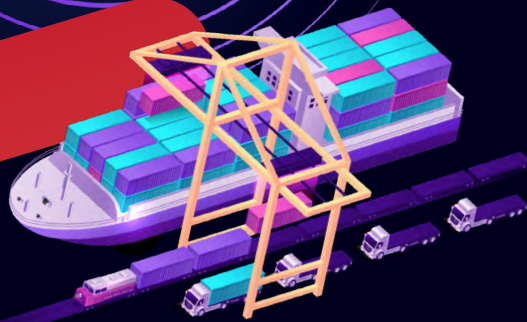




HACK THE PORT



MARITIME
& CONTROL SYSTEMS
CYBERSECURITY CON

Hack The Port Introduction



Hack The Port 2022 is a competition sponsored by [U.S. Cyber Command](#), [the NSA](#), and [the Maryland Innovation & Security Institute \(MISI\)](#), that simulated a real-world attempt to compromise the security of a functional maritime port in the United States. The competition took place in Florida during March, 2022.

The competition organizers invited “red teams” to try to Hack The Port, that is, to seriously compromise the security of the technological infrastructure of the port, and “blue teams” to act as defenders. The competition included six scenarios, encompassing all aspects and possible risks of a real-world industrial port.

The red teams were allowed to use any means that real-world threat actors would employ in their attempt to breach the networks, including phishing, metasploit, DDOS attacks and others.

This whitepaper will outline the findings and the results of the exercise, and it details the success of [SCADAFence](#) in successfully defending the port against the attacks.

The Attack Scenarios



The Gantry Crane

An industrial port's gantry crane is a large overhead crane that sits astride the port and is used for loading and unloading containers on ships, and for installing engines and other heavy equipment used in ship building and repair. The cranes are controlled and operated via a computer with specialized software. This attack scenario invited red team participants to attempt a breach of the crane's control system and gain enough access to allow them to disrupt the crane's movement and to lower a ship's engine directly into the ocean.



The Water Filtration System

The water filtration system at a major port is responsible for providing clean water to shipboard personnel, and the entire port. The goal of this challenge was to sabotage the water filtration system by accessing the devices that control the machinery, and trick it into adding an incorrect ratio of additives into the water. A key part of this challenge was to prevent the system's detectors from discovering the changes.



The Ship Board Network

This scenario challenged red teams to access the bridge control systems of the actual vessels as they attempted to dock at the port and shut down the ship's propellers, thereby halting the ship and in effect, causing gridlock at the port.



The Ballast Control

This challenge also required accessing a ship's bridge control systems. In this scenario, red teams attempted to gain access to the ship's ballast control system and cause the HMIs to incorrectly indicate that the system is pumping water even though it is not.



The Surveillance System

Like any major industrial facility, Hack The Port's organizers included a surveillance system in their port, consisting of cameras which record digital footage to be saved for later review when needed. Red teams were challenged to shut down this network and to make sure no data was preserved that might implicate the threat actors later.



The Access Control System

Secure ID cards issued to each worker at a port is a critical aspect of maritime security. Ensuring that each person has the exact level of access to restricted areas helps keep the area secure. This challenge required red teams to gain access to the gate control systems and to card readers, and to allow unauthorized entry into the port.

The Red-Teams' Attacks - Detected by SCADAfence

Scanning the Network

As expected, the red teams began each scenario with reconnaissance of the network.¹ This begins with a scan to gather information in order to obtain the following: An inventory of devices attached to the network, services that run on those devices, device types, IP addresses, open ports, the manufacturer names, and what OS software the devices were running. They then used this information to correlate those devices with known vulnerabilities, and continued looking for anything else they could find, in order to gain further network access.

The screenshot displays the SCADAfence Assets Manager interface for host 10.89.0.32. The host is identified as 'kali' and is categorized as a 'Network Scanner'. The interface shows various details such as 'Tech.', 'OS', 'Hostname', 'First seen', 'Last seen', and 'NIC Type'. Below the details, there is a section for 'Open Alerts' with a table of alerts. The alerts table has columns for ID, Severity, Description, Status, Details, MITRE ATT&K, and Last Event Time. Several alerts are circled in red, including 'Network Scanner tool detected', 'Network Scanner was detected', 'Admin Weak authentication', 'Anomalous network behaviour - not acc...', and 'User \borris.cassidy on 10.89.0.32 (kali) connected to 10.88.5.29 (low-hm) using ...'. The 'Additional Details' section shows 'Topics' and 'Organization Details'.

