Linus Fulton

# Exercise 1

## Task 1: What measures have you taken to protect yourself from cyber crimes?

My main action in protecting myself from the danger of password leaks is to using reputable password manager in combination with a 2FA app. The password manager generates complex passwords for all my accounts, and protects these behind a master password that is long and complex enough to not be brute-forceable, but is easy for me to remember (see: https://xkcd.com/936/). Having unique passwords for all accounts makes data leaks not be as bad, since the leaked password isn't reused anywhere else. The 2FA app further secures my accounts, so that simply having the password isn't enough to access the account.

I semi-regularly check sites such as haveibeenpwned, and change the passwords of any accounts that have been involved in a data leak. I have been part of several data leaks (all 5+ years back, no more recent ones luckily), though none of the accounts were very important ones. I'm using an ad-blocker with built in phishing and malware protection, which along with some common sense not to click any suspicious links means i have luckily never had any problems with any cyber crimes. I do regularly get scam e-mails (such as fake Post-Office notifications), but these are usually easy to recognise.

To improve my measures, I could start using hardware-based 2FA such as YubiKeys. I should also start regularly reviewing app permissions, and removing those that do not need access to certain systems (camera, microphone, etc.).

## Task 2: Company Security Policy

Password Policy:

Purpose: The purpose of the Password Policy is to make sure that all employees maintain secure passwords. This protects company data, as well as systems and networks for outside sources.

Scope: This policy applies to employees and all others who have access to the companies systems.

Policy:

- Password Creation:
    - Minimum Length: Any password must be at least 8 characters long.
    - Complexity: Any password must include at least one letter, one number, and one special character (!, #, @, etc.).
    - Avoid Common Passwords: Avoid common passwords such as "password", "12345678", or any easily guessed personal information.

- Password Management:
    - Unique Passwords: Employees must use a different passwords for different accounts.
    - Password Changes: Employees must NOT change their passwords regularly.

- Password Protection:
    - Password Sharing: Do NOT share passwords with other employees or anyone outside the company.
    - Storage: Password should NOT be written down or stored unencrypted. Use a password manager to store passwords.
    - MFA: Use MFA wherever possible, ideally using a specialised MFA app.

- Incident Response:
    - Reporting: If an employee thinks their password has been stolen, they must change it immediately and report the incident.
    - Audits: Regular audits will be conducted to test the policy.

### Physical Access Policy:

Purpose: The purpose of the Physical Access Policy is to guard the companies possessions, such as physical assets, data, and employees.

Scope: This policy applies to employees and all others who have access to the companies systems.

Policy:

- Access Control:
    - Authorisation: Only authorised people are allowed to enter the company building. Access depends on the job and need of the person.
    - Identification: Employees must wear a ID while inside the company.
    - Visitor Access: All visitors must be signed in and approved, and be escorted by an employee at all times.

- Restricted Areas:
    - Sensitive Areas: Certain areas, such as server rooms, are accessible only to certain employees. These employees are identified by a special ID.
    - Locking: Restricted Areas must be locked with either locks, keypads, or biometric security.
    - Employees must make sure no unauthorised persons follow them into restricted areas.

- Security Measures:
    - Surveillance: The company is monitored by CCTV cameras 24/7. The footage is kept for 90 days before being deleted.
    - Alarm Systems: Alarm systems are installed at every entrance and will call the authorities unauthorised access is attempted outside of work hours.
    - Emergency Exits: Emergency exits are closed and alarmed to prevent unauthorised access. These exits should only be used in an emergency.

- Incident Response:
    - Breach Reporting: Any breach or attempted breach must be reported to the security team.
    - Investigation: Any incidents will be investigated.

## Task 3: Threat Modelling

### Task 3A: Threat Dragon

See json and pdf files in Github.

### Task 3B: Personal Threat Model

Not done.

## Task 4: Personal Security Audit

### Task 4A: Network Scan

I scanned my local network at 10.10.24.181/24 on MacOS

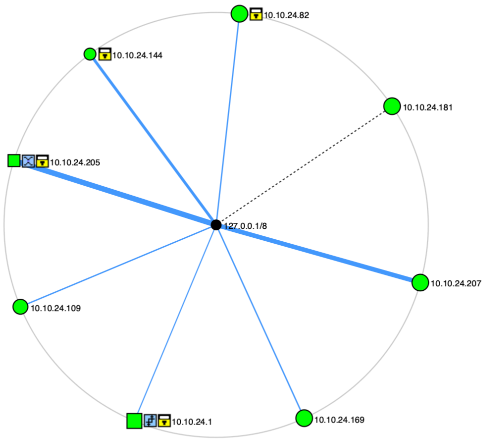
Linus Fulton

1. Did you find any devices you did not know were in your network?
There are 8 devices on my network (10.10.24.0/24). Due to this being a larger network that is used for several students in my dorm, it’s impossible to say if these are legit devices or dangerous one.

