

612.5

Covfefe Down!



© 2022 Jeffrey Shearer, Jason Dely, Tim Conway, and Chris Robinson. All rights reserved to Jeffrey Shearer, Jason Dely, Tim Conway, and Chris Robinson and/or SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With this CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, USER AGREES TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, USER AGREES THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If User does not agree, User may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP® and PMBOK® are registered trademarks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

All reference links are operational in the browser-based delivery of the electronic workbook.

SANS

Covfefe Down!

Copyright 2022 Jeffrey Shearer, Jason Dely, Tim Conway, and Chris Robinson | All Rights Reserved | Version H01_02

This page intentionally left blank.

Covfefe Down!

The plant is currently
shutdown. Do not touch
anything until after the
morning meeting!

This page intentionally left blank.

Background

- During a scheduled maintenance and upgrade of some equipment at the Houston plant, there was a major storm that came in. Many workers were trapped and had to remain in the plant for about a week.
- Food was scarce and alcohol was in abundant supply.
- Floods damaged some equipment.
- Power outages occurred on and off throughout two evenings.
- There has been an ongoing labor dispute at the site as well. In preparation for a potential strike, there has been contractor and staff augmentation cross training.

This page intentionally left blank.

Current Status

Prior to plant start up –

- Operators are reporting inconsistencies across many elements of the environment.
- The vendors and integrators involved in the upgrades and maintenance have left to return to their homes.
- Plant managers have requested individual pod status updates in 30 minutes

This page intentionally left blank.

Prep for the Meeting

- Take the next 30 minutes to troubleshoot issues
- When all local issues are resolved, validate your local operation
- Identify any odd behaviors within your environment and report them in the meeting

This page intentionally left blank.

Status Meeting

- Field personnel Pod updates
- Operator Status
- Next Steps

This page intentionally left blank.

Post Meeting

- Continue to plug away
- Grab available personnel resources to resolve remaining issues
- Return the plant to acceptable pre startup condition

- Covefe CEO statement: “We did not come all this way and do all of this work to NOT grind beans!!!!”

This page intentionally left blank.

Quick Start Guide

Important!

- Log in to the ranges.io portal at
- <https://www.ranges.io>
- Select “Sign up”
- Provide your name, email, and create a password
- Verify your email and then create your display name for the scoreboard
- Navigate to your “Events page” and wait for your instructor to give you an Event code for this class run
- When this opening presentation is complete, and everyone is ready your instructor will launch the event and you will have access to the challenges.

This page intentionally left blank.

Points

- Each question has a point value based on difficulty
- Answer correctly and you get points
- Wrong answers will cause you to lose points, and the penalties are unique to each question. In some cases, you may receive a free attempt and in other cases you will not (it will alert you with each challenge).
- How many points you are penalized for incorrect attempts varies by question, so pay attention to the information at the top of each challenge
- Do not brute force answers even if you lose no additional points; it is a violation of the Rules of Engagement

This page intentionally left blank.

Penalties

50pts

L1 Q1 DNS Record

BRIEFING

Government intel-sharing has led to the discovery of potential attacker activity against the network of Spader Technologies. The shared intel was a malicious IP address of 51.11.247.89. This IP address was observed in some of the Spader Technologies network data.

Based on the exported packet capture provided, what DNS name is tied to the IP address 51.11.247.89?

Evidence provided: spader-dns-traffic.zip

DOWNLOADS

Challenge Files

spader-dns-traffic.zip [Download](#)

SRL-ST-Grid-Diagram.pdf [Download](#)

Enter flag

[Try flag](#)

50pts

L1 Q4 Proxy download

0 Attempts made

⚠ Your first attempt is free, incorrect attempts 2-6 deduct 10 points from your current score

50pts

L1 Q4 Proxy download

Flag incorrect!

2 Attempts made

⚠ Your first attempt is free, incorrect attempts 2-6 deduct 10 points from your current score

This page intentionally left blank.

Scoreboard

- Top 10 individuals displayed on screen
- Stats
 - Score
 - Time since last score
 - Game Progress
 - Level Progress

LEADERBOARD							
POSITION	DISPLAY NAME	POINTS	PROGRESS	SUCCESS RATE	COMPLETED	ATTEMPTS	TIME SINCE LAST SCORED
1st	aln	1,110pts	<div><div style="width: 38%;">38%</div></div>	90%	9	10	05 : 21 : 32 : 35
2nd	Shi	210pts	<div><div style="width: 13%;">13%</div></div>	100%	3	3	00 : 19 : 16 : 28
3rd	fra	110pts	<div><div style="width: 8%;">8%</div></div>	67%	2	3	15 : 19 : 35 : 47
4th	You: tct	10pts	<div><div style="width: 4%;">4%</div></div>	100%	1	1	00 : 00 : 01 : 08
5th	T	0pts	<div><div style="width: 0%;">0%</div></div>	0%	0	0	-- : -- : -- : --

This page intentionally left blank.

Hints

- Take good notes!
- We have provided you with all the tools you need to solve the challenges
 - Pay attention to the answer format requirements for some questions!!!
 - Feel free to use your own tools
- Use the internet for research
- **Questions have hints available!**
 - Small penalties for hints vary by Level and impact how many points can be earned for a challenge
 - Tie-breaker at the end

This page intentionally left blank.

Hints - Examples

HINTS

Stuck? Reveal a hint.

Revealing a hint will cost you 1 points. You have 3 hints remaining.

50pts 49pts with hint penalty

L1 Q2 Who is talking

This page intentionally left blank.

Quick Start Guide

Important!

- Log in to the ranges.io portal at
- <https://www.ranges.io>
- Select “Sign up”
- Provide your name, email, and create a password
- Verify your email and then create your display name for the scoreboard
- Navigate to your “Events page” and wait for your instructor to give you an Event code for this class run
- When this opening presentation is complete, and everyone is ready your instructor will launch the event and you will have access to the challenges.

This page intentionally left blank.

Join Key

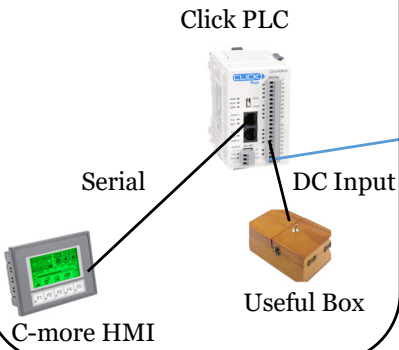
*Will be provided
by instructor*

This page intentionally left blank.

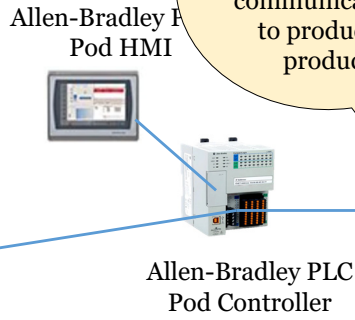
Covfefe Coffee Factory : Logical Overview (I)

Section 5 Goal:
Pod to Line
Controller
communications
to produce a
product

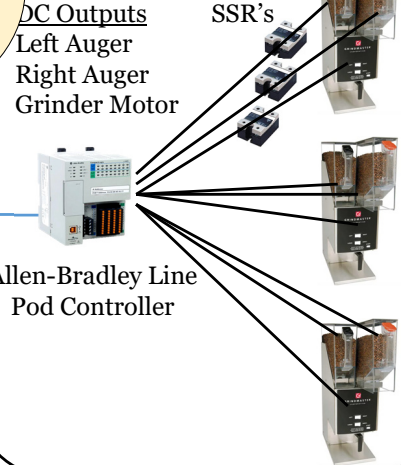
Student Kit



Train

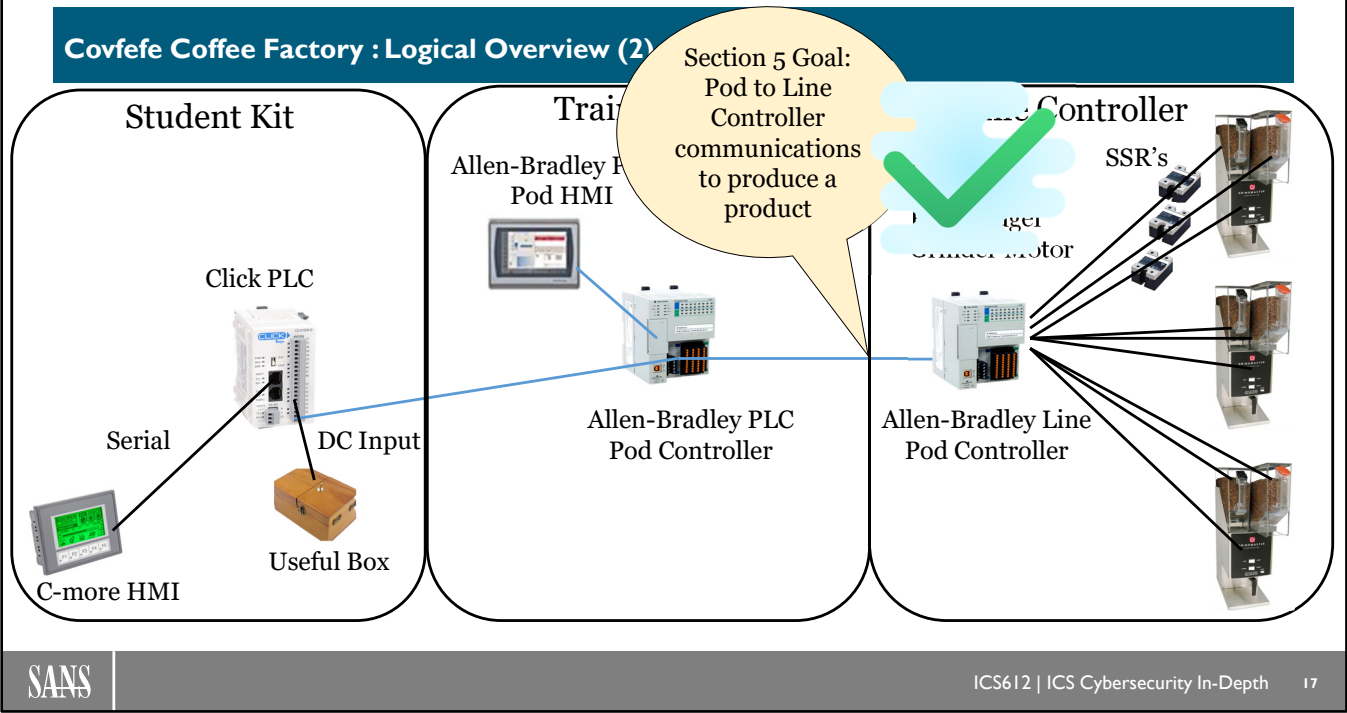


Line Controller



This page intentionally left blank.

Covfefe Coffee Factory : Logical Overview (2)



This page intentionally left blank.

Section 5: Eval Link

This page intentionally left blank.



This page intentionally left blank.

COURSE RESOURCES AND CONTACT INFORMATION

AUTHOR CONTACT



Jason Dely
jdely@sans.org

Jeff Shearer
jshearer@sans.org

Tim Conway
tconway@sans.org

Chris Robinson
crobinson.sd@gmail.com



SANS INSTITUTE

11200 Rockville Pike
Suite 200
North Bethesda, MD 20852
301.654.SANS(7267)



ICS RESOURCES

<https://ics.sans.org>
<https://ics-community.sans.org/>
Twitter: @sansics



SANS EMAIL

GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

This page intentionally left blank.

