DHBW
Duale Hochschule
Baden-Württemberg
Stuttgart
Campus Horb

Datensicherheit

Sicherheitsmechanismen im Netzwerk

09.12.2011

Jonas Bartusch und Yassin Uddin

Gliederung

Grundprinzipien der Internet-Sicherheit

Angriffe

- Ziele
- Methoden

Sicherheitsmechanismen

- Firewalls
- Intrusion Detection System
- Honeypot

Gliederung

Grundprinzipien der Internet-Sicherheit

Angriffe

- **Ziele**
- **Methoden**

Sicherheitsmechanismen

- Firewalls
- Intrusion Detection System
- Honeypot

Grundprinzipien der Internet-Sicherheit

- Vertrauen: Beziehungen zwischen Rechnern, die autorisiert sind, sich miteinander verbinden
- Authentifizierung: Prozess den dieser Rechner verwendet, um sich gegenseitig zu identifizieren
- Vertrauen und Authentifizierung stehen im umgekehrten Verhältnis zueinander
- Rechner können durch Hostnamen oder IP-Adresse authentifiziert werden. Solch ein Verfahren wird durch RHOSTS Einträge realisiert

Ziele

Angriffe

Unberechtigter Zugang:

- Nutzung einer Netzwerkressource ohne entsprechende Legitimation

Methode:

- Spoofing
- …

Ziele

Diebstahl von Informationen

Angriffe

Methode:

- Sniffing
- Scanning
- …

Ziele

Angriffe

Nicht verfügbare Dienste:

- Benötigte Dienste durch Ausfälle nicht mehr verfügbar
- Heimtückische Datenpakete machen das Netzwerk Zeitweise unbrauchbar (durch systematische und gezielte Überlastung)
- Netzwerkzerfall in mehrere Teile durch Ausfall einer kritischen Netzwerkkomponente (z.B. Router)

Methode:

- DOS/DDOS
- Ping of death
- ..

Angriffe

Spoofing

- Fortgeschrittene Technik der Fälschung von Daten , durch Vortäuschung einer falschen Absenderadresse
- Oft mit der Absicht durch die gefälschte Absenderadresse authentifiziert zu werden
- Kann durch Abweisung der Pakete aus dem Internet verhindert werden

- Beispiele für mögliche Methoden:
  IP-Spoofing, ARP-Spoofing, DNS-Spoofing

Angriffe

ARP-Spoofing

ARP übernimmt Hardware-IP-Mapping.

Werkzug: Cain und Abel

http://www.oxid.it/cain.html

Ziel: Modifizierung des ARP-Cache

Angriffe

ARP-Spoofing

Funktion:

- Angreifer behält Hardware-Adresse bei, jedoch wird vorgegeben, dass Sie die IP eines Vertrauenswürdigen Hosts haben
- Diese Information wird an das Ziel und an den Cache gesendet

ARP-Spoofing

Angriffe

Nachteil:

- Kann durch statisches Adress-Mapping verhindert werden

Schutz:

- Statisches Adress-Mapping, ARPWatch (http://ftp.su.se/pub/security/tools/audit/arpwatch/arpwatch.tar.gz)

Angriffe

Sniffing

- Das heimliche Abfangen von Datagrammen, die über ein Netzwerk gesendet werden
- Legitimer Zweck, da für Administratoren wichtig

Funktion:

- LAN-Interface im Promiscous Mode

Sniffing

Angriffe

Schutz:

- Es gibt drei NetzwerkInterfaces, die ein Sniffer nicht überqueren kann: Switches, Router und Bridges
- Verschlüsselte Arbeitssitzungen

Tools: wireshark, Cain und Abel

Angriffe

Scanner

Scanner sind Programme, mit deren Hilfe ein Angreifer seinen Ziel-Host nach vermutlich fehlerhaften Diensten abtasten kann

Funktionsweise:

- Anfragen an TCP/IP-Ports
- Auswertung der Antworten
- Erhalt der Informationen über die Dienste

Scanner

Angriffe

Dienste:

- Unter welcher User-ID laufen diese Dienste?
- Werden anonyme Logins unterstützt?
- Wird eine Authentifizierung bei gewissen Netzwerkdiensten benötigt?

