

## Bijlage informatie en opdrachtenformulier

### Opdracht 2 onderdelen:

#### 1. Firewall log:

##### Begin log:

#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tpack tcpwin  
icmptype icmpcode info path

```
2022-06-09 13:07:37 ALLOW UDP 172.16.20.12 172.16.20.11 55818 53 0 - - - - - RECEIVE
2022-06-09 13:07:37 ALLOW UDP 172.16.20.11 192.36.148.17 58962 53 0 - - - - - SEND
2022-06-09 13:07:38 ALLOW UDP 172.16.20.12 172.16.20.11 50267 53 0 - - - - - RECEIVE
2022-06-09 13:07:40 ALLOW UDP 172.16.20.11 202.12.27.33 58962 53 0 - - - - - SEND
2022-06-09 13:07:41 ALLOW UDP 172.16.20.11 192.203.230.10 57598 53 0 - - - - - SEND
2022-06-09 13:07:44 ALLOW UDP 172.16.20.11 192.228.79.201 58962 53 0 - - - - - SEND
2022-06-09 13:07:44 ALLOW UDP 172.16.20.11 192.33.4.12 58962 53 0 - - - - - SEND
2022-06-09 13:07:44 ALLOW UDP 172.16.20.11 202.12.27.33 57598 53 0 - - - - - SEND
2022-06-09 13:07:48 ALLOW UDP 172.16.20.11 192.228.79.201 57598 53 0 - - - - - SEND
2022-06-09 13:07:37 ALLOW UDP 172.16.20.11 192.36.148.17 58962 53 0 - - - - - SEND
2022-06-09 13:07:38 ALLOW UDP 172.16.20.12 172.16.20.11 50267 53 0 - - - - - RECEIVE
2022-06-09 13:07:40 ALLOW UDP 172.16.20.11 202.12.27.33 58962 53 0 - - - - - SEND
2022-06-09 13:07:41 ALLOW UDP 172.16.20.11 192.203.230.10 57598 53 0 - - - - - SEND
2022-06-09 13:07:38 ALLOW UDP 37.235.128.2 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:40 ALLOW UDP 37.235.128.3 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:42 ALLOW UDP 37.235.128.2 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:44 ALLOW UDP 37.235.128.25 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:46 ALLOW UDP 37.235.128.2 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:48 ALLOW UDP 37.235.128.2 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:50 ALLOW UDP 37.235.128.2 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:52 ALLOW UDP 37.235.128.25 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:54 ALLOW UDP 37.235.128.2 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:38 ALLOW UDP 37.235.128.2 172.16.20.11 1024 1024 0 - - - - - RECEIVE
2022-06-09 13:07:48 ALLOW UDP 172.16.20.11 192.33.4.12 57598 53 0 - - - - - SEND
2022-06-09 13:07:57 ALLOW UDP 172.16.20.11 172.16.20.11 59546 53 0 - - - - - SEND
2022-06-09 13:07:57 ALLOW UDP 172.16.20.11 172.16.20.11 59546 53 0 - - - - - RECEIVE
2022-06-09 13:07:57 ALLOW TCP 172.16.20.11 172.16.20.12 55772 135 0 - 0 0 0 - - - SEND
2022-06-09 13:07:57 ALLOW TCP 172.16.20.11 172.16.20.12 55773 62141 0 - 0 0 0 - - - SEND
2022-06-09 13:07:57 ALLOW TCP 172.16.20.11 172.16.20.12 55774 135 0 - 0 0 0 - - - SEND
2022-06-09 13:07:57 ALLOW TCP 172.16.20.11 172.16.20.12 55775 62141 0 - 0 0 0 - - - SEND
2022-06-09 13:07:59 ALLOW ICMP 172.16.20.11 172.16.20.11 - - 0 - - - - 8 0 - SEND
2022-06-09 13:07:59 ALLOW ICMP 172.16.20.11 172.16.20.11 - - 0 - - - - 8 0 - RECEIVE
2022-06-09 13:07:59 ALLOW TCP ::1 ::1 55776 135 0 - 0 0 0 - - - SEND
2022-06-09 13:07:59 ALLOW TCP ::1 ::1 55776 135 0 - 0 0 0 - - - RECEIVE
2022-06-09 13:08:00 ALLOW TCP 172.16.20.11 172.16.20.11 55778 389 0 - 0 0 0 - - - SEND
2022-06-09 13:08:00 ALLOW TCP 172.16.20.11 172.16.20.11 55778 389 0 - 0 0 0 - - - RECEIVE
2022-06-09 13:08:00 ALLOW TCP 172.16.20.11 172.16.20.11 55780 389 0 - 0 0 0 - - - SEND
2022-06-09 13:08:00 ALLOW TCP 172.16.20.11 172.16.20.11 55780 389 0 - 0 0 0 - - - RECEIVE
2022-06-09 13:08:01 ALLOW ICMP 172.16.20.11 172.16.20.11 - - 0 - - - - 8 0 - SEND
2022-06-09 13:08:01 ALLOW ICMP 172.16.20.11 172.16.20.11 - - 0 - - - - 8 0 - RECEIVE
2022-06-09 13:08:04 ALLOW TCP 127.0.0.1 127.0.0.1 55782 389 0 - 0 0 0 - - - SEND
```