Station and Network Information

RAW Stations

Pod 1
Pod 2
Pod 3
Pod 13

Mixing Stations

Pod 4
Pod 5
Pod 6
Pod 14


Grind Stations

Pod 7
Pod 8
Pod 9
Pod 15

Packing Stations

Pod 10
Pod 11
Pod 12

Server Information

 172.20.3.(Pod# + Student#) – Operator Workstation
172.20.1.21 – OPC UA Server
172.20.1.10 – DNS Server
172.30.1.(Pod# + Student#) – RDG Server

172.20.1.20 – LICSRV
172.20.1.21 – DATASRV
172.20.1.22 – HMISRV
172.20.1.23 – HISTSRV

172.30.2.(Pod# + Student#) – File Share



Classroom Pod Information

172.16.(pod#).2 - AB PLC
172.16.(pod#).3 - PanelView
172.16.(pod#).4 - Remote I/O



Pod Firewall Information

172.16.(pod#).10 – Student 1 FW
172.16.(pod#).20 – Student 2 FW



Student Kit Information

172.16.(pod#).11 – S1 Windows VM
172.16.(pod#).12 – S1 Click Plus
172.16.(pod#).13 – S1 Kali VM
172.16.(pod#).14 – S1 RELICS VM
172.16.(pod#).21 – S2 Windows VM
172.16.(pod#).22 – S2 Click Plus
172.16.(pod#).23 – S2 Kali VM
172.16.(pod#).24 – S2 RELICS VM

Subnet & Gateway

172.16.(pod#).1 – Gateway
255.255.255.0 – Subnet Mask

This page intentionally left blank.

This page intentionally left blank.

Index

A

Access Control Entries (ACEs)	3:10
Access Control Lists (ACLs)	3:9-10, 3:12, 3:20-21
Active Directory (AD)	1:13-14, 2:8, 2:68, 4:19
Address Resolution Protocol (ARP)	2:105, 2:107-108, 2:119
Advanced Persistent Threat (APT)	2:89, 3:63
Adversarial Value	2:53, 2:113
Alarm Management	1:113, 1:117, 1:121, 4:26
Alarm System Design	1:121-122
Alarms and Conditions (AC)	2:21, 2:98
ANSI/ISA-88	1:10
ANSI/ISA-95	1:10-11
ANSI/ISA-99	1:10-11
Application-Specific Integrated Circuits (ASIC)	1:69
Area/Line Controller	2:16
ARP cache poisoning	2:108
ARP poison	2:108, 2:112
ARP spoofing	2:107-108, 2:119
Authentication, Authorization and Accounting (AAA)	2:78, 3:36, 3:45
Automatic Device Replacement (ADR)	4:68
AutoSol	2:20

B

BeyondTrust	3:48
Binary	1:100, 1:103-108, 1:110, 1:135, 1:137, 2:101

C

Cache Poisoning	2:108-109, 3:70
Certificate Authorities (CA)	3:51
CIMPLICITY	2:20
Citrix Desktop	3:48
Command and Control (C2)	2:68, 2:105, 3:70

Commercial Off-The-Shelf (COTS)	2:16-17, 2:26, 3:22, 3:30, 3:33, 3:35
Common Industrial Protocol (CIP)	1:2, 1:21-24, 1:97, 1:138, 1:142-144, 1:158, 1:161, 2:2, 2:9, 3:2, 3:51, 4:2
Communications Mapping	2:75
community string	3:69
Computer Integrated Manufacturing (CIM)	1:9
Conduits	2:48, 2:57-58, 2:66-67, 2:75, 4:12
Critical Assets	2:48-49, 2:55, 2:59, 4:46

