Utredning av IDPS system som används för att förbättra nätverkssäkerheten

Sebastian Sergelius

Sebastian Sergelius

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informationsteknik
Identifikationsnummer:	**5684**
Författare:	Sebastian Sergelius
Arbetets namn:	Utredning av IDPS system som används för att förbättra nätverkssäkerheten
Handledare (Arcada):	Jonny Karlsson
Uppdragsgivare:	Magnus Westerlund

Sammandrag:

IDS, *Intrusion Detection System* (Intrångdetekteringssystem) uppgift är att upptäcka intrång i ett datasystem och registrera när intrången påbörjades, som sedan rapporteras till Administratorn eller säkerhetspersonalen. IDS upptäcker attackerna med hjälp av sensorer uppkopplade till monitorer.

IPS, *Intrusion Prevention System* (Intrångsskyddsystem) specialiserar sig på att förhindra intrång och andra sabotageprogram från att nå data i ett nätverk. IPS observerar trafiken som kommer in till nätverket och kontrollerar trafiken till en flagglista. En flagglista är en lista på kända intrångsattacker.

IDPS, *Intrusion Detection Prevention System* (Intrångdetektering och Intrångsskyddssystem) är den nyaste säkerhetsstandarden för aktiva nätverkssäkerheten. IDPS är en kombination av sina företrädare; IDS och ISP.

I det här arbetet har jag jämfört mellan två IDPS program med öppen källkod dvs. Snort och Suricata. I jämförelsen ingår båda IDPS precision när det gäller identifiering av intrång, falsklarm och kapaciteten. En begränsad kapacitet innebär flera falsk negativ, eftersom om paket hastigheten överstiger IDPS granskningskapacitet, kommer vissa virus inte att bli upptäckta.

Nyckelord:	Aktiv nätverkssäkerhet, kryptografi, intrångsdetekteringssystem, Intrångsskyddsystem, brandvägg, Snort, Suricata, McAfee, F-Secure
Sidantal:	48
Språk:	Svenska
Datum för godkännande:	11.12.2016

DEGREE THESIS	
Arcada	
Degree Programme:	Informationsteknik
Identification number:	**5684**
Author:	Sebastian Sergelius
Title:	An investigation of IDPS systems being used for improving network security
Supervisor (Arcada):	Jonny Karlsson
Commissioned by:	Magnus Westerlund

Abstract:

IDS, *Intrusion Detection Systems* detect intrusions in the network and report them to the administrator or to the Anti-virus. IDS is able to detect the intrusions with sensors that are connected to a monitor.

IPS, *Intrusion Prevention Systems* prevent the intrusions and other viruses from reaching the network. IPS observes the traffic inside a network and compares it to a list of known intrusions.

IDPS, *Intrusion Detection Prevention System* is the most modern form of active network security. IDPS is a combination of its representatives; IDS and IPS.

In this thesis a comparison of two IDPS program that are open source. The name of the IDPS are Snort and Suricata. The study will compare both IDPS for the attack detection rate, false positive and capacity. A limitation to the capacity will increase the rate of false negative. If packet rate is greater than the IDPS capacity, then some intrusions will pass throw without detection.

Keywords:	Aktiv nätverkssäkerhet, kryptografi, intrångsdetekteringssystem, Intrångsskyddsystem, brandvägg, Snort, Suricata, McAfee, F-Secure
Number of pages:	48
Language:	Swedish
Date of acceptance:	11.12.2016

INNEHÅLL

Figurer

Tabeller

Terminologi och förkortningar

IDS = Intrångdetekteringssystem

IDPS = Intrångdetektering och Intrångsskyddssystem

IPS = Intrångsskydd

DDos = Distribuerad överbelastningsattack

Bot = Robot

PKI = Publika Nyckel Struktur

AES = Advanced Encryption Standard

TCP = Transmission Control Protocol

UDP = User datagram protocol

IP = Internet Protocol

RTS = request to send

NIDPS = Nätverks IDPS

HIDPS = Värd IDPS

CIDPS = Trådlös IDPS

1 INLEDNING

1.1 Bakgrund

För att ett multinationellt företag skall lätt kunna kommunicera med arbetstagaren, konsulter, leverantörer och kunder så behöver företaget skapa ett stort internt nätverk. När man skapar ett nätverk, är det viktigt att man ordentligt skyddar nätverket så bra som möjligt, så att inga intrångattacker kan komma åt informationen i nätverket. Det räcker inte mera med att bara ha en statisk brandvägg för att skydda ett stort nätverk, utan det gäller att installera ett aktivt nätverks säkerhet som kan övervaka all trafik som går igenom nätverket samt trafiken mellan servrarna inne i nätverket. Eftersom det finns massor med olika sätt man kan konfigurera sitt nätverk på är det viktigt att man veta vilka funktioner man vill ha i det aktiva nätverket.

Målet i ett aktivt nätverk är att skapa ett kommunikationsnätverk som överförs från statisk låg nivås nätdrift till ett dynamisk och anpassningsbart beteende. Det här görs för att kunna öka på kommunikationshårdvarans prestation genom att anpassa hårdvaran till specifika applikationskrav. Det här möjliggör också ett mera flexibelt kommunikationsnätverk.

IDPS, *Intrusion Detectin Prevention System* (Intrångdetektering och Intrångsskyddssystem) är det modernaste och effektivaste nätverksskydd för företag eller organisationer. Ett ordentligt IDPS är planerat specifikt för det nätverk det skall skydda, dvs. Vad för struktur IDPS skall ha, hur många sensorer man skall ha och vart man placerar dem i nätverket osv. Det här är orsaken till varför en installation av IDPS till ett företag kan kosta över 100.000€.

1.2 Målsättning och Syfte

Målet med detta arbete är att undersöka och jämföra styrkorna och svagheterna i olika aktiva nätverk samt kort förklara vad ett aktivt nätverk är uppbyggt av.
Jag kommer att kort beskriva om fyra olika IDPS; Snort, Suricata, McAfee och F-Secure styrkor och svagheter. Jag har valt att undersöka Snort och Suricata

eftersom de är baserade på öppen källkod medan McAfee Endpoint Security och F-secure Business Suite är IDPS designade för stora och små företag.

1.3 Metoder, avgränsningar och struktur

Arbetet består av att samla ihop från olika artiklar, studier och experiment och formulerar kort vad det innebär i att ha ett IDPS (Intrångdetektering och Intrångsskyddssystem).

Undersökningen kommer också bara att gå igenom nätverks baserade IDPS. Jag kommer alltså att exkludera värd baserade och trådlös baserade IDPS. Den största delen kommer att handla om skillnaden mellan Snort och Suricata eftersom båda IDPS-systemen är öppen källkod och är relativt lätta att hantera.

I kapitel 2 ges en översikt på kända nätverksattackerna, vad olika attacktyper gör, vad för motiv det finns för att göra en intrångsattack och hur man skyddar sig mot intrångsattacker.

Kapitel 3 beskriver om intrångdetekteringssystem och intrångsskydd (IDPS). Först förklaras vad Intrångsdetekteringssystemets (IDS) uppgift är, hur IDS är uppbyggd och vad har den för styrkor och svagheter. Efter det förklaras vad intrångsskydd (IPS) har för uppgifter, hur IPS är uppbyggd och vad IPS har för styrkor och svagheter. Till slut förklaras vad IDPS är och vad för funktioner IDPS har.

Kapitel 4 beskrives vad Snort, Suricata, McAfee och F-Secure har för funktioner. Efter det Jämförs Snort och Suricata prestations förmågor i en sluten kontrollerad miljö.

Kapitel 5 är slutsatserna på hela litteraturstudien. En kort beskrivning på jämförelsen om Snort och Suricata och sedan en kort beskrivning på vad för undersökningar man skulle kunna göra i fortsättningen.

2 NÄTVERKSATTACKER

2.1 Attacktyper

2.1.1 Nätverksskanning

Nätverksskanning är det första steget mot en intrångsattack. Syftet i en nätverksskanning är att få fram så mycket information som möjligt om nätverket man vill nå.

Det finns massor med olika sätt att skanna för att få fram vilka portar eller adresser som är öppna och obevakade.

En **Ping-skanning** är den simplaste formen av skanning, attackeraren skickar iväg en ICMP ekobegäran för varje maskin i nätverk. Varje adress som svara på pingen är registrerade till att vara aktiva.

En **TCP-skanning** är också en simpel variant att skanna igenom alla öppna TCP anslutna portar på offrets sida, alla maskiner som svara på pingen märks som aktiva. Efter det så försöker den skapa en anslutning till nätverket med en av TCP typiska portar (HTTP eller port 80). Det går också att göra en TCP skanning som gör allt samma som vanligt, men den skapar inte en anslutning till nätverks. Det här gör det mycket svårare att upptäcka skanningen, eftersom den inte skapar en log fil på anslutnings begäran.

Stealth FIN, Xmas, ACK och NULL skanning är speciella former av skannings tekniker. Varje skannings teknik sänder ut ett speciellt paket till offrets adress, som bestämmer om porten är öppen eller inte i Real-time Transport Protocol (RTS) format. Om det inte kommer ett svar from RTS så är porten öppen.

FIN skanning är skanning som kan smyga förbi brandväggar och innehåller en FIN flagga i sig, som är ett paket som beskriver att det var den sista biten som sänds. Xmas skanning innehåller en FIN, URG (som är en flagga som beskriver att ärendet är brådskande) och PUSH flagga (som ber att skicka buffert data) i sig, genom att titta på svaret man får från RTS kan man lättare besluta vad för

operativsystem som mottagaren kör. ACK skanning innehåller en ACK (acknowledgment) flagga som är designade att kunna lätt smyga förbi brandväggen, ACK skanning undersöker om porten är filtrerad eller inte filtrerad istället för om porten är öppen eller stängd. En NULL innehåller inga flaggor i sig.

En **UDP skanning** är när man testa vilka UDP portar som är öppna i ett eller flera nätverk. Skanningen fungerar med man skickar ett UDP paket till varje port inom specifika parametrar, och om porter svara ”ICMP port unreachable” så vet man att porten är stängd.

2.1.2 Buffertöverskridning

En buffertöverfyllning händer då när ett program försöker lagra mer data i en buffert än vad det finns plats för. Detta gör så att den informationen efter bufferten blir överskriven, vilket kan leda till störningar, krasch eller säkerhetshål. En buffert är plats vart program tillfälligt lagrar data som används i applikationen. En buffertöverskridning kan skapa med att skicka en speciellt strukturerad värde som en parameter till ett system. Till exempel när man begär en server att byta namn på en katalog till ett ovanligt långt namn, om en katalog kan högst ha ett 128 täcken långt namn och man begär katalogen ha ett 300 täcken långt namn, skriver man in 172 täcken till ett annat ställe i programmet.

