# Datensicherheit

## Sicherheitsmechanismen im Netzwerk

Jonas Bartusch
Duale Hochschule Baden-Württemberg
Stuttgart Campus Horb
72160 Horb am Neckar, Deutschland

Yassin Uddin
Duale Hochschule Baden-Württemberg
Stuttgart Campus Horb
72160 Horb am Neckar, Deutschland

*Abstract*—Die steigende Internet-Euphorie der letzten Jahre lässt oft vergessen, dass jeder Rechner, der an ein offenes Netzwerk wie das Internet angebunden ist, per se einen Angriffspunkt für Hacker und Cracker darstellt. Dieser Artikel entstand als Seminararbeit der Dualen-Hochschule Stuttgart Campus Horb des Studiengangs AI2009 und soll Heimanwendern und Administratoren aufzeigen, welchen Risiken Rechner und Daten im Netz ausgesetzt sind und wie man diese vor potentiellen Angriffen schützt.

***Keywords-Netzwerk; Sicherheitsmechanismen; Angriff***

## I. EINLEITUNG

Dieser Artikel ist in zwei Abschnitte unterteilt. Der erste Abschnitt befasst sich mit Angriffsmöglichkeiten und den Zielen die dahinter stecken. Desweiteren wird im zweiten Teil erläutert welche Sicherheitsmechanismen das System schützen und auf die Vor- und Nachteile eingegangen.

## II. ANGRIFFE

Im Nachfolgenden Abschnitt, wird zunächst auf die Ziele eines Angreifers eingegangen. Desweiteren werden Methoden genannt und erläutert, mit denen er diese Ziele erreichen kann.

### *A. Angriffsziele*

- Eines der Ziele ist der unberechtigte Zugang im Netzwerk. Es wird drauf abgezielt, Netzwerkressourcen zu nutzen ohne die entsprechende Legitimation zu besitzen. Eine Möglichkeit diesem Ziel nach zu kommen ist beispielsweise Spoofing.
- Der Diebstahl von Informationen ist ein weiteres Angriffsziel. Mögliche Informationen, die ein Angreifer abfangen möchte sind: Nutzerdaten, die Kommunikation zwischen Nutzern des Netzwerks, oder gar komplette Dateien. Eine Technik hierfür ist z.B. Sniffing.
- Außerdem kann es der Angreifer darauf abgesehen haben, benötigte Dienste innerhalb des Netzwerks zeitweise unbrauchbar zu machen. Dies erreicht er meist durch systematische und gezielte Überlastung. Wenn es zum Ausfall einer kritischen Netzwerkkomponente, wie Beispielsweise einem Router kommt, kann dies dazu führen, dass das Netzwerk in mehrere Teile zerfällt. Um dieses Ziel zu erreichen eignen sich DOS und DDOS-Attacken.

### *B. Angriffsmöglichkeiten*

#### *1) Spoofing*

Spoofing ist eine Technik der Fälschung von Daten in einem Netzwerk durch Vortäuschung einer falschen Absenderadresse, meist mit dem Hintergrund, durch die gefälschte Absenderadresse authentifiziert zu werden. Zum Vorteil des Angreifers hinterlässt ein Spoofing Angriff relativ wenig Spuren. In diesem Artikel sollen zwei Arten des Spoofings näher erläutert werden.

##### *a) ARP-Spoofing*

ARP-Spoofing ist eine Technik, die den ARP-Cache ändert. Der ARP-Cache enthält Informationen über das MAC-IP-Mapping. ARP-Spoofing funktioniert wie folgt:
Der Angreifer behält seine MAC-Adresse bei, gibt jedoch vor, dass die IP-Adresse die eines vertrauenswürdigen Hosts ist. Diese Information werden gleichzeitig an das Ziel und den Cache gesendet. Ein Werkzeug welches ARP-Spoofing ermöglicht ist Cain und Abel.

##### *b) DNS-Spoofing*

Mittels DNS-Spoofing legt ein Angreifer den DNS-Server offen und ändert explizit die Tabellen zur Zuordnung von Hostnamen und IP-Adressen. Diese Änderungen werden in die Übersetzungstabellen-Datenbanken auf dem DNS-Server geschrieben. Wenn ein Client also eine Auflösung eines Hostnamens anfordert, erhält er eine gefälschte Adresse; welche die IP-Adresse eines Rechners ist, der sich komplett unter der Kontrolle des Angreifers befindet. Die Wahrscheinlichkeit für solch einen Angriff ist relativ gering, da diese Art von Angriff nicht leicht durchzuführen ist. Wenn ein Angreifer eine DNS-Spoofing Attacke erfolgreich durchführt, ist die Gefährdung des Opfer-Systems sehr groß, da der Angreifer sich so authentifizieren kann.

#### *2) Sniffing*

Sniffing ist die Fähigkeit heimlich Datenpakete abzufangen, die über ein Netzwerk gesendet werden. Neben freien Softwarelösungen gibt es auch Hardwarelösungen die sich zum sniffen eignen. Bei einem Sniffer wird die Netzwerkkarte in den “Promiscous Mode” geschalten um alle Datenpakete abzufangen. Der "Promiscous Mode", ist ein Empfangsmodus

für Netzwerkgeräte der den gesamten Netzwerkverkehr abfängt.
Zum Schutz vor Sniffing sollte man in seinem Netzwerk, drei Netzwerk-Interfaces, welche ein Sniffer nicht überqueren kann, einplanen. Solche Netzwerk-Interfaces sind Switches, Router und Bridges. Desweiteren wird empfohlen Arbeitssitzungen zu verschlüsseln.

*3) Scanner*

Ein Scanner ist ein Programm, mit dessen Hilfe ein Angreifer seinen Ziel-Host nach vermutlich fehlerhaften Diensten abtasten kann. Dies funktioniert indem der Angreifer, Anfragen an die TCP/IP-Ports des Hosts sendet und die Antwort auswertet. Bei der Auswertung erhält der Angreifer Informationen über die Dienste des Opfers. Solche Informationen sind beispielsweise die User-ID des Diensts, ob anonyme Logins unterstützt werden und ob eine Authentifizierung bei gewissen Netzwerkdiensten benötigt wird.

*4) Denial of Service (DOS)*

Denial of Service, sind Angriffe die nicht nur einzelne Hosts sondern ganze Netze lahmlegen können. Sie zählen zu den destruktiven Programmen. Die Funktionsweise von DOS Attacken ist simpel, da sie meist Schwachstellen im System(Rechner, Übertragungsprotokolle, …) ausnutzen oder etwa Systemressourcen aufbrauchen, um eine Dienstverweigerung zu erreichen. Jedoch werden DOS-Attacken häufig verwendet um den eigentlichen Angriff zu verschleiern oder sind etwa notwendig um sicherheitsrelevante Systeme(z.B. IDS, IPS, Honeypots, …) in einen instabilen Zustand zu versetzen. Es werden zwei Typen von DOS-Attacken unterschieden.

*a) Hostbasierte DOS-Attacke*

Hat der Angreifer bereits Zugang zum System, so kann er dieses meist mit einfachen Mitteln handlungsunfähig machen. Ein solches Ziel kann erreicht werden, indem Plattenplatz, Arbeitsspeicher und Rechenleistung aufgebraucht oder Hardwarefehler ausgenutzt werden.
Sicherheitsmaßnahmen gegen Hostbasierte DOS-Attacken bieten beispielsweise die Programme "quota" und "ulimit".

*b) Netzwerkbasierte DOS-Attacke*

Die Bedrohung durch Netzwerkbasierte DOS-Attacken ist größer als bei den Hostbasierten. Dies liegt daran, dass der Angreifer keinen Zugang in das System braucht. Es gibt folgende Möglichkeiten einen DOS-Angriff auf Netzwerkebene durchzuführen.

