# Laboratory Footprinting and Reconnaissance

# What we will learn in this laboratory

1. Setting a hacking virtual machine in Microsoft Azure
2. Footprinting concepts
3. Footprinting through Search Engines and Advanced Google Hacking
4. Footprinting through Web Services and Social Networking Sites
5. Website Footprinting
6. Network Footprinting

**This is an invented story for academic purposes, the companies mentioned here are not malicious in any way:** A malicious activity has been detected from different companies around world. Your mission is to perform a **Passive** and **Active** Footprinting to get the most amount of information from those companies and build a blueprint with the **security profile** of the suspect organization.

Suspect organizations:

* NEC Laboratories Europe GmbH.

<https://uk.nec.com/en_GB/emea/about/neclab_eu/index.html?>

* Facultad de Informática, Universidad de Murcia.

<https://www.um.es/informatica/>

* Laboratorio de Informática, Escuela Colombiana de Ingeniería.

<http://laboratorio.is.escuelaing.edu.co/>

**Your mission is:** Choose one of the 3 target organizations and make a full footprinting using: footprinting through search engines and Advanced Google Hacking, footprinting through Web Services and Social Networking Sites, Website footprinting and network footprinting, amongst others, to get the most available and public information from the company and build a blueprint (report) that contains the target security profile.

1. **Connecting to Microsoft Azure**

To achieve this mission, you are provided with some services in Microsoft Azure, which are accessed following these steps:

1. Connect to the following webpage and select “Activate”:

<https://azure.microsoft.com/en-in/free/students/>

1. Then, log in with your student’s credentials, for example:

[juan.perez@urosario.edu.co](mailto:juan.perez@urosario.edu.co)

1. Read the FAQ of the program “Azure for Students” at:

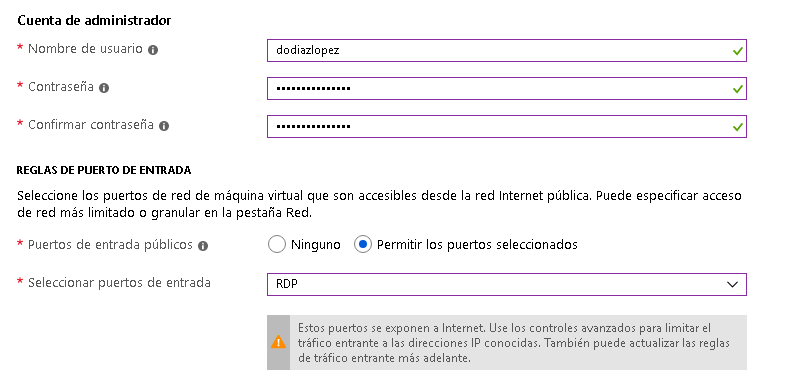
<https://azure.microsoft.com/es-es/free/free-account-students-faq/>

1. You can check your credits at <https://www.microsoftazuresponsorships.com/>
2. To connect to Azure follow this URL: <https://portal.azure.com/>

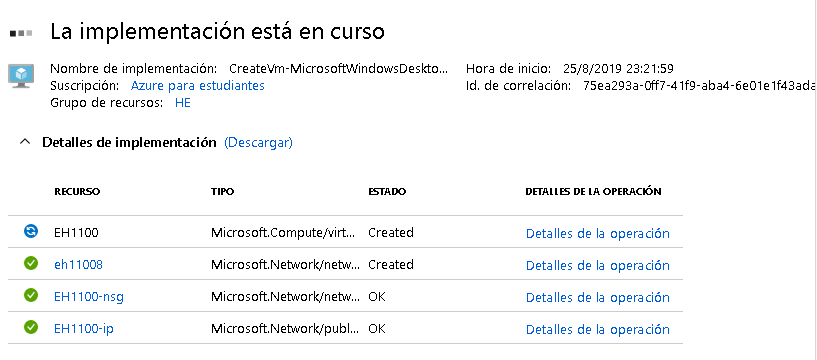
**Creating your first virtual Machine in Azure:**

1. Login in Azure through this URL <https://portal.azure.com/>
2. Go to the section “Virtual Machines” in the left panel
3. Press “Add” (Agregar)
4. Create and select a “Resource Group”
5. Create a Virtual machine with the following data and select “Review and Create”:

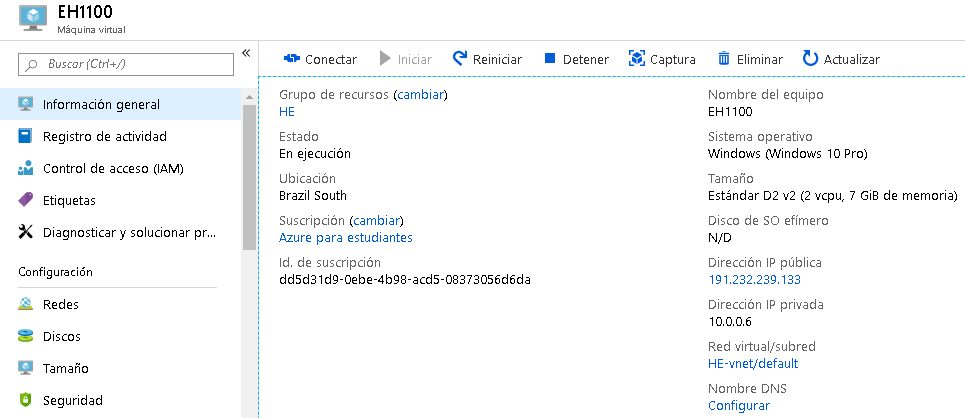




1. When the Virtual machine is getting created, you will see an image like the following:

