

Forum: [Hack Forums](#)

Thread: [\[Linux\]ASM\[Reverse Shell\]- Target WIndows/linux/mac](#)

CryptixHacking - January 16, 2018, 7:15 am

<https://hackforums.net/showthread.php?tid=5785622>

This is a linux based application I developed allowing you to create reverse shells for windows/linux/mac.

It uses a ASM payload and allows customization of payload then builds to a binary stub file.

So if you are on linux and need a reverse shell compiler that can build to windows/mac/linux this might work well.

And for those of you that dont know what a reverse shell ASM shellcode is - It is a program that when ran connects to a server and the server can then control that systems command prompt or shell.

Purple Kief - January 16, 2018, 7:40 am

OP why are you creating a thread here to link to your other thread?

CryptixHacking - January 16, 2018, 8:19 am

(Jan 16, 2018 08:40 AM)Purple Kief Wrote: [\[CITE\]](#) OP why are you creating a thread here to link to your other thread?

Tbh I couldnt decide which section it should of been placed in.

HangMansheart - January 16, 2018, 10:32 pm

So essentially, a listener for nc?

CryptixHacking - January 17, 2018, 5:52 am

(Jan 16, 2018 11:32 PM)HangMansheart Wrote: [\[CITE\]](#) So essentially, a listener for nc?

Yes and No

I mean the target systems nore your system needs netcat/nc is not needed at all here but it is a easy to use server to control the target systems that connect to you.

You can use basically any raw tcp socket server to handle the reverse shells though I just suggest using NC as the server as its cross OS compatible can handle multiple connections and is stable.

The stub is coded in ASM and hooks directly into the systems shell or command prompt and pipes the shell/cmd to your server for control.

So yea it works like a nc exec reverse shell but its just a ASM direct shellcode that can be edited to connect to your server be it NC or not.

I am working on a updated version of this which uses C/C++ and not ASM so that if users have a 0 in IP or Port will not cause build issues.

speckled_eggz - January 17, 2018, 7:28 am

Nice tool. I'll be sure to use it. Also, will any other communication protocols be implemented (not just TCP)?

CryptixHacking - January 17, 2018, 7:42 am

(Jan 17, 2018 08:28 AM)speckled_eggz Wrote: [\[CITE\]](#) Nice tool. I'll be sure to use it. Also, will any other communication protocols be implemented (not just TCP)?

Maybe in the updated version I will add more protocol support but for now just TCP is used.

I am working on updating the application to use C/C++ as the ASM has issues when settings IP / Port if your IP / Port has any 0s in it.

It will still be able to compile stub to windows executables and linux/mac binaries just will use gcc rather than nasm.

HangMansheart - January 17, 2018, 9:21 pm

(Jan 17, 2018 06:52 AM)CryptixHacking Wrote: [\[CITE\]](#) Yes and No

I mean the target systems nore your system needs netcat/nc is not needed at all here but it is a easy to use server to control the target systems that connect to you.

You can use basically any raw tcp socket server to handle the reverse shells though I just suggest using NC as the server as its cross OS compatible can handle multiple connections and is stable.

The stub is coded in ASM and hooks directly into the systems shell or command prompt and pipes the shell/cmd to your server for control.

So yea it works like a nc exec reverse shell but its just a ASM direct shellcode that can be edited to connect to your server be it NC or not.

I am working on a updated version of this which uses C/C++ and not ASM so that if users have a 0 in IP or Port will not cause build issues.

Ah, I wasn't aware. Looks very nice :)