

**IE4012**

**Offensive Hacking: Tactical and Strategic**

**4th Year, 1st Semester**

Lab Report

**NETGARAGE IO WARGAME**

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the

Bachelor of Science Special Honors Degree in Information Technology

02/03/2020

**Declaration**

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

Registration Number: IT17108546

Name: Jayawardhana D D T

**Table of Contents**

[1. Solutions to NetGarage IO levels 1](#_Toc34078556)

[Level01 1](#_Toc34078557)

[Level02 1](#_Toc34078558)

[2. References 2](#_Toc34078559)

**List of Figures**

Figure 2.1 Getting hold of the SL Army personnel……………………………………………3

Figure 2.2 Intitle search query…………………………………………………………………4

Figure 2.3 inurl search query…………………………………………………………………..4

Figure 2.4 filetype search query……………………………………………………………….5

Figure 2.5 site search query……………………………………………………………………6

Figure 2.6 Information gathered through Shodan……………………………………………..7

Figure 2.7 results for available webcams……………………………………………………...8

Figure 2.8 Webcam feed………………………………………………………………………8

Figure 2.9 Webcam feed………………………………………………………………………9

Figure 2.10 Search result of ‘tplink’ search query…………………………………………...10

Figure 2.11 Login interface of the router…………………………………………………….10

Figure 2.12 Details of the router……………………………………………………………..11

Figure 2.13 Search results of query ‘slt.lk’…………………………………………………..11

Figure 2.14 slt.lk website information………………………………………………………..12

Figure 2.15 slt.lk website information………………………………………………………..12

List of Acronyms and Abbreviations

EDGAR:Electronic Data Gathering, Analysis and Retreival System 5

i.e:that is 9

IDS:Intrusion Detection System 5

IoT:Internet of Things 9

IP:Internet Protocol 9

IPS:Intrusion Prevention System 5

PHI-Protected Health Information 5

PII-Personally Identifiable Information 5

SL:Sri Lanka 6

URL:Uniform Resource Locator 7

# Solutions to NetGarage IO levels

Netgarage IO is a war-game developed so that aspiring ethical hackers and cyber security students can increase their practical skills in assembly language. According to its website, it currently has levels up to the 33rd level. However, in this document, only the first 2 levels will be explored.

To begin the game, you should visit the official site of Netgarage IO;

**https://io.netgarage.org/**

The website gives you an overall idea about the game and there have been many write-ups and walkthroughs written in multiple languages to explain the process and procedure to be followed in order to advance through the levels.

## Level01

As the official website points out, we need to use **‘ssh’** in order to login to the war-game. The format to be followed for establishing the connection and the username with the password is given for one to enter level 01.

This can be done in two ways.

* Through Putty – Download and install Putty and use Putty to connect to the wargame.
* Through command prompt – use the ‘ssh’ command in the command prompt to login to the first level.

The method explained in this article follows the process of playing the wargame through the command prompt in a Windows 10 machine.

To enter into the first level, the following command should be typed in the command prompt.

**ssh level1@io.netgarage.org**

Entering the password which is ‘**level1**’ will land you in level 01.