ID	Severity	Description	Status	Details	MITRE ATT&K	Last Event Time
2673	Critical	Network Scanner tool detected	Created	A scanning tool detected from 10.89.0.32 (kali).	Discovery > Network C...	03/22/2022 16:10:11
265	Warning	Network Scanner was detected	Created	Asset 10.89.0.32 (kali) was identified as a network scanner, sending requests to to...	Discovery > Network C...	03/22/2022 13:35:25
311	Warning	Admin Weak authentication	Created	Admin user Administrator on 10.89.0.32 (kali) connected to 10.88.5.22 using HTTP...		03/22/2022 16:25:00
264	Warning	Anomalous network behaviour - not acc...	Created	Host 10.89.0.32 (kali) tried to connect to 2670 ports that did not communicate back	Command And Control ...	03/22/2022 13:35:25
3705	Warning	User Weak authentication	Created	User \borris.cassidy on 10.89.0.32 (kali) connected to 10.88.5.29 (low-hm) using ...		03/22/2022 16:10:33

Host view 10.89.0.32 scanning the network

¹ Reconnaissance is the first step of the kill-chain:

- <https://collaborate.mitre.org/attackics/index.php/Discovery>

- <https://attack.mitre.org/tactics/TA0043/>

- <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

Metasploit Certificate Usage

During a routine scan, one of the first things the SCADAfence Platform detected was a self-signed Metasploit certificate. A certificate signed by the Metasploit Framework, instead of a certificate signed by a trusted company such as DigiCert or GoDaddy. This indicates unauthorized or malicious activity being sent through the network. Specifically, it was issued by a router with an IP address of [c][d] 10.88.0.252 (NAT).

Alerts Manager > Metasploit TLS Certificate usage detected

Metasploit TLS Certificate usage detected In Progress Resolve Download PCAP

20.228.221.179 (vmware-locks1.internal.portcosmar.biz) communicated with 10.88.0.252 (ip-10-88-0-252.ec2.internal) and used a Metasploit TLS Certificate
ID: 4285 Severity: Threat Created: 03/23/2022 23:04:39

Explanation
We have detected the use of a TLS Metasploit Certificate which is often used by Metasploit to...

Resolution recommendations
Check if source host is allowed to use Metasploit

Time	Source	Destination	Protocol	Length	Info
1 0.000000	20.228.221.179	10.88.0.252	TLSv1.2	3067	Server Hello, Certificate, Server Key Exchange, Server I

Frame 1: 3067 bytes on wire (24536 bits) captured on interface eth0
Ethernet II, Src: Cisco_59:41:25 (a8:00:05:59:41:25), Dst: 08:00:27:00:00:00 (08:00:27:00:00:00)
Internet Protocol Version 4, Src: 20.228.221.179, Dst: 10.88.0.252
Transmission Control Protocol, Src Port: 443, Dst Port: 443
Transport Layer Security

Wireshark · Follow TCP Stream (tcp.stream eq 0) · SF_SIGNATURE_ENGINE_ALERT_623a39e79a4ad89e229aeab1.pcap

```
...P...L...00.U...3.FS.....  
.N1..i.}*H5y..0..$......#...... .http/1.1.....  
1..  
..*...0...0..h.....x...0  
..*..H..  
...0]1.0 ..U...US1.0 ..U...TX1.0  
..U...Austin1.0  
..U..  
..Rapid71.0...U...MetasploitSelfSignedCA0..  
220220042600Z..  
320319042600Z0W1.0 ..U...US1.0 ..U...TX1.0  
..U...Austin1.0  
..U..
```

Detecting a Metasploit Certificate Usage. Every alert includes the PCAP file to help further investigate the issue.

