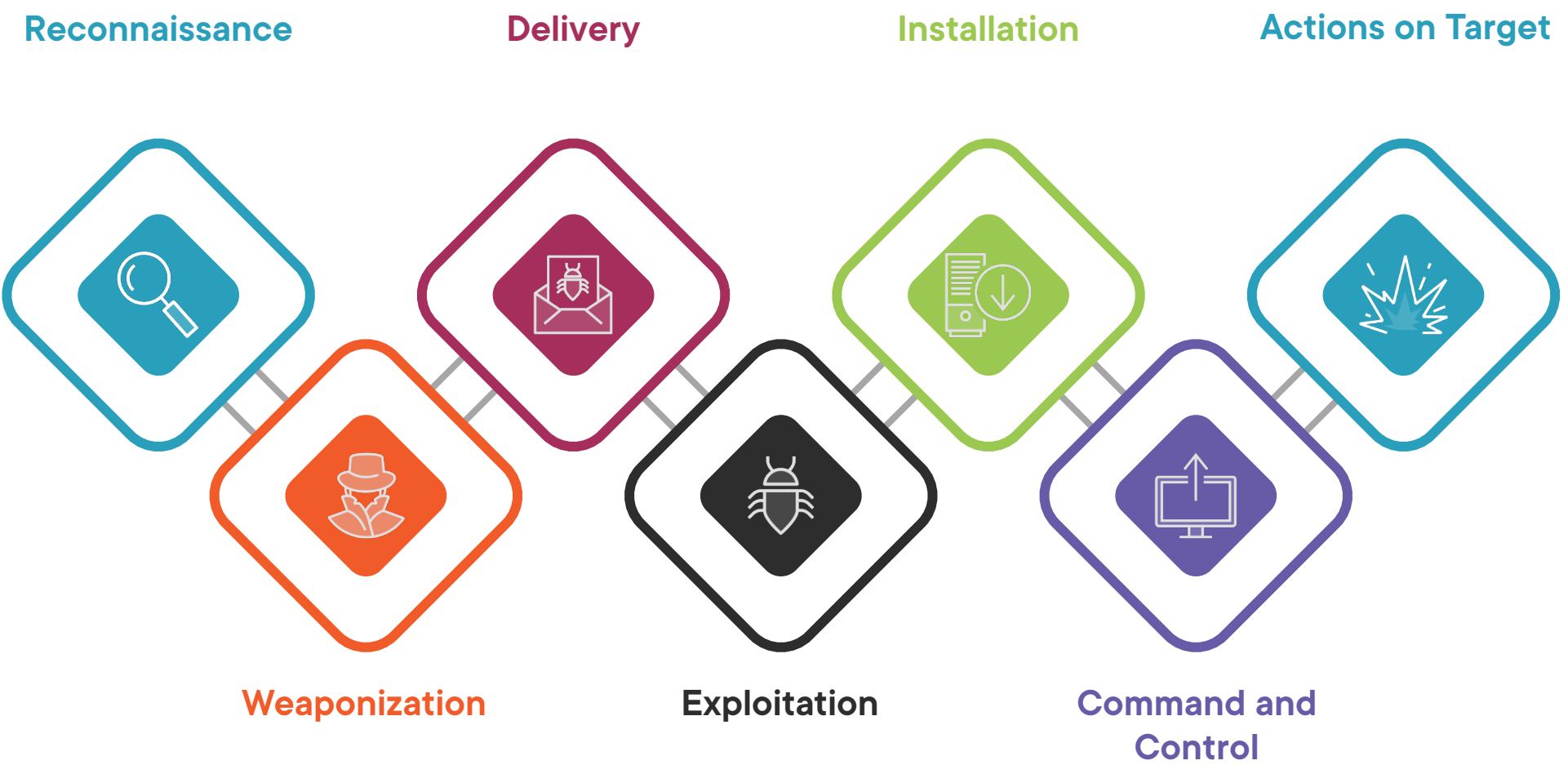
Perform malicious actions to gain control of a system



Command and Control

Manage, control and enable the attack campaign





Assante and Lee
2015

Stage 1

Stage 2



Develop & Test

Develop new capability, tune and validate



Install & Modify

Embed the new capability and fine tune it



ICS Attack

Enabling, initiating or supporting activities



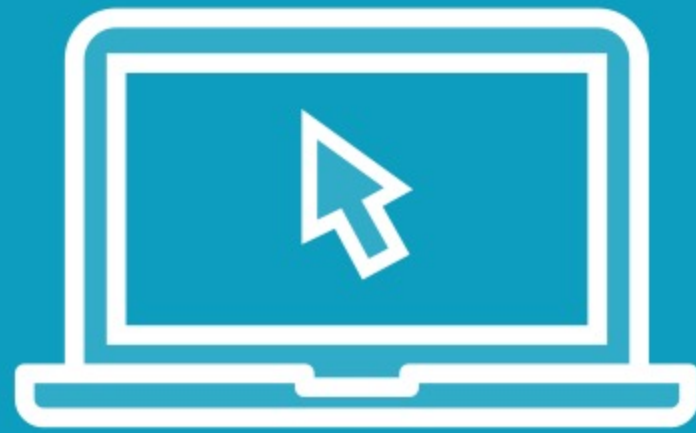
Deliver
Bring the new capability to the target system



Execute
Launch the intended action against the target



Demo



Finding Internet Connected Operational Technology



Warning!



Seek permission, and know the law.



Host Sur

Rockwell Automation

8585/index.html

...

☆

Allen-Bradley

1769-L30ER/A LOGIX5330ER

Rockwell Automation

Expand

Minimize

Home

Diagnostics

Home

Device Name	1769-L30ER/A LOGIX5330ER
Device Description	
Device Location	
Ethernet Address (MAC)	
IP Address	
Product Revision	32.011
Serial Number	
Uptime	26 days, 22h:24m:42s

Resources

[Visit AB.com for additional information](#)

Contacts

Copyright © 2009 Rockwell Automation, Inc. All Rights Reserved.

Host Sur xRockwell Automation x+

8585/index.html

Allen-Bradley

1769-L30ER/A LOGIX5330ER

Rockwell Automation

ExpandMinimize

Home

Diagnostics

Diagnostic Overview

Network Settings

Application Connections

Bridge Connections

Ethernet Statistics

Ring Statistics

Advanced Diagnostics

Diagnostic Overview

Network Settings

Application Connections

Bridge Connections

Ethernet Statistics

Ring Statistics

Network Interface

Ethernet Address (MAC)

