

Forum:[Hack Forums](#)

Thread: [Pentesting - Can't get by the IDS](#)

the-no-1 - January 27, 2020, 2:23 pm

Hello,

I have been asked to pentest a website (all parties have signed documentation to approve).

However I can't get by what looks like an IPS. I change my VPN to different locations and I try and do a dirscan or a ping and it gets blocked after 20 seconds. Any advice to get past this?

Thanks

veiled - January 27, 2020, 6:10 pm

this is going to be worth more than your time

<https://medium.com/@z3roTrust/evasion-obfuscation-techniques-87c33429cee2>

for your run of the mill pentest, you honestly could say, "x had y ips and an adversary would not be able to access content behind said ips without more time" etc

CyberStrike - January 27, 2020, 6:21 pm

Well automated tools often do things too quickly, why are you not manually navigating with an intercepting proxy? You need to map out functionality, figure out access controls, authentication, and MANY other things for a legit pentest. Don't be that guy who fires off a bunch of tools and proceeds to find nothing then calls it a day.

Edit: Check for a WAF also.

Dirk Rathken - February 5, 2020, 9:57 pm

automated tools will be detected almost everytime, def do what CyberStrike suggested, load up your attack proxy and start manually crawling the site... maybe keep a mind map for notes on where things are such as :

- Buttons - and what they do
- user input
- search boxes
- comment boxes
- ect ect.

remember hacking this website is just using inherent flaws in what the website does against it, in order to find these flaws you'll often need to know what the website does, and at least be able to take a guess as to how it does it.

lulzcat - February 6, 2020, 9:43 pm

You say you're pinging so I'm guessing that you're not hitting the web app but rather the server infrastructure so try packet fragmentation with nmap and see what results you get.

EDIT: I missed the "dirscan" part, to be honest, I'm not overly familiar with this but my assumption is that this is some sort of directory scanning tool? If so I'm also presuming this is against the file system and not crawling their web page structure? If it's touching the web app in any way, then

check for web app firewalls.