17 Oktober 2015 - Blog Post #502

IDS koncept

Brug IDS systemet til lidt at kigge efter det ukendte

Når man snakker IDS systemer som eks SNORT så bygger disse typisk på at man kender noget "ondsindet" eller noget man ikke ønsker, og ud fra det bygges der en IDS rule.
Det kunne eks være at man gerne vil have en alert når der hentes en EXE fil fra en given URL i en bestemt størrelse med et bestemt navn. Dette er den typisk tankegang man benytter. Med denne tankegang kan det godt være svært at fange andet ondsindet, så som en server der er blevet komprimiteret og pludselig begynder at snakke på andre porte end det der var hensigten.

Koncept og ide

Jeg har igennem et stykke tid fået testet mit eget koncept, ved at bygge IDS rules ud fra det jeg kender, altså en lidt omvendt tankegang med IDS Rules end den mere tiltænkte tangegang og metodik. Meningen er at hvis jeg ved hvordan en given server eller switch skal "snakke" på tråden og hvem den må det med, så skaber det et fint overblik hvis noget af mit udstyr begynder at snakke uventet. Det det giver mig en fin mulighed for at finde det uventet meget præcist hver gang.

Ideen til dette koncept fik jeg da jeg laver mange IDS rules dagligt i forbindelse med analyser af malware. Dette var en nem måde for mig at finde hver gang et stykke malware lagde en bagdør ind i systemerne og benyttede disse bagdøre ud imod Internettet, så sprang de direkte ind i mine IDS alerts med det samme. Firewall syntes jeg ofte er for spartane i deres natur og de giver mig ikke mulighed for at se hvad der egentelig skete og her hjælper fuld PCAP med rigtig meget som firewall logs bare ikke kan. Derfor er fuld PCAP af al ens traik bare et "must have"

Eksempel på en mail server

Typisk har vi med systemer at gøre, vi godt ved hvordan snakker. Et tænkt eksempel her.
En mail-server køre på IP 192.168.1.1 denne må snakke på TCP PORT 25 med ANY. Derudover må den hente NTP på UDP PORT 123 fra ntp1.tele.dk. Jeg forventer ikke at se nogen anden form for trafik. Lad os antage at serveren blev komprimiteret via en exploit på netop port TCP port 25 som er den eneste der er åben, så ville serveren ofte begyndet at snakke på andre porte til C&C serveren (hackeren). Typisk føler en hacker han er er smart og vil snakke på via en ICMP eller måske en DNS tunnel igennem systemet. Fordi der er en regeler der kigger på både UDP og ICMP, så vil denne begynde at sende bunkevis af Alerts til IDS Systemet. Det kunne være mange andre typer trafik der blev benytte til C&C trafik. Men så snart det falder uden for mine opsatte regler har vi en alert.

Netop ved at kigge efter når noget snakker som det ikke skal, så kan der være mange fordele i det.
Vi lærer rent faktisk at kende vores systemer på et andet grundlang end tidligere, hvor vi kun styrede trafikken i firewalls ved at lukke porte op eller i, og hvem behandler lige de 10 pakker der kom og blev droppet i en firewall, typisk ingen ! og hvad indelholdet de 10 pakker af data og hvortil ville nogen forsøge at sende det. Men reagerer vi på de 10 pakker, så kan vi stoppe/spotte et angreb langt tidligere. Da vi med IDS får lige præsic de pakker der blev forsøgt med via alert loggen, der så også fortæller hvor i mine pcap filer jeg skal begynde at lede og undersøge data. Man kan hele tinden vende tilbage til den enhed der forsøgte at sende de 10 pakker og undersøge denne.

Eksempler på rules

alert icmp 192.168.1.1 any -> $EXTERNAL_NET any (msg:"NF - ICMP Mail Server Out - Not allowed"; priority:1; sid:7000001; rev:1;)
alert udp 192.168.1.1 any -> !193.162.159.194 any (msg:"NF - Mail Server using UDP - Not allowed"; priority:1; sid:7000002; rev:1;)
alert tcp 192.168.1.1 !25 -> $EXTERNAL_NET !25 (msg:"NF - Mail server TCP - Not allowed"; priority:1; sid:7000003; rev:1;)

3 Rules pr. host

Der skal benyttes min.3 rules pr host på TCP, UDP og ICMP.
Det er vigtigt at man beskriver i sine IDS Rules hvad der ikke skal alertes på og vær ikke for rundt håndet med at åbne porte som eks en ![80,443] - Den er "farlig"

Tests

Jeg har testet dette koncept på følgende typer af enheder, Wireless Routers, Firewalls, Klienter, Proxy Gateways, Mail-servers, Switches, File Servers, Print servers, DNS Servers, Samsung TVs, Playstations, NAS servers, Xbox, Iphones, ipads, Sonos, Linux, Windows i forskellige versioner samt i et AD miljø. Alle enheder har nogle helt bestemte metoder de snakker på, det er også det man kan kalde for et fingerprint, og jeg forventer aldrig at se de begynder at snakke anderledes end det jeg har opsat disse til at måtte kunne. Jeg har på dette grundlag fået mange oplevelser når en iphone eksempelvis begynder at snakke med "noget" bare 1 gang om ugen med få pakker. Eller en Firewall der står og kalder hjem til producenten helt uventet, som jeg bestemt ikke mener firewalls skal, dette resulterede også i en udskiftning en enheden, da det ikke var muligt at slå fra. Jeg har sågår fundet ganske almindeligt software, hvor dette sort set viker som malware og hvor producenten lige pludselig sender uventet commands til dette og opretter forbindelse til softwaren udefra der i virkeligheden giver fuld adgang til hele systemet, Det virker i bedste RAT stil, denne type software får man hurtigt luset ud i. Vær desuden opmærksom på at i disse tests var IDS'en placeret på indersiden af primeter firewallen, således at det er muligt at se alle de interne ip adresser.

