



Intrusion Detection Basics

- Ziele von Angriffen
- Formen von Angriffen
- Vorgehensweise von Eindringlingen
- Überwachungsmöglichkeiten
- Tools: tripwire, iptraf, tcpdump, snort



Ziele von Angriffen (Auswahl)

- Sport: Der Angreifer sucht eine Herausforderung. Lästig aber oft harmlos.
- Vandalismus: Der Angreifer will Zerstörung anrichten. Sonderform von Sport 8-(
- Diebstahl von Ressourcen (z.B. ftp).
- Diebstahl / Spionage.
- Störung des Geschäftsbetriebes.
- Image-Schaden für den Angegriffenen.



Konkrete Formen von Angriffen

- (D)DoS: (Distributed) Denial of Service
- Übernahme von Rechnern durch Erlangen von Superuser-Rechten -> meist unauffällig.
- Abhören / Stehlen von Inhalten, Passwörtern, Kreditkartennummern usw.
- Defacement: Verändern z.B. von Webseiten
- Fernsteuern, TCP-Hijacking



Vorgehensweise Intrusion

- Lernen: Network Mapping, Hardware, Betriebssysteme (wie verhindern?)
- Adressen- und Portscans (wie verhindern?)
- Eindringen über einen angreifbaren, offenen Port in einen Rechner mit unsicherem Betriebssystem (wie verhindern?)
- Verseuchen des Systems
- Erlangen der Superuser-Rechte und Übernahme der Kontrolle über das System



Was passiert auf dem System?

- Installation von Programmen, die:
 - Bestehende Programme ersetzen,
 - deren Verhalten verändern,
 - fernsteuerbar sind,
 - Daten ausspionieren und weiterleiten.
- Erkennbar daran, dass Programme und andere Files sich verändert haben.
- Wie kann man das überwachen: tripwire
- Stichwort: root kits



Was passiert im Netzwerk?

- Netzwerks-Scan, Port-Scan
- Verfälschte IP-Adressen
- Unvollständiger Verbindungsaufbau
- Veränderte Pakete (ICMP mit Daten!)
- Pakete werden unterwegs verändert
- Performance-Einbrüche
- Merkwürdige Datentransfers



Spooftng, Fälschung

- Adressen (Source, Destination)
- Portnummern, Flags
- Mac-zu-IP-Adressen-Zuordnung (ARP-Spoofing)
- Wie schafft man Abhilfe?



Fragmentierung

- IP-Pakete werden fragmentiert, wenn sie Netzwerksabschnitte durchlaufen, die das erfordern.
- „Bösartigen Inhalt“ kann man auf mehrere Fragmente verteilen.
- Fragmente werden einfach weggelassen.
- Sehr kleine Fragmente: Der TCP-Header wird zerlegt und nicht mehr erkannt.



Beispiele DoS-Attacken

- „Brute Force“: Von einem oder mehreren Rechnern an viele andere Rechner Anfragen mit gespoofter Source-Adresse (des Opfers!) schicken -> was passiert?
- Fragmentiertes ICMP ohne End-Fragment -> was passiert?
- SYN-Flooding: Wieso ist das ein Problem?



Bekannte Angriffe

- smurf: Reflektor mit Source-Spoofing
- Tribe Flood Network: Master steuert geknackte Hosts für DoS-Attacke
- WinFreeze: ICMP Redirect auf sich selbst (geht nur bei Windows NT4)
- LOKI: ICMP als Tunnel zur Client/Server Fernsteuerung (Host muss gehackt sein)



Die elegante Variante

- MITNICK-Attacke: SYN-Flooding mit TCP-Hijacking...
- Durch SYN-Flooding wird der Zielhost blockiert: 3-way-Handshake unvollständig.
- Das blockierte System wird durch Spoofing ersetzt, weil es nicht mehr reagiert.
- Der Angreifer hat somit eine Vertrauensbeziehung zwischen zwei Teilnehmern „gekapert“ und kontrolliert sie.



Die Praxis der Überwachung

- tcpdump erzeugt tonnenweise Informationen, die man erstmal analysieren muss.
- Beispiel: http Header-Analyse (einfach)
- iptraf muss beobachtet werden – personalintensiv (besonders nachts :-)
- Abhilfe schafft **snort**, das automatisch das Netzwerk überwacht.
- **snort** bietet laut LANline sogar mehr als kommerzielle Systeme!

Exkurs: Hex -> ASCII

```
#include <stdio.h>
main(){
    int wert;
    while( scanf("%2x", &wert) != EOF ){
        printf ( "%c", wert );
    }
}
```



tcpdump benutzen (Beispiel)

- Schreibt normalerweise nur Header
- Aufruf:
 - tcpdump ...
 - -s <number_of_bytes_per_packet>
 - -i <interface>
 - -x (oder je nach Version -X)
 - dst host 192.109.16.6 and dst port http
- Hex-Packetdump nach ASCII konvertieren



Mehr Infos...

- <http://cebu.mozcom.com/riker/iptraf/index.html>
- <http://www.snort.org>
- Stephen Northcutt, Judy Novak:
IDS: Intrusion Detection-Systeme
(Verlag mitp Bonn 2001)
- Joseph Brunner: *Linux Security*
(Verlag Addison Wesley 2002)



Aufgaben IDS

- Experimentieren Sie mit den Tools wie iptraf, tcpdump, ethereal
- Analysieren Sie snort und seine Konfigurations-Möglichkeiten
- Lesen Sie über IDS in den Quellen nach, insbesondere auch im Internet
- Wo müsste snort installiert werden?