2.1.3 Social manipulering

Ett av det äldsta och det effektivaste sättet att tränga sig in till ett nätverk är via social manipulering. Iden bakom socialmanipulering är att man tränger sig in i systemet med hjälp av någon från insidan av nätverket. Ett av de lättaste sätten är att föreställa sig till någon användare av systemet och be om att byta deras lösenord. Det här exemplet fungerar bara om attackeraren har någon användare från systemets bas uppgifter, till exempel användarnamn eller för och efternamn.

2.1.4 Distribuerad överbelastningsattack (DDos)

En överbelastningsattack som strävar efter att förhindra tillgång till nätverks resurser, kan vara mycket skadliga och svåra att skydda sig emot. En typisk överbelastnings attack brukar överbelasta nätverket med trafik som blockerar all trafik och hindrar berättiga användare från att nå servisen på nätverket. En överbelastnings attack kan riktas mot flera olika nivåer på nätverksstacken.

I **applikations** lager överbelastningsattack tar och överanstränger applikationens funktioner eller tjänster. Det här gör så att andra användare inte kan nå servern för att servern är överbelastad med andra uppgifter. Nätverket kan fungera bra men ingen kan kommunicera med servern.

I **nätverks** lager överbelstingsattacken så tar man och skickar över stora mängder med data till nätverket. Den här sortens attack målinriktar sig mest mot nätverks infrastruktur. Den höga trafiken kan också skapa hög belastning på offrets CPU i själva nätverksservern som kan förvärra nätverks problem.

I **data-link** lager överbelastningsattacken kan attackera både nätverket och värden, Data-link överbelstingsattack mål är att bryta kontakten mellan värden och det lokala nätverket med att överbelasta Ethernet nätverk med ogiltiga ramar.

Den största Ddos attacken har haft en trafikhastighet på över 400 gigabits per sekund.

2.2 Motiv för attacker

Det är viktigt att ha en bra uppfattning om vad för motiv en attackerare kan ha. Om man vet motivet bakom en attack, så är det lättare att se vad man skall skydda i sitt system. Tack vare det kan man också förstå vad attackeraren är kapabel att göra.

2.2.1 Informationsstöld

Informationsstöld är den allra vanligaste formen av attack. Med informationsstöld menas att en attackerare lägger beslag på konfidentiell information som gjorts åtkomligt genom nätverksintrång. Kritisk informationen kan vara i form av kund-information, affärskritisk information eller immateriella rättigheter. Ett av det mest kända sättet att bli attackerad är via Adobe Flash spelarens sårbarheter, varefter attackeraren lätt kan samla ihop all information.

2.2.2 Spionage

När målet av en intrångsattack är att övervaka alla aktiviteter i det infekterade nätverket så är attacken en spionageattack. All informationen som attackeraren samlat ihop kan sedan säljas vidare.

2.2.3 Sabotage

När målet av attackeraren är förstörelse, utpressning eller ärekränkning av det infekterade nätverket kallas det för Sabotageattack. Det var det här som hände till Sony för ett par år sedan när alla användarens information blev läckta ut på nätet. Datat som läcktes ut från var personlig data på de anställda, e-post meddelande inom företaget, chefernas löner och outgivna filmer.

2.3 Attackens ursprung

2.3.1 Script kiddies

Script kiddies är ofta människor som inte har en bra kunskap i hur man kan attackera en dator/ nätverk men har redskap som kan göra allvarliga skador. Script kiddies har oftast inte heller så stora motiv bakom varför de attackerar, ibland kan deras enda orsak för att attackera vara för att se om de kunde göra det.

Fast script kiddies kanske inte kunskaper i att attackera är de ändå ett av de största hoten för nätverkssäkerhet eftersom script kiddies ofta har massor med tid och håller sig uppdaterade med alla nyaste säkerhetshål.

2.3.2 Anställd

Anställda för företag kan läcka ut viktig/skadlig information ur företaget avsiktligen eller av misstag. De anställda är ett av det största hotet mot stora företag eftersom det handlar om personer som använder sig av nätverket varje dag och har en bra uppfattning om vad informationen i nätverket är värd.

Misstag förekommer för det mesta av de oerfarna anställda som kan vara lika farliga som en planerad attack.

2.3.3 Bots

Bots förekommer för det mesta i grupper. När man talar om grupper av botar kallas det botnet. Botnet är alltså ett system på flera robotar som arbetar tillsammans för en person som kallas bot herde. Bot herden tar och distribuerar virus/trojaner via nätet till datorer som sedan förvandlar dem till bots. När det har hänt så kan datorn som har blivit smittad göra automatiserade uppgifter över internet utan att ägaren till datorn vet om det. De kriminella bot herden använder sedan botnet till vad de vill använda botnätet till, som kan vara allting från epost spam till Ddos attacker på andra datorer och servrar. (*Essential guide.* 2012)

2.3.4 Hackers

Hackers är människor som är experter på datorer och har ofta massor med redskap till sin användning som de har antingen själv skapat eller har en bra uppfattning till hur intrångsredskapen fungera.

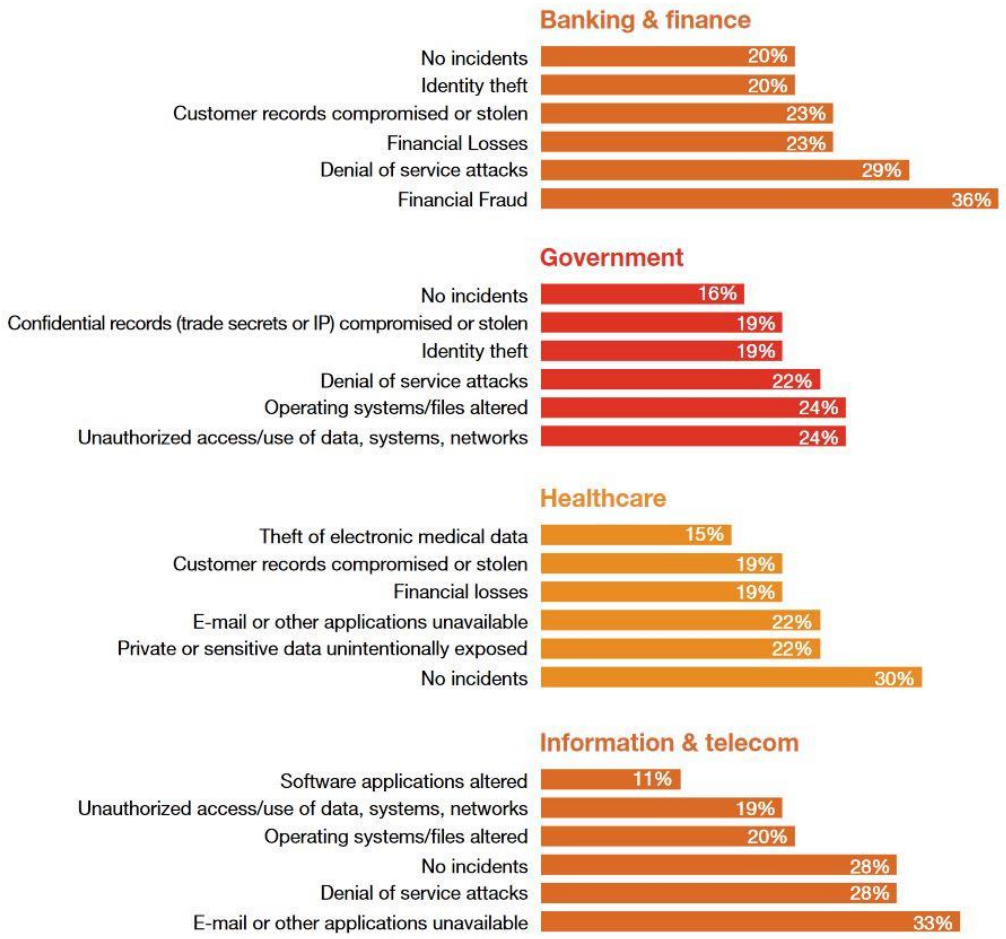
Expert hackers är ofta mycket stolta över sina intrångsattacker och föredrar kvalité över kvantitet. Det betyder att intrångsattacker oftast är unika (zero day attack) och därför har en mycket större chans att inträngа sig utan att bli upptäckta.

2.4 Försvarsmekanismer

IT- baserade attacker har blivit allt vanligare i dagens samhälle, det har också under de senaste åren blivit allt vanligare för vanliga brottslingar och kriminella organisationer att använda sig av illvilliga program och virus för intrång.

För att lättare kunna se hur viktigt det är att ha ett aktivt nätverk, så har ”Computer Crime and Security Survey” undersökningen som är gjord av United States Secret Service (publicerad 2014) samlat ihop från över 3000 företag kronofogden och statliga anstalters svar på hur deras nätverk har klarat sig under de senaste åren. (*US cybercrime*) I den här undersökningen kommer det fram att 7 % av alla organisationerna hade en förlust på över 1$ miljon direkt relaterat till IT-relaterad brottslighet och 19 % hade en förlust som varierade från 50 000$ upp till 1 000 000 $ i skador.

Över tre fjärdedelar (77 %) av alla företag rapporterade att de hade upptäckt en intrångattack inom de 12 senaste månaderna och 34 % av dem nämnde att intrångattackerna hade ökat sedan förra året. I Figur 1 visas vanliga attacker inom olika branscher.



*Figur 1. Upptäckta attacker inom olika brancher. (*US cybercrime: Rising risks, reduced readiness*)*

Enligt undersökningen har man estimerat att intrångs hot bara kommer att öka för varje år så det är viktigt att man har en bra uppfattning om vad man skall gör om man upptäcker ett intrång.

2.4.1 Kryptografi

Kryptografi är en av de vanligaste metoderna för att sätta upp en säker förbindelse mellan två datorer i ett nätverk. Idén är att man skall kunna skicka meddelande mellan datorerna utan att en utomstående skall kunna läsa meddelandet. Kryptering delas oftast till två kategorier, symmetrisk och asymmetrisk kryptering.

Symmetrisk kryptering är när man använder sig av samma krypterings nyckel för att kryptera och dekryptera data, den här nyckeln kallas till en symmetrisk nyckel. Nackdelen men en symmetrisk kryptering är att det är lätt att nyckeln blir upptäckta av en utomstående. Algoritmen man använder sig av är cipher, och när ett meddelande krypteras med cipher, tar man och omformerar den oformaterade texten till en ciphertext.

Asymmetrisk kryptering är när man använder sig av nyckel par, publika nyckel som är tillgänglig alla och privata nyckel som är bara tillgänglig för ägaren. När två användare vill göra asymmetrisk krypterad förbindelse, växlar båda användare sina publika nycklar med varandra. Efter det kan de kryptera meddelande med den publika nyckel de fick från varandra. Det krypterade meddelande kan sedan sickas över till mottagaren som kan dekryptera meddelandet med sin privata nyckel.

