Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 11: Perimetersikkerhet i Nettverk

Spørsmål 1: TLS/SSL-Inspeksjon

a. Hvordan kan en brannmur dekryptere og lese TLS-trafikk, og hva kalles denne metoden?
b. Hvordan kan en bruker vite om TLS-trafikk blir dekryptert?

Spørsmål 2: CAA og CT kombinert med TLS/SSL Inspeksjon

Se forelesningen om nøkkelhåntering og PKI for å friske opp kunnskapen DNS CAA (Certificate Authority Authorization) og CT (Certificate Transparency).

a. Er CAA kompatibel med TLS-Inspeksjon? Forklar hvorfor eller hvorfor ikke.
b. Er CT kompatibel med TLS-Inspeksjon? Forklar hvorfor eller hvorfor ikke.
c. Er «Certificate Pinning» kompatibel med TLS-Inspeksjon? Forklar hvorfor/hvorfor ikke. Certificate Pinning er ikke forklart i forelesningene, men du kan lese om det f.eks. på: https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

Spørsmål 3: Windows Defender Brannmur

Windows Defender Brannmur er integrert med Windows 10. Hvis du har Windows 10 sjekk reglene for inkommende og utgående trafikk. Finn regler for innkommende trafikk for tredjeparts-programmer du har installert, det vil si regler som ikke er generiske for Windows 10 eller for datamaskinen. Hva ville skje hvis du fjernet en regel for et tredjepartsprogram?

Spørsmål 4: Grunnratefeilslutning i inntrengingsdeteksjon

Den såkalte grunnratefeilslutning er en type feilresonnering som kan føre til falske alarmer i et inntrengningsdeteksjonssystem (IDS).

a. Hva menes med grunnratefeilslutning?
b. Grunnratefeilslutning er en typisk i medisinsk diagnostikk, og i juridisk resonnering (hvor det kalles aktoratfeilslutning). Gi eksempler på grunnratefeilslutning i hver disiplin.
c. Hva kan gjøres for å unngå grunratefeilslutning?
d. Anta at A betyr «Angrep», og at D betyr «Deteksjon» av en angrepssignatur. Betydningen av den betinget sannsynlighet p(D|A) er sannsynligheten for et faktisk angrep gitt at angrepssignatur er detektert. Hvordan kan en betinget sannsynlighet inverteres, dvs. hvordan kam man konvertere p(D|A) til p(A|D), og hvilken grunnrateratesannsynligheten er nødvendig for å gjøre det?

Spørsmål 5: WLAN-Sikkerhet

a. Hva betyr forkortelsene STA, AP,AS, BSS, ESS og DS i sammenheng med IEEE 802.11 WLAN? Gi en kort forklaring av hvert begrep og hvordan de er relatert.
b. Sett opp en liste, og gi en kort forklaring av de 5 driftsfasene IEEE 802.11i.