INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Intrusion Detection System – ein Security-Element

Was passiert in Ihrem Netzwerk? Wissen Sie über alle Aktivitäten bescheid? In Anbetracht des riesigen Datenaufkommens ist dies von Hand nicht mehr zu bewältigen. Intrusion Detection Systeme, kurz IDS genannt, untersuchen alle Datenpakete auf Manipulationen und geben bei Veränderungen Alarm. Unser INFONEWS zeigt Ihnen Grundlagen und Möglichkeiten zum Einsatz von IDS auf.

Dies ist eine kostenlose Dienstleistung der GO OUT Production GmbH (www.goSecurity.ch).

Inhaltsverzeichnis

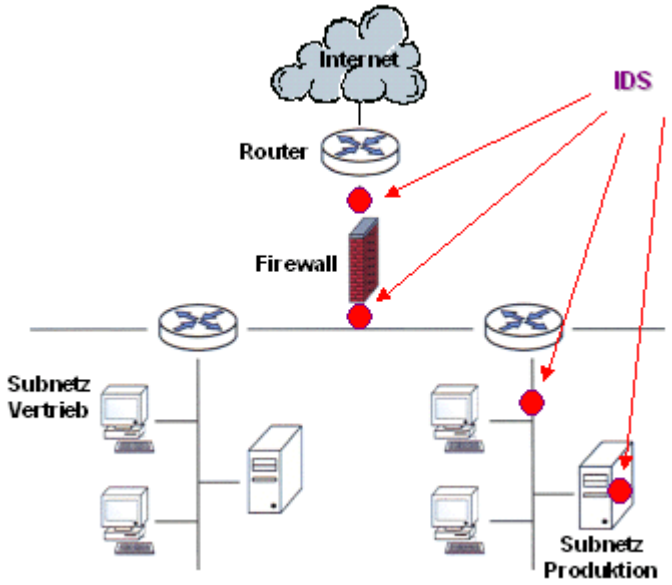
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Was ist ein IDS?

IDS steht für Intrusion Detection System und IDR für Intrusion Detection Respons. Ein IDS/IDR überwacht und protokolliert den gesamten Datenverkehr des Netzwerkes in Echtzeit und erlaubt es Unregelmässigkeiten zu erkennen und abzuwehren. Es unterstützt somit eine Firewall, welche nicht zwischen „Gut“ und „Böse“ unterscheiden kann, sondern Datenpakete anhand des Zielportes und ev. der Ziel-IP passieren lässt. Angreifer können so problemlos Zugriff auf lokale Ressourcen erhalten, Informationen manipulieren und vertrauliche Daten einsehen und auch Datenbestände löschen. Eine Beschreibung für diese Angriffsversuche ist sehr detailliert im Internet frei nachzulesen. Entsprechende Tools sind ebenfalls im Internet und über die CD der gebräuchlichsten Computerzeitschriften zu bekommen. Zu bedenken ist auch, dass Angriffsversuche häufig auch aus dem lokalen Netzwerk heraus gestartet werden, welche Firewallsysteme - sofern überhaupt möglich - nicht überwachen.



1.1 Arten des IDS

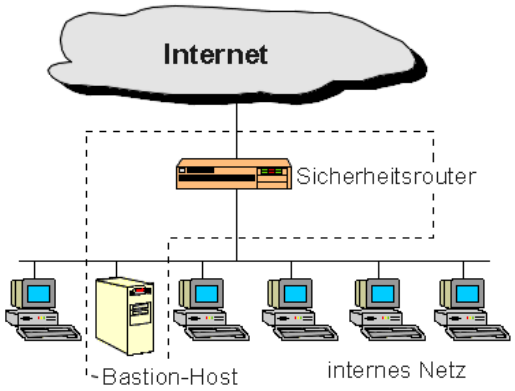
1.1.1 Host IDS (HIDS)

Bei dieser Art des IDS werden auf jedem Host Agents installiert. Die-ser Agent überprüft Event Logs, kritische System Daten, unautorisierte Zugriffe oder suspekte Da-ten. Immer wenn etwas nicht in das Schema passt wird ein Alarm generiert. Zum Beispiel kann ein HIDS die erfolgten Login Zugriffe überwachen und zu viele falsche Passwort-Eingaben aufzeichnen.

