* Initial **ping** of website may not return anything useful as they block ICMP requests BUT you will see the IP address
* 
* **Nslookup** - Used to query DNS servers to obtain domain name or IP address mapping information  
  
* Can use [**IPChecker**](https://ipinfo.info/html/ip_checker.php) to find DNS information, Top Level Domain, and Registration information
* Kali Linux has built in tool called **whois** that provides this same information   
  
* **WhatWeb** used to identify and fingerprint web technologies and frameworks used on a particular website.  
  - Analyzes the HTTP headers, HTML code, and other components of a website to determine the software, content management systems (CMS), server types, scripting languages, and various other details that might be running on the web server.
* whatweb --help shows all available options  
  
* Set Aggression levels (1 **default**, 3, or 4) using --aggression (1,3,4)  
    
  
* Use -v to make returned info more readable (verbose option)
* 
* Use --no-errors to not output error codes in results
* Can use to scan domain name, IP address, or range of IP addresses  
  
* To save scan output to file use the --log command  
  A screenshot of a computer

  Description automatically generated