Eksamen
CYB 2100 – Cyberforsvar
Høyskolen Kristiania
November 2024

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. Alle marger skal være standard 2,5 cm. 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 forøvrig retningslinjene for kildehenvisning, plagiat og formelle krav til innlevering.

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

Kristiania

Oppgave 1 (40% vekting)

1.a I forbindelse med analyse av skadevare kan man dele de ulike metodene inn i statisk og dynamisk analyse, samt online og offline analyse. Drøft fordeler og ulemper ved dynamisk, statisk, offline og online analyse av skadevare. Få frem likheter og forskjeller ved de ulike mulighetene. Hva er en særlig utfordring ved bruk av onlinetjenester?

1.b Tenk deg at du jobber som en skadevareanalytiker i et cyberdefense centre i en stor norsk bedrift. Du får en henvendelse fra en leder som er engstelig for at vedkommende er infisert med skadevare etter å ha installert mistenkelig programvare fra en intern webserver.

I lenken under finner du en pakkedump av hendelsen, og du skal selv finne frem til den mistenkelige filen og svare på spørsmålene under.

https://drive.google.com/file/d/1WTr2AhEXhbTDaBGdUjygmUXn-8Z_dZyW/view?usp=drive_link

Filen er pakket og passordbeskyttet (passord: EksamenNov24).

Oppgaven skal løses på den virtuelle maskinen «CYB2100», som vi har brukt i forbindelse med øvinger. I terminalen lager du en mappe på ditt hjemmeområdet med navn «kadidatnr-1b». Er ditt kandidatnummer 1313 blir altså mappenavnet 1313-1b. Last ned filen til mappen og pakk den ut ved hjelp av kommandolinjen. Deretter skal du svare på følgende spørsmål:

- Er filen signert, og i så fall av hvem?
- Når ble filen første gang observert på VirusTotal, og hva er resultatet på Virustotal?
- Hva vil være din vurdering og tilbakemelding til den bekymrede lederen?

Det er viktig at du dokumenterer det du gjør med bilder og tekst. Mappestrukturen og kommandoene du bruker må komme tydelig frem.

1.c Selskapet du jobber i benytter ClamAV som antiskadevare. Lag en signatur for filen i oppgave 1.b i ClamAV. Oppgaven skal løses på CYB2100 i terminal og i en katalog med navn «kadidatnr-1c», hvor du bytter ut «kadidatnr» med ditt kandidatnummer. Signaturen skal være så bra at den ikke treffer på andre filer dersom den brukes på en Windowsmaskin. Du skal selvsagt legge ved skjermbilde av signaturen og skjermbilde av at den virker når du kjører den i terminalen på Cybuntu. Mappestrukturen og kommandoene du bruker må komme tydelig frem.

1.d Til slutt skal du analysere en minnedump fra maskinen hvor filen fra oppgave 1b kjører. Oppgaven skal løses på CYB2100 og i en katalog med navn «kadidatnr-1d», hvor «kadidatnr»

byttes ut med ditt kandidatnummer. Oppgaven skal løses med Volatility, og du skal svare på følgende spørsmål:

- Hva er PID og PPID og hvilke verdier har disse i dumpen vår?
- Har prosessen vår noen nettverksforbindelser åpne, i så fall hvilke?
- Bruk Yara funksjonen yarascan i Volatility og lag deteksjon.

Minnedumpen finner du her:

https://drive.google.com/file/d/1hPjVuG-0mIavdt87YWgbNVPvR0aLJpii/view?usp=sharing

Filen er pakket og passordbeskyttet (Passord: EksamenNov24). Det er viktig at du beskriver din fremgangsmåte og legger ved gode bilder som dokumenterer stegene dine. Du skal selvsagt legge ved bilde av Yararegelen.

Oppgave 2 (30% vekting)

2.a AI har for fullt gjort sitt inntog i de fleste industrier, dette gjelder selvsagt også innen cyberforsvar. Beskriv 3 områder du mener AI vil hjelpe cyberforsvar aller mest og begrunn hvorfor du mener akkurat disse tre er de viktigste områdene.

2.b I denne oppgaven skal vi ta utgangspunkt i datasettet vi har brukt i faget. Har du ikke datasettet lastet inn finner du en kopi av dette her:

https://s3.amazonaws.com/botsdataset/botsv1/botsv1-attack-only.tgz

Demonstrer at du har et fungerende datasett ved å kjøre en passende spørring som lister opp indexene dine i Splunk.

Lag en tabell i Splunk som sorterer protokoller som kjører over TCP i datasettet. Du kan basere deg på antall forbindelser og sortere fra høyest til lavest. Deretter skal du lage et kakediagram som viser de fire protokollene med høyest forekomst. Forklar hvordan du gikk frem og dokumenter med bilder.

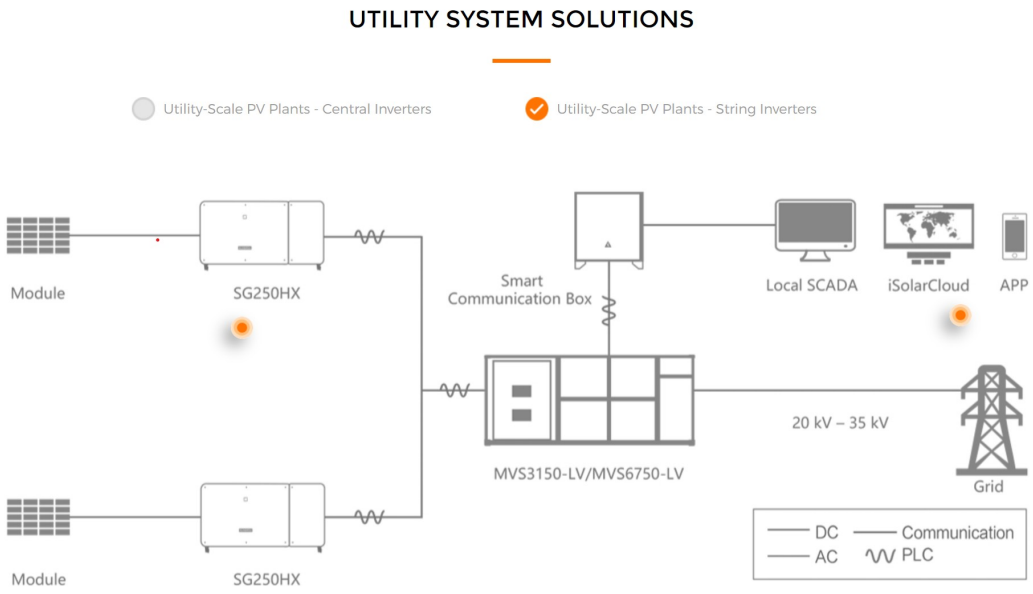
2.c Med utgangspunkt i datasettet nevnt i 2.b skal du svare på følgende spørsmål;

- Hvilken IP ser ut til å scanne webserveren hvor imreallynotbatman.com kjører?
- På hvilken IP adresse, og tcp port finner vi imreallynotbatman.com? Og hvilken server kjører den på?
- Hvilken IP ser ut til å trigge Suricata med en Cross site scripting advarsel?
- Hvem forsøker å logge seg på 192.168.250.40:8191? Og hva får vedkommende til svar?
- Hvor mange av passordene i bruteforce angrepet mot imreallynotbatman.com inneholdt kun tall, og hvor mange startet med bokstaven s?

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 dokumenterer med skjermbilder. Legg også ved SPLene dine inn i teksten som del av svaret.

Oppgave 3 (30% vekting)

3.a Illustrasjonen under er hentet fra selskapet SunGrow sin nettside og viser et standard oppsett av solkraftanlegg fra leverandøren. Hva er potensielt problematisk med dette oppsettet fra et cyberforsvarsperspektiv? Videre er SunGrow et kinesisk selskap, hvorfor kan dette være ekstra problematisk sett fra et cybersikkerhetsperspektiv? Greit ut om bruken av kinesisk teknologi i kritisk infrastruktur.



3.b Se for deg at du er CISO i et energiselskap. Selskapet har allerede besluttet å benytte en løsning som illustrert på tegningen over fra den gitte leverandøren. Hva kan du gjøre som CISO for å forbedre sikkerheten? Ta utgangspunkt i NSM grunnprinsipper for IKT sikkerhet og velg 3 prinsipper som har størst effekt på sikkerheten. Bruk gjerne tilhørende tiltak for å argumentere for dine valg.

3.c I begynnelsen av året ble et energiselskap i Lviv utsatt for et cyberangrep som resulterte i at flere hundre bygninger mistet oppvarming i flere dager. Grei ut om hvem som sannsynligvis sto bak, og hvilket verktøy som ble brukt. Bruk NIST CSF for å forklare hvordan dette kunne vært unngått. For å begrense lengden på denne oppgaven velger du ut de tre subkategoriene du mener hadde vært mest effektive i dette tilfellet.

Slutt på oppgavesettet.