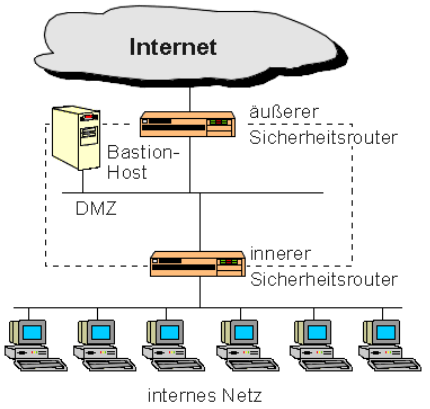
Ein anderer Mechanismus ist den Status eines Systems und der Daten zu überwachen, meistens über einen Snapshot Mechanismus. Will ein Angreifer oder ein Trojanisches Pferd Veränderungen an dem System erreichen, schlägt das HIDS Alarm.

1.1.2 Network IDS (NIDS)

Diese Systeme beobachten den Netz-Verkehr in Echtzeit um DOS Attacken oder gefährliche Inhalte zu analysieren bevor das Ziel er-reicht wird. Das wird durch den Vergleich mit einer Datenbank erreicht (Signaturen Datenbank). Diese Datenbank wird in regel-mässigen Abständen gepflegt und erweitert. Wird ein verdächtiger Netz-Verkehr erkannt, kann so-wohl ein Alarm gegeben werden als auch die Verbindung unterbrochen werden. Die meisten heute bekannten Systeme arbeiten im “promiscous mode”. Das bedeutet das alle Pakete eines Segmentes interpretiert werden egal ob Sie für die IDS Maschine bestimmt sind oder nicht. Das heisst allerdings auch dass speziell bei höherer Bandbreite eine erhebliche Anzahl Frames von der IDS Maschine interpretiert werden müssen.



Viele Angriffe können auch erst erkannt werden wenn eine Serie von Paketen zum Ziel gelangt sind. Um diese Attacken zu erkennen müssen diese Paket von der IDS Maschine zwischen gespeichert werden.



1.1.3 Network Node IDS (NNIDS)

Einige neue Systeme heben die Einschränkungen der NIDS auf. Diese Systeme arbeiten grundsätzlich auf die gleiche Weise wie NIDS, allerdings werden nur Pakete analysiert die für diese Node bestimmt sind. Man könnte diese Systeme auch als HIDS bezeichnen, wenn nicht NNIDS sich in erster Linie mit der TCP Analyse beschäftigen und nicht mit Log-Analyse ... Das bedeutet auch das aufgrund der geringeren Paketanzahl eine sehr viele bessere Performance erreichbar ist. Speziell für schnelle Netzsegmente oder VPN Implementierungen sind solche Systeme geeignet. Die Kombination von Agents auf den Servern und der Einsatz von NIDS in nicht belasteten Segmenten erzielen damit den besten Erfolg.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Welche Vor- und Nachteile bietet IDS?

Host-basierte IDS-Systeme

+ Erkennt eine Vielzahl lokaler Attacken.
+ Verschlüsselung stellt normalerweise kein Problem dar, wenn die Daten auf dem Server entschlüsselt werden.
+ Kein Problem mit geswitchten Netzwerken.
- Häufig muss jeder Host separat installiert und gewartet werden.
- Da sich das IDS auf dem Host be-findet, kann auch das IDS attackiert und lahmgelegt werden.
- Erkennt unter Umständen keinen weit gestreuten Netzwerk-Scan.
- Kann mit einer DoS-Attacke (Denial of Service) überschwemmt werden.
- Beansprucht Rechenleistung und Netzwerkressourcen des zu schüt-zenden Servers.

Netzwerk-basiert IDS-Systeme

+ Man kann ein recht grosses Netzwerk mit nur wenigen Rechnern beobachten.
+ Das System ist transparent, da das Gerät Traffic-Informationen sammelt.
+ Der gesamte Traffic zwischen der Konsole und dem NIDS-Collector kann verschlüsselt werden oder für vollständige Sicherheit über ein separates Netzwerk laufen.
- Es kann im System eine grosse Menge an Traffic geben, womöglich mehr, als das System verarbeiten kann. Dies erschwert das Entdecken von Eindringlingen, wenn die Aus-lastung hoch ist.
- Die Notwendigkeit, Datenpakete in kürzester Zeit zu verarbeiten, kann dazu führen, dass man einige Funktionen nicht nutzen kann, wenn das System mit der Menge an Traffic Schritt halten soll.
- Vollständig geswitchte Netzwerke können schwierig zu überwachen sein, da nicht wie bei nicht geswitchten Netzwerken der gesamte Traffic über alle Ports repliziert wird.
- Verschlüsselter Traffic kann nicht analysiert werden

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.1 Probleme beim Einsatz von IDS

Der Einsatz von IDS erfordert genaues Planen, z.B. welche Angriffsziele geschützt werden sollen. Signaturen für den Einsatz von NT müssen in einer UNIX Umgebung nicht aktiviert werden. Der Einsatz von Port Scannern oder anderen Tools gibt Auskunft darüber welche Systeme potentielle Ziele sind. Je nachdem wie diese Ergebnisse ausfallen und welche Bedrohungsszenarien erkannt werden wird sich auch die einzusetzende IDS SW/HW herausbilden. Speziell für NIDS/NNIDS gilt es das nicht nur eine Paket für Paket Analyse betrieben wird sondern auch eine Serie von Paketen beobachtet werden. Fragmentierte Pakete müssen erst wieder zusammengesetzt werden, bevor Sie Ihr wahres Erscheinungsbild zeigen. Das erfordert grosse und schnelle Puffer wie auch leistungsfähige Maschinen. Werden Load Balancer eingesetzt so muss gewährleistet sein, dass Pakete einer existenten Verbindung zu einer IDS Maschine geleitet werden um die Überprüfung der Aktionen zu gewährleisten. Noch extremer wird diese Anforderung im Bereich Gigabit, da es sich hier um eine rein geswitchte Architektur handelt. Der Einsatz von Wire-Taps führt nicht mehr zu dem gewünschten Erfolg, auch eventuelle SPAN-Ports sind überlastet, nur der Einsatz von Load Balancern, Switches mit integriertem IDS oder NNIDS führen da noch zum Erfolg.

Diese Anforderungen sollten so wenig wie möglich Fehlalarme (False Positiv) erzeugen. Denn viele Fehlalarme blenden vor der eigentlichen Gefahr und veranlassen den Administrator zu einer oberflächlichen Kontrolle.

2.2 Analyseverfahren

Bei den Analyseverfahren haben sich in den letzten Jahren drei Richtungen herauskristallisiert. Die älteste Methode, Einbrüche festzustellen, ist **Misuse Detection**. Bei diesem Verfahren wird ein Mustervergleich (Pattern Matching) vorgenommen. Die Daten der Event-Box werden mit Angriffsmustern (Attack Signatures) aus einer Datenbank verglichen. Ist dieser Vergleich positiv, dann wurde eine Verletzung der Security Policy erkannt, und es wird entsprechend reagiert. Im kommerziellen sowie im nichtkommerziellen Bereich ist Misuse Detection immer noch das am häufigsten benutzte Verfahren. Es ist einfach zu realisieren, anzuwenden und nicht sehr anfällig für falsche Alarme (False Positives). Der grosse Nachteil dieses Verfahrens ist, dass es nur bekannte Angriffe erkennt, was zur Folge hat, dass neue Angriffe, die sich noch nicht in der Signatur-Datenbank befinden, keinen Alarm auslösen (False Negatives) und somit unbemerkt bleiben.

