WORKSHEET

F11.4 Network attacks

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

BugBotLab

Name _____ Class _____ Date _____

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

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

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

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

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

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

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",
]
```

Plan your program here, then type it in and press Run.

Do it on the robot

www.bugbotlab.com/learn/f11-4-network-attacks/

The simulator checks it and tells you when it passes. Nothing to install, no account.

Challenges

1. How many tries does brute force need, at most, for a 6-digit PIN?
2. Why is a DDoS from a botnet harder to block than a DoS from one computer?
3. Explain in one sentence how SQL injection lets someone log in without a password.