D

Data Access (DA)	2:98
Data Concentrator	2:16, 2:21
Data Loss Prevention (DLP)	4:66
Data Relevance	2:76
Data Server	2:16-17, 2:19, 2:30, 2:34, 2:77, 3:20-21
Default Route	2:70, 2:72
DeltaV	2:12, 2:20-21
Demilitarized Zone (DMZ)	1:1, 1:12-13, 2:1, 2:7-8, 2:120, 3:1, 3:11-22, 3:24, 3:29, 3:33, 3:36, 3:42, 3:46, 3:49, 3:83, 4:1, 4:8, 4:13, 4:23, 4:56
Device-Level Authentication	3:50
Direct Loss	2:49, 2:51, 2:55, 2:59
Direct Relevance	2:76
Discrete	1:13, 1:28-29, 2:8, 2:11-13, 2:23-24, 2:29, 2:91
Distributed Component Object Model (DCOM)	2:96
Distributed Control System (DCS)	1:13, 1:42, 2:8, 2:13, 2:15, 2:19-22, 2:24, 2:29, 4:19, 4:44
DNS cache poisoning	2:109, 3:70
DNS spoofing	2:107, 2:109, 3:70
Domain Name System (DNS)	1:13, 1:168, 2:8, 2:24, 2:68, 2:72, 2:107, 2:109, 2:122, 3:70, 3:85, 4:78, 5:21
Dynamic Host Configuration Protocol (DHCP)	1:13, 2:8
Dynamic Naming Services (DNS)	1:13, 1:168, 2:8, 2:24, 2:68, 2:72, 2:107, 2:109, 2:122, 3:70, 3:85, 4:78, 5:21

E

Electronic Operator Interface (EOI)	1:111-112, 1:117, 1:123-124, 2:10
Engineered Trust Boundary	2:69
Enterprise Resource and Planning (ERP)	2:11, 2:13-14
Ettercap	2:106, 2:112, 2:115
evil twin	2:107, 2:110

F

FactoryTalk	1:25, 1:123, 2:20, 2:26
File Transfer Protocol (FTP)	3:67
Firewalls	1:1, 1:12, 2:1, 2:7, 2:58, 2:66, 2:96, 2:120, 3:1, 3:8-10, 3:12, 3:14-15, 3:20-22, 3:24-25, 3:33, 3:36, 3:38, 3:49, 3:53, 3:83, 4:1, 4:8, 4:19, 4:23, 4:38, 4:41-42, 4:45, 4:49, 4:66, 4:74
Forced Proxy	2:111
Function Block Diagram (FBD)	1:41-42, 1:69

H

Head End Process (HEP)	2:4-6, 2:15-16, 2:19-20, 2:24, 2:26-27, 2:30, 2:34, 2:40, 2:46-47, 2:73, 2:86, 2:121
Historian	1:12, 1:14, 1:55, 1:113, 2:8, 2:16-17, 2:19, 2:30, 3:4-5, 3:7, 3:16, 3:19, 3:27-28, 3:30-34, 3:39, 3:41-43, 3:46, 3:57, 3:65, 3:83, 4:46
Historian Server	2:16-17, 2:19, 2:30, 3:42
Historical Access (HA)	2:98
Human Asset	2:52
Human Machine Interface (HMI)	1:4-5, 1:12-16, 1:19, 1:21-25, 1:28, 1:36, 1:38-39, 1:55-61, 1:65-66, 1:97-98, 1:103, 1:111-118, 1:120, 1:122-125, 1:127, 1:130, 1:132-139, 1:141, 1:151, 1:157, 1:161, 1:165, 2:7-10, 2:17, 2:19, 2:26, 2:30, 2:37, 2:44, 2:77, 2:85, 2:95, 2:114-117, 2:120, 3:6-7, 3:15-18, 3:20-22, 3:26, 3:31-33, 3:35-37, 3:39-40, 3:46, 3:57, 4:6, 4:13, 4:34, 4:46, 4:50, 4:56-57, 4:59, 4:68, 5:16-17

Hybrid	2:11-12, 2:24-25, 2:29, 2:54, 2:56
HyperText Transfer Protocol (HTTP)	3:12, 3:67, 3:74
HyperText Transfer Protocol Secure (HTTPS)	2:101, 3:12, 3:67

I

ICS Data Point	2:26
Identity Service Engine (ISE)	3:36
IEC 61131-3	1:41, 1:148
Ignition	2:20
Indirect Loss	2:49, 2:51, 2:55, 2:59
Indirect Relevance	2:76
Industrial Demilitarized Zone (IDMZ)	1:1, 1:12, 2:1, 2:7, 2:37-38, 2:66, 2:120, 3:1, 3:15-19, 3:34, 3:36, 3:46, 3:49, 3:83, 4:1, 4:12, 4:56
Information System (IS)	2:12-13
Inline Proxy	2:111
Instruction list (IL)	1:41, 1:72-73
Integration Process	1:4-5, 1:35, 1:39, 1:98, 1:139, 3:28
Intercepting Proxy	2:111
Internet Control Message Protocol (ICMP)	3:68
Internet Protocol (IP)	1:21-24, 1:97, 1:138, 1:144-146, 1:154, 1:161, 2:9, 2:24, 2:68, 2:104, 2:108-109, 2:114-116, 3:68, 3:70, 4:35

J

Jump Host	3:16, 3:47-49, 3:55
-----------	---------------------

K

Kali Linux	2:112, 3:75
Kepware	1:151, 2:20, 2:26
Keyboard, Video, Mouse (KVM)	4:13

L

Laboratory Information Management Systems (LIMS)	2:17
Ladder Diagram (LD)	1:41-42, 1:69
Logging	2:63, 3:47, 4:4-5, 4:17-19, 4:22, 4:24-25, 4:28-29, 4:42, 4:51, 4:58, 4:74
Logical Asset	2:52

M

Man-in-the-Middle attack (MITM)	2:4-5, 2:47, 2:73, 2:86, 2:106-107, 2:113, 2:115
Management of Change (MoC)	4:40
Manufacturing Execution System (MES)	1:12, 2:7, 2:11-15, 2:20-21
Matrikon	2:20
Mean Time Between Failure (MTBF)	2:10, 2:60
Metasploit	3:74-75
Microsoft RDP Gateway	3:48
Mimikatz	3:76, 3:78
Mobile Device Management (MDM)	3:36

N

National Security Agency (NSA)	3:73
Network Security Monitoring (NSM)	2:77, 4:9, 4:12, 4:16, 4:36
Network Time Protocol (NTP)	1:13, 2:8, 2:72, 4:19, 4:28, 4:53-59, 4:61-62, 4:74
NIST CyberSecurity Framework (NIST CSF)	2:60, 3:58
Nmap	1:162, 2:77, 3:75, 4:39

O

Oasys	2:20
Object Linking and Embedding (OLE)	2:95
OLE for Process Control (OPC)	1:168, 2:4-5, 2:17, 2:47, 2:73, 2:86, 2:95-103, 2:122, 3:85, 4:19, 4:78, 5:21
Opcenter	2:20
Operational Technology (OT)	1:10-12, 1:42, 1:164, 2:15, 2:25, 2:27-28, 2:56, 2:61, 2:63, 2:89, 2:94, 2:105, 3:36,

	4:24-25, 4:49
Organizational Value	2:53
OSI Pi	2:20, 2:26
Overall Equipment Effectiveness (OEE)	2:17

P

PanelView (PV)	1:15-16, 1:21-24, 1:97, 1:111, 1:138, 1:141, 1:151, 1:153, 1:161, 1:168, 2:9, 2:85, 2:114-117, 2:122, 3:6-7, 3:26, 3:39-40, 3:57, 3:85, 4:6, 4:50, 4:78, 5:16-17, 5:21
Physical Asset	2:52
Pivoting	3:74
Port Forwarding	3:74
Precision Time Protocol (PTP)	4:57-59
Process and Instrumentation Diagram (P&ID)	1:36
Process Control Design	1:35
Process Controller	2:16, 2:21, 2:23
Process Flow Diagram (PFD)	1:36, 1:38
Programmable Automation Controller (PAC)	1:13, 1:55-61, 2:8, 2:21-22, 2:29, 2:91
Proportional, Integral, and Derivative (PID)	1:148
Protocol-Level Attack	2:94
Proxy	2:58, 2:105, 2:107, 2:111, 2:119, 3:11-14, 3:16-18, 3:74
Public Key Infrastructure (PKI)	3:51, 3:56
Purdue Model	1:9-12, 1:15-16, 1:166, 2:7, 2:15, 4:23

R

Redirection	3:74
Relay Logic	1:42, 1:47-53
Relevance	1:10, 2:21, 2:76
Remote Desktop Gateway (RDG)	1:168, 2:122, 3:46, 3:49, 3:55-56, 3:85, 4:78, 5:21
Remote Desktop Resource Authorization Policies (RD RAPs)	3:49
Remote Terminal Unit (RTU)	2:21
Rogue Access Point	2:107, 2:110

RSLinx	1:142-146, 1:153, 2:20, 2:26
--------	------------------------------

S

Samba	3:71
Secure File Transfer Protocol (SFTP)	3:67
Secure SHell (SSH)	3:47, 3:67, 3:74, 4:13
Security Exceptions	2:59, 2:64
Security Information and Event Management (SIEM)	4:13, 4:21, 4:25
Security Objectives	2:59-60, 2:63-64, 3:35
Security Operations Center (SOC)	4:13, 4:25
Security Zones	2:48, 2:57, 2:59, 3:15, 3:20-22, 3:25, 3:46, 4:12
Sequential Function Chart (SFC)	1:41, 1:43, 1:69
Server Message Block (SMB)	3:4-5, 3:27, 3:43, 3:65, 3:71-73, 3:77-78, 3:84
Shell	3:58-64
Simple Network Management Protocol (SNMP)	3:69
SOCKS Proxy	3:74
Spoofing	2:101, 2:107-109, 2:119, 3:70
Standard Operating Procedure (SOP)	4:38-39, 4:44-45
State Diagrams	1:85-87, 1:89
State Transition Tables	1:85-87, 1:89-93
Structured Text (ST)	1:41, 1:43-46, 1:69
Supervisory Control And Data Acquisition (SCADA)	1:2, 2:2, 2:10, 2:13, 2:15, 2:20-21, 2:42, 3:2, 3:37, 4:2, 4:19

T

Telnet	2:77, 3:67, 3:73, 4:35
Thermocouple	1:15-16, 1:21-24, 1:28-29, 1:97, 1:101-103, 1:110, 1:138, 1:161, 2:9, 2:29, 2:85, 3:6-7, 3:26, 3:57, 4:6, 4:50
Timer On (TON)	1:63, 1:131
Transparent Proxy	2:111, 2:119
Trust Boundaries	2:13, 2:48, 2:58-59, 2:65-66, 2:72, 4:12
Trust Boundary	2:13, 2:69, 3:19, 3:51
Tunneling	2:96, 3:70, 3:74

U

Unified Architecture (UA)	1:168, 2:97-102, 2:122, 3:85, 4:78, 5:21
USB-to-Serial	1:133-135, 1:137
User-Level Authentication	3:50

V

Virtual Private Network (VPN)	1:1, 2:1, 2:37, 3:1, 3:47, 3:52-53, 4:1, 4:41
Visualization Server	2:16-17
VMware Horizon	3:48

W

Windows Event Collector (WEC)	4:21
Windows Event Forwarding (WEF)	4:21
Windows Internet Naming Service (WINS)	1:13, 2:8
Windows Management Instrumentation (WMI)	4:21