Angriffe

(D)DDOS

- (Distributed) Denial of Service, können vorübergehend das gesamte Netzwerk lahmlegen
- Destruktive Programme
- Schwachstellen im System(Rechner, Übertragungsprotokolle, ...) ausgenutzt oder begrenzte Systemressourcen aufgebraucht, um eine Dienstverweigerung zu erreichen..

Angriffe

(D)DDOS

- Notwendig um sicherheitsrelevante Systeme in einen instabilen Zustand zu versetzen(z.B. IDS, ...).
- Man unterscheidet zwei Arten Von DOS-Attacken.

Angriffe

Hostbasierte DOS-Attacke

Wenn der Angreifer bereits Zugang zum System besitzt, kann er mit meist sehr einfachen Mitteln das System handlungsunfähig machen. Dazu gehören beispielsweise

- **Plattenplatz aufbrauchen (Sicherheitsmaßnahme: quota)**
- **Arbeitsspeicher / CPU Reserven aufbrauchen (Sicherheitsmaßnahme: ulimit)**
- **Hardwarefehler ausnutzen (Sicherheitsmaßnahme: neuer Kernel)**

Netzwerkbasierte DOS-Attacke

Angriffe

Die Bedrohung ist größer als bei Hostbasierten DOS-Attacken.

Vorteil: Angreifer brauch nicht zwingend Zugang zum Netzwerk.

Angriffe

Netzwerkbasierte DOS-Attacke

Beispiele:

- Email-Bomben -» Netzwerk und Speicherressource
- Broadcast-Angriff
- Kernel-Angriff -» Netzwerkpufferüberlauf

Angriffe

Netzwerkbasierte DOS-Attacke

Beispiele:

- DOS-Angriffe auf TCP/IP-Ebene
  - IP-Fragmentangriff (teardrop, newtear, bonk)
  - IP-Bombing (meist als DDOS-Attacke)
  - SYN-Flood Attacken (massenhafte Verbindungsanfragen)

Gliederung

Grundprinzipien der Internet-Sicherheit

Angriffe

- Ziele
- Methoden

Sicherheitsmechanismen

- **Firewalls**
- **Intrusion Detection System**
- **Honeypot**

Sicherheitsmechanismen

Firewall

Konzept zur Trennung von Netzwerkbereichen, dessen korrekte Umsetzung sowie dauerhafte Pflege

Sicherheitsmechanismen

Firewall

Paketfilter

- versucht Sicherheitsrichtlinien bezüglich des Netzwerkverkehrs durchzusetzen
- Durch festgelegte Regeln können Datenpakete gefiltert, protokolliert, markiert und geändert.(Pakettyp nicht Inhalt)
- können Datenpakete auf einen Proxy umleiten
- Paketfilter arbeiten auf Schicht 3/4 des ISO/OSI Modells

Firewall

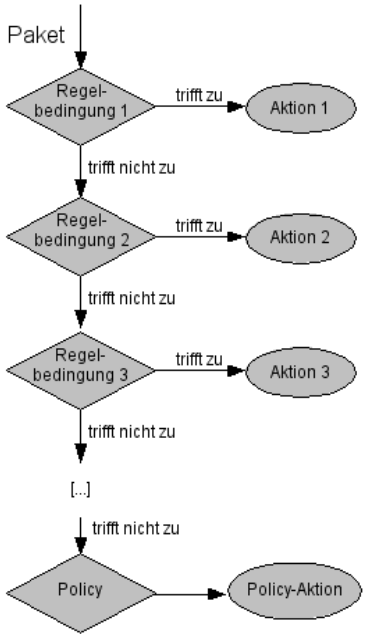
Proxy

- Application Level Gateway
- befindet sich zwischen Client und Server
- Proxys arbeiten auf Applikationsebene(schicht 5-7 des ISO/OSI Modells)

