


# Firewalls und Intrusion Detection Systeme



Grundlagen, Planung und  
Realisierungsvorschläge mit Open  
Source Komponenten

ias

Wilhelm Dolle, Head of Networking Division & IT-Security (Wilhelm.Dolle@brainMedia.de)  
[www.brainMedia.de/security](http://www.brainMedia.de/security)



- Allgemeines zur Sicherheit von IT-Systemen
  - Paketfilter und Proxys
    - Intrusion Detection
  - Zusätzliche Maßnahmen
    - Zusammenfassung

**Sicherheit ist ein kontinuierlicher Prozess**, der eine ständige Überwachung und Verfeinerung benötigt um sinnvoll zu funktionieren.

- Protection Phase
- Detection Phase
- Response Phase

- Erstellen von Sicherheitsrichtlinien
- Risikomanagement
  - Risikoanalysen
  - Vorgehen bei „Katastrophen“
- Zugriffskontrollen
- Betriebssystem und Applikationen härten
- Filtern von kritischen Inhalten
- Verschlüsselung
- Benutzerschulungen

- Netz- und Hostbasierte Intrusion Detection Systeme
- Auditing (Logfiles)
- Unter Berücksichtigung des Datenschutzes möglichst viele verwertbare Daten sammeln (z.B. als externe Datenquelle für Forensik)
- Detection kann wichtiger als Protection sein
- Qualitätskontrolle des Schutzsystems

- (Automatische?) Reaktion auf Vorfälle
- Analyse der Vorfälle (evtl. digitale Forensik)
- Bestimmen der verantwortlichen Schwachstellen
- Disaster Recovery
- Erkenntnisse in neue (verfeinerte) Mechanismen einfließen lassen
- Richtlinien anpassen



- Allgemeines zur Sicherheit von IT-Systemen
  - Paketfilter und Proxys
    - Intrusion Detection
  - Zusätzliche Maßnahmen
    - Zusammenfassung

# Definition einer Firewall

Firewalls und Intrusion Detection Systeme: Paketfilter und Proxys

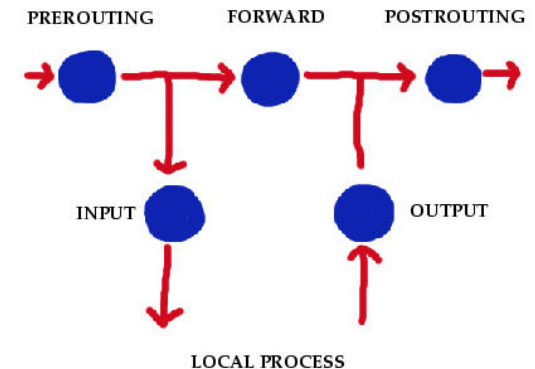
- organisatorisches und technisches Konzept zur Trennung von Netzbereichen, dessen korrekte Umsetzung und dauerhafte Pflege
- typische Umsetzung
  - je ein Paketfilter zwischen zwei Netzen
  - dazwischen liegt ein Zwischennetz (DMZ)
  - Paketfilter lassen nur Daten vom direkt angebundenen Netz in die DMZ und zurück durch
  - direkte Verbindung aus einem Netz zu dem Paketfilter des anderen Netzes oder gar ins andere Netz ist verboten



- Routing von Paketen zwischen Netzen
- Reine Paketfilter arbeiten auf den Schichten 3 (Network Layer) und 4 (Transport Layer) des OSI Modells
- Reine Paketfilter sehen keine Applikationsdaten
- Pakete weiterleiten, verwerfen, ablehnen, modifizieren oder loggen nach Kriterien wie IP Quell-/Zieladresse, Protokoll, TCP/UDP Quell-/Zielport, ICMP-Typ, Paketgröße/-validität, Fragmentierung, Zustand der Verbindung
  
- Beispiel: Iptables

- Userspace Tool zum Filtern von Paketen im Kernel
- ersetzt Ipchains
- benötigt Kernel mit Netfilter-Unterstützung
- Informationen unter [netfilter.samba.org](http://netfilter.samba.org)
  
