ITS – Eksamen 2022

A.

1.

Princippet går ud på at brugeren ikke skal blive overrasket, når de bruger systemet. Det betyder man skal prioritere funktionalitet og brugen af systemet.

2.

STRIDE er et acronym, som bruges til at huske følgende:
Spoofing – at prøve at udgive sig, for at noget andet fx webside eller bruger

Tampering – uatoriseret ændring af code, filer eller pakker over netværk

Repudiation – nægte sig skyldig i ens handlinger

Information disclosure – udgive data, som er hemmeligt

Denial of service – Bruger mange resourcer på et netværk eller på en server, så brugere ikke kan få adgang, eller har meget langsom adgang

Escalation of privilege – Bruge fejl i programmer til at få adgang til mere data eller få rettigheder til at gøre flere ting i programmet

De fleste trusler falder ind under disse kategorier, og kan derfor bruges, når man prøver at finder trusler mod ens system.

3.

Multi-factor authentication er, når man bruger flere metoder, til at verificere brugeren. Disse metoder skal alle verificere brugeren, før de kan få adgang. Det giver bedre beskyttelse mod angreb.

4.

ISPs bruger fx ingress filtering, som kun lader pakker fra IP adresser, som ligger inden for en forventet range, eller adresser, som de ved er legitime.

5.

True, since anomaly-based IDS can also find people who have stolen credentials.

6.

En af kravene for en hash funktion er, at to forskellige beskeder ikke kan lave den samme hash kode. I dette tilfælde, vil det ikke være muligt, at finde en fil med samme hashkode, og attackeren har derfor kun finde den ene fil de allerede har adgang til.

7.

Det giver mere sikkerhed.

8.

Det ideelle ville være at bruge begge dele, men da salt primært hindre brugen af dictionary attacks,ville jeg mene det bedste er at bruge iterated hashing, da denne er mere generel, og nemt kan opscaleres, når compute power øges med tiden.

9.

En god måde at beskytte sig mod replay-attacks er ved at bruge one time password generators. Det fungere ved, at der bliver genereret en TVP, som sendes med, og som også lægges som med det der skal sendes, når det bliver hashet, så hashen bliver anderledes.

10.

Hvis attackeren har fået adgang til en brugers browser, kan der fx køres javaScript kode i browseren, dog skal attackeren nok have administrator eller root user adgang, for at kunne lave nogle af de mere farlige ting på computeren.

11.

Da et XSS angreb fx kan gemme og ændre i HTML koden, vil jeg mene serveren er vulnerable mod attacks, da integriteten af siden ikke længere holder. Både data og functionalitet af siden er ikke sikker.

12.

Det gøres, da det bliver sværere at reverse engineer og lukke botnets, da DNS kan resolve URL'en til forskellige IP adresser.

B.

1.

Man bruger multi-faktor authentication, da man brugere flere forskellige metoder, til at sørge for man vågner.

Man kunne også sige man bruger princippet om Defense-In-Depth, hvilket vil sige man har flere lag af sikkerhed, som backer hinanden op, og der skal derfor brydes flere lag

2.

Man bryder Access Control, da alle kan få adgang til bilen og ikke kun ens ven.

3.

Audit and Accountability da man kan se, hvem der kommer ind, og kan holde en log over, hvad de har gjort, da de har fået en token.

4.

Man bryder least-privilege.

5.

Man følger small-trusted base, da der er færre steder, der kan være fejl i koden, og da det er nemmere at lave sikkerheds analyser på.

C.

1.

Clienten starter med at sende et hello som indeholder følgende i plaintext:

Protocol versions

algorithms-list

client-nonce

client-key-share + PSK-label

Så svare serveren med et hello og sender følgende i plaintext:

server-nonce

server-key-share + PSK-label

og følgende krypteret:

server selected connection option

server certificate and signature

server finshed MAC

Så svarer clienten med følgende data krypteret:

client certificate and signature

client finished MAC

Nu kan dataen blive sendt mellem dem

Når de er færdige med at sende hinanden data, sender de en close-notify besked og lukker forbindelsen.

2.

1.

3.

5.

4.

1., 2.

5.

Nej, hvis en attacker allerede har fået certificaterne, er det ligemeget om det bliver sværrere for eavesdropper at lytte med.

6.

Gatewayen validere certificatet ved at:

Checke at den nuværende dato er inden for rangen

At det ikke er blevet revoked

At det verificeres

Checker om domaine navnet matcher det URL domaine som browseren gerne vil hen til

Det er så her netværket kan følge med i, hvor brugeren gerne vil hen på nettet

7.