Um dieses Defizit auszugleichen, wurde ein neuer Weg eingeschlagen und **Anomaly Detection** entwickelt. Anmaly Detection geht davon aus, dass alles, was nicht zur Menge des "normalen" Verhaltens gehört, also demnach "anormal" ist, ein Angriff sein muss. Diese Methode hat gegenüber Misuse Detection den Vorteil, dass sie es ermöglicht, neue Angriffe zu erkennen, da sie ein abnormles Verhalten darstellen. Zudem muss keine Datenbank mit Angriffsmustern aktualisiert und gepflegt werden. Aber auch hier tauchen wieder Schwierigkeiten auf, die die Verbreitung von Anomaly Detection im kommerziellen Bereich stark behindern. Verfahren zur Anomalieerkenung müssen zuerst das "normale" Verhalten eines Netzes

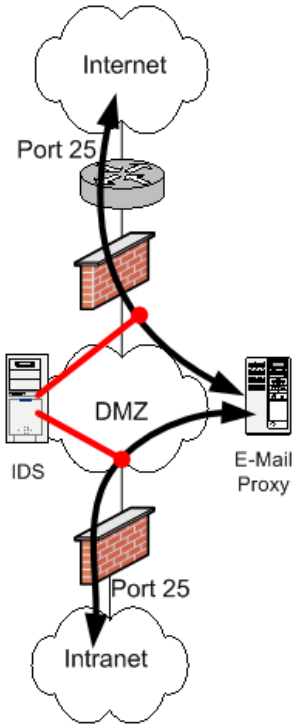
oder Computersystems erlernen, indem sie Profile für die Benutzer und das System anlegen. Diese Phase stellt an sich schon eine Hürde dar und könnte auch von einem Gegner ausgenutzt werden, um dem IDS Angriffe als normales Verhalten beizubringen. Das IDS könnte somit zukünftige Angriffe dieser Art nicht mehr erkennen. Ein weiteres Manko besteht in der hohen Rate an False Positives, die durch Störungen in der normalen Systemaktivität ausgelöst werden, aber keine Angriffe darstellen. Zusätzlich ist die Implementierung von Anomaly Detection gegenüber der Misuse Detection schwieriger, da die angewandten Verfahren oft komplexer sind.

Ein noch sehr junges Verfahren, das als **Buglar Alarm**, Passive Traps, oder Strict Anomaly Detection bezeichnet wird, benutzt einen relativ simplen aber dafür effektiven Ansatz. Es besagt, dass alles was nicht "gut" ist, "schlecht" sein muss. Diese Aussage erinnert an Anomaly Detection. Es wird aber Mustererkennung wie bei Misuse Detection für die Erkennung benutzt, d.h. das bekannte, normale Verhalten des Systems wird als Signatur in eine Datenbank abgelegt und jede Systemaktivität, die nicht einem der Muster aus der Datenbank entspricht, ist anormales Verhalten und signalisiert einen Angriff. Es müssen nur relativ wenige Muster in der Datenbank abgespeichert werden. Diese Muster müssen nicht wie bei Misuse Detection für jeden neuen Angriff aktualisiert werden, sondern nur bei Veränderungen des IT-Systems. Dadurch ergibt sich ein geringerer Verwaltungsaufwand im laufenden Betrieb als bei normalen Misuse Detection Systemen.

Damit das Ganze etwas klarer wird, ein kleines Beispiel:

2.2.1 Ein Beispiel

Der E-Mail-Proxy in einem DMZ-Netzsegment darf nur TCP-Pakete auf Port 25 empfangen und absenden. Des Weiteren dürfen diese Pakete nur an das Internet oder an das gesicherte/interne Netz geschickt werden. Das ist das normale Verhalten, welches als ein Muster in einer Datenbank abgelegt wird. Das IDS überprüft nun den Paketfluss des E-Mail-Proxies mit dem gespeicherten Muster. Sollte der E-Mail-Proxy diesem Verhalten einmal nicht folgen, so besteht die Wahrscheinlichkeit eines Angriffs. Die Muster müssen sich nicht auf abstrakte Netzverbindungen beziehen, sondern können auch tiefere Ebenen wie Headerinformationen der einzelnen Netzwerkschichten oder Systemaufrufe eines Betriebssystems widerspiegeln.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Damit die Fehlerquote bei der Erkennung von Angriffen vergleichbar gering bleibt, müssen Anomalien, wie sie immer mal wieder in Netzwerken auftreten, als Ausnahme explizit angegeben werden oder in einem Toleranzbereich fallen. Somit können False Positives zwar auftreten, sind aber weitaus seltener als bei Anomaly Detection, False Negatives sind nahezu ausgeschlossen. Wenn Angriffe unter der Toleranzgrenze bleiben, dann werden sie natürlich detektiert.

