IN1020 - Datasikkerhet og nettverkskommunikasjon: Løsningsforslag gruppetime 9 (uke 43)

1 Teori- og diskusjonsoppgaver

1. DNS

   (a) Et DNS-navn er 2 eller flere ord med punktum imellom som man bruker for å koble opp mot maskiner på internett i stedet for å huske på IP-adressen til maskinen. Vi benytter dette da IP-adresser ikke er særlig menneskevennlig (vanskelig å huske). Det er også flere tjenester som bedre lar seg løse ved å koble navn til IP-adressen, som f.eks. aliasing (fler DNS-navn til én IP) og round-robin DNS (samme DNS-navn går på rundgang mellom flere IP-adresser).

   (b) De holder oversikten over hvilke maskiner som har ansvaret for hvert TLD (Top Level Domain). TLDer er det høyeste nivået i DNS-hierarkiet, ordet etter det siste punktumet (f.eks .org, .net, .com, .no).

2. Forbindelsesstrategier

   - Pull: En klient initierer en forbindelse til en tjener (innholdsleverandør) med forespørsel om en tjeneste. Eks. HTTP eller FTP.
   - Push: En tjener "dytter"innhold til en klient når den har noe relevant å levere. Initiert av innholdsleverandøren. Eks "Pushmeldinger"på mobil, HTTP/2 Push.
   - Publish-subscribe: Mange klienter abonnerer på en tjeneste. Tjeneren dytter innhold til abonnentene nå den har noe interessant å levere. Eks. Rich Site Summary (RSS)

3. Aksessmodeller

   - Klient-tjener: Typisk pull-tjeneste. Tjeneren har en spesiell rolle der den leverer en tjeneste til mange potensielle brukere. Eks. HTTP eller IMAP mail.
   - P2P: alle noder i nettverket er likeverdige og samarbeider om å levere en tjeneste. Eksempler: Bittorrent, The Onion Router (TOR), Bitcoin

4. CDN

   (a) Innhold som trenger å leveres til svært mange brukere over hele verden kopieres til mange maskiner som ligger fysisk nær sluttbrukerne. Dette gjør at kildemaskinen ikke blir overbelastet og sparer kapasitet på nettverket.

   (b) i. Å ha innholdet fysisk nærmere brukeren reduserer round trip time (RTT) og gjør det derfor raskere å aksessere,
   ii. Ved å cache innholdet nær brukeren sparer man trafikk over backbone-nettet
   iii. Ved å distribuere innholdet, avlaster man tjeneren som leverer dette innholdet, noe som gir en mer skalerbar tjeneste.

5. En måte å strømme video ved hjelp av HTTP-tjenere. Videoen "klippes" opp i små uavhengige segmenter som kan kodes i flere kvalitetsnivåer. Dette gjør at en klient kan spørre etter høy kvalitet i perioder når den opplever gode nettverksforhold og redusere kvaliteten når forholdene er dårligere.

6. HTTP

   (a) En TCP-forbindelse opprettes med et 3-veis håndtrykk, om SSL skal brukes, forhandles dette frem ved å først bruke asymmetrisk kryptering til å utveksle en felles nøkkel for videre symmetrisk kryptering av forbindelsen. Klienten sender så en GETforespørsel på det aktuelle dokumentet til HTTP-tjeneren. Tjeneren leverer et "200 OKsvar tilbake sammen med det aktuelle dokumentet. Om hjemmesiden inneholder dokumenter fra flere kilder opprettes tilsvarende forbindelser for å hente resten av det aktuelle innholdet.

   (b) HTTP bruker TCP og har port 80 som standard.

   (c) En ikke-persistent forbindelse blir lukket så snart et svar er levert. Påfølgende forespørsler må åpne en ny forbindelse. En persistent forbindelse vil gjenbruke den samme forbindelsen til flere forespørsler.

   (d) https med digitale sertifikater hindrer falske nøkler og falske tjenester. Den offentlige nøkkelen til en entitet inngår i en ubrutt kjede av sertifikater (med nøkler) som går god for hverandre, helt opp til det øverste nivået, rot-sertifikatet. Det er vanskelig for svindlere å generere og spre falske nøkkelpar til allerede etablerte tjenester.