IP Address

Subnet Mask255.255.255.0

Default Gateway

Primary Name Server

Secondary Name Server

Default Domain Name

Host Name

Name ResolutionDNS Enabled

SMTP Server

Ethernet Interface Configuration

Obtain Network ConfigurationStatic

Switchesn/a

Ethernet Port 1

Interface StateEnabled

Link StatusActive

Speed100 Mbps

DuplexFull Duplex

Autonegotiate StatusAutonegotiate Speed and Duplex

Ethernet Port 2

Interface StateEnabled

Link StatusActive

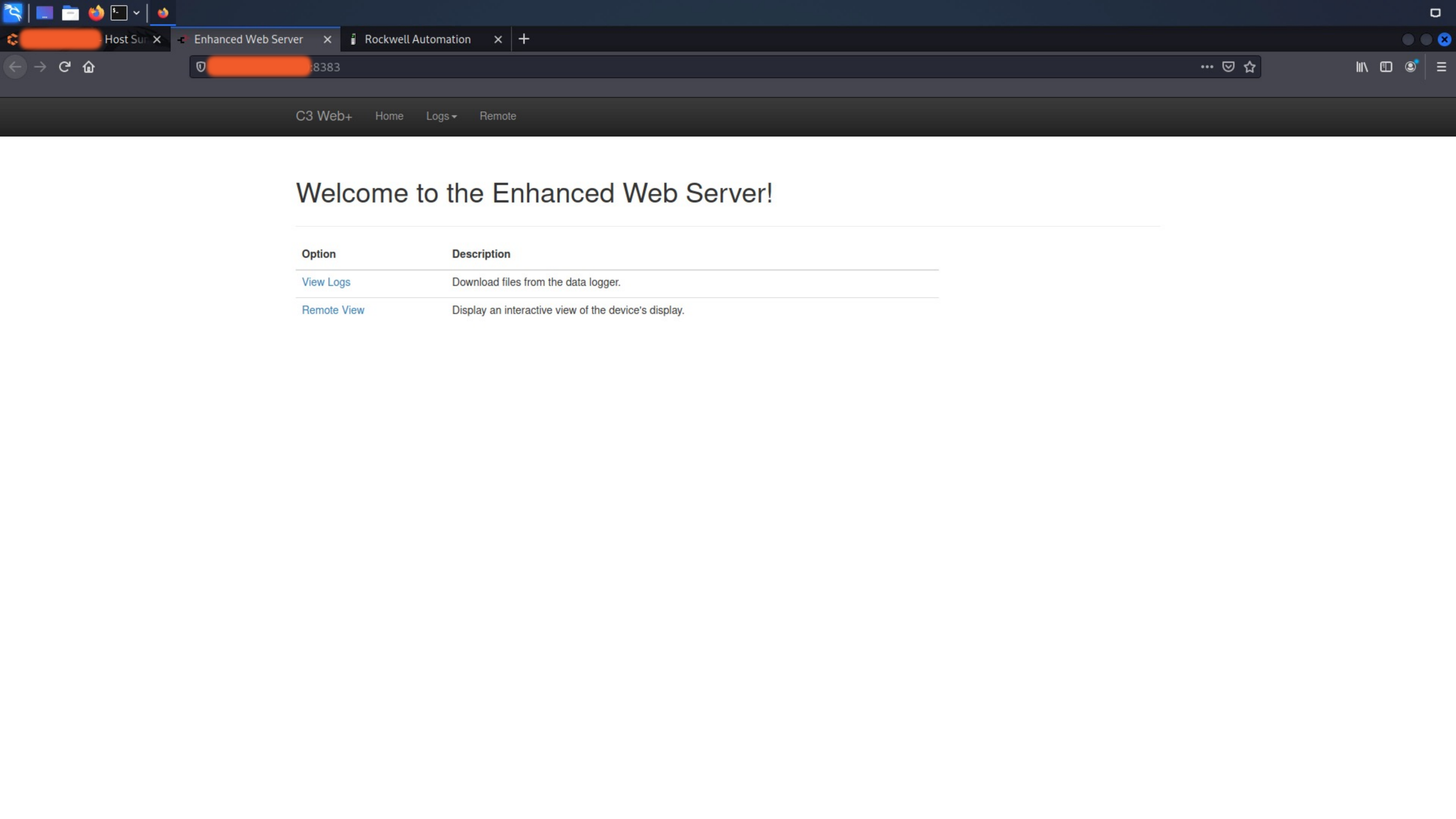
Speed100 Mbps

DuplexFull Duplex

Autonegotiate StatusAutonegotiate Speed and Duplex

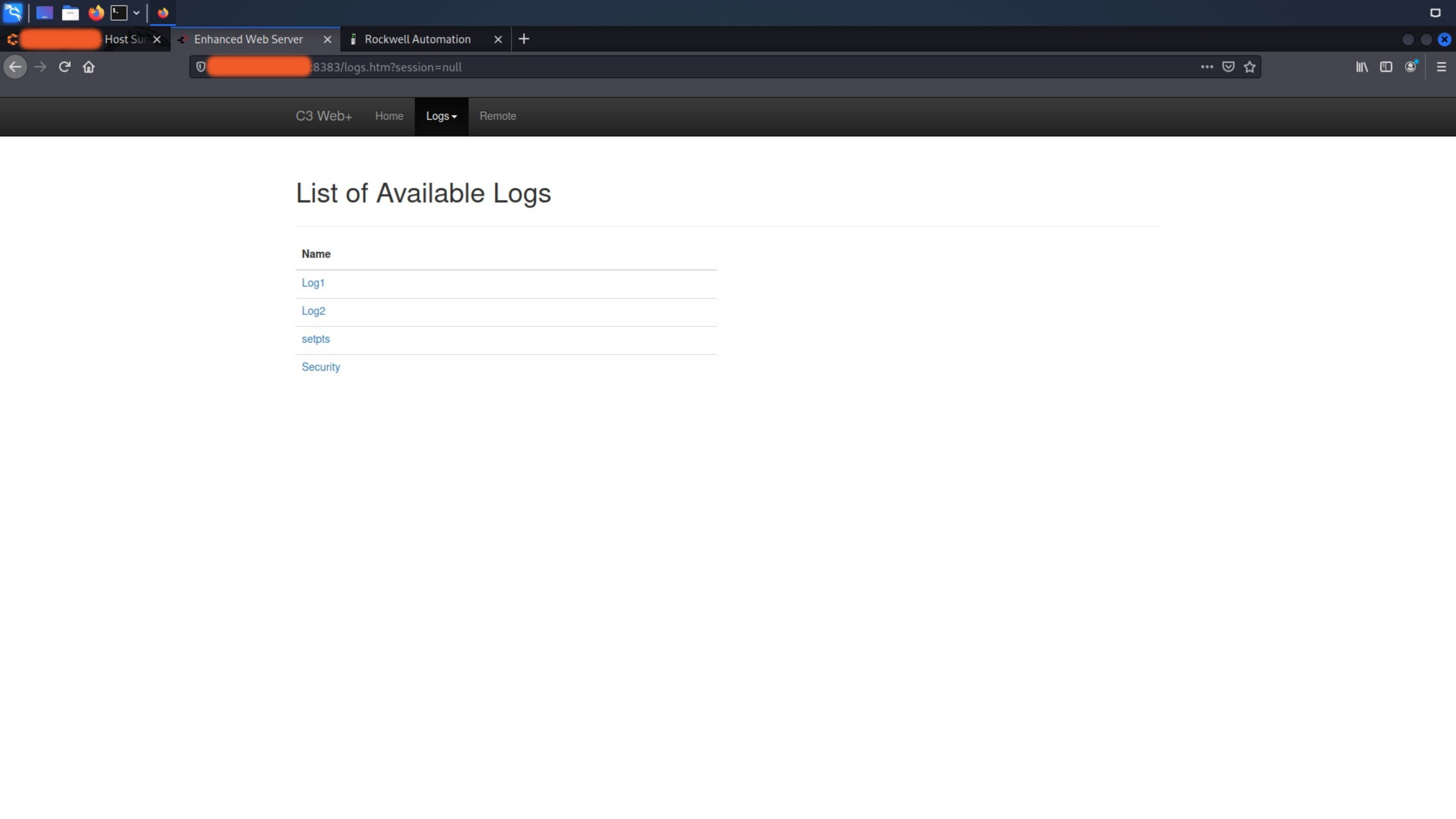
Seconds Between Refresh: 15Disable Refresh with 0.

Copyright © 2009 Rockwell Automation, Inc. All Rights Reserved.



