Opdracht 2

# **2.1:The security cube**

## 2.1.1:

**Adobe Encryption Error:**

Confidentiality:

Even with a password hint only known to the user, brute force attacks would still easily render the encryption useless. The keys and database were kept on the same system, which is a result of faulty Accounting.

The encryption error here was mostly human error. They should not have decided to use the same key for every password and they should have kept the unlock key elsewhere.

Integrity:

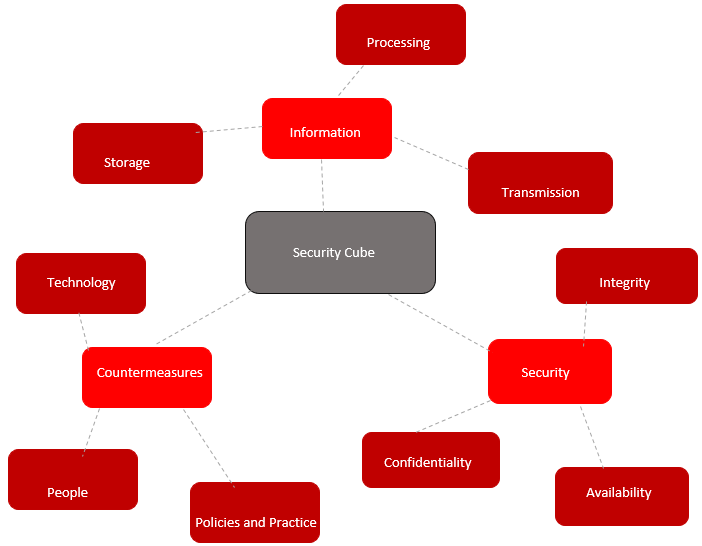
They used the same key for all encrypted data and the encryption was insecure.

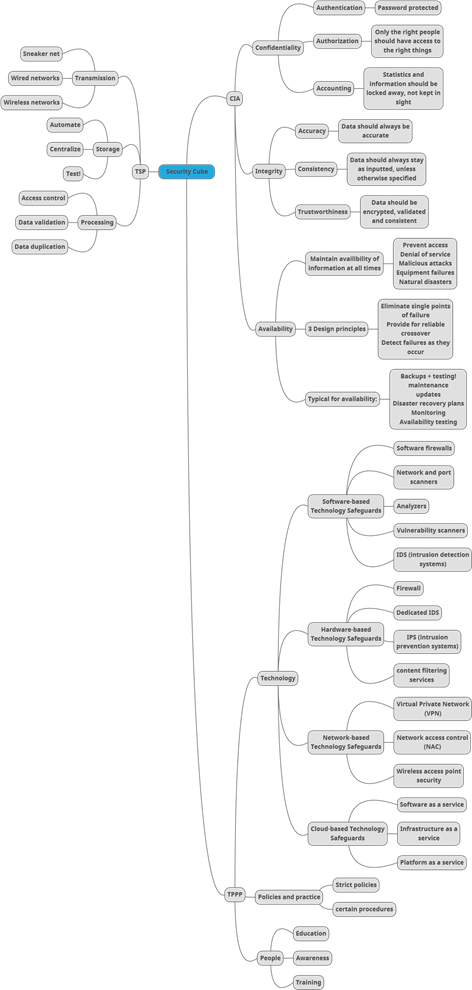
Password hints were not encrypted and thus easily accessed.

They kept the database in the same location as the keys used to unlock the encryption.

Availability:

In the result of availability nothing much was harmed. Servers went down for a while to find out what was stolen from where, but for the rest there were no availability issues.

**2.1.2**

****

## 2.1.3

Network sniffing: Het betrokken deel van de security cube is de Transmission layer in dimension 2 ‘State of Data’. Network sniffing maakt gebruik van de transmissie van data om daar unencrypted files uit te halen. Als je connectie en files encrypted zijn, is er dus geen probleem.

