Veikko Vähäsöyrinki Week1 homework

Task 1:
I got insterested about cyber security from listening Herrasmieshakkerit podcast. From that I have learned a lot about techniques cyber criminals use, so educating myself about the cyber security field is one measure. Probably the biggest protection I use is a password manager with a master password. For almost every account I have generated a strong unique password which is stored to the password manager. I also use Firefox with fortified privacy settings instead of Googles spyware called Chrome. For some services which have my payment info I use 2-factor authentication. I also have multiple emails, critical email accounts are from protonmail. One email I use only for banks and for finnish authorities, and one is for normal use. One is a ”throwaway” email. I use linux as my main operating system, currently dual booting Arch and Pop os. I have spent time on learning linux system administration. I have also changed my root user's password. I have not been a victim of a cyber crime, atleast checking from haveibeenpwned.com. I could improve on keeping the latest updates of my software and os.

Task 2: Threat model

Identify your assets that could be targeted by cyber criminals

- Assess the threats and likelyhoods of them for each of your assets
- Identify vulnerabilities for example weak or repeated passwords
- Evaluate impact if an asset is compromised
- Mitigate or mitigation plan; determine what you can do now and what to do if compromised

My personal assets that interest cyber criminals:
Money, personal information: social security number, full name,

Task 3

Company password policy

Scope

This policy applies to every employee of the company.

Purpose

The purpose of this password policy is to establish the framework for administering passwords for the company as part of its efforts to maintain the confidentiality, integrity and availability of the company information.

Responsibility

The IT department of the company is responsible for administering, maintaining and updating this policy with the approval of the chief technology officer, chief information officer and/or chief operating officer.

Objectives

The objective of this policy is to provide secure and appropriate access to the company applications, and to the company systems and data used, processed, stored, maintained and/or transmitted in and through those information systems.

Password guidelines

1. Passwords must be a minimum of 12 characters.
2. When an initial password is created for a new user ID, or reset, an individual must change the password at the next logon for applications which enable user-initiated password changes.
3. the company will force password changes at least every 6 months on systems accessing sensitive business information.
4. Passwords should be a combination of alphanumeric characters, numbers and symbols, and should not be easily guessed. Examples of passwords that are not acceptable include user ID, dictionary words, first or last name of user, family member, city, town, street, etc.
5. Enforcement of strong passwords will be automated.
6. User IDs and passwords or open computer application sessions should not be shared.
7. Screensavers with passwords should be used for desktop computers and should be activated after no more than 5 minutes of inactivity.
8. Alternate authentication technologies, e.g., biometrics or proximity cards, may be used in place of password protections.

Password administration

1. Failed login attempts may be recorded and reviewed for follow-up action.
2. Users will be locked out of the system after 5failed login attempts and must contact the help desk for access resetting. Manager approval may be required to fulfill a password reset request.
3. Access privileges will be reviewed prior to granting access based on factors including job title and function (role-based access) or the individual (user-based access).
4. User IDs, passwords or email accounts are not to be transferred to another individual.
5. New accounts may be obtained by calling the IT help desk. Management approval is required before any account can be created.

Noncompliance with this policy

The company employees and authorized contractors who do not comply with this policy and the procedures that may be developed from it are subject to possible disciplinary measures as may be determined by the company's general counsel and/or human resources.

Management review and audit availability

The company executives will review and update this policy on a quarterly basis. As changes to company policies are indicated, the company management may initiate a change management request to alter the policy (or policies). All company policies will be available for review during scheduled audits.

Physical access policy

Scope

This policy applies to all of the company’s facilites.

Purpose

The purpose of this physical access policy is to establish the rules for granting, managing and monitoring the passage in the company’s facilities.

Responsibility

The security department of the company is responsible for administering, maintaining and updating this policy and it is responsible to deploy the actions required in this policy.

Objectives

The objective of this policy is to provide the necessary physical and information security to the company’s employees and facilities.

