

**EKSAMEN FOR CYB 2100 - CYBERFORSVAR**

**HØYSKOLEN KRISTIANIA**

**HØSTEN 2022**

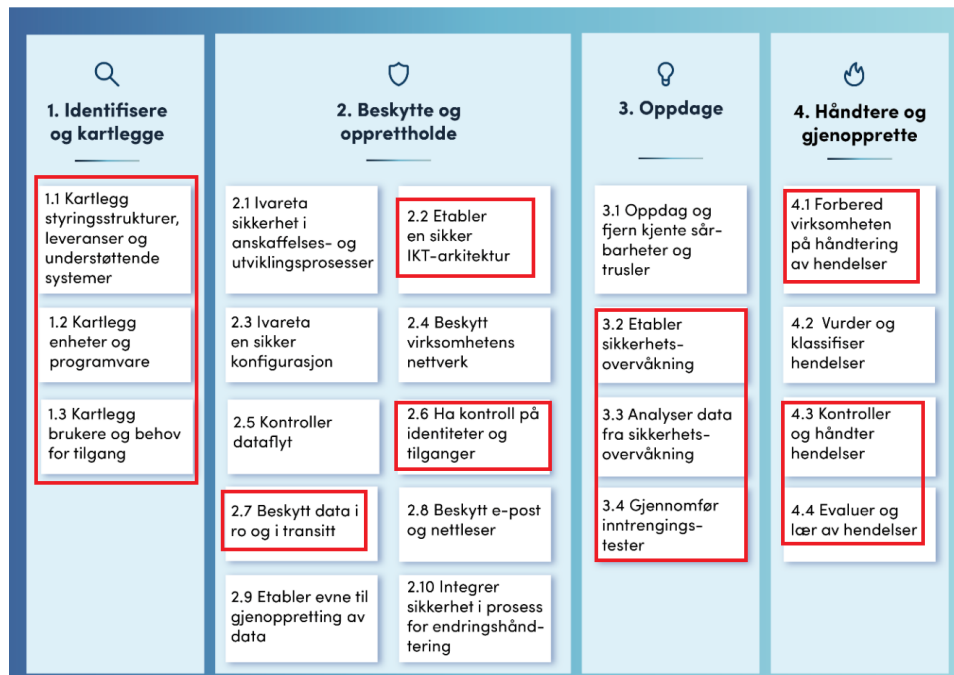
**KANDIDAT 1041**

OPPGAVE 1 .....	3
1.a).....	3
1. IDENTIFISERE OG KARTLEGGE .....	3
2. BESKYTTE OG OPPRETTTHOLDE .....	4
3. OPPDAGE .....	5
4. HÅNDTERE OG GJENOPPRETTE .....	5
1.b).....	6
1.c).....	6
Oppgave 2.....	7
2.a).....	7
2.b).....	7
2.c).....	9
Oppgave 3.....	9
3.a).....	9
3.b).....	10
3.c).....	11
3.d).....	11
Metodikk .....	12

# OPPGAVE 1

1.a)

Ifølge min evaluering utgjør disse prinsippene best effekt:



Hentet fra NSM<sup>1</sup>

Om full oppfølging av NSMs grunnprinsipper oppnår en god balanse i CIA-modellen; så blir følgende hovedformål å unngå at tilgjengelighet svekker konfidensialitet.

## IDENTIFISERE OG KARTLEGGE

Første kategori gav ingen valg, men alle tre punktene er kritiske for videre håndtering av virksomhetens sikkerhet. Formålet er grovt sett å identifisere bevisste og ubevisste sikkerhetsbrudd. Følgende mål er basert på punkt 1.1, 1.2 og 1.3 i NSMs grunnprinsipper og egne evalueringer<sup>2</sup>:

- Identifiser virksomhetens strategi og prioriterte mål
  - Retningslinjer for behov av godkjente IKT-produkter
    - Kartlegge ønsker og nødvendighet ift. lovlig bruk
    - Etabler oversikt over integrering av produkter og mennesker ifm. partnere
- Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.
  - Kartlegg firmware, OS, servere, applikasjoner og andre IKT-produkter
    - Implementasjonsplan før integrering av produkter
      - Etabler en arkitektur
        - Definer brukerkategorier, ansvar og roller knyttet til tilgangsnivåer
          - Eks: Administrasjon/HR, leverandører, salgsteam, konsulenter, internt/eksternt etc...

