**TASK-4**

To Find:

5 ROUTERS

5 PRINTERS

5 WEB CAMERAS

which are connected in open network having default username/password vulnerability.

Condition:

USE GOOGLE DORKS ONLY AND GAIN THE ACCES.

Summary:

In this document we are going to use google dorks to find out the publicly available printers, routers and webcams that are vulnerable to default username and password vulnerability.

DEFAULT USERNAME/PASSWORD VULNERABILITY:

This is a vulnerability where few pre-defined sets of

username and passwords when applied to devices give the

access the to the website such vulnerabilities are what the

hackers check in the first place.

To find ROUTERS:

Google dork: intitle:"router"inurl:"home.asp"

I found this google dork in the Google hacking data base (GHDB) which helps to find the routers available in open network.

Router 1:

<https://files.i4wifi.cz/inc/_doc/Promo/WA-2204A/home.asp.htm>

Graphical user interface

Description automatically generated with medium confidence

Router 2:

<http://www.corky.co.uk/home.asp>

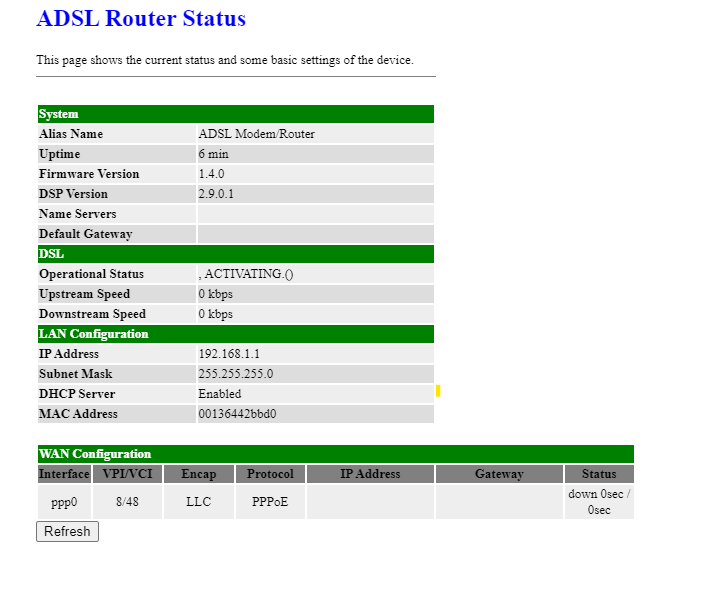
Text, letter

Description automatically generated

Router 3:

<https://www.joyce.cz/files/technicka-podpora/managementy/WELL/PTI-8411g/status-1.asp.htm>

Google dork: intitle:"router"inurl:"1.asp"



Router 4:

<http://81.16.122.79/index.htm>

Google Dork: intitle:"router"inurl:"81.asp"

The following router is vulnerable for default username and password, where the default password being admin.

Graphical user interface

Description automatically generated

The following page appears after using default password.

Graphical user interface, website

Description automatically generated

Router 5:

Google Dork: intitle:"router"inurl:"145.asp"

<http://91.183.145.195:8080/login.cgi>

Graphical user interface, application

Description automatically generated

To find Printers:

The google dork that can be used is: inurl:printer/main.html

Printer 1:

<http://188.26.120.48/admin/plock.html>



This printer is vulnerable for default username and password vulnerability where username is admin and password is access.

Graphical user interface, application

Description automatically generated

This is the admin dashboard for the printer.

Printer 2:

<http://ps-km20p-z211.mat.fce.vutbr.cz/admin/password.html>



The default usernames and passwords are given here, and it is vulnerable to default username and password vulnerability.

Printer 3:

<http://201.0.21.240/printer/main.html>

Graphical user interface

Description automatically generated

This printer is vulnerable for default username and password vulnerability where username is admin and password is access.

Printer 4:

<http://146.57.32.206/user/prnset.html>

Graphical user interface, text, application

Description automatically generated

This printer is vulnerable for default username and password vulnerability where username is user and password is access.

This is the user admin page for the following printer.

Graphical user interface

Description automatically generated

Printer 5:

<http://88.119.159.46/admin/administrator_settings.html>

Graphical user interface, text, application

Description automatically generated

The default usernames and passwords are given here, and it is vulnerable to default username and password vulnerability.

To find Webcams:

We can use the Google Dork: inurl:"webcamxp 5"

This helps us to find out the cameras that are connected in an open network.

Webcam 1:

<http://24.144.198.239:8585/>

Webcam 2:

<http://91.233.46.24:8014/>

Webcam 3:

<http://186.67.227.66:8080/>

Webcam 4:

<http://75.149.26.30:1024/>

Webcam 5:

<http://186.67.227.66:8080/>

Conclusion:

As we can see above,

We have used google dorks to find out the publicly available printers, routers and web cameras in the open network.

We have also tested then for default username and password vulnerability, which showed that some of them had the default username and password vulnerability.

This vulnerability has severe impact as the attacker can access the administrator dashboard and can make changes to the entire system.