- Broadcast

Ein Angreifer generiert pro Sekunde 100 Broadcast-Anfragen. Wenn angenommen 150 Rechner im Subnetz aktiv sind und deshalb antworten, müssen 15.000 Antwortpakete übertragen werden. Der Rechner, der diese Anfrage gestellt hat, ist mit den Antworten hoffnungslos überlastet und verliert im Extremfall seine Netzverbindung. Gegenmaßnahmen können beispielsweise durch die Limit Option im Paketfilter oder durch das Herausfiltern von ICMP Paketen realisiert werden.

- Kernel-Angriff

Auch die Netzwerkmodule des Kernels sind nicht vor Angriffen sicher. So kann beispielsweise durch eine SYN-Flood-Attacke der Netzwerkpuffer zum Überlaufen gebracht werden. Kernelparameter bieten einen guten, meist ausreichenden Schutz.

- DOS-Angriffe auf TCP/IP-Ebene

Durch Massenanfragen werden Schwachstellen im IP-Stack ausgenutzt. Die Schwachstellen lassen sich nur bedingt beseitigen, sodass solche Angriffe meist als DDOS Attacken durchgeführt werden. Zu diesem Angriffstyp zählen:
IP-Fragmentangriff (teardrop, newtear, bonk)
IP-Bombing (meist als DDOS-Attacke)
SYN-Flood Attacken (massenhafte Verbindungsanfragen)

*5) Distributed Denial of Service (DDOS)*

Während bei normalen netzwerkbasierten DOS Attacken nur ein Angreifer beteiligt ist, sind bei DDOS Attacken mehrere Angreifer beteiligt, die simultan einen DOS Angriff auf einen Host ausführen. Ein DDOS-Angriff wird zentral kontrolliert, es gibt also einen oder mehrere Server (so genannte Master), die viele Clients (auch einfach als Daemons bezeichnet) kontrollieren. Diese Angriffe sind erst seit 1999 bekannt. Die dokumentierten Angriffe gingen meistens von vier Werkzeugen aus: trinoo, TFN Tribe Flood Network, stacheldraht (basiert auf trinoo und TFN) und shaft.
Verhinderung eines Einbruchs durch Kombination von Sicherheitsmaßnahmen wie kontinuierliche Aktualisierung der Software, Einsatz von Proxies, Paketfiltern, Einbruchserkennung und Gegenmaßnahmen bei erfolgreichem Angriff.

## III. SICHERHEITSMECHANISMEN

### *A. Firewall*

Eine Firewall ist laut Definition ein Konzept zur Trennung von Netzwerkbereichen, dessen korrekte Umsetzung sowie dauerhafte Pflege. Es werden zwei Typen unterschieden:

*1) Paketfilter*

Ein Paketfilter ist ein Programm, das versucht Sicherheitsrichtlinien bezüglich des Netzwerkverkehrs durchzusetzen. Dies funktioniert indem Pakete durch festgelegte Regeln gefiltert, protokolliert, markiert und geändert werden. Ein Paketfilter arbeitet auf den Schichten 3 und 4 des ISO/OSI-Schichtenmodells. Desweiteren können Datenpakete beispielsweise auf einen Proxy umgeleitet werden. Um einen kleinen Einblick in die Paketfilter zu bekommen werden diese Beispielhaft anhand von "iptables" erläutert. Dabei kann nur ein kleiner Ausschnitt des mächtigen Werkzeugs gezeigt werden.

*a) Iptables*

Das Programm kommuniziert mit dem Linux Kernel, und weist diesen an, Pakete nach bestimmten Regeln zu filtern. Da die Einstellung bei jedem Neustart gelöscht wird und die Regeln neu gesetzt werden müssen, sollte dies mit Hilfe der Programme "iptables-save" und "iptables-restore" geschehen. Regeln werden in Ketten gehalten, d.h. jede Kette ist eine Sammlung von Regeln. Regeln werden nach dem folgenden Prinzip abgearbeitet:

WENN (Filteroption) DANN Aktion (löschen, akzeptieren, ... des Paketes)

Regeln werden solange nacheinander abgearbeitet, bis keine Regel in der Kette zutrifft, dann entscheidet die Policy bzw. Sicherheitspolitik(siehe Grundlagen) der Kette was mit dem Paket geschieht. Aus Sicherheitsaspekten wird eine prohibitive Sicherheitspolitik empfohlen, bei dieser werden alle Pakete verworfen für die keine Regeln definiert wurden.
Standardmäßig gibt es drei Tabellen denen wiederum Ketten zugeordnet sind.

