Performing Target Recon

Document Metadata

Let start with the documents metadata first.

Document metadata is additional information that is attached to a document file, providing context and details about that document.

In Simple terms, Think of a document as a book. The words and content inside are like the story of the book. Metadata is all the extra information on the book's cover and first few pages that tells you more about the book itself.

So, to gather documents related to our target. We can use google dorks.

Suppose our target is dell.com.

```
site:dell.com filetype:pdf
```

```
wget <URL>
```

Now once the file is downloaded we will use exiftool to find interesting metadata from the documents.

```
$ exiftool reseller-terms-of-sale.pdf
```

So this gives out a lot of information, we have found potential dell employees, the software they are using and their email address.

We can also automate the document search and the viewing of metadata using Metagoofil and Metafoge.

So first we will discover and download all the documents related to our target using Metagoofil.

```
sudo metagoofil -w -d dell.com -l 10 -n 20 -t pdf,doc,docx -o
~/Desktop/Dell
```

Now that we have discovered and downloaded the documents related to the target, we can use metaforge on it to display its metadata.

```
cp ~/Desktop/*.* ~/Desktop/Metaforge/media

python3 metaforge.py
```

Client Fingerprinting

The Next technique to perform Target Recon is Client Fingerprinting. In this technique, we try to find out which client software like browser and OS, the target is using.

To do this, we can make use canary tokens.

Canary Tokens - canarytokens.org

- Once the victim clicks on the link, we can deduce information like OS and Browser used.

Now that we know about the target organization's employee names, their email addresses, the Operating system and browser in use, which ISP they are using and where they are located. With all this information, we can tailor specific spear phishing campaigns on these employees and if one of them, gets trapped we will have a initial access inside the target network.
