Oppgave 1a)

Mange organisasjoner og selskaper utsettes for angrep grunnet manglende sikkerhet. NSM (Norsk sikkerhetsmyndighet) er blant annet de som har utarbeidet et rammeverk for sikkerhet som består av fire kategorier med prinsipper og tiltak i hver kategori for å beskytte virksomhetene. Dette rammeverket er dedikert til både offentlige og private norske organisasjoner og som er laget for å hjelpe virksomhetene med å styrke sikkerheten sin som minimere risikoen for uautorisert tilgang og annen ondsinnet angrep. Som CISO ville det vært gunstig å benytte seg av NSM sine grunnprinsipper for å styrke sikkerheten i virksomheten.

Den første kategorien i NSMs rammeverk er **Identifisere og kartlegge.** (Ramberg, Lesson 1.2.pdf) I denne kategorien er alle tre prinsippene like viktige. Prinsippene kan gi CISO en full oversikt over styringsstrukturen i virksomheten. Her er det snakk om å kartlegge leveranser og tjenestene i virksomheten, å få oversikt over hvilke enheter og programmer virksomheten har, og hvilke brukere virksomheten består av. Manglende oversikt over infrastrukturen og risikovurdering kan gi økt sjanse for at virksomheten er sårbar og kan utsettes for angrep dersom de ikke har noe informasjon om sikkerheten i infrastrukturen sin. Disse prinsippene er viktige siden det hjelper CISO med å forstå hvilke sikkerhetsimplementasjoner som bør tas i bruk i virksomheten. Kartlegging kan gi en oversikt over hvilke enheter eller ressurser som må sikres og kan bidra implementere sikkerhetstiltak som kan tas i bruk for sikring av virksomheten. I den andre kategorien som er **Beskytte og opprettholde,** (Ramberg, Lesson 1.2.pdf) er prinsippene: Etablere en sikker IKT arkitektur, Ha kontroll på identiteter og tilganger og beskytte data i ro og i transitt, tre viktige prinsippene som kan bidra til økt sikkerhet på virksomheten. Hvis virksomheten har en usikker IKT arkitektur kan dette medføre til at systemet består av sikkerhetshull dersom arkitekturen ikke vedlikeholdes og er bygget på en god nok måte. Dette kan utnyttes av en angriper som gir vedkommende uautorisert tilgang eller utføre angrep som kan sabbotere systemet. Derfor er det viktig for virksomheten å etablere en sikker IKT arkitektur. Deretter er det viktig for CISO i virksomheten å ha kontroll på hvilke brukere som skal ha tilgang på hva. Hvis en angriper får uautorisert tilgang til en bruker med høye privilegier, kan dette medføre til at hackeren får kontroll over systemet og gi uautorisert tilgang til sensitive data og ressurser i virksomhetens system. Dette kan videre medføre til at angriper modifiserer eller sletter ting på systemet

som gir virksomheten konsekvenser. Derfor er det viktig å gi brukerne de rette privilegiene som kan minimere risikoen for databrudd og kompromittering av datasystemet. Det er veldig viktig at CISO etablerer en beskyttelse mot virksomhetens data. Dette kan gjøres ved å ta i bruk kryptering metoder som skal forhindre i at dataen leses av i transitt. Hvis dataen i virksomheten er ukryptert kan dette medføre til at konfidensiell data misbrukes og leses av angriperen utilsiktet.

Oppdage (Ramberg, Lesson 1.2.pdf) er den tredje kategorien i NSMs rammeverk og de viktige prinsippene er: Oppdage og fjerne kjente sårbarheter og trusler, Etablere sikkerhetsovervåkning. Hvis IT systemet består av sårbarheter kan dette gi økt risiko for cyberangrep som kan utnyttes av angripere til å utføre farlig angrep som å kjøre skadelig kode eller malware som kan sabotere eller distrahere systemet. Videre kan de utføre angrep som gir dem uautorisert tilgang til systemet og på denne måten stjele sensitiv data av kunder og ansatte og medføre til databrudd. Derfor kan det være en fordel for CISO å oppdage og eliminere sårbarheter og truslene på systemet som beskytter systemet mot cyberangrep. Videre kan det være lurt å etablere en sikkerhetsovervåkning over systemet ved bruk av monitorerings-vertøy som kan gi en kontinuerlig overvåkning av systemet. Dette er viktig siden det kan bidra med å detektere uautoriserte og sikkerhetstruende aktiviteter på systemet. Analyse verktøy kan bidra virksomheten med å analysere systemet for å samle inn logger og data som hjelper CISO med å oppdage truslene og stoppe dem fra å kompromittere systemet. Uten sikkerhetsovervåkning vil angripere være i stand til å utføre handlingen på systemet utilsiktet og ved å implementere sikkerhetsovervåkning kan dette bidra med å forhindre dette.

Håndtere og Gjenopprette (Ramberg, Lesson 1.2.pdf) er den siste kategorien i rammeverket og de viktigste prinsippene her er: Forbered virksomheten på håndtering av hendelser og evaluer og lær av hendelser. Hvis virksomheten ikke implementerer plan for hendelseshåntering, kan dette gjøre det vanskelig for dem å begrense og eliminere truslene og skadene fra virksomheten når den inntreffer. Derfor er det viktig å han en plan for hendelseshåndtering som bidrar CISO med å håndtere hendelser dersom de inntreffer. Dette hjelper med å detektere og fjerne skadelige hendelser og minimere skaden fra systemet. Som CISO er det også viktig å lære av sine feil neste gang en hendelse inntreffer i virksomheten og implementerer de nødvendige sikkerhetstiltakene og forbedrer

hendelsesprosessen er tiltak som kan tas i bruk å forhindre at hendelsen oppstår. Ved manglende læring kan dette gi økt sannsynlighet for at en skadelig hendelse oppstår.

1b)

Et effektive tiltak virksomheten kan benytte seg av for å forbedre motstandsdyktigheten mot ramsonware er å etablere kontinuerlig patching rutiner av systemet (Ramberg, Lesson 8.2.pdf, 2022). Hvis virksomheten ikke patcher systemet kan angripere benytte seg av blant annet av de utdaterte programvarer eller nettverket som et mål for å spre ramsonware til systemet. Virksomheten bør sørge for en kontinuerlig patching av systemet som kan bidra med å tette sikkerhetshullene i systemet. Patching gjøres ved å oppdatere systemet som videre forbedrer og sikrer systemet mot å bli utsatt for ramsonware angrep.

Andre tiltak som kan være effektiv mot ramsonware er awareness trening for ansatte (Ramberg, Lesson 8.2.pdf, 2022). I en bedrift er det oftest slik at menneskene er et mål som angripere kan misbruke for å få uautorisert tilgang til systemet. Ansatte er uaktsomme og har manglende informasjonssikkerhets kunnskapene som trengs og utsettes derfor for ramsonware angrep. Dette gjør at angripere benytter seg av social engineerings taktikkene sine mot ansatte for å få tilgang til systemet. De kan ved å ringe, sende SMS, mailer eller linker til ansatte som manipulerer dem til å oppgi brukeropplysningene sine til systemet som sendes direkte til angriperen. Eller så kan mailene manipulere ansatte til å laste ned ramsonware til maskinene sine utilsiktet, dette kan gi konsekvenser for virksomheten og sette dem for utpressing og dersom ikke de betaler til angriperen kan dette medføre til datalekkasje av konfidensiell data. Social engineering kan i verste fall gi hackeren full kontroll slik at systemet kompromitteres. Ansatte bør opplæres til å kunne detektere phishing epost og SMS. Da lærer de å unngå svindelforsøk som kan bidra til å styrke informasjonssikkerhetene blant ansatte som gir dem økt beskyttelse mot social engineerings metoder. Dermed gir dette en god forståelse for hvor viktig det er å unngå slike svindelforsøk. Dette vil bidra med at bedriften klarer å opprettholde konfidensialiteten slik at sannsynligheten for at bedriften utsettes for ramsonware minimeres.

Et tredje tiltak som forbedrer resillience til virksomheten er å benytte seg av monitorerings-vertøy. Dette kan gjøres ved å blant annet benytte seg av antivirus, ved å benytte seg av gode antivirus program kan dette beskytte maskiner mot å bli utsatt for ramsonware.

Antivirus monitorer systemet og varsler dersom den detekterer ramsonware på systemet og dermed forhindrer det fra å infisere maskinene. Andre ting bedriften kan gjøre er å ta i bruk SIEM (Security Information and Event Manager). SIEM kan brukes til å overvåke brukeraktivitetene og dersom en ondsinnet hendelse oppdages kan dette hjelpe CISO med å jobbe for å forhindre ramsonware angrep fra å kompromittere systemet som bidrar med å ivareta sikkerheten i bedriften.

1c)

Hoved oppgavene til en SOC innebærer blant annet **deteksjon** av ondsinnede hendelser. (Ramberg, Lesson 3.2.pdf, 2022) Dette er et av de viktigste tjeneste en SOC tilbyr og dersom en hendelse blir detektert, jobber SOC med å forhindre at hendelser oppstår i virksomheten. For en SOC kan det være en fordel å samle inn data fra systemlogger, IOC-er, brannmurer og monitorerings-verktøy (SIEM) for analyse som kan bidra med å detektere en farlig hendelse. Eksempelvis kan virksomheten utsettes for aktiviteter, malware, ramsonware og andre typer ondsinnede angrep som inntar i systemet som kan forårsake skade på systemet. Videre har vi **hendelseshåndtering,** dette er også en viktig tjeneste som SOC bør benytte seg av. Når man har etablert et SOC-team er det viktig å ta grep dersom en farlig hendelse oppstår. For å utføre denne jobben er det viktig å ha en prosess for hendelseshåndtering, og da er det snakk om å ha en plan for hvordan man skal gå fram for å redusere eller fjerne hendelsen fra systemet. I prosessen handler det om å gjøre forberedelser før hendelsen inntar (Preperation) deretter detektere og analysere for å bekrefte at del er en hendelse og videre begrense det (Containment) før man fjerner den helt (Eradiction). Uten hendelseshåndtering er ikke virksomheten i stand til å eliminere en kritisk hendelse dersom den oppstår. Dette kan distrahere, skade eller sabotere systemet som kan gi en enorm konsekvens for bedriften og i verste fall medføre datatap, gjøre dataen utilgjengelig eller spre seg til de andre maskinene i nettverket.

Sårbarhetshåndtering (Ramberg, Lesson 3.2.pdf, 2022) er også viktig for et SOC-team for hvis laptoper, operativsystemet, servere og de andre enhetene i virksomheten består av sårbarheter kan dette gi økt risiko for at de utsettes for ondsinnede hendelser og aktiviteter i systemet. Derfor kan det være gunstig å ha en sårbarhetshåndtering slik at de kan identifisere det og fikse sårbarhetene for å tette sikkerhetshull dersom det er noen sårbarheter. Sårbarhetshåndtering kan oppnås ved å benytte seg av automatiserte verktøy

for sårbarhets identifikasjon. Deretter kan det å benytte seg relevante kilder brukes til å avgjøre hvilke sårbarheter som bør prioriteres ut i fra alvorlighetsgrad, de sårbarhetene med høyest alvorlighetsgrad bør prioriteres fremfor de lave. Eksempelvis er CVE (Common Vulnerability Exposures) en god kilde til å identifisere kjente sårbarheter, de har en liste over sårbarheter som er kategorisert på ulike alvorlighetsgrad som et SOC-team kan benytte seg av under sårbarhetshåndteringen.

Siste tjeneste som kan være viktig for å etablere et SOC-team er å ha en **Awareness.** (Ramberg, Lesson 3.2.pdf, 2022) Det ikke bare ansatte som må ha Awareness på plass, for et SOC-team er dette også like viktig med hensyn til å de jobber med å identifisere og fjerne trusler i systemet. Det viktig å ha gruppemedlemmer som har godt nok kompetanse for å utføre jobben. Ofte er det slik at noen SOC-team ikke har den kunnskapen som trengs for å utføre monitorering av systemet, ansatte i teamet har ikke ferdighetene som trengs for å identifisere en kritisk hendelse eller trussel og kan dermed ikke forhindre det heller.

Awareness er viktig for et SOC-team, for det kan hende at team – medlemmene er ukritiske i møte med ondsinnede angrep. Jobben de utfører avhenger av at de ikke blir infisert selv. Derfor trenger de opplæring i hvordan man skal unngå phishing og andre trusler som kan bidra til å forhindre i at de blir utsatt for malware angrep, tap av konfidensiell data og liknende. I tillegg kan awareness bidra med å gi SOC teamet den treningen som kan hjelpe dem med å detektere potensielle angrep som kan bidrar til å forhindre fremtidige hendelser.

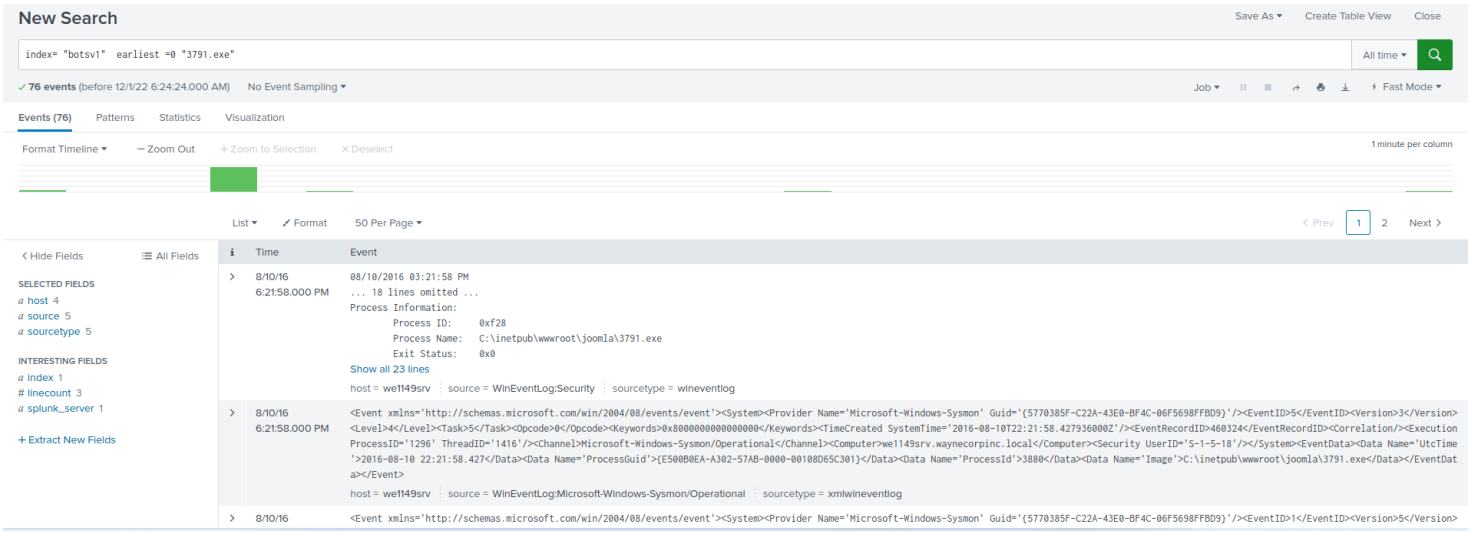
2 a)

Splunk er et SIEM-verktøy som brukes for å samle inn og analysere data som brukes til å monitorering av data og utføre søkeoperasjoner mot dem. De viktigste komponentene i et Splunk oppsettet er: Forwardere, indexer og search head (Ramberg, Lesson 5.1, 2022). Splunk samler i logg og analyserer loggdata fra systemet som videre sendes til forwarderen. Forwarderen er har som oppgave å samle inn data og disse sendes videre til indexeren som prosesserer og behandler dataen. Det finnes to typer forwardere, den ene er universal forwarderen som har til oppgave å sende ikke prosesserte data videre til indexer. På den andre siden har vi en heavy forwarder som prosesser, indexerer og parser dataen lokalt før den videresendes til indexeren. Indexeren omgjør disse dataene til å bli eventer og lagrer disse slik at man kan utføre søkeoperasjoner mot dataen. Indexing er viktig med hensyn til at

den behandler store mengder av data og lagrer dataen lokalt. Dette er en viktig komponent som SIEM avhenger av for å kunne fungere. I Splunk er search index en komponent som brukes til å utføre spørringer mot dataen i indexer ved å skrive inn søkeord. Når brukere utfører søkeoperasjonene sine går search head igjennom indexer i Splunk slik at spørringene genereres direkte på indexer og dersom search head fant relaterte resultater sendes de tilbake til brukeren.

2b)

«Vedlegg 1: Åpner splunk og kjører følgende kommando «index "botsv1" earliest=0 "3197.exe "» og får opp:»

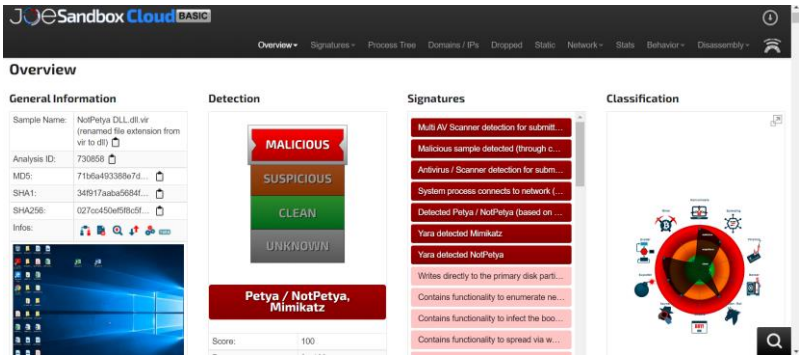


Path-en til programmet 3197.exe er "C:\inetpub\wwwroot\joomla\3791.exe" path formatet hinter om at serveren kjører Microsoft Windows operativsystemet og webserveren som er brukt er «Microsoft IIS/ 8.5». En barriere som kunne forhindre en angriper fra å laste opp 3791.exe er å benytte seg av autentisering. Serveren burde ha benyttet seg av autentisering metoder for opplastning av filer, som krever innlogging for å opplastning av filer for å bekrefte at denne opplastningen ble utført av en troverdig bruker og ikke en angriper. På denne måten kan dette øke sikkerheten i serveren og minimere risikoen for at den ondsinnede file "3791.exe" filen fra å laste opp på serveren. En annen barriere er at serveren tillater kun spesifikke filtyper som kan lastes opp på serveren. Ettersom "3791" er en exe fil ville kan det være en fordel å blokkere opplastninger for exe- filer. Dette forhindrer angriperen fra å laste opp den ondsinnede "3791.exe" filen.

2.c)

SIEM er verktøy for monitorering av systemet og detekterer ondsinnede aktiviteter dersom det skulle oppstå, eksempler på SIEM verktøy er Splunk og Microsoft Sentinel. Disse har noen fellestrekk, men er i tillegg på mange måter ulike. Hoved fordelene med Sentinel er at det er en cloud native SIEM løsning med innbygget SOAR (Ramberg, Lesson 4.2.pdf, 2022). I tillegg har løsningen avanserte analysetjenester, integrert threat intelligence og sentinel tar i bruk AI for å detektere og redusere ondsinnede handlinger på systemet. Sentinel er enkelt å konfigurere i sammenliknet med Splunk for bedrifter og organisasjoner som benytter seg av Microsoft produkter slik som Azure, dette gjør det raskere for brukere å komme i gang. (blog.r2ut.com, u.d.). Sentinel tillater forbrukere å skalere opp eller ned på ressurser etter behov, dette kan blant annet bidra med til å redusere kosten (Warner, 2022). Et SOC-team kan samle datalogger fra overalt både lokalt og internettjenestene siden Sentinel støtter tredjeparts applikasjoner som gjør dette mulig. Oppsummert er Sentinel en enklere tilnærming fremfor Splunk og har flere fordeler og tilbyr funksjonaliteter som Splunk ikke har. Den er i tillegg mye enklere å bruke og administrere og bidrar med å gjøre jobben for SOC mye mer enklere og effektiv og egner seg godt for alle typer bedrifter om det er liten eller stor.

3a)



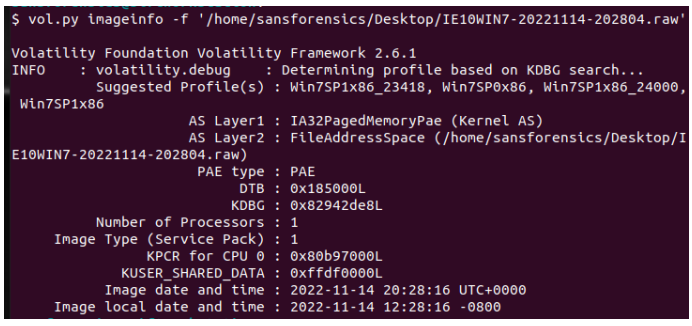
(Vedlegg 2: Limte inn sjekksummen «027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745» inn i Joe Sandbox som er et online verktøy for malware analyse. Verktøyet detekterte at dette er en Petya/NotPetya angrep)

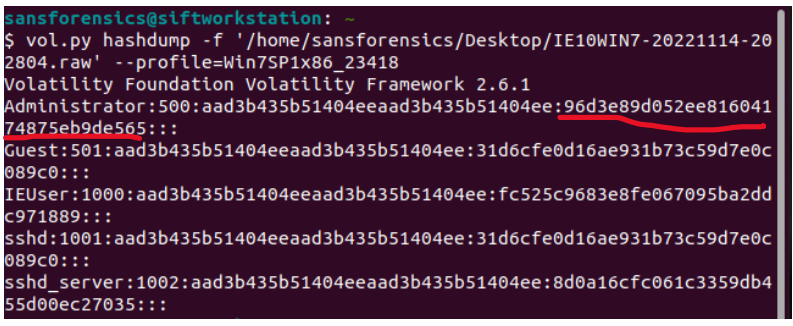
Petya var et ramsonware angrep som ble oppdaget i 2016. Den infiserte hovedsakelig maskiner som kjørte Windows operativsystem (Wikipedia, 2022) og spredde seg hovedsakelig via email. Når man trykket på den krasjet den maskinen og startet en

automatisk reboot. Deretter overskriver den MBR (Master Boot Record) (Ramberg, Ramsonware , 2022) på maskinen og krypterer deretter harddisken. Videre så fikk man opp en melding som krevde at brukerne måtte betale i bitcoin dersom de ønsket å aksessere maskinen og tilgang til filene sine. På denne måten ble ofrene utsatt for pengeutpressing og så lenge de ikke betalte angriperne ble de nektet tilgang til maskinen.

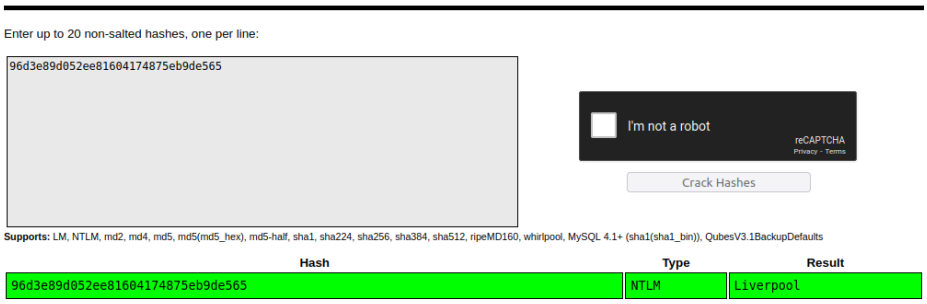
NotPetya er et var et ramsonware angrep som ble først oppdaget i 2017 og er en variant av Petya angrepet. Dette var et angrep som hovedsakelig var designet av GRU Russiske militæret (Sandworm) med hensikt til å angripe Ukraina. NotPetya spredde seg ved at en insider gjorde det mulig for angripere å få uautorisert tilgang til MEDoc (Ramberg, Lesson 8.2.pdf , 2022). Angriperne implementerte inn bakdører i systemet som medførte at NotPetya angrepet spredde seg videre til nettverket som infiserte organisasjonene i andre land. Dette infiserte blant annet organisasjoner i andre land slik som Maersk i Danmark. NotPetya hadde de samme funksjonalitetene som Petya og spredde seg via Enternalblue, som er den samme spredningsvektoren WannaCry brukte for å spre seg. Sammen med Enternalblue benyttet NotPetya seg også av Mimikatz som er et passwordharvesting-verktøy for å samle inn passord. Disse kombinert gjorde det mulig for angrepet å spre seg til alle maskinene i nettverket. NotPetya krypterte absolutt alt på maskinen og det var ikke mulig å dekryptere filene slik som i Petya. Angrepet slettet alle filene i de påvirkede maskinene som gjorde det til umulig for gjennompretting. Så hvis man ble infisert gikk alt av data og filer tapt.

3b)





«Vedlegg 3 og 4: Skriver inn «vol.py imageinfo -f '/home/sansforensics/Desktop/IE10WIN7-20221114-202804.raw'» og finner hvilke profiler som befinner seg i minnet deretter kjører jeg «vol.py hashdump -f '/home/sansforensics/Desktop/IE10WIN7-20221114-202804.raw' --profile=Win7SP1x86_23418» og finner NTLM sjekksummen (96d3e89d052ee81604174875eb9de565) til Administrator»



«Vedlegg 6: Limer inn hashen til Administrator inn i crackstation.net og for å knekke passordet og finner at admin passordet er «Liverpool».»

3c) (Bruker Ubuntu i denne oppgaven)

```
rule detected_mal {

        meta:
                description = "mimikatz detection rule"
                version = "1.0"

        strings:
                $Warning = "Malecious files detected:" ascii
                $file1 = "mimikatz(1).exe" ascii
                $ApplicationType1 = "winx64" ascii
                $md5sum ="e930b05efe23891d19bc354a4209be3e" ascii
                $file2 = "mimikatz.exe" ascii
                $ApplicationType2 = "win32" ascii
                $md5sum2 = "46f366e3ee36c05ab5a7a319319f7c72" ascii
                $path = "/home/usah001/Nedlastinger" ascii

        condition:
                $Warning and $file1
                and $ApplicationType1 and $md5sum
                and $file2 and $ApplicationType2 and $md5sum2 and
                $path and filesize  < 1MB

}
```

Vedlegg 7: lagde en regel som treffer på winx32 og win64 versjonen av mimikatz.exe der filstørrelsen varierer med 10 prosent

```
usah001@usah001-VirtualBox:~/yara$ yara mimkatz.yar -r -s
'/home/usah001/yara/mimkatz.yar'
detected_mal /home/usah001/yara/mimkatz.yar
0x78:$Warning: Malecious files detected:
0xa5:$file1: mimikatz(1).exe
0xd4:$ApplicationType1: winx64
0xef:$md5sum: e930b05efe23891d19bc354a4209be3e
0x124:$file2: mimikatz.exe
0x150:$ApplicationType2: win32
0x16c:$md5sum2: 46f366e3ee36c05ab5a7a319319f7c72
0x1a0:$path: /home/usah001/Nedlastinger
```

Vedlegg 8: skriver inn kommandoen: «yara mimkatz.yar -s -r 'filplasseringen'» i terminalen og får opp at regelen kjører og treffer på de to filene»

3 d)

Lateral movement er teknikker angripere bruker for å utvide tilgangen sin til nettverket etter å ha fått uautorisert tilgang (Ramberg, lesson 10.1.pdf, 2022). Tiltak som gir beskyttelse mot lateral movement er å blant annet ta i bruk autentisering (Ramberg, lesson 10.1.pdf , 2022). Autentisering er et bra tiltak for det kan bidra med å gjøre det vanskelig for angripere å grave seg dypere inn i nettverk og dermed minimerer sjansen for at en angriper utfører ondsinnede handlinger utilsiktet. Det viktig for brukere med høye privilegier å ikke gjenbruke passordene sine på de ulike delene av nettverket, for dette kan gi økt risiko for angripere å få uautorisert tilgang som gjør at de kan opptre som brukerne selv. Det kan blant

annet gi dem tilgang til konfidensiell data og misbruke disse til å stjele sensitiv informasjon som benyttes til noe ondsinnet, eksempelvis kan angriperen lekke konfidensiell data til offentligheten. Multifaktorisering på webtjenester kan brukes for å autentisere brukere som bekrefter at brukere ved innlogging, dette gir brukere beskyttelse mot å bli utsatt for bruteforce angrep. Andre metoder er å implementere innloggingsrestriksjoner, biometri og smart kort som kan bidra med å gjøre det komplisert for angripere å autentisere seg. Slik kan autentisering være redusere risikoen for lateral movement i nettverket.

Andre tiltak som gir best beskyttelse mot lateral movement er å ta i bruk least priviliges som går ut på å begrense tilgangsrettighetene til brukerne. Brukere på serveren bør ikke ha de samme privilegiene som admin brukeren. Dette kan medføre til at en angriper kan stjele sensitiv informasjon, modifisere eller sabotere hele systemet dersom vedkommende bryter seg inn på en bruker med høye privilegier. Brukere bør tildeles kun privilegiene som er kun nødvendige for å utføre oppgavene sine og ikke mer. Derfor er least priviliges også et viktig tiltak som forhindrer lateral movement i systemet.

Et siste tiltak som kan bidra til å forhindre lateral movement er å ta i bruk nettverksmonitorering. Monitorering av nettverket er et av de beste tiltakene man kan implementere siden den overvåker systemet for sårbarheter og varsler dersom en ondsinnet aktivitet befinner seg i nettverket. Dersom et nettverk består av mange sårbarheter er sannsynligheten stor for at den kan kompromitteres. For monitorering av systemet er det viktig å aktivere logger på systemet. Ved bruk av systemlogger kan man på denne måten detektere om en angriper har kompromittert systemet. Dette kan SOC benytte seg av for å fjerne angriperen som videre kunne gi økt sikkerhet mot lateral movement i systemet.

Bibliografi

blog.r2ut.com. (u.d.). Hentet fra Comparing Microsoft Sentinel vs. Splunk (Microsoft Sentinel vs. Splunk: Which Should You Choose?): https://blog.r2ut.com/comparing-microsoft-sentinel-vs.-splunk#:~:text=Microsoft%20Sentinel%20is%20generally%20rated,Incident%20Management%2C%20and%20Security%20Intelligence.

Ramberg, H. (2022). Lesson 8.2.pdf . I *Case Study - Petya & NotPetya* (ss. 18 , 20). Oslo , Norge .

Ramberg, H. (2022). lesson 10.1.pdf. I *Lateral movement* (s. 7). Oslo, Norge .

Ramberg, H. (2022). lesson 10.1.pdf . I *Lateral movement defense* (ss. 23 -28). Oslo , Norge.

Ramberg, H. (2022). Lesson 3.2.pdf. I *SOC Services* (ss. 5-14). Oslo , Norge.

Ramberg, H. (2022). Lesson 4.2.pdf. I *SIEM* (ss. 13,17,18). Oslo , Norge .

Ramberg, H. (2022). Lesson 5.1. I *Splunk* (ss. 11-13). Oslo , Norge.

Ramberg, H. (2022). Lesson 8.2.pdf. I *Ramsonware* (ss. 10-15).

Ramberg, H. (2022). Ramsonware . I *Case Study - Petya & NotPetya* (ss. 18-20). Oslo ,Norge.

Ramberg, H. (u.d.). Lesson 1.2.pdf. I *Security Basics* (ss. 14-15).

Warner, P. (2022, 03 28). *Wizardcyber.com*. Hentet fra Microsoft Sentinel Vs Splunk: https://wizardcyber.com/microsoft-sentinel-vs-splunk/

Wikipedia. (2022, 11). Hentet fra Petya and NotPetya: https://en.wikipedia.org/wiki/Petya_and_NotPetya