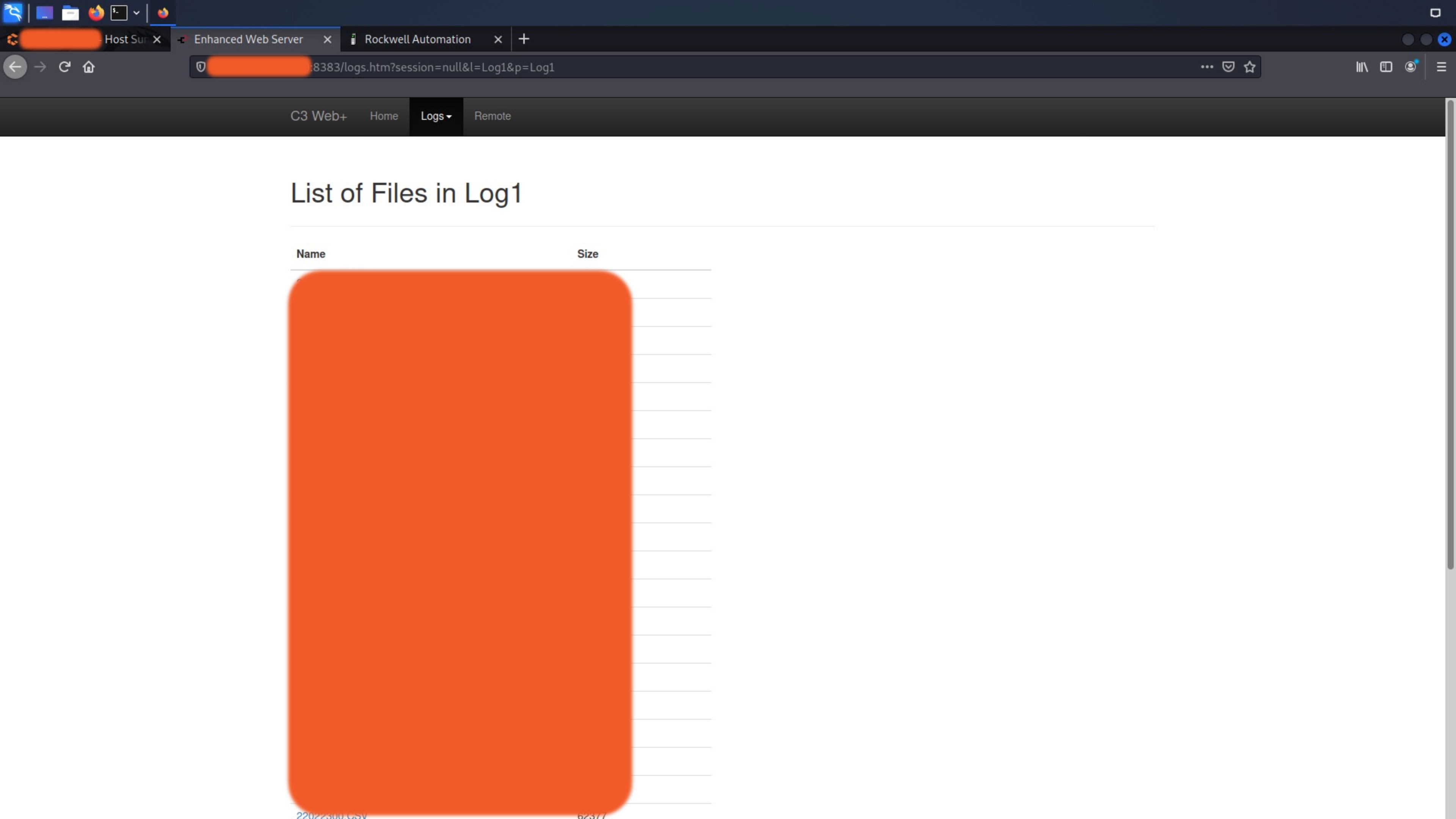
Welcome to the Enhanced Web Server!

Option	Description
View Logs	Download files from the data logger.
Remote View	Display an interactive view of the device's display.



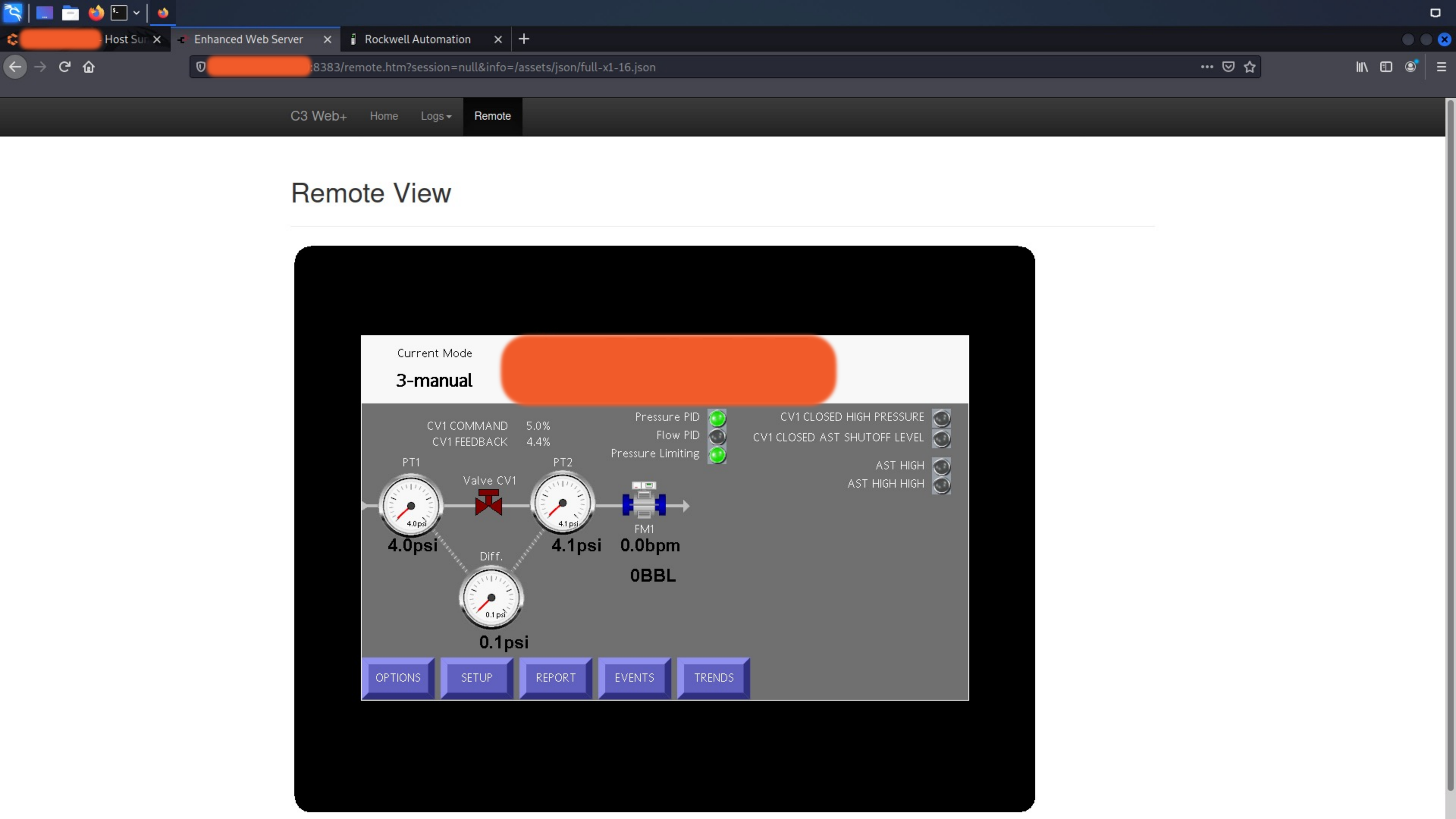
List of Available Logs

Name
Log1
Log2
setpts
Security



List of Files in Log1

Name	Size
22022300.CSV	82377



Host Sur

SIMATIC 300-Station

8082/Portal0000.htm

English

SIEMENS

SIMATIC 300-Station

SIMATIC S7 CP

Start page

Identification

Rack configuration

Diagnostic buffer

Industrial Ethernet

PROFINET IO

Configured Connections

IP access protection

Media Redundancy

General:

Station name:

Module name:

Module type:

Status:

Operating state: RUN

Host Sur

SIMATIC 300-Station

8082/Portal2000.htm

English

SIMATIC S7 CP

Start page

Identification

Rack configuration

Diagnostic buffer

Industrial Ethernet

PROFINET IO

Configured Connections

IP access protection

Media Redundancy

Identification

Identification:

Plant designation:

Location identifier:

Serial number:

Order number: 6GK7 343-1CX10-0XE0

Version:

Hardware: 4

Firmware: V2.3.2

Transferring data from

Host Sur

SIMATIC 300-Station

8082/Portal2000.htm

English

SIMATIC S7 CP

Start page

Identification

Rack configuration

Diagnostic buffer

Industrial Ethernet

PROFINET IO

Configured Connections

IP access protection

Media Redundancy

Rack configuration

Rack configuration (UR, Rack: 0)

Slot	Status	Module name	Order number	Version	LED state
1					
2			6ES7 313-6CF03-0AB0	V2.6.11	SF - RUN - STOP - FRCE - BUS1F
3					
4			6ES7 331-7KB02-0AB0		
5			6GK7 343-1CX10-0XE0	V2.3.2	SF - RUN - STOP - BUS1F - MAINT
6					
7					
8					
9					
10					
11					

