

whatsbcn Improved readme

c4f1f18 · 13 years ago

69 lines (57 loc) · 1.69 KB

[Preview](#)
[Code](#)
[Blame](#)
[Raw](#)
[Copy](#)
[Download](#)

skpd - Process dump to executable ELF for linux

Features:

- It supports:
- static binaries.
- dynamic binaries.
- compressed files (at least upx)
- elfuck encrypted.
- 32 and 64 bits support.
- Generates an ELF file from a running process.
- If the original file was encrypted, the new one will not.
- i386, x86_64, MIPSEL

Use:

Usage: ./skpd {-p pid | -f file} [-o output_file] [-v]

1. Launch telnet client on one terminal

```
whats@x61s:~$ telnet
telnet>
```

2. Search the pid

```
whats@x61s:~$ ps aux | grep telnet
whats      7029  0.0  0.0   3088  1212 pts/1    S+   21:36   0:00 telnet
whats      7031  0.0  0.0   2952   740 pts/0    S+   21:36   0:00 grep --colou
```

3. Launch skpd dumping the process to the new file t

```
whats@x61s:~/code/pd/skpd/src$ ./skpd -p 7029 -o t
skpd 1.0 - <whats[@t]wekk.net>
=====
[*] Attached to pid 7029.
[*] Reading /proc/7029/maps ...
[*] Rebuilding ELF headers.
[*] File t saved!
[*] Done!
[*] Dettached.
```

4. Exec the new created file

```
whats@x61s:~/code/pd/skpd/src$ ./t
t> open www.wekk.net 80
Trying 64.22.71.90...
Connected to www.wekk.net.
Escape character is '^['.
```

References:

- This is a process dump based on ilo pd
 - <http://www.phrack.com/issues.html?issue=63&id=12&mode=txt>
- How the symbol resolution is made
 - <http://em386.blogspot.com/2006/10/resolving-elf-relocation-name-symbols.html>
- A Manu Garg article about auxiliary vectors
 - <http://manugarg.googlepages.com/aboutelfauxiliaryvectors>
- The source code
 - /usr/src/linux/fs/binfmt_elf.c

