

Forum:[Hack Forums](#)

Thread: [reverse shell](#)

SIM-5457022 - July 8, 2024, 11:09 am

how does one install a reverse shell onto someone else computer without them knowing?

BiNBo - July 8, 2024, 11:34 am

I would recommend some further research, you should have a better understanding of a what a reverse shell actually is before moving forward. A reverse shell is a type of connection where the compromised computer initiates an outgoing connection to an attacker's computer. This allows the attacker to gain remote access and control of the compromised computer. You don't "install" a reverse shell like an application because it's not exactly a piece of software, but a shell can be established with the right malicious software. Reverse shells are often delivered through malicious code, such as malware or exploits targeting vulnerabilities in software. They can be triggered through various means, like phishing emails, infected websites, or compromised software downloads.

In short, a reverse shell isn't a piece of software in the way that a word processor or a web browser is. It's not an application you download and install. Rather, a reverse shell is a type of network connection. It's a way for two computers to communicate, where the compromised machine (the victim) initiates the connection to the attacker's machine.

BlackSoulZN5006 - July 8, 2024, 12:53 pm

You can code a reverse shell in C# totally fine

h44y - July 8, 2024, 3:48 pm

Well first off you should start by scanning your target. Do they have any open attack surfaces?

If not, welp, you're going to have to be creative...

For starters you could try a relatively straight forward phising attempt. Beware that this might leave some traces back to you if you're not careful. Learn about opsec before exposing yourself.

Best of luck, do your due dilligence and don't make any hasty decisions.

Oh, and never hack where you rest at.

SIM-5457022 - July 9, 2024, 12:33 am

(Jul 8, 2024 11:34 AM)BiNBo Wrote: [\[CITE\]](#) I would recommend some further research, you should have a better understanding of a what a reverse shell actually is before moving forward. A reverse shell is a type of connection where the compromised computer initiates an outgoing connection to an attacker's computer. This allows the attacker to gain remote access and control of the compromised computer. You don't "install" a reverse shell like an application because it's not exactly a piece of software, but a shell can be established with the right malicious software. Reverse shells are often delivered through malicious code, such as malware or exploits targeting vulnerabilities in software. They can be triggered through various means, like phishing emails, infected websites, or compromised software downloads.

In short, a reverse shell isn't a piece of software in the way that a word processor or a web browser

is. It's not an application you download and install. Rather, a reverse shell is a type of network connection. It's a way for two computers to communicate, where the compromised machine (the victim) initiates the connection to the attacker's machine.

I know what a reverse shell is. I asked how do you get it installed on a victim's computer without detection.

a shell is just the cmd of a computer. A regular shell is where you dial in on a computer .

regular shell me -> connects to victims computer.

reverse shell is the opposite... victims computer ---> connects to my server or computer.

I understand this. I am asking how do you install one remotely as possible.

BiNBo - July 9, 2024, 5:57 am

(Jul 9, 2024 12:33 AM)SIM-5457022 Wrote: [\[CITE\]](#) I know what a reverse shell is. I asked how do you get it installed on a victim's computer without detection.

a shell is just the cmd of a computer. A regular shell is where you dial in on a computer .

regular shell me -> connects to victims computer.

reverse shell is the opposite... victims computer ---> connects to my server or computer.

I understand this. I am asking how do you install one remotely as possible.

I see, I think the issue here might be one lost in translation. When you say install, the context you're using it comes off as if you want to install a piece of software. I could be wrong, but I think you're somewhere between trying to establish a foothold and maintaining persistence. There's a number of methods for establishing the foothold, in particular in relation to remote code execution. You could send out malicious emails to the target(s) and see if you can drop a stager or loader of some sort (phishing). You could try exploiting known vulnerabilities or search for some of your own depending on the target (SQL injection, cross site scripting, server side request forgery, etc.)

Once you've established your foothold, in this case a reverse shell, you'll need to establish persistence. Depending on your T&T, there's a few ways at establishing persistence. So let's say you get a target to click on a link and get a dropper successfully on the machine. From here you can deliver your payload, like a RAT, to be stealthily delivered. From there it might modify or create entries in the registry (on windows machines) usually run and runonce keys. These entries instruct the system to execute the payload on startup. Some payloads will install itself as a service, others use DLL injection, some simply resides in memory which makes it incredibly difficult to detect.

DramaKing - July 9, 2024, 7:54 am

(Jul 9, 2024 12:33 AM)SIM-5457022 Wrote: [\[CITE\]](#) regular shell me -> connects to victims computer.

Actually, you seem to be describing a bind shell.

First of all, instead of us throwing out general tips, it would be helpful to know what kind of access you have. Are you connected on a local network to the target? Is the target remote? Do you not have a target and just want to spread a RAT across the Internet?

Forum members are not going to be able to do your reconnaissance, enumeration, and footprinting, which will give you the best chance of success. It's going to take legwork; otherwise, you could be trying to get a Windows reverse shell on a Mac, or using every exploit you can find in a very noisy

manner, hoping one works. Or you avoid detection by WD, but the target is running CrowdStrike Falcon.

What you're calling 'install,' hackers call 'persistence.'

happygonutty - July 9, 2024, 8:25 am

(Jul 8, 2024 11:09 AM)SIM-5457022 Wrote: [\[CITE\]](#) how does one install a reverse shell onto someone else computer without them knowing?

One simply goes to github.com or the market place section here in this forum. ?

DramaKing - July 9, 2024, 9:05 am

(Jul 9, 2024 08:25 AM)happygonutty Wrote: [\[CITE\]](#) One simply goes to github.com or the market place section here in this forum. ?

C'mon happy. Be helpful. He seems to at least know what a revshell is. How to infect a computer(?) while bypassing security measures seems to be the issue.

happygonutty - July 9, 2024, 11:26 am

(Jul 9, 2024 09:05 AM)DramaKing Wrote: [\[CITE\]](#) C'mon happy. Be helpful. He seems to at least know what a revshell is. How to infect a computer(?) while bypassing security measures seems to be the issue.

Fine I'm just messing with you guys. Hahaha. Well I know this is going to only be used for "educational" purposes only so the first best way to put a revshell in a target machine to assess first what is the operating system version and if OP has physical access to it or remote only.

If physical access, then what OP needs is to escalate root/admin privilege. If it ain't physical and remote with knowledge of target then best way is to conduct vulnerability assessment. Else if this is more than education purpose then one has to go to extremity and do some clever social engineering skills to drop the payload.

How about that? ?

SIM-5519216 - July 11, 2024, 11:42 am

(Jul 8, 2024 11:09 AM)SIM-5457022 Wrote: [\[CITE\]](#) how does one install a reverse shell onto someone else computer without them knowing?

either have a shell and install a reverse shell or encrypt a thing that makes the reverse shell in the background somehow i guess