Host Sur

SIMATIC 300-Station

8082/Portal4000.htm

English

SIMATIC S7 CP

Start page

Identification

Rack configuration

Diagnostic buffer

Industrial Ethernet

PROFINET IO

Configured Connections

IP access protection

Media Redundancy

Industrial Ethernet

Parameters

Statistics

TCP connections

UDP connections

Network attachment:

MAC address (active):

MAC address (factory setting):

Device name: pn-io

Physical properties:

Port number	Link status	Settings	Mode	Media Redundancy
1	OK	automatic	100 Mbit/s full duplex	---
2	OK	automatic	100 Mbit/s full duplex	---

IP parameters:

IP address:

Subnet mask: 255.255.255.0

Default router:

Router used:

IP settings: IP address obtained from STEP 7 configuration

Name

Passwort

[Login](#)

[► Start page](#)

- ▶ Remote Control

► Control Functions

- System Diagnostics

► File Browser

Miniweb Start Page

Welcome on

Device Status of
The runtime is running

General Device Information	
Device Type	TP700 Comfort
Image version	V11.00.01.00_01.19
Bootloader version	1.08
Bootloader release date	25.3.2011
Device Name	

Hint:
When the devicename contains an underscore (_) some browsers have a bug that makes it impossible to log in. One possible solution may be to use the IP address of the device instead of the name, or to use another browser.

Host Sur

Miniweb Start Page

SIMATIC 300-Station

8083/www/start.html

⋮

🔒

☆

🔍

📄

👤

☰

SIEMENS

SIMATIC HMI Miniweb on

Name

Passwort

Miniweb Start Page

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

▶ Start page

▶ Remote Control

▶ Control Functions

▶ System Diagnostics

▶ File Browser

Device Status of

The runtime is running

General Device Information	
Device Type	TP700 Comfort
Image version	V11.00.01.00_01.19
Bootloader version	1.08
Bootloader release date	25.3.2011
Device Name	

Hint:

When the devicename contains an underscore (_) some browsers have a bug that makes it impossible to log in.
One possible solution may be to use the IP address of the device instead of the name, or to use another browser.

Host Sur

Remote Control

SIMATIC 300-Station

8083/RemoteControl.html

SIEMENS

SIMATIC HMI Miniweb on

Welcome Administrator
You are logged in.
[Logout](#)

