Eksamen

Oppgave 1
Det innebär att förhindra information som läcker ut, manipuleras eller förstörs. Det handlar också om att göra information tillgänglig när den behövs till rätt person. Det omfattar information som är tryckt på papper, lagrad elektronik som överförs på mejl, post, visas på film eller yttras i konversation.

CIA-modellen:
C = Confidentiality. Att undvika oauktoriserad tillgänglighet till information. Skydda data, ge bara tillgång till de som fått tillåtelse, spärra alla andra från att lära sig något om datan.
I = Integrity. Förhindra manipulering av information. Att information ej har blivit ändrad på ett oauktoriserat sätt.
A = Availibility. Se till att information är tillgänglig för, och möjlig att ändras inom rimlig tid av de som är auktoriserade till det.

Med dessa tre principer utgör de varje organisations säkerhetsinfrastruktur. CIA är så grundläggande för informationssäkerhet att när som helst när data läcks ut, ett system attackeras, en användare tar ett phishing-bete, ett konto kapas, en websida skadas eller andra säkerhets incidenter inträffar är det säkert att en eller flera av dessa principer har överträtts.

Oppgave 2
Ett av det vanligaste sättet att råka ut för en attack mot just dig är att du inte har uppdaterat din software. En uppdatering hjälper inte bara för att fixa bugs, utan även för att hjälpa dig med sårbarheter. Operativsystem på din dator, mobila enheter eller en programvara som kör ditt trådlösa nätverk måste regelbundet uppdateras för att hjälpa dig från hackers.Så håll alltid allt uppdaterad. Ditt datasystem, din mobiltelefon, alla dina applikationer håll de uppdaterade för att hjälpa dig att bli skyddad mot hackare som utnyttjar sårbarheter i dina programvaror.

Brist på information är en annan vanlig anledning att du råkar ut för en attack. Många tänker det där händer inte mig eller att de är immun för att få en attack emot sig. Men med ett litet klick på en websida kan leda till stora problem i ditt liv privat och i arbete. För att försvara dig bättre mot att bli hackad så läs på och studera olika sätt som hackare kan ta sig in på ditt datasystem på. Information och förståelse kan hjälpa dig ta bättre beslut för att vara skyddad.

En hacker kan få fäste i ditt system för att du har brist på skydd. Antivirusprogram, kryptering av din hårddisk, inget bioslösenord eller lösenord när du loggar in på din dator. Alla dessa är exempel på saker folk inte har på sin dator för att skydda sig. De

flesta har ett inbyggt antivirusprogram, men man behöver så mycket mer för att skydda sig. Se till att du har alla antivirusprogram du behöver och skapar ett lösenord med hög bitstyrka eller ett med många olika typ av ord som inte är på engelska.

En hacker får tilgang til kontoene dine ved å enten gjette eller brute force passordet. Tiltak for å forhindre dette er å velge seg et langt passord som inneholder bokstaver, tall og spesialtegn.

Oppgave 3.
Når man snakker om skadevare blander man ofte virus og ormer. Både virus og ormer er ondsinnede software som utfører uønskede og vanligvis skadelige handlinger.

Hovedforskjellen er distribusjonsmetoden.Et virus går inn og endrer et system eller filer lokalt, og uten disse filene kan ikke viruset leve eller spre seg. Så måten virus kan spre seg på er om noen laster ned en av disse filene som inneholder viruset. Et virus inneholder ofte en skadelig kode som kan utføre handlinger etter en bestemt tidsperiode.
En orm derimot kan spre seg automatisk over nett fra maskin til maskin uten at den infiserer og endrer andre programmer lokalt. Oftest med hjelp av epost. Ormen lager en kopi av seg selv og sender den til neste maskin
.
Nå som AI er på fremmarsj kan vi ikke utelukke at skadevare software utviklerne begynner å ta bruk dette for lage “smarte” skadevare software. Dette er skadevare software som på egenhånd kontinuerlig endrer seg selv gjennom læring for å tilpasse seg anti-malware tiltak og selvstendig kan avdekke og utnytte nye uoppdagede sårbarheter.
For å beskytte oss mot dette kan vi utvikle AI anti-virus som på egenhånd kan identifisere og håndtere nye trusler gjennom læring.

