

Forum:[Hack Forums](#)

Thread: [how to bypass \(conection refused\) when try to spawn a reverse shell](#)

wacamole - September 14, 2023, 2:52 pm

hi im new on pen testing i can execute system commands on target but when try to summon a reverse shell got connection refused i know its a firewall blocking outbound connections and in may be but my question its there its a method for bypass the connection problem and get reverse interactive shell? its a linux machine got vulns but i cant exploit those because i cant spawn interactive shell ty ???

DramaKing - September 14, 2023, 3:59 pm

If a port is blocked by a firewall, it's blocked.
The port isn't blocked. It's closed.
Is your handler actually running?

wacamole - September 14, 2023, 4:06 pm

ty for response i just got dumb shell php one i tryend via python php bash perl and cant get reverse shell i was thinking on port forwarding with ngrok but its complex with restricted shell and dumb shell is there a way for open port from test server?

ps my port open and no problem handling other rev conections

DramaKing - September 14, 2023, 4:20 pm

(Sep 14, 2023 04:06 PM)wacamole Wrote: [\[CITE\]](#) ty for response i just got dumb shell php one i tryend via python php bash perl and cant get reverse shell i was thinking on port forwarding with ngrok but its complex with restricted shell and dumb shell is there a way for open port from test server?

ps my port open and no problem handling other rev conections

So it's a reverse shell that you're trying to inject from a web shell? Ngrok won't help if your listener is accessible from the Internet. Is the server sending a RST packet? That shouldn't be right with a revshell.

wacamole - September 14, 2023, 5:06 pm

(Sep 14, 2023 04:20 PM)DramaKing Wrote: [\[CITE\]](#) So it's a reverse shell that you're trying to inject from a web shell? Ngrok won't help if your listener is accessible from the Internet. Is the server sending a RST packet? That shouldn't be right with a revshell.

yup weebely php i can execute cmd but i cant bypass that tools like chissel can work on this specific case? not an expert in networking but studying from this specific case i dont have checked the RST but im gonna take a look again ty for response

Mad76e. - September 15, 2023, 11:39 am

(Sep 14, 2023 02:52 PM)wacamole Wrote: [\[CITE\]](#) hi im new on pen testing i can execute system commands on target but when try to summon a reverse shell got connection refused i know its a firewall blocking outbound connections and in may be but my question its there its a method for bypass the connection problem and get reverse interactive shell? its a linux machine got vulns but i cant exploit those because i cant spawn interactive shell ty ???

Drama king is correct

Moreover windows10/11 has become somewhat good to detect and block those generic shells automatically.

DramaKing - *September 15, 2023, 12:27 pm*

(Sep 15, 2023 11:39 AM)Mad76e. Wrote: [CITE](#) Drama king is correct

Moreover windows10/11 has become somewhat good to detect and block those generic shells automatically.

Irrelevant when this is a Linux box.

Mad76e. - *September 16, 2023, 4:13 am*

Oh...

clearly I missed that, sorry