LAB 3

Passive and active reconnaissance

1. Banner grabbing - use telnet to do banner grabbing against any of the other virtual machines like this:

telnet {IP address} {port number} . Try port numbers 21,22 , 25 ,80 ,110 ,443 , 3389

Try to perform the same against a real web server on your choice.

A program called netcat can also do the same function instead of telnet. Please try it!

Type in : nc {IP address of the machine } {port number}

2. Google hacking

Commands:

Filetype – directs google to search only within the test of a particular type of file.

Inurl – this operator directs Google to search only within the specified URL of a document

Link – search only within hyperlinks for a specific term –

Intitle – Search for a term in the title of the document

Here are some examples.

Please be careful ,some of the links could lead to a honeypot !

Please check the following link:

https://www.google.dk/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=inurl%3Aadmin.php

Try to connect to any of the servers listed. What do you see?

3. Run the following command: intitle:admbook+intitle:version+filetype:php

4. Next command: allinurl:tsweb/default.htm

5. DNS servers

Type in the following command: nslookup google.com.Run commands dig and fierce. Compare the results from all 3 of them.

6. Using shodan website – navigate to shodanhq.com and register there.

Commands:

country: filters results by two letter country code

hostname: filters results by specified text in the hostname or domain

net: filter results by a specific IP range or subnet

os: search for specific operating systems ν port: narrow the search for specific services

Launch the command: apache country: DK

Next command: apache hostname:dk