Prüfen, ob Port auf Firewall freigeschaltet ist

Author : aklyachkin

Categories : Power Systems

Tagged as : AIX, firewall, inetd, netcat, network, NIMsecurity

Date : 06.06.2014

Das kann man eben einfach mit telnet machen, ist es so schwierig?

Das Problem aber, wenn man eine dynamische Verbindung testet. Z.B. NIM Client baut eine Verbindung mit NIM Server über den Port 1059 auf, dann öffnet er einen beliebegen Port aus dem Bereich 512-1023 und der NIM Server muss mit diesem Port eine Verbindung aufbauen kann. Falls wir mit telnet es testen, scheitert der Test, weil kein Port auf dem Client zum Zeitpunkt des Testes offen ist.

Dann muss man einen Port erst öffnen und nur danach testen. Auf Linux kann man es einfach mit nc (netcat) machen. Auf AIX auch, falls nc installiert ist.

Ich habe aber ein anderes Problem gehabt - der NIM Client ist in einer DMZ und man darf nichts auf den Client installieren. OK. Wahrscheinlich darf man, aber erst muss man irgendwie das alles durchkriegen. Und zwar durch den Firewall.

Kollegen, die für den Firewall zuständig sind, haben sich brav gemeldet, dass alles offen ist, und das Problem liegt an meinem Server. Dann muss ich entweder bestätigen, dass das Problem an NIM Server liegt, oder beweisen, dass das Problem doch im Firewall.

Dafür muss ich ohne netcat einen Port öffnen und mit telnet die Verbindung testen.

Auf jedem AIX Server ist immer inetd Server installiert. Ja, er wird sehr oft gleich dicht gemacht, aber für einen kleinen Test kann er sehr nützlich sein.

Erst müssen wir einen neuen Service in /etc/services eintragen, z.B.:

testme 1022/tcp

Wir haben definiert, dass der Service "testme" auf dem Port 1022 hören soll. Der Port 1022 habe ich ausgewählt, weil ich den testen wolllte. Falls ihr einen anderen Port brauchen - feel free, aber erst prüft, ob der Port schon in /etc/services eingetragen ist und ob ein Program schon mit dem Port was macht.

Dann tragen wir noch eine Zeile in /etc/inetd.conf ein:

testme stream tcp nowait root /tmp/check_port

"testme" - das ist der Name unseren Services. Wir werden den Service unter User root starten lassen (aber das ist nicht notwendig - so einen einfachen Service können wir auch unter nobody starten), und für den Service wird das Script /tmp/check_port ausgeführt.

Jetzt müssen wir das Script check_port anlegen. Es ist sehr einfach. Weil wir inetd verwenden, müssen wir nicht an Sockets und die ganze Geschichte mit TCP/IP denken. Inetd macht alles für uns und übergibt

unserem Script das ganze Input an Standard Input (stdin) und alles, was wir an Standard Output (stdout) schreiben, wird dem Client übergeben. Deshalb hat das Script nur 5 Zeilen:

```
#!/usr/bin/ksh

LANG=C

read request

echo "Hey! You sent the following request:"

echo $request
```

Nicht vergessen - chmod +x /tmp/check_port. Sonst funktioniert nichts ;-) Und wir können gleich ohne inetd prüfen:

```
# /tmp/check_port

test

Hey! You sent the following request:

test

#
```

Cool! Jetzt können wir inetd "refresh"-en oder erneut starten:

```
# refresh -s inetd
```

und wieder prüfen, ob was auf dem Port 1022 sichtbar ist:

```
# netstat -an | grep '*.1022'

tcp4 0 0 *.1022 *.* LISTEN
```

und noch eine Prüfung:

```
# telnet localhost 1022

Trying...

Connected to loopback.

Escape character is '^]'.

test

Hey! You sent the following request:

test
```

Connection closed.

Noch cooler! Alles funktioniert! Jetzt können wir endlich den Firewall testen. Dafür müssen telnet von einem anderen System laufen lassen:

telnet X.X.X.X 1022

Falls alles geht, Du hast gewonnen! Falls Du nur "Trying..." siehst und nichts mehr, dann ist das Problem offensichtlich auf der Firewall Seite. In meinem Fall lag das Problem aber nicht an NIM oder am Firewall, sondern an NAT ;-)

Viel Spaß!

P.S. Ach ja. Nicht vergessen - nach dem Test alles weg aus /etc/inetd.conf!!!