2.3 Nach welcher Art von Eindringlingen sollte man Ausschau halten?

Es gibt Tausende von Methoden, mit denen man sich unerlaubten Zugriff auf Computer verschaffen kann, und jeden Monat tauchen Dutzende neue auf: von Buffer Overflows und Directory Traversal Exploits bis zu Attacken vom Typ Denial of Service (DoS) und Distributed Denial of Service (DDoS).

Theoretisch sollten alle Systeme im Fall bekannter Sicherheitslücken gepatcht oder mit entsprechenden Workarounds versehen sein, so dass keine Notwendigkeit mehr für ein Signatur-basiertes IDS bestehen dürfte. Leider sieht die Wirklichkeit so aus, dass viele Systeme nicht oder nicht gleich gepatcht oder aktualisiert werden.
Tatsache ist, dass es sich bei den meisten Löchern um recht alte und gut bekannte Probleme handelt, für die Fixes längst verfügbar sind.

2.4 Reaktion auf Angriffe

Die meisten Systemkonsolen von IDS sind so konfiguriert, dass sie alle aufgezeichneten Daten in einer Datenbank speichern und eine E-Mail an den zuständigen Security Officer (SO) schicken, sobald ein Angriff festgestellt wird. Das Problem dabei ist, dass ein Angriff wie mit Nimda oder Code Red leicht dazu führen kann, dass ein Administrator mit E-Mails überschwemmt wird. Das Resultat ist ein System, das zu viele Informationen liefert, die nicht alle verarbeitet werden können. Eine praktikable Möglichkeit zur Vorbeugung besteht darin, die Schwelle für eine Benachrichtigung per E-Mail oder Pager möglichst hoch anzusetzen, aber auch die Konsole ein Alarmsignal von sich geben zu lassen, wenn sie ein Problem feststellt. Auf diese Weise hat der SO die auffälligen auffälligen Probleme im Blick, bemerkt aber auch ernste Schwierigkeiten, wenn das System immer mehr Alarmsignale aussendet.

Falls der SO nicht immer zur Stelle ist oder es Grund für erhöhte Alarmbereitschaft gibt, können einige IDS-Systeme so konfiguriert werden, dass sie automatisch auf Angriffe reagieren. Dies kann wie oben beschrieben eine einfache Benachrichtigung per E-Mail oder an einen Pager sein, aber auch aktivere Massnahmen umfassen, um einen akuten Angriff zu stoppen und so die Schwachstelle abzudichten.

Das direkte Eingreifen zur Unterbrechung der Kommunikation zwischen einem Angreifer und dem Opfer wird oft als Session Sniping oder Knockdown bezeichnet und erfolgt durch das Einfügen von Paketen, um die Verbindung zu unterbrechen, welche die Response ausgelöst hat. Die effektivste Methode, eine TCP-Verbindung abzubrechen, ist ein Reset der Verbindung mithilfe gefälschter

Pakete. Hierzu muss das IDS gefälschte Pakete an eines oder beide Systeme schicken, bei denen das TCP Reset-Bit gesetzt ist.

Andere Interventionsmethoden umfassen die Neukonfigurierung der Perimeter-Router und Firewalls, um die IP-Adresse des Angreifers zu blockieren, oder das Blockieren der Protokolle, die für den Angriff verwendet werden. In hartnäckigen Fällen kann es besser sein, jegliche Kommunikation zu dem angegriffenen System zu unterbrechen, anstatt es der Gefahr einer Beschädigung auszusetzen. Zu den weiteren Reaktionsmöglichkeiten zählt, aktiv Informationen über den Host oder die Website des Angreifers herauszufinden oder sogar eine Gegenattacke zu starten. Bevor man solche Funktionen aktiviert, sollte man aber auf jeden Fall juristischen Rat einholen.

3 Produkte

In den letzten Monaten sind zahlreiche Produkte auf dem Markt lanciert worden. Viele Unternehmen bieten ihre Lösungen in einer fix fertigen Box an. Der Benutzer braucht lediglich noch die Sonde anzuschliessen und die fertigen Einstellungen anzuwählen. Die optimale Konfiguration benötigt jedoch oft sehr viel mehr Zeit, als angegeben.