2022-06-09 13:08:04 ALLOW TCP 127.0.0.1 127.0.0.1 55782 389 0 - 0 0 0 - - - RECEIVE  
 2022-06-09 13:08:06 ALLOW TCP 172.16.20.11 172.16.20.11 55785 389 0 - 0 0 0 - - - SEND  
 2022-06-09 13:08:06 ALLOW TCP 172.16.20.11 172.16.20.11 55785 389 0 - 0 0 0 - - - RECEIVE  
 2022-06-09 13:08:06 ALLOW TCP 172.16.20.11 172.16.20.11 55786 389 0 - 0 0 0 - - - SEND  
 2022-06-09 13:08:06 ALLOW TCP 172.16.20.11 172.16.20.11 55786 389 0 - 0 0 0 - - - RECEIVE  
 2022-06-09 13:08:07 ALLOW TCP ::1 ::1 55787 445 0 - 0 0 0 - - - SEND  
 2022-06-09 13:08:07 ALLOW TCP ::1 ::1 55787 445 0 - 0 0 0 - - - RECEIVE  
 2022-06-09 13:08:12 ALLOW ICMP 127.0.0.1 127.0.0.1 - - 0 - - - - 8 0 - SEND  
 2022-06-09 13:08:12 ALLOW ICMP 127.0.0.1 127.0.0.1 - - 0 - - - - 8 0 - RECEIVE  
 2022-06-09 13:08:12 ALLOW ICMP 127.0.0.1 127.0.0.1 - - 0 - - - - 8 0 - SEND  
 2022-06-09 13:08:12 ALLOW ICMP 127.0.0.1 127.0.0.1 - - 0 - - - - 8 0 - RECEIVE  
 2022-06-09 13:08:29 ALLOW UDP 172.16.20.11 172.16.20.11 64920 53 0 - - - - - - SEND  
 2022-06-09 13:08:29 ALLOW UDP 172.16.20.11 172.16.20.11 64920 53 0 - - - - - - RECEIVE  
 2022-06-09 13:08:29 ALLOW UDP 172.16.20.11 192.36.148.17 57562 53 0 - - - - - - SEND  
 2022-06-09 13:08:30 ALLOW UDP 172.16.20.11 172.16.20.12 64920 53 0 - - - - - - SEND  
 2022-06-09 13:08:31 ALLOW UDP 172.16.20.11 8.8.8.8 64920 53 0 - - - - - - SEND  
 2022-06-09 13:08:33 ALLOW UDP 172.16.20.11 202.12.27.33 57562 53 0 - - - - - - SEND  
 2022-06-09 13:08:37 ALLOW UDP 172.16.20.11 192.228.79.201 57562 53 0 - - - - - - SEND  
 2022-06-09 13:08:37 ALLOW UDP 172.16.20.11 192.33.4.12 57562 53 0 - - - - - - SEND  
 2022-06-09 13:09:04 ALLOW TCP 127.0.0.1 127.0.0.1 55794 389 0 - 0 0 0 - - - SEND  
 2022-06-09 13:09:04 ALLOW TCP 127.0.0.1 127.0.0.1 55794 389 0 - 0 0 0 - - - RECEIVE