DDos Attack: Hier wordt de availability van de CIA triad betrokken. Ze proberen de availability van service neer te halen door deze te flooden. (ze gaan dus heel veel bots tegelijk de site laten bezoeken)

Rogue WiFi access point: Confidentiality en Integrity zijn er hierbij betrokken. Confidentiality omdat er nu ‘hackers’ aan confidential informatie kunnen waar ze anders misschien niet aan konden. Integrity omdat de access point moet aangesloten worden aan het netwerk, dus ‘moet’ van binnenuit gebeuren. Qua integrity zou er geen ander probleem mogen zijn als alle bestanden goed encrypt zijn etc.

Electromagnetic pulse: Hierbij worden Availability en Technology getroffen. De Technology wordt zo goed als helemaal vernietigd door de EMP en moet dus vervangen worden. De Availability zal daarom hieronder lijden.

Social engineering: De people zijn de groep die ‘getarget’ wordt bij deze ‘scam’. Bv: Je krijgt een email van je ‘baas’ die vraagt om iets door te sturen, maar het blijkt uiteindelijk je baas helemaal niet te zijn. Hier kan je helaas weinig tegen doen, misschien het enige wat je kan doen is je mensen hiertegen opleiden. Human errors zijn toch nog steeds niet te vermijden.

Whistleblower: Een whistleblower target de Policies en Practices. Hij legt unethical en mogelijk illegal violations voor van een bedrijf. Deze violations kunnen zijn van company policies tot wetten en regulaties.

# 2.2:**Controlling access: AAA Concepts**

## **2.**2.1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Paswoord | req 1 | req 2 | req 3 | req 4 | Secure? |
| Teamlid1 (MailChain5$) | X | X | / | X |  |
| Teamlid2 (KwadeSteelpan33) | X | X | / | / |  |
| Teamlid3 (HentaiSenpai15) | X | X | / | / |  |
| Teamlid4 (BasicFit12) | X | / | / | / |  |
| #4ssFrX^-aartPOknx25\_70!xAdk<d! | / | X | X | X |  |
| TelevisieTopTemptation! | X | / | / | / |  |
| J0n@than#81 | X | / | / | X |  |
| Test1234 | X | / | / | / |  |
| generated 01 (waw]u`N7{.4\6yPF) | / | X | X | X |  |
| generated 02 (h=DQ2PX$E\_A.)ukp) | / | X | X | X |  |
| generated 01A  (place friendly must equally) | X | X | / | / |  |
| generated 02A  (faster brought special slip) | X | X | / | / |  |

## 2.2.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Aantal karakters | 2 (binair) | 10 (decimaal) | 26 | 128(ASCII) |
| 5 | 2^5 | 10^5 | 26^5 | 128^5 |
| 8 | 2^8 | 10^8 | 26^8 | 128^8 |
| 16 | 2^16 | 10^16 | 26^16 | 128^16 |
| 32 | 2^32 | 10^32 | 26^32 | 128^32 |
| 64 | 2^64 | 10^64 | 26^64 | 128^64 |
| 128 | 2^128 | 10^128 | 26^128 | 128^128 |

Conclusie uit tabel:

Als je wachtwoord een 5-letter woord is met alleen maar kleine letters. Bijvoorbeeld kleuren werden vroeger vaak gebruikt zoals ‘zwart’, ‘groen’ of ‘paars’. Dan zijn er 26^5 mogelijkheden om je wachtwoord te kraken. Uitgerekend zijn dit 11 881 376 mogelijkheden. Voor heel wat mensen lijkt dit misschien veel maar dat is het totaal niet.