Fordi der skal sættes en forbindelse op mellem client og gateway, hvor clienten kan se, at de sender deres CA publickey til gatewayen, som så også bekræfter, at de godt må sende data videre. Clienten bliver nødt til at have en korrespondance med gatewayen, for at gatewayen kan bekræfte, at clienten er legitim.

D.

1.

I et stateless packet-filter bliver være pakke processeret uafhængigt af andre pakker, mens i et stateful packet-filter bliver der holdt øje med bestemte detaljer, når pakker bliver processeret, så de kan bliver brugt, når den kommer flere pakker.

2.

Jeg går ud fra en attacker har bedst chancer, hvis de bruger mulighed 2, da pakker der kommer fra en igangværende forbindelse, vil blive behandlet anderledes, da der er større tillid til denne kilde. Dette vil gøre sig gælende, hvis den infectede computer sætter forbindelsen til Command and Control serveren.

3.

I DMZ’en, da der sidder firewalls på begge sider af denne, og der så ikke kommer data direkte ind på det internal network.

4.

Et network kunne tjekke hvilken port der bliver forbundet igennem, og smide al data væk, som kommer fra port 445 eller som skal sendes til port 445.

5.

Da de fleste regler for packet-filter firewalls er baseret på TCP header fieldet, er det ikke et problem, da hver pakke har samme source og destination fields. Dog, hvis der er en intelligent packet filtering, som kigger på payloadet af dataen, kan det godt være et problem, hvis dataen er splittet op. Så skal der i hvert fald være et stateful packet filter, som kan samle hele payloadet, og undersøge dette, under dets kriterier.

E.

1.

Bob skal bruge deres nøgle k, for at kunne decryptere beskeden, og kan derfor ikke have m, uden at bruge k. Jeg går ud fra det var meningen der skulle stå, at Bob bruger k og t, til at bevise, at alice har sendt beskeden, da det kun vil være muligt for Bob og Alice at kryptere og dekryptere med en kode, som kun de har.

2.

Meningen med en initialization vector, at ændre på nøglen gennem kryptering af dataen, så det ikke er den samme key, der bliver brugt for al dataen i en payload.

3.

Da c_i bliver beregnet af det forrige c_i – 1, vil det være muligt at dekryptere dataen, op til der hvor IV'en er blevet ændre. Hvis altså c_j er ændret, vil det være muligt at dekryptere alle c_i hvor i < j, mens de andre dele ikke kan dekrypteres.

4.

Authenticated Encryption (AE) er kombinationen mellem kryptering og authentication af dem, som sender dataen. Dette kan opnås ved brug af et block cipher til kryptering og en MAC algorithm til

authentication. Der findes dog også specielle algoritmer, som kan gøre begge dele, hvilket gør det muligt at bruge en enkelt symmetrisk nøgle til begge dele. Dette er normalt ikke så smart, men disse algoritmer er designet til det.

F.

1.

Den sammenligner username sat til ingenting, som er false, så længe, der ikke er en bruger, hvor deres brugernavn er ingenting, med 1 = 1, som er sandt, og returnere derfor alle records. Da if statementet så skal evalueres, tjekker den, om der er flere en 0 rækker i resultatet, hvilket der er, og vi får et succesfult login.

2.

En måde at beskytte sig mod SQL-injektions er ved at lave input sanitazation. Der er flere ting man kan tjekke for, når man lave et bruger input:

Ikke tillade escape charaters i inputtet

Lave en blacklist med input og keywords, som man ikke vil have i sit input

Lave en whitelist med input, og afvise alle andre input

Den sidste er den fortrukkende version, da man for det meste kan finde andre escape charaters eller sekvenser her af, som igen bryder koden, og at en blacklist aldrig bliver helt færdiglavet.

Derudover kan man også bruge prepared statements. Prepared statements ændre hvornår koden bliver compilet, så den bliver compilet, før der overhovedet er kommet et input. Inputtet kan derved ikke ændre på koden.

3.

Man kunne starte med at retunere alle records igen, derefter lave nogle if statements, hvor man sammenligne tegnene i passwordsne med tegn, og derefter returnere en sleep værdi, hvis man har det rigtige bogstav. Til sidst kan man så udkommentere resten af koden, så man er sikker på, hvornår man er færdig.

4.

Det samme som i 3. Der burde stadig være et delay i svaret fra serveren, siden vi bruger sleep funktionen, som pause execution af programmet for nogen tid. Det kan dog godt være vi skal have en længe sleep timer, for at være sikker på andre processer i programmet ikke kommer til at ændre på vores resultat.