PROCESS CONTROL SYSTEMS FORUM

EMERALD Monitoring and Situational Awareness in Process Control Networks

Alfonso Valdes, SRI International

March, 2007

www.thei3p.org

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

Collaborating to Advance Control System Security

Outline

- Threats
- Session Overview
- Review of vulnerability demonstration
- The EMERALD/PCS IDS appliance
- Monitoring and Situational awareness in the attack scenario

Note: Technology is only part of the picture, and does little without addressing "People and Process"

Threats to Process Control Systems

- Automation is ubiquitous in critical infrastructure
- Formerly proprietary standards, isolated networks (Security through obscurity and isolation)
- Increasingly, open standards (TCP/IP), common platforms, interconnected to business systems
- Of interest to hacktivists, terrorists

Vulnerabilities in Testbed Architecture

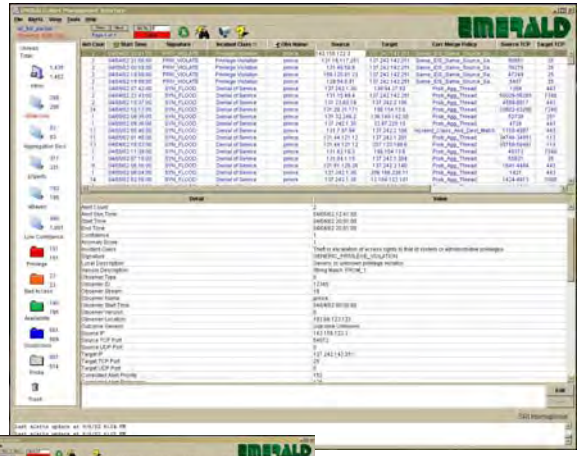
- Vulnerability scenario leverages common tactics and tools against a representative PCS/corporate networked system
- Imagine the scenario as having happened to another system, and consider similarities to your system
- We considered variations in topology and configuration
- Scenario progression depends on common problems identified during assessments and site visits

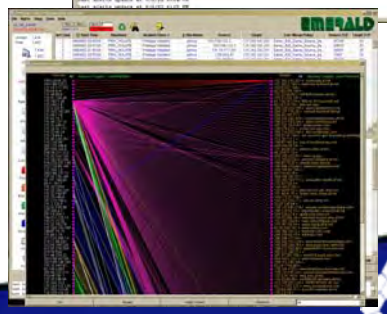
Integrated Monitoring and Correlation

- Barrier defenses (switches, firewalls, network segmentation) are essential, but
- Monitoring is essential to detect when these have been bypassed or penetrated
- One detection approach may not alert on a critical exploit
- Correlation of related events provides the operator coherent situational awareness

EMERALD IDS for PCS

- **Multi-algorithm IDS appliance**
  - Pattern Anomaly
  - Bayes analysis of TCP headers
  - Stateful protocol analysis (eXperts)
  - Complemented by custom SNORT ruleset
- **Alerts (potentially from multiple IDS appliances) forwarded to correlation framework**
- **PCS Enhancements**
  - Digital Bond PCS rule set
  - Model-Based Detection
  - MODBUS service discovery





Intrusion Detection Approaches

- **Signature: Match traffic to a known pattern of misuse**
  - Stateless: String matching, single packet
  - Stateful: Varying degrees of protocol and session reconstruction
  - Can be very specific and accurate
  - Typically does not generalize to new attacks
- **Anomaly: Alert when something "extremely unusual" is observed**
  - Learning based, sometimes statistical profiling
  - In practice, not used much because of false alarms
  - Learning systems are also subject to concept drift

Intrusion Detection Approaches (2)

- **Probabilistic (Statistical, Bayes): A middle ground, with probabilistically encoded models of misuse**
  - Some potential to generalize
- **Model based (some group this with anomaly detection): Alert when observed behavior is outside of a model or specification**
  - High potential for generalization and leverage against new attacks

Our Hypothesis

- **By comparison to enterprise systems, control systems exhibit comparatively constrained behavior:**
  - Fixed topology
  - Regular communication patterns
  - Limited number of protocols
  - Simpler protocols
- **As such, model-based IDS approaches may be more feasible**
- **Such an approach nicely complements a signature system**
- **Benefits are a compact, inherently generalized knowledge base and potential to detect zero day attacks**

Protocol Model: Individual fields

- **MODBUS function codes are one byte**
  - 256 possible values, but
  - MSB is used by servers to indicate exception
  - Valid range for requests is 1-127
- **Range is partitioned into public, user-defined, and reserved**
  - This suffices to construct a “weak specification” model
- **Many actual devices support a much more limited set of codes**
  - Permits stronger, more tailored model

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Protocol Model: Dependent Fields

- **Encode acceptable values of a field given the value of another field**
  - Dependent fields include length, sub-function codes, and arguments
  - For example, “read coils” function implies the length field is 6
  - For other function codes, length varies but a range can be specified
- **Specifications for multiple ADUs: future work**

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

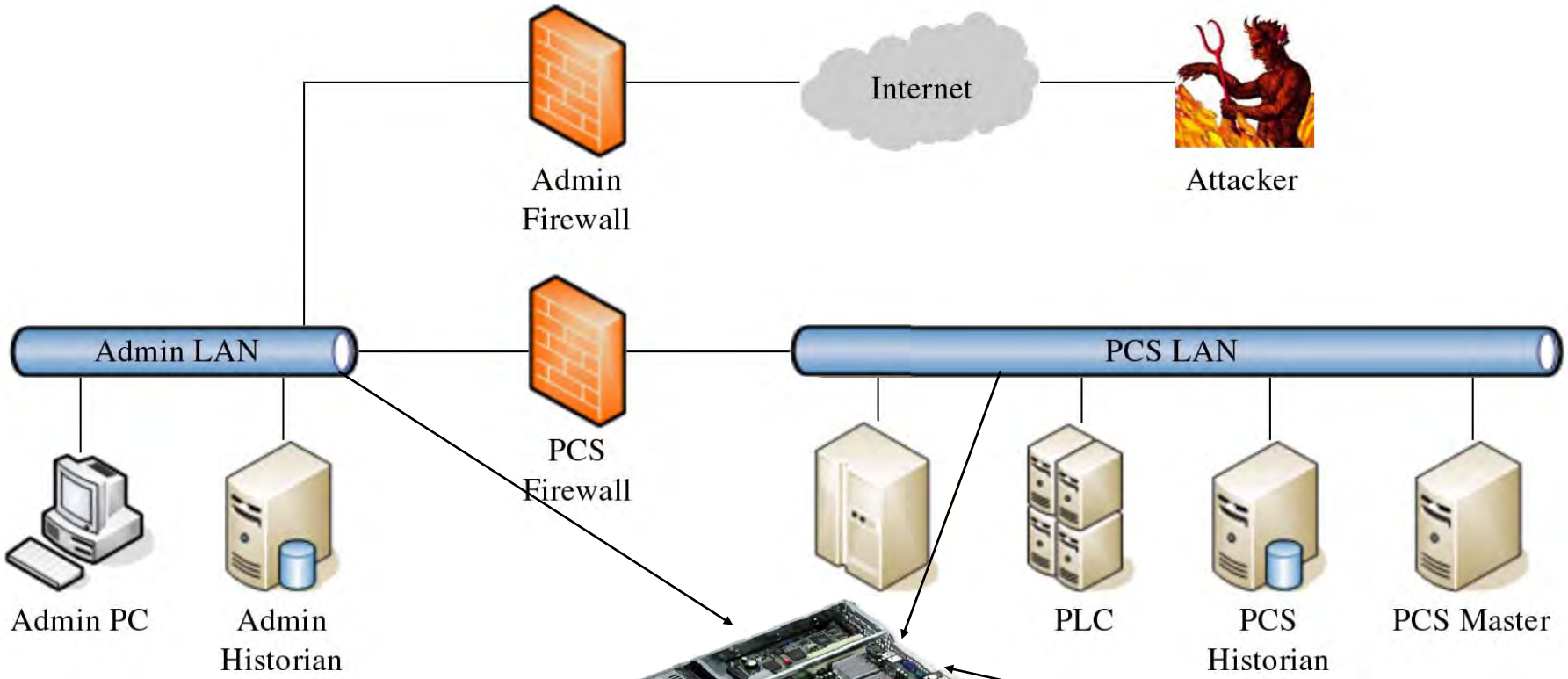
Detecting Unusual Communication Patterns

- Communications between the various LAN's are restricted by policy
- Attacker exploits some allowed paths (admin historian to PCS historian) but over disallowed protocols
- Detection of exceptions is via SNORT rules
- More complex networks (more devices) can be accommodated via IP address assignment with appropriate subnet masks

Detecting Changes in Server/Service Availability

- **EMERALD TCP service monitoring**
  - New service discovery (suspicious in a “stable” system)
  - Service up/down/distress
- **EMERALD for PCS includes analogous capability for MODBUS function codes**
  - Alerts when a device responds to a new function code (MODBUS service discovery)
  - Alerts when a function code previously considered valid for a device results in error replies

Testbed Architecture



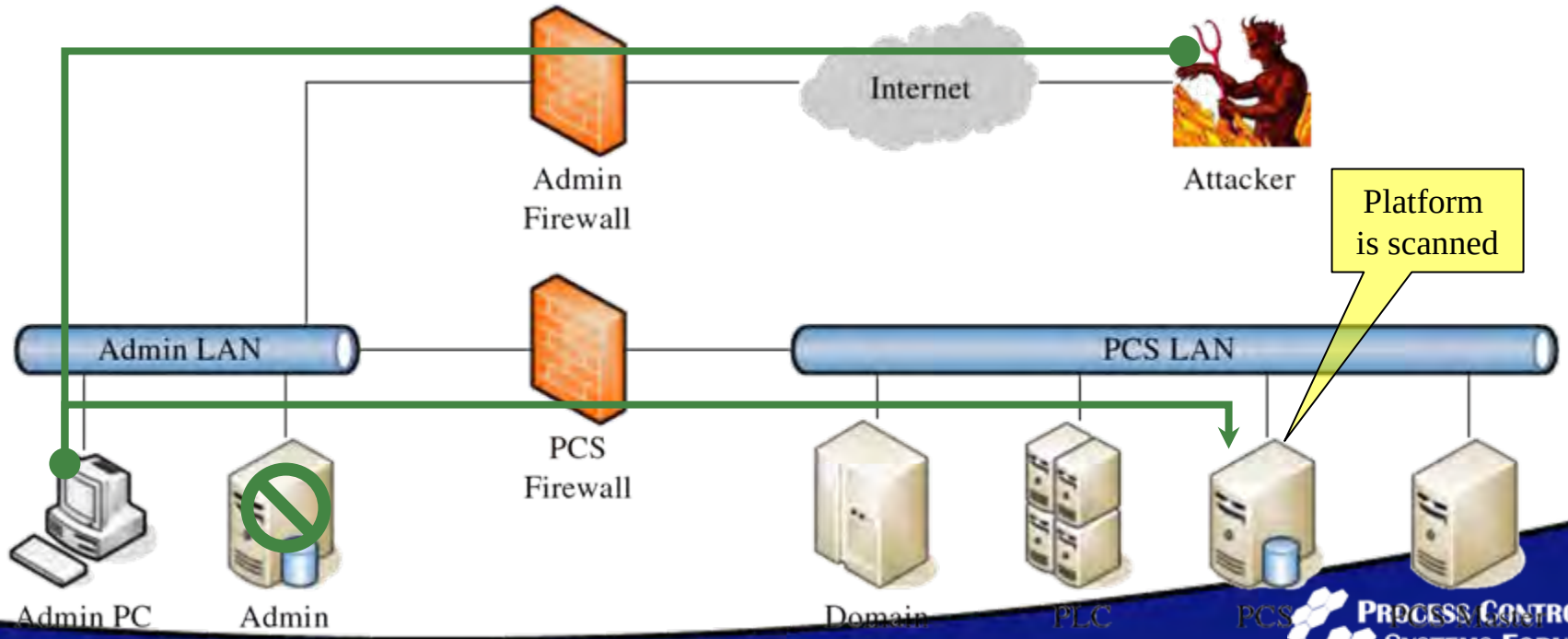
PCS-Enabled NIDS/Mcorr Appliance

Alerts and Diagnostics
- SHARP (PNNL)
- SecSS (Tulsa)
- APT (UIUC)