- grosse Menge an neuem Code
- enthält evtl. noch kritische Fehler

- Paketfilter
- Connection tracking / stateful packet filtering
- Network address translation (NAT)
- Packet mangling
- einfache Bandbreitenbeschränkung
- Limitierungen
- erweitertes Logging möglich
- übersichtlicher Paketfluss



- REJECT: aktive Ablehnung einer Verbindungsanfrage durch ICMP Paket vom Inhalt "Admin hat's verboten" oder "Dienst nicht verfügbar,,
- DROP/DENY: kommentarloses Wegwerfen der Verbindungsanfrage (Timeout für Anfragenden)
- REJECT besser (z.B. schnellere Fehlersuche), DROP/DENY kostet nur Zeit (z.B. ident)
- kein „Verstecken“ des Rechners durch DROP/DENY sinnvoll

# Proxys (Application Level Gateways)

Firewalls und Intrusion Detection Systeme: Paketfilter und Proxys

- Proxys arbeiten auf den Schichten 5 bis 7 des OSI-Modells und können daher Applikationsdaten berücksichtigen
- erweiterte Filtermöglichkeiten im Vergleich zu einem reinen Paketfilter
- logische Trennung der Clients vom Netz (und damit von den Servern die angesprochen werden)
- Beispiele: TIS Firewall Toolkit, Squid, ...



- Allgemeines zur Sicherheit von IT-Systemen
  - Paketfilter und Proxys
    - **Intrusion Detection**
  - Zusätzliche Maßnahmen
    - Zusammenfassung

# Wozu benötigen wir Intrusion Detection?

Firewalls und Intrusion Detection Systeme: Intrusion Detection

- Intrusion detection is needed in today's computing environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in our computing systems. – SANS Institute ID FAQ

# Was ist ein Intrusion Detection System?

Firewalls und Intrusion Detection Systeme: Intrusion Detection

- erkennt (detects) Einbrüche (Intrusions)
- erkennt Veränderungen wichtiger Dateien
- erkennt die Installation von Hintertüren
- erkennt verbotene Aktionen im Logfile
- erkennt unerlaubten Netzwerkverkehr
  
- ermöglicht (automatische) Reaktionen



# Mögliche Fehler eines IDS

Firewalls und Intrusion Detection Systeme: Intrusion Detection

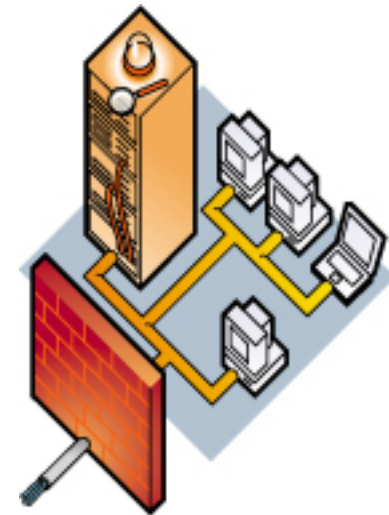
- Falsch positiv (eine erlaubte Aktion wird als Angriff identifiziert)
- Falsch negativ (ein Angriff wird vom IDS nicht erkannt oder als unbedenklich klassifiziert)
- Subversionsfehler (sehr komplexe Fehler; der Angreifer kann das IDS unterminieren)

### Hostbasierte IDS überwachen nur einen einzigen Rechner

- beobachtet systemrelevante Dateien und Befehle
- meldet ungewöhnliche Dateien und Administrationsvorgänge
- beobachtet offene Ports und Netzwerkverbindungen

### Netzbasierte IDS sammeln Informationen aus einem ganzen Netzsegment

- untersucht und protokolliert (bei Bedarf) sämtliche Netzwerkpakete
- erkennt mögliche Angriffe an „Fingerabdrücken“
- unterzieht die protokollierten Daten statistischen Analysen (Anomalieerkennung)



