

HJEMME EKSAMEN VÅR 2022 TK2100 Informasjonssikkerhet

Oppgave 1. Generelt (10 %)

Definer «informasjonssikkerhet». Ta utgangspunkt i CIA-modellen.

Informasjonssikkerhet går ut på å oppnå mest mulig fra CIA-modellen, som står for Konfidensialitet (Confidentiality), Integritet (Integrity) og Tilgjengelighet (Availability).

En kan for eksempel låse et brev i en sikkerhetsboks får å oppnå konfidensialitet og integritet målene, men tilgjengeligheten til den informasjonen er svært liten.

På den andre siden kan en sende ut en ukryptert melding over hele verden, hvor integriteten og tilgjengeligheten er svært god, men man vil ikke ha noe konfidensialitet.

Oppgave 2. Konto hijacking og identitetstyveri (10 %)

Drøft hva en hacker kan gjøre hvis han/hun får kontroll over (hijacker) din private epostkonto. Reflekter over mottiltak mot slike angrep. Se problemstillingen i sammenheng med identitetstyveri, og diskuter også hva en hacker kan bruke din BankID til hvis angriperen får tilgang til din personlige kode og din kodebrikke.

Hvis en hacker får kontroll over din private epost kan de logge seg inn på nesten alle tjenester som tillater passordtilbakestilling over epost. Hvis angriperen dermed får kontroll over dine sosiale medier, er det mulig at de kan påvirke, evt ødelegge, ting som vennskap og rykte. Hvis kontoen de får tilgang til er høyprofil og eier for eksempel et selskap, kan de også påvirke selskapets aksjer.

Det finnes flere mottiltak til epost hijacking, en vanlig måte å motvirke det på er å ha «multi-factor authentication» (som ikke er SMS basert, ettersom SMS hijacking er også mulig). Videre kan man ha flere eposter, som også har MFA og forskjellige sterke passord, på denne måten vil ikke angriperen ha kontroll over alt med en epost, altså å ikke ha alle sine egg i en kurv.

Hvis en angriper får kontroll over BankID kan de gjøre mye skummelt, ikke bare inkludert få tilgang til pengene til pengene på kontoen. De kan ta opp forskjellige lån i ditt navn og sende pengene til seg selv. Videre kan de skrive under på flere forskjellige kontrakter i ditt navn.

Oppgave 3. Skadevare (10 %)

Det finnes flere måter å klassifisere skadevare (malware), historisk har vi delt inn i klasser basert på følgende egenskaper: Spredning, Skjuling og Nyttelast.

Definisjoner:

- Spredning
 - o Virus: endrer og infiserer eksisterende filer eller systemer og formerer seg lokalt
 - o Orm: malware som sprer kopier av seg selv uten å infisere andre filer, samt vanligvis uten medvirkning fra mennesker. Har også vanligvis en egenskap å spre seg over nett. Videre vil de i det fleste tilfeller ha en ondsinnet nyttelast, som for eksempel å installere bakdører.
- Skjuling
 - o Rootkit: endrer på operativ systemet for å skjule seg selv.
 - o Torjaner: en applikasjon som gjør noe ondsinnet i bakgrunnen.
- Nyttelast
 - o Skadevare kan ha all type nyttelast som irritasjon, skjulte botnets, blackmail, identitetstyveri, osv.
 - o

Basert på denne metoden klassifiser følgende skadevare, og begrunn hvorfor du har valgt den klassifiseringen (oppgi kilder du har brukt for å underbygge svaret):

- ILOVEYOU
 - o ILOVEYOU kom ut i 2000 og er en orm ettersom den spredde seg over nett (spredde seg over epost), og brukeren måtte manuelt åpne en fil i eposten. (kilde: TK2100_03_Malware.pdf side 32)
- Stuxnet
 - o Stuxnet er en orm, produsert av CIA og Isreal, som brukte flere ukjente exploits for å infisere atomreaktorer i Iran. Stuxnet brukte en infisert usb pinne og exploits som gjorde at ormen installerte seg selv inn i systemet og nettverket når pinnen ble satt inn. (kilder: <https://www.malwarebytes.com/stuxnet> TK2100_04_Kinetisk.pdf)
- Brain
 - o Brain er et ikke destruktivt virus som kom ut i 1986, Brain infiserte floppy disk og erstattet boot sektoren med seg selv, mens den originale sektoren ble flyttet til et annet sted.
- WannaCry
 - o WannaCry er en nettverksorm som sprer seg selv ved bruk av en exploit i TCP port 445 (Server Message Block) som heter ETERNALBLUE, hvis den får kontakt bruker den en annet exploit som heter DOUBLEPULSAR for å installere seg selv på det nye systemet. (kilder: <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry> <http://blog.talosintelligence.com/2017/05/wannacry.html>)

Oppgave 4. Kryptering (10 %)

Forklar forskjellen på RSA kryptering og RSA signering, forklar hvordan de to anvendelsene fungerer.

