

IDS/IPS bringes oftere og oftere i anvendelse for hhv. at detektere og forhindre angreb. Alligevel er disse systemer ofte sårbare. Manglende eller forkerte konfigurationer resulterer således i at systemet er relativt ineffektivitet i dens detektion af selv basale angreb. Og i værste fald kan implementeringen af IDS/IPS føre til krænkelse af fortrolighed, integritet og tilgængelighed af hele organisationens netværk.

IPS forsøger at forhindre angreb. Dvs. der reageres på en bestemt signatur, eller usædvanlige handlinger – og derefter blacklistes den IP-adresse hvorfra disse handlinger stammer. Mens denne funktionalitet giver fordele mht. at forhindre en række angreb, der krænker integritet og fortrolighed, øger den dog åbenlyst risikoen for DoS-angreb. En angriber kan således forfalske en afsenderadresse, som han ønsker spærret, og sende en række ikke-tilladte pakker mod det netværk hvorpå IPS er implementeret. IPS vil her efter spærre adgangen fra den forfalskede afsenderadresse (ofret).

Helt galt går det hvis angriberen er i stand til at blacklist root DNS-servere. Resultatet vil være at trafik fra disse ikke bliver modtaget. Resultatet kan være at hele organisationens netværk bliver gjort utilgængeligt. Alternativt kan angriberen være i stand til at svare i stedet for root DNS-serverne, og dermed forgifte organisationens navn til IP-konverteringer. Her vil angriberen f.eks. kunne få et givent DNS-navn til at pege på et system, han har kontrol over i stedet. Herefter vil organisationens trafik kunne køres gennem angriberens computer, og angriberen er i en optimal position til at krænke de transmitterede datas integritet, fortrolighed, og tilgængelighed.

Derudover er den tid hvori IDS/IPS beholder IP-fragmenter, ofte sat enten højere eller lavere end på de systemer som IDS/IPS beskytter. Beholder IDS/IPS IP-fragmenterne kortere tid end de beskyttede systemer, da vil angriberen kunne sende forsinkede IP-fragmenter. Således vil den sam-

lede pakke blive samlet af de beskyttede systemer, men ikke af IDS/IPS. Derfor reagerer IDS/IPS ikke på denne trafik, selvom den måtte være ondsindet. Omvendt, beholder IDS/IPS IP-fragmenterne længere end det beskyttede system, da kan IDS/IPS bl.a. blive tvunget til at samle pakkerne for tidligt. Alt imens det beskyttede system får en helt anden (og potentiel ondsindet) pakke. Omgåelse af detektion fra IDS/IPS er således ofte muligt.

Nøje risikovurdering og sårbarhedsanalyse bør således foretages ifm. den eventuelle implementering af IDS/IPS.

Når Ezenta foretager en sikkerhedstest af IDS/IPS, tjekkes om systemet er i stand til at detektere et givent angreb, samt om IDS/IPS selv er sårbar over for disse angreb.

Angrebne består af variationer af følgende:

- Buffer overflows
- Integer overflows
- Heap overflows
- Format string-angreb
- Cross Site Scripting
- SQL injection
- Forceful browsing
- Brute forcing
- Packet Spoofing
- Flood Attacks
- Obfuscation
- Session splicing
- Fragmenteret angreb