   Digitale sertifikater hindrer ikke svindler i å opprette et gyldig domene, f.eks. sparebnak1.com, generere privat/offentlig nøkkelpar, og få dette signert av en tiltrodd sertifikatutsteder. Denne fremgangsmåten benyttes ofte i svindel-angrep

   HTTPS bidrar altså **kun** til å krypterer kommunikasjonen og verifiserer motparten.

   (e) HTTPS har port 443 som standard.

7. Sosial manipulasjon:

   (a) Phishing-angrep utnytter menneskelige svakheter: Uvitenhet, godtroendehet, mangel på bevissthet rundt farene ved også digital svindel.

   (b) Sikkerhetstiltak for å forebygge phishing angrep: Opplæring, slik at folk kan klare å identifisere potensielle farer, f.eks. personer som utgir seg for å være legitime personer, og falsk epost. Praktiske sikkerhetstiltak kan være god filtrering av epost, benytte epost-autentisering, samt forsøke å avdekke og deretter tydelig varsle om falske tjener-sertifikater.

   (c) i. Snike seg inn etter andre ("tailgating"). Bære store esker og få hjelp til å åpne døra. Produsere og benytte et falskt tilgangskort.

   ii. Sende tilpasset phishing-epost med skadevare vedlagt Sende tilpasset phishing-epost med lenke til webside som inneholder en exploit for en zero-day-sårbarhet som finnes på direktørens maskin.

8. Ingen fasit. Tips til hvordan finne ut informasjon om bildet: Kommandoen exiftool på en Unix-maskin på Ifi (feks. login.ifi.uio.no). Google maps el. for å plassere GPS-koordinatorer på kartet. Du kan også finne informasjon om enheten benyttet til å ta fotoet, inkludert OS-versjon. Er dette noe som potensielt kan utnyttes? Tidspunkt bildet er tatt.

   Brukernavn kan f.eks. brukes i phishing, eller kanskje brute-force-angrep.

9. Dataangrep:

   (a) Dette er selvsagt basert på WannaCry, så hovedpersonen hadde nok ikke gjort noe galt her. Det som sikkert er skjedd er at en av kollegaene har åpnet en mail der ransomware-en lå. WannaCry er en orm, så denne kunne derfra infisere andre maskiner i nettverket. Hvis studentene mener hovedpersonen er skyldig selv kan årsakene være mange.

   (b) Det riktige svaret er kryptovirus/løsepengevirus/ransomware.

(c) Arbeidsplassen kunne tatt regelmessige backup av dataene sine og lagret dem adskilt fra arbeidsstasjonene. De kunne også fokusert på opplæring om hvilke e-post man bør åpne og hvilke som er mistenkelige. Dette er ikke en garanti, siden mennesker ikke klarer å ha fullt fokus og ta gode valg absolutt hele tiden. De kunne også hatt en form for spam-filter i epost-tjeneren sin, som kanksje kunne klart å filtrere vekk også denne typen skadevare. Arbeidsplasser bør også oppdatere operativsystemene de benytter med alle tilgjengelige sikkerhetsoppdateringer, siden slike type angrep svært ofte utnytter kjente sårbarheter i f.eks. operativsystem. En seriøs arbeidsplass bør ikke bruke operativsystemer som er så gamle at OS-leverandøren ikke lengre støtter operativsystemet, og dermed heller ikke bruker ressurser på f.eks. sikkerhetsoppdateringer. Når angrepet først er i gang og man ser skadevare spre seg kan det faktisk være lurt å bare skru av alle maskinene. Dra ut kontakten. Selv om krypteringen har startet tar det litt tid å komme gjennom alle filene, så noe kan reddes på denne måten. I etterkant bør man ikke betale. Det er svært sjelden man får data tilbake, dekryptert, ved å betale utpresserne, i tillegg kan det være usolidarisk ettersom man da er med på å oppfordrer angriperne til å fortsette siden det tydeligvis er vellykket.

(d) Tilgjengelighet. Ikke integritet, siden den ikke fjerner eller endrer filene, slik et integritetsangrep typisk gjør.

(e) wannaCrypt0r fra mai 2017, som rammet helsetjenester, banker og en rekke andre selskaper over hele verden.

10. Tjenestenektangrep:

(a) Tjenestenektangrep berører sikkerhetsmålet tilgjengelighet, i og med at tjenester som utsettes for angrepet blir utilgjengelig for den som har legitimt behov for tjenesten.