Et fremtidig problem med virus er at pengene man tjener på hacking kan øke pga dataen man kan skaffe er mer verdifull. som gjør at det blir flere såkalte «hackere». Dette kan gjøre at de flinkeste hackerne ender opp med å lage skadvare som er bedre enn antiviruset, og andre sikkerhetstiltak. Dette kan bli et stort problem for mange ettersom de ikke har kontroll på hva som er trygt og ikke trygt å gjøre. Nesten alle har både bankappen og bank id på samme mobil, som gjør at viss hackeren får tilgang til mobilen din og pinkodene dine kan personene trekke penger fra deg, og skrive under på avtaler med din digitale signatur.

En måte man kan beskytte datasystemer er at flere folk blir flinkere til å bruke bra passord og ikke ha samme pinkode på alle ting. Mange har samme pinkode på mobil, mobilbank og bank id på mobil. Som gjør at om noen

Oppgave 4
Forskjellen på Diffie-Hellman (DH) og RSA som asymmetriske algoritmer er at Diffie-Hellman er en nøkkelutvekslings algoritme, mens RSA er en krypterings algoritme. Nøkkelutvekslings algoritme kan to parter ved hjelp av hver sin vilkårlige private nøkkel og hvert sitt utregnet felles offentlig tall som deler, regne seg frem til en felles delt hemmelig krypteringsnøkkel. For å knekke Diffie-Hellman bruker man diskre logaritme. Mens med RSA tar utgangspunkt i to veldig store primtall for å genere en privat- og en offentlig nøkkel, og man bruke det for å for eksempel en melding. Man kan knekke RSA ved hjelp av faktorisering.

Diffie-Hellman kan brukes for å utveksle krypteringsnøkkel. RSA kan også brukes for å utveksle krypteringsnøkkel, men kan i tillegg bruke for å kryptere/dekryptere og for digital signering (autentisering).

I asymmetrisk kryptering har man et nøkkelpar, en offentlig nøkkel og en privat nøkkel. Den offentlige nøkkelen brukes for kryptering, for eksempel kryptering av en melding, og den private nøkkelen brukes for å dekryptere meldingen. I praksis vil to parter som ønsker å kommunisere ha vært sitt nøkkelpar. Partene holder sin private nøkkel hemmelig, men deler sin offentlige nøkkel med den andre. Når den ene parten sender en melding bruker vedkommende den andre partens offentlige nøkkel for kryptere, og mottakeren bruker sin private nøkkel for å dekryptere meldingen. På denne måten kan man dekryptere uten å måtte dele en privat nøkkel.

I praksis brukes Diffie-Hellman i SSH, TLS(HTTPS) for sikker nøkkelutveksling. RSA Brukes til blant annet å kryptere e-post.

Oppgave 5.
Da TPC/IP modellen ble utviklet på 80-tallet og ble bygd for tilgjengelighet slik at man raskt og effektivt kunne kommunisere og dele data. Hvis vi ser det i lys CIA-modellen er ikke TCP/IP modellen er en sikker modell. Modellen oppfyller ikke kravet til konfidensialitet**,** da det er ingen krav om kryptering, og hvem som helst kan lytte til trafikken. Videre er det ingen sikkerhet mot endring/manipulering av trafikken, og oppfyller derfor ikke kravet til Integritet**.**

Med disse sårbarhetene gjør det at World Wide Web, som brukes av mange, den største og mest utsatte angrepsflaten, og er også her mesteparten av malware spres. De store sårbarhetene åpner for at angripere kan spoofe, stjele, endre og slette data og omdirigere trafikk.

En angriper som får tilgang til nettverket kan manipulere MAC-adresser og ARP-meldinger gjennom ARP-spoofing og -cache-poisioning for å lese og endre data mellom klient og tjener (man in the middle angrep).