### Ursprungszustand ermitteln:

- `/usr/bin/find / -type f -perm +6000 -exec /bin/lS -ail { } \; > setuidgid.original`
- `/bin/lS -ailR /etc > etc.original`

### Überprüfung:

- `/usr/bin/find / -type f -perm +6000 -exec /bin/lS -ail { } \; | diff setuidgid.original -`
- `/bin/lS -ailR /etc | diff etc.original -`

- Scan: extensives nachforschen welche Dienste ein Rechner oder eine Rechnergruppe anbietet
- Portscan fragt höflich und formgerecht alle möglichen Dienste (65535 statusbehaftete (TCP) und noch mal so viele statuslose (UDP)) Quellen auf Basis von IP ab
- praktisch ungefährlich (keine unnötigen Dienste)
- Portscan ist nicht notwendigerweise eine Angriffsvorbereitung (schon gar kein Angriff)
- sogar Bannerscans (Serversoftware und Versionsnummer abfragen) sind legal
- trotzdem loggen?

- PortSentry  
([www.psionic.com/abacus/port Sentry/](http://www.psionic.com/abacus/port Sentry/))  
entdeckt Portscans und kann in Echtzeit darauf reagieren
- Unterstützt TCP und UDP
- Unter Linux werden auch Stealth Scans, wie zum Beispiel SYN/half-open, FIN, NULL, X-MAS und oddball entdeckt

- Tripwire ([www.tripwire.org](http://www.tripwire.org), seit Oktober 2000 unter GNU GPL) testet die Integrität von Dateien und erkennt Manipulationen am Filesystem.
- Sowohl die Regeln, als auch die Datenbank werden kryptographisch verschlüsselt um Manipulationen zu verhindern.

- Übersicht über den Normalzustand im Netzwerk bekommen
  - ntop
  - Ethereal
  - arpwatch – Kontrolle der MAC-Adressen im Netzwerk



- Netzwerkmonitor (www.ntop.org)
  - Konsolenausgabe
  - eigener Webserver, Benutzerpasswörter, OpenSSL

**Global Traffic Statistics**

Local Domain Name	tecsle.it
Sampling Since	Fri May 19 09:14:22 2000 [1:26:36]
<b>Total</b>	188,547
Dropped by the kernel	0
Dropped by ntop	0
<b>Unicast</b>	61.0% 115,090
<b>Broadcast</b>	13.1% 24,665
<b>Multicast</b>	25.9% 48,792