Die meisten uns bekannten Produkte setzen auf Snort auf. Aus diesem Grund wollen wir diese Freeware-Lösung etwas genauer unter die Lupe nehmen.

3.1 Snort

Snort arbeitet bei der Analyse der gesammelten Daten nach dem Prinzip der Muster Erkennung. Die zahlreichen Optionen von Snort erlauben Zugriff auf alle wichtigen Bestandteile der zu untersuchenden Pakete. Snort kann anhand der Quell- und Ziel-IP-Adressen, Quell- und Zielports, TCP-Flags, des Datenteils und noch diverser anderer Merkmale Pakete analysieren. Den Datenteil eines Paketes kann Snort anhand von Binärmustern in Form von Hexadecimal-Code analysieren oder mit Pattern-Matching auf Strings untersuchen.

Sollte man doch nach einer Möglichkeit der Anomalieerkennung suchen, bietet Snort über seine Plugin-Schnittstelle das Plugin Spade, welches von Silicon Defense entwickelt wird. Es bietet eine statistische Anomalieerkkennung, ist aber noch in seinem frühen Entwicklungsstadium. Nichtsdestotrotz bietet Spade schon eine beachtliche Stabilität und wird im praktischen Umfeld schon erfolgreich eingesetzt. Allerdings wird empfohlen, für den Einsatz von Spade einen gesonderten Snort-Prozess laufen zu lassen, der nur für den Zweck der Anomalieerkennung konfiguriert ist.

Im Allgemeinen bietet die Plugin-Schnittstelle von Snort die Möglichkeit, Pakete zu analysieren und gegebenenfalls zu verändern, noch bevor die eigentliche Analyse von Snort die Pakete untersucht.

Snort bietet diverse Möglichkeiten, auf einen erkannten Einbruch aufmerksam zu machen. Sie lassen sich entweder einzeln oder kombiniert nutzen. Die erste Möglichkeit, quasi der Klassiker, ist die Benachrichtigung über syslog. Soll Snort Alarmmeldungen in seinem eigenen Logfile protokollieren, so kann es dies auf zwei Arten tun, entweder schnell oder vollständig. Die erste Methode empfiehlt sich bei hohem Netzaufkommen, da hier nicht alle Paket Header gesichert werden. Daraus ergibt sich schon, was die zweite Methode tut, nämlich alle Meldungen samt

kompletten Paket Headern gesichert. Die letztere Methode ist allerdings dadurch auch erheblich langsamer, da hier ein nicht zu verachtender Aufwand für die Formatierung der entsprechenden Daten betrieben werden muss.

Nach einem erfolgten Angriff ist es elementar, die gesammelten Daten zu sichten, um sie für etwaige Massnahmen auszuwerten. Mit diversen Zusatzprogrammen ist es möglich, die Daten grafisch aufzuarbeiten. Hier stehen ACID und SnortSnarf an erster Stelle. ACID greift auf Daten zurück, die Snort in eine Datenbank loggt. Bis dato bietet Snort Unterstützung für Oracle, MySQL, PostgreSQL oder ODBC. ACID basiert auf PHP und bereitet die gesammelten Daten grafisch auf. SnortSnarf wurde von der Firma Silicon Defense entwickelt und besteht aus einer Reihe von Perl-Scripten. Prinzipiell bereitet es die Daten auch auf, aber trotzdem ist der Output teilweise noch sehr kryptisch. Hier hat ACID die Nase vorn.
Neben der grafischen Aufbereitung steht dem Administrator natürlich nichts im Weg, wenn er selbst Einblick in die Logdateien nehmen will. Snort sammelt seine Daten in einem Verzeichnis und diversen Unterverzeichnissen, die nach der IP-Adresse benannt werden, von der der Angriff ausging. Daten über Portscans werden in einer gesonderten Datei gesichert.

Snort bietet in beschränktem Masse Möglichkeiten der Intrusion Response. Über die libnet lässt sich die sogenannte Flexible Response nutzen. Somit kann man über die Rules von Snort Reaktionen auf Angriffe auslösen. Die Möglichkeiten erlauben eine explizite Beendigung der TCP-Verbindung über ein RST-Paket oder über ICMP. Bei letzterem besteht die Wahl zwischen ``Net unreachable", ein ``Host unreachable", ein ``Port unreachable" oder allen dreien auf einmal.

