

# [TOOL] Fwknop – Firewall Knock Operator

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0046.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/19/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 19 Sep 2004 14:07:17 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Fwknop – Firewall Knock Operator

---

## SUMMARY

## DETAILS

fwknop stands for "Firewall Knock Operator" and is a piece of software that was released at the <http://www.defcon.org/html/defcon-12/dc-12-index.html>> DEFCON 12 conference in July, 2004 in Las Vegas.

fwknop implements network access controls (via iptables) based on a flexible port knocking mini-language, but with a twist; it combines port knocking and passive operating system fingerprinting to make it possible to do things like only allow, say, Linux-2.4/2.6 systems to connect to your SSH daemon.

fwknop supports shared, multi-protocol port knock sequences along with both relative and absolute timeouts, and coded port knock sequences encrypted with the Rijndael block cipher.

### Capabilities:

fwknop implements a flexible port knocking scheme based around log messages generated by the iptables firewall in the Linux kernel. fwknop supports both shared and encrypted port knock sequences, passive OS

## Securiteam: [TOOL] Fwknop – Firewall Knock Operator

fingerprinting, multi-protocol knock sequences (tcp, udp, and icmp), firewall access across multiple ports and protocols, firewall access timeouts, relative timeouts between knock packets, and more. There are two primary modes of execution; server mode, and client mode. When run in server mode, fwknop becomes a daemon and watches iptables log messages as they are written via syslog to a named pipe /var/lib/fwknop/fwknopfifo. If a valid knock sequence is seen, then fwknop will modify the iptables ruleset to grant the appropriate access to the originating IP address. Knock sequence parameters are defined in the file /etc/fwknop/access.conf. When run in client mode, fwknop generates either an encrypted knock sequence, or a shared knock sequence. Shared knock sequences are defined in the file ~/.fwknoprc.

### Download Information:

To obtain the latest version of fwknop visit:

<<http://www.cipherdyne.org/fwknop/download/>>

<http://www.cipherdyne.org/fwknop/download/>

The project's CVS repository is available at:

<<http://www.cipherdyne.org/cgi/viewcvs.cgi/fwknop/>>

<http://www.cipherdyne.org/cgi/viewcvs.cgi/fwknop/>

### ADDITIONAL INFORMATION

To keep updated with the tool visit the project's homepage at:

<<http://www.cipherdyne.org/fwknop/>> <http://www.cipherdyne.org/fwknop/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.