Till exempel. Alice och Bob vill skapa en säker förbindelse. Alice skickar sin publika nyckel till Bob, och Bob skickar sin publika nyckel till Alice. Alice kan kryptera ett meddelande med Bobs publika nyckel och skickar det till Bob. Bob kan sedan dekryptera det med sin privata nyckel och läsa texten i oformaterad text.

2.4.2 Brandvägg

En brandvägg är en säkerhets system som ligger mellan webbsidan/ intranätet/ datorn/ servern som skall skyddas uppkopplingen till internet. Brandväggar kan antingen vara hårdvara eller mjukvara baserade system.

Hårdvara baserad brandvägg är brandväggar som är kopplade in i bredbandsroutrar eller så kan man köpa dem enskilt. De är oftast lätta att konfigurera och uppdatera med nya regler. Hårdvara baserade brandväggar brukar oftast också ha extra säkerhets funktioner som virtuellt privat nätverk (VPN), som är när en dator som är kopplad upp till det publika närverket, beter sig som om den skulle vara direkt kopplad till det privata nätverket.

Mjukvara baserad brandvägg är applikationer som man installerar på datorn. Mjukvara baserad brandvägg används oftast för enskilda datorer och är anpassad just för den datorn. Mjukvara baserad brandvägg skyddar nätverket genom port filtrering, applikations filtrering och paket skanning. Mjukvara baserad brandvägg burkar oftast också innehålla web filtrering. Nackdelen med en mjukvara baserad brandvägg är att den bara skyddar den datorn som den är installerad till.

Nackdelen med en brandvägg är att om något virus kommer förbi brandväggen så kan brandväggen inte göra någonting åt det viruset, varefter det kan fritt göra vad det vill. Det här kan man fixa med att ha ett IDS och/eller IPS aktivt säkerhet som jag kommer att ta upp i nästa kapitel. (Larry L. Peterson)

3 INTRÅNGDETEKTERINGSSYSTEM OCH INTRÅNGSSKYDD

3.1 Intrångdetekteringssystem (IDS)

3.1.1 Vad är IDS?

Den första gången man nämnde IDS var i ett tekniskt dokument skrivet på 1980-talet av James Anderson. I det här dokumentet föreslog han att med hjälp av revisionsinformation skulle man kunna identifiera missbruken som hände i system. 1987 publicerade Dorothy Denning ett dokument på hur ett avvikelseupptäckarsystem skulle kunna implementeras.

IDS primära uppgift är att upptäcka missbruk av datasystem. IDS är designade att upptäcka de här missbruken under pågående intrångsattacker och alarmera säkerhetspersonalen om det. Den kan också göra självständiga beslut för att minska på skadorna från missbruket.

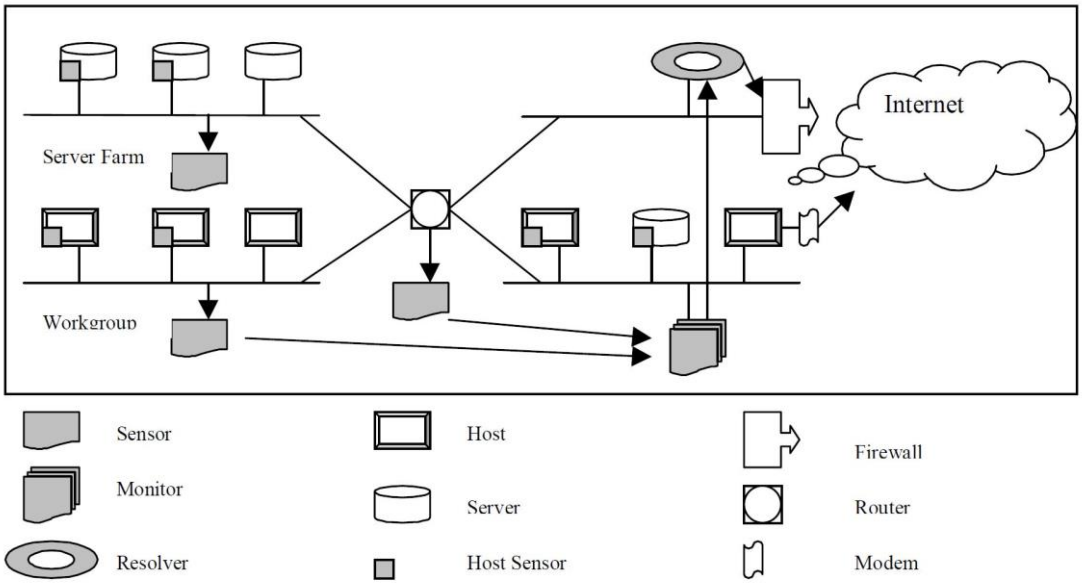
Den andra uppgiften IDS har är att samla ihop data från systemet för att lättare kunna återställa allting efter intrånget, identifiera metoderna som var använda i attacken och erbjuda legalt bevis mot åtalaren efter intrångsattack.

Till IDS uppgifter hör:

- Utskilja skillnader mellan normala användarens beteende och skadliga handlingar.
- Ta hand om komplexa interaktioner i ett nätverk, och kunna navigera sig igenom nätverk och systems arkitektur.
- Rapportera attacker i realtid, dvs. när ett intrång pågår så att säkerhetspersonalen kan reagera på rätt sätt.
- Medarbeta med andra säkerhetsmekanismer och kunna registrera misslyckade samt lyckade intrångsattacker från andra säkerhetsmekanismer.
- Reagera till intrångsattacker med att öka övervakningen av den relevanta platsen, höja säkerheten på den relevanta platsen eller begränsa påträngande beteende.
- Märka missbruks på alla ställen i nätverket.
- Minimera sin inverkan på normalt beteendet och registrera så lite som möjligt falska positiva resultat.

3.1.2 Uppbyggnad

IDS har utvecklat mycket sedan det introducerades på 1980-talet, från att vara en simpel satsorienterad struktur till ett komplex distribuerad realtidsnätverk av olika komponenter. I Figur 2 ser man uppbyggnaden av ett nätverk baserat IDS med sensorer, övervakare och lösaren.



Figur 2. Hur ett IDS nätverk ser ut (Active Network Security, Theuns Verwoerd, 1999)

En IDS är ofta konstruerad av en sensor, övervakare, lösare och kontroller:

Sensor fungerar som ett IDS ögon och samlar ihop data. Datat som en sensor samlat ihop kan vara applikationsloggar, händelseloggar, revisionsinformation och statusloggar, Sensorn kan också övervaka nätverkssegment. Det kan finnas flera sensorer i ett system som tar och sammanfattar all data de har övervakat och skickar det vidare till övervakaren.

Övervakaren är behandlaren av IDS. Den tar emot den sammanfatta informationen, som den fick från sensorn och granskar om det finns några misstänksamma aktiviteter varefter den skapar en rapport som sedan sänds till lösaren.

Lösaren tar emot misstänksamma rapporterna och bestämmer vad som är den lämpliga reaktionen till rapporten. Lösaren kan till exempel alarmera säkerhetspersonalen eller konfigurera om brandväggen.

Kontrollens uppgift är att förenkla administrativa uppgifterna för personalen med att försnabba konfigureringen av IDS-komponenterna. Till exempel höja på mängden uppgifter som samlas in.

3.1.3 Teknik

Det finns två huvudmetoder som använd inom IDS, dvs. missbruks och avvikelsedetektion. Dessutom finns det andra metoder som är baserade på vart man lägger sensorerna och övervaka i nätverket.

Missbruksdetektion fungerar med att observera och jämföra beteenden på vanligt beteendet mot kända intrångbeteendes mönster. Den går igenom metoder som kan lätt känna igen attackmönster, det kändaste mönstret är signaturanalys, som är när man söker efter ett specifikt mönster i ett nätverk. Det kan vara en viss sekvens av byte i nätverket eller en känd instruktionssekvens från ett virus. Signaturanalyser har blivit populärt eftersom det är relativt enkelt både att implementera det samt att förstå sig på data som kommer från analysen.

Det dåliga med den här tekniken är att den försöker representera attacker på ett specifikt sätt. Om en attack varierar från det specifika sättet kan attacken bli maskerad till normalt beteende och på det sättet smita förbi sensorn. En annan negativ sak med missbruksdetektion är att man måste hela tiden uppdatera metoden med nya attackfunktionsregler. Vilket gör att attackmetodlistan som jämförs blir större, som leder till trögare jämförelse i realtid.

Avvikelsedetektion fungerar igen på att observera beteenden som väntas dyka upp i trafiken, som användare och processer. Om någon handling inte beter sig som den skall, flaggas det som misstänksamt beteende. Metoderna skiljer beteendet mellan normalt, oregelbundet och intrångsbeteende med olika tekniker. Till exempel statiska mätningar, expert system, neutrala nätverk och analysering av användarbeteendets. Alla beteenden observeras och jämförs till kända mönster eller förväntade beteenden.

Placeringen av sensorerna kan antingen göras nätverksbaserat (network-based) eller värdbaserat (Host-based). Nätverksbaserade sensorer övervakar trafiken mellan servrar och/eller datorer. Det positiva med en nätverksbaserad sensor är att de upptar ingen nätverks belastning under övervakningen och det räcker med en sensor för att övervaka hela nätverkssegment. Det negativa med nätverksbaserade sensorer är att de har svårigheter att hantera moderna nätverksmodeller, som krypterade meddelanden.

Värdbaserade sensorer observerar samma trafik som värden observerar. Det är oftast värdbaserade sensorer som märker när någon från inom systemet missbrukar systemet och sedan alarmerar det till säkerhetspersonalen.

Övervakning av processmönster är en metod som centrerar sig på att övervaka och upptäcka alla attacker i realtid och erbjuda en omfattande sammanfattningar på data. Största nackdelen med realtids upptäckande metoder är att det tar massor med resurser att processa all data i realtid och att kunna uppfatta komplexa distribuerade attacker. De flesta realtids system brukar designas så att sensorerna och övervakaren ligger på samma ställe så att kommunikationen mellan dem skall vara så snabbt som möjligt.

3.1.4 Styrkor och svagheter i IDS

När man skapar IDS kan man konfigurera det så att de fungerar som en extra nivå av säkerhet till andra säkerhetssystem. Om en intrångsattack klarar av att anfalla nätverkets säkerhetssystem kan IDS alarmera felet och reparera det medan ett intrång är på gång. IDS kan också visa i realtid hur säkert systemet är samtidigt som alla logfiler som är skapade av IDS är krypterade så att bara administratorn har rättighet att läsa dem. Logfilerna kan ge en helhets bild på intrånget och erbjuda alternativ lösningar till problem för framtida intrång.