En avsender Alice ønsker å sende en epost til Bob og ønsker både å oppnå konfidensialitet og integritet, tegn og forklar hvordan dette kan oppnås.

Siden RSA er asymmetrisk og gir to nøkler, K^+ og K^- , der bits som er kryptert med K^+ kan kun bli dekryptert av K^- , og omvendt. Det er viktig å huske at bits som er kryptert av en nøkkel ikke kan bli dekryptert av samme nøkkel.

Kryptering av tekst handler dermed om å kryptere bits med en annen sin offentlig nøkkel, mens signering blir dermed gjort ved å kryptere bits med din egen private nøkkel.

Hvis Alice vil sende en sikker epost til Bob, så kan hun først kryptere meldingen med sin egen private nøkkel, så Bob sin offentlige nøkkel. Når Bob får den krypterte meldingen vil han først dekryptere med sin private nøkkel, og så dekryptere med Alice sin offentlige nøkkel.

Oppgave 5. Kryptering (utregning) (10 %)

Formelen for dekryptering er: $M = C^d \bmod n$ der M er det originale tallet og C det krypterte tallet. (TK2100_01-kryptering.pdf side 58)

Dermed blir fremgangsmåten ved hjelp av GeogebraCAS

(<https://www.geogebra.org/cas>) som bruker Mod(Dividend number, Divisor number):

Input:	Output:	ASCII kode:
Mod(1759^(2753),3233)	68	D
Mod(2160^(2753),3233)	117	u
Mod(1992^(2753),3233)	32	[Mellomrom]
Mod(690^(2753),3233)	107	k
Mod(1632^(2753),3233)	97	a
Mod(2235^(2753),3233)	110	n
Mod(1992^(2753),3233)	32	[Mellomrom]
Mod(1859^(2753),3233)	82	R
Mod(2680^(2753),3233)	83	S
Mod(2790^(2753),3233)	65	A

Som blir til klarteksten: «Du kan RSA»

Oppgave 6. Nettverk (10 %)

Forklar hvilke sikkerhetsutfordringer vi har på linklaget i TCP/IP modellen. Tegn og forklar hvordan en angriper kan utføre «Man-in-the-Middle» angrep mot et mål som er koblet til samme switch som angriperen, og vis hvorfor dette er mulig ved å forklare hvordan ARP protokollen fungerer.

TCP/IP og Switch bruker MAC adresser for å sende informasjon til riktig maksin, men det er mulig å endre sin egen MAC adresse. På denne måten kan man spoofe mac adresser (late som at man er en annen).

ARP protokollen er en tabell som inneholder IP og MAC adresser og cacher alt som blir sendt til den, selv om den allerede har en MAC-adresse koblet til en IP-adresse. Nå kan Eve, som vil høre på samtalen til Alice og Bob, si til Alice sin ARP protokoll at Bob sin MAC-adresse er Eve sin MAC-adresse. Samt si til Bob at Alice sin MAC-adresse er Eve sin MAC-adresse.

Nå vil Eve høre alt det Alice sender til Bob, og vice-versa. Nå trenger eve bare å videresende det de får inn, og ingen ville lagt merke til at de blir avlyttet.

Oppgave 7. Phishing (10 %)

Forklar hva phishing er og hvordan en hacker kan utnytte dette for å angripe et selskap. Drøft tekniske og personellmessige løsninger på denne angrepsvinkelen.

Phising er en anngripsmetode som går ut på å få offeret til å dele personlig informasjon om seg selv, som passord, identitet, bank informasjon, osv. Dette blir ofte gjort ved bruk av ondsinnede nettsider som ser troverdige ut. En angriper kan gå løs på et selskap ved å sende personale emailer som linker til en ond kopi av selskapets nettside som videresender informasjonen som blir tastet inn. Angripere kan bruke sofistikerte metoder for å skjule forfalskninger, som å bytte ut i med l, eller a (latin) med a (cyrillic) osv.

For å forhindre phising angrep kan man lære opp personale om at phising er en ting, og at de kommer til å bli utsatt for det og være oppmerksom på lenker man klikker. Fra et teknisk standpunkt kan selskapet blackliste alle url adressene som de vet er falske. ikea.com vil for eksempel blackliste ikea.com (liten L).

Oppgave 8. Hjemmekontor (10 %)

Under pandemien har det blitt vanlig med hjemmekontor for de fleste selskaper og ansatte med typisk «kontorarbeid». Drøft hvilke utfordringer dette utgjør for

datasikkerheten i selskapene. Hva mener du må endres for å ivareta sikkerheten hvis hjemmekontor blir den «nye normalen» også etter pandemien?

problemet med hjemmekontor er at et selskap ikke har lyst til å legge ut sitt interne nettverk på internett og gjøre det åpent for masse forskjellige angrep. Videre er et annet problem det at personale kan ha sensitiv informasjon på deres hjemme pc, dermed kan det svakeste punktet bli inngangsdøren til personalet.

Løsninger nettverksproblemet kan være ting som VPN programmer, som gjør det mulig å logge inn på selskapets interne nettverk over en privat tunell og MFA for å komme seg inn på nettverket.

Løsningen for sensitiv informasjon på harddisk kan være påbud om å kun lagre informasjon på selskapets servere, altså å ha så lite informasjon som mulig på selve pcen. Videre kan en kreve at personale må bruke disk kryptering som BitLocker.


Oppgave 9. Praktisk SSL analyse (10 %)

Du skal utføre en analyse av «Usikre TLS ciphers» ved hjelp av standard verktøy for dette. Du skal teste følgende domene:

`https://demo.testfire.net`

Dette er et test-domene som er laget for å lære seg om penetrasjonstesting, og eiet av IBM. (Du skal ikke besøke URLen selv, kun bruke standard verktøy for SSL/TLS analyse, du har heller ikke tillatelse til å bruke andre typer hacker/pentest verktøy.) Vurder hvor sikker krypteringen (TLS) er på denne webserveren, trekk spesielt frem svake algoritmer som brukes i kryptert kommunikasjon med serveren.

Jeg velger å bruke ssllabs.com/ssltest/ og får dette resultatet når det gjelder Cipher Suites

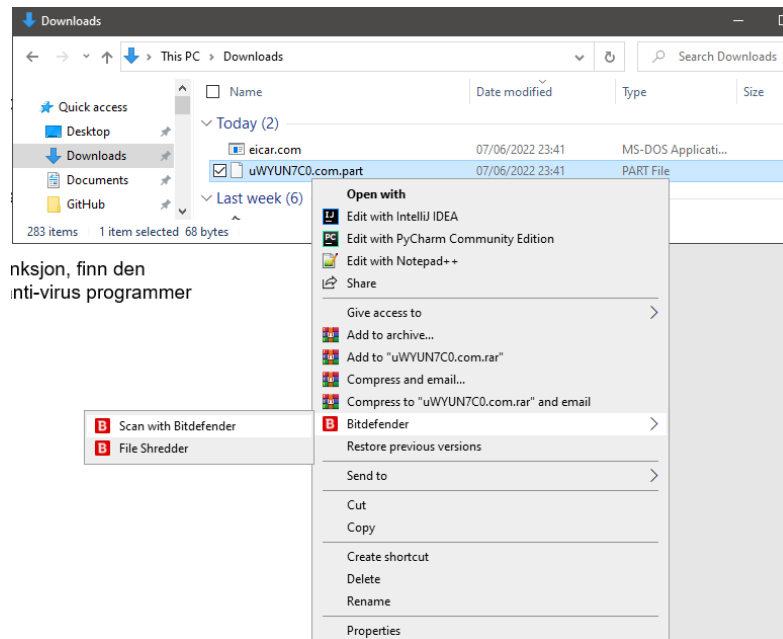
 Cipher Suites			
# TLS 1.2 (server has no preference)			
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 1024 bits FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 1024 bits FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	EC DH sec571r1 (eq. 15360 bits RSA) FS		128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 1024 bits FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 1024 bits FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	EC DH sec571r1 (eq. 15360 bits RSA) FS		256
# TLS 1.1 (server has no preference)			
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	256
# TLS 1.0 (server has no preference)			
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	EC DH sec571r1 (eq. 15360 bits RSA) FS	WEAK	256

Som man ser leser nettsiden nesten alt som svakt.

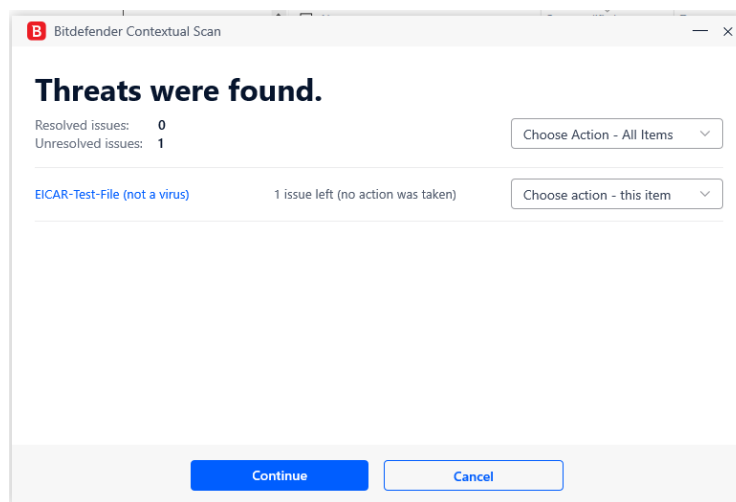
Oppgave 10. Praktisk anti-virus (10 %)

I denne oppgaven skal du demonstrere din kunnskap om bruk av anti-virus programvare. Last ned test filen EICAR fra https://www.eicar.org/?page_id=3950, du kan enten laste ned en av filene eller du kan opprette en ny fil med de 68 karakterene som utgjør «virusets» signatur som beskrevet nederst på siden (og som brukt i øvingstimene). Du skal videre demonstrere følgende:

- **Scan filen med ditt anti-virus program, vis at anti-virus programmet oppdager filen og rapporterer den som skadevare**



- o personlig bruker jeg Bitdefender, der er det så enkelt at test filen blir funnet og satt i karantene med en gang... Så man må ta den ut av karantene for å kunne scanne den manuelt.



- o Her kan man se at filen ble sett, og man kan velge hva man vil at skal skje med den.
- Gå inn i ditt anti-virus program sin karantene (quarantine) funksjon, finn den detekterte filen og eksporter den ut av karantene (for noen anti-virus programmer er det mulig du må skru av sanntidsbeskyttelse først)

The screenshot shows the Bitdefender Antivirus interface. On the left is a dark sidebar with icons for Dashboard, Protection, Privacy, Utilities, Notifications (with a red badge showing 4), and Settings. The main area is titled 'Antivirus' with tabs for Scans, Settings (selected), and Advanced. Under the Settings tab, there are sections for 'Manage exceptions', 'Quarantined threats', 'Scan CD & DVD', 'Scan flash drives', and 'Scan mapped network drives'. Each section has a description and a dropdown menu. The 'Quarantined threats' section has a red box around the 'Manage quarantine' link. Below the main interface is a window titled 'Manage Quarantine' showing a table of 'Quarantined Items'. The table has columns for File Name, Threat Name, Original Location, and Date. One item is listed: '0ZGPKtux.com.part' with threat name 'EICAR-Test-File (not ...)' and location 'C:\Users\... Download...'. At the bottom of the window are 'Restore' and 'Delete' buttons.

[Return to Protection](#)

Antivirus

Scans Settings Advanced

Manage exceptions
Add or remove items to be excepted from scan. [Manage exceptions](#)

Quarantined threats
Restore or delete threats that have been quarantined. [Manage quarantine](#)

Scan CD & DVD
Check if content on CDs and DVDs is threat-free. Ask every time

Scan flash drives
Check if content on flash drives is threat-free. Autoscan

Scan mapped network drives
Scan mapped network drives on connection. Disabled

Manage Quarantine

Quarantined Items

Restored files will be automatically excepted from scanning. [View Settings](#)

<input type="checkbox"/> File Name	Threat Name	Original Location	Date
<input checked="" type="checkbox"/> 0ZGPKtux.com.part	EICAR-Test-File (not ...)	C:\Users\... Download...	07-Jun-22 11:36 PM

Restore Delete

- o Her ser man karantenen til Bitdefender, og hvordan man tar den ut av karantene. Dette var nødvendig før steg 1, ettersom filen ble satt i karantene til å begynne med...