The policy

Every employee must have an ID card with a photo. The ID card must be weared at all times in the company’s facilities. The ID card contains a NFC tag. The ID cards must be renewed every 3 years along with a new photo. Renewal request must be made at least 2 days prior to the security department. A lost ID card must immediately be notified with a call to the company’s security hotline. A temporary card expiring in 12 hours may be granted from the reception to the employee. Every employee must only be granted a necessary rights for passage. These rights have to be managed and refreshed to match the position employee works in.

Outside of the facility

Physical access must be restricted to the whole facility. A barbed wire fence must be present around the facility at the border of the company’s lot. The barbed wire fence must comply the local laws regarding construction. CCTV cameras must monitor the land between the fence and the facility’s walls. The cameras must not have a blind spots and the CCTV cameras must be monitored 24/7 from the monitoring room.

The parking lot

There can only be one controlled gate to grant passage of employees to the parking lot. Every employee must register his/her car’s registration number to grant passage. Employee can have maximum 2 cars registered. Employee must show his/her ID card and the car’s regristration number must match to grant passage to the parking lot.

Inside of the facility

Every door must have an ID card reader to manage passage excluding the toilets. The door is locked at all times and can be opened with the ID card if the employee has the appropriate rights. The card readers must collect the complete NFC tag data from every scan. The data must be stored at the monitoring room.

Visitors and guests

Visitors can be granted a temporary ID card. Visitors must be approved at least 3 days prior by the chief security officer. Unexpected visitors must not be allowed passage under any circumstances except the police, fire or ambulance crew.

Noncompliance with this policy

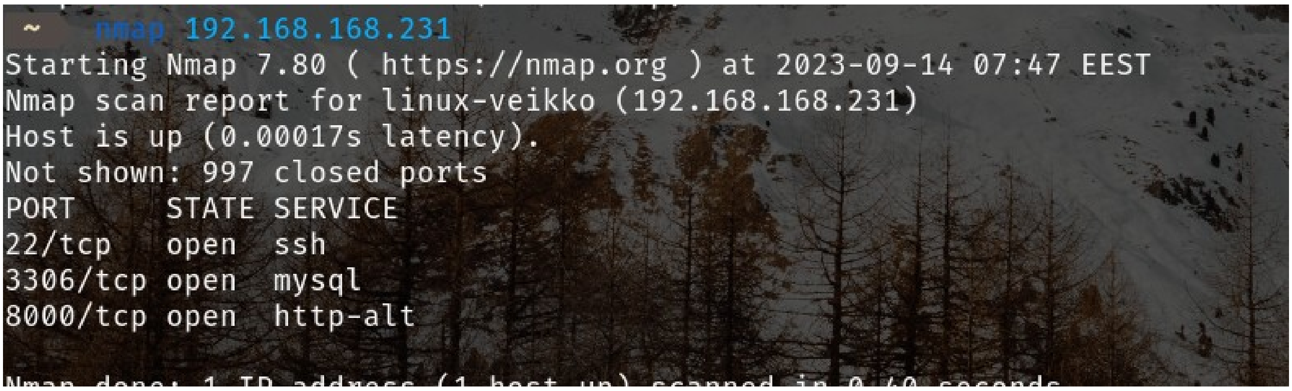
The company employees and authorized contractors who do not comply with this policy and the procedures that may be developed from it are subject to possible disciplinary measures as may be determined by the company's general counsel and/or human resources.

Management review and audit availability

The company executives will review and update this policy on a quarterly basis. As changes to company policies are indicated, the company management may initiate a change management request to alter the policy (or policies). All company policies will be available for review during scheduled audits.