IDS är också bra på att extrahera information från spårnings intrångsattacker, vilket hjälper IDS definiera när ett intrång påbörjades samtidigt som den identifierar källan av intrånget. IDS kan dessutom upptäcka vad intrångsattacken var

efter från systemet, vilket gör det lättare i fortsättning att skydda sig mot just den intrångsattacken.

Men IDS är inte perfekt. Det finns massor med nackdelar i hela systemet. IDS kan till exempel aldrig stoppa en attack helt och hållet, utan den kan bara upptäcka ett intrång och alarmera det vidare till säkerhetsmekanismer som kan blockera attacken. Vissa IDS påstås att de kan blocka intrångsattacker, men de kan bara göra det om man har konfigurerat in i IDS en säkerhetsmekanism, som brandvägg eller antivirus. IDS är uppbyggd för att samla ihop information av intrångsattacker och försöker sedan spåra sig till källan av attacken. Men eftersom nätverk ofta är mera komplicerade och intrångsattacken inte alltid blir upptäckt förrän det redan är inne i systemet, så kan IDS bara spåra sig tillbaka till platsen varifrån intrångsattacken tog sig in i det skyddade nätverket.

Vissa intrångsattacker är designade för att attackera IDS. De gör det med att anfalla IDS sensorer och korrumperar informationen som sensorerna har samlat ihop till oläsbar information, i vissa fall kan attackeraren till och med imitera sig till en sensor och mata in i systemet falsk data.

3.2 Intrångsskydd (IPS)

3.2.1 Vad är IPS?

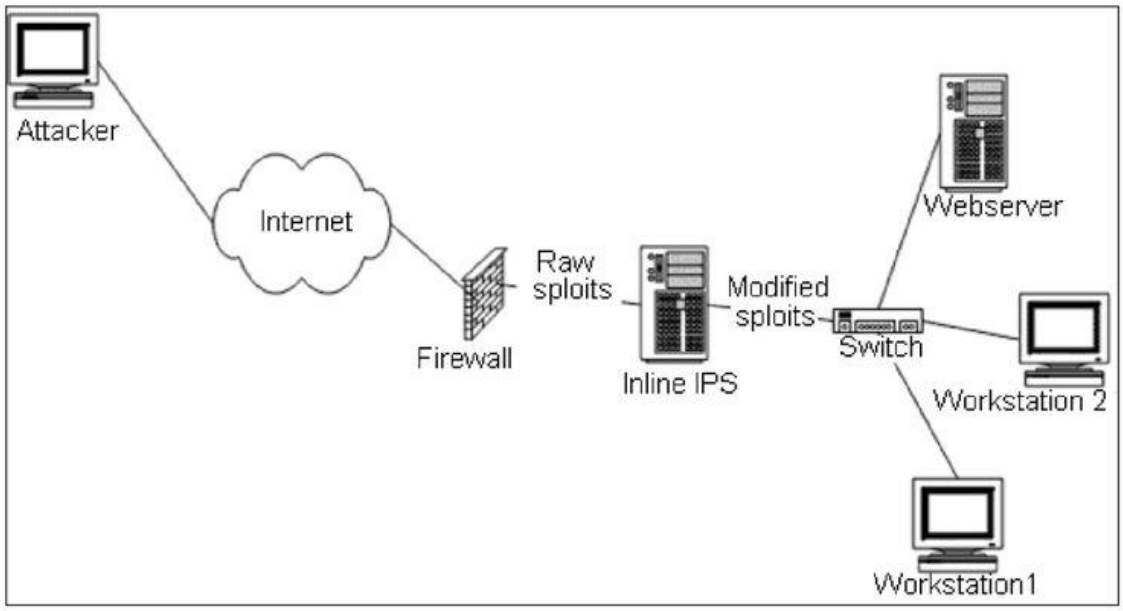
IPS är ett program som specialiserar sig på att hindra intrångsattacker och andra sabotage program från att nå datornätverket. Man kan ganska bra jämföra IPS med en brandvägg, förutom att IPS har omsatta roller när det kommer till reglernas uppbyggnad. I stället för att varje regel som sätts in i systemet ger tillåtelse till systemet och i slutet en generell regel, som förbjuder allting annat (som det fungerar i brandväggar), så fungerar IPS med att varje regel du lägger till i systemet förbjuder den till systemet och sedan har en generell regel i slutet av listan, som beskriver att allting annat har tillgång till nätverket. Om det inte finns inne i systemet en orsak till varför trafiken skulle blockas, så låter IPS trafiken igenom. Det är därför IPS oftast arbetar tillsammans med både IDS och brandväggar och är till och med inkorporerad in i vissa brandväggar.

IPS observerar all trafik som kommer från internet in till nätverket och kontrollerar trafiken som går igenom IPS.

Orsaken till varför man använda sig av IPS är för att blockera kända intrångsattacker till nätverket. IPS är mycket effektiv på att stoppa kända attacker, Oberoende om det är någonting som IDS hittade eller något som fanns i IPS registret. IPS kan också erbjuda en effektiv motreaktion mot en överbelastningsattack.

3.3 Intrångs motåtgärder

IPS har fyra olika motåtgärdsklasser som den kan använda för att hindra intrångsattacker in i systemet. Namnen på alla klasser är baserade på vilket lager av nätverket som motåtgärders. I Figur 3 kan man se hur ett IPS nätverk är uppbyggd



Figur 3. Hur ett IPS nätverk ser ut, (Intrusion prevention and active response 2005)

Datalänk motåtgärd: Om ett intrång upptäcks, kan man med administrativa rättigheter stänga switchporten som är ansluten till det systemet varifrån intrånget upptäcktes. Den här lösningen är bara möjligt för attacker som är genererade inne i det lokala systemet.

Nätverk motåtgärd: Nätverks motåtgärden påverkar på den externa brandväggen eller routern med att lägga till mera offentliga regler, som blockerar all kommunikation från individuella IP-adresser eller hela nätverk. IPS kan genomföra samma uppgift utan att kommunicera med den externa maskinen, eftersom paket från specifika IP-adresser kan bli blockerade efter att intrångsattacken har blivit upptäckt.

Transport motåtgärd: Transport motåtgärden skapar ett TCP RST packet för att förstöra illvilliga TCP sessioner eller emittera ett par ICMP-paket till respons till illvillig UDP trafik.

Applikation motåtgärd: Ändrar på den illvilliga applikationens data så att det blir oanvändbart/ofarligt förrän det når sitt mål. För att kunna använda sig av den här motåtgärden, måste IPS vara inmatat i kommunikations väg och alla Transport lagrets checksummor måste räknas på nytt.

3.3.1 Risken med falska positiva och falska negativa attacker

Eftersom falska positiv och falska negativ attacker finns i IDS så kommer falska positiv och falska negativ attacker naturligt att också finnas i IPS.

En falskt positiv attack är när IDS identifierar ett vanligt paket till en intrångsattack medan ett falskt negativ attack är när en intrångsattack inte blir upptäckt.

Falska positiva och falska negativa attack är någonting som uppkommer i alla IDS system oberoende om hur mycket man försöker arbeta emot det. Falska positiv gör inte bara administratörens jobb mera komplicerat, men om det skapas för mycket data i systemet, så kan det göra hela IDS oanvändbart. I ett stort nätverk kan det skapas upp till 1 miljon alarmeringar eller händelser under en dag och under all falska positiva data kan det smita förbi riktiga intrångsattacker. Oftast skapa falska positiv genom daglig trafik användning, till exempel nä en användare vill laddan ner någon fil från det publika nätet.

Eftersom IDS är passivt och rapporterar bara vidare problemet till säkerhetsadministratorn, blir det inte så stora straff för systemet när IDS skapar ett falskt

positiv. Men när man tar IPS med i bilden, så kan det bli en katastrof. Istället för att vara passiv till attackerna, så kan IPS automatiskt ändra på nätverket genom att antingen med att ändra nätverkstrafik eller gränsa kommunikationen mellan värden och nätverket.

3.4 Nästa generations Intrångdetekteringssystem och Intrångsskydd (IDPS)

3.4.1 Vad är IDPS?

IDPS är nästa steg från IPS, det är en kombination av både IDS och IPS. IDPS kan konfigureras antingen som bara ett IDS alarmeringssystem, eller så kan fullt utvecklat systemet så den också kan stoppar intrångsattacker i IPS läget.

Det finns tre typer av IDPS system; Nätverks IDPS (NIDPS), som övervakar all trafik som går igenom nätverket, trådlös IDPS (CIDPS), som övervakar över all trafik som överförs trådlöst och värd baserad IDPS (HIDPS), som baserar sig på att övervaka alla paket som skickas till en specifik dator.

Lika som IDS lagrar IDPS all data av händelserna, som skickas över till nätverkets administratör/säkerhetsmekanism, var alla händelser blir undersökta för potentiellt hot. Intrångsskyddet stoppar alla upptäckta hot som IDPS, antingen med att avbryta intrångsattacken, om konfigurering av nätverkets miljö eller med att ändra på själva innehållet på intrångsattacken.

Oftast när man installerar ett IDPS, brukar man installera IDS och IPS på olika ställen i nätverket. IDS borde läggas inne i eller i närheten av brandväggen för att kunna övervaka de interna aktiviteterna, bevaka över användarna av nätverket och ge bra blid på alla händelser, både i realtid och gamla sparade händelse. IPS systemet borde läggas i yttersta lagret av nätverket för att kunna lättare stoppa zero-day attacker.

3.4.2 Funktioner

Ett IDPS system borde innehålla en viss mängd funktioner för att kunna räknas som ett ordentligt IDPS system.

I Tabell 1 kan man se en jämförelse mellan olika funktioner styrkor och svagheter i ett IDPS system.

Funktioner		Styrkor	Svagheter
Teknologi lay-out	Tråd nätverk	Tråd nätverk är snabbare och billigare.	De är mycket beroende på plattformens struktur och är inte lätta att installera.
	Trådlöst nät-verk	Är skalbar och oberoende av plattform infra-struktur.	Förut intrång som kan hända i tråd nätverk måste man också skydda trådlösa nätver-ket från attacker.
		Mobila agenter konsumerar minder energi.	
Upptäck-nings metoder	Missbruk	Missbruksdetektion är pålitlig, effektiv och genererar få falska positiv.	Missbruksdetektion är mycket begränsad inom okända attackers upptäckning. De har också svårigheter att upptäcka kända attacker som har en okänd signatur.
			Falsklarm kan förekommas från dåligt be-kräftade signaturer.
			Eftersom varje händelse skall jämföras mot alla signaturer som är registrerade, leder det till en förminskning av upptäcknings-hastigheten och helhetsprestationen.
	Avvikelse	Avvikelsedetektion använder sig av färre regler och kan därför öka på upptäcknings-hastigheten och effektivitet.	Avvikelse upptäckare har en högre falsk positiv alarm eftersom händelser som avvi-ker från det normala beteendet är inte alltid en attack.
		Det är möjligt att identifiera det flesta nya at-tacker utan någon uppdatering, eftersom nya attacker oftast avviker sig från reglerna.	Det kan vara svårt att bestämma var grän-sen mellan ett normalt och onormalt bete-ende går.
			Attacker kan ändra sitt beteende så att det liknar normalt beteendet.
Upptäck-nings tid	Realtid	Kan upptäcka och förhindrar intrång i real-tid.	Realtids upptäckning kan inte hantera krypterade paket.
		Den kan fylla nätverkets säkerhets luckor som är sårbara mot Ddos attacker.	Källidentifiering baserar sig på paketet nät-verk adressen, därför kan källadressen för-falskas så det blir svårt att spåra attacken automatiskt.