(b) Å spre skadevaren løsepengevirus (kryptevirus/ransomware) er en vanlig angrepsform. Skadevarer virker ved å kryptere sentrale (ofte alle) filer i et IT-system (på f.eks. en datamaskin), med en for offeret ukjent krypteringsnøkkel, slik at systemet ikke fungerer og blir utilgjengelig. En annen form er tradisjonelle DDoS-angrep, som består i å "bombardere" tjenester med nettverktrafikk på en slik måte at tjenestene/serverne overbelastes og dermed ikke er tilgjengelige for andre . I DDoS-angrep bruker hackerne ofte såkalte *botnett*, som er nettverk av maskiner de har tatt kontroll over med f.eks. skadevare, uten av eier/bruker av maskinen er klar over det. Det skal som regel ganske store mengder samtidig nettverkstrafikk til for å kjøre en tjeneste i senk. En annen form for tjenestenektangrep (nevnt i læreboka) er f.eks. å bombardere en bruker med så mye søppel-epost (spam) at vedkommende ikke får tak i og lest epost som er reell.

(c) Tiltak mot løsepengevirus er nevnt i oppgave 1 c). Mot DDoS-angrep kan det være vanskelig å beskytte seg, men et tiltak er å ha tilstrekkelig robuste systemer, men f.eks. redundans, samt mulighet til avvis en del trafikk fra spesielle domener/IP-ranger i f.eks. en brannmur. Internettleverandører kan også gjøre tiltak for å stanse denne typen skadelig trafikk på et nivå utenfor selve virksomheten som er målet for angrep. For søppel-epost kan spamfiltrering være et godt tiltak.

11. HTTP-cookies:

En HTTP-cookie hjelper nettsider med å holde på info om brukere, slik at preferanser ikke tilbakestilles og brukeren logges ut hver gang de går til en annen del av siden. F.eks. at handlekurven din i en nettbutikk ikke slettes. Det finnes persistente cookies og session cookies. Førstnevnte lagres i brukerens sekundærminne, som kan være slitsomt ettersom de tar plass. Nettsider bruker cookies til å samle mye ekstra info om de besøkende. Hvilke knapper de trykket på, hvor lenge de var der. I tillegg har vi third party cookies, som er det vi ofte tenker på når vi snakker om

reklame og cookies. Disse er fra andre domener, som kan plante cookiene sine på andre nettsider, ved at sistnevnte brukes ressursene deres, slik som bilder, scripts, etc. Det er ofte disse som gjør at andre nettsider får nyss om hva du har sett på. Man har mulighet til å skru av third-party cookies i browseren sin.

12. Case-oppgave:

    Mulige scenarier: Brukere havner på en falsk nettside (følger en falsk lenke, Googler bankens navn istedenfor å huske adressen el.). Bruker må selv vite forskjell på www.dnb.no, www.d-nb.com, d-nb.org, osv. TLS-basert autentisering er syntaktisk, og gir ikke brukeren bevis for at en nettside er ekte. Bruker benytter et åpent trådløst nett: DNS-forfalskning i et kompromittert eller falskt aksesspunkt kan også sende brukeren til en falsk nettside.

13. Case-oppgave:

    Nei. Kanksje brukeren har forlatt maskinen sin for å få en kaffe eller gå på toalettet? Om maksinen da ikke er låst kan en annen person bruke denne, utgi seg for å være brukeren og sende data til tjeneren. En annen mulighet er at brukerens datamaskin er infisert med en trojaner som genererer og sender data til serveren uten at brukeren vet om det (til tross for at brukeren fysisk sitter foran datamaskinen og aktivt utfører transaksjoner, f.eks. til en nettbank).

    Hvis sesjonen mellom klient og server ikke er beskyttet med TLS (Transport Layer Security) eller f.eks. VPN (Virtual Private Network), kan sesjonen også være et offer for et Man-in-themiddel-angrep. I et Man-in-the-middle-angrep bryter uvedkommende inn i kommunikasjonen og kan endre eller slette data utvekslet mellom klienten (brukerens datamaskin) og tjener

2 Praktiske oppgaver for å bli kjent med nyttige nettverksverktøy

Praktiske oppgaver uten løsningsforslag.