WHEN {PUFFY} MEETS ^REDDEVIL^

SATURDAY, JULY 21, 2007

Fl0p - Passive L7 Flow Fingerprinter

Checking back my old posts and I just figured out I have this post in my saved draft and never be posted online. It's all about identifying the flow by fingerprinting the application bytes in packets exchange of the connection stream. Thanks to Michal Zalewski who writes this tool called Fl0p, from the description -

fl0p is a passive L7 flow fingerprinter that examines TCP/UDP/ICMP packet sequences, can peek into cryptographic tunnels, can tell human beings and robots apart, and performs a couple of other infosec-related tricks.

If you are on FreeBSD, you can just install it via package/port system, but for gentoo users, you will have to install via source -

shell>wget http://lcamtuf.coredump.cx/soft/fl0p-devel.tgz

shell>tar xvzf fl0p-devel.tgz

shell>cd fl0p

shell>make
./Build all
Your system type is: FreeBSD

Please help with p0f 2:
http://lcamtuf.coredump.cx/p0f-help/

GNU make not found; failing back to regular (BSD?) make.
gcc -g -ggdb -Wall -DUSE_BPF=\"net/bpf.h\"
-I/usr/include/pcap -I/usr/local/include/pcap
-I/usr/local/include -o fl0p fl0p.c crc32.c -lpcap
strip fl0p 2>/dev/null || true

Running fl0p -

shell>./fl0p -h

Usage: ./fl0p [-f file] [-i device] [-s file] [-o file]
[-u user] [-e ms] [-T ms] [-FUKrqvpdtl] ['filter rule']
-f file - read fingerprints from file
-i device - listen on this device
-s file - read packets from tcpdump snapshot
-o file - write to this logfile (implies -t)
-u user - chroot and setuid to this user
-e ms - pcap capture timeout in milliseconds (1)
-q ms - packet timing threshold in milliseconds (400)
-F - disable fuzzy matching on all signatures
-U - display fingerprints for unidentified streams
-K - do not display known signatures (implies -U)
-r - resolve host names (not recommended)

ABOUT ME

GEEK00L

VIEW MY COMPLETE PROFILE

NSM ALLIANCE

Sguil
NSM Wiki
Taosecurity
Infosecpotpourri
Inline
Jontow
Vodun
Shirkdog
Transporter
Fifarek
Ayoi
Johncrackernet

HITB ALLIANCE

HackInTheBox
Adli
Mel
RedDragon
Takizo
Xwings
Hackathology

MYOSS ALLIANCE

BSDFreak
Lbe
Mypapit

BSD PORTS

OpenBSD Ports
FreeBSD Ports

BLOG ARCHIVE