- Grundlagen

Das Programm `iptables` bietet folgende Optionen zur Verwaltung von Filterregelketten:
Kette erstellen (`-N`)
Kette löschen (`-X`)
Policy für eine eingebaute Kette ändern (`-P`)
Regeln einer Kette auflisten (`-L`)
Regeln aus einer Kette entfernen (`-F`)

Verwaltung der Regeln in einer Kette:
Neue Regel an eine Kette anhängen (`-A`)
Neue Regel an bestimmte Position in der Kette einfügen (`-I`)
Regel an bestimmter Position in der Kette ersetzen (`-R`)
Regel an einer bestimmten Position in der Kette löschen (`-D`)

Mit einer Regel wird entschieden was mit einem Paket passieren soll. Jede besitzt bestimmte Parameter nach denen sie überprüft ob die Informationen eines Paketes auf sie zutreffen. Wenn die Parameter zutreffend sind, wird das Paket meist an ein neues Ziel verwiesen oder es wird eine Methodeangewandt. Für die Bearbeitung der Pakete gibt es mehrere Ziele und Methoden (Policy). Diese werden mit dem Parameter -j initialisiert, häufig benutzte sind:
ACCEPT: das Paket kann passieren
REJECT: das Paket wird zurückgewiesen und ein Fehlerpaket wird gesendet
LOG: schreibt einen Eintrag in die syslog
DROP: das Paket wird ignoriert und keine Antwort gesendet
REDIRECT: die Ziel-Adresse des Paketes wird hiermit so verändert, dass es zum lokalen Rechner gesendet wird
MASQUERADE: die Quell-Adresse des Paketes wird durch die IP-Adresse der Schnittstelle ersetzt, auf dem es den Rechner verlässt

- Filter-Tabelle

Die Filter-Tabelle ist zuständig für die Filterung am Host, sie besteht standardmäßig aus drei Ketten: Input, Output und Forward.

**Input**: Pakete mit Zieladresse des lokalen Rechners. Input-Kette kann Paket entweder verwerfen oder durchlassen.
Bsp.: `iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP`
Mit `-p` wurde das Protokoll ICMP bestimmt, die `-s` Option legte die Quelladresse der Pakete fest.

Die folgenden Filteroptionen können angegeben werden:
Quell- und Zieladresse festlegen:
`-s`, `--source` oder `-src` - Quelladresse
`-d`, `--destination` oder `--dst` - Zieladresse

**Output**: Lokaler Prozess kann neues Paket erzeugen und diese ins Netzwerk versenden. Die Output-Kette prüft diese und leitet sie an die Netzwerkschnittstelle weiter.
Bsp.: `iptables -A OUTPUT -f -d 192.168.1.1 -j DROP`
Diese Regel verwirft alle Fragmente(Parameter -f), die an 192.168.1.1 gehen.

**Forward**: Forward-Kette prüft Pakete die vom inneren ins äußere Netz und umgekehrt, übertragen werden sollen.
Bsp.: `iptables -A FORWARD -m limit -j LOG`
Diese Regel logt alle Pakete die das Limit übersteigen.

- NAT-Tabelle

Network-Adress-Translation, in der NAT Tabelle werden die folgenden Ketten gespeichert:
PREROUTING: Alle Pakete kommen hier durch bevor eine Routing-Entscheidung getroffen wird.
POSTROUTING: Alle Pakete kommen am Ende der Verarbeitung hier durch.
**Output**: Wie bei Filter-Tabelle.
*Bsp.:* `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport http -j REDIRECT --to-port 3128`
Dieses Statement leitet alle Port 80 Anfragen auf Adapter eth0 an Port 3128 ('transparenter Proxy')

- Mangle-Tabelle

Die Mangle-Tabelle wird zur Paketmanipulation verwendet, sie besteht aus einer PREROUTING- und OUTPUT-Kette.