Werkwijze password kraken:

**Bruteforce:**

Bij bruteforce gaat de computer echt alle mogelijkheden af en genereert die ze meestal ook ter plaatse. Bijvoorbeeld: a, aa, ab, ac, …, zzzzz. Zoals je kunt zien is deze methode zeer inefficiënt. Wel is ze 100% trefzeker. (als het password in de tussentijd niet veranderd wordt uiteraard)

Volgens wikipedia is dit de geschatte tijd:

De formule voor de schatting van de maximum tijd om een wachtwoord te vinden (gebaseerd op drie miljoen wachtwoorden per seconden) is:  
  
seconden = (karakter ^ posities) / 3000000

**Tables:**

Het is ook mogelijk om te ‘bruteforcen’ door gebruik te maken van tables. Bijvoorbeeld een table met “de 1000 meeste gebruikte wachtwoorden”. In plaats van alle mogelijkheden te genereren ga je hier alle wachtwoorden in het bestand af.

Het grote nadeel hiervan is dat de kans vrij klein is dat degene wiens wachtwoord je wilt kraken er in staat.

Dit kan wel handig zijn als je gewoon iemand in het algemeen zijn wachtwoord wilt kraken. Als je een miljoen gebruikersnamen hebt is de kans niet onrealistisch dat iemand zijn wachtwoord dan wel een vrij populair en insecure wachtwoord is dat dus in die table staat.

**Rainbow Tables:**

Dit is een table met alle wachtwoorden en hun hashes. Deze techniek is veel sneller dan bruteforce.

Dit gebruik je dan om de hashes te vergelijken. Zo kun je dan ook terug aan het originele wachtwoord.

Voorbeeld:

Een heel bekende password cracker is Hydra. Deze staat standaard op Kali Linux. Hiermee kun je zowel bruteforce als wordtables.

Password entropy:

Dit wordt uitgedrukt in ‘bits’, het aantal bits geeft een soort van moeilijksgraad voor de onvoorspelbaarheid van het wachtwoord. 0 bits staat bijvoorbeeld voor een paswoord dat al is gekraakt en in een gekende database staat waar een cracker automatisch overgaat.

## **2.**2.3

* **Zoek een gepaste paswoordmanager. (Verantwoord je keuze!)**
* **Creëer een trial en verken de tool in VM ware.**

**⇒ Set a master password**

**⇒ install Paswoordmanager**

**⇒ log in and explore.**

**⇒ Neem printscreens!**

## **2.**2.4

**Als wachtwoorden op servers worden opgeslagen als ‘plain tekst’ liggen de wachtwoorden voor het rapen wanneer de database wordt gehacked.**

**Hoe worden wachtwoorden opgeslagen in een database? Verklaar in je eigen woorden!**

Wachtwoorden worden encrypted opgeslagen in een database. Dit gebeurt met behulp van een encryption tool (bv sha-256) De wachtwoorden zien dus niet zichtbaar zonder een juiste encryption key, met deze encryption key kan je de wachtwoorden ‘unlocken’ en ze dus zien. Met ‘zien’ bedoelen we dat in plaats dat je het wachtwoord rechtstreeks kunt aflezen je het woord helemaal in andere tekens ziet staan. Bijvoorbeeld bij sha-256 zal je dan 256 karakters hebben als encrypted wachtwoord.

Deze kunnen nog steeds ‘gekraakt’ worden. Daarom is het altijd aangeraden om iets te gebruiken als ‘salt’. Hierdoor komt er een random tekenreeks voor- of achteraan bij waardoor het nog veel veiliger wordt opgeslagen.

**Klopt de eerdere wachtwoord policy nog steeds?**

Neen, stel bij een breach, dan zou je de passwords gewoon kunnen aflezen als die als plain text opgeslagen zouden zijn. Als deze encrypted zijn, dan zou zelfs bij een eventuele breach je niks kunnen beginnen met deze encrypted passwords. Tenzij de encryption key ook geleaked zou zijn samen met de database, dan zouden ze deze wel kunnen zien. Dit gebeurt wel maar zelden.

Vandaar dat het aangeraden wordt om op elke website een uniek wachtwoord te gebruiken.

## **2.**2.5

Two factor authentication: Een tweede code die je krijgt via sms, mail, app, etc..  
 om in te loggen. Je hebt je passwoord nog steeds  
 nodig.