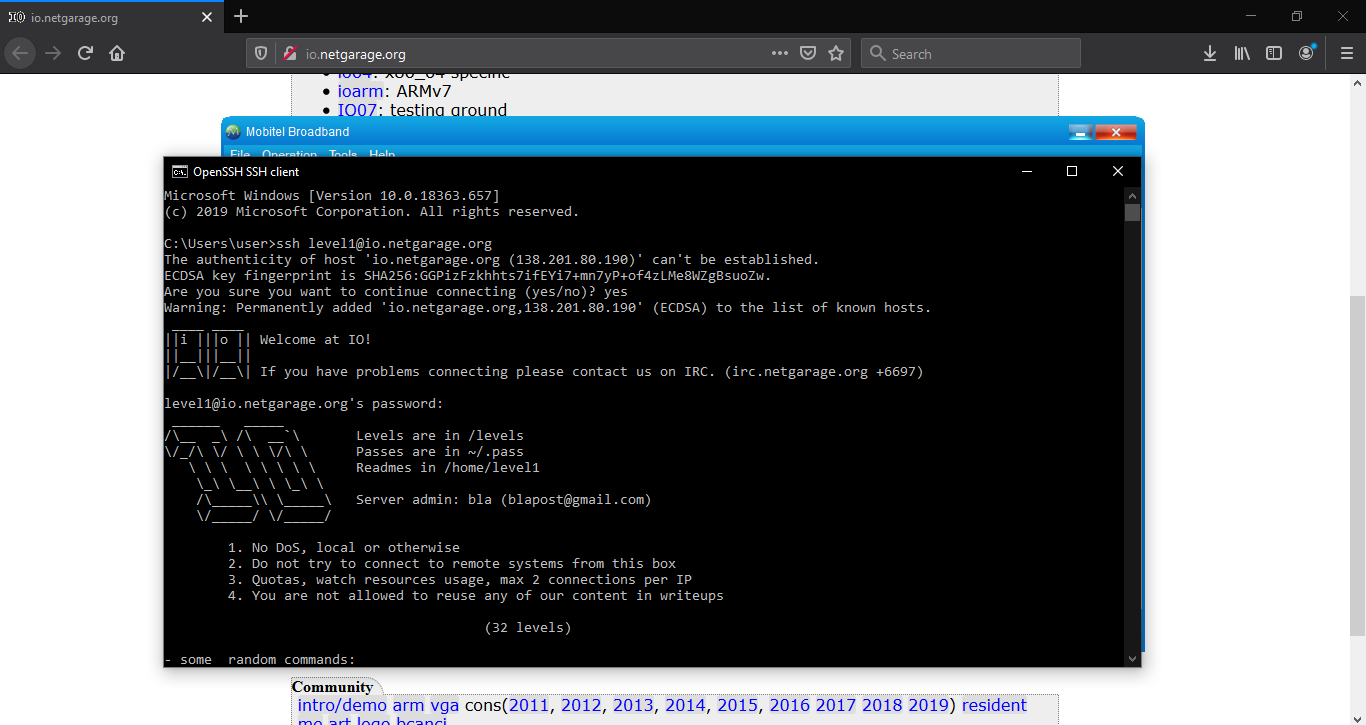
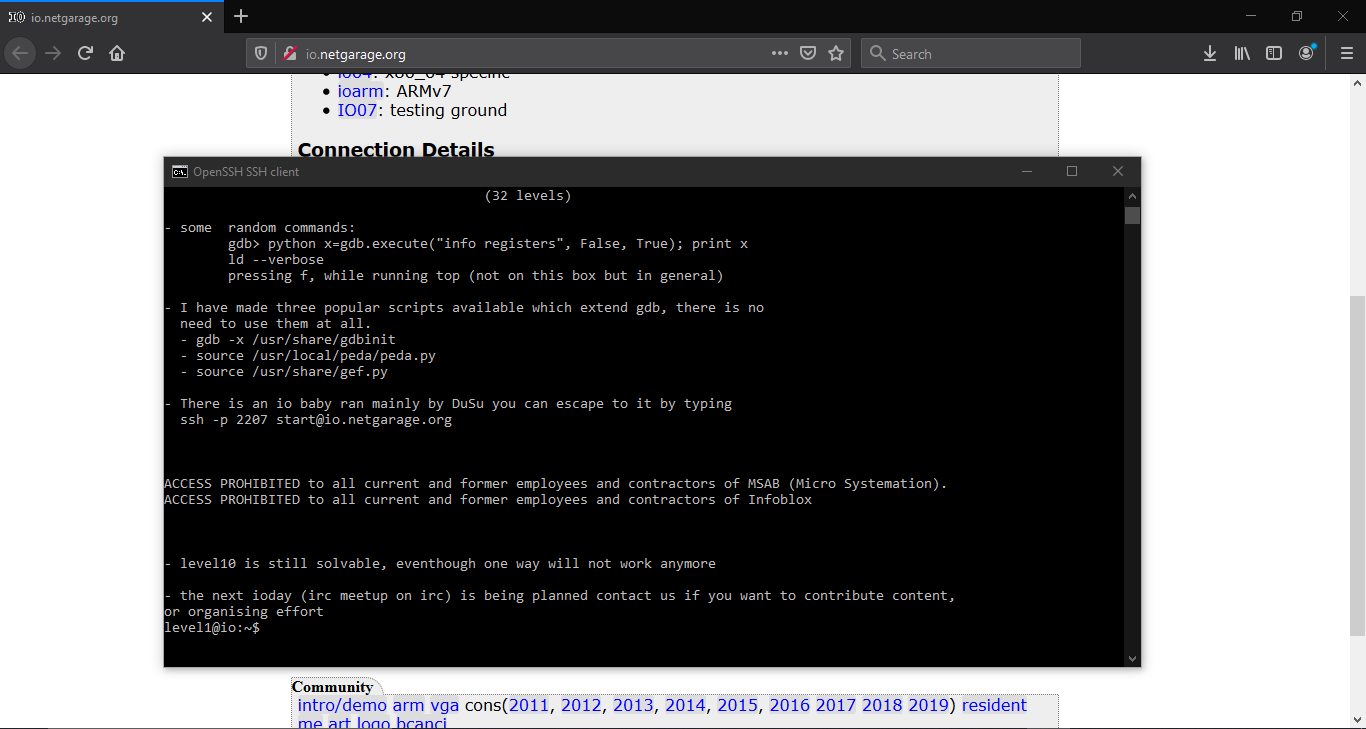