**IP Protocol Distribution**

Protocol	Data Sent	Data Received
UDP	2.0 KB 100%	0.7 KB 100%

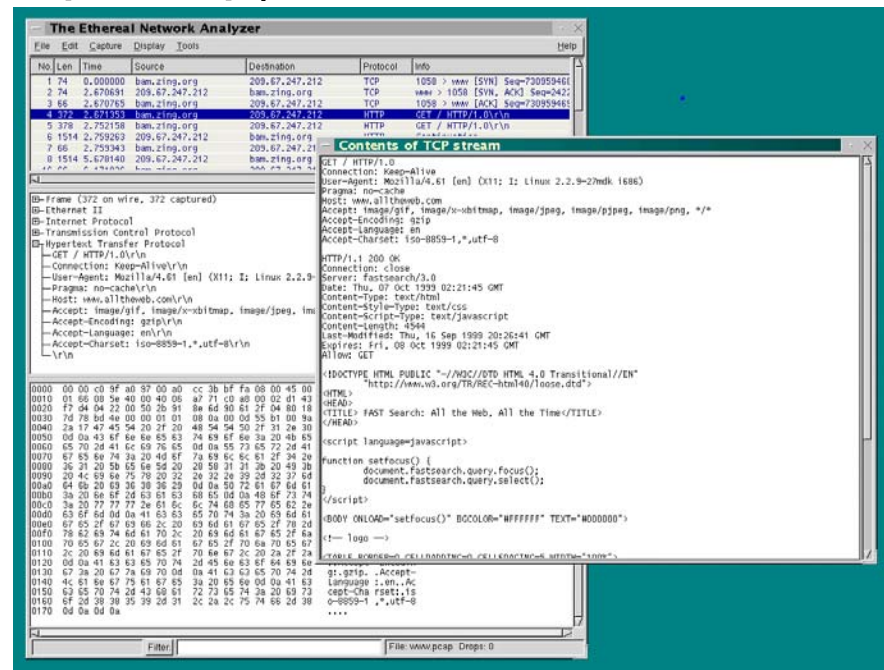
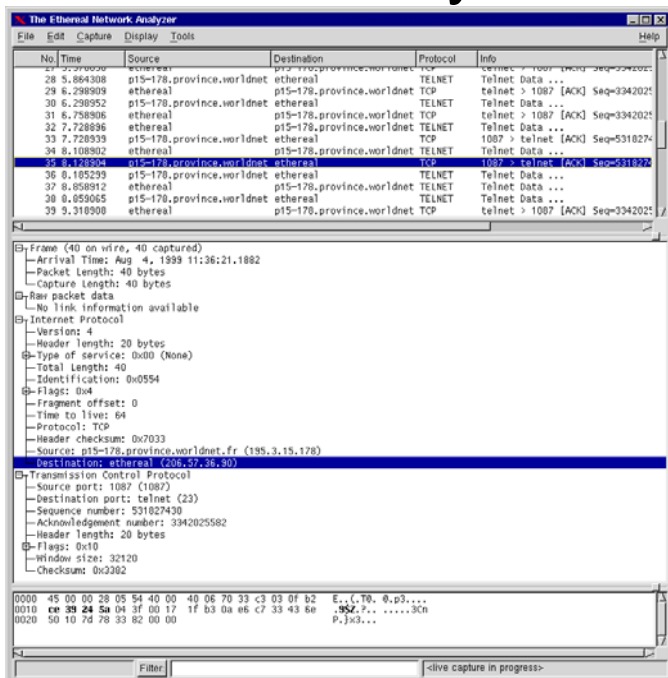
**Last Contacted Peers**

Receiver Name	Receiver Address	Sender Name	Sender Address
tar	193.43.104.13	tar	193.43.104.13

**IP Service/Port Usage**

IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
domain	53	16,077 Kb	tar	16,077 Kb	tar

- Network Protocol Analyzer ([www.ethereal.com](http://www.ethereal.com))
  - GUI
  - Capture Files von vielen anderen Tools analysieren (z.B. tcpdump)



# SNORT – Features (1)

Firewalls und Intrusion Detection Systeme: Intrusion Detection

- buffer overflows
- stealth port scans
- cgi-Angriffe
- SMB und NetBIOS Tests
- Portscanner (wie nmap)
- DDoS Clients

- TCP-Stream Reassemblierung
- IP-Defragmentierung (ab Version 1.7)
- SPADE (statistical packet anomaly detection engine – ab Version 1.7)
- HTTP Präprozessor erkennt UNICODE
- Sicherheitsfeatures (chroot, User snort/snort)
  
- Flexible Response (SNORT kann direkt Gegenmaßnahmen einleiten)

- gewünschte Regeln aktivieren (lieber mehr als weniger)
- nach und nach Regeln die falsch positive Ergebnisse liefern entfernen
- aktuelle Regeln/Signaturen z. B. aus der ArachNIDS Datenbank auf [www.whitehats.com](http://www.whitehats.com) (geht auch automatisch)

