Mit linux kann man Systeme im Internet scannen.

Der Befehl hierzu lautet: nmap 192.16.1.101 -sT -p 1-33000 -O -r -R -v

Danach kommt eine Ausgabe

Initiating Parallel DNS resolution of 1 host. at 16:23
Completed Parallel DNS resolution of 1 host. at 16:23, 0.00s elapsed
Initiating Connect Scan at 16:23
Scanning Node2.workgroup.foo (192.168.1.101) [33000 ports]
Discovered open port 22/tcp on 192.168.1.101
Discovered open port 111/tcp on 192.168.1.101
Discovered open port 604/tcp on 192.168.1.101
Discovered open port 632/tcp on 192.168.1.101
Discovered open port 701/tcp on 192.168.1.101
Discovered open port 2049/tcp on 192.168.1.101
Discovered open port 3306/tcp on 192.168.1.101
Completed Connect Scan at 16:23, 7.34s elapsed (33000 total ports)
Initiating OS detection (try #1) against node2.workgroup.foo (192.168.1.101)
Nmap scan report for node2.workgroup.foo (192.168.1.101)