Hold stadig øje med det uventet

Det er vigtigt at man ikke slår alle andre rules fra i sin IDS, da uønsket ting jo stadig godt kan ske på grupper på tilladte porte og fra systemer der er overvåget på denne måde.
Så pointen er at man får det snævret extremt meget ned til de tilladte ting og det uventet og ikke tilladte bliver mere synligt meget meget hurtigt.

Implementering

Opret en local.Rules file for dit eget miljø, for hver enhed kræver det 3 Rules. Såfremt du har mange af en type enhed der alle snakker på samme måde, kan der nemt oprettes variabler som eks $SMTP_SERVERS. Disse tilføjes i snort.conf. For det ikke skal blive for uoverskueligt så lav en gruppe af gangen og undersøg hver gang du ser at en rule sender alerts, for om det er tilladt trafik eller ej. Dette kan typisk være den tunge del under oprettelsen, Men når man først er kommet igang får man hurtigt oprette fingerprint på de efterfølgende. Men det er det hele værd når det først er opsat så efterlader en meget lille spillerum til en hacker eller malware. Derudover vil man opdage mange fejl konfigurationer som er efterladt af admins som der samtidigt kan ryddes op i.

Udfordringen og det man ikke opdager

Bruger noget malware eller en hacker noget som ligger inde for de tilladte porte eller destinationer, så vil disse alerts ikke sige noget og her er det andre IDS rules skal tigger eller andre sikkerheds systemer. Men det er helt klart at alt i dit net skal opføre sig meget "korrekt". Så der er desuden vigtigt at man efterfølgende har muligheden for at "spole tiden tilbage via sine pcap files" for at undersøge hvad der skete. Defor er det vigtigt at man altid har pcap files liggende. Jeg vil altid anbefale at der ligger min 90 dages pcap trafik. (Dette kan for mange være den dyre del) Det behøver heller ikke at være IDS systemet der også skal opsamle trafikken, det kan andre enheder fint gøre og opsættet behøver ikke at koste det vilde. Det er alligevel det færreste der har internet forbindelser der ligger over 1 Gbit, men kommer man over dette, skal man forvente at det begynder at koste dyrt i opsamlingen af trafikken. Mange gør den fejl at de vil have fuld PCAP og IDS systemer på samme enhed, men det er altså ikke nødvendigt, og det kan give god mening at skille disse to ting ad, for fuld PCAP bliver for det meste kun brugt til efterfølgende analyser. Ved store belastninger kan jeg anbefale at der min benyttes SNORT v3 da denne er multi threaded.

Fald grupper

Ved brugen af gateway proxyes til HTTP trafik der eks benyttes i forbindelse med AV scanning osv så kan jeg ikke anbefale at ens servers benytter disse, da disse hurtigt fjerner "fælden med IDS"

Brug derfor disse udelukkende til klienter.

Benytter man Windows så vil disse gerne hente opdateringer, Til dette bør der benyttes en indtern WSUS ellers prikkes der for mange huller i ens IDS Rules, da man vil opdage at windows update benytter nye IP'er hver gang de henter updates. Det er heller ikke tilsigtet at man exkluder port 80,443 for så er man tilbage til de kendet kæmpehuller der netop er port 80 og 443. Her vil man opleve at man simpelt hen er nød til at tilføje disse porte, men det er heldigvis på meget begrænste antal enheder, men her kan man faktisk tilføje yderligere IDS rules der alerter når noget ikke er som det bør være. Men man vil være tvunget til at forholde sig til alt det der default vil snakke i en Windows "dåse" og hvordan man får dem til at være yderst stille under en boot sekvens. Men der skal faktisk ikke meget til i virkeligheden.

Min oplevelese er at det er svært en benytte i et klient miljø, med mindre man 100% kan kontroller alle sider af dette. Har brugerne admin rettigheder så glem det.
Derfor anbefaler jeg også at det er servers siden man kigger på med mindre det er som i mit tilfælde hvor det er forbundet med malware analyse og fingerprint af trafikken fra enkelte hosts.

Mange net er blevet så store i dag, at mange ikke kender deres eget net og hvad der køre på det, derfor kan det være svært for mange at komme igang med dette koncept, Men er det tilfældet at det er blevet så stort så man ikke mere kender sine egne enheder, så er det nok mere end på tide man kommer igang med dette. For kender man ikke sine enheder så ved man heller ikke hvad man skal beskytte. Men når først man får fuld PCAP så finder man hurtigt alle IP adresser der snakker ud og glemt udstyr bliver hurtigt fundet.

APT

Enheder der eksempelvis er ramt af malware som kun åbner forbindelser efter portknocking og magic packets som vi kender det for APT-Regin kan desuden blive fanget på denne måde, såfremt man placerer en IDS Sensor foran ens primeter udstyr. Her behøver man ikke kende Magic Packet eller sekvensen, det faktum alene at en forbindelse blev oprettet til noget den ikke burde er nok til en IDS Alert.

PCAP
or it didn't happen