

Forum:[Hack Forums](#)

Thread: [\[Linux\] ASM shellcode Creator \[Reverse Shell\]](#)

CryptixHacking - January 16, 2018, 6:58 am

asmTshell

is a exploit pen test application I developed for users using linux such as debian ubuntu or kali OS.

This tool allows you to build a reverse shell binary file and can be set to run on any OS be it windows linux or mac.

Once the target windows/linux/mac system runs the shell binary they connect to your server giving you full control of the systems command prompt or shell from your server.

It works by utilizing a linux asm compiler called "nasm"

It takes target asm payload and allows you to customize the payload to your desired IP and port # through a easy GUI. Once configuration is done from GUI it will edit your input to the needed ASM hex strings using a custom python script. After which it will compile your new ASM into your target binary file.

To get a server running you can use netcat nc or ncat

Code ncat -lvkp 1344

ncat to accept more than one client connection to server

nc -lvp 1344

netcat -lvp 1344

Once target system runs the shell binary they will connect to your server allowing you to control there OS from the shell.

Limitations

"keep in mind that your port or ip should not contain a 0, which could break it. If your IP contains a zero like 192.168.0.1 or your port contains a zero like 80, the build will not work"

--Read--

can test using 127.1.1.1 as localhost server IP

FIX MY REP AND ILL POST DOWNLOAD
Positive rep me for download

AV scan -

<https://www.virustotal.com/#/file/253d12fb5ddd6c58e02b5bbe0822012aef3624dae01a95927f148ba1da15a4c5/detection>

Leo Mikaelson - January 17, 2018, 5:53 am

Will be checking this out later. Thanks for this in advance.

CryptixHacking - January 17, 2018, 5:59 am

(Jan 17, 2018 06:53 AM)Leo Mikaelson Wrote: [\[CITE\]](#) Will be checking this out later. Thanks for this in advance.

Cool thanks for taking the time to check it out,

Sense this versions stub uses ASM and has issues with using 0 in IP and Port I will be soon updating it to use C/C++ to allow better control and customization of target stub. But other than that this version works pretty well give your IP or port does not contain any 0's dang ASM code :p

DI?E - January 19, 2018, 11:42 am

Looks nifty. I'll try it out. Thanks for the contribution.

Betty Blue - January 20, 2018, 9:07 pm

(Jan 17, 2018 06:59 AM)CryptixHacking Wrote: [\[CITE\]](#) Cool thanks for taking the time to check it out,

Sense this versions stub uses ASM and has issues with using 0 in IP and Port I will be soon updating it to use C/C++ to allow better control and customization of target stub. But other than that this version works pretty well give your IP or port does not contain any 0's dang ASM code :pWhy? Is it being treated as a NULL byte?

CryptixHacking - January 20, 2018, 9:31 pm

(Jan 20, 2018 10:07 PM)Deadhead Wrote: [\[CITE\]](#) Why? Is it being treated as a NULL byte?

When using a 0 in IP or Port will result in the ASM code containing a 0x00 hex code and nasm uses C to compile the ASM. In ASM C language this 0x00 Hex is treated as a terminator which causes the program to either hang or crash. This is what causes the nullbyte issue when using a 0 in IP or Port that and because how the shellcode ASM is setup.

The ASM code treating IP or Port incorrectly is due to how the shells code works in that it does not store or push a string as the IP/Port if the shells code was changed to handle the IP/Port differently then the ASM might not have such a issue.I could just recode a C shell and have it handle the IP and port from strings so that the ASM can handle the hex change but I think will be easier to convert to C and compile that rather than ASM.

I will soon be releasing a c/c++ version that doesn't use ASM which should solve any such issues.

Betty Blue - January 20, 2018, 10:06 pm

(Jan 20, 2018 10:31 PM)CryptixHacking Wrote: [\[CITE\]](#) When using a 0 in IP or Port will result in the ASM code containing a 0x00 hex code and nasm uses C to compile the ASM. In ASM C language this 0x00 Hex is treated as a terminator which causes the program to either hang or crash. This is what causes the nullbyte issue when using a 0 in IP or Port that and because how the shellcode ASM is setup.

The ASM code treating IP or Port incorrectly is due to how the shells code works in that it does not store or push a string as the IP/Port if the shells code was changed to handle the IP/Port differently then the ASM might not have such a issue. I could just recode a C shell and have it handle the IP and port from strings so that the ASM can handle the hex change but I think will be easier to convert to C and compile that rather than ASM.

I will soon be releasing a c/c++ version that doesn't use ASM which should solve any such issues. You're not treating the address as a string?

Smile? - January 20, 2018, 10:23 pm

Any method how to use it?

icy? - March 22, 2018, 8:37 am

I would love an update on this tutorial, seems valuable but sloppily written. Props to OP

kanishk - May 21, 2018, 11:56 pm

The file asmTshell is not running , giving abnormal behaviour error

CryptixHacking - December 4, 2018, 5:48 am

(May 21, 2018 11:56 PM)kanishk Wrote: [\[CITE\]](#) The file asmTshell is not running , giving abnormal behaviour error

If you mean the compiler/builder GUI is not working try updating your terminal system and binaries, As it would seem your linux/mac OS needs a update as the compiler/GUI of asmTshell should run fine. Could also be a permission error as you do not have permission to execute the asmTshell GUI binary. Maybe try chmod the file to 777.

If you mean the client trojan does not run. This is probably due to the fact that this shell trojan is coded and compiled from ASM code.

Due to the ASM restrictions of the code the "IP ADDRESS" of the server MUST NOT contain any 0. If the "Server IP ADDRESS" contains a 0 the binary file will fail with errors and not connect to server for shell control.

You can try renewing your external IP so that ISP "internet service provider" assigns you a new external IP address, Or use a VPN/Proxy that supports port forwarding, Changing the server IP so that it contains no 0's should fix and solve any compile or connect errors.

Sadly I do not plan to update this utility or the ASM code it uses for the binary clients. But with the correct ASM code it may be possible to use DNS or the IP as a internal locked string.

Download - <https://www.dropbox.com/s/0cwhldcqjwvrgo3/asmshell.tar?dl=0>