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Vulnerability Scenario

- **Demonstration**



Detections

- **Scans: Bayes sensor, unusual comms**
  - Aggregation presents thousands of probes as single alert
- **Compromise exploits (UPnP): SNORT Bleeding Edge**
- **tftp: Unusual Comms**
- **MODBUS Exploits: New Modbus services, spec based detection, Digital Bond set**

Alerts

EMERALD Alert Management Interface

File Alerts View Tools Help

emerald_db
Showing: Inbox

Prev Next
Page 1 of 1

Go To 1
Online

I3P

23 Inbox
15 EMERALD
2 UIUC
6 UTULSA
Trash

Alert Gen Time	Alert Count	Start Time	Signature	Incident Class	Obs Name	Source	Target
01/17/07 16:14:41	9	01/17/07 15:53:36	DYN_UNAUTHORIZED_T...	Connection Violation	snort_ipv4	10.0.0.1... [2]	10.0.0.1... [4]
01/17/07 16:12:20	2	01/17/07 15:11:51	IncompleteMBTransaction	Suspicious Usage	cis.utulsa.edu-modbus...	10.0.0.10	10.0.0.101
01/17/07 16:12:19	10866	01/17/07 15:05:48	DYN_UNAUTHORIZED_T...	Connection Violation	snort_ipv4	10.0.0.10... [2]	10.0.0.101... [2]
01/17/07 16:09:50	29	01/17/07 15:49:32	DYN_BLEEDING-EDGE_...	Privilege Violation	AlertMgr	192.168.0.100	10.0.0.11
01/17/07 16:09:50	217	01/17/07 15:43:59	PORT_SCAN	Probe	eBayes-TCP	192.168.0.100	10.0.0.11
01/17/07 16:09:50	7	01/17/07 15:49:32	DYN_BLEEDING-EDGE_...	Privilege Violation	snort_ipv4	192.168.0.100	10.0.0.11
01/17/07 16:05:01	3	01/17/07 15:04:32	newEntryLog	Action Logged	cis.utulsa.edu-modbus...	10.0.0.10	10.0.0.101
01/17/07 16:00:58	2	01/17/07 15:58:59	DYN_BLEEDING-EDGE_...	Privilege Violation	snort_ipv4	10.0.0.11	10.0.0.10
01/17/07 15:58:01	1	01/17/07 15:58:01	NEW_SVC	Suspicious Usage	eBayes-TCP-host	192.168.0.100	10.0.0.11
01/17/07 15:51:46	4618	01/17/07 15:43:55	DYN_UNAUTHORIZED_...	Connection Violation	AlertMgr	192.168.0.100	10.0.0.11
01/17/07 15:51:46	4621	01/17/07 15:50:21	DYN_UNAUTHORIZED_...	Connection Violation	AlertMgr	10.0.0.11	192.168.0.100
01/17/07 15:51:45	4619	01/17/07 15:50:21	DYN_UNAUTHORIZED_...	Connection Violation	snort_ipv4	10.0.0.11	192.168.0.100
01/17/07 15:51:45	4617	01/17/07 15:43:55	DYN_UNAUTHORIZED_...	Connection Violation	snort_ipv4	192.168.0.100	10.0.0.11
01/17/07 15:27:59	8	01/17/07 15:22:47	DYN_MODBUS_TCP_W...	Suspicious Usage	snort_ipv4	10.0.0.7	10.0.0.100
01/17/07 15:27:59	31	01/17/07 15:22:47	DYN_UNAUTHORIZED_T...	Connection Violation	snort_ipv4	10.0.0.7... [2]	10.0.0.7... [2]
01/17/07 15:26:29	2	01/17/07 14:24:37	mbWriteViolation	Integrity Violation	cis.utulsa.edu-modbus...	10.0.0.7	10.0.0.100
01/17/07 15:26:29	2	01/17/07 14:24:37	RogueDeviceViolation	Connection Violation	cis.utulsa.edu-modbus...	10.0.0.7	10.0.0.100
01/17/07 15:22:47	7	01/17/07 15:05:48	SUSPICIOUS	Suspicious Usage	AlertMgr	10.0.0.7... [2]	10.0.0.100... [2]
01/17/07 15:20:13	4	01/17/07 14:14:36	newEntryLog	Action Logged	cis.utulsa.edu-modbus...	10.0.0.10	10.0.0.100
01/17/07 15:07:00	2	01/17/07 15:05:48	NEW_MB_UNIT	Suspicious Usage	emodbus	10.0.0.10	10.0.0.100... [2]
01/17/07 14:35:48	1	01/17/07 14:35:48	APT_FW	Access Violation	APT	0.0.0.0	10.0.1.0
01/17/07 14:35:47	1	01/17/07 14:35:47	APT_FW	Access Violation	APT	172.16.1.0	0.0.0.0
01/17/07 14:22:19	1	01/17/07 14:22:19	newEntryLog	Action Logged	cis.utulsa.edu-modbus...	10.0.0.7	10.0.0.100

Detail	Value
Corr Alert Rank Std	0.0
Command	MB_READ_INPUT_REGISTERS_FC
Command Arguments	transaction ID: 73
Correlated Observer Location	172.16.10.120
Correlated Observer Namelist	cis.utulsa.edu-modbus-passive-scanner
Dynamic Signature	DynSig-0
class	10
code_name	Incomplete Modbus Transaction
description	This sensor has detected an incomplete modbus transaction, due to a time-out or the re-use of an active