Start page

Remote Control

Control Functions

System
Diagnostics

File Browser

Miniweb Start Page

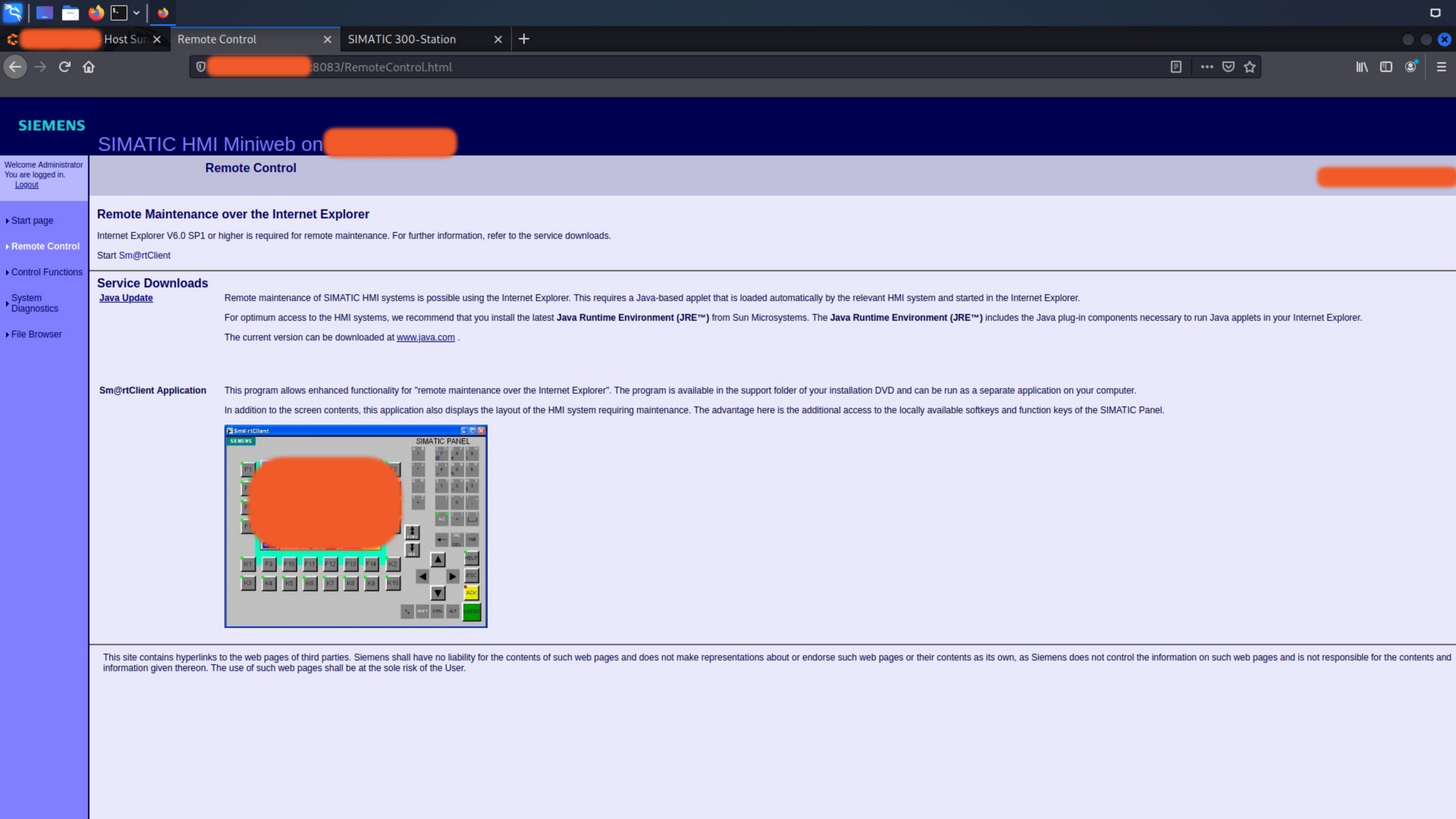
Welcome on

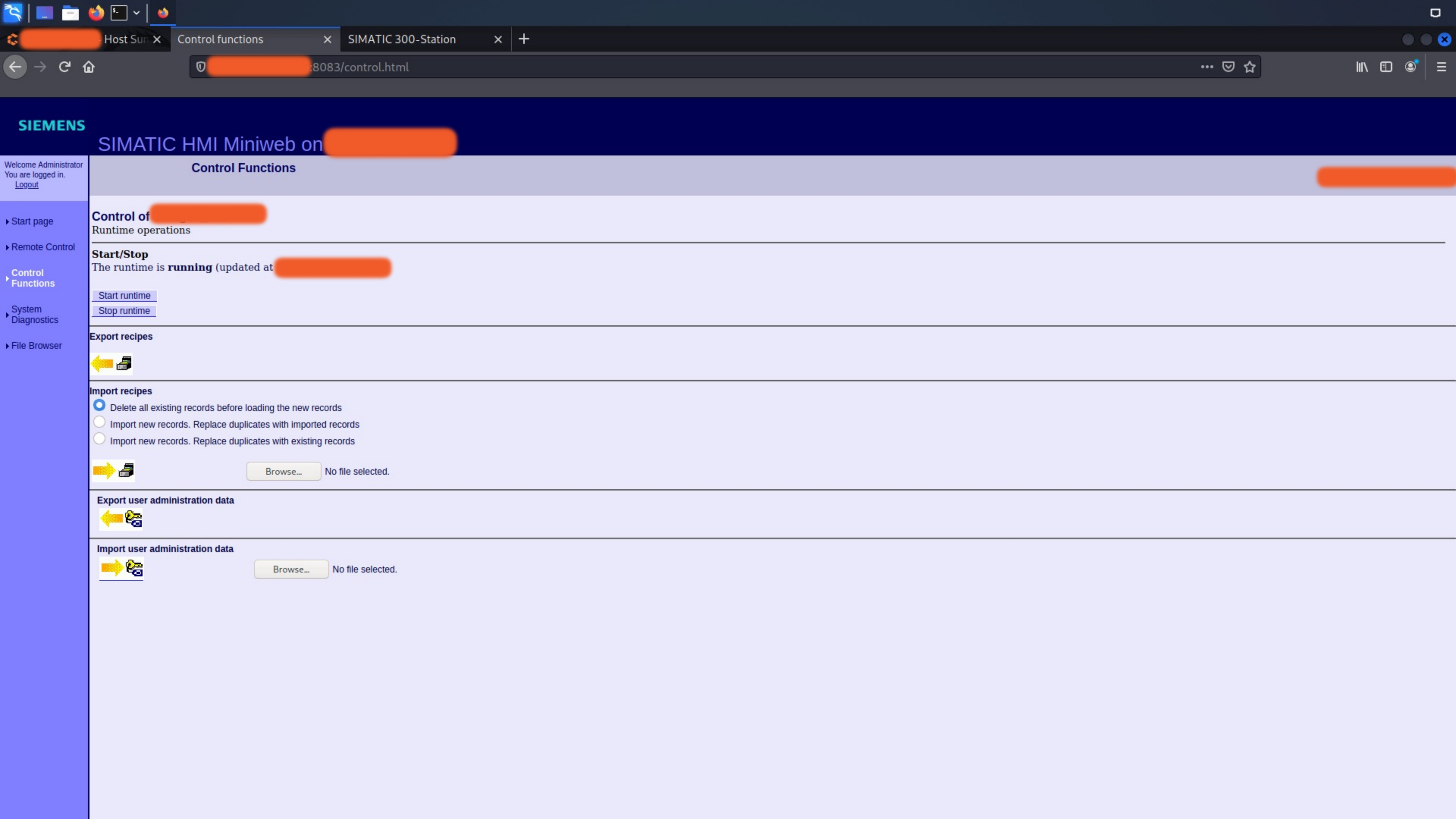
Device Status of

The runtime is running

General Device Information	
Device Type	TP700 Comfort
Image version	V11.00.01.00_01.19
Bootloader version	1.08
Bootloader release date	25.3.2011
Device Name	

Transferring data from





Host Sur

System Diagnostics

SIMATIC 300-Station

8083/StatusDetails.html

SIEMENS

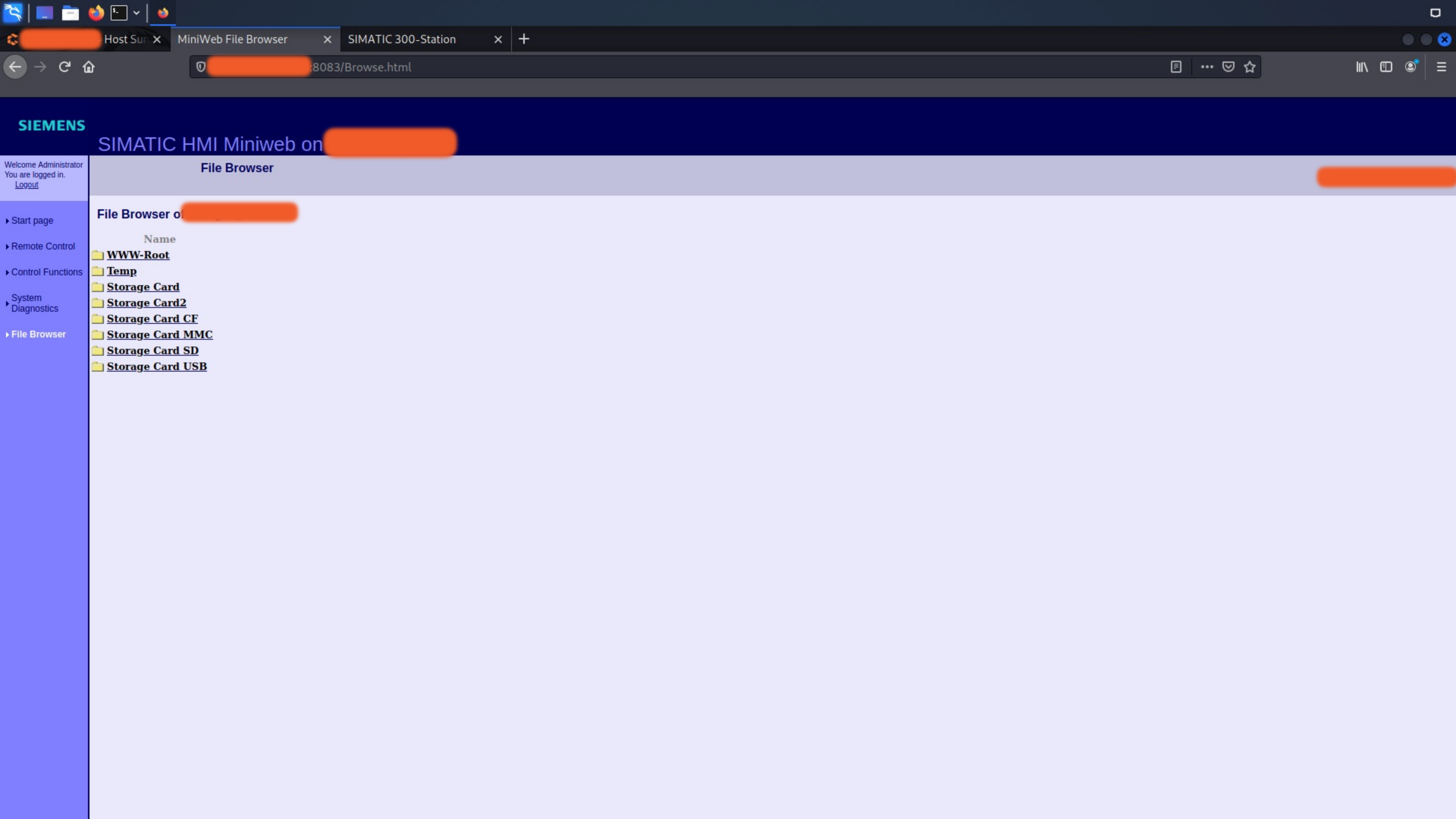
SIMATIC HMI Miniweb on

Welcome Administrator
You are logged in.
[Logout](#)

System Diagnostics

System diagnostics of

message number	timestamp	state	message text
70037			
70037			
70037			
70037			
70037			
70037			
70037			
70037			
230000			
230005			
70033			
80015			
80026			
140000			
110001			
80028			
70033			
80015			
140000			
80026			
110001			
80028			
70033			
80015			
80026			
140000			
110001			
80028			
70033			
80015			
80026			
140000			
110001			
80028			
70033			
80015			
80026			
140000			
110001			
80028			
70033			



