Knowledge Check Quiz Case Study Week 11 (Ukraine Power Grid)

Due Apr 3 at 11:59pm **Points** 17 **Questions** 17
Available until Apr 3 at 11:59pm **Time Limit** None

Instructions

Answer the following questions on the case study material this week.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	10 minutes	17 out of 17

Score for this quiz: **17** out of 17
Submitted Feb 14 at 11:21am
This attempt took 10 minutes.

Question 1 — 1 / 1 pts

What was the **target of the attack**?

- Bank
- Water Services
- Power Grid — Correct!
- Fuel Enrichment Plant

Question 2 — 1 / 1 pts

Where did the attack occur?

Correct!

- (selected) Ukraine
- Europe and US
- Iran
- Australia

Question 3

1 / 1 pts

When did the first attack occur?

- April 2014
- April 2000
- December 2016

Correct!

- (selected) December 2015

Question 4

1 / 1 pts

When did the second attack occur?

- April 2000

Correct!

- (selected) December 2016

- April 2014
- December 2015

Question 5

1 / 1 pts

What was the **impact** from these attacks?

- Raw sewage was spilled
- Personally Identifiable Information stolen
- Credit card information stolen
- Power outages

Correct!

Question 6

1 / 1 pts

What makes this case study **significant**?

Correct!

- Malware introduced to critical infrastructure
- Wide spread attack on credit card terminals
- Exposed personally identifiable information
- Attack on security service for targeted victims

Question 7

1 / 1 pts

How did these attacks occur?

Correct!

- (selected) Phishing campaign to introduce malware
- PING flood and botnets attacked websites
- Radio signals to SCADA devices causing pumps to fail
- Malware introduced by contractors carrying USB sticks

Question 8

1 / 1 pts

What **technical concerns** contributed to this incident?

Correct!

- Adobe Flash vulnerability used to inject malicious code
- (selected) Malware targeted industrial control systems
- Radio signals to SCADA devices causing pumps to fail
- RAM scraping malware installed on Point of Sale terminals

Question 9

1 / 1 pts

What **human behavior** contributed to this incident?

Correct!

- Misinterpreted attacks as normal failures
- (selected) Employee opens attachment on phishing email
- Disgruntled employee sabotaged operations

- Contractor USB sticks used to install malware

Question 10

1 / 1 pts

What **business decisions** contributed to this incident?

Correct!

- Business networks connected to ICS network
- Announced security patch not installed
- Workarounds to address problem equipment masked attack
- Old versions of Office and Windows

Question 11

1 / 1 pts

Which **malware** was used in the first attack?

Correct!

- Black Energy
- Stuxnet
- Poison Ivy
- Crash Override

Question 12

1 / 1 pts

Which **malware** was used in the second attack?

- Black Energy
- Crash Override

Correct!

- Poison Ivy
- Stuxnet

Question 13

1 / 1 pts

Which recommendation for improving ICS security relates to **Architecture**?

- Perform network security monitoring
- Properly segment networks from each other

Correct!

- Use backup and recovery tools to take digital images of selected systems
- DMZs and properly tuned firewalls between network segments

Question 14

1 / 1 pts

Which recommendation for improving ICS security relates to **Passive Defense**?

- Plan and train to incident response plans

- Train defenders on using tools

Correct!

- Application Whitelisting
- Make backups of critical software installers

Question 15

1 / 1 pts

Which recommendation for improving ICS security relates to **Active Defense**?

- Ensure logging is enabled on devices

Correct!

- Train defenders to hunt for odd communications
- Limit remote connections only to personnel that need them
- Establish a central logging and data aggregation point

Question 16

1 / 1 pts

Which of the following characteristics is true for the **first attack**?

- 1 substation attacked
- Portion of capital region impacted

Correct!

- Telephone Denial of Service
- Outage lasted 1 hour

Question 17

1 / 1 pts

Which of the following characteristics is true for the **second attack**?

- 225,000 customers impacted
- 50+ substations attacked
- Outage lasted several hours
- Denial of Service attack on protective relays

Correct!

Quiz Score: **17** out of 17