Edit

ONTROL FORUM
to Advance Control System Security

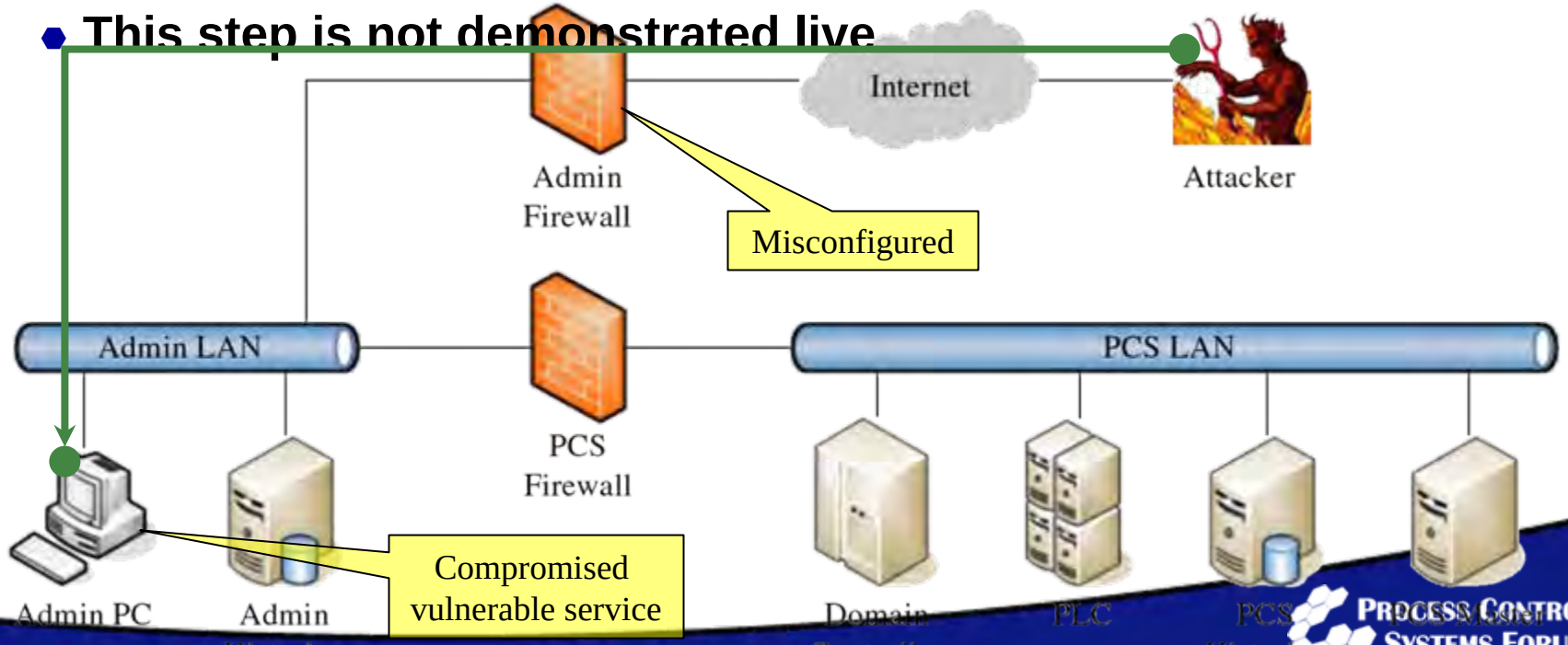
Summary

- Barrier protections are essential in PCS
  - DMZ
  - Switches, firewalls, VPN
- IDS is an important orthogonal defense
  - Detect probe, bypass, penetration
- Multi-component, multi-approach detection provides complementary views of an attack
- Alert correlation presents actionable situational awareness picture

Backup

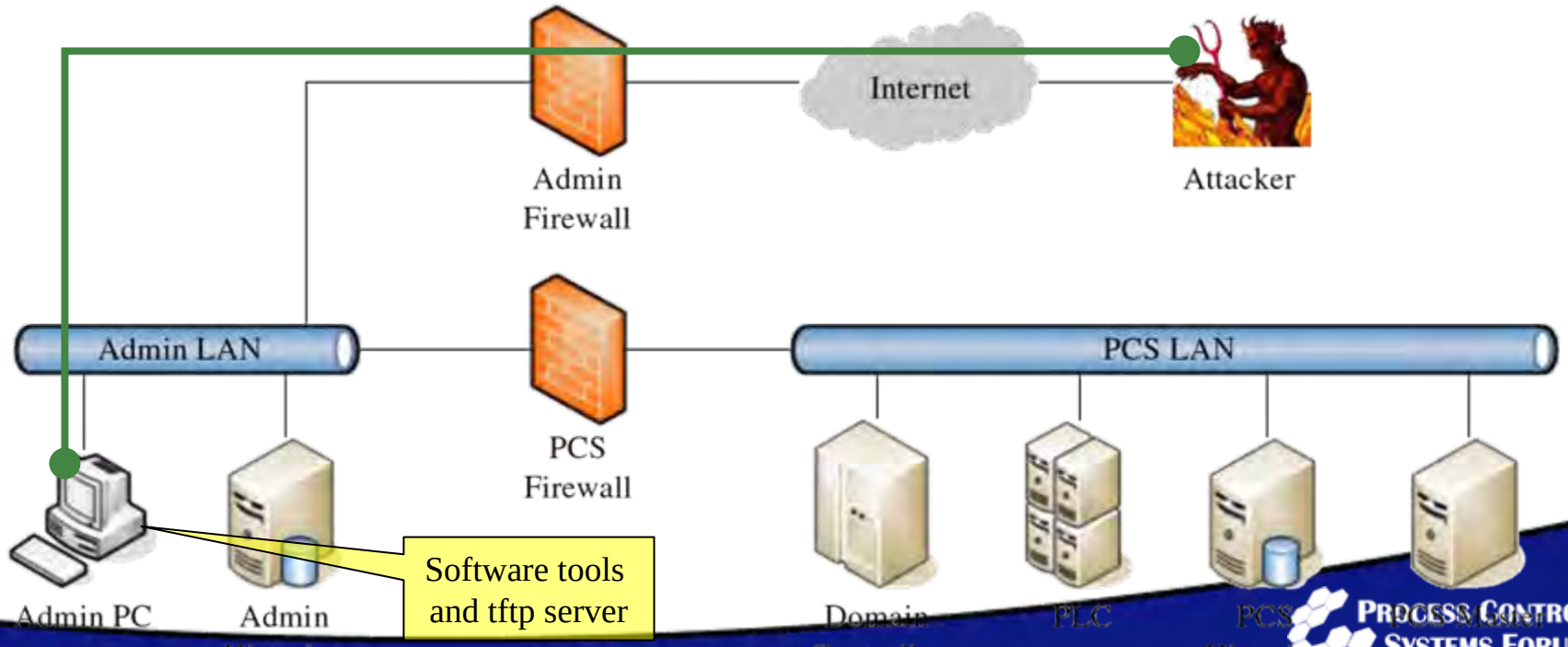
Vulnerability Scenario, Step 1

- Firewall misconfiguration allows access and compromise of a PC
- Host-based firewall fails to prevent the compromise
- Future events will issue from this platform, directed by the attacker
- This step is not demonstrated live