SIEMENS

SIMATIC HMI Miniweb on 192.168.0.8083

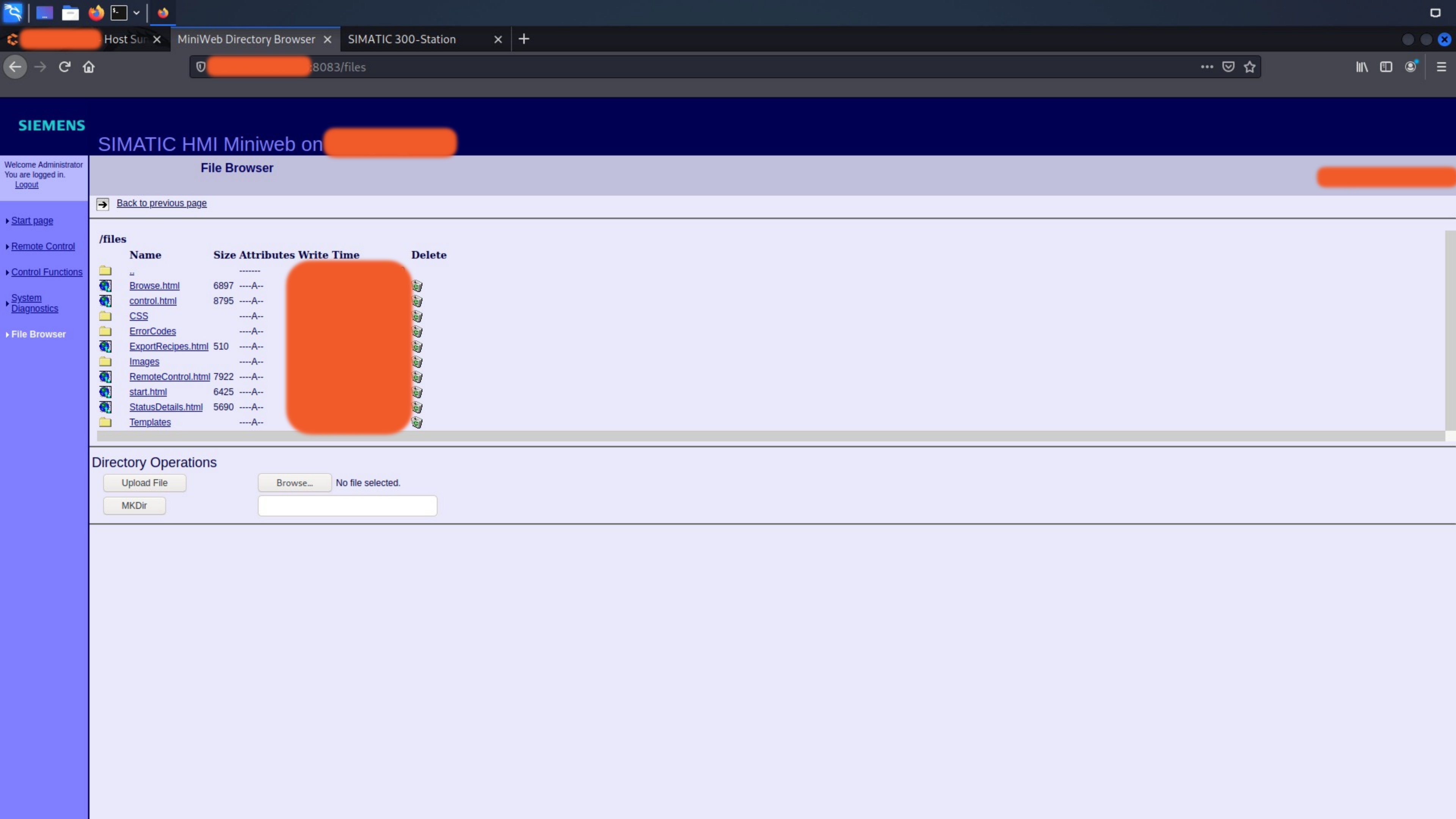
File Browser

Welcome Administrator
You are logged in.
[Logout](#)

- Start page
- Remote Control
- Control Functions
- System Diagnostics
- File Browser

File Browser on 192.168.0.8083

- Name
- WWW-Root
 - Temp
 - Storage Card
 - Storage Card2
 - Storage Card CF
 - Storage Card MMC
 - Storage Card SD
 - Storage Card USB



SIEMENS

SIMATIC HMI Miniweb on 192.168.0.8083

File Browser

[Back to previous page](#)

/files				
	Name	Size	Attributes	Write Time
	..		----	
	Browse.html	6897	---A--	
	control.html	8795	---A--	
	CSS		---A--	
	ErrorCodes		---A--	
	ExportRecipes.html	510	---A--	
	Images		---A--	
	RemoteControl.html	7922	---A--	
	start.html	6425	---A--	
	StatusDetails.html	5690	---A--	
	Templates		---A--	

Directory Operations

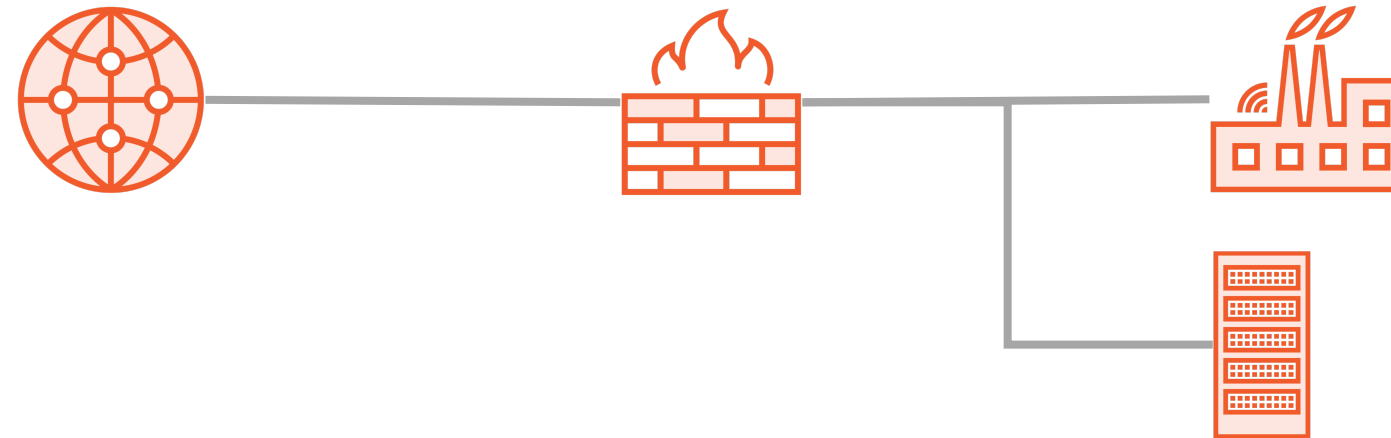
No file selected.