### **Eindlog**

## **2. Interview Mr. Ouwaardgee**

- Vraag 1: Hoe lang werkt u voor KAS?  
 Antwoord: Bijna 4 maanden, ik ben begonnen als stage, student van het ROCvA en mocht na mijn afstuderen hier blijven.
- Vraag 2: Bent u de enige Databasebeheerder?  
 Antwoord: Ja
- Vraag 3: Vind u het ook belangrijk dat een security Audit uitgevoerd door ons zal worden?  
 Antwoord: Ja, ik heb zelf niet heel veel kennis van Database security, want vaak denk ik dat er iets aan de hand is met de Database Server.
- Vraag 4: Ohw, hoe vaak en waarom denkt u dat?  
 Antwoord: Ik ben de enige die in de database kan, maar ik heb al 2 keer gezien dat er toch query's zijn uitgedraaid terwijl ik dat niet heb gedaan.
- Vraag 5: Weet u zeker dat u de enige bent die in de database kan inloggen?  
 Antwoord: Ja, ik ben wel de enige, echter vanwege personeelstekort heb ik het wachtwoord niet aangepast, mocht ik een keer ziek raken dan kan alsnog mijn college de database in.
- Vraag 6: Misschien heeft je collega wel die query's uitgedraaid?  
 Antwoord: Nee, wij hebben afgesproken als hij in de database moet inloggen dat het altijd gemeld moet worden. En dat is de afgelopen 3 maanden niet het geval geweest.
- Vraag 7: Wat voor gegevens zijn te vinden in jullie database?  
 Antwoord: NAW Klantgegevens, welke product zij bij ons hebben ingekocht, welke diensten afgenomen zijn, etc.
- Vraag 8: Die Query's die jij niet kan plaatsen, maar jij toch wel terug kan zien in de database log. Wat bevatten die Query's aan informatie?  
 Antwoord: Het lijkt wel een dump van de database met gegevens van onze klanten.
- Vraag 9: Weet je ook hoeveel records er dan opgevraagd zijn uit de database?  
 Antwoord: Ja, in de log is dat terug te zien.
- Vraag 10: Heb je dit wel vermeld aan je leidinggevende.  
 Antwoord: Nee, ik heb die uitdraai niet gemaakt dus niet mijn fout.

Vraag 11: Wat nou als het hier gaat om hack en bedrijfsdata dat weggelekt is naar externe partijen?  
 Antwoord: Ja lastig..

### 3. **Risico matrix**

Vul de risicomatrix in, maar vermeld eerst hieronder welke 3 afwijkingen/issues.

- 1) Afwijking: Een beschrijving van het gevonden issue
  - a. Details van het issue
  - b. Conclusie met impact
- 2) Afwijking: Een Beschrijving gevonden issue
  - a. Details van het issue
  - b. Conclusie met impact
- 3) Afwijking: Een Beschrijving gevonden issue
  - a. Details van het issue
  - b. Conclusie met impact

Beschrijf jouw conclusies/onderbouwing. Nummer de resultaten en zet ze in het schema.

Kans ↑	Risicomatrix			
	Impact →			

Uitleg kleuren Kans en Impact.

Groen is Laag

Geel is Gemiddeld

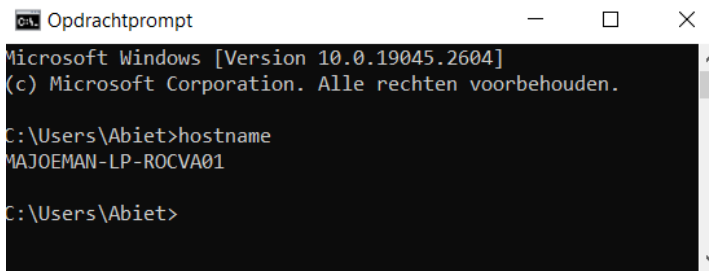
Orange is Bovengemiddeld

Rood is Ernstig

## Opdrachten/Invulformulier opdracht 1

### Tools gebruik:

Lever je printscreens waarop je gehele bureaublad te zien is.  
Je opent ook een dos box (cmd) waarop je pcnaam te zien is.  
Dit doe je als volgt, Windows toets, cmd, (enter)  
Typ de volgende commando in: hostname  
En je pcnaam zal getoond worden.



```
Microsoft Windows [Version 10.0.19045.2604]
(c) Microsoft Corporation. Alle rechten voorbehouden.

C:\Users\Abiet>hostname
MAJOEMAN-LP-ROCVA01

C:\Users\Abiet>
```

Je levert dus 3 printscreens. Van MBSA, NMAP en Proceschecker.  
Van NMAP levert je 1 printscreen waarop de 2 poorten staan waarvan er ook aangegeven moet worden voor welke protocol/programma de poorten gebruikt worden.