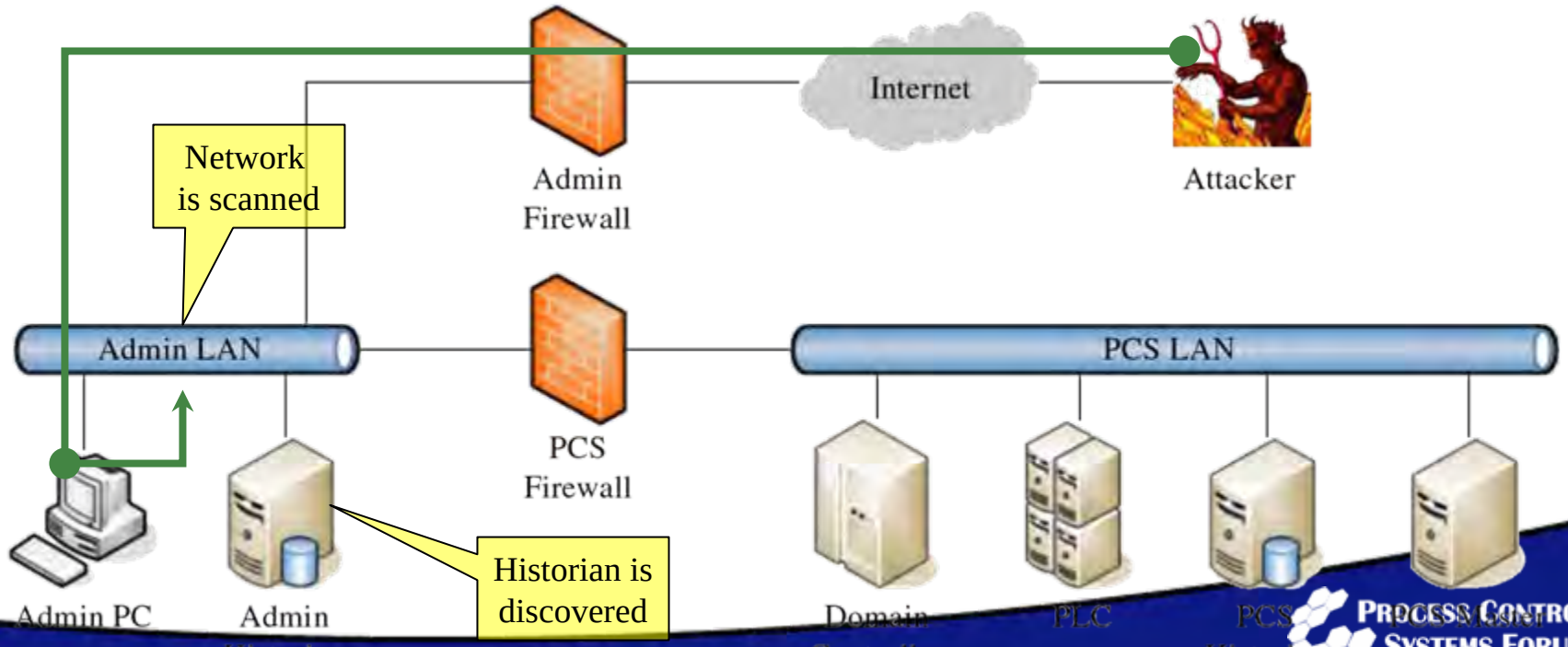
Vulnerability Scenario, Step 2

- Download software tools to the compromised Admin PC
- Set up a tftp server for later distribution