Attempted Attack Via RDP (Remote Desktop Protocol)

The SCADAfence Platform detected that attackers tried over 4,700 times to establish a connection with the FLOW-HMI machine. They were eventually able to create a successful RDP session.

Link Inspector for 10.88.0.108 and 10.88.5.29

C...	Tr...	Dest. Port	Direction	Total	A to B Bytes	B to A Bytes	A to B Pack...	B to A Pack...	First seen	Last Seen
735	TCP	80 (HTTP)	→	128.02 MB	44.63 MB	83.39 MB	257.69K	159.95K	03/23/2022 14:38:19	03/23/2022 16:30:34
4748	TCP	3389 (RDP)	→	50.34 MB	28.21 MB	22.13 MB	155.56K	99.22K	03/23/2022 14:01:06	03/23/2022 15:46:57
41251	TCP	generic (dynamic)	→	36.4 MB	36.4 MB	954 B	551.53K	15	03/23/2022 15:00:22	03/23/2022 15:54:01
70	TCP	445 (Microsoft-DS)	→	65.16 KB	49.34 KB	15.82 KB	636	231	03/23/2022 15:00:21	03/23/2022 15:46:57
17	TCP	443 (HTTPS)	→	16.83 KB	16.83 KB	0 B	255		03/23/2022 14:54:54	03/23/2022 15:46:59

1 - 5 of 2155 items

Open Alerts

ID	Severity...	Description	Status	Details	MITRE ATTACK	Last Event Time
14029	●	Network Scanner tool detected	In Progress	A scanning tool detected from 10.88.0.108 (desktop-dimmy)	Discovery > Network C...	03/23/2022 14:57:22

An alert showing a successful RDP connection to the FLOW-HMI

Several other successful RDP sessions on 10.88.5.29 from known malicious actors (10.88.0.252, 10.88.0.106) that happened on the same day, were not preceded by targeted scans or brute force login attempts, and were therefore not reported.

Link Inspector For 10.88.0.252 and 10.88.5.29

First seen: 03/22/2022 15:23:49 Last Seen: 03/22/2022 21:58:25

10.88.0.252 (ip-10-88-0-252.ec2.internal) 10.88.5.29 (flow-hr)

C...	Tr...	De...	Direction	Total	A t...	B t...	A t...	B t...	First seen	Last Seen
72	TCP	3389 (RDP)	→	108.58 MB	3.28 MB	105.31 MB	28.86K	86.64K	03/22/2022 21:46:12	03/22/2022 21:57:20
2217	TCP	5357 (WSDAP)	→	10.97 MB	5.18 MB	5.79 MB	54.66K	32.8K	03/22/2022 21:46:15	03/22/2022 21:52:38
2701	TCP	generic (DCE-)	→	1.81 MB	1.8 MB	3.96 KB	28.16K	25	03/22/2022 16:00:00	03/22/2022 21:46:26
163	TCP	80 (HTTP)	→	1.01 MB	459.68 KB	546.72 KB	4.07K	3.22K	03/22/2022 20:51:28	03/22/2022 21:58:15
49	TCP	445 (Microsof)	→	75.93 KB	58.02 KB	17.91 KB	745	260	03/22/2022 16:00:15	03/22/2022 21:52:38

1 - 5 of 11 items

Link inspector showing a successful RDP connection to the FLOW-HMI

Successful PLC Scan Using Allen-Bradley ENIP

In another attempted attack, [The SCADAfence Platform](#), caught red team attackers attempting to use Allen-Bradley's ENIP protocol to retrieve details from a PLC. The SCADAfence Platform was able to detect that the attackers successfully acquired details such as the identity of a device, the model name, the session details and additional information from the PLC.

