OSINT

Website Recon

It is first important to take a look at the companies website for any information that could be useful, such as email addresses, twitter accounts, and other social media linked to the company.

Whois Enumeration

Running the linux `whois` command could be very helpful in getting info on a company. It also lists dns name servers, which could be useful for later in the pen test. If you know the ip, you can also do a reverse lookup using the command `$ whois <ip>`

Google Hacking

Google has different operators that help to narrow down searches. Here are some useful ones:
`site:mtggoldfish.com`
`filetype:php`
`intitle:"index of" "parent directory"` (Helpful for finding open directories)
`ext:<file-extension, such as pl for perl or jsp(java server pages)>`
You can also use the minus sign (-) to exlude certian terms:
`site:reddit.com -filetype:html`

The Google Hacking Database also has some more search quieries that can help find specific info.