<sup>1</sup> Nasjonal Sikkerhetsmyndighet (i.d.), Grunnprinsipper For IKT-Sikkerhet Versjon 2.0, <https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf>, s. 7

<sup>2</sup> Nasjonal Sikkerhetsmyndighet (i.d.), Grunnprinsipper For IKT-Sikkerhet Versjon 2.0, <https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf>, s. 11, s. 12, s. 14, s. 15, s.16, s.17

- Kontroller identiteter og tilgang
- Identifiser virksomhetens prosesser for risikostyring knyttet til IKT
  - Identifiser naturen av virksomheten i markedet
    - Identifiser potensielle og reelle aktører i markedet
      - Identifiser motivasjonsfaktorer for angrep mot virksomheten

### BESKYTTE OG OPPRETTOLDE

Andre kategori tjener hovedformålet best om punkt 2.2, 2.6 og 2.7 er valgt. Dette utelukker mange av mulighetene for fleksibilitet i strukturen, som noen andre punkter tar hensyn til. Følgende funksjoner bør implementeres og er en blanding av øvrige punkter fra NSM og egne evalueringer<sup>3</sup>:

- Funksjonalitet for å styre brukere og kontoer. Forhindre angrep ute- og innenfra.
  - Retningslinjer for tilgangskontroll og opplæring av ansatte.
    - Knytte privileger til roller og minimer eksponering av rettigheter.
  - Gjenbruk av identiteter mest mulig på tvers av systemer.
    - "Single sign on" og MFA
  - Logg funksjonalitet, som kan spores.
  - Revideres jevnlig
- Funksjonalitet for å ha kontroll og oversikt på enheter (f.eks. klienter)
  - Implementasjon av nettversk-soner
  - Minimer og kontroller medbrakte enheter
    - Sikker "bring your own device" policy
  - Reguler tilgang til tjenester basert på kjennskap til både brukere og enhet
- Funksjonalitet for å styre tilgang til ressurser og tjenester
  - Helst med ett verktøy som gjerne holde styr på dette og øvrige punkt.
  - Reguler tilgang til tjenester basert på kjennskap til både brukere og enhet
- Funksjonalitet for å ha kontroll på programvare
  - Klienter bør holdes adskilt fra virksomhetens servere
- Operativsystemer
  - Sporbar logging
  - Etabler en formell prosess for administrasjon av kontoer, tilganger og rettigheter
- Verktøy for drift og virtualisering av hele eller deler av IKT-arkitekturen («on-prem» og «sky»)
  - Etabler risikoprofil
  - Drift av soner bør skje sentralt (ikke lokalt på hver svitsj).
- Nettverksenheter (svitsjer, rutere, aksesspunkter) og brannmurer
  - Kritiske del-nettverk må skilles fysisk
  - Del opp domenearkitektur og nettverk iht. virksomhetens behov og risiko
- Mekanismer for å håndtere skadevare (antivirus)
- Kryptografiske moduler
  - Sikker nøkkelgenerering

---

<sup>3</sup> Nasjonal Sikkerhetsmyndighet (i.d.), Grunnprinsipper For IKT-Sikkerhet Versjon 2.0, <https://nsm.no/getfile.php/133735-1592917067/NSM/Files/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf>, s. 21, s. 22, s. 23, s.30, s. 31, s. 32, s. 33

- Common Criteria, FIPS 140-2<sup>4</sup>
    - Beskytt data i transitt og i ro
    - Definer kritiske volumer, enheter og filer som skal beskyttes
- Digitale sertifikater og Public Key Infrastructure (PKI)
  - Definer sårbare kanaler for sending av data
    - Hvilket nivå?
      - Applikasjonslaget (TLS)
        - Nettverkslaget (IPsec)
          - Datalinklaget (MACsec)
- Verktøy for systemovervåkning
  - Wireshark
- Verktøy for styring av sikkerhetskonnfigurasjoner
  - Bør skje sentralt og likt per type enhet
    - Minimere dobbeltarbeid og menneskelige uregelmessigheter
- Sikkerhetskopiering og gjenoppretting
  - Ivareta tilgjengeligheten av kritiske data
    - Risiko for data-angrep, driftsfeil, naturskade og geopolitisk situasjon ...
      - Backup av internett og elektrisitet forbindelse, dupliser datasenter på alternativ lokasjon, alternativ lagring ...
- Bygg IKT-systemet med IKT-produkter som fungerer godt sammen sikkerhetsmessig
  - Sikker samhandling mellom APIer
- Sett opp "out of band" infrastruktur

Herding er ett viktig konsept i den totale informasjonssikkerheten. Dette gjelder for alle overnevnte IKT-produkter.