*2) Proxy*

Ein Proxy, oder auch Application Level Gateway, befindet sich zwischen Client und Server. Proxies arbeiten auf Applikationsebene(Schicht 5-7 des ISO/OSI Modells), daher bieten sie sich als Virenscanner und Kindersicherungen an.

*B. Honeypot*

Ein Honeypot ist ein Rechner, der absichtlich innerhalb eines Systems Sicherheitslücken aufweist. Somit bringt ein Honeypot den Vorteil, dass sich ein Angreifer mit dem unwichtigen Teil des Netzwerks befasst und andere Rechner mit wichtigen Inhalten vernachlässigt. Außerdem sollen Angriffsweisen der Angreifer analysiert werden. Falls ein Honeypot allerdings entarnt wird, besteht die Gefahr, dass er als Einstiegspunkt in das Netzwerk missbraucht wird. Es existieren auch ganze Netzwerke aus Honeypots, sogenannte Honeynets. Sie dienen beispielsweise zur Analyse von Viren und deren Eigenschaften, sich in einem Netzwerk zu verbreiten. Oft werden solche Analysen von Antivirus Software Herstellern durchgeführt.

- Honeypots die Angriffe ausschließlich erkennen und somit als Frühwarnsystem oder Ablenkung dienen , sind sogennante Production Honeypots (PH). Sie simulieren Dienste, keine

Schwachstellen und Lösen bei einem Verbindungsversuch einen Alarm aus. Andere Systeme können dann abgesichert werden.

- Eine deutlich komplexere Klasse der Honypots sind die Research Honeypotss (RH). Sie dienen zur Analyse von Angriffstaktiken oder –trends. Außerdem stellen sie das Angriffswerkzeug fest. Anhand der Angriffe wird gefiltert welche Dienste besonders beliebt sind. Sämtliche Kommunikation wird mit kommentiert, dadurch können Regeln einer Firewall oder eines Intrusion Detection Systems verbessert werden.

Es gibt drei verschiedene Anwendungstypen eines Honeypot:

*1) Low Interaction Honeypot*

Der simpelste Typ eines Honeypot ist ein Low Interaction Honeypot. Er emuliert lediglich einen einzigen Dienst und ist aufgrund seiner einfachheit sehr leicht zu enttarnen. Er dient zur Erfassung von automatisierten Attacken. Es wird beispielsweise ein Login angeboten, der bei jedem Versuch fehlschlägt und eine Fehlermeldung zurück gibt. Somit ist jeder Login-Versuch als Angriff anzusehen. Low Interaction Honeypot Produkte sind unter anderem: honeyd, mwcollet, nepenthes honeytrap und multipot.

*2) Medium interaction Honeypot*

Komplexer wird die Konfiguration eines Medium Interaction Honeypots. Dieser emuliert bekannte oder beliebige Schwachstellen und ist um einiges schwieriger zu enttarnen

*3) High Interaction Honeypot*

Kaum zu endtarnen sind die High Interaction Honeypots. Dabei handelt es sich um ein komplettes System und nicht nur kleineren Dienstemulationen. Sie werden durch Firewalls vom restlichen System getrennt um Zugriffe zu vermeiden. Protokolldateien werden auf einem externen Server gesichert, um das verwischen der Fußspuren des Angreifers zu verhindern.

### *C. Intrusion Detection System (IDS)*

Ein IDS ist ein System zur Erkennung von Angriffen gegen ein Computersystem oder Netzwerk. Es kann sowohl als Ergänzung der Firewall, als auch der direkten Überwachung eines Computers verwendet werden. Durch ein Intrusion Prevention System (IPS), kann das IDS um weitere Funktionen, wie Beispielsweise dem Verwerfen von Daten ergänzt werden. Desweiteren kann ein Honeypot Bestandteil eines IDS sein. Es existieren drei IDS Architekturen:

*1) Host-Basierte IDS*

Die älteste Architektur ist das Host-Basierte IDS. Es wird auf allen zu überwachenden Systemen installiert und kontrolliert anhand von Prüfsummen, ob Veränderungen am System vorgenommen wurden. Dadurch haben sie den Vorteil sehr spezifische Aussagen über Angriffe tätigen zu können. Desweiteren bieten sie eine umfassende Systemüberwachung. Der Nachteil ist allerdings, dass bei einem Ausfall des Systems auch das IDS ausser Gefecht ist. Außerdem kann ein Host-Basiertes IDS durch DOS-Angriffe ausgehebelt werden. Samhain ist beispielsweise solch ein Host-Basiertes IDS.