Gaining Access

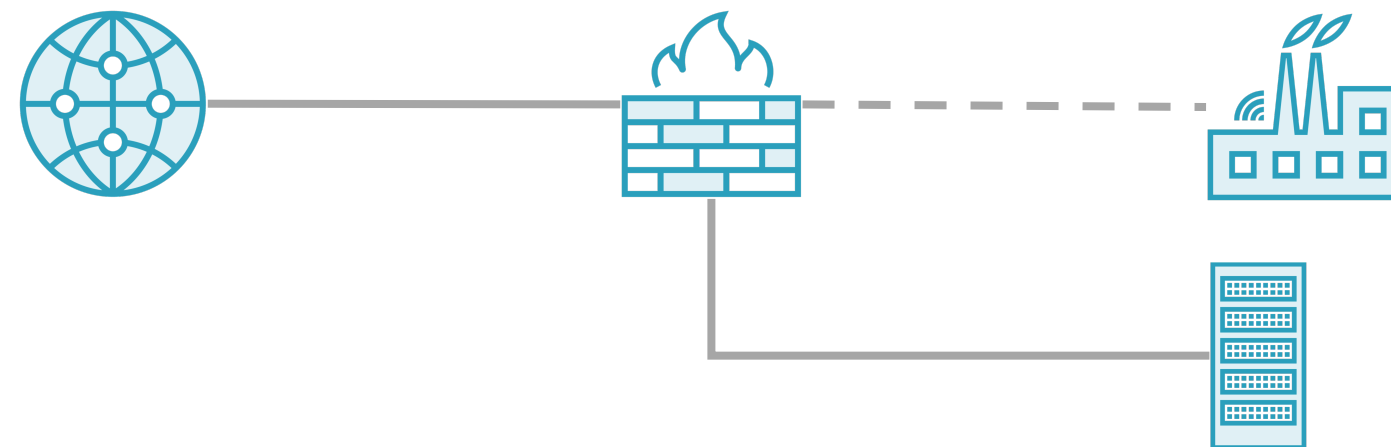


Gaining Initial Access

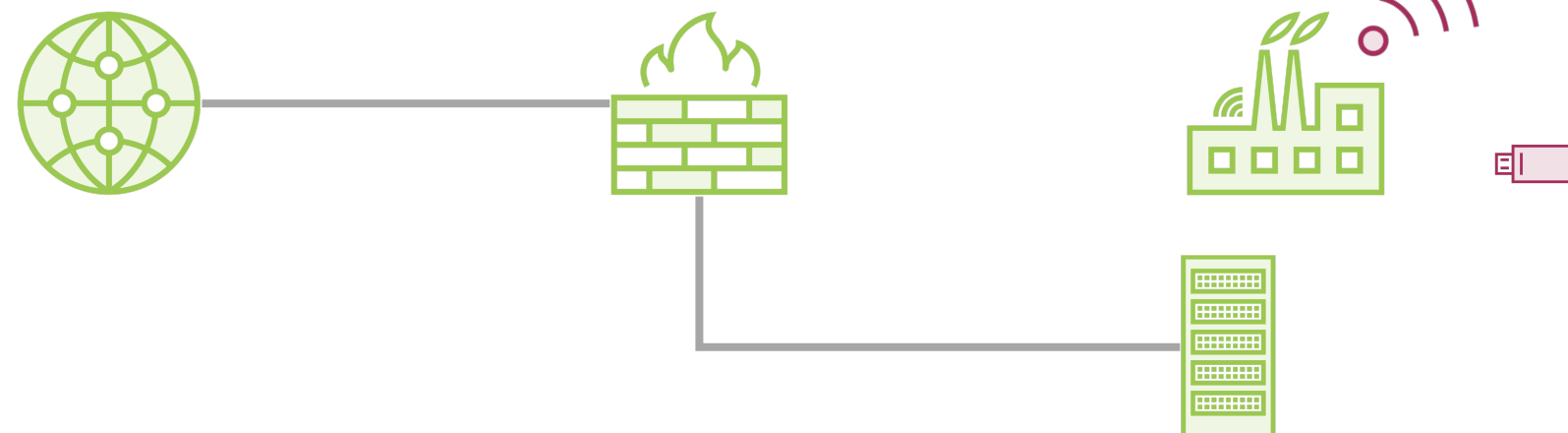
Direct access



Screened subnet



Air gap



Gaining Initial Access



Drive-by compromise



Transient cyber assets



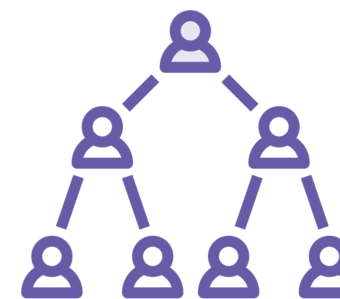
Public-facing application



Wireless compromise



Remote services



Supply chain





Attacks and Exploits

Network and Application Attacks for
CompTIA PenTest+

Matt Lloyd Davies





System Hacking

CEH Ethical Hacking Path

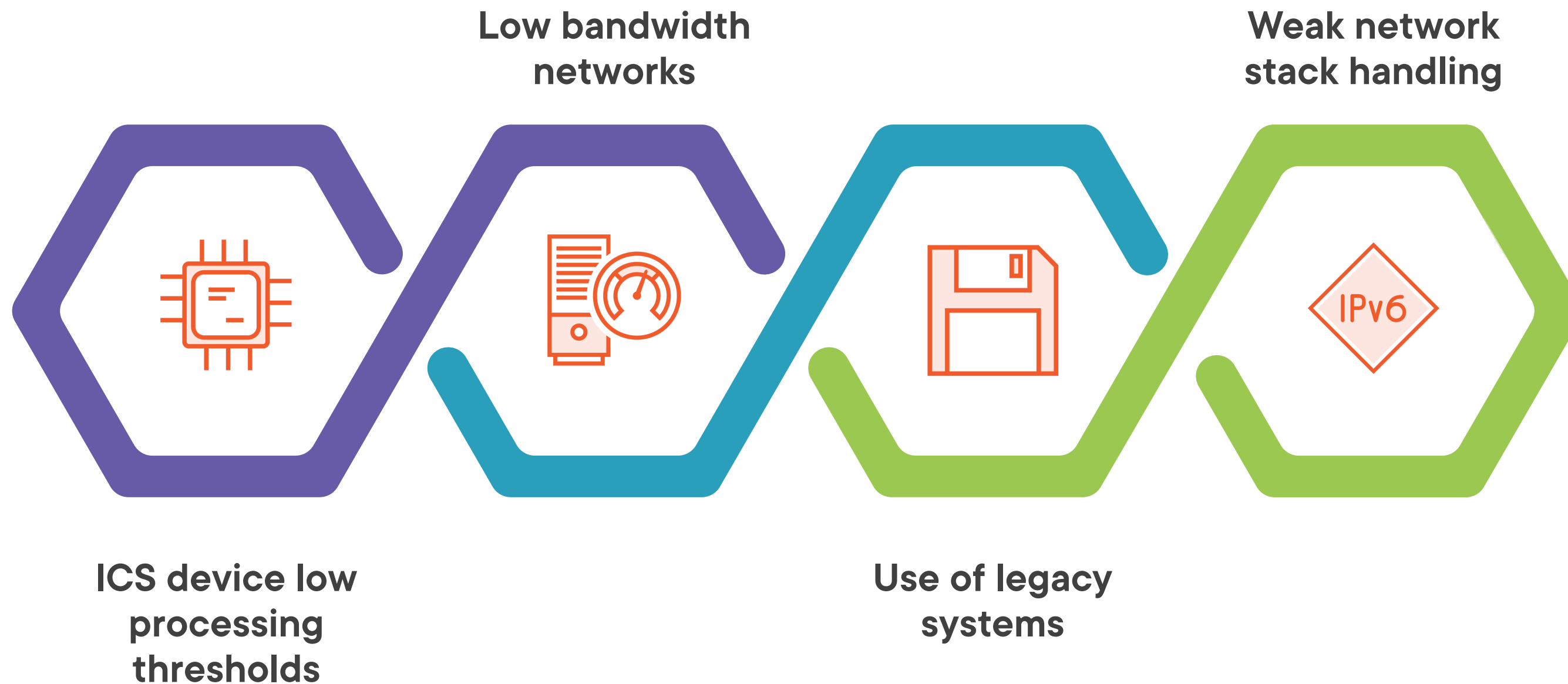
Dale Meredith