	Icke realtid	Den har hög kapacitet att bevisa av intrångsattacken.	Den kan inte stoppa attacken i realtid för att minska på skadorna.
		Den har mindre resursförbrukning.	
Data	Distribuerad	Den distribuerade data utnyttjar informationstrafiken från olika källor för att undersöka säkerheten av nätverket.	Data som transporteras mellan värdövervakaren och sensorn kan generera hög nätverkstrafik.
	Central	Alla sensorer, övervakaren och lösaren styrs direkt av en centraliserad kontrollpanel.	Informationen som används av systemet kommer från paketen i nätverket, vilket betyder att all data måste flytta sig från inträngnings plats, vilket ger attacken möjlighet att förstöra eller modifiera informationen förrän den hinner fram.
			Intrång kan inaktivera programmen i systemet så kan gör IDPS oanvändbar.
Svar typ	Passiva	Den passiva svarstypen underlättar flödet av informationen genom att låta alarmhändelserna komma åt informationstillgången.	Passiva svarstyp avslöjar tillgångarna till intrånget medan säkerhetsadministratorn undersöker alarmet.
	Aktiva	Den aktiva svarstypen blockerar alarmet omedelbart och skyddar informationstillgången.	Den optimala konfigurationen under aktiv svar är sämre än en under passiva svar.
Alarm hantering	Kvalitets förbättring	Är enkel att implementera och är tillgängligt för de flesta nuvarande alarm korrelations system.	Det är ineffektivt att använda sig av den här metoden individuellt, och ger ingen lösning till förminskning av falska positiv.
	Alarm korrelation	Är intuitivt och effektivt i en verklig miljö.	De flesta algoritmerna är baserade på att gå ihop med bara missbruks upptecknings metod.
Struktur	Individuell	Den är lätt att installera på grund av sin individuella struktur.	Den producerar mera irrelevanta och falska alarm.
	Samarbete	Samarbetes IDPS är mera effektiva på att upptäcka och stoppa intrång över internetet.	Kan ha olika lösninger från olika IDPS för samma attack.
		De kan minska beräknings kostnader genom att dela intrångsdetektionsresurserna mellan nätverken.	För deras distribuerade arkitektur så har de mindre skalbarhet.
		De erbjuder omfattande information om intrångsförsök för alarm korrelations ändamål.	Olika detektionstekniker behöver olika beräkning krafter och hastigheter.

Tabell 1. Jämförelse mellan olika funktioner i IDPS (Intrusion Detection and prevention System in cloud Computerng)

4 JÄMFÖRELSE MELLAN IDPS SYSTEM

4.1 Snort

Snort är en öppen källkod nätverks (NIDPS) skapat av Martin Roesch år 1998. När Snort skapades var det en IDS men uppdaterad snabbt med intrångsskydds-delen.

Snorts arkitektur är fokuserad på prestation, enkelhet och flexibilitet, och kan göra protokollanalys, innehållsökning, upptäcka virus som överbelastningsflöde, port skanning, os fingeravtryck och så vidare. Andra styrkor i Snort är paketanalyse-ring vilket rapporterar till administratorn intrångets orsak och föreslår vad för åt-gärder som börs göra.

Flexibiliteten gör så att det är lätt att installera nya regler till systemet. En regel är när man blockerar specifika sårbarheter i systemet. Enkelhet kommer fram i form av en versatil GUI gränssnitt, om man inte vill använda sig av GUI kan man an-vända sig ave UNIX operativsystemets terminal.

Eftersom Snort är multiplattform så kan installeras Snort till Linux, Windows och Mac. Snort kan också paketfånga (pcap) paketen i off-line läget. Snort är en en-trådig motor och skriver loggar i Unified2 format. Unified2 är en IDS händelsefil-format.

4.2 Suricata

Lika som Snort är Suricata också en öppen källkod NIDPS program skapat Open Information Security Foundation (OISF). första beta versionen kom i December 2009, och den första standardiserade versionen kom fram i Juli 2010.

Suricata är också en regelbaserad IDPS motor för att övervaka nätverkstrafiken och ge varningar till administratören när misstänkta händelser inträffas. Suricata är en multitråds IDPS som skriver också sina loggar i Unified2 format. Suricata använder också en sniffer motor för att analysera trafiken i nätverkssystemet.

multi tråds kapaciteten tillåter sniffern att snabbt matcha flera trafikregler. Suricata kan också paket fånga i off-line läget. Samma som Snort så kan man installera Suricata till Linux, Windows och Mac. Både Suricata och Snort är programmerad i C.

4.3 McAfee Endpoint Security

McAfee endpoint security är ett IDPS designad för stora företag med komplexa nätverks strukturer. När man installerar McAfee nätverket till ett företag behöver man också installera en specifik sensor hårdvara komponent. McAfee nätverket erbjuder på fyra olika stadiers hårdvara sensorer; NS9200 (250.000 €), NS7200(80.000 €), NS5200 (30.000€) och NS3200 (3200 €). Prisklassen varierar mycket när man värderar två sensorer från olika standarder, man om man varierar mellan samma standards sensorer, som NS5200 (30.000€) och NS5100 (28.000€) så är prisen mera jämnt.

McAfee använder sig av en heuristisk detektor samt en blandning av IPS regler vilket gör detektorn till en extremt bra emot nya virus, intrång och för nya sårbarheter och utnyttjan. Men tack vare att den effektiviteten så höjs också falskpositiv värdet lite. Falskpositiv värdet är estimerat att höjas med 0.002 procent upp till 0.04 procent, beroende på vad för arbete man håller på med. De flesta falskpositiv kom ändå från när användaren försöker ladda ner eller installera någonting på deras dator.

För falskpositiv förhindrande använder sig McAfee av en ”Contextual” metod, för att kontrollera om det var användaren som starta scriptet eller inte. Metoden tar i beaktan om var användaren surfar på websidor, hur användarens mus beter sig, digitala signatur av nerladdade filer och om sidan är pålitlig.

För att lättare kunna förhindra polymorf virus använder McAfee sig av emulatorer. Ett polymorft virus är ett virus som byter sin krypterings metod och nyckel, som den använde för att kryptera det originella viruset, varje gång viruset kopierar sig själv så byter sin krypterings metod. Emulatorn kan kämpa emot det här med att simulera en virtuell dator, var man lägger den misstänkta filen. Den misstänkta

filen tars isär som ett operativsystem och sedan sparas en data struktur. Det här ger en god insikt på den misstänkta filen, och ger en hög hotförutsägelse.

I tabell 2 kan man se resultatet på ett kvalitetstest gjort för McAfee 2016 i augusti.

	July	August	Industry average
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 162 samples used	97.6%	93.7%	98.0%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 15,151 samples used	99.7%	99.9%	99.0%
Protection Score			4.5/6.0

	Standard PC	Industry average	High end PC	Industry average
Slowing-down when launching popular websites 40 websites visited	15%	16%	10%	17%
Slower download of frequently-used applications 20 downloaded files	4%	5%	1%	3%
Slower launch of standard software applications 12 test cases applied	7%	7%	22%	15%
Slower installation of frequently-used applications 19 installed applications	17%	26%	39%	49%
Slower copying of files (locally and in a network) 7,605 files copied	22%	13%	30%	10%
Performance Score				5.0/6.0

	July	August	Industry average
False warnings or blockages when visiting websites 500 samples used	0	0	0
False detections of legitimate software as malware during a system scan 1,332,434 samples used	0	0	3
False warnings concerning certain actions carried out whilst installing and using legitimate software 41 samples used	0		0
False blockages of certain actions carried out whilst installing and using legitimate software 41 samples used	1		0
Usability Score			6.0/6.0

Tabell 2. McAfee kvalitettest (AV-TEST Product Review and Certification Report – Jul-Aug/2016)

4.4 F-Secure Business Suite

F-Secure Business Suite är ett IPDS som är designad för medel/små företag. F-secure erbjuder ingen sensor komponent så om man vill ha en sån måste man

beställa det från något annat företag. Som exempel Cisco eller Juniper som skapar sensor komponenter i olika storlekar, om det är i tal om ett lite företag räcker Cisco ASA 5500-X serien (1850€ - 16.000€). Samma som McAfee, har F-Secure plattformsstöd för Linux, Mac och Windows Vista, Windows 7, Windows 8/8.1 och Windows 10.

F-Secure är optimerad att vara lätt och ha så lite inverkan som möjligt på nätverkets prestation. Användningen och uppdateringen av systemet är lätt, även med de komplexa kraven från medel/små företagen.

F-Secure använder sig av ett beteendebaserad IDPS som heter DeepGuard. DeepGuard är ett flerskikts IDPS, vilket betyder att den består av flera olika moduler som är designade för olika hot. Modulerna består av:

Surfskydd, som skyddar användarens webbläsare genom att kontrollera om de webbsidorna som användaren surfar på är säkra. För att effektiv kunna hantera alla miljontals webbsidorna tillgängliga på internet, fungerar surfskyddet med att kontrollera med F-Secures Security Cloud om websidan är pålitlig.

Filskanning, som skyddar nätverket med att skannar igenom alla filer som skall installeras, laddas eller modifieras innanför nätverket. Den här funktionen är en heuristisk identifierare (samma som används av McAfee) som identifierar virus och andra skadliga programvaror, som har likadan uppbyggnad som tidigare virus den har upptäckt.

Filanalys, är när DeepGuard kontrollerar med moln nätverket om det har kommit någon ny information om det skannade programmen, databasen ligger hos F-secure analys lab.

Beteendeanalys, övervakar och avlyssnar på misstänksamma filer, både vid applikationen start och medan applikationen är igång. Det här tillåter DeepGuerd att identifiera Exploitbaserade attacker oberoende vad för sårbarhet som används.

Exploit analys Fungera på samma sätt som beteendeanalys, men övervakar och söker efter kända beteenden av ett exploit program i alla skannade program.

I tabell 3 kan man se resultatet på ett kvalitetstest gjort för F-secure 2016 i augusti.