*2) Netzwerk-Basierte IDS*

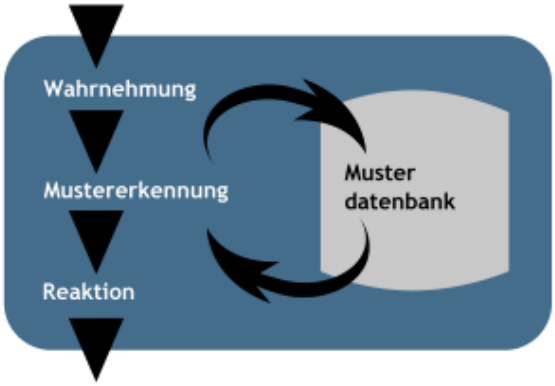
Die Netzwerk-Basierten IDS versuchen alle Netzwerkpakete aufzuzeichnen, zu analysieren und verdächtige Aktivitäten zu melden. So sollen über den Netzwerkverkehr, Angriffsmuster frühzeitig erkannt werden. Ein Sensor des Systems kann ein ganzes Netzsegment überwachen. Außerdem ist die Sensorfunktion durch das Ausschalten eines Zielsystems nicht gefährdet. Doch eine lückenlose Überwachung ist nicht immer gewährleistet. Denn ein 1 GBit LAN übersteigt die Bandbreite des Sensors. Auch in geswitchten Netzwerken ist keine lückenlose Überwachung möglich. Ein Beispiel für ein Netzwerk-Basiertes IDS ist Snort.

*3) Hybride IDS*

Eine Mischung aus Host- und Netzwerk-Basierten IDS ist das Hybride IDS. Dieses besteht aus drei Komponenten: Einer Managementkomponente, Hostbasierten und Netzwerkbasierten Sensoren.

ABBILDUNG I. ABLAUF EINES HYBRIDEN IDS

Wie in Abbildung 1 beschrieben, gilt es zunächst Angriffe




durch Vergleichen von Angriffssignaturen zu erkennen. Die Wahrnehmung geschieht durch die Sensoren, welche Logdateien oder Netzwerkverkehrsdaten sammeln, anhand einer Musterdatenbank vergleichen und je nach Resultat des Vergleichs einen Alarm auslösen. Die Benachrichtigung bei Funden erfolgt, abhängig von den Einstellungen, per E-Mail oder SMS, in den meisten Fällen an den Administrator. Je nach Umfang des Systems, ist es auch möglich eine Sperrung und/oder Isolierung des Eindringlings zu erzielen. Dynamische IDS haben desweiteren die Möglichkeit durch heuristische Methoden bisher unbekannte Angriffe zu erkennen. Das Ziel bei diesen Verfahren ist es Angriffe schon anhand von Ähnlichkeiten, mit einem bekannten Angriff, zu erkennen. Dynamische IDS haben allerdings das Problem, dass sie viele falsche Warnungen melden oder aber Angriffe gar nicht erkennen. So ist es möglich das IDS gar als Angriffsziel zu nutzen. Aus diesen Gründen sind dynamische IDS nicht weit verbreitet und es wird primär auf statische Systeme gesetzt. Prelude ist ein Beispiel für ein Hybrides IDS.

[1] K. Siyan and C. Hare, “Internet Firewalls & Netzwerksicherheit,” SAMS, 1955.

[2] R. L. Ziegler, “Linux Firewalls,“ 1st ed., New Riders Press, November 1999.

[3] Anonymous, “Der neue Hacker`s Guide,” 2.Auflage, Markt+Technik, Juli 2001