En angriper kan utnytte hand-shake prosessen i TCP-protokollen for å utføre SYN flod angrep(DoS) angrep samt skjule avsenderadresse (IP-spoofing). I TCP kan også utnytte ACK-num og metningskontroll. En angriper kan også prøve å gjette ACK-nummer for å kunne sesion-hijacke.

Tiltak for å sikre oss på best mulig måte:

- Bruke brannmur i routere og i maskiner
- Bruke antivirus og sørge for at OS og andre apper alltid er oppdatert.
- Ta i bruk protokoll for autentisering
- Kryptere pakker
- Øke kunnskapen om informasjonssikkerhet i befolkningen

Oppgave 6.

Det er viktig og sikre webapplikasjon for SQL Injection, en måte du kan stoppe det på er å gi brukeren feilmeldingene, du burde heller lagre disse i en notisblokk eller noe annet sted bare selskapet kan se. du kan også validere input føre det blir sendt til backend din så ikke kode som ikke har noe der å gjøre kommer igjennom. man må også beskytte seg for cross site scripting, samme her må du validere input føre det blir sendt videre.

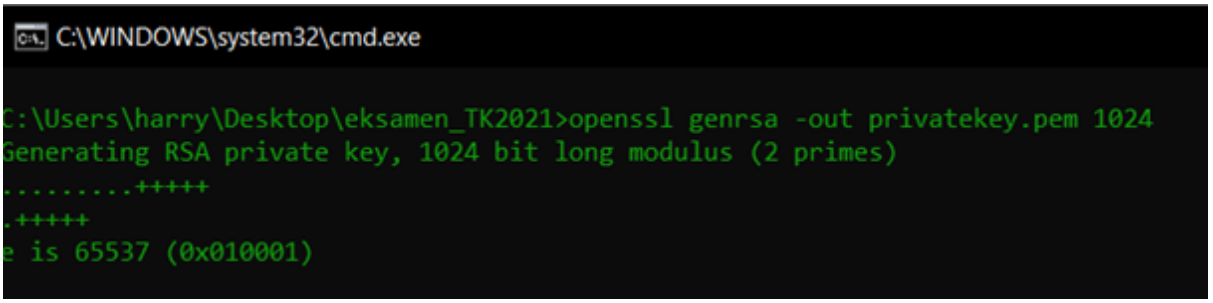
passe på at urlene har god sikkerhetskontroll så det ikke er bare å skrive hack.com/admin. dette kan man sikre med aksess kontroll.
se om det er noe feil med sesjon cookies så ikke hvem som helst kan ta de å endre de så man kan logge inn uten passord osv.

Oppgave 7.

En utfordring kan være at man ikke har like sikkert hjemmenettverket som arbeids nettverket. Dette gjør at hackere lettere kan bruke dette som angrepspunkt. Et annet problem er om mye av arbeidet er lagret og huset brenner ned så kan man miste viktig data. En annen ting er at det er større sjanse at noen bryter seg inn i private hjem, det er også oftest mindre sikkerhet på låser i private hjem. Så om dette er et planlagt angrep for å stjele pc-en, eller ikke så kan dette medføre lekkasje av sensitiv data og kundeinformasjon. Mange kan også besøke farlige nettsider som gjør at man kan få virus på datamaskinen man bruker til jobb, eller at man putter inn en minnepenn man har brukt før som inneholder et virus som sprer seg med at man putter den i en ny datamaskin. Man kan også være mer utsatt for phishing-angrep, når man sitter hjemme og får en melding med «viktige» nyheter er det lettere å ta en 5 minutter til å lese, dette kan hackere bruke for å få deg til å komme inn på flaske nettsider som prøver å få tak i passordene dine.