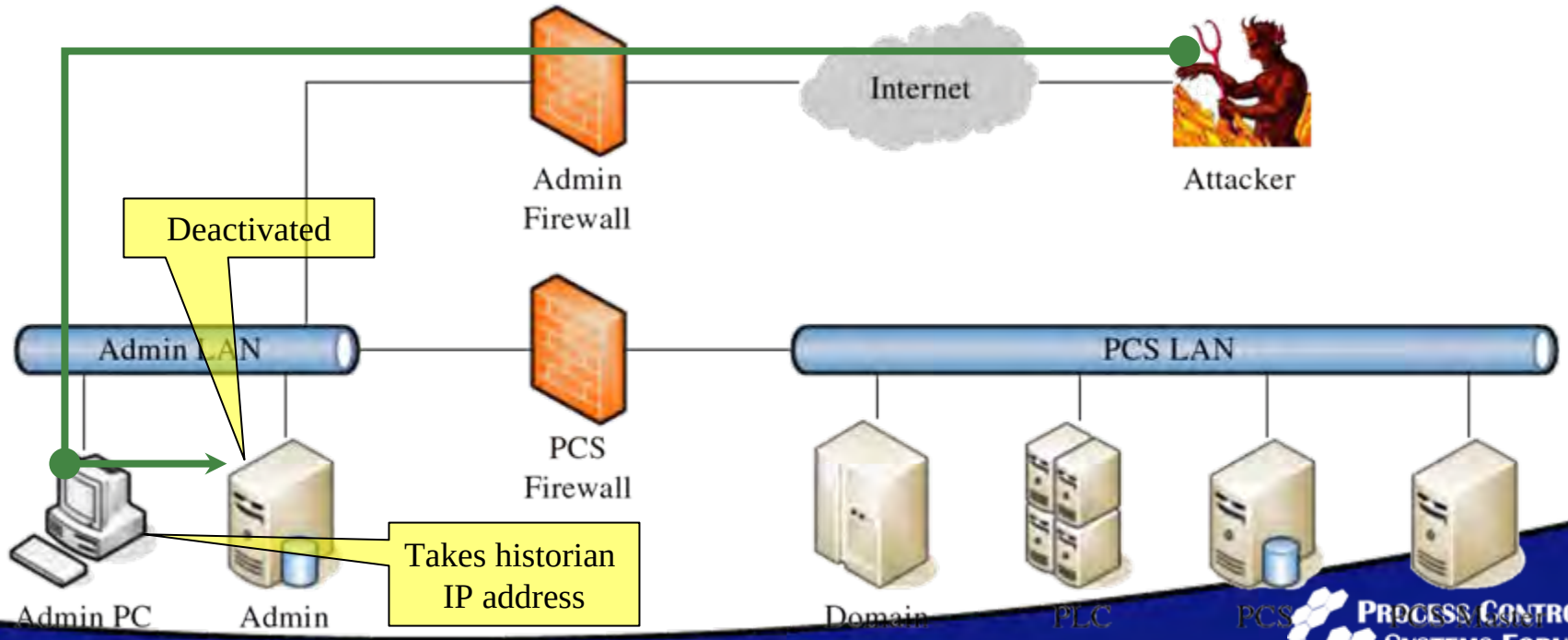
Vulnerability Scenario, Step 3

- Scan the administrative network
- Discover the Admin Historian
- Does not see the PCS network



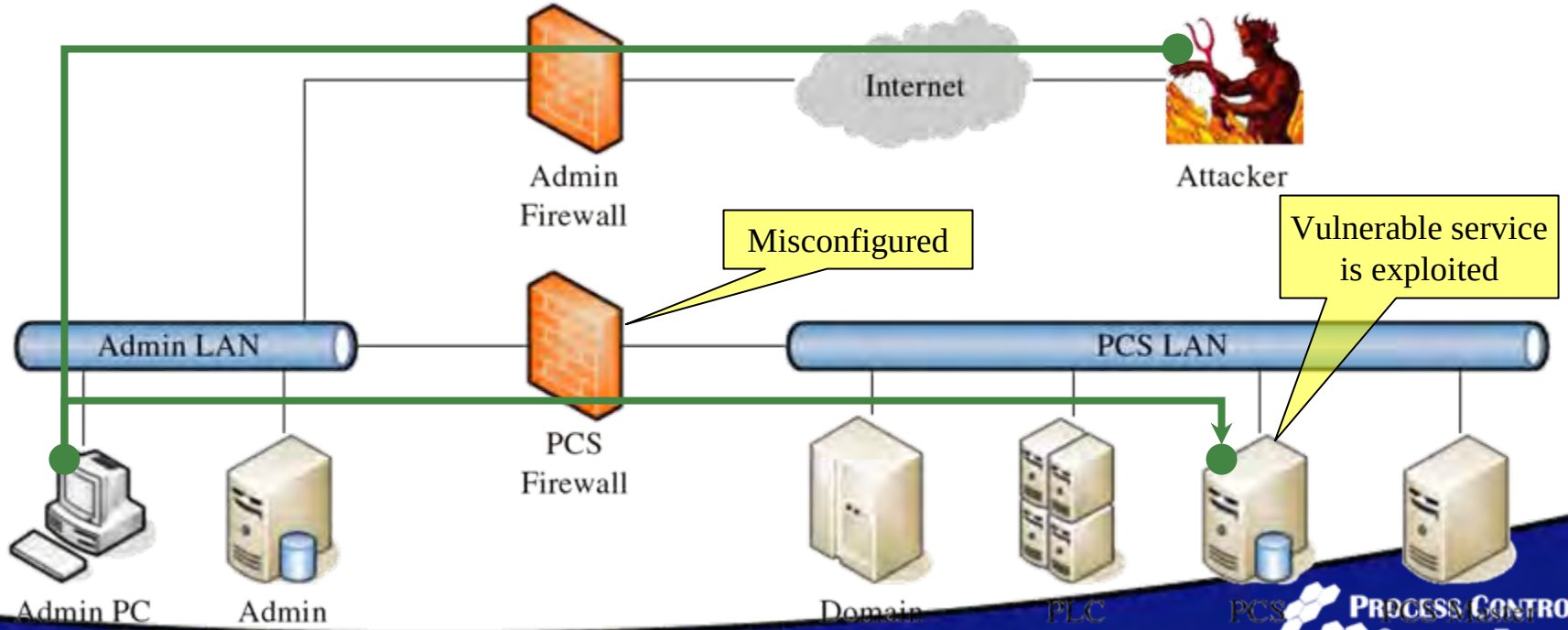
Vulnerability Scenario, Step 4

- Achieve elevated access to the Admin Historian
- Discover relationship to PCS Historian across firewall
- Push the Admin Historian off the network and assume its address