Sicherheitsmechanismen

Paketfilter (iptables)

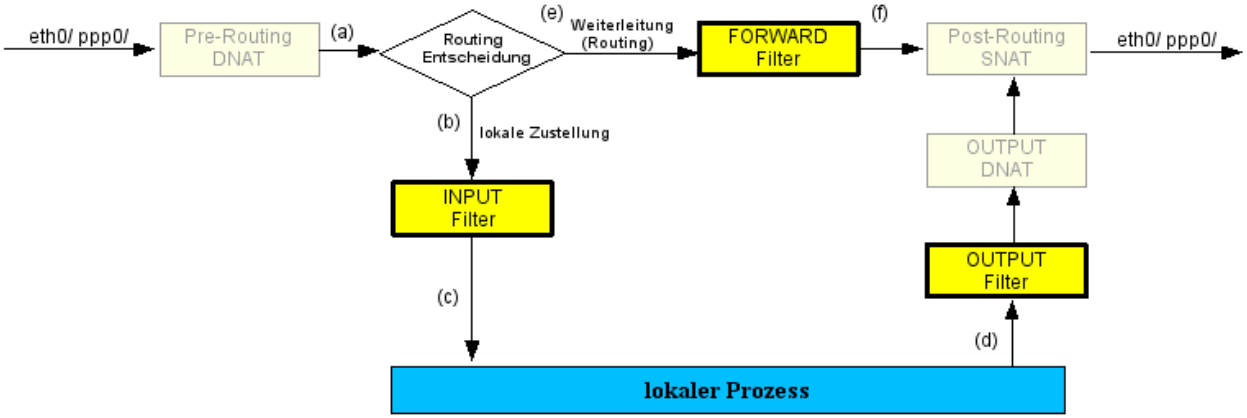
- iptables kommuniziert mit dem Linux Kernel, und weist diesen an, Pakete nach bestimmten Regeln zu filtern.
- automatisches Setzen von Regeln durch iptables-save und iptables-restore(init-skript)
- jede Kette ist eine Sammlung von Regeln
- WENN (Filteroption) DANN Aktion (lösche, Akzeptieren, ... des Paketes)
- Regeln werden solange nacheinander abgearbeitet, traf keine Regel zu so entscheidet die Policy der Kette(prohibitive Sicherheitspolitik) was geschieht



Sicherheitsmechanismen

Filtertabelle

- Standardmäßig gibt es drei Ketten Input, Output und Forward
- Input: Pakete mit Zieladresse des lokalen Rechners. Input-Kette kann Paket entweder verwerfen oder durchlassen.



Filtertabelle

- Output: Lokaler Prozess kann neues Paket erzeugen und diese ins Netzwerk versenden. Die Output-Kette prüft diese und leitet sie an die Netzwerkschnittstelle.
- Forward: Forward-Kette prüft Pakete die vom inneren ins äußere Netz und umgekehrt, übertragen werden sollen.
- lokaler Prozess: z.B. Mozilla

