Eksamen for CYB 2100 – Cyberforsvar
Høyskolen i Kristiania
Høsten 2022

Eksamen: Individuell hjemmeeksamen

Varighet: 7 dager

Gradering: Nasjonal karakterskala A – F (F er ikke bestått)

Vekting: 100% av vurderingen

Hjelpemidler: Alle

Akademisk kontakt: Henrik Ramberg, henrik.ramberg@kristiania.no

Besvarelse: Oppgaven skal leveres som en Word-fil med skriftstørrelse 12 og 1,5 linjeavstand. Besvarelsen har en maksimal begrensning på 10 sider inkludert figurer og tabeller. Referanselisten kommer i tillegg. Vær klar og tydelig i din besvarelse, og kom til poenget.

Plagiatkontroll: Det forventes at studenten egenhendig produserer sin egen besvarelse. Være nøye med bruk av kildereferering. Det er krav til APA7 referansestil.

Les igjennom hele oppgaven før du begynner på besvarelsen. Lykke til!

Eksamensoppgave

Oppgave 1 (30% vekting)

Forestill deg at du akkurat har blitt ansatt som CISO i et norsk selskap som produserer varer til norske og internasjonale kunder. Tradisjonelt har mye av varene blitt solgt utenom internett, og selskapet har ikke hatt noen strategisk ambisjon rundt digitalisering.

Med ny daglig leder i selskapet er strategien endret, og virksomheten ønsker nå å utnytte potensialet rundt digitalisering og salg via internett.

Bedriften har i dag omtrent 50 ansatte som alle har en laptop med Windows 10, tilknyttet virksomhetens Active Directory. Stort sett benytter selskapet seg av on-prem løsninger for epost, websider og samhandlingsløsninger.

Dessverre har ikke virksomheten hatt særlig fokus på sikkerhet over tid, og har ingen god oversikt over hva som befinner seg i egen infrastruktur. Dette gjelder både maskinvare og programvare. Det er heller ingen god systematikk rundt konfigurasjon, oppdateringer, logging eller backup.

1.a Forklar hvordan du som CISO ville gått frem for å heve IT sikkerhetsnivået for virksomheten. Bruk NSMs grunnprinsipper som grunnlag for ditt svar. For å begrense lengden på besvarelsen velger du maksimalt 3 prinsipper under hver kategori og begrunner hvorfor du mener akkurat disse prinsippene gir best effekt.

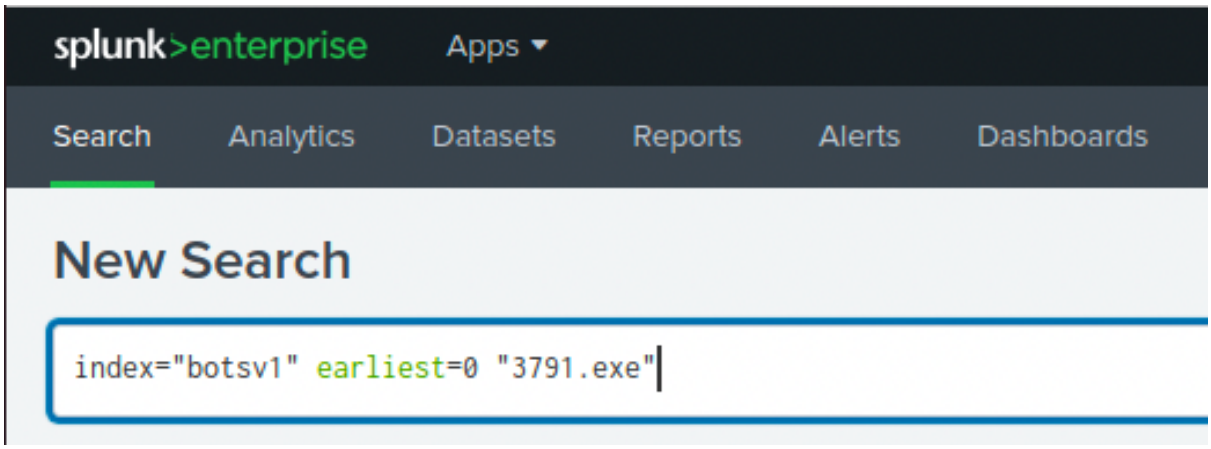
1.b Etter hvert som selskapet gjennomfører sin digitalisering og får større eksponering mot internett er det rimelig å anta at trusselbildet mot selskapet endres. Ledelsen i selskapet er bekymret for ransomware. Beskriv 3 tiltak du mener er de mest effektive for å forbedre virksomhetens motstandsdyktighet (resillience) mot ransomware.

1.c Virksomheten har begrensede ressurser til å etablere en intern SOC, likevel har styret besluttet at dette er en viktig prioritering. Hvilke SOC-tjenester ville du som CISO anbefale at bedriften etablerer dersom det bare er ressurser til å etablere 4 tjenester? Argumenter for hvorfor du valgte akkurat disse tjenestene.

Oppgave 2 (30% vekting)

2.a Beskriv de viktigste elementene i et vanlig Splunk oppsett. Forklar hva de ulike komponentene gjør og sammenhengen mellom dem.

2.b Kjør følgende spørring mot datasettet (botsv1) vi har brukt i kurset:



Hva er path til 3791.exe på serveren? Ut ifra path, hvilket operativsystem kjører serveren og hvilken webserver er brukt? Beskriv 2 barrierer som kunne hindret at en angriper fikk lastet opp den ondsinnede 3791.exe til serveren.

2.c En av de beste alternativene til Splunk for sikkerhetsmonitorering er Microsoft Sentinel. Hva er hovedfordelene ved å velge Microsoft Sentinel fremfor Splunk?

Oppgave 3 (40% vekting)

3.a Ta utgangspunkt i sjekksummen:

027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745

Forklar angrepet der denne skadevaren er brukt, og hvem som sto bak.

3.b Ved å aksessere lenken under finner du en minnedump (passord: Eksamen2022 md5sum: 723b780905a9cc8529f645a117b1c09c). Du skal finne passordet til Administrator ved bruk av Volatility. Hva er passordet? Vis ved hjelp av et skjermbilde hvordan du kom frem til svaret.

https://drive.google.com/file/d/1YvbgLkI-3R8Aj-SiK49nwmQHo2hzQoY_/view?usp=sharing

Legg ved et skjermbilde som viser at du har funnet Administratoren sin NTLM sjekksum ved hjelp av Volatility.

3.c Denne oppgaven anbefales det på det sterkeste at du løser på Linux. I en nettleser navigerer du til:

https://github.com/ParrotSec/mimikatz

Last ned Win32 og x64 utgaven av mimikatz.exe. Nå skal du lage en Yara-regel som slår ut på begge filene du lastet ned. Yara-regelen må ta høyde for at filstørrelsene kan variere med inntil 10%. Regelen skal ikke slå ut på andre filer dersom den kjøres rekursivt mot / på maskinen. Legg ved skjermbilde av Yara-regelen din i svaret. Legg også ved skjermbilde av at du kjører regelen og at den treffer på de to filene.

3.d Beskriv de 3 tiltakene du mener er best for å beskytte seg mot lateral movement i egen infrastruktur. Argumenter for hvorfor du valgte akkurat disse 3 tiltakene.

Slutt på oppgavesettet.