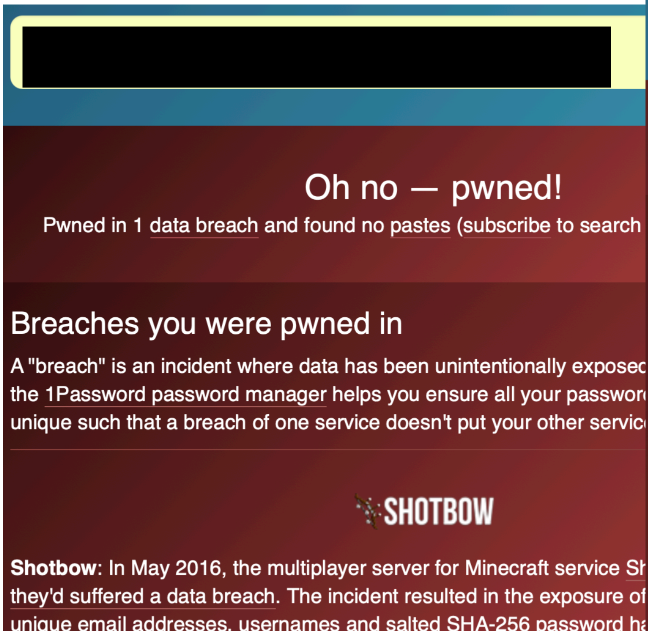
2. Were there any open ports which should have been closed?
While several open ports were found on devices, its hard to say if they should be open or not. One open port is 53 (DNS). Since this devices has the address “10.10.24.1”, it is probably the default gateway, and also the DNS server. Therefore it being open isn’t too unusual. Another open port on another device is “62078”, which is apparently part of Apple’s iPhone sync services.

3. Did nmap find any vulnerabilities with the scripts?
nmap did not find any vulnerabilities

4. Screenshot the topology of your network. You can redact device information if you want.
My Macbook is the host “10.10.24.181”.



Task 4B: Account Security
I have 2 main emails accounts, both of which have been part of data leaks. These leaks include data such as emails, passwords, usernames, phone numbers, and much more (see screenshots below). I have changed the passwords for all the accounts, except those which do not offer password changes (such as BlankMediaGames and MangaDex). Here I sadly needed to leave the passwords be, however they are not services i currently still use. They also have very weak passwords, none of which i use now (from before I started learning about proper account security).



[redacted]

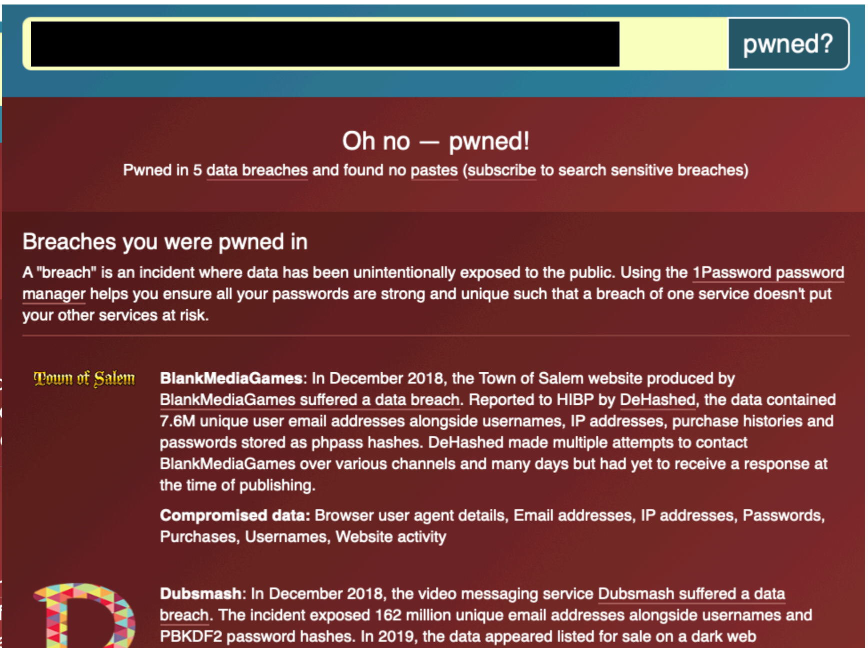
Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed
the 1Password password manager helps you ensure all your passwor
unique such that a breach of one service doesn't put your servic

**Shotbow**: In May 2016, the multiplayer server for Minecraft service Sh
they'd suffered a data breach. The incident resulted in the exposure of
unique email addresses, usernames and salted SHA-256 password ha



[redacted] pwned?

Oh no — pwned!

Pwned in 5 data breaches and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

**BlankMediaGames**: In December 2018, the Town of Salem website produced by BlankMediaGames suffered a data breach. Reported to HIBP by DeHashed, the data contained 7.6M unique user email addresses alongside usernames, IP addresses, purchase histories and passwords stored as phpass hashes. DeHashed made multiple attempts to contact BlankMediaGames over various channels and many days but had yet to receive a response at the time of publishing.

**Compromised data:** Browser user agent details, Email addresses, IP addresses, Passwords, Purchases, Usernames, Website activity

**Dubsmash**: In December 2018, the video messaging service Dubsmash suffered a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hashes. In 2019, the data appeared listed for sale on a dark web