	July	August	Industry average
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 162 samples used	100%	98.7%	98.0%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 15,151 samples used	100%	100%	99.0%
Protection Score			6.0/6.0

	Standard PC	Industry average	High end PC	Industry average
Slowing-down when launching popular websites 40 websites visited	9%	16%	11%	17%
Slower download of frequently-used applications 20 downloaded files	8%	5%	6%	3%
Slower launch of standard software applications 12 test cases applied	5%	7%	12%	15%
Slower installation of frequently-used applications 19 installed applications	25%	26%	82%	49%
Slower copying of files (locally and in a network) 7,605 files copied	23%	13%	23%	10%
Performance Score				4.5/6.0

	July	August	Industry average
False warnings or blockages when visiting websites 500 samples used	0	0	0
False detections of legitimate software as malware during a system scan 1,332,434 samples used	6	3	3
False warnings concerning certain actions carried out whilst installing and using legitimate software 41 samples used	0		0
False blockages of certain actions carried out whilst installing and using legitimate software 41 samples used	0		0
Usability Score			5.5/6.0

Tabell 3. F-Secure kvalitettest (AV-TEST Product Review and Certification Report – Jul-Aug/2016)

4.5 Jämförelse av Suricata och Snort

4.5.1 Mätningar

Till experimentet har man valt att jämföra prestationen mellan två NIDPS. Mätningarna kommer att vara av träffsäkerheten, falsklarm och kapaciteten. Har man

begränsningar i kapaciteten, kan det förekomma falska negativ. När NIDPS överstiger sin kapacitet, kommer paketens övervakning att sänkas vilket ger illvillig data möjligheten att smita igenom systemet. I undersökningen definierar man NIDPS träffsäkerhet med att räkna bevakningen, sannolikhet av falsklarm, sannolikhet av uppteckning, attackresistans, möjligheten att hantera hög bandbredds trafik och kapaciteten. I tabell 4 visar man några av metriken som utgör kapaciteten. Undersökningen nämnde att följande metriker borde registreras: bitgrupper per sekund, paket per sekund och mängden nätverksattacker. Tillsammans med, antal paket tappade, positiva attacker negativa attacker, negativa falsklarm och det totala antalet alarmen som var registrerade per NIDPS. Värd resurserna som var bevakade var CPU, och minnesutnyttjningen, lagringen, nätverks bandbredd och filens statistik.

Test Metrics	Resources Used
Packets per Second	CPU Cycles, network interface bandwidth, memory bus bandwidth.
Bytes per second (average packet size)	CPU Cycles, network interface bandwidth, memory bus bandwidth.
Protocol Mix	CPU cycles and memory bus bandwidth.
Number of unique hosts	Memory size, CPU cycles, memory bus bandwidth.
Number of new connections per second	CPU cycles and memory bus bandwidth.
Number of concurrent connections	Memory size, CPU cycles, memory bus bandwidth.
Alarms per second	Memory size, CPU cycles, memory bus bandwidth.

*Tabell 4. Metrik kapacitet (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

4.5.2 Testplattform

Den här undersökningen är uppbyggd i en virtuell miljö för att lättare kunna transportera experimentet. Den valda virtuella plattformen var Vmware workstation 6.5

och Ubuntu 10.4.TLS 32 bit var operativ systemet. De var valt för att de är de mest populära Linux-operativsystemen. NIDPS hårdvaran var konfigurerad med 2.8 GHz (E5462) Quad-Core Intel Xeon, med fyra kärnor i sig och 3 GB av DDR2 800MHz fullt buffrat minne. Vardera NIDPS system hade också 20 GB av hårddisk. Snort och Suricata är konfigurerade att använda identiska regler i sig. Suricata använder sig av en annan klassifikations konfiguration från Snort, som använder sig av 134 avkodare och 174 förbehandlings regler. Båda NIDPS använder sig av MySQL, Barnyard och AcidBase som inloggningsmetod. Versionen som används i Snort är v2.8.5.2 och för Suricata används v1.0.2. Båda systemen använder sig av Snort v2.8.5.2 VRT regler kombinerat med Emerging Threats regler. Efter att alla regler har blivit inmatade i systemen så hade Suricata 11039 uppteckningsregler medan Snort hade 11065 regler. Skillnaden mellan mängden regler ligger i att Suricata misslyckade parserat vissa VRT regler.

4.5.3 Trafik

När man väljer trafiken till ett NIDPS undersökning, så måste man ta till beaktan om attack trafiken kommer att vara för sig själv eller vill man lägga till bakgrunds trafik i undersökningen. Bakgrunds trafik kan vara antingen genererat på riktigt eller simulerat. Det är mera användbart att använda sig av riktig nätverks bakgrunds trafik i en undersökning, men det kan uppkomma oberäknade problem eftersom nätverk är dynamiskt. I den här undersökningen har man löst problemet med att lagra trafiken i en pcap fil. Den här lösningen låter dem göra undersökningen off-line.

Det finns flera olika testtrafikresurser på nätet för nerladdning men de flesta av dem är rensade, vilket gör dem oanvändbara i NIDPS innehållsmatchning, som använder sig av ”deep packet inspection”. Trafiken som används i undersökningen är lagrad från ett sysselsatt universitets websida och applikationsserver. Den här trafiken var sedan ihopsatt med utnyttjningspaket med hjälp av Metasploit Framework. Metasploit Framework innehåller totalt 587 utnyttjnings moduler som gör det lätt att generera attacker. Utnyttjningstrafik var lagrad med hjälp av att skapa attacker med Metasploit mot en Microsoft Windows 2000 maskin. Attackerna som är använda i undersökningen kan man se från Tabell 5 som var

lagrade med Wireshark. Med hjälp av Edicap, som är en del av Wireshark, kunde man modifiera tidsstämpeln på utnyttjningstrafik så att den är samma som bakgrundtrafiken. När all trafik är lagrad så slår man ihop all trafik i kronologisk ordning så att attacktrafiken är blandas emellan bakgrundtrafiken.

Code	Name	Description
ms03_026_dcom	Microsoft RPC DCOM Interface Overflow	Module exploits a stack buffer overflow in the RPCSS service
ms05_039_pnp	Microsoft Plug and Play Service Overflow	Stack buffer overflow in the Windows Plug and Play service
ms05_047_pnp	Microsoft Plug and Play Service Registry Overflow	Stack buffer overflow in Windows PnP services. Causes Reboot
ms06_040_netapi	Microsoft Server Service NetpwPathCanonicalize Overflow	Stack buffer overflow in the NetApi32 CanonicalizePathName() function using the NetpwPathCanonicalize RPC call in the Server Service
ms05_017_msmq	Microsoft Message Queueing Service Path Overflow	Exploits a stack buffer overflow in the RPC interface to the Microsoft Message Queueing service
ms01_033_idq	Microsoft IIS 5.0 IDQ Path Overflow	exploits a stack buffer overflow in the IDQ ISAPI handler for Microsoft Index Server

*Tabell 5. Utnyttjningar som var använda i undersökningen (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

4.5.4 Stressning av Systemets

NIDPS kapacitet är anslutet med CPU:s kapacitet, så borde Snort och Suricata utsättas för CPU försämring för att kunna utvärdera deras effektivitet under en stressfull miljö. I Vmware har man därför tillåtit ett par av de logiska och fysiska kärnorna vara begränsade. Både Snort och Suricata kan spela om pcap filen internt. Det här är gjord med den maximala hastigheten som NIDPS kan erbjuda, vilket ger en god metrik för prestationerna av systemet. När man använder sig av den här metoden kan man inte räkna med den maximala förlustfria skalan MLFR. Det är därför man har i den här undersökningen använt dig av TCPReplay istället, som kan kontrollera trafikens hastighet och tillåta stressfull testning under nätverket.

4.5.5 Systemets övervakning och Experimentprotokoll

Resurserna som kommer att vara övervakade är: CPU användningen, minnes användningen, beständig lagringsbandbredd och nätverksbandbredden. Detta utfördes genom att användningen av Linux kommando verktyget Dstat.

Attacktrafiken kördes igenom på både NIDPS med fyra olika varianter av CPU konfigurationer: 2 processors kärnor, 1 kärna, 50 % och 75 % belastning. Möjligheten för NIDPS att läsa paketen, samtidigt som träffsäkerheten var mätt, med extra uppmärksamhet var lagt på falska negativ uppteckning. Testtrafiken spelades sedan in till miljön med TCPReplay som 40 gånger så snabbt som det var lagrat med. Resultatet från det här var en uppspelningshastighet på 3.1 Mbps och en paket förlust på under 2 %.

Varje gång testet kördes, lagrades trafiken med en tidsstämpel från när det började och när det slutade. Det här gav bra referenser till när man analyserar alarmen och systemets statistik. För varje testkörning lagrades alarm informationen med Acidbase, samtidigt som de odefinierbara alarmen arkiverades för framtida referenser. Statistiken som producerad i NIDPS var antalet genererade alarm,

hur många paket var processade och vad var förhållandet mellan nätverksprotokollens användning. All trafik som kom från 192.168.16.2 och 192.168.16.128 var registrerade som illvilligt trafik.

4.6 Resultat

Resultatet från Undersökningen från både NIDPS av Noggrannhet, paketförlust, systemutnyttjande och off-line hastighet. Varje del tars nu upp enskilt.

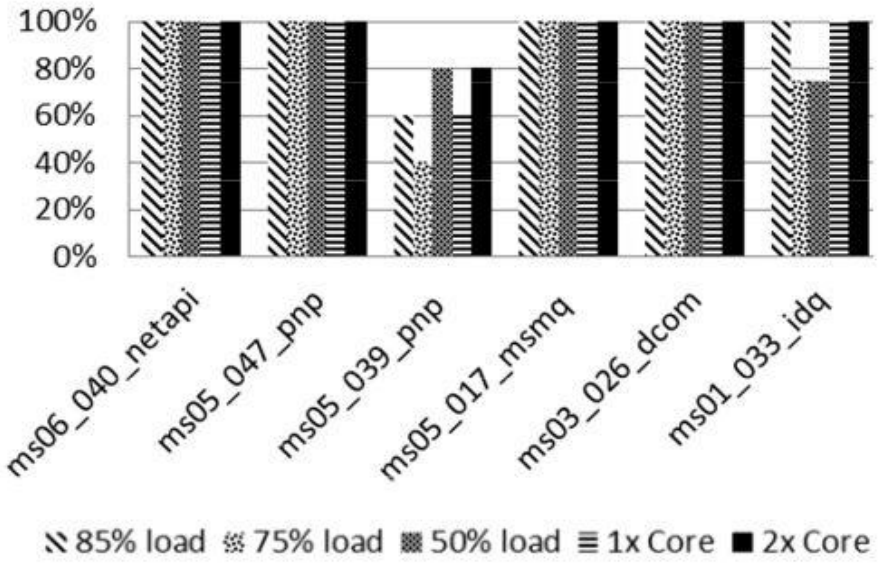
4.6.1 Noggrannhet

För att kunna bestämma noggrannheten behöver man en alarmkontrollant. De här är alarmen som genererade utan något system stress, som en sorts baslinje. Avvikelse från baslinjen under stressen registreras som noggrannhetsändring.