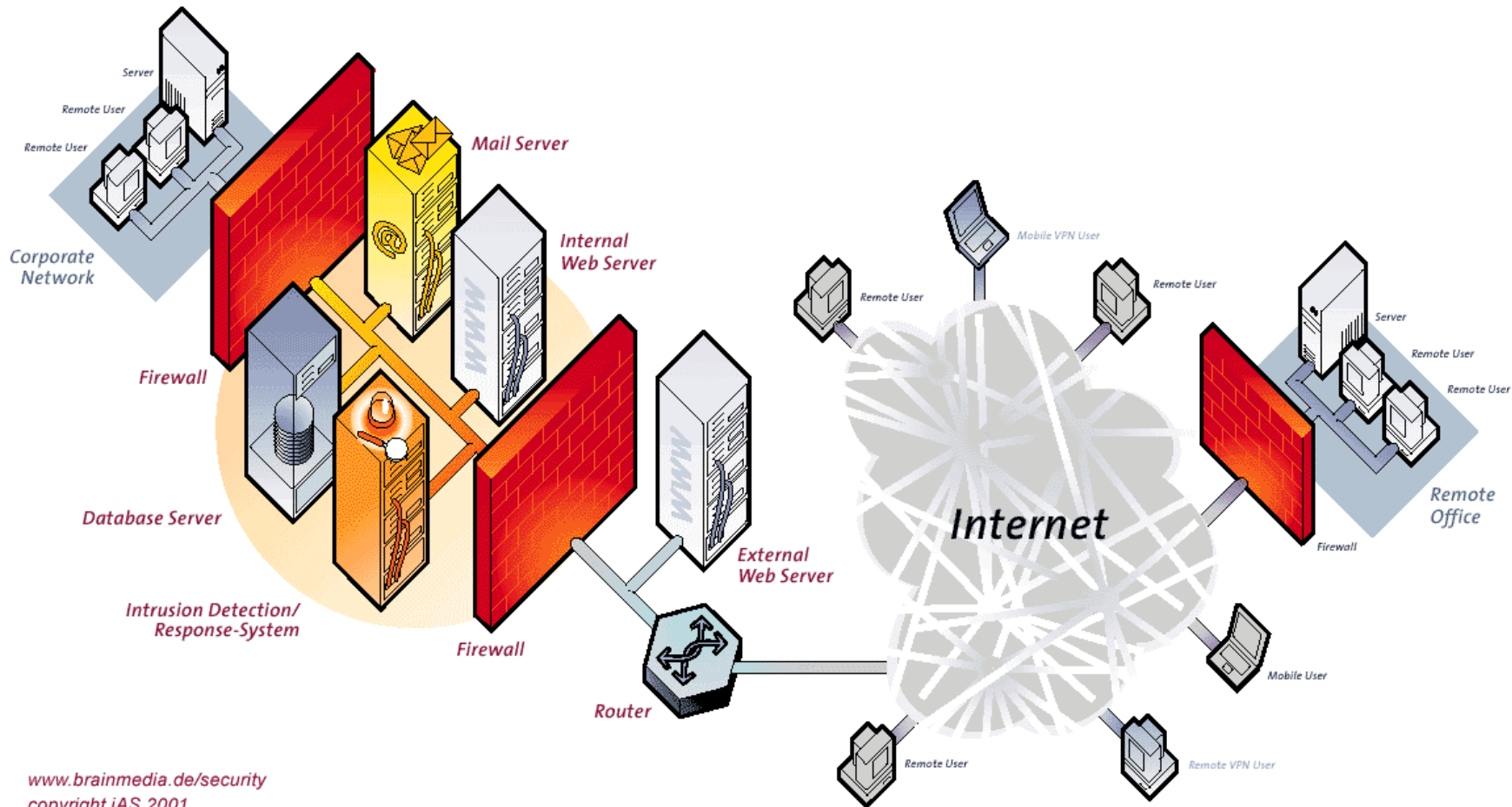
- Netzwerkverkehr wird anhand von Regeln nach bekannten Signaturen untersucht

```
alert TCP $EXTERNAL 80 -> $INTERNAL  
any (msg: "IDS215/client-netscape47-  
overflow-retrieved"; content: "|33 C9 B1 10  
3F E9 06 51 3C FA 47 33 C0 50 F7 D0 50|";  
flags: AP;)
```

