|  |  |  |
| --- | --- | --- |
| **Liza Kapopara** |  | **SEIT4530** |
| **21SE02IT025** |  | **Cryptography and network security** |

**ASSIGNMENT 6 Finding Live subdomain using Httprobe : command 1: cat folder/recon/final.txt | httprobe**

* cat folder/recon/final.txt:

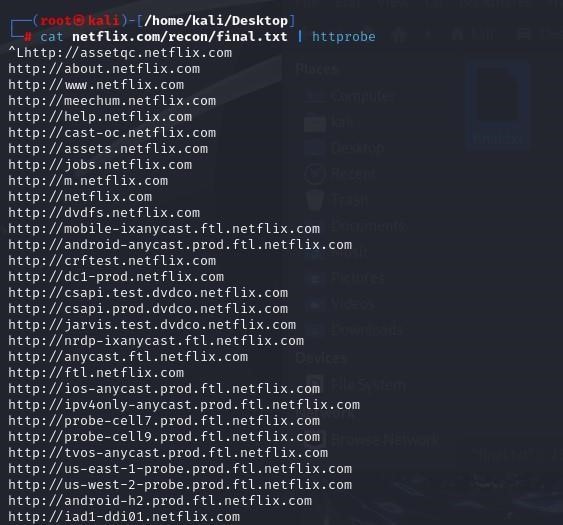
This command reads the contents of the file final.txt located in the folder/recon directory and outputs it to the standard output (usually the terminal).

* |:

This is a pipe. It takes the output of the command on the left (cat folder/recon/final.txt) and sends it as input to the command on the right (httprobe).

* httprobe:

httprobe is a tool that takes a list of domains or subdomains and checks whether they are alive by probing for HTTP or HTTPS services. It reads input line by line (in this case, the domains/subdomains from final.txt) and checks if the domain is alive by attempting to connect to it over HTTP or HTTPS. The result is a list of live subdomains.



**Meghavi Lodaliya SEIT4530**

**21SE02IT031 Cryptography and network security**

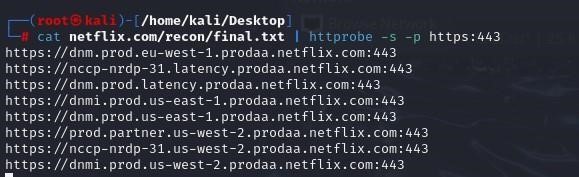
# Command 2: cat folder/recon/final.txt | httprobe -s -p https:443

* httprobe -s:

The -s option forces httprobe to use HTTPS only. This means it will only check if the subdomains are alive on the HTTPS protocol.

* -p https:443:

The -p option allows you to specify a port for the protocol. In this case, it&#39;s explicitly specifying port 443 for HTTPS. While https usually defaults to port 443, this command makes it explicit.



# Command 3: cat folder/recon/final.txt | httprobe -s -p https:443 | sed &#39;s/https\?:\/\///&#39; | tr -d &#39;:443&#39;

* | sed &#39;s/https\?:\/\///&#39; sed is a stream editor used for parsing and transforming text.

This specific sed command uses a regular expression to remove the http:// or https:// prefix from each URL.

The s indicates substitution, and https\? matches http or https. The \? makes the preceding character optional.

The :\/\// matches the :// part of the URL, and the whole match is replaced with an empty string (i.e., removed).

* | tr -d &#39;:443 tr is a command used for translating or deleting characters.

The -d option tells tr to delete specific characters. In this case, it deletes :443 from the URL, which is the port specification for HTTPS.

