

# Knowledge Check Quiz Case Study Week 5 (RSA Security)

Due Feb 20 at 11:59pm	Points 18	Questions 18
Available until Feb 20 at 11:59pm	Time Limit None	

## Instructions

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

## Attempt History

	Attempt	Time	Score
LATEST	<u>Attempt 1</u>	15 minutes	17 out of 18

Score for this quiz: **17** out of 18  
Submitted Jan 24 at 11:25am  
This attempt took 15 minutes.

Correct!

Question 1

1 / 1 pts

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

☒ Security Access

☐ Water Services

☐ Power Grid

☐ Bank

Question 2

1 / 1 pts

**Where** did the attack occur?

- ☐ Iran
- ☐ Ukraine
- ☐ Australia
- ☒ United States

**Correct!**

**Question 3**

**1 / 1 pts**

When was the attack **discovered**?

- ☒ March 2011
- ☐ April 2007
- ☐ April 2000
- ☐ August 2014

**Correct!**

**Question 4**

**1 / 1 pts**

What was the **impact** from the attack?

- ☐ Credit card information stolen
- ☐ Widespread power outages

**Correct!**

- ☐ Centrifuges were destroyed
- ☒ Corporate secrets stolen

**Question 5****1 / 1 pts****What makes this case study significant?**

- ☐ Malware introduced to critical infrastructure
- ☐ Denial of service attack on critical infrastructure
- ☐ Insider attack on industrial control systems
- ☒ Attack on company providing service for targeted victim

**Correct!****Question 6****1 / 1 pts****How** did the attack occur?

- ☒ Phishing campaign to gain credentials
- ☐ Distributed denial of service attack on government websites
- ☐ Radio signals to SCADA devices causing pumps to fail
- ☐ Malware introduced in firmware updates

**Correct!****Question 7****1 / 1 pts**

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

Correct!

- ☐ PING flood and botnets
- ☐ SCADA system insecure
- ☒ Adobe Flash vulnerability used to inject malicious code
- ☐ Malware designed to impose damage

### Question 8

1 / 1 pts

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

Correct!

- ☐ Security team ignored warnings from anti-intrusion system
- ☐ Contractor USB sticks used to install malware
- ☐ Disgruntled employee sabotaged operations
- ☒ Employees open attachment on phishing email

### Question 9

0 / 1 pts

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

Not Answered

- ☐ Heavy dependence on IT services
- ☒ Failed to isolate sensitive network assets

**Correct Answer**

- ☐ Old versions of Office and Windows
- ☐ Old operating systems on ICS networks

**Question 10****1 / 1 pts**Which **malware** was used in the attack?**Correct!**

- ☒ Poison Ivy
- ☐ Black Energy
- ☐ Black POS
- ☐ Stuxnet

**Question 11****1 / 1 pts**What does the acronym **RAT** stand for?**Correct!**

- ☐ Realtime Audio Transfer
- ☐ Radio Assessment Token
- ☐ Reliable Access Technology
- ☒ Remote Access Toolkit

**Question 12****1 / 1 pts**

**What is the definition of an Intrusion Detection System?****Correct!**

Security service that monitors and analyzes network or system events to detect unauthorized access



Undocumented way of gaining access to a computer system



Program that is covertly inserted into another program with malicious intent



Tricking individuals into disclosing sensitive personal information through deceptive computer-based means

**Question 13****1 / 1 pts****What is the definition of Malware?**

Security service that monitors and analyzes network or system events to detect unauthorized access



Integrated collection of security measures designed to prevent unauthorized access



Undocumented way of gaining access to a computer system

**Correct!**

Program that is covertly inserted into another program with malicious intent

**Question 14****1 / 1 pts**

What is the definition of **Phishing**?

☐

Program that is covertly inserted into another program with malicious intent

☐

Flaw or bug that allows access in unexpected or unauthorized ways

☒

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means

☐

Security service that monitors and analyzes network or system events to detect unauthorized access

**Correct!****Question 15****1 / 1 pts**

Which strategy for detecting Advanced Persistent Threat is used to identify phishing campaigns?

☒

Rule Sets

☐

Statistical and Correlation Methods

☐

Automatic Blocking of Data Exfiltration

☐

Manual Approaches

**Correct!**

**Question 16****1 / 1 pts**

Which strategy for detecting Advanced Persistent Threat is used to configure tools to work together to analyze network traffic?

**Correct!**☐ Automatic Blocking of Data Exfiltration☒ Statistical and Correlation Methods☐ Manual Approaches☐ Rule Sets**Question 17****1 / 1 pts**

Which strategy for detecting Advanced Persistent Threat is used to review log entries?

**Correct!**☐ Rule Sets☐ Statistical and Correlation Methods☒ Manual Approaches☐ Automatic Blocking of Data Exfiltration**Question 18****1 / 1 pts**

Which strategy for detecting Advanced Persistent Threat is used to alert on characteristics of outgoing traffic?



**Correct!**

- ☐ Rule Sets
- ☐ Statistical and Correlation Methods
- ☐ Manual Approaches
- ☒ Automatic Blocking of Data Exfiltration

Quiz Score: **17** out of 18