ANSWERS

# F11.4 Network attacks

Cyber security · GCSE · OCR J277 1.4.1, Edexcel 1CP2 4.2.1 · about 20 min

## What this lesson is about

Brute force, denial of service, data interception and SQL injection, and detecting a flood.

- Brute force
- Denial of service
- Data interception
- SQL injection
- Detecting a flood

## Questions

**6 marks in all**

**1.** What is a brute force attack? [1 mark]

- ☐ **A** Trying every possible password until one works
- ☐ **B** Flooding a server with requests
- ☐ **C** Reading data as it travels
- ☐ **D** Tricking a database

> **Answer:** A. It relies on speed and short passwords.

**2.** What does a denial of service attack do? [1 mark]

- ☐ **A** Floods a system so it cannot serve real users
- ☐ **B** Steals passwords
- ☐ **C** Encrypts files for ransom
- ☐ **D** Reads private messages

> **Answer:** A. It attacks availability.

**3.** How is intercepted data made useless to an attacker? [1 mark]

- ☐ **A** By encrypting it
- ☐ **B** By compressing it
- ☐ **C** By deleting it
- ☐ **D** By sending it faster

> **Answer:** A. Encrypted data is unreadable without the key.

**4.** What is a botnet? [1 mark]

- ☐ **A** Many hijacked computers used together in an attack
- ☐ **B** A kind of firewall
- ☐ **C** A password manager
- ☐ **D** A backup system

> **Answer:** A. A DDoS uses a botnet to flood from many places at once.

5. How is SQL injection prevented? [1 mark]

- ☐ **A** Validating input and keeping it separate from the query
- ☐ **B** Using a faster database
- ☐ **C** Encrypting the web page
- ☐ **D** Adding more servers

> **Answer:** A. Never trust user input in a query.

6. How many possible codes does a 4-digit PIN have? [1 mark]

> **Answer:** 10000. 10 to the power 4.

## The task: flood detector

Count how many requests come from each address in `requests`. Print `<address>: <n>` for each, sorted from the most requests to the fewest. Any address with 5 or more requests is an attack: print `BLOCK` on its line, and at the end print `blocked: <addresses>`, the blocked addresses joined by `, `.

```
# the two lines every program starts with: the commands, then the robot
from bugbot import *
connect()

requests = [
    "10.0.0.5", "10.0.0.9", "10.0.0.5", "10.0.0.5", "10.0.0.2",
    "10.0.0.5", "10.0.0.5", "10.0.0.9", "10.0.0.5", "10.0.0.5",
]
```

**The hint students can ask for:** Count the requests per address into a dictionary, then sort those counts from the largest down. Mark and collect any address that reaches the threshold, and list the collected ones at the end.

### A solution

```
from bugbot import *
connect()
requests = [
    "10.0.0.5", "10.0.0.9", "10.0.0.5", "10.0.0.5", "10.0.0.2",
    "10.0.0.5", "10.0.0.5", "10.0.0.9", "10.0.0.5", "10.0.0.5",
]
counts = {}
for address in requests:
    counts[address] = counts.get(address, 0) + 1
blocked = []
for address, n in sorted(counts.items(), key=lambda kv: kv[1], reverse=True):
    if n >= 5:
        print(f"{address}: {n} BLOCK")
        blocked.append(address)
    else:
        print(f"{address}: {n}")
print("blocked:", ", ".join(blocked))
```

Any program that meets the task's checks is marked correct in the simulator; this is one way, not the only way.