### OPPDAGE

Tredje kategori utelater punkt 3.1. Formålet er mindre avhengighet av automatisert teknologi, og mer kompetanserettet handling. Avgjør hva som skal overvåkes, filtrer sikkerhet relevans, bevar integriteten av analysert data og etabler retningslinjer ift. lovverk. Forbered og vær bevisst på utfordringen av å filtrere diverse alarmtyper i forbindelse med falsk positiv og reelle hendelser. Implementasjon av Intrusion detection (IDS) og protection (IPS) systemer som Suricata (integrerbar med Splunk). Utfør penetrasjonstester med tydelige mål og omfang, med og uten automatiserte verktøy som GVM (Greenbone Vulnerability Management).

### HÅNTERE OG GJENOPPRETTE

Fjerde kategori utelater punkt 4.2. Etter min evaluering kan selskapet nedprioritere dette punktet på grunn av virksomhetens størrelse. Formålet er å kunne håndtere angrep et lite selskap potensielt kan gjennomgå. Unnlattelse av punkt 4.2 forutsetter flittig bruk av tilgjengelig kunnskap allerede i bruk (eks: MITRE). Denne kategorien er skillet mellom virksomhetens død eller overlevelse, og det første kommer av lite prioritering av gjenopprettelse.

---

<sup>4</sup> Datatilsynet (24. januar, 2012), Kryptering, <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonsikkerhet-internkontroll/kryptering/>

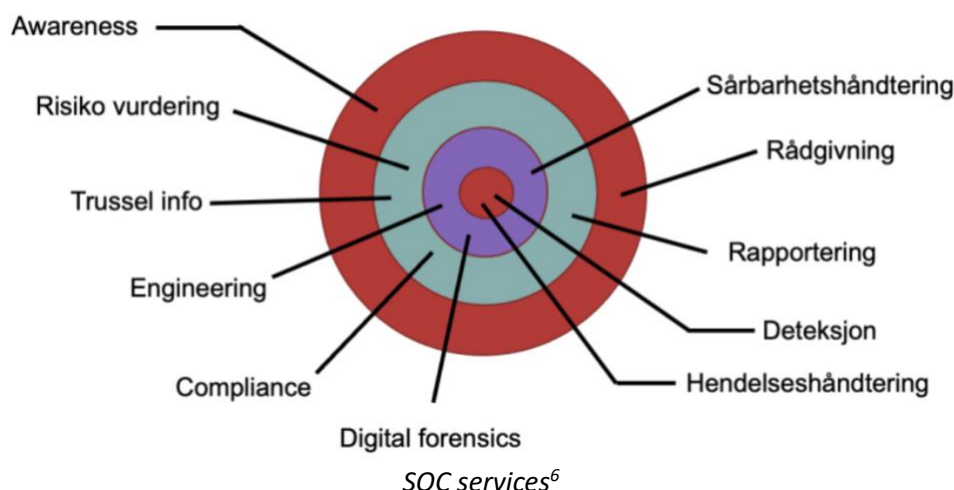
## 1.b)

Motstandsdyktigheten (og eneste virkemiddel) mot ransomware, krever forståelse av hver enkelt hendelse (ingen "silver bullet") og god planlegging<sup>5</sup>. Skadevaren trenger en inngangsvektor (ofte epost/vedlegg), målet er å få kjørt ondsinnet kode på verten. Med dette i tankene blir tiltakene:

- **Backup**
  - Offline content - gjerne backup på en "out of band" arkitektur.
- **Implementasjon av IAM**
  - Gjerne på alle nivåer av systemet for alle brukere
  - Eventuelt så kan Zero Trust Architecture kan være et langsiktig mål
- **Opplæring av ansatte**
  - Følge stramme policyer og gjennomtenkte rutiner før og ved innvirkning

## 1.c)

Begrunnelsen min bruker følgende bilde som utgangspunkt:



En CISO er en senior utøvende posisjon som overser virksomhetens informasjonssikkerhet<sup>7</sup>. Ofte må en CISO rapportere videre til en CTO/CSO/CRO/COO/CEO. Med dette inkludert i tankene passer disse valgene ifølge min evaluering:

### 1. Deteksjon

#### a. Viktighet i å oppdage hendelser før og etter innvirkning

##### i. Bruk av SIEM for å gjenkjenne potensielle trusler og sårbarheter

1. Standard i dag å benytte AI og machine learning for avansert bruker og entitet analyse<sup>8</sup>

### 2. Hendelseshåndtering

#### a. Viktighet i å respondere på hendelsene man oppdager

<sup>5</sup> Henrik Ramberg (26. oktober, 2022), Lesson 8.2, <https://kristiania.cloud.panopto.eu/Panopto/Pages/Viewer.aspx?id=31393ecb-bfe4-4a29-b214-af34011da44e&query=silver%20bullet&start=1986.411>, minutt 33:00 - 33:06

<sup>6</sup> Henrik Ramberg (i.d.), SOC Services, [https://kristiania.instructure.com/courses/9527/files/938455?module\\_item\\_id=337125](https://kristiania.instructure.com/courses/9527/files/938455?module_item_id=337125), s. 5

<sup>7</sup> CISCO (i.d.), What is CISO?, <https://www.cisco.com/c/en/us/products/security/what-is-ciso.html>

<sup>8</sup> IBM (i.d.), What is Siem?, <https://www.ibm.com/topics/siem>

- i. Typiske aktiviteter man finner i hendelseshåndtering<sup>9</sup>:
    - 1. Forberedelse
    - 2. Identifisering
    - 3. Skadebegrensning
    - 4. Rense/utslette
    - 5. Gjenopprettelse
    - 6. Lære
  - ii. Gjerne kunne respondere på tvers av IKT-plattformer
- 3. Sårbarhetshåndtering
  - a. Håndtering av nøkkelinformasjon
    - i. Minimere tiden fra sårbarhetsoppdagelse (lokalt og offentlig) til håndtering
    - ii. Minimere håndteringstid. Spesielt kritiske funn.
    - iii. Minimer tiden for patching av ukjente sårbarheter internt
    - iv. Minimer antall ganger en sårbarhet inntreffer og på hvilken gruppe eller enhet
      - a. Overnevnte punkter gjenspeiler virksomhetens effektivitet og risikobilde (KPI).
- 4. Rapportering
  - a. Analyse og presentasjon av beregninger (metrics).
    - i. Slik at virksomheten og overordnede kan kartlegge og se fremgang.
  - b. Rapportering av SOC modenhet.

## Oppgave 2

### 2.a)

Splunk har tre hovedkomponenter:

- 1. Forwarder
  - a. Et middel som kan kjøres i IT systemet som samler data og sender det til "Indexer"
    - i. Universal Forwarder - sender rå data videre.
    - ii. Heavy Forwarder - analyserer og indekserer kilde data før videresending
- 2. Indexer
  - a. Transformerer og indekserer data til eventer som kan søkes på av "Search Head"
    - i. Separerer data i "buckets"
- 3. Search Head
  - a. En UI som klienter kan bruke til å interagere med Splunk.
    - i. Kan kjøre søk og spørringer
    - ii. Tilbyr distribuert søkearkitektur som tillater håndtering av enorme datamengder.

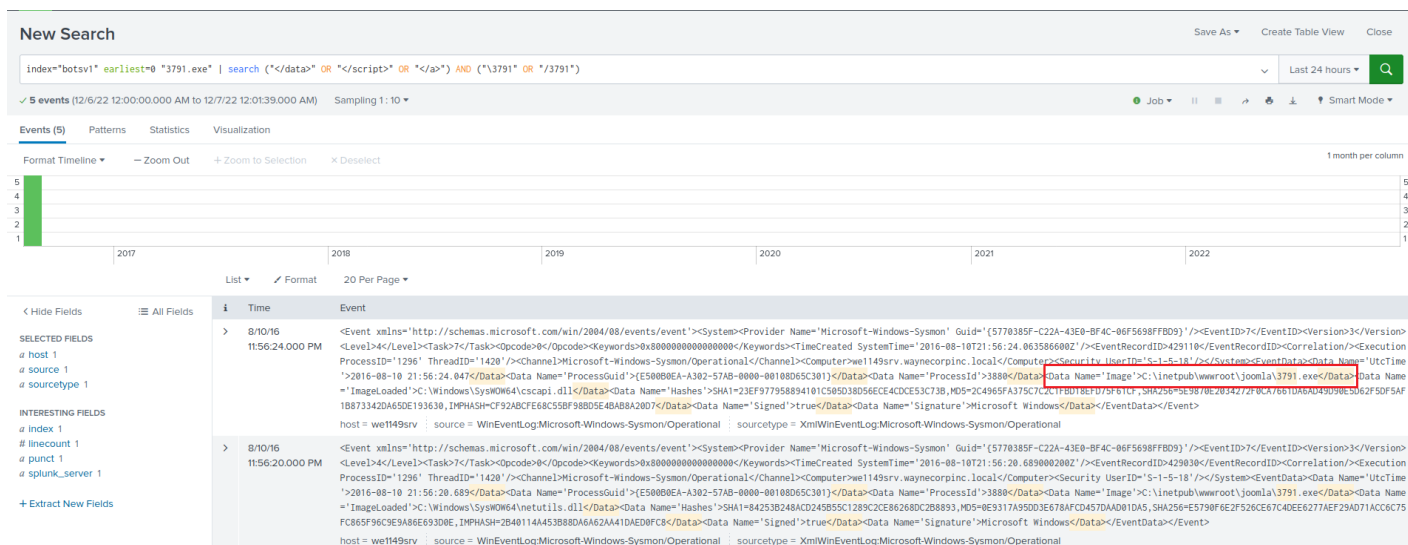
### 2.b)

