Web Server fingerprinting is detecting the daemon providing the web server service such as Apache, ngnix or others, as well as the version of this daemon and the OS of the machine hosting the server.

We can use the Netcat tool to help us with this. Netcat is known as the TCP/IP swiss army knife. Netcat can be used a server or as a client. To fingerprint a webserver with Netcat we can use it as a client to manually send requests to the server.

* This activity is called banner grabbing, All we have to do is connect to the daemon with netcat and read the banner is sends back to our client.
* Text

  Description automatically generatedTo connect to a server with netcat all we have to do is type “nc <target address> 80”. After this we need to send a valid HTTP request to the target server, we can do this with the **HEAD** http verb.

Text

Description automatically generated with medium confidence

After the 2 empty lines are sent, the server should respond back with a banner often containing info about the web server and sometimes the server OS. Even if you receive a 404 or something you can still get valuable info on a server and its OS.

**OpenSSL:**

For clients that exclusively use HTTPS, we can use the OpenSSL command line tool.

Graphical user interface, text, application, email

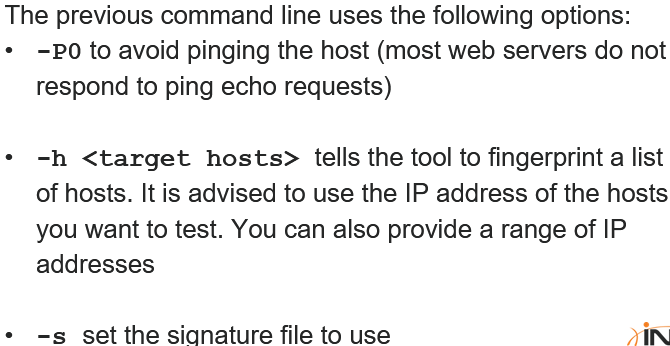
Description automatically generatedBasically the same thing with a different command.

These banners can be customized by admins, so they may not always return useful things.

There are automatic tools available to perform this and other scans to get info about servers.

Such as:

Graphical user interface, text, application, email

Description automatically generated

Visit <https://www.openssl.org/> for more info on openssl. (From What I saw when testing, I still got sever info on http sites from just using netcat) A screenshot of a computer

Description automatically generated with medium confidence

^^ if we have 1 command to execute on a Unix system we can create a reverse shell in 1 command