Eksamen
CYB 2100 – Cyberforsvar
Høyskolen i Kristiania
November 2023

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 PDF-fil med skriftstørrelse 12 og 1,5 linjeavstand. Fonten skal være av typen «Times New Roman» eller «Arial», med svart farge på hvit bakgrunn. Besvarelsen har en maksimal begrensning på 10 sider inkludert figurer og tabeller. Referanselisten kommer i tillegg. Vær klar og tydelig i din besvarelse. Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

Plagiatkontroll: Det forventes at studenten egenhendig produserer sin egen besvarelse. Være nøye med bruk av kildereferering. Det er krav til APA7 referansestil. Det gjennomføres plagiatkontroll på alle innleveringer, bacheloroppgaver og masteroppgaver. Se for øvrig retningslinjene for kildehenvisning, plagiat og formelle krav til innlevering.

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

Oppgave 1 (30% vekting)

1.a Tomra er et stort teknologiselskap som er representert i flere land, med flere tusen ansatte. Selskapet er notert på Oslo Børs, og er for mange kjent som selskapet som håndterer retur av flasker. I juli meldte selskapet selv om et omfattende cyberangrep på egen infrastruktur. Selskapet har vært åpne om angrepet og har kommet med en rekke oppdateringer siden første pressemelding. Ut fra opplysninger du finner i offentlige

tilgjengelige kilder skal du argumentere for hvordan selskapet kunne ha avverget eller dempet konsekvensene av angrepet ved hjelp av tiltak du finner i rammeverk for cybersikkerhet. Rammeverket du refererer til må være omtalt i forelesning eller i pensumlitteraturen. For å begrense omfanget på oppgaven tar du for deg de tre tiltakene du mener hadde hatt størst effekt på denne hendelsen. Du må argumentere for hvorfor du valgte disse tiltakene.

1.b Ut i fra de opplysningene du kan finne om Tomra-angrepet skal du peke på tre SIEM kilder som du vurderer som de mest effektive for å oppdage denne hendelsen. Du skal argumentere for hvorfor akkurat disse kildene er de beste for å oppdage hendelsen.

1.c Tomra skriver i en av sine pressemeldinger følgende: "We have taken measures to implement one of the most modern and secure cyber security architectures – a so called Zero Trust architecture – to prevent future disruptions and to protect ourselves, our customers, partners, and suppliers...». I forelesningene har vi sett ulike prinsipper som inngår i begrepet Zero Trust Architecture. Velg ut tre prinsipper du mener hadde vært de beste for å forhindre og minimere hendelsen til Tomra. Argumenter for hvorfor prinsippene du valgte er de beste i forbindelse med denne hendelsen.

Oppgave 2 (30% vekting)

2.a Last inn datasettet du finner ved hjelp av lenken under (md5sum: 6ea8f15cc4ccf6186db7a31415c09c58).

https://s3.amazonaws.com/botsdataset/botsv2/botsv2_data_set_attack_only.tgz

Demonstrer at du har et fungerende datasett ved å kjøre en passende spørring som lister opp indexene dine i Splunk. Forklar hvordan du gikk frem for å laste inn datasettet, og bruk bilder som dokumentasjon.

Lag en visualisering i Splunk som viser distribusjonen av protokoller som kjører over TCP basert på datasettet du akkurat lastet inn. Du kan basere deg på antall forbindelser og kun de fem protokollene med størst forekomst. Forklar hvordan du gikk frem og dokumenter med bilder.

2.b Med utgangspunkt i datasettet nevnt i 2.a;
- Finner du noen e-postadresser som tilhører personen Amber?
- Hvem sender Amber epost til?
- Sender Amber vedlegg, og hva er i såfall navn på eventuelle vedlegg?
- Hvilken epost ser ut til å være knyttet til «matar»?
- Og hvem sender personen knyttet til «matar» epost til?

Kjør spørringer mot datasettet for å finne svar på spørsmålene. Forklar hvordan du går frem og hvilke spørringer du kjørte. Det er viktig at du dokumenter med skjermbilder.

2.c Elastic Stack, også kjent som ELK stack, er en populær SIEM og et godt alternativ til andre SIEMer slik som Splunk og Microsoft Sentinel. Hva er hovedfordelene og de største ulempene ved å velge ELK som SIEM? Hvilken type organisasjoner mener du bør vurdere å bruke ELK som SIEM?

Oppgave 3 (40% vekting)

3.a QR koder har den siste tiden blitt svært populært å bruke i forbindelse med epost phishing. Fenomenet QR koder i forbindelse med e-post phishing har fått navnet quishing. Forklar forskjeller og likheter mellom quishing og tradisjonelle hyperlinker i epost phishing. Hva slags ekstra utfordringer kan quishing gi fra et cyberforsvar-perspektiv?

3.b Tenk deg at du jobber som hendelseshåndterer i et stort norsk selskap. Du får en henvendelse fra en medarbeider som er engstelig for at vedkommende er infisert med skadevare etter å ha åpnet en mistenkelig epost. Som hendelseshåndterer er det din oppgave å komme til bunns i saken. Du har bedt vedkommende om en kopi av den mistenkelige e-posten, og har fått oversendt filen i lenken under. Filen er zip'et og passordbeskyttet (passord: EksamenNovember).

https://drive.google.com/file/d/1b9g1dE6hp0kbDRI4-RloeYYWYHY7BI6Z/view?usp=sharing
(md5sum: 84e6847c397a2c2e1be83ae9b3c648d3)

Hva har medarbeideren mottatt? Er det skadevare i eposten? Forklar hvordan du går frem for å analysere e-posten og innholdet. Forklar hvordan du kommer frem til svaret og dokumenter nøye med bilder.

PS: Det anbefales at denne oppgaven løses på den virtuelle maskinen «CYB2100», som vi har brukt i forbindelse med øvinger.

3.c På linken under finner du en minnedump (Passord: EksamenNovember)

https://drive.google.com/file/d/1foMbzNpXto7FGvWwaVTkditUNe3Vi-4v/view?usp=sharing
(md5sum: f2ae5236214d5c419b00d3fb5af5a74c).

Du skal ved hjelp av Volatility identifisere en prosess som blir detektert som ondsinnet hos VirusTotal. Dump prosessen til fil ved å bruke Volatility og test mot VirusTotal. Hvilken skadevare er det eventuelt snakk om? Dokumenter grundig med skjermbilder og forklar hvordan du gikk frem. Om du skulle finne flere ondsinnede prosesser dokumenterer og vurderer du de også.

Bruk Yara modulen i Volatility for å detektere prossessen du identifiserte i minnedumpen. Når du skal lage Yara regelen kan du ikke bruke hashing funksjonen, og regelen skal være så

presis som mulig samtidig som den er fleksibel nok til å detektere varianter av samme program. Legg ved bilde av Yara scriptet og et skjermbilder som viser at reglen treffer på minnedumpen. Skulle du finne flere ondsinnede prosesser lager du regel for de også.

PS: Det er et krav at denne oppgaven løses på den virtuelle maskinen «CYB2100», som vi har brukt i forbindelse med øvinger.

3.d Cyber resilience er et begrep som brukes stadig oftere i forbindelse med cybersikkerhet. Argumenter for hvordan NIS2 og «Cyber Resilience Act» (CRA) kan påvirke cyber resilience. Hva mener du er de tre mest effektive tiltakene en mellomstor norsk bedrift kan gjøre for å forbedre sin cyber resilience? Begrunn hvorfor du mener akkurat disse tiltakene er de beste.

Slutt på oppgavesettet.