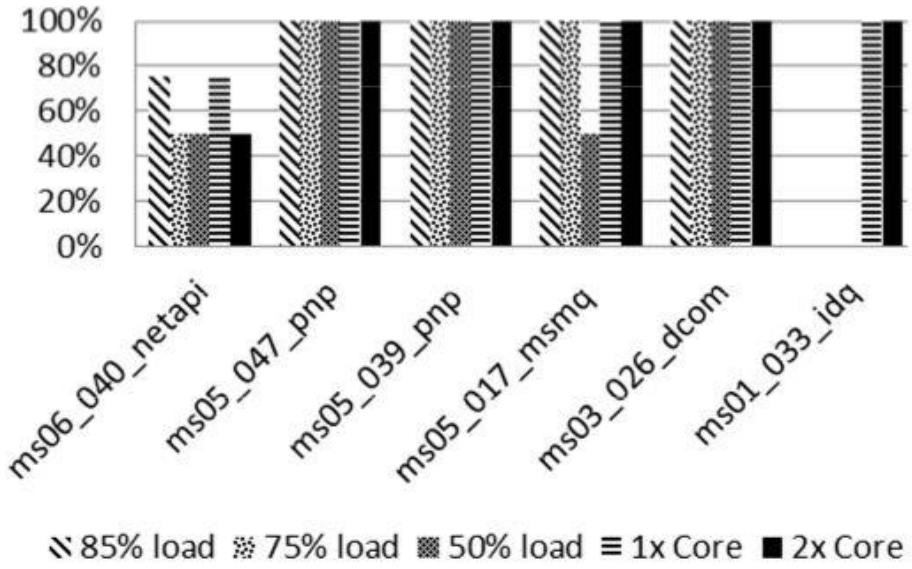
Tabell 4 visar mängden av alarmtyper som har blivit genererade under attackerna gjorda mot vardera NIDSP. Figur 4 visar att Suricatas alarmerades av varje utnyttjare, under alla konfigurationer men några alarm missades vilket ledde till ett förminskning i uppteckningsskala.

Alert	Snort	Suricata
ms05_040_pnp	4	4
ms05_047_pnp	1	1
ms05_039_pnp	1	6
ms03_026_dcom	1	2
ms01_033_1dq	2	4
ms05_017_msmq	2	3

*Tabell 4. Alarmen genererad av Snort och Suricata (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

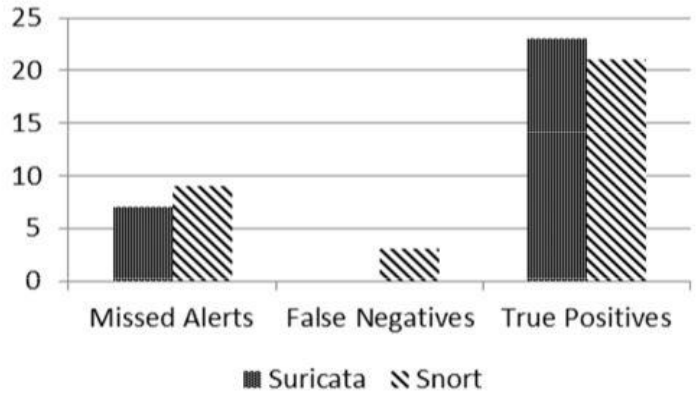


*Figur 4.Suricata alarm (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*



*Figur 5. Snort alarm (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

I Figur 5 visar man att Snort hade problem att alarmera ms01_033_idq. Det här är en falsk negativ som är orsakad av överbelastning.

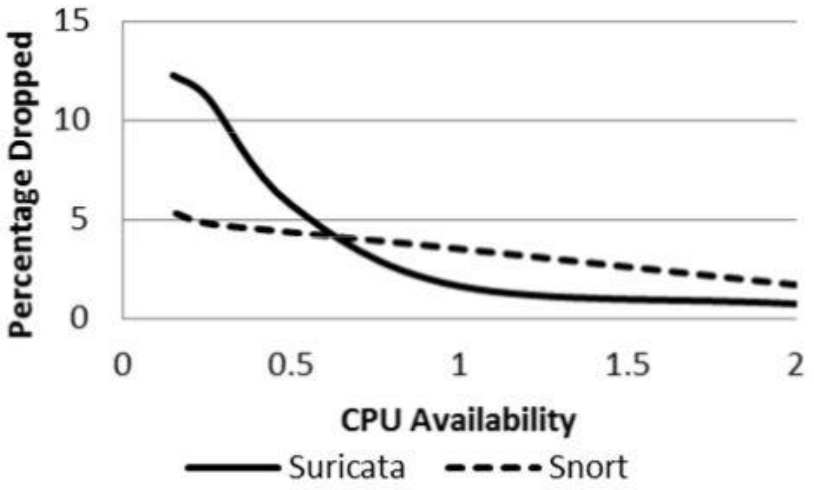


*Figur 6. Intrång noggrannhets mätning (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

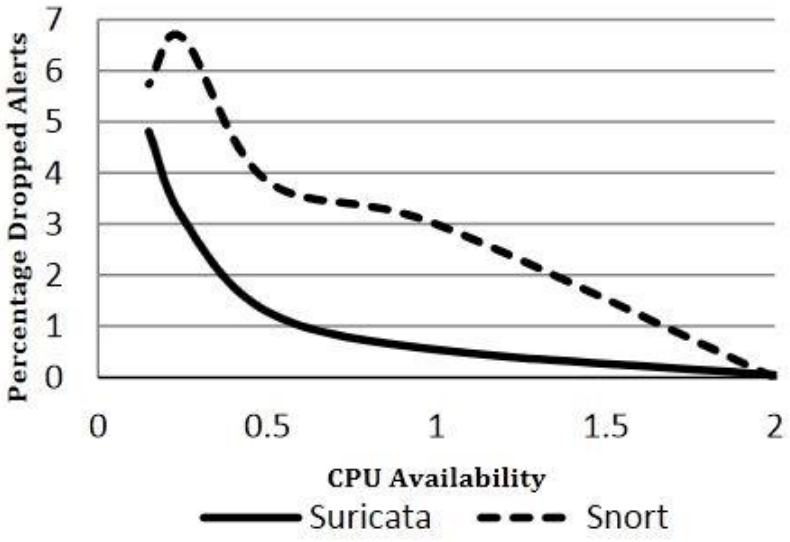
Figur 6 visar antalet falska positiv och riktiga positiv från båda NIDPS i relation till missade alarmen av båda systemen.

4.6.2 Paketförlust

Falska negativ kan vara orsaken till sänkningen av paket. Figur 7 visar mängden paket som tappades av Snort och Suricata och CPU tillgänglighetens fall. Medan Snorts procenthalt håller sig relativt linjärt så har Suricatas prestation avtagit märkbart efter att CPU tillgänglighet sjunker under 1 kärna. I Figur 8 visar man hur antalet kärnor och stressning av CPU verkar på falska negativ på båda systemen.



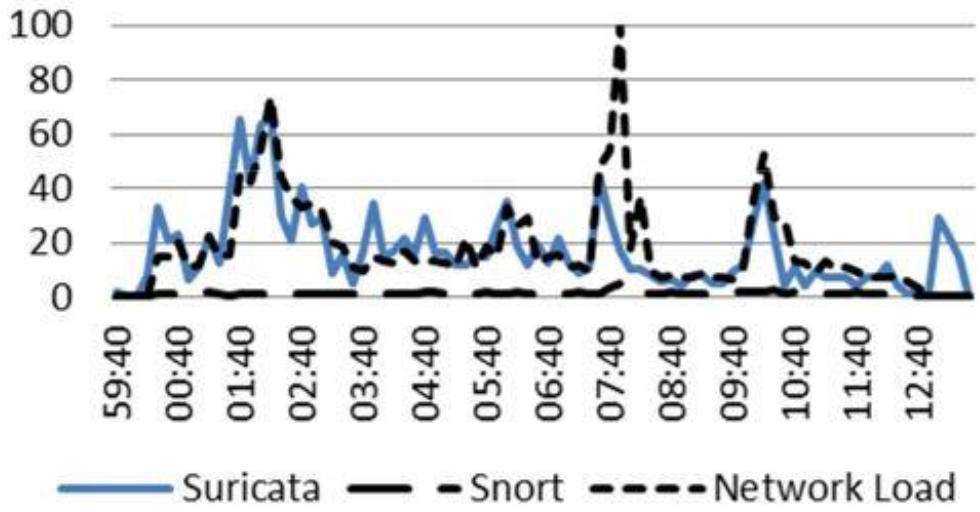
*Figur 7. Paket förlust i 3.2 MBps (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*



*Figur 8. Falska negativ (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

4.6.3 Systemutnyttjning

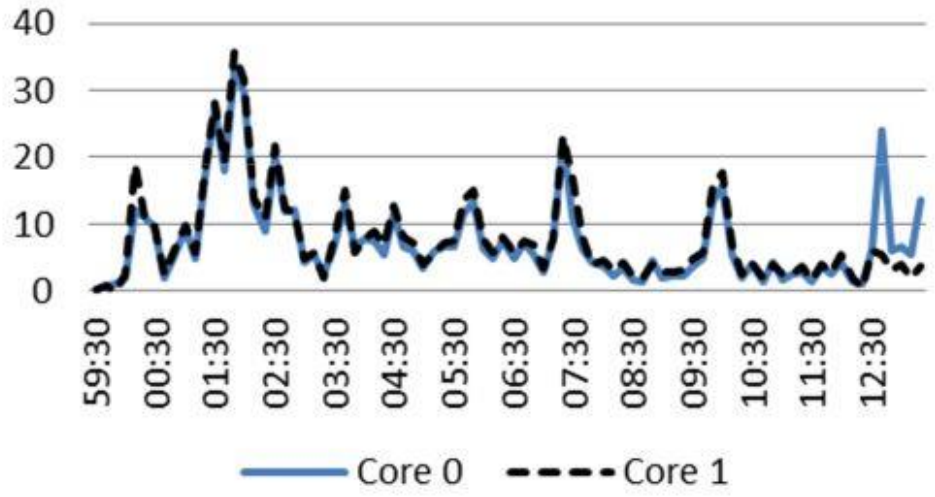
Figur 9. visar förhållandet mellan CPU utnyttjningen och nätverks genomströmning av både Suricata och Snort. Den avbildar hur CPU last ökar relativt till nätverkets genomströmning. Det här beteendet framträder mera i Suricata, Snort visar liknande beteende i en minder skala.