Sicherheitsmechanismen

NAT-Tabelle

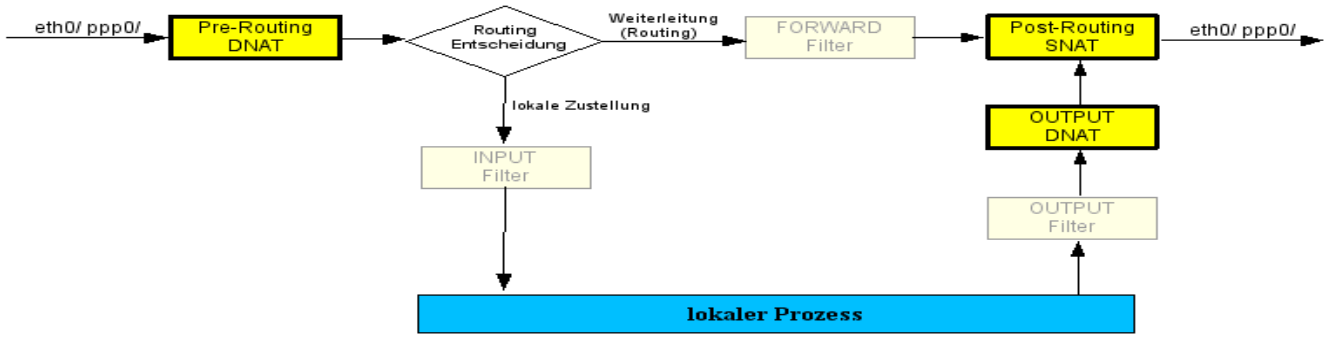
Network-Adress-Translation

In der NAT Tabelle werden die folgenden Ketten gespeichert:

PREROUTING-, POSTROUTING -, OUTPUT-Kette

Source-NAT(SNAT): es wird die Quelladresse eines Paketes manipuliert

Destination-NAT(DNAT): es wird die Zieladresse eines Paketes manipuliert



Mangle-Tabelle

Beispiele:

Schutz vor Portscannern:

```
root@linux # iptables -A FORWARD -p tcp --tcp-flags ALL
    NONE -m limit --limit 1/h -j ACCEPT
root@linux # iptables -A FORWARD -p tcp --tcp-flags ALL
    ALL -m limit --limit 1/h -j ACCEPT
```

Schutz vor "Ping of Death":

```
root@linux # iptables -A FORWARD -p icmp --icmp-type
    echo-request -m limit --limit 1/s -j ACCEPT
```

Mangle-Tabelle

Beispiele:

Pakete zu loggen:

```
root@linux # iptables -A FORWARD -m limit -j
   LOG
```

Sicherheitsmechanismen

Proxy

logische Trennung der Kommunikationspartner

unabhängige Verbindungen: Client-Proxy und Proxy-Server

Dadurch werden

- Authentifizierung und Autorisierung (benutzerabhängige Nutzung von Diensten)
- Zwischenspeicherung (Cache) von Daten
- Filterung von Dateninhalten (Virenscanner, Kindersicherung)
- Löschen der Datenherkunft (Anlegen von personenbezogenen Profildaten unterbinden)

ermöglicht.

Proxy

Als repräsentative Vertreter seien an dieser Stelle

- SOCKS (Dante) als generischer Proxy
- squid und wwwoffle als HTTP-Proxies,
- Exim und pop3gwd als Email-Proxies.
- bnc und tircproxy als IRC-Proxies

genannt.

Sicherheitsmechanismen

Intrusion Detection System (IDS)

- System zur Erkennung von Angriffen gegen ein Computersystem oder Netzwerk
- Firewallergänzung oder direkte Überwachung eines Computers
- Architekturen: Host-Basierte IDS, Netzwerk-Basierte IDS und Hybride IDS
- Honeypot kann Bestandteil eines IDS sein
- Ein IDS wird durch ein IPS (Intrusion Prevention System) um zusätzliche Funktionen, wie z.B. das Verwerfen von Daten ergänzt

Intrusion Detection System (IDS)

Host Basierte IDS:

- Älteste Art
- Auf jedem zu überwachendem System zu installieren
- Anhand von Prüfsummen werden Veränderungen am System überprüft

Intrusion Detection System (IDS)

Host Basierte IDS:

Vorteile:

- Sehr spezifische Aussage über Angriff
- Umfassende Systemüberwachung

Nachteile:

- Aushebelung durch DOS-Angriffe
- Wenn das System außer Gefecht ist, ist auch das IDS außer Gefecht

Sicherheitsmechanismen

Intrusion Detection System (IDS)

Netzwerk-Basierte IDS:

- Versucht alle Netzwerkpakete aufzuzeichnen, zu analysieren und verdächtige Aktivitäten zu melden
- Versucht Angriffsmuster aus Netzwerkverkehr zu erkennen
- Ein Sensor zur Überwachung eines ganzen Netzsegments
- 1 Gbit LAN kann Bandbreite des Sensors Übersteigen → Keine lückenlose Überwachung

Intrusion Detection System (IDS)

Netzwerk-Basierte IDS:

Vorteile:

- Sensor kann ganzes Netzwerk überwachen
- Sensorfunktion durch Ausschalten eines Zielsystems nicht gefährdet

Nachteile:

- Keine lückenlose Überwachung bei Bandbreitenüberlastung
- Keine lückenlose Überwachung in geswitchten Netzwerken

Intrusion Detection System (IDS)

Hybride IDS:

- Mischung aus beiden Prinzipien
- Komponenten: Management, Hostbasierte Sensoren, Netzbasierte Sensoren

Intrusion Detection System (IDS)

Hybride IDS:

Funktionsweise:

- Vergleich mit bekannten Angriffssignaturen (Nur bekannte Angriffe werden erkannt)
- Wahrnehmung durch Sensoren die Logdateien oder Netzwerkverkehrsdaten sammeln, vergleichen und ein Alarm auslösen

Intrusion Detection System (IDS)

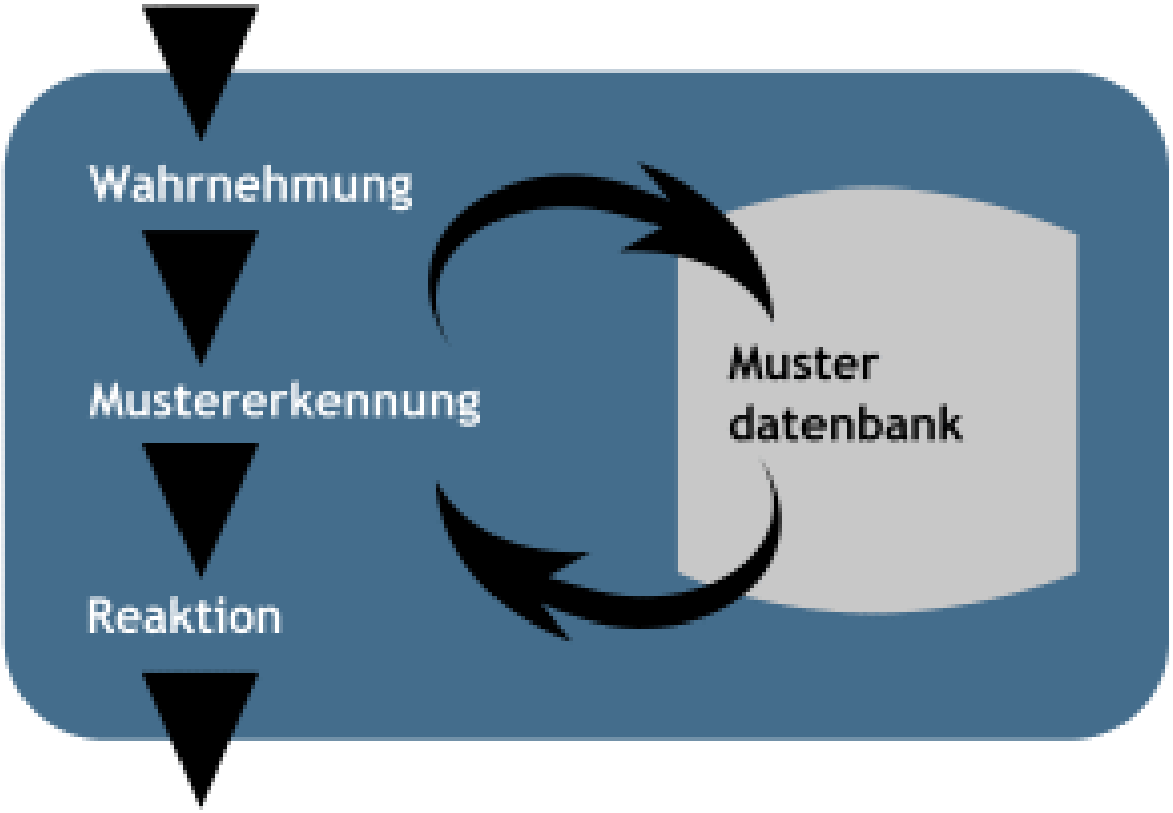
Hybride IDS:

Funktionsweise:

- Benachrichtigung durch e-mail oder sms an Administrator . Je nach Umfang auch Sperrung/Isolierungdes Eindringlings
- Heuristische Methode um bisher unbekannte Angriffe zu erkennen (Dynamische IDS nicht so weit verbreitet wie statische)
- Ziel: Ähnliche Angriffe zu erkennen

Sicherheitsmechanismen

Intrusion Detection System (IDS)



Intrusion Detection System (IDS)

Hybride IDS:

Problem:

- Viele falsche Warnungen oder Angriffe die nicht erkannt werden
- IDS kann als Angriffsziel genutzt werden

Produkte: Snort, Samhain, Prelude, Projekt Hogwash, Xray IDS

Honeypot

Definition:

Ein Honeypot ist ein Rechner innerhalb eines Systems der absichtlich Sicherheitslücken autweist.

Honeypot

Vorteile:

- Angreifer sollen sich auf diesen unwichtigen Teil des Netzwerks konzentrieren und somit die restlichen Rechner des Netzwerks vernachlässigen
- Ziele und Angriffsweisen des Angreifers sollen analysiert werden

Honeypot

Nachteile:

- Der Honeypot kann als Einstiegspunkt in das Netzwerk missbraucht werden

Sicherheitsmechanismen

Honeypot

Klassifizierungen

Production Honeypots (PH)

- Ausschließlich erkennen von Angriffen
- Dient als Frühwarnssytem oder Ablenkung
- Keine Schwachstellen sondern Dienstsimulation
- Alarm nach Verbindungsversuch --» Absicherung der anderen Systeme

Sicherheitsmechanismen

Honeypot

Klassifizierungen

Research Honeypots (RH)

- viel komplexer als PHs
- Analyse von Angriffstaktiken oder -trends
- Feststellen von Angriffswerkzeugen
- Filtern welche Dienste besonders beliebt sind
- Jede Kommunikation wird mit kommentiert --» Verbesserung der eigenen Firewall/IDS-Regeln (in großen Unternehmen)

Sicherheitsmechanismen

Honeypot

Typen

Low Interaction Honeypots:

- Emuliert lediglich einen Dienst
- Sehr leicht zu enttarnen
- Erfassen von automatisierten Attacken
- Bsp.: Login wird angeboten und schlägt bei allen Zugriffsversuchen mit einer Fehlermeldung fehl

Beispiele: honeyd, mwcollet, nepenthes, honeytrap, multipot

Honeypot

Typen

Medium Interaction Honeypots:

- Bekannte oder beliebige Schwachstellen werden emuliert
- Schwieriger zu enttarnen
- Konfiguration um einiges komplexer

Honeypot

Typen

High Interaction Honeypots:

- Extrem schwer zu enttarnen
- Keine Dienstemulation
- Durch Firewall von restlichem System getrennt
- Protokolldateien werden auf externem Server gesichert

Honeynets

- Simulierte Vernetzung mehrerer Honeypots
- Dient beispielsweise zur Analyse von Viren und deren Eigenschaften sich in einem Netzwerk zu verbreiten
- Oft angewandt von Antivirus Software Herstellern

Literatur

- Internet Firewalls & netzwerksicherheit - Karanjit Siyan, Chris Hare
- hacker's guide - anonymous -
- Linux Firewalls - Robert L- Ziegler

Danke für die Aufmerksamkeit