4 10.88.0.22 → 10.89.0.32

# Conn.	Command description
99	List Identity (Response:Success)
90	Register Session (Response:Success)
84	List Services (Response:Success)
12	List Interfaces

^ CVEs

CVE ID	Published ↓	Score	Status	Vendor	Total Assets	Description	In...
CVE-2017-7924	09/20/2017 19:29:00	7.5	Created	rockwellautomation	1	An Improper Input Validation issue was discovered in Rockwell Automation MicroLogix 1100 cont	
CVE-2017-7901	06/30/2017 06:29:00	8.6	Created	rockwellautomation	1	A Predictable Value Range from Previous Values issue was discovered in Rockwell Automation All	
CVE-2017-7898	06/30/2017 06:29:00	9.8	Reviewed	rockwellautomation	1	An Improper Restriction of Excessive Authentication Attempts issue was discovered in Rockwell /	
CVE-2017-7903	06/30/2017 06:29:00	9.8	Created	rockwellautomation	1	A Weak Password Requirements issue was discovered in Rockwell Automation Allen-Bradley Micr	
CVE-2017-7902	06/30/2017 06:29:00	9.8	Created	rockwellautomation	1	A "Reusing a Nonce, Key Pair in Encryption" issue was discovered in Rockwell Automation Allen-B	

Starting and Stopping a PLC

One of the most significant attacks the SCADAfence Platform was able to detect was an actual start/stop commands sent to a PLC. After gaining access to the PLC, the threat actors maintained their attack on the compromised device sending commands to change the device's operating mode.

Had this been a real-world attack, the threat actors could have used PLC start/stop commands to launch attacks with potentially lethal consequences.

Alerts Manager > **PLC start command issued**

- **PLC start command issued**

10.88.6.12 (siemens-engineer) sent a PLC start command to PLC on 10.88.6.10, using s7comm_plus protocol.
ID: 14375 Severity: **Threat** | Last Event Time: 03/23/2022 21:09:43 | Total Events: 2
MITRE ATT&CK: Execution > Change Operating Mode, Evasion > Change Operating Mode, ...

Alerts Manager > **PLC stop command issued**

- **PLC stop command issued**

10.88.6.12 (siemens-engineer) sent a PLC stop command to PLC on 10.88.6.10, using s7comm_plus protocol.
ID: 14374 Severity: **Threat** | Last Event Time: 03/23/2022 21:08:38 | Total Events: 2
MITRE ATT&CK: Execution > Change Operating Mode, Evasion > Change Operating Mode, ...

Engineering station 10.88.6.12 sent a PLC stop & start commands to PLC 10.88.6.10



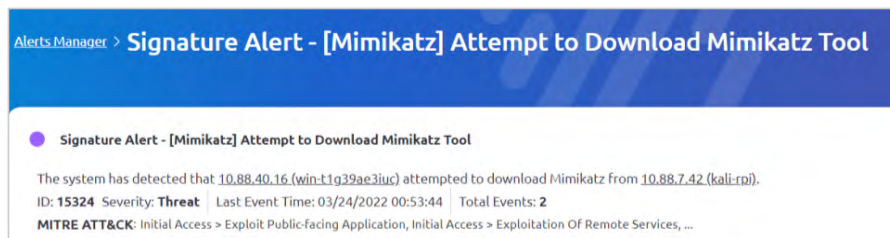
Downloading Mimikatz on a Compromised Domain Controller

One important way threat actors launch significant attacks is by first gaining a foothold in a network, then using that entry point to penetrate further into the network where they can work undetected. The SCADAfence Platform detected one of the most significant attacks of the Hack the Port event using this technique.

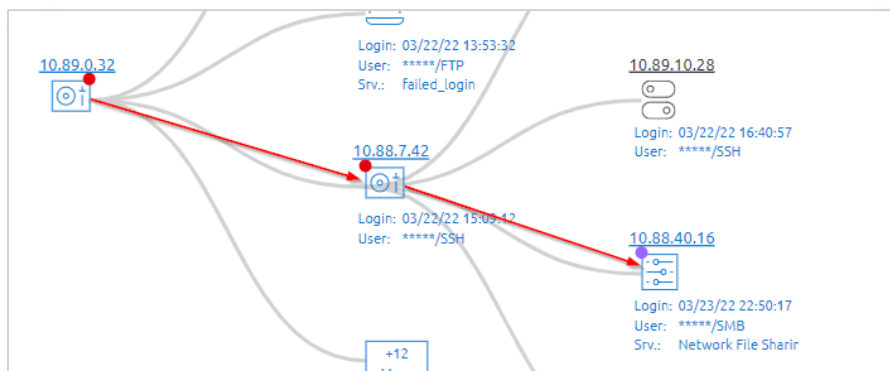
The Red Team attackers initial breach was a successful brute-force attack which they used as a launching point, and then, using compromised SSH access they continued through an intermediary device to then access a domain controller.

