Oblig 4 IN2120 2026:

Obligen skal besvares i devilry som én pdf-fil (det inkluderer skissen dere skal levere i oppgave fire). Alle oppgavene gir maks ti poeng, med unntak av oppgave fire – som gir maks 20. Obligen kan følgelig gi 120 poeng (De ekstra poengene er lagt til for å hjelpe dere med å få nok poeng til å bestå).

Oppgave 1: Du har en klient A (IP-adresse: 192.168.20.24), som må kunne kommunisere med en FTP-server B (IP-adresse: 192.168.56.23).

Begge sider må kunne initiere kommunikasjonen. Det står en brannmur mellom disse på IP-adresse 192.168.1.23 - lag IP-tableregler som støtter dette.

Oppgave 2: Filen pakkedump.pcap inneholder ett passord, hvilket?

NB: Pcapen skal bare brukes i denne oppgaven, og har ingen sammenheng med øvrige oppgaver i obligen (eksempelvis IP-adresser).

Oppgave 3: Forklar (på maks fem linjer) hvorfor Diffie-Hellman gir fremoverhemmelighold, og hvorfor offentlig/private nøkler ikke gjør det (m.a.o. hvordan DH gjør det).

Oppgave 4: Du har et nettverk bestående av 20 klienter, tre printere, tre domenekontrollere (hvorav en er virtuell), to epostservere, en webserver, to filservere og to databaseservere. Epost og webserverne må kunne nås fra Internett.

Lag, og legg med en nettverksskisse, og gi en kort begrunnelse for hvor du ønsker å sette opp brannmurer, IDSer og hvordan du ønsker å dele opp nettverket ditt.

Oppgave 5: Lag snort-regler som genererer alarm for innkommende RDP-sesjoner mot domenekontrolleren på 10.0.23.23.

Oppgave 6: Forklar kort med egne ord hva som menes med anomalibasert IDS.

Oppgave 7: Sikkerhetssjefen din ber deg sette opp en honeypot i nettverket ditt - hva er det, og hvorfor (maks fem linjer)?

Oppgave 8: Forklar kort (maks fem linjer) fordeler og ulemper med å plassere en IDS henholdsvis på rett på innsiden og rett på utsiden av den ytre brannmuren.

Oppgave 9: Virksomheten din har reservert enkelte IP-adresser mot noensinne å skulle bli brukt. Dette kalles mørke IP-adresser, forklar kort hvorfor dette gjøres for å øke sikkerheten.

Oppgave 10: Mange virksomheter konfigurerer alle sine klienter til å automatisk logge seg inn på en VPN inn mot virksomhetens nettverk, når de ansatte er utenfor kontoret.

Forklar kort hvorfor de ønsker dette.

Oppgave 11: Forklar rollen til en gateway-node i sammenhengen av en TLS-inspeksjon. Hva gjør at den kan få tilgang til HTTPS-trafikken i klartekst?