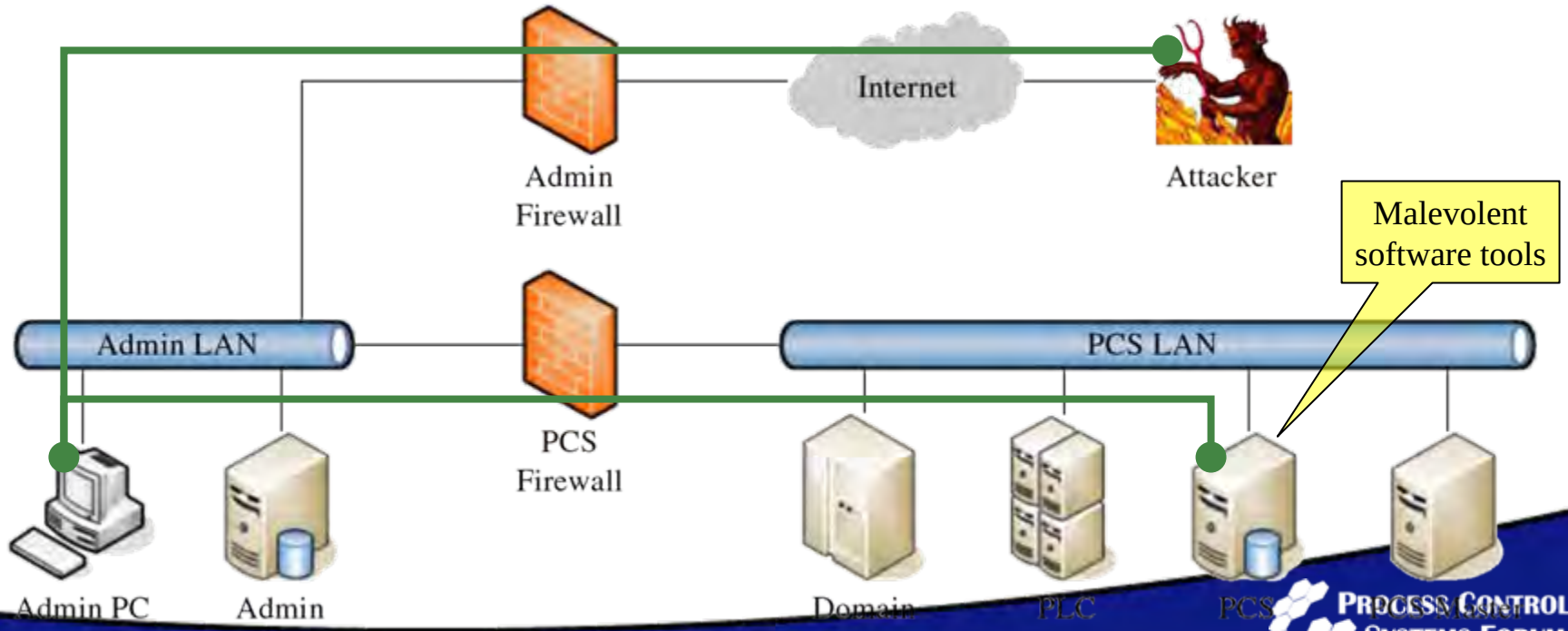
Vulnerability Scenario, Step 6

- Firewall configuration allows visibility of potential vulnerabilities
- Discover vulnerable authentication service on the PCS Historian
- Exploit to connect with system privilege to the PCS Historian



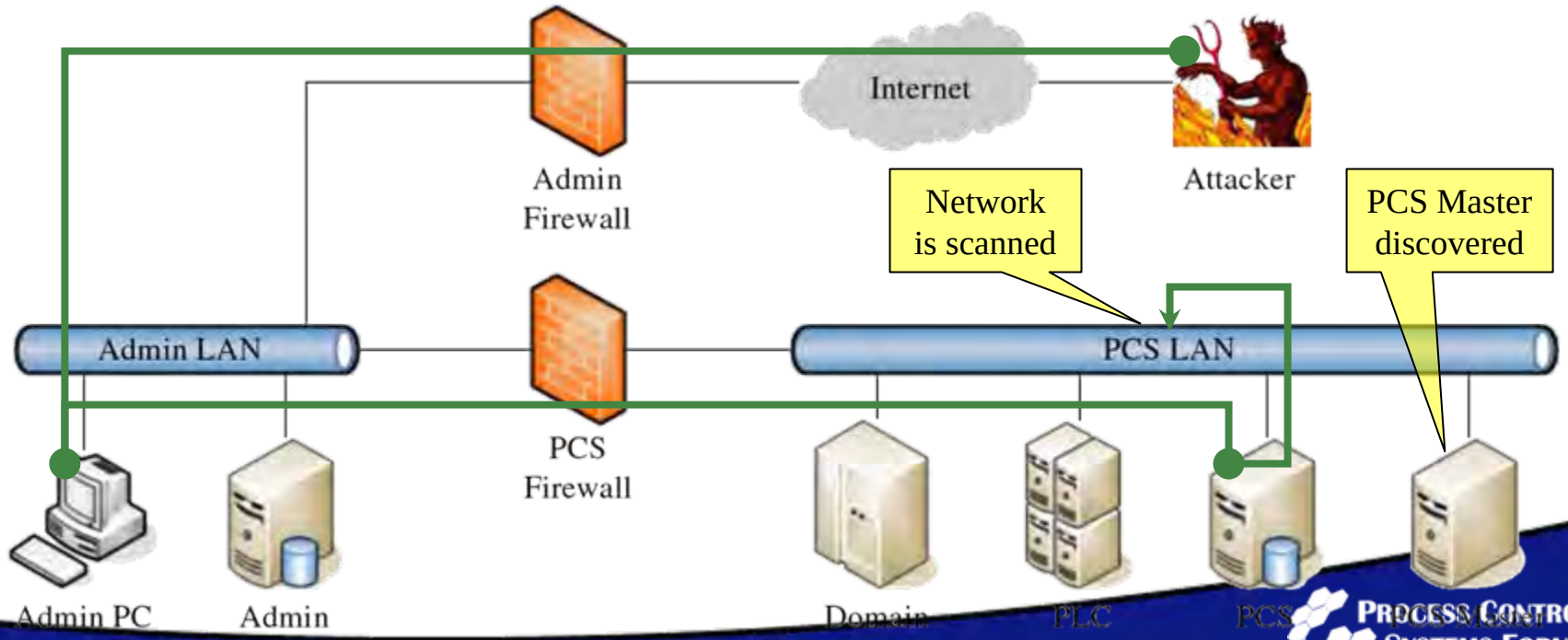
Vulnerability Scenario, Step 7

- Download a "rogue master" and other tools from the Admin PC
- PCS Historian is now the launching point for subsequent events