From that point, the attackers attempted to download Mimikatz onto a compromised domain controller in order to steal passwords (hashes) and other sensitive information. The SCADAfence Platform was able to detect the download.

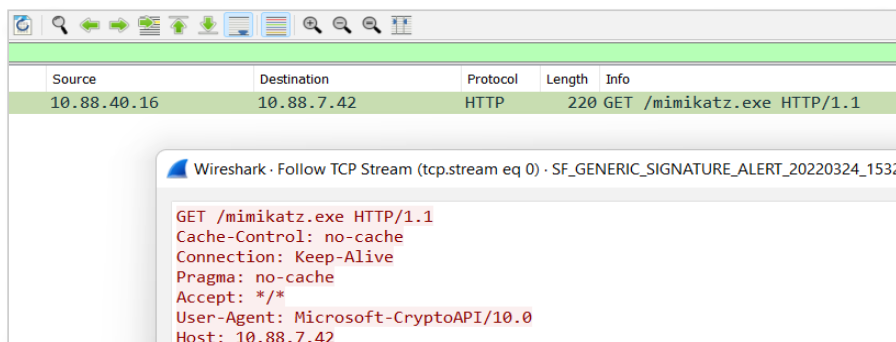
In a real world scenario the attackers would have been able to use the information they gathered to compromise other devices on the network.



Detecting the attempt to download the Mimikatz tool



Mapping the attacker's path to the domain controller



Attached Pcap showing http download of Mimikatz executable

Connecting to the TIA Portal

Among the most important devices that control the workings of an industrial port, (or any other computer controlled manufacturing or production environment) are the HMI's and operator / engineering stations.

Gaining access to these and the PLCs by which they are controlled, is among the top prizes for a threat actor. During the Hack the Port event, the SCADAfence Platform detected an external connection to port 8888. Port 8888 is used for the integrated configuration web application of Siemens TIA Administrator (TIA Portal).

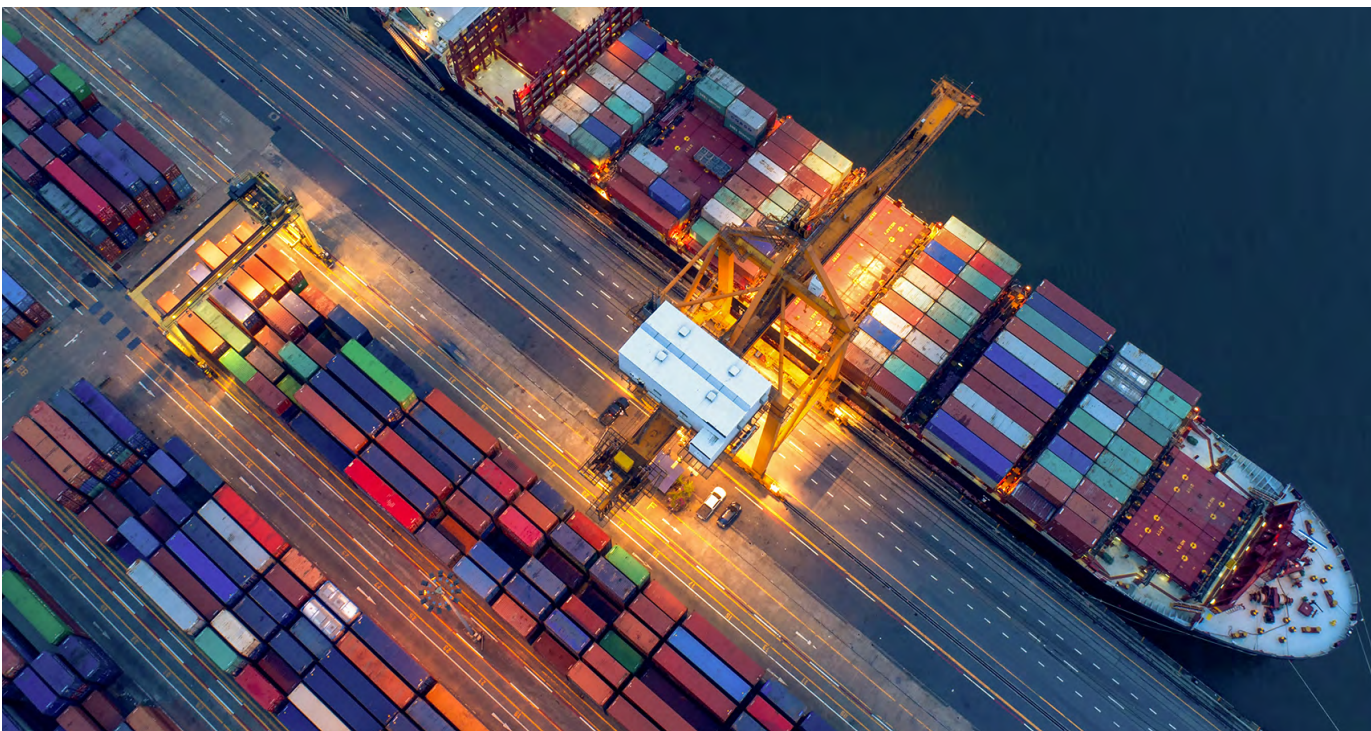
This indicated that the threat actors were attempting to gain access to the PLC. Again, the two-way communication detected by the Platform, indicated that they had successfully established this connection and the PLC was compromised.