- Path til 3791 på serveren er: "C:\inetpub\wwwroot\joomla\3791.exe".

---

<sup>9</sup> Henrik Ramberg (i.d.), Hendelseshåndtering,

[https://kristiania.instructure.com/courses/9527/files/938455?module\\_item\\_id=337125](https://kristiania.instructure.com/courses/9527/files/938455?module_item_id=337125), s. 8



| search ("</data>" OR "</script>" OR "</a>") AND ("3791" OR "/3791")

Følgende tanker og handlinger ble gjort for å finne filens sti:

- ".exe" er en filnavn-utvidelse for kjørbare filer i operativ systemer fra Microsoft.
  - Filen ble sendt over HTTP, og den må inneholde linken til den kjørbare filen. Da å kjøre en kjørbare fil direkte i HTML ikke er tillatt<sup>10</sup>. Typisk sett bruker man `<a>`, `<data>` eller `<script>` for formålet, der `<data>` tillater friere tøyler for spesielle formater<sup>11</sup>. Alle tager må lukkes.
- Slashen "\" brukes av Microsoft for å skille kataloger/folder og UNIX systemer bruker "/". Filen er sannsynligvis i en folder i ett filsystem.
- Begrenser resultater videre med event sampling på 1:10.
- Ut ifra overnevnte path:
  - "\inetpub" er en standardfolder i Microsoft Internet Information Services (IIS)<sup>12</sup>
  - "\wwwroot" er en folder relatert til ASP.NET, en open source rammeverk for web utvikling<sup>13</sup>.
  - "\joomla" er en open source "Content Management System" (CMS) for web utvikling<sup>14</sup>
  - Kombinasjonen av overnevnte stier er typisk i en windows server på et windows operativ system.
- Denne praktiseringen av å skjule eller representere noe inni noe annet kalles for steganografi<sup>15</sup>. Det er vanskelig å behandle og oppdage konsekvensene etter innvirkning. Følgende barrierer bør implementeres<sup>16</sup>:
  - Endpoint protection platform (EPP)
    - Proaktiv tilnærming

<sup>10</sup> Dorgelo, W. (23. november, 2010), <https://stackoverflow.com/questions/4252913/open-an-exe-file-through-a-link-in-a-html-file>

<sup>11</sup> Javatpoint (i.d.), HTML Data Tag, <https://www.javatpoint.com/html-data-tag>

<sup>12</sup> Microsoft (10. mars, 2022), IIS 8.0 Using ASP.NET 3.5 and ASP.NET 4.5, <https://learn.microsoft.com/en-us/iis/get-started/whats-new-in-iis-8/iis-80-using-aspnet-35-and-aspnet-45#:~:text=will%20be%20at-,c%3A%5Cinetpub,-%5Cwwwroot>

<sup>13</sup> Microsoft (i.d.), What is ASP.NET?, <https://dotnet.microsoft.com/en-us/learn/aspnet/what-is-aspnet>

<sup>14</sup> Microsoft (19. mai, 2022), Joomla! FAQ, <https://learn.microsoft.com/en-us/iis/develop/installingpublishing-apps-with-webmatrix/joomla-faq>

<sup>15</sup> Store norske leksikon (17. desember, 2021), Steganografi, <https://snl.no/steganografi>

<sup>16</sup> CrowdStrike (9. februar, 2022), EPP vs. EDR, <https://www.crowdstrike.com/cybersecurity-101/endpoint-security/epp-vs-edr/>



- Gjerne flere atferdsmessige oppdagelsesmetoder
  - Endpoint detection and response (EDR)
    - Reaktiv tilnærming
      - Oppdager og responderer på hva EPP ikke fikk med seg.