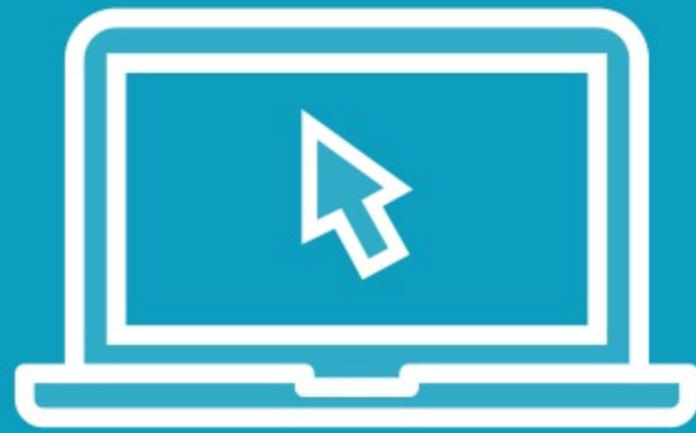
Internal Reconnaissance



Special Considerations for ICS



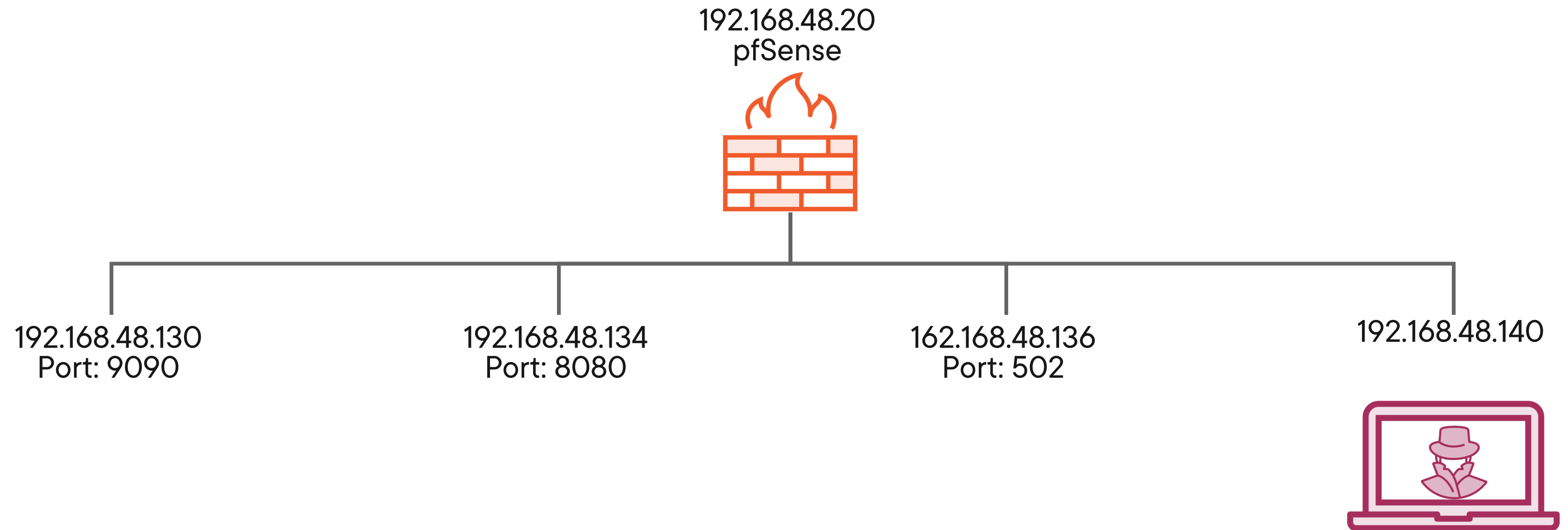
Demo



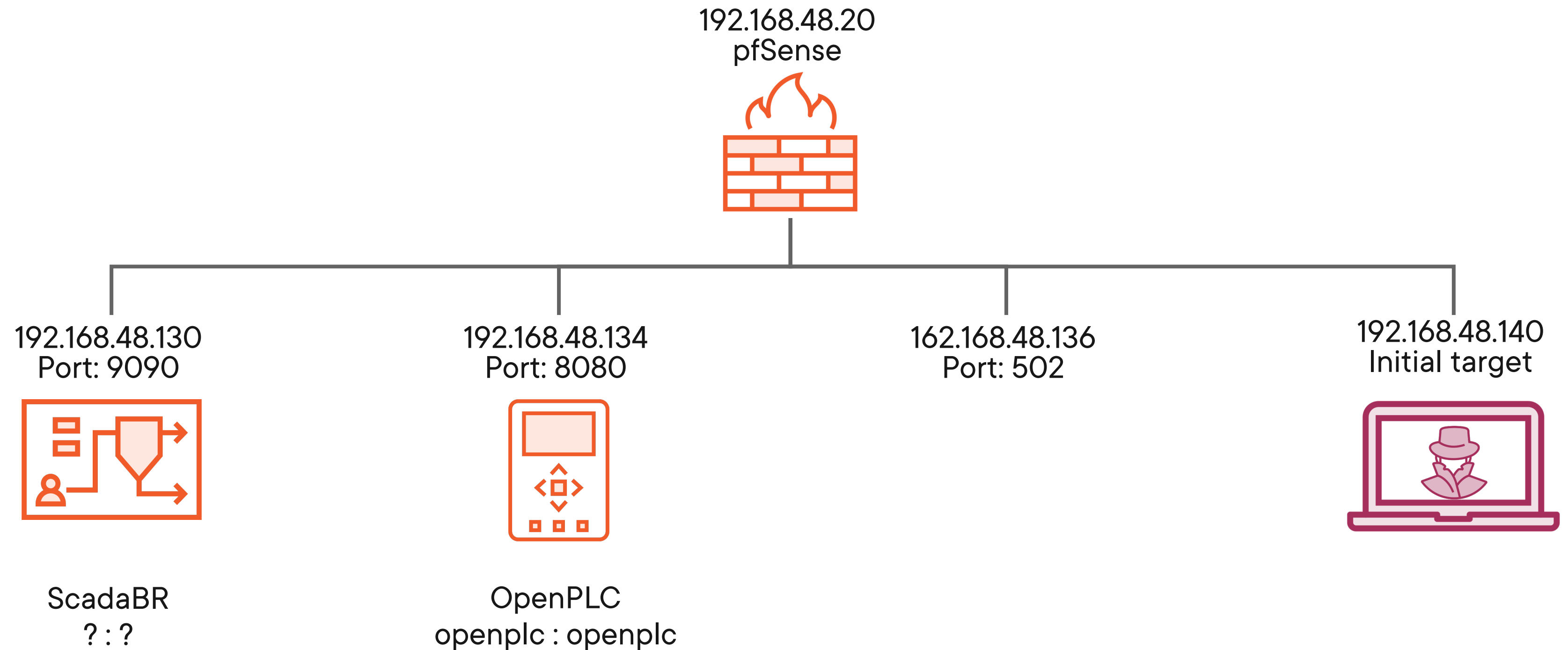
Internal Reconnaissance: Discovering ICS Devices



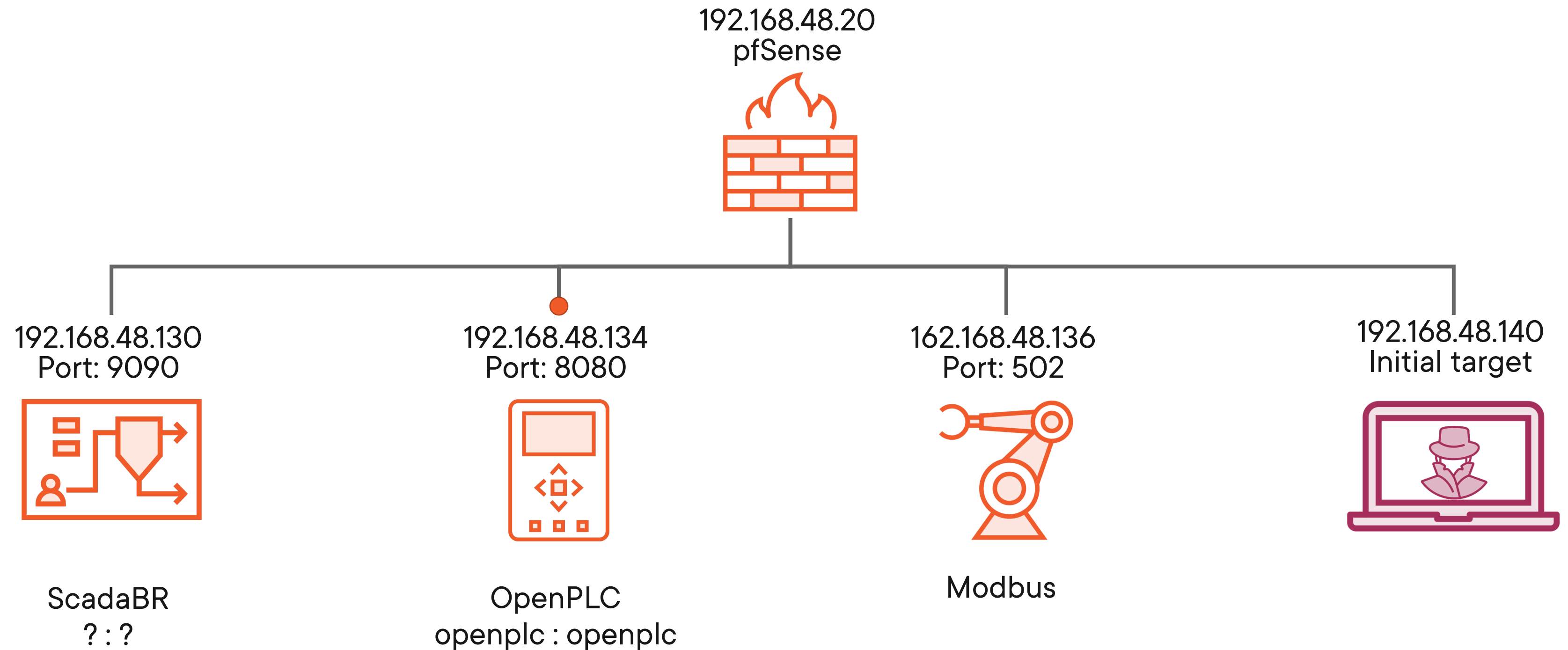
Internal Reconnaissance



Internal Reconnaissance



Internal Reconnaissance



Resources



Additional Resources



Mitre ATT&CK ICS

collaborate.mitre.org/attackics



SANS Information Security White Papers

sans.org/white-papers



Dragos

dragos.com/resources



Pluralsight

pluralsight.com

