Hacking Firewalls

In theory, a firewall should block unauthorized access on every port. (A *port* is just a software-defined channel you can use to connect to a computer. They exist so that computers can connect to multiple other network endpoints at once.) In practice, many default firewall configurations allow access on one port or another. Use the `knock` command to test a port for vulnerability. For instance, if you suspect that port `8080` is vulnerable, type `knock 8080` and press enter.

If the port is indeed vulnerable, the hacktool will automatically compromise the firewall and move on to the next securty measure.

Common Firewall Model Numbers and Vulnerable Ports

Firewall model	Vulnerable port
BH91	7762
CC31	1249
CO84	1899
DD58	4501
DX96	2940
DZ75	5012
EY56	8446
EZ64	1230
FR467	6311
HS94	7679
IA576	5785
IH610	6282
IL164	1859
JQ418	5108
JU95	4590
JW819	3904
KK477	9423
KR046	5641
LG312	0758
LX567	2201
MI463	1837
NL51	5966
NN689	1218
OL345	9275
OY564	9221
PA16	7210
PH471	4408
QA63	3995
QB16	4606
QC00	5279
RB240	0648

Firewall model	Vulnerable port
RM19	9100
RT532	7094
SE48	5116
TC576	8431
TG646	3641
TI49	5529
TZ630	8660
UU85	4580
VB545	3225
VD978	3374
VS942	2925
WZ970	4908
XX813	3171
YH840	6062
ZB833	4554
ZP04	1776