

Intrusion Detection mit PortSentry

Autor: Sebastian Wolfgarten, sebastian@wolfgarten.com

Homepage: <http://www.wolfgarten.com>

Erstellungsdatum: 24. Dezember 2001, 20:59 Uhr

Einleitung:

Kaum sind Jens und ich aus dem Urlaub zurück, veröffentliche ich meinen nächsten Artikel: Er erklärt einfache TCP/UDP Port Scan Detection mit PortSentry und zeigt wirkungsvolle Gegenmaßnahmen auf, so dass Angreifer erfolgreich abgewehrt werden können.

Inhalt:

PortSentry ist ein (einfaches aber wirkungsvolles) Port Scan Detection Utility, d.h. es erkennt Port Scans auf TCP oder UDP Basis und kann entsprechende Gegenmaßnahmen einleiten, so daß es einem Angreifer fast unmöglich gemacht werden kann, einen Host anzugreifen. Gegenmaßnahmen sind dabei beispielsweise das Setzen einer IPChains/IpTables Regeln oder ähnliches.

PortSentry ist durch die Firma PSIONIC entwickelt worden und es kann unter <http://www.psionic.com/tools/portsentry-1.1.tar.gz> heruntergeladen werden. Man muss es mit "tar xvzf portsentry-1.1.tar.gz" entpacken und mit "make linux" und "make install" wird das Programm nach "/usr/local/psionic/portsentry" installiert.

Bevor man PortSentry startet, sollte man die zentrale Konfigurationsdatei ändern. Ich habe dazu die Datei "/usr/local/psionic/portsentry/portsentry.conf" editiert und mir folgende Optionen eingestellt:

```
---schnipp---
```

```
# Hier sind alle TCP und UDP Ports aufgeführt, die das Programm
# ueberwachen soll - das sind die Standardports. Es koennen hier noch
# beliebige andere Ports angegeben werden.
TCP_PORTS="1, 11, 15, 79, 111, 119, 143, 540, 635,1080, 1524, 2000, 5742,
6667, 12345, 12346, 20034, 27665, 31337, 32771, 32772, 32773, 32774,
40421, 49724, 54320"
UDP_PORTS="1, 7, 9, 69, 161, 162, 513, 635, 640, 641, 700, 37444, 34555,
31335, 32770, 32771, 32772, 32773, 32774, 31337, 54321"
# PortSentry ueberwacht ausserdem alle TCP/UDP HighPorts
ADVANCED_PORTS_TCP="1023"
ADVANCED_PORTS_UDP="1023"
# NETBIOS Sachen und nen paar UDP Sachen lassen wir mal aus
ADVANCED_EXCLUDE_TCP="113,139"
ADVANCED_EXCLUDE_UDP="520,138,137,67"
# In der nachfolgenden Datei stehen die zu ignorierenden Hosts/Netze
# drine
IGNORE_FILE="/usr/local/psionic/portsentry/portsentry.ignore"
# Wen haben wir schon entdeckt und bekämpft?
```

```
HISTORY_FILE="/usr/local/psionic/portsentry/portsentry.history"
# Wer ist auf der Blacklist?
BLOCKED_FILE="/usr/local/psionic/portsentry/portsentry.blocked"
# Ja, bitte beziehe DNS Informationen
RESOLVE_HOST = "1"
# Ja, UDP und TCP Aktionen wollen wir bekämpfen!
BLOCK_UDP="1"
BLOCK_TCP="1"
# Hier ist unsere sehr einfache, aber wirkungsvolle Bekämpfungsmethode:
# Wir setzen eine Iptables Regel und sperren dem Remote Host den
# Zugriff auf unseren Rechner, fertig :-))
KILL_ROUTE="/usr/local/sbin/iptables -A INPUT -s $TARGET$ -j DROP"
---schnapp---
```

So einfach kann Intrusion Detection sein :-)) Zugegebenermaßen nicht gerade eine High-End Lösung aber dennoch sehr wirkungsvoll.

Ich habe mit nmap, einem populären Port Scanner von insecure.org einen Half-Open TCP Scan durchgeführt und dieser wurde von PortSentry einwandfrei erkannt und vereitelt. Half-Open Scans sind normalerweise sehr schwer zu erkennen, da die Verbindung zwischen dem lokalen Computer und dem scannenden Remote-Computer eigentlich nie richtig zustande kommt. Der Remote Computer sendet ein SYN Flag und sobald der gescannte Computer geantwortet hat, wird durch den Remote Computer ein Reset-Flag (RST) gesendet, wodurch die Verbindung wieder getrennt wird. Sollte Half-Open Scans tauchen in den Logfiles normalerweise kaum bis gar nicht auf. Sobald ein Angreifer einen PortScan macht, wird die Iptables Regel ausgeführt und jeglicher Datenverkehr zwischen dem PC des Angreifers und dem lokalen PC wird gesperrt. Ein Blick in die IP Tabeß Regeln Filter mit "iptables -t filter -L" gibt Auskunft über die gesperrten Hosts. Außerdem findet sich ein Eintrag in /var/log/messages. Im Downloadbereich unter Site www.wolfgarten.com habe ich ein Startskript für PortSentry zur Verfügung gestellt. Damit dieses beim Systemstart gestartet wird, müssen noch die entsprechenden Symbolic Links sowie ein "chmod +x /etc/init.d/portsentry" gesetzt werden. Die Links lauten:

für SuSE Linux:

```
"ln -s /etc/init.d/portsentry /etc/init.d/rc2.d/S21dportsentry"
```

```
"ln -s /etc/init.d/portsentry /etc/init.d/rc2.d/K03portsentry"
```

für Debian Linux:

```
"ln -s /etc/init.d/portsentry /etc/rc2.d/portsentry"
```

```
"ln -s /etc/init.d/portsentry /etc/rc0.d/portsentry"
```

```
"ln -s /etc/init.d/portsentry /etc/rc6.d/portsentry"
```