- Printscreen MBSA:
- Printscreen NMAP:
- Printscreen Sysinternals > Proceschecker:  
Uitleg Proceschecker 2 poorten die open staan:

### Firewall log analyseren:

Wat is je opgevallen aan de log:

### Adviesrapport n.a.v. interview:

Beschrijf niet gewenste handelingen van de databasebeheerder.  
Maak ook een adviesrapport om de niet gewenste handelingen te stoppen. Je beschrijft duidelijk wat er aangepast dient te worden. Als er technische handelingen aangebracht moeten worden dan vermeld je stap voor stap hoe dit doorgevoerd moet worden:

### Maak een risico matrix

Lever een risico matrix van 3 afwijkingen en onderbouw je keuze.

Kans ↑	Risicomatrix		
Impact →			

Onderbouwing afwijking 1:  
Onderbouwing afwijking 2:  
Onderbouwing afwijking 3:

## Opdracht 3 onderdelen:

### 3.1. Uitsnede van databaselek. Vind in de log de databaselek en onderbouw waarom het om een databaselek gaat.

```
2022-06-07T14:03:22.152020Z 9 Query show character set where charset = 'utf8mb4'
2022-06-07T14:03:22.160165Z 9 Query SET NAMES 'utf8mb4'
2022-06-07T14:03:22.164496Z 9 Query SHOW SESSION STATUS LIKE 'Ssl_cipher'
2022-06-07T14:03:22.175642Z 9 Query USE 'apotheek'
2022-06-07T14:03:22.176530Z 9 Query set autocommit=1
2022-06-07T14:03:22.180315Z 10 Connect root@localhost on using TCP/IP
2022-06-07T14:03:22.180749Z 10 Query set autocommit=1
2022-06-07T14:03:22.181132Z 10 Query SELECT current_user()
2022-06-07T14:03:22.183258Z 10 Query SET CHARACTER SET utf8
2022-06-07T14:03:22.183660Z 10 Query SET NAMES utf8
2022-06-07T14:03:22.183929Z 10 Query SET SQL_SAFE_UPDATES=1
2022-06-07T14:03:22.184322Z 10 Query SELECT CONNECTION_ID()
2022-06-07T14:03:22.184725Z 10 Query show character set where charset = 'utf8mb4'
2022-06-07T14:03:22.186794Z 10 Query SET NAMES 'utf8mb4'
2022-06-07T14:03:22.187321Z 10 Query SHOW SESSION STATUS LIKE 'Ssl_cipher'
2022-06-07T14:03:22.189638Z 10 Query USE 'apotheek'
2022-06-07T14:03:22.189935Z 10 Query set autocommit=1
2022-06-07T14:03:22.190360Z 10 Query SHOW SESSION VARIABLES LIKE 'sql_mode'
2022-06-07T14:03:22.197608Z 10 Query SHOW SESSION VARIABLES LIKE 'version_comment'
2022-06-07T14:03:22.201995Z 10 Query SHOW SESSION VARIABLES LIKE 'version'
2022-06-07T14:03:22.204790Z 10 Query SELECT current_user()
2022-06-07T14:03:22.205147Z 10 Query SHOW SESSION VARIABLES LIKE 'lower_case_table_names'
2022-06-07T14:03:23.078974Z 9 Query SHOW DATABASES
2022-06-07T14:03:23.087182Z 10 Query show engines
2022-06-07T14:03:23.090034Z 10 Query show charset
2022-06-07T14:03:23.092672Z 10 Query show collation
2022-06-07T14:03:23.101004Z 10 Query show variables
2022-06-07T14:03:23.105527Z 10 Query SHOW SESSION VARIABLES LIKE 'version_compile_os'
2022-06-07T14:03:23.107371Z 10 Query SHOW SESSION VARIABLES LIKE 'offline_mode'
2022-06-07T14:03:23.145497Z 10 Query SHOW SESSION VARIABLES LIKE 'wait_timeout'
2022-06-07T14:03:23.151599Z 10 Query SHOW SESSION VARIABLES LIKE 'interactive_timeout'
2022-06-07T14:03:24.795789Z 9 Query SHOW FULL TABLES FROM 'apotheek'
2022-06-07T14:03:24.814249Z 9 Query SHOW PROCEDURE STATUS WHERE Db='apotheek'
2022-06-07T14:03:24.845482Z 9 Query SHOW FUNCTION STATUS WHERE Db='apotheek'
2022-06-07T14:03:24.851656Z 10 Query SHOW FULL COLUMNS FROM 'apotheek'.gasten
2022-06-07T14:03:24.859973Z 10 Query SHOW FULL COLUMNS FROM 'apotheek'.medicijnen
2022-06-07T14:03:24.867911Z 10 Query SHOW FULL COLUMNS FROM 'apotheek'.medicijngebruik
2022-06-07T14:03:24.972940Z 10 Query select distinct gasten.voornaam, gasten.achternaam, medicijnen.atclaatst, medicijnen.atclaatst_naam_tekst, gasten.email from medicijngebruik
inner join medicijnen on medicijngebruik.atclaatst = medicijnen.atclaatst
inner join gasten on medicijngebruik.gast_id = gasten.gast_id
Order by achternaam
LIMIT 0, 1000
2022-06-07T14:03:42.165885Z 9 Query SELECT st.* FROM performance_schema.events_statements_current st JOIN performance_schema.threads thr ON thr.thread_id = st.thread_id WHERE thr.processlist_id = 10
2022-06-07T14:03:42.193014Z 9 Query SELECT st.* FROM performance_schema.events_stages_history_long st WHERE st.nesting_event_id = 36
2022-06-07T14:03:42.198695Z 9 Query SELECT st.* FROM performance_schema.events_waits_history_long st WHERE st.nesting_event_id = 36
2022-06-07T14:04:53.578809Z 9 Quit
2022-06-07T14:04:53.578948Z 9 Quit
C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqld.exe, Version: 8.0.29 (MySQL Community Server - GPL). started with:
TCP Port: 3306, Named Pipe: MySQL
Time Id Command Argument
C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqld.exe, Version: 8.0.29 (MySQL Community Server - GPL). started with:
TCP Port: 3306, Named Pipe: MySQL
Time Id Command Argument
```