- Sensor muss zu überwachenden Verkehr „sehen“ können
- Weitere aktive Snort-Prozesse (Sensoren nach Bedarf)
- „Vor“ einem Paketfilter (Angriffserkennung)
- „Hinter“ einem Paketfilter (Einbruchserkennung, sehr hohe Empfindlichkeit)

# Sinnvolles Plazieren der Sensoren

## Firewalls und Intrusion Detection Systeme: Intrusion Detection



[www.brainmedia.de/security](http://www.brainmedia.de/security)  
copyright iAS 2001



- Auswertung von „rohen“ Daten ist recht mühsam
- Loggen in lokale Dateien skaliert nicht
- Oracle, MySQL, PostgreSQL, ODBC
- Zentrale Datenbank (evtl. zusätzlich zur lokalen Datenerfassung)

# SNORT – Arbeitserleichterungen (1)

## Firewalls und Intrusion Detection Systeme: Intrusion Detection

- Analysis Console for Intrusion Databases (ACID, [www.cert.org/kb/acid](http://www.cert.org/kb/acid))

The screenshot shows the ACID web interface in a Netscape browser window. The title is "Snort Analysis Console for Intrusion Databases". The time window is set to [2000-07-29 10:05:05] - [2000-08-05 14:09:40].

**# of Sensors:** 2  
**Unique Alerts:** 3  
**Total Number of Alerts:** 11962

- Source IP addresses: 480
- Dest. IP addresses: 26

**Traffic Profile by Protocol**

TCP (19%)
UDP (74%)
ICMP (7%)

**Search**

- Alert Listing
- Most recent 15 Alerts: any protocol, TCP, UDP, ICMP
- Graph Alert detection time

ACID v0.9.2 ( by Roman Daniliv as part of the AirCERT project )

The screenshot shows the "ACID Packet Display" interface in a Netscape browser window. The title is "ACID Packet Display". The URL is [http://127.0.0.1:8080/acid/acid\\_pkt\\_main.php?submit=%230-%28](http://127.0.0.1:8080/acid/acid_pkt_main.php?submit=%230-%28).

**Meta**

ID #	1 - 11594
Time	2000-08-05 13:23:57
Signature	TCP

**IP**

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
128.2.66.93	205.164.217.39	4	5	0	710	3016	0	0	64	49982

**Options** none

**TCP**

source port	dest port	R	U	R	A	P	S	F	seq #	ack	offset	res	window	urp	chksum
1	0	R	G	C	K	S	H	T							
1120	80			X	X				700156471	579464	255	0	32120	0	27266

**Options** none

length = 1340

```
000 : 47 45 54 20 2F 20 48 54 50 2F 31 2E 30 0D 0A GET / HTTP/1.0..
020 : 48 6F 73 74 3A 20 77 77 72 2E 73 6E 6F 72 74 2E Host: www.snort.
040 : 6F 72 67 0D 0A 41 63 63 65 70 74 3A 20 74 65 78 t/html; text/pla
060 : 74 2F 68 74 6D 6C 2C 20 74 65 78 74 2F 70 6C 61 in; audio/mod.i
080 : 69 6E 2C 20 61 75 64 69 6F 2F 6D 6F 64 2C 20 69 mage/*; video/*;
0a0 : 6D 61 67 65 2F 2A 2C 20 76 69 64 65 6F 2F 2A 2C .video/mpeg; ap
0c0 : 20 76 69 64 65 6F 2F 6D 70 65 67 2C 20 61 70 70
```

Go to the next page in History list

# SNORT – Arbeitserleichterungen (2)

Firewalls und Intrusion Detection Systeme: Intrusion Detection

- SNORT Report (www.circuitsmaximus.com)

**SNORT REPORT**

Timeframe: 2001-06-13 20:07:11 to 2001-06-20 20:07:11  
Current Time: 2001-06-20 20:28:25  
Unique Signatures: 6  
Number of Alerts: 729