3.1.1 Die Konfiguration von Snort

Da Snort in erster Linie ein regelbasiertes IDS ist, benötigt es eine Art Wissensbasis, eine 'Datenbank' in der die so genannten Signaturen definiert sind. Als Signaturen werden in diesem Kontext die Charakteristika eines Pakets bezeichnet, die dieses Paket und seine Eigenschaften (z.B. Flags, Source- und Destination-Port und/oder -IP-Adresse) oder 'bösartig' definieren. Ohne eine solche Wissensbasis ist Snort quasi blind, es kann zwar die Pakete von der Netzwerkkarte dekodieren, weiss aber nicht welche dieser Pakete unerwünscht sind und welche nicht.

Weitere Informationen und Downloadmöglichkeit finden Sie unter: http://www.snort.org/

Weitere kostenlose Tools:
Hummer Project: http://www.csds.uidaho.edu/~hummer

SHADOW: http://www.nswc.navy.mil/ISSEC/CID/

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4 Wie werte ich die Informationen eines IDS aus?

Die Auswertung von IDS-Daten stellt sich zu Beginn als sehr schwer heraus. Grafische Tools wie ACID, welches sehr einfach zu Snort installiert werden kann, helfen Ihnen bei der Auswertung. Wir schauen uns ACID etwas genauer an.

Dieses Bild zeigt einen Virus, der aus der DMZ an eine IP-Adresse im Internet geschickt wurde.

	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
☐	#450-(2-71032)	Virus - Possible scr Worm	2003-09-23 10:47:26	192.168.1.11:110	212.223.134.114:56979	TCP
☐	#451-(2-71033)	Virus - Possible pif Worm	2003-09-23 10:47:50	192.168.1.11:110	212.223.134.114:56979	TCP

Das Detail zur ersten Meldung sieht wie folgt aus:

Meta

ID #	Time	Triggered Signature
2 - 71032	2003-09-23 10:47:26	Virus - Possible scr Worm

Sensor	name	interface	filter
	192.168.0.240	eth0	*none*

Alert Group	
	none

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
192.168.1.11	212.223.134.114	4	5	0	1500	15465	0	0	128	39853

FQDN	Source Name	Dest. Name
	mail.goout.ch	*Unable to resolve address*

Options	
	none

TCP

source port	dest port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	seq #	ack	offset	res	window	urp	chksum
110	56979				X	X				3867819748	1761562734	5	0	64173	0	16929