Figure .2: Initial Interface of Level1

Figure .1: Logging into Level1

Inside level 1, there is a folder called ‘levels’ in the root directory. When accessing this, one can observe files of different formats named after different levels to be within the directory.

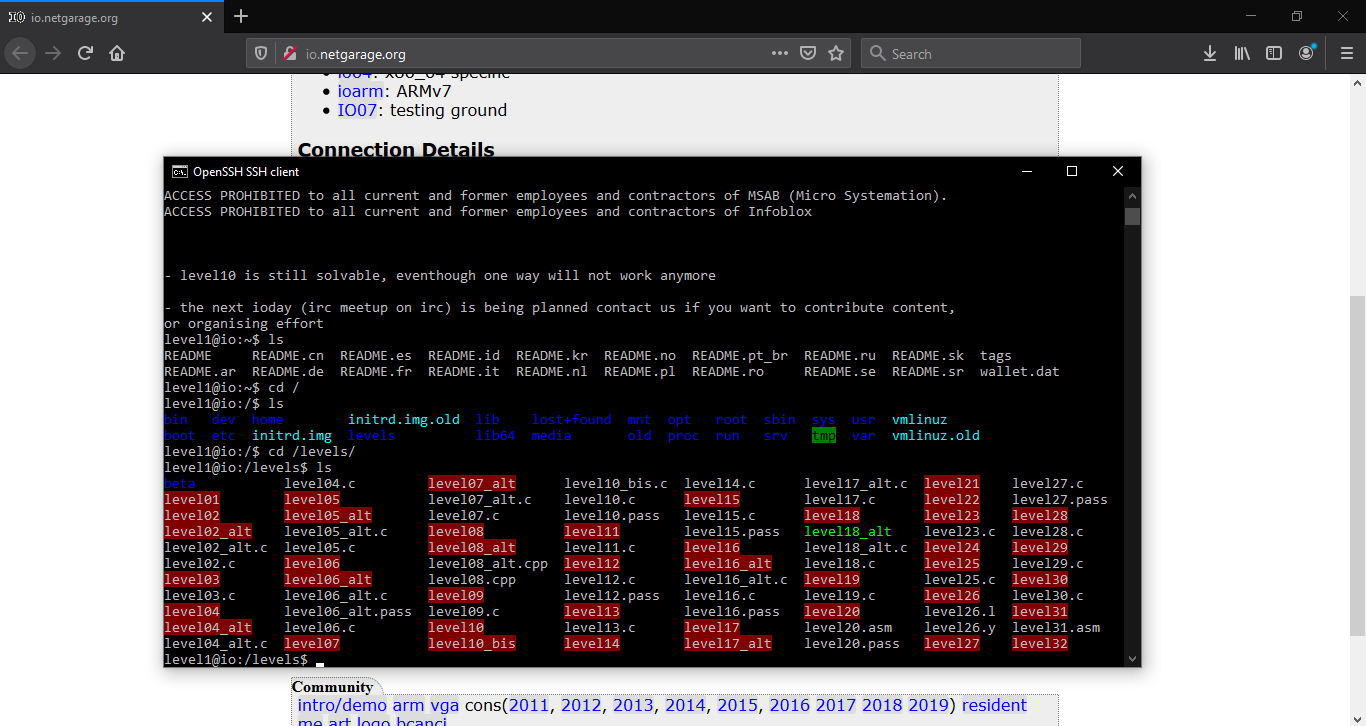


Figure .3: File Structure of the 'levels' Directory

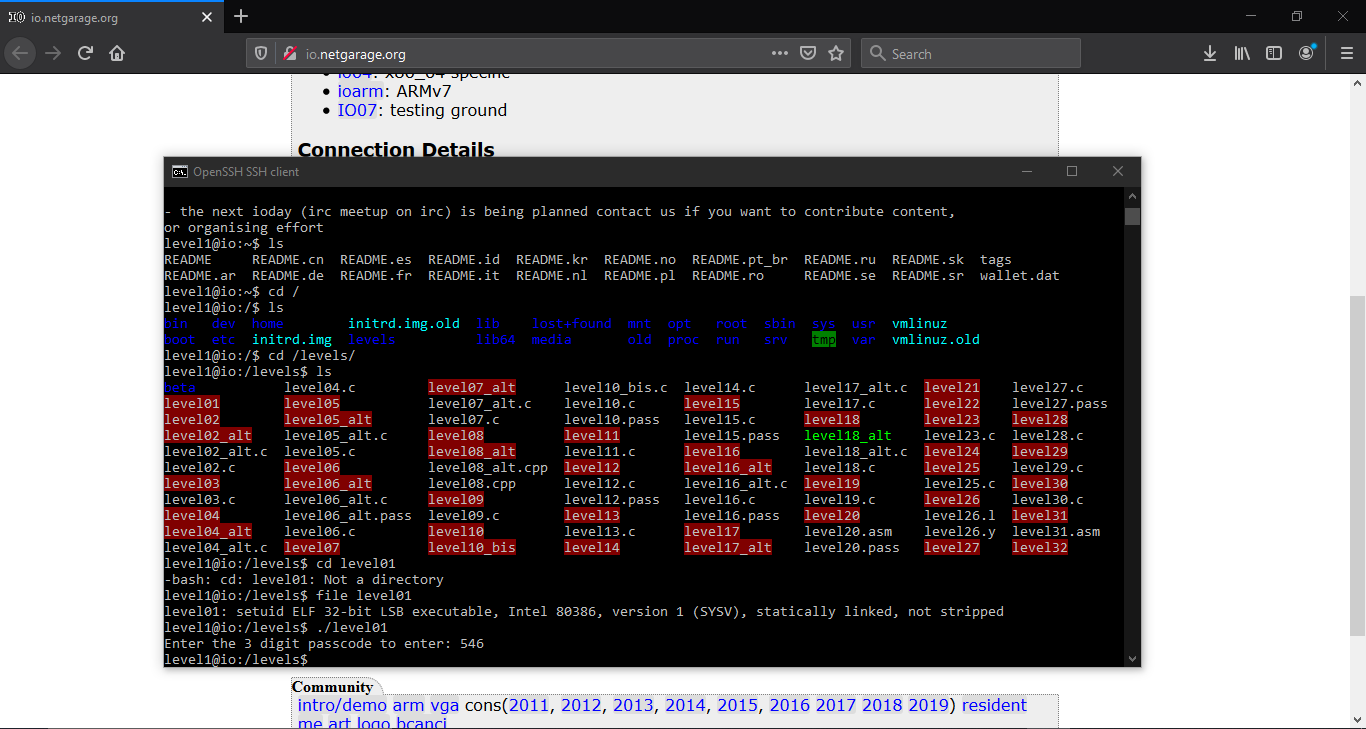


Figure .4: Trying to Execute 'level01' File

## Level02

# References

[1] Jitendra Kumar Singh, The Art of Reconnaissance: Information Gathering Techniques. Available: [https://www.udemy.com/the-art-of-reconnaissance-information-gathering-techniques/?couponCode=JUNE2018&site\_ref=discudemy.com](https://www.udemy.com/the-art-of-reconnaissance-information-gathering-techniques/?couponCode=JUNE2018&site_ref=discudemy.com%20) [online]

[2] g2rrard, Passive VS Active Information Gathering. Available: [http://themitigators.com/index.php/2018/10/10/passive-vs-active-information-gathering/](http://themitigators.com/index.php/2018/10/10/passive-vs-active-information-gathering/%20) [online]

[3] Sachin Wagh. Information gathering – first step of hacking. Available:[https://secur1tyadvisory.wordpress.com/2015/07/10/information-gathering-first-step-of-hacking/](https://secur1tyadvisory.wordpress.com/2015/07/10/information-gathering-first-step-of-hacking/%20) [online]

[4] Johnny Long, Google Hacking for Penetration Testers. Available: [http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf](http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf%20) [online]

[5] J.M Porup, What is Shodan? The search engine for everything on the internetAvailable: <https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html> [online]

[6] Banner Grabbing. Available: <https://en.wikipedia.org/wiki/Banner_grabbing> [online]