In a real-world breach of this nature, threat actors could use this access to reprogram the PLC and to have full control of the PLC.

Link Inspector for 10.88.0.108 and 10.88.5.29

Conve...	Trans...	Dest. Port	Direction	Total ↓	A to B Bytes	B to A Bytes	A to B Packets	B to A Packets	First seen
1314	TCP	3389 (RDP)	→	4.89 GB	334.05 MB	4.56 GB	2.84M	4.37M	03/23/2022 18:18:16
4973	TCP	8888 (DDI-TCP-1)	→	1.43 GB	206.33 MB	1.22 GB	993.92K	1.13M	03/22/2022 13:51:25

A connection is established to TCP port 8888, which is one of TIA Portal ports, advised by Siemens to be restricted for local user access

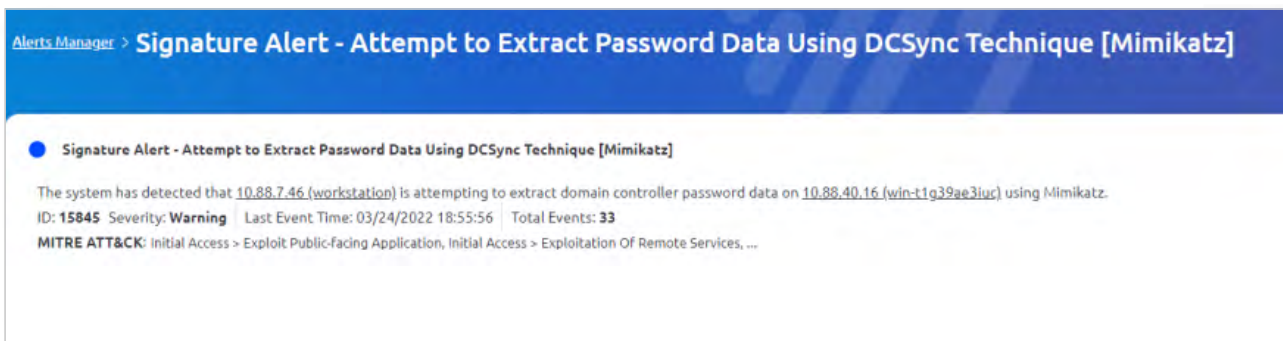


DCSync Attack

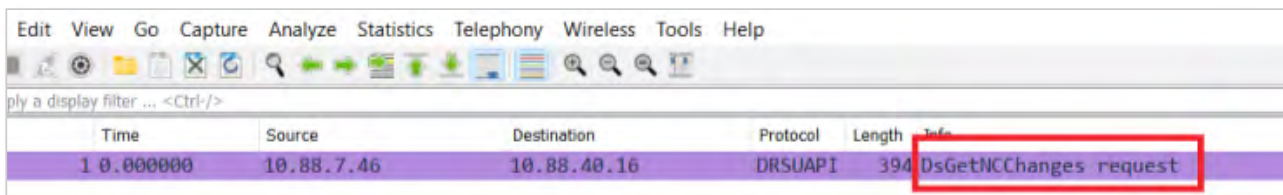
Hack the Port included a number of Raspberry PI devices with notable vulnerabilities. Most red teams were able to gain a foothold into the Raspberry PI network and use it as a jump point to gain deeper access into the network, by using one or more intermediary devices.

In this case, the Raspberry PI network was compromised in order to launch a DCSync attack against a domain controller.