Options	
	none

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Weiter kann das TCP-Paket im Detail angeschaut werden:

```
 length = 1460

000 : 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65   Content-Type: te
010 : 78 74 2F 70 6C 61 69 6E 3B 20 63 68 61 72 73 65   xt/plain; charse
020 : 74 3D 75 73 2D 61 73 63 69 69 0D 0A 43 6F 6E 74   t=us-ascii..Cont
030 : 65 6E 74 2D 49 44 3A 20 3C 55 36 4F 69 78 70 37   ent-ID: <U6Oixp7
040 : 4A 35 64 33 35 4A 65 3E 0D 0A 0D 0A 5B 41 74 74   J5d35Je>....[Att
050 : 61 63 68 6D 65 6E 74 20 64 65 6E 69 65 64 20 62   achment denied b
060 : 79 20 67 6F 48 6F 73 74 69 6E 67 20 46 69 72 65   y goHosting Fire
070 : 77 61 6C 6C 20 53 4D 54 50 20 70 72 6F 78 79 20   wall SMTP proxy
080 : 28 74 79 70 65 20 22 61 70 70 6C 69 63 61 74 69   (type "applicati
090 : 6F 6E 2F 6F 63 74 65 74 2D 73 74 72 65 61 6D 22   on/octet-stream"
0a0 : 2C 20 66 69 6C 65 6E 61 6D 65 20 22 30 30 37 5B   , filename "007[
0b0 : 31 5D 2E 73 63 72 22 29 5D 0D 0A 2D 2D 55 4E 7A   1].scr")]..--UNz
0c0 : 6B 52 64 33 37 36 4A 7A 35 31 38 39 34 0D 0A 0D   kRd376Jz51894...
0d0 : 0A 2D 2D 55 4E 7A 6B 52 64 33 37 36 4A 7A 35 31   .--UNzkRd376Jz51
0e0 : 38 39 34 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70   894..Content-Typ
0f0 : 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6F   e: application/o
100 : 63 74 65 74 2D 73 74 72 65 61 6D 3B 0D 0A 09 6E   ctet-stream;...n
110 : 61 6D 65 3D 30 30 37 5B 31 5D 2E 68 74 6D 0D 0A   ame=007[1].htm..
120 : 43 6F 6E 74 65 6E 74 2D 54 72 61 6E 73 66 65 72   Content-Transfer
130 : 2D 45 6E 63 6F 64 69 6E 67 3A 20 62 61 73 65 36   -Encoding: base6
140 : 34 0D 0A 43 6F 6E 74 65 6E 74 2D 49 44 3A 20 3C   4..Content-ID: <
150 : 55 36 4F 69 78 70 37 4A 35 64 33 35 4A 65 3E 0D   U6Oixp7J5d35Je>.
160 : 0A 0D 0A 50 47 68 30 62 57 77 2B 43 67 6B 38 61   ...PGh0bWw+Cgk8a
170 : 47 56 68 5A 44 34 4B 43 51 6B 38 64 47 6C 30 62   GVhZD4KCQk8dGl0b
180 : 47 55 2B 49 46 64 46 51 69 35 45 52 53 42 4C 62   GU+IFdFQi5ERSBLb
190 : 47 56 70 62 6D 46 75 65 6D 56 70 5A 32 55 67 50   GVpbmFuemVpZ2UgP
1a0 : 43 39 30 61 58 52 73 5A 54 34 4B 0D 0A 43 51 6B   C90aXRsZT4K..CQk
1b0 : 38 62 47 6C 75 61 79 42 79 5A 57 77 39 49 6E 4E   8bGluayByZWw9InN
1c0 : 30 65 57 78 6C 63 32 68 6C 5A 58 51 69 49 47 68   0eWxlc2hlZXQiIGh
1d0 : 79 5A 57 59 39 49 69 38 76 61 57 31 6E 4C 6E 64   yZWY9Ii8vaW1nLnd
1e0 : 6C 59 69 35 6B 5A 53 39 6A 4C 32 74 68 4C 32 5A   lYi5kZS9jL2thL2Z
1f0 : 74 4C 33 4E 30 0D 0A 65 57 78 6C 4C 6D 4E 7A 63   tL3N0..eWxlLmNzc
200 : 79 49 2B 43 67 6B 4A 50 47 31 6C 64 47 45 67 61   yI+CgkJPG1ldGEga
210 : 48 52 30 63 43 31 6C 63 58 56 70 64 6A 30 69 5A   HR0cC1lcXVpdj0iZ
220 : 58 68 77 61 58 4A 6C 63 79 49 67 59 32 39 75 64   XhwaXJlcyIgY29ud
230 : 47 56 75 64 44 30 69 56 32 56 6B 4C 43 41 79 0D   GVudD0iV2VkLCAy.
```

Hier sieht man, dass der Virus (ein Attachement) durch die Firewall bereits gelöscht wurde und somit keine Gefahr mehr für das Netzwerk darstellt.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

5 Weitere Literatur

http://downloads.securityfocus.com/library/intrusion.pdf
Dieses englische Dokument zeigt Strategien und Möglichkeiten für IDS.

http://www.bsi.bund.de/literat/studien/ids/ids-stud.pdf
Dieses Dokument ist eines der besten frei erhältlichen Publikationen zum Thema IDS. Es werden sämtliche gängigen Ansätze und Technologien be-sprochen.

http://www.computec.ch/dokumente/intrusion_detection/ids/ids.txt
Dieses Dokument ist eines der besten frei erhältlichen Publikationen zum Thema IDS. Es werden sämtliche gängigen Ansätze und Technologien be-sprochen.

Weitere Informationen oder INFONEWS Dokumente finden Sie unter:
www.goSecurity.ch