Task 4A

NMAP



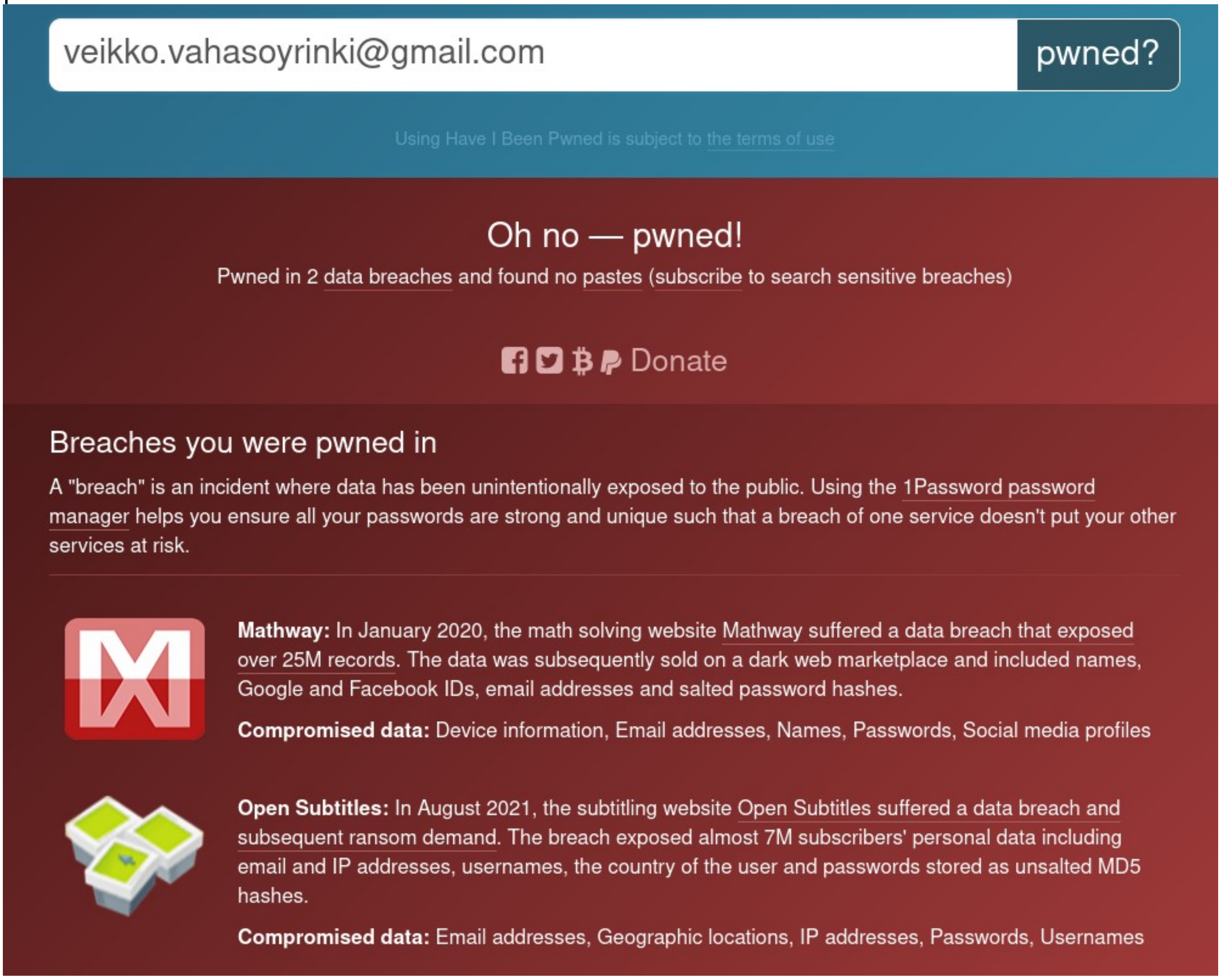
```
 ~   nmap 192.168.168.231
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-14 07:47 EEST
Nmap scan report for linux-veikko (192.168.168.231)
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3306/tcp open  mysql
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

There are no unexpected results.

Task 4B

No pownage was found with my current email. However, my throwaway email account has been part of data breaches.



veikko.vahasoyrinki@gmail.com
pwned?
Using Have I Been Pwned is subject to the terms of use

Oh no — pwned!

Pwned in 2 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.

Mathway: In January 2020, the math solving website Mathway suffered a data breach that exposed over 25M records. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.

Compromised data: Device information, Email addresses, Names, Passwords, Social media profiles

Open Subtitles: In August 2021, the subtitling website Open Subtitles suffered a data breach and subsequent ransom demand. The breach exposed almost 7M subscribers' personal data including email and IP addresses, usernames, the country of the user and passwords stored as unsalted MD5 hashes.

Compromised data: Email addresses, Geographic locations, IP addresses, Passwords, Usernames

I already knew about this.