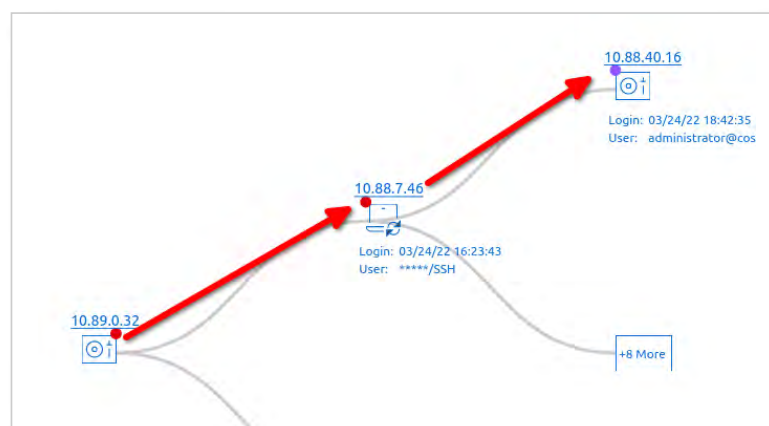
The attacker first compromised the Raspberry PI and used that as a jump point to access an HMI via SSH, before finally attacking the domain controller. The attackers used their control to extract information from the domain controller using the SMB protocol.



An alert showing the DCSync attack



The attached PCAP shows the DCSync attack



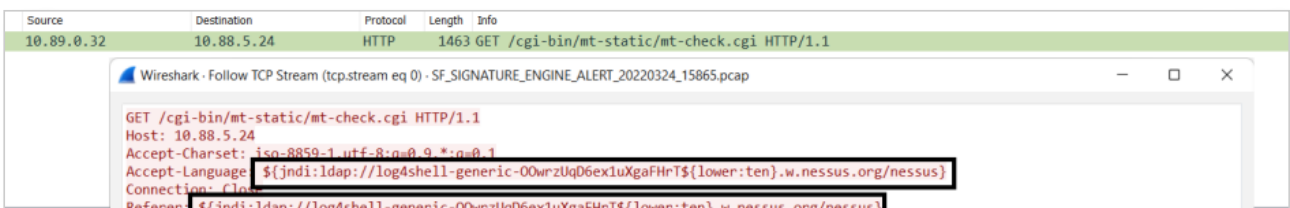
The attacker's path to the domain controller

Log4J Strikes Back

A major vulnerability was identified in open source logging library Apache Log4J at the end of 2021. [SCADAfence added support for the Log4J vulnerability immediately after the attack was discovered](#). At Hack The Port, the red team used this known vulnerability to stage an attack, hoping that it wouldn't be discovered. The target of this attack was an IO-link ENIP adapter, AL1970. The SCADAfence Platform immediately detected the attempt to use the Log4J vulnerability in order to execute code remotely on the device.