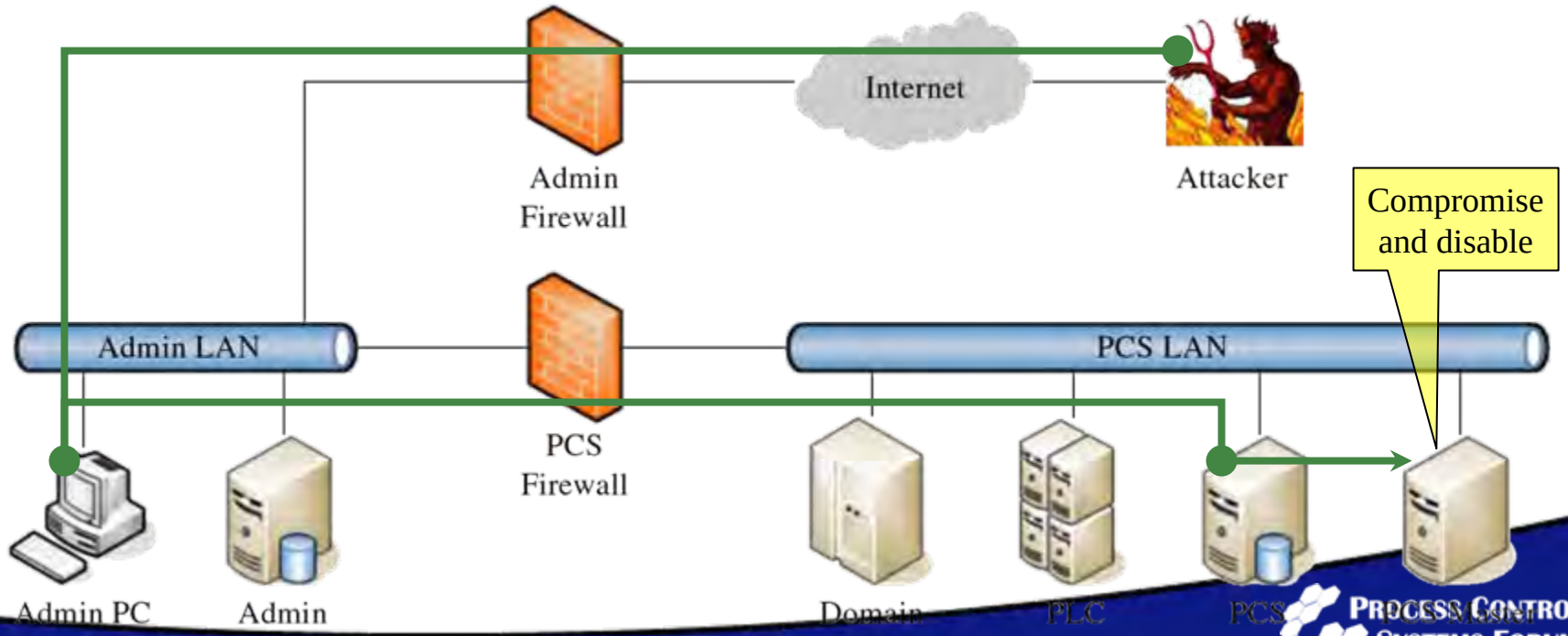
Vulnerability Scenario, Step 8

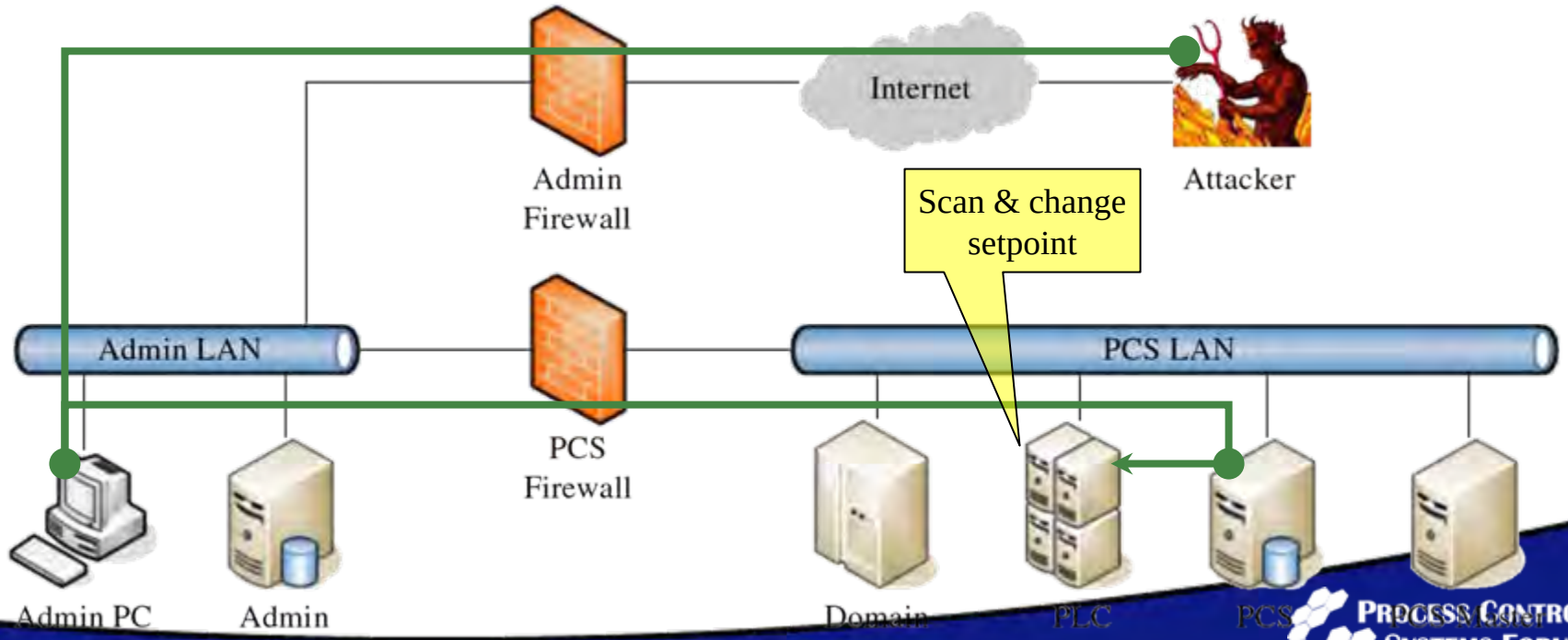
- Scan the PCS network
- Discover a vulnerable PCS Master box



Vulnerability Scenario, Step 9

- Exploit buffer overflow flaw in a vulnerable messenger service
- Disable the PCS Master



Vulnerability Scenario, Step 10

- Scan on the PCS LAN for Modbus-communicating platforms
- Send unauthentic Modbus command to change a PLC setpoint