Voordeel: Betere beveiliging, maakt de werkwijze van hackers  
 een stuk moeilijker, ze hebben niet enkel het paswoord  
 nodig, maar ook het persoonlijk toestel voor de 2FA  
 code.

Verschil 2FA en 2stepV: 2stepV maakt gebruik van een vooraf ingestelde  
 beveiligingsvraag of dergelijke info that de gebruiker  
 moet doorgeven. 2FA bestaat uit een authenticatie  
 waar een persoonlijke bezitting of toestel voor nodig is.  
 2StepV kan dus minder efficiënt zijn omdat er bij  
 eventueel genoeg kennis over het slachtoffer toch een  
 antwoord gegeven kan worden op de

beveiligingsvraag.

Toepassingen: 2FA wordt voornamelijk gebruikt bij goed beveiligde  
 websites met belangrijke gebruikersinfo. Een goed  
 voorbeeld is online bankieren, waar je niet enkel de  
 kaartinfo nodig hebt, maar ook de effectieve bankkaart  
 alsook de pincode om het via een extern toestel te  
 verifiëren.

## 

## 2.2.6

· Maak je passwoord lang genoeg

· Gebruik geen namen uit het alledaags leven (bv naam van je hond)

· Verwerk symbolen in je passwoord ($, #, @, etc)

· Gebruik een variatie van hoofdletters en kleine letters

· Verwerk cijfers in je passwoord

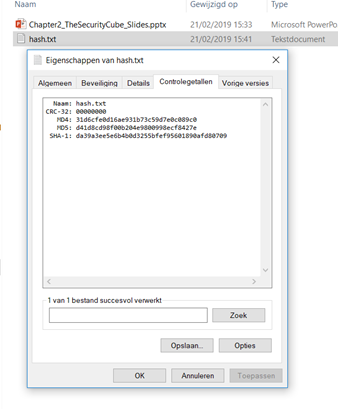
Het beste is nog steeds om een random generated password te gebruiken. Deze kan je opslaan in een password manager.

# 

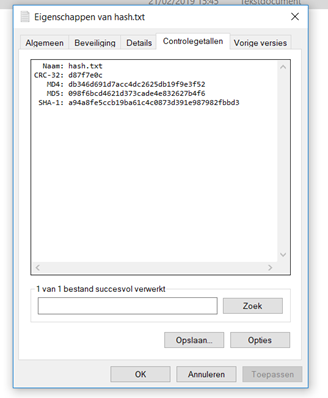
# 

# 2.3:**Data with a hash**

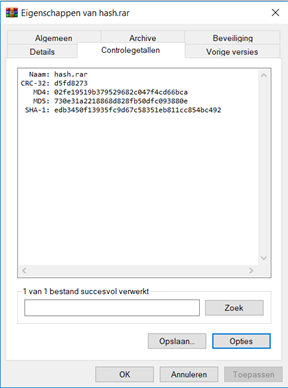
Nieuw textbestand aangemaakt:



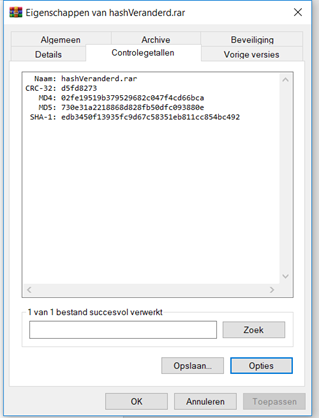
Bij het wijzigen van het textbestand verandert de MD5 code:



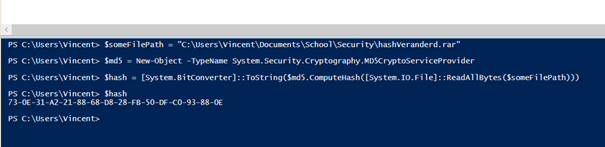
Dit principe geldt ook voor ZIP bestanden:



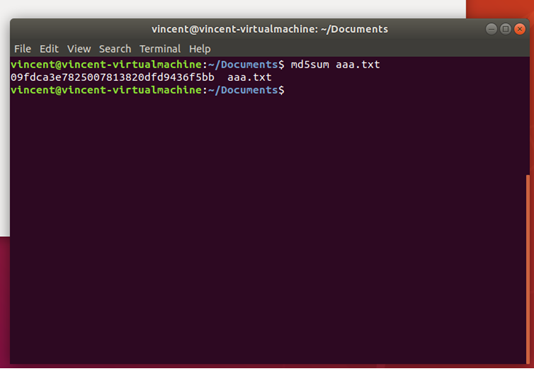
Wanneer de bestandsnaam gewijzigd wordt, verandert de MD5 ook:



MD5 kan ook berekend worden via powershell met dit commando



Alsook in Linux met volgend commando:



Alternatieven: sha2, scrypt, bcrypt

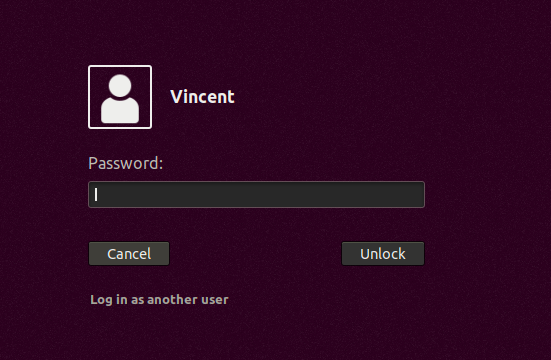
Nadeel MD5: MD5 kan snel gedecrypt worden, waardoor het bestand zichtbaar is.

Checksum: Facebook-authenticatie  
Reden: Het gekozen wachtwoord van de gebruiker wordt gehasht

Paswoorden: Wachtwoorden worden op een server opgeslagen in de databank,  
 deze zijn normaal gezien gehasht voor security.

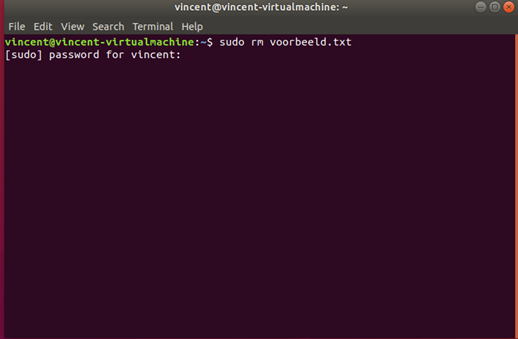
# 2.4:**AAA in Windows en Linux**

Linux  
**Authentication**  
Bij het opstarten is er een wachtwoord vereist om toegang te verkrijgen tot het systeem.



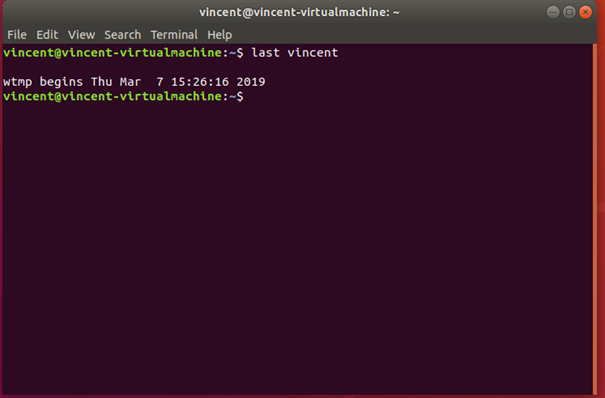
**Authorization**

Wanneer er in de terminal een commando uitgevoerd moet worden dat superuser rechten vereist, horen we eerst sudo voorafgaand het commando te typen, dit zal een wachtwoord van de gebruiker vragen vooraleer het commando uitgevoerd wordt.



**Accounting**

In linux kan men het commando ‘last’ gebruiken in de terminal om na te gaan sinds wanneer een gebruiker is ingelogd.