De bovenstaande uitsnede van de database log is gevonden via:

Administration - Server Logs

Local instance MySQL80

Server Logs

Error Log File General Log File Slow Log File

Timestamp	Thread	Command	Detail
2023-03-17 13:29:02.05...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:05.06...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:08.08...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:11.09...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:14.10...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:17.11...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:20.12...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:23.13...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:26.14...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:29.15...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:32.16...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:35.17...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:38.18...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:41.19...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:44.21...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:47.22...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:50.23...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:53.24...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:56.25...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:29:59.26...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:02.28...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:05.29...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:08.30...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:11.31...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:14.32...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:17.33...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:20.34...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:23.35...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:26.37...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:29.38...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:32.39...	12	Query	SHOW GLOBAL STATUS
2023-03-17 13:30:35.40...	12	Query	SHOW GLOBAL STATUS

Log File Location: C:\ProgramData\MySQL\MySQL Server 8.0\Data\SRV002.log

Showing: 1109 records starting at byte offset 160144

### 3.2. Communiceren van de datalek.

Hoe, wat en naar wie communiceer je als er sprake is van een datalek.

Zie o.a. deze site: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken>

Zie communicatiematrix, vermeld hoe, wat en naar wie je gaat communiceren:

	Gevonden zwakheden	Beschrijving gevonden bewijzen	Inhoudelijk gevonden bewijzen	Aangebrachte aanpassingen	Bericht mogelijk datalek
Opdrachtgever					
Security-officer van Kas					
Directie van Kas					
Lokale media					
Nationale media					
Meldloket datalekken					
Politie					
De IT-afdeling van Kas					
De Marketing van Kas					
De receptie van Kas					

Je mag het internet gebruiken wanneer je wel/niet moet communiceren.