

Forum:[Hack Forums](#)

Thread: [Detect IDS/IPS or Firewall.](#)

hack3rcon - March 10, 2019, 11:55 pm

Hello.

How can I understand the target using any IDS/IPS or Firewall devices? For example, example.com

Thank you.

sh4moon - March 11, 2019, 8:57 am

for WAF (web application firewall) it's pretty easy. just try to do something it won't like, for example attempt a xss attack or sql injection. basically try to trip it. or there's an nmap script that'll detect it. for network-based firewalls or IDS/IPS, there are a few things you could try. I can't remember exactly how it works off the top of my head, but you can use nmap ACK scan to detect a firewall. you could do a traceroute and if that gets stopped somewhere along the way it's probably because there's a firewall or IDS/IPS of some kind. these are just some of your options. I'd suggest you experiment with it. hope this helped.

Fallenour - March 11, 2019, 10:48 am

(Mar 10, 2019 11:55 PM)hack3rcon Wrote: [\[CITE\]](#) Hello.

How can I understand the target using any IDS/IPS or Firewall devices? For example, example.com

Thank you.

It really depends on the series of systems and controls that they use. Some will give error messages that indicate at what point of the communication the connection was dropped, blocked, or intercepted, and some won't.

For instance, a poorly configured mod security instance will tell you that your connection attempt was blocked by mod security. An IPS will simply drop your connection, and tell you the connection was dropped by "insert IPS here".

Web email security systems will tell you that your attachment was blocked by the Fireeye NX/MX device, or by their email AV. Sometimes they'll have something like a spam filtering system, and it'll return a rejection notice.

It all really depends on the organization and environment.

The easiest way to learn how to detect them, and more importantly, how to bypass them, is to build a simulated environment of your target enterprise via OSINT, then building that environment, and then the subsequent security systems. Then go out and implement the best practices for those systems, as that's likely what their organization did.

Once you have that up, try to successfully hack the environment. If you can, odds are, you can hack the real one.

I used to do pentesting for banks, and this is what I would do on a regular basis. It helped me a lot, I hope it helps you as well.