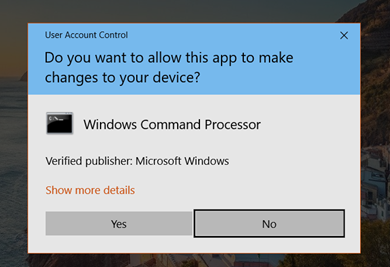


Windows

**Authentication**

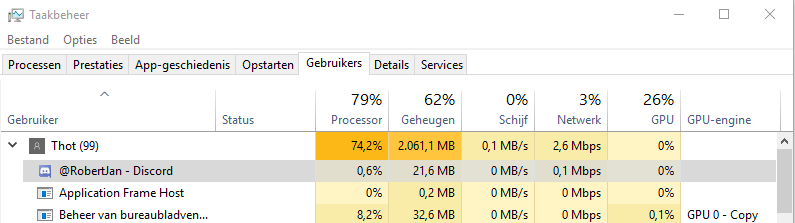
Net zoals bij Linux wordt er een verificatie scherm getoond voor in te loggen.****

**Authorization**  
Wanneer we een programma willen uitvoeren dat wijzigingen aan ons systeem kan aanbrengen horen we goedkeuring van de administrator te verkrijgen, dit kan als administrator zijnde door de melding goed te keuren, of door het wachtwoord in te voeren.

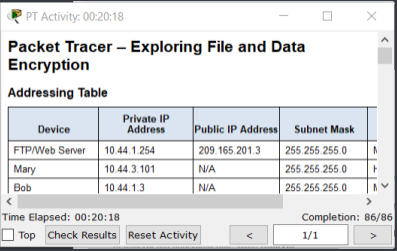
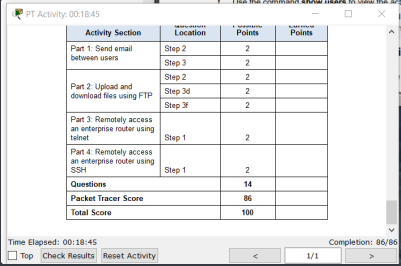


**Accounting**

Bij Windows komt dit overeen zoals in Linux, dit kan terug gevonden worden in het venster van taakbeheer in plaats van de terminal.



# 2.5: Extra opdracht



|  |  |  |  |
| --- | --- | --- | --- |
| Persoon | Done | Doing | Problems |
| Vicky | 2.5 | / | / |
| Bram | 2.1 – 2.2 | / | / |
| Vincent | 2.3 - 2.4 | / | / |
| Igor | 2.6 – 2.7 | / | / |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Persoon | Opdrachten | Tijd 1 | Tijd 2 | Totaal |
| Vicky | 2.5, 2.1, 2.3, 2.4 | 40 min | 6 uur | 6.40 uur |
| Igor | 2.6, 2.7, 2.2 | 1 uur | 5 uur | 6 uur |
| Bram | 2.1, 2.2 | 2.30 uur | 2 uur | 4.30 uur |
| Vincent | 2.3 – 2.4 | 1 uur | 30 min | 1.30 uur |

Er waren problemen met de samenstelling van het document alsook ontbrekende en een aantal foutieve delen in oefeningen. Dit hebben Vicky en Igor vooral voor hun rekening genomen met hulp van Bram. Vincent heeft meer inzet getoond dan bij de vorige opdracht maar ondanks dit heeft Vicky zijn oplossing nog steeds moeten nakijken en moeten aanpassen/aanvullen. Zou het misschien mogelijk zijn eerder individueel punten te geven sinds wij opdrachten aan elkaar toewijzen?want we horen deze steeds aan te passen omdat het 1 wat minder is dan het andere. Dit was ook het geval bij de presentatie, Vincent was niet voorbereid en had weinig inzet getoond en wij vermoeden dat door zijn minieme inbreng het algemeen cijfer lager lag.