Earliest Alert: 2001-06-13 20:25:54  
Latest Alert: 2001-06-20 19:33:26

Types of Traffic

TCP	98%
UDP	6%
ICMP	
Portscan	

Timeframe:  GO

Num	Signature	# Alerts	# Sources	# Dest.	Detail
0	Portscans	714	11	N/A	Summary
1	MISC Large ICMP Packet	7	5	1	Summary
2	ICMP Source Quench	3	1	1	Summary
3	spp_http_decode: IIS Unicode attack detected	2	1	1	Summary
4	MISC source port 53 to <1024	1	1	1	Summary
5	BACKDOOR DeepThroat 3.1 Client Sending Data to Server on Network	1	1	1	Summary
6	ICMP superscan echo from windows	1	1	1	Summary

Page begun: June 20, 2001, 20:28:24  
Page finished: June 20, 2001, 20:28:25

IP Address: ( ) .com)

Whois lookup: ARIN RIPE APNIC Geektools  
DNS lookup: TRIUMF Princeton

Earliest Alert from This IP: 2001-06-18 23:59:30  
Latest Alert from This IP: 2001-06-19 00:00:02

Signatures with ( ) as a Destination

Signatures with ( ) as a Source

CID:9457 [**] spp_http_decode: IIS Unicode attack detected [**] 2001-06-18 23:59:30 :1079 -> :80 TCP TTL:64 TOS:0x0 ID:4010 IPLen: DgmLen:94 HLen:5 CSumIP:0x9E43 ***AP*** Seq:0x83093040 Ack:0x1B086132 Win:0x7D78 CSumTCP:0x54FF	Payload (Hex): 4745 5420 2F73 6372 6970 7473 2F2E 2E25 6330 2561 662E 2E2F 7769 6E6E 742F 7379 7374 656D 3332 2F63 6D64 2E65 7865 3F2F 632B 6469 720A	Payload (ASCII): GET /scripts/..%0%a f../winnt/system32/c md.exe/?c+dir.
CID:9460 [**] spp_http_decode: IIS Unicode attack detected [**] 2001-06-19 00:00:02 :1081 -> :80 TCP TTL:64 TOS:0x0 ID:4029 IPLen: DgmLen:96 HLen:5 CSumIP:0x9E2E ***AP*** Seq:0x84596502 Ack:0x1B08DF4F Win:0x7D78 CSumTCP:0x44A0	Payload (Hex): 4745 5420 2F73 6372 6970 7473 2F2E 2E25 6330 2561 662E 2E2F 7769 6E6E 742F 7379 7374 656D 3332 2F63 6D64 2E65 7865 3F2F 632B 6469 722B 5C0A	Payload (ASCII): GET /scripts/..%0%a f../winnt/system32/c md.exe/?c+dir+).

Page begun: June 20, 2001, 20:33:40  
Page finished: June 20, 2001, 20:33:41



- Allgemeines zur Sicherheit von IT-Systemen
  - Paketfilter und Proxys
    - Intrusion Detection
  - **Zusätzliche Maßnahmen**
    - Zusammenfassung

- monolithischer Linux-Kernel (kernelbased Root-Kits) – trotzdem Zugriff auf /proc/kmem
- Linux-Kernelpatch LIDS ([www.lids.org](http://www.lids.org))
- keine unnötigen Dienste installieren/anbieten
- Buffer-Overflows / Format-String
  - Nicht ausführbare Speichersegmente: OpenWall (Linux), PaX (Linux), Solaris ab 2.6
  - Schutz vor Überschreiben von Zeigern: StackGuard, FormatGuard (beides Patches für den gcc), StackShield, Libsafe, Libverify



- Allgemeines zur Sicherheit von IT-Systemen
  - Paketfilter und Proxys
    - Intrusion Detection
  - Zusätzliche Maßnahmen
    - **Zusammenfassung**

- Sicherheit ist ein kontinuierlicher Prozess („Security is a process, not a product.“ – Bruce Schneier)
- Ein Sicherheitssystem sollte die folgenden Abwehrreihen bereitstellen:
  - Paketfilter und Proxys
  - Hostbasierte IDS
  - Netzbasierte IDS
  - Zusätzliche Maßnahmen