Oppgave 8

1. Genererer 1024 bit RSA-nøkkel i fil privatekey.pem



2. Innholdet i filen privatekey.pem:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDY7R7maHrZyTa5uhap9HtYiPHDBU+k+9rydOb7PWbugwdn5Zl+
EJNUXgFzqltdWHDn9o+GEJn+UxZBTquIj7NuwCZyb6SLVoRAfE6pwkSG3d6lL1qU
NQ7DST/RNiYjStL5HLuuaHCYzpRX5QDCL9bx0tb3RtpITI9AsZR8reSGVQIDAQAB
AoGAW0XSJZI6dp5SF210EcibiZH9X1hBvaJ26mNDuNyKDbs2B4I0xjVFOE9hfwBj
9u+6ee9lTjx3/umIyKvIQuprzVwT8a01qZ6jdzSvDIuv54ns+KYhN3hla5k+Tew7
eM0Zh7XCXr3W+ejh2Ic4UnDuT5WcUl3t+haizQhkVESmcCECQQD407/YRSyfjuip
IiGF+bjsjsossc3R4cpui+BGk7TLyeFWJ25kRDUA70pNNDZ/K/JPBJ8nvMYU3zuF
oLJajIlpAkEA3y30aWyLlJILmC64lBzNIJIlRTTjrAklZEVODm12nT3o9tg9YLUW
IJaVzckYYiEqnGWMRCLA+rs6kfWC0BesDQJBAJ7Gp6U+RsIt88JxGAkgl2LDnri0
YIxr0ruFoAAJIpXjZVmPYb6zU0scZkIrbhbqGP1ZCqHVsGQDKj0TlJt5D/kCQCdY
kLhtXIZK4SRpSD1Efp15Zny3AFR6IE93MHW2sqyyF3o9UUTVaBtCsRJgm53hPwPn
mzz/64nIrGDDKdbJ9ZkCQQD0lPKHNJRwAuNen/ul8MLwJ4/yP65DERnnL4R58gpi
rq0CMKZImoj3m6eviYGS34GgJwU2/LPKFS22R7y3Nbe/
-----END RSA PRIVATE KEY-----
```

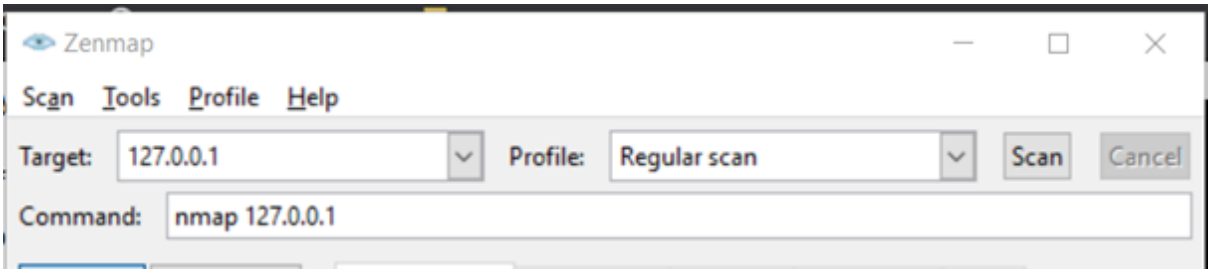
3. Vi henter ut public keyen fra filen privatekey.pem, og skriver det ut til en ny fil publickey.pem:

4. Innholdet i filen publickey.pem:

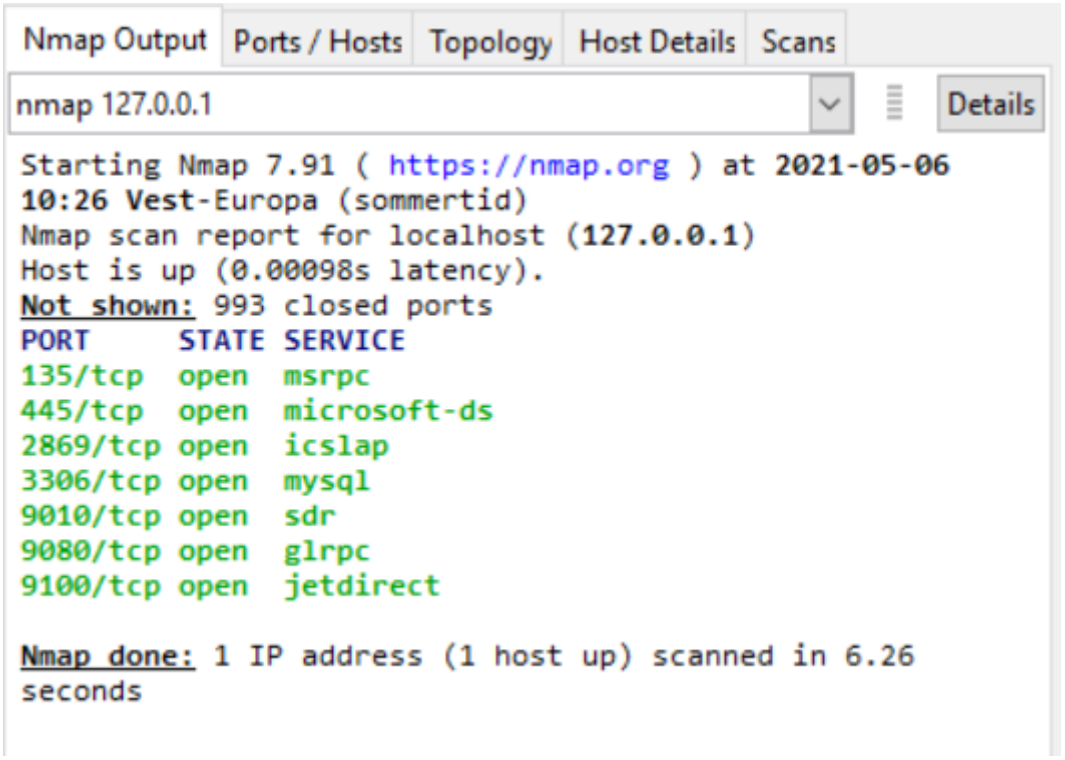
```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDY7R7maHrZyTa5uhap9HtYiPHD
BU+k+9rydOb7PWbugwdn5Zl+EJNUXgFzqltdWHDn9o+GEJn+UxZBTquIj7NuwCZy
b6SLVoRAfE6pwkSG3d6lL1qUNQ7DST/RNiYjStL5HLuuaHCYzpRX5QDCL9bx0tb3
RtpITI9AsZR8reSGVQIDAQAB
-----END PUBLIC KEY-----
```

Oppgave 9

Vanlig scan av egen PC:



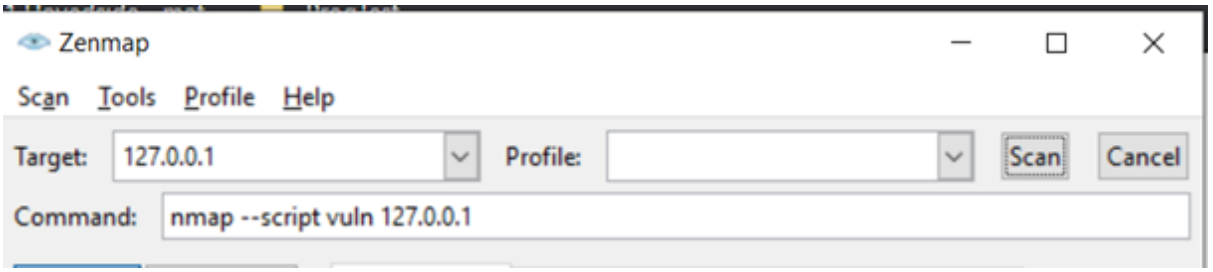
Output:



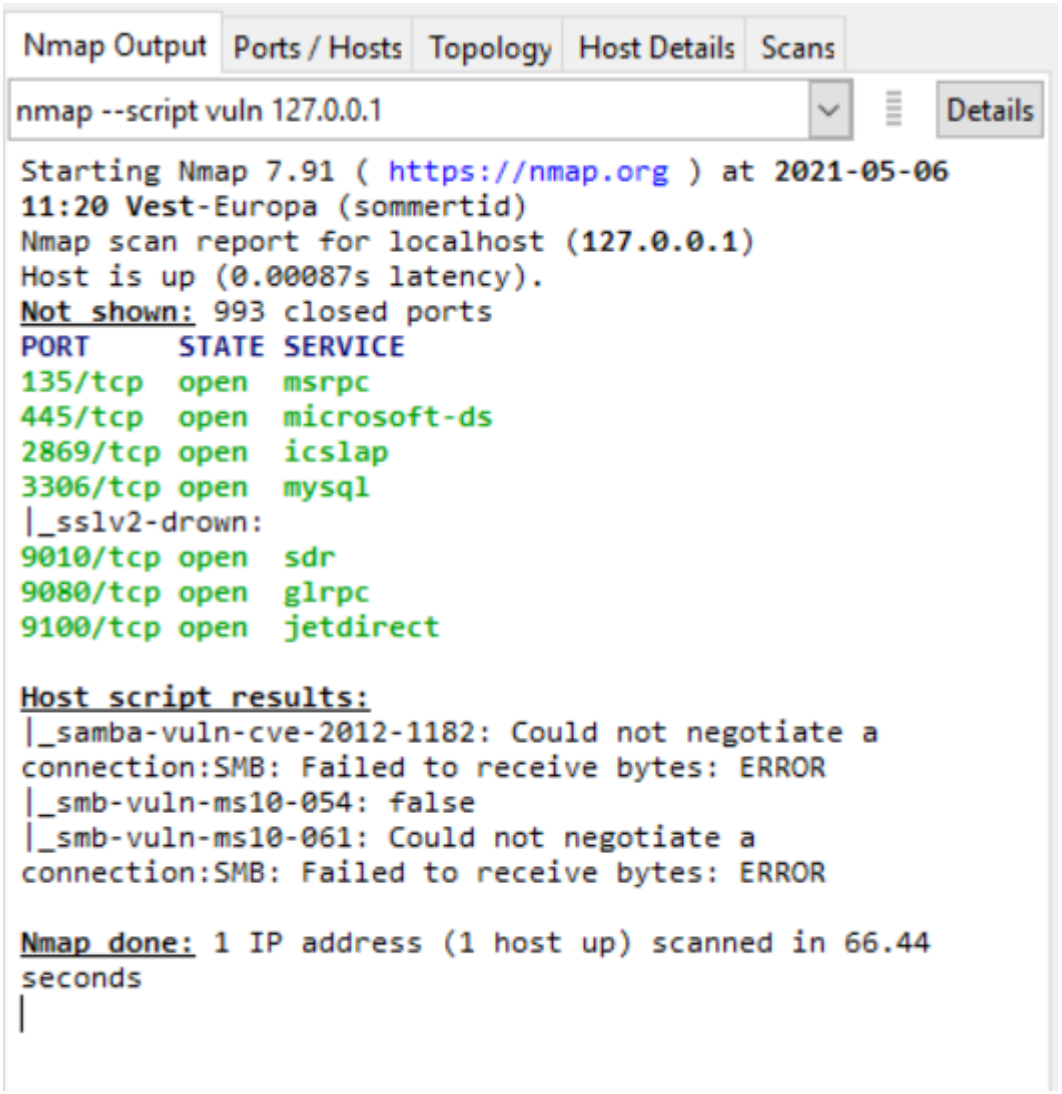
Vurdering av resultatet:

- Pingingen viser latency (forsinkelse) på 0.00098 sekunder, som er gjennomsnitthastigheten på de 4 fire ICMP pakkene som ble sendt
- Scan av TCP-portene lister opp portene samt portnummer, om de er åpne eller lukket og service-protokoll. Åpne porter som er en mulig sårbarhet som angripere kan utnytte. Jeg må vurdere om jeg skal stenge portene.

Scan egen PC med --script vuln



Output:



Vurdering av resultatet:

- Pingingen viser latency (forsinkelse) på 0.00087 sekunder, som er gjennomsnitthastigheten på de 4 fire ICMP pakkene som ble sendt
- Scan av TCP-portene lister opp portene samt portnummer, om de er åpne eller lukket og service-protokoll. Åpne porter som er en mulig sårbarhet som angripere kan utnytte. Jeg må vurdere om jeg skal stenge portene.

- Tre av av de åpne portene bruker SSL2? Protoll som påvirker krypterin av HTTPS. Står ikke eksplisitt at PCen min er utsatt.
- samba-vuln-scriptet feilet