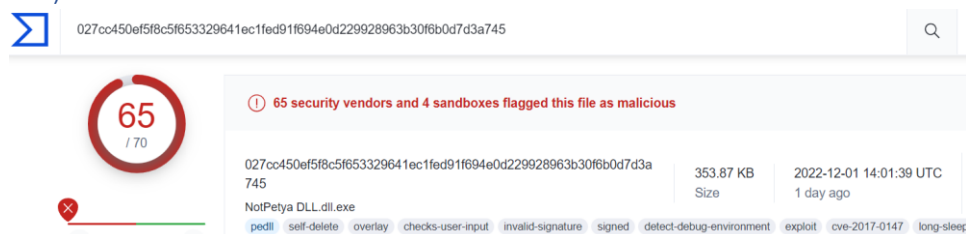
## 2.c)

Hovedfordelene MS Sentinel har overfor Splunk:

- Høyere affinitet til Microsoft produkter
- Integrert i skyløsningen Azure
- Bruker ikke spørringer på søk. Lettere å bruke.
- Mer fleksibel pris<sup>17</sup>

## Oppgave 3

### 3.a)



Følgende analyse er funnet i CISAs varslingside<sup>18</sup>:

NotPetya er en variant av Petya skadevaren som krypterer fil-utvidelser av en hardkodet liste. Denne skadevaren krypterer også "Master Boot Record" (hovedpartisjonssektor, MBR), hvis den får tak i admin rettigheter. Dette gjør den infiserte maskinen ubrukelig. NotPetya er annerledes ift. sine forgjengere i måten den forplanter seg. Følgende punkter beskriver skadevarens egenskaper:

- Benytter "Lateral Movement" teknikker
  - PsExec - et lovlig Windows administrasjonsverktøy
  - WMI - et lovlig Windows komponent
  - EternalBlue - den samme Windows SMBv1 exploit brukt i WannaCry
  - EternalRomance - en annen Windows SMBv1 exploit
- Krypterer filer med en dynamisk generert 128-bit (AES) nøkkel og lager en unik ID av offeret.
  - Ingen relasjon mellom generert nøkkel og offerets ID
    - Mer destruerende enn i en typisk ransomware situasjon
- Forplanter seg i et nettverk ved bruk av en modifisert versjon av Mimikatz
  - stjeler legitimasjon og bruker et av overnevnte LM teknikker til å få adgang andre steder i nettverket
- Ved innvirkning skriver skadevaren en tekst dokument i "C:\\" som inkluderer en statisk lommebok lokasjon for Bitcoin, samt en unik nøkkel for bruk under betaling.

NotPetya ble brukt mot en ukrainsk programvare for skatteregnskap (M.E.Doc), 27.juni.2017.

Produktet ble rammet av en bakdør i utviklingsmiljøet siden 14.april det samme året. Denne bakdøren muliggjorde blant annet bruk av vilkårlig kode og kommandoer, samt uautoriserte filoverføringer.

<sup>17</sup> Gartner (i.d.), Microsoft Sentinel vs Splunk Enterprise Security, <https://www.gartner.com/reviews/market/security-information-event-management/compare/product/microsoft-sentinel-vs-splunk-enterprise-security>

<sup>18</sup> CISA (1. july, 2017), Alert (TA17-181A), <https://www.cisa.gov/uscert/ncas/alerts/TA17-181A>

NotPetya er lenket til russiske ondsinnede cyber aktiviteter, definert av USAs RIS Group som "Grizzly Steppe". Russiske grupper som APT28, APT29 og Fancy Bear er mistenkte navn av RIS<sup>19</sup>. Skadevaren inneholder også kode tilsvarende det som er i Mimikatz<sup>20</sup>.

### 3.b)

Følgende MD5 sum ble oppgitt av nedlastet fil: 723b780905a9cc8529f645a117b1c09c. Ved dobbeltsjekk, stemte dette ikke ...

```
sansforensics@siftworkstation: ~/Documents
$ md5sum IE10WIN7-20221114-202804.raw
23e1eef47016b22b4b501bae3132aaf9  IE10WIN7-20221114-202804.raw
```

Volatility ble brukt på følgende måte:

```
sansforensics@siftworkstation: ~/Documents
$ volatility imageinfo -f IE10WIN7-20221114-202804.raw
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/sansforensics/Documents/IE10WIN7-20221114-202804.raw)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82942de8L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x80b97000L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2022-11-14 20:28:16 UTC+0000
      Image local date and time : 2022-11-14 12:28:16 -0800
```

```
sansforensics@siftworkstation: ~/Documents
$ volatility -f IE10WIN7-20221114-202804.raw hivelist --profile=Win7SP1x86_23418
Volatility Foundation Volatility Framework 2.6.1
Virtual Physical Name
-----
0x91804950 0x1fbaa950 \Device\HarddiskVolume1\Boot\BCD
0x9180e008 0x20d70008 \SystemRoot\System32\Config\SOFTWARE
0x91820688 0x1bcf6688 \??\C:\Windows\System32\Config\COMPONENTS
0xa0085330 0x1efee330 \??\C:\System Volume Information\Syscache.hve
0xa0194540 0x13895540 \??\C:\Users\sshd_server\ntuser.dat
0x8201a008 0x1301a008 \??\C:\Users\sshd_server\AppData\Local\Microsoft\Windows\UsrClass.dat
0x87c0e308 0x280dd308 [no name]
0x87c1a008 0x2806b008 \REGISTRY\MACHINE\SYSTEM
0x87c439c8 0x27fd69c8 \REGISTRY\MACHINE\HARDWARE
0x87cb79c8 0x1abfe9c8 \SystemRoot\System32\Config\SECURITY
0x87ccc99c8 0x164c29c8 \SystemRoot\System32\Config\DEFAULT
0x87ccb008 0x1a60c008 \SystemRoot\System32\Config\SAM
0x881ca9c8 0x14b699c8 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x88d32008 0x065e5008 \??\C:\Users\IEUser\ntuser.dat
0x88d36008 0x01d4d008 \??\C:\Users\IEUser\AppData\Local\Microsoft\Windows\UsrClass.dat
0x8985a008 0x18e9d008 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
```

```
sansforensics@siftworkstation: ~/Documents
$ volatility -f IE10WIN7-20221114-202804.raw --profile=Win7SP1x86_23418 hashdump -y 0x87ccb008 > hashResults.txt
Volatility Foundation Volatility Framework 2.6.1
sansforensics@siftworkstation: ~/Documents
$
```

hashResults.txt  
~/Documents

```
1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:96d3e89d052ee81604174875eb9de565:::
2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
3 IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
4 sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
5 sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16fc6c061c3359db455d00ec27035:::
```

Decrypt MD5, SHA1, MySQL, NTL x +

https://hashes.com/e...

Found:

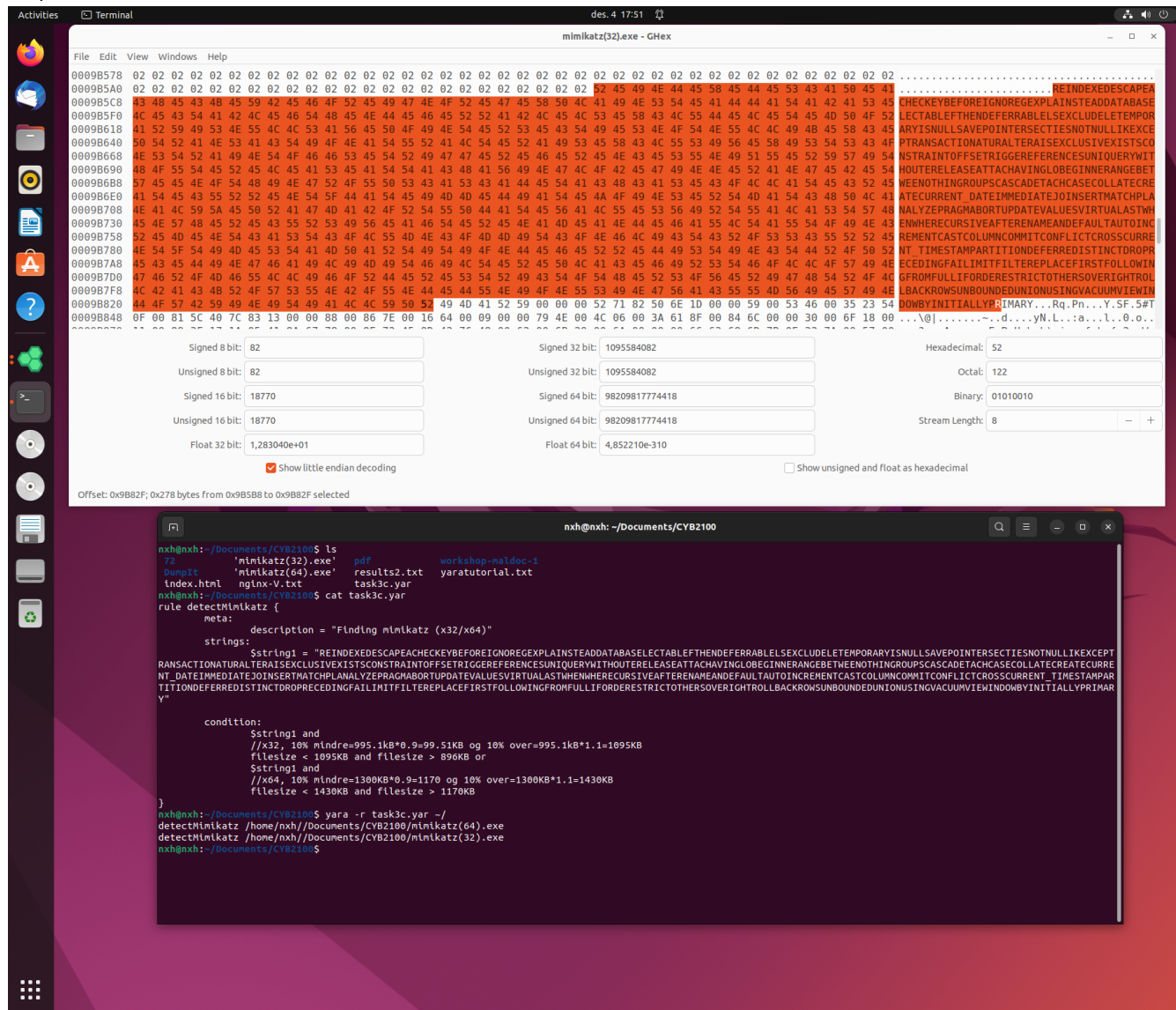
96d3e89d052ee81604174875eb9de565: Liverpool

Passordet er Liverpool.

<sup>19</sup> CISA (29. desember, 2016), JAR-16-20296A, [https://www.cisa.gov/uscert/sites/default/files/publications/JAR\\_16-20296A\\_GRIZZLY%20STEPPE-2016-1229.pdf](https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf), s. 4

<sup>20</sup> Flynn, J.F (i.d.), The Mimikatz Story, <https://www.jamesfrancisflynn.com/062022mimikatz#:~:text=bank%20robberies%2C%20and-,NotPetya,-was%20able%20to>

### 3.c)



Bildet over ble utført på følgende måte:

1. Jeg tolket at filstørrelsen kan variere med 10% hver retning (+/-).
2. En unik streng ble funnet i Ghex (en hex editor)
3. Strengen ble brukt i variabel \$string1 for å identifisere både 32- og 64-bit Mimikatz.exe

### 3.d)

Følgende punkter er hentet fra National Cyber Security Center<sup>21</sup>:



1. **Implementasjon av prinsippet om minste privilegium**
  - a. En hierarkisk modell for konto som gir tilgang til bare nødvendige egenskaper.
    - i. Gjelder også administrative konto
  - b. Mulig å implementere tidsbaserte brukerrettigheter
2. **Bruk enheter som kan lagre passord i hardware**
  - a. Forutsetter at man ikke lagrer passordet i plain text

<sup>21</sup> NCSC (8. februar, 2018), Preventing Lateral Movement, <https://www.ncsc.gov.uk/guidance/preventing-lateral-movement>

- i. Forutsetter ingen innlogging fra noen andre steder enn den enheten man stoler på ift. nettverksoner.
  - b. Anmodes til å separere profesjonelt og personlig bruk av enheter.
- 3. Nettverksegregering**
- a. Betraktelig vanskeligere for ondsinnet aktører å bruke ett utgangspunkt til å komme seg videre.
  - b. Forutsetter at kommunikasjon mellom enheter i ett nettverk ikke blir automatisk klarert.

## Metodikk

*Skjermdump metode:*

- PrtSc 
- Shift+  Win + s

*Referanse stil:*

Fotnoter med APA 7