An alert showing the Log4J attack



The attached PCAP showing IP 192.168.0.32 is attacking 10.88.5.24 using the Log4j/Log4Shell vulnerability



Value Analysis Changes from A Compromised Domain Controller

One of the most vital features of the SCADAfence Platform, the [value Level feature](#), goes beyond basic OT command level detection, and retrieves actual OT variable values that were sent to the PLC.

During the Hack the Port event, the SCADAfence Platform detected value level changes that originated in a compromised domain controller. Unexpected changes in values indicate a breach, and in a real world scenario can indicate a major attack. In this case, the attacker changed the values in the PLC via the Modbus protocol, to a significantly higher value in order to disrupt both the PLC and connected machinery/sensors. The attacker's intent was to cause damage by having harmful additives dumped into the water supply.



The SCADAfence Platform Value detects changes on a PLC, done from a compromised domain controller via the Modbus protocol.

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostn...	Protocol
2	10.88.40.16	win-t1g39ae3iuc	10.88.40.10		Modbus/TCP
# Conn.	Command description				Last Seen
11	Request: Function 0x3: Read Holding Registers				03/24/2022 19:27:44
44	Request: Function 0x10: Write Multiple Registers				03/24/2022 19:28:27
1 - 2 of 2 items					
2	10.88.40.10		10.88.40.16	win-t1g39ae3iuc	Modbus/TCP
# Conn.	Command description				Last Seen
11	Response: Function 0x3: Read Holding Registers				03/24/2022 19:27:44
44	Response: Function 0x10: Write Multiple Registers				03/24/2022 19:28:27

An alert showing the value level changes on the PLC

Detecting All New Red Team Scenarios

As one of the red teams completed working on the attack scenario, another red team took it in turn. The SCADAfence Platform was able to detect the change due to new IP addresses being added to the network. The same IP address being used by a new device potentially indicated that a device that was using the IP has left the scene and a new device entered, taking the same IP and thus triggering a corresponding event.

Alerts Manager > IP address is used by another device

IP address is used by another device In Progress Resolve

IP address [10.88.0.242 \(develwin\)](#) that was used by an asset with MAC address 76:C8:5F:97:00:8E is now used by another device with MAC address 96:89:80:13:47:81
ID: **15885** Severity: **Information** Created: 03/24/2022 19:35:49

Explanation	Resolution recommendations
Change of IP-MAC bond can occur as a natural process in a network with dynamic IP address allocation (DHCP)	<ol style="list-style-type: none">1. Ensure that dynamic IP allocation is allowed by existing network policy2. Limit unauthorized access into your IT and OT system3. Make sure the administrative access to DHCP should be restricted to a limited number of individuals

Scenario changes were detected via IP/MAC correlation



Conclusion: The SCADAfence Platform Demonstrates Its Superiority



The SCADAfence Platform succeeded in detecting the widest variety of attempted red team attacks against the fictional port. From untrusted x.509 certificates and DCSync attacks to unauthorized PLC start/stop commands and others, the SCADAfence Platform generated alerts to breaches on their network, without a large number of distracting false positives.

” *the SCADAfence blue team provided the most comprehensive reporting details for the entire blue team channel, with the fewest false positives.*

the.storyteller 03/29/2022

first of all please make sure your whole team knows you provided the most comprehensive reporting details for the entire BLUE team channel

The SCADAfence team is congratulated by the Hack The Port event organizers

In real world scenarios, the SCADAfence Platform's ability to detect cyber security breaches and generate accurate alerts would have protected the port from experiencing a major security incident, as it does today with many industrial ports around the world.

This [case study](#) is a perfect example.





HACK THE PORT

About SCADAFence

SCADAFence is the global technology leader in OT cyber security. The solution enables organizations with large-scale OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and user experience. The SCADAFence solution seamlessly integrates OT security within existing security operations, bridging the IT/OT convergence gap. SCADAFence delivers security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAFence enables organizations in manufacturing, building management and in critical infrastructure industries to operate securely, reliably and efficiently as they go through the digital transformation journey. To learn more go to www.scadafence.com

Our offices

Headquarters: Tel Aviv

Regional: New York, Munich, Tokyo

Contact us: info@scadafence.com

www.scadafence.com



SCADAFence