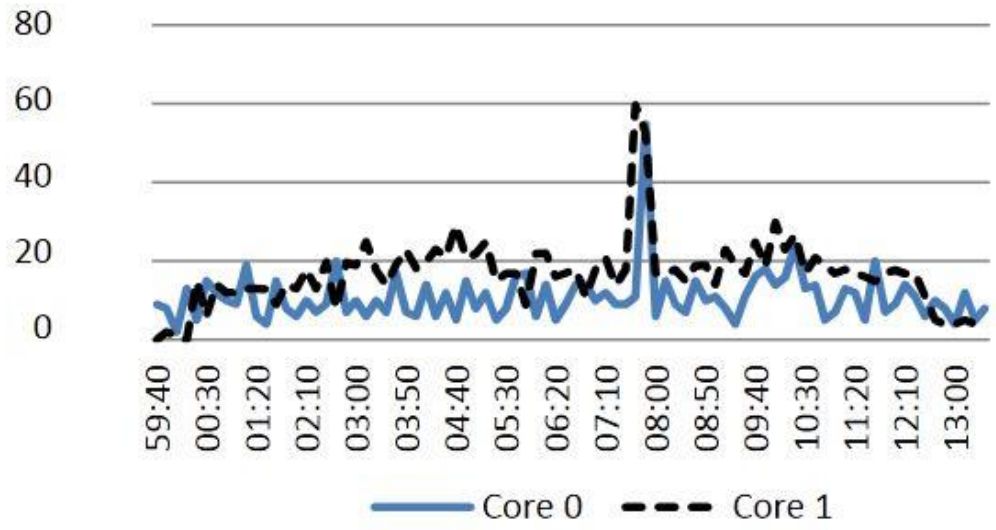
*Figur 9. Nätverks genomströmning och CPU utnyttjning av en enkel källas konfiguration (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

Med 2 kärnors möjlighet har Suricata en lägre tappning kurs än vad Snort hade. För att undersöka det här, så utvärderades båda systemen att använda sig av båda kärnorna.

Figur l0 visar hur Suricata använder sig likformigt av båda kärnorna medan i Figur 11 ser man Snort ha en mera oregelbunden balans av sin utnyttjning. Det här är förväntat av Suricata som har en flertråds design medan Snort inte har det.

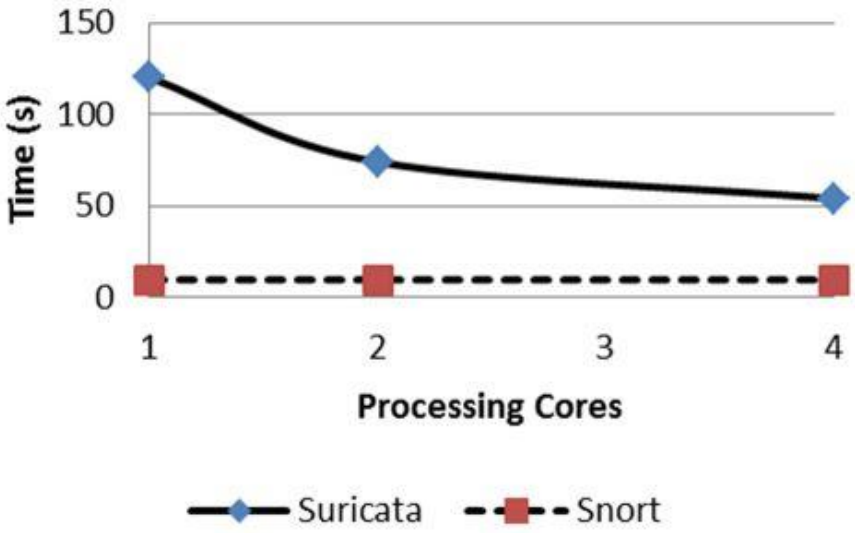


*Figur 10. Suricata med båda kärnorna (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*



*Figur 11. Snort med båda kärnorna (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

Både NIDPS har möjligheten att processa trafiken i off-line läge genom att ta emot en pcap fil och processa det i maximala kapaciteten. Det här var gjort för att kunna identifiera hur snabbt vartdera systemet kan processa trafiken. Samma fil användes till båda Systemen. Tiden för båda system hittar du i Figur 12.



*Figur 12. Pcap processtid (*David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine)*

Flera kärnor hjälper inte Snort prestera bättre medan Suicatas prestation höjdes med 220 % när man använde sig av 4 kärnor.

4.7 Diskussion

Som man kan se i undersökningen hittade Suricata mera intrång än vad Snort gjorde, men la också en större del stress på själva CPU: n. Undersökningen visar också att Suricata ökar sin prestationsförmåga med mera kärnor i användning medan Snort presterar exakt lika effektivt med en kärna som med två eller flera kärnor. Det betyder att Suricata metoden har större risk för falska positiva desto mindre kärnor som är i användning och därför är det bäst att använda i miljöer med minst två kärning CPU. Eftersom det viktigaste uppgiften in IDPS är att ha en bra träffsäkerhet av intrångsattackerna så besluter man att Suricata är det mera effektiva IDPS systemet. Men det gäller också att påpeka att Snort fungerar bra i mindre nätverk med liten trafik.

5 SLUTSATS

Det här examensarbetet gick ut på att undersöka och jämföra skillnaden på olika IDPS. Första delen av examensarbetet är mera teoretiskt när jag går igenom alla

delar i ett aktivt nätverk. Examenarbetet var en litteraturstudie så forskningen jag går igenom här är inte genererat själv utan är tagit från andra undersökningar från nätet och tolkat det med mina ägna ord. Undersökningen är gjord av två öppen källkod IDPS, så det är inte de bästa som finns på marknaden men eftersom installation av mjukvaran och hårdvaran av ett kommersiellt IDPS kan kosta från 2000 € upp till över 100.000 € så jag tror att det räcker med att jämföra skillnaden Snort och Suricata. Jag tog också fram två kommersiella IDPS, McAfee och F-Secure, men beskriver bara snabbt vad för funktioner de använder sig av.

Resultatet visar Suricata med mindre falska negativ, falska positiv och mera intrångsdetektioner prestera bättre med kom med en kostnad på CPU: n och mängden kärnor som användes.

För vidare undersökning skulle man kunna höja på mängden kärnor som användes i Suricata, för att kunna få en bättre bild av Suricats prestation. Man skulle också kunna göra en jämförelse mellan ett NIDPS och ett CIDPS för att få en bild på hur bra en trådlös IDPS presterar relaterat till ett nätverk IDPS.

6 KÄLLOR/REFERENCES

School of Electronic Information and Engineering, Beijing Jiao Tong University, P. R. China, P. Dong; T. Zheng; H. Zhang; X. Du; M. Guizani

A. Freitas, J. Timmis, 2007, *Revisiting the foundations of artificial immune systems for data mining*, IEEE Transactions on Evolutionary Computation 11 (4) 521–540.

Bush, Stephen F., and Kulkarni, Amit B. *Active Networks and Active Network Management.* Hingham, US: Kluwer Academic Publishers, 2001. ProQuest ebrary. Web. [11 April 2016].

Makoto Kubota, 2006*, Intrusion detection and prevention system*, 24.04.2016

Krawetz, N 2006, *Introduction to Network Security, Course Technology / Cengage Learning*, Boston, MA, USA. Available from: ProQuest ebrary. [11 April 2016].

Anita K. Jones and Robert S. Sielken *Computer System Intrusion Detection: A Survey1*, Department of Computer Science University of Virginia Thornton Hall Charlottesville, 19 April 2016

Larry L. Peterson and Bruce S. Davie, 2012 *Computer Networks a systems approach*, Cryptographic, Morgan Kaufmann, s. 635-647

Larry L. Peterson and Bruce S. Davie, 2012 *Computer Networks a systems approach*, Firewall, Morgan Kaufmann, s. 681-686

TechTarget, IDS or IPS [www] Tillgänglig: http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both Hämtad: 20.04.2016

How stuff works, How Firewalls work, [www] tillgänglig: http://computer.howstuffworks.com/firewall.htm Hämtad: 20.04.2016

http://searchsecurity.techtarget.com/guide/Best-Intrusion-Detection-and-Prevention-Products-2011 Hämtad: 20.04.2016

The CERT® Division of the Software Engineering Institute at Carnegie Mellon University*, US cybercrime: Rising risks, reduced readiness*, https://collabra.email/wp-content/uploads/2015/04/2014-us-state-of-cybercrime.pdf Hämtad 20.04.2016

F-Secure, 2014 Botnets skapade [www], Tillgänglig: https://www.f-secure.com/en/web/labs_global/botnets Hämtad 20.04.2016

TechTarget, scriptkiddy [www] Tillgägnlig: http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy Hämtad 21.04.2016

SANS, Honeypot, [www] Tillgägnlig: https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9 Hämtad 23.04.2016

Trend micro, 2015 *Understanding Targeted attacks: goals and motives* [www] Tillgänglig: http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-goals-and-motives Hämtad: 24.04.2016

802.11 Security, 2003, *Denial of Service attacks*, Bruce Potter & Bob Fleck s. 19-23

Windows Security, Intrusion Detection System [www] tillgänglig: http://www.windowsecurity.com/articles-tutorials/intrusion_detection/Intrusion_Detection_Systems_IDS_Part_I__network_intrusions_attack_symptoms_IDS_tasks_and_IDS_architecture.html Hämtad: 25.04.2016

Michael Rash, Angela Orebaugh & Graham Clark, 2005 *Intrusion Prevention and Active Response: Deploying Network and Host IP*

David J. Day & Benjamin M. Burns, 2011, *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engine*

Mcafee network security platform, [www] tillgänglig: http://www.mcafee.com/us/resources/data-sheets/ds-network-security-platform-ns-series.pdf Hämdtad: 15.11.2016

Guide to intrusion Detection and Prevention System, 2007 [www] tillgänglig: https://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-94-guide-to-intrusion-detection-and-prevention-systems-2007.pdf Hämdtad: 20.11.2016

Suricata Download, [www]] tillgänglig: https://oisf.net/suricata/ Hämdtad: 25.11.2016

Aldeid, *Suricata vs Snort,* [www] tillgänglig: https://www.aldeid.com/wiki/Suricata-vs-snort Hämdtad: 25.11.2016

Christoph Alme and Declan Eardly*, McAfee Anti-Malware engine: Values and Technologies* [www] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25219/en_US/mcafee_engine_technologies.pdf Hämdtad: 26.11.2016

F-Secure, *The easy way to security and simplicity*, [www] http://www.viruslogic.com/datasheets/BusinessSuitebrochure.pdf Hämdtad: 26.11.2016

F-Secure, *DeepGuard:Proactive on-host protection against new and emerging threats*, [www] https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf Hämdtad: 26.11.2016

Zonealarm, *What's the difference between Hardware and Software firewalls?* [www] http://www.zonealarm.com/firewall-blog/blog/difference-hardware-software-firewalls/ Hämdtad: 1.12.2016