Knowledge Check Quiz Case Study Week 3 (Estonia)

Due Feb 6 at 11:59pm **Points** 16 **Questions** 16
Available until Feb 6 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	6 minutes	16 out of 16

Score for this quiz: **16** out of 16
Submitted Jan 19 at 1:19pm
This attempt took 6 minutes.

Question 1

1 / 1 pts

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

Correct!

- (selected) Country Internet
- Power Grid
- Water Services
- Bank

Question 2

1 / 1 pts

Where did the attack occur?

- Australia
- Ukraine

Correct!

- (•) Estonia
- United States

Question 3

1 / 1 pts

When did this attack **begin**?

- April 2000

Correct!

- (•) April 2007
- July 2010
- April 2014

Question 4

1 / 1 pts

What was the **duration** of this attack?

Correct!

- (•) 3 weeks
- 3 months

- 3 days
- 3 hours

Question 5

1 / 1 pts

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

- Credit card information stolen
- Corporate secrets stolen
- Widespread power outages

Correct!

- (selected) Government and business activities interrupted

Question 6

1 / 1 pts

What makes this case study **significant**?

- Supply chain attack on industrial control systems
- Malware introduced to critical infrastructure

Correct!

- (selected) Denial of service attack as cyber warfare
- Insider attack on industrial control systems

Question 7

1 / 1 pts

How did the attack occur?

- Malware introduced in firmware updates
- Radio signals to SCADA devices causing pumps to fail
- Phishing campaign to gain credentials

Correct!

- (●) Distributed denial of service attack on government websites

Question 8

1 / 1 pts

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

- Adobe Flash vulnerability used to inject malicious code

Correct!

- (●) PING flood and botnets
- SCADA system insecure
- Malware designed to impose damage

Question 9

1 / 1 pts

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

- Contractor USB sticks used to install malware

Correct!

- (●) Coordinated cyber attack as political protest
- Security team ignored warnings from anti-intrusion system

- Employees open attachment on phishing email

Question 10

1 / 1 pts

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

- Old versions of Office and Windows
- Security patch not installed
- Subcontractor with weak security practices given access
- Heavy dependence on IT services

Correct!

Question 11

1 / 1 pts

What is the definition of a **Denial of Service attack**?

- Integrated collection of security measures designed to prevent unauthorized access
- Exploits a security vulnerability occurring in the database layer
- Type of malware that appears to perform a desirable function while allowing unauthorized access

Correct!

Malevolent effort to deny access to an electronic resource by its intended users

Question 12

1 / 1 pts

What is the definition of a **Botnet**?

Correct!

Collective computing network using software that automates routine, repetitive tasks

Citizen involvement with cyber attacking the systems of a perceived adversary

Individual who possesses an intimate working knowledge of computers to gain unauthorized access

Simple command used to check availability of the targeted computer

Question 13

1 / 1 pts

What is the definition of **Patriot Hacking**?

Individual who possesses an intimate working knowledge of computers to gain unauthorized access

Simple command used to check availability of the targeted computer

Correct!

Citizen involvement with cyber attacking the systems of a perceived adversary

Collective computing network using software that automates routine, repetitive tasks

Question 14

1 / 1 pts

What is the definition of a **Ping**?

Correct!

Simple command used to check availability of the targeted computer

Collective computing network using software that automates routine, repetitive tasks

Citizen involvement with cyber attacking the systems of a perceived adversary

Individual who possesses an intimate working knowledge of computers to gain unauthorized access

Question 15

1 / 1 pts

Which **3 lessons learned** were identified to implement after this attack?

Correct! ☑ Develop and implement large scale system of security measures

☐ Use paper submission of all government documents

Correct! ☑ Increase expert awareness and competence in cyber security

Correct! ☑ Raise public awareness on cyber security

☐ Remove all World War II statues

Question 16

1 / 1 pts

Which **3 technical measures** were taken to recover from the attack?

Correct! ☑ Filtered out malicious traffic

Correct! ☑ Applied security patches

☐ Highlighted need to raise international awareness

☐ Revived paper submissions of government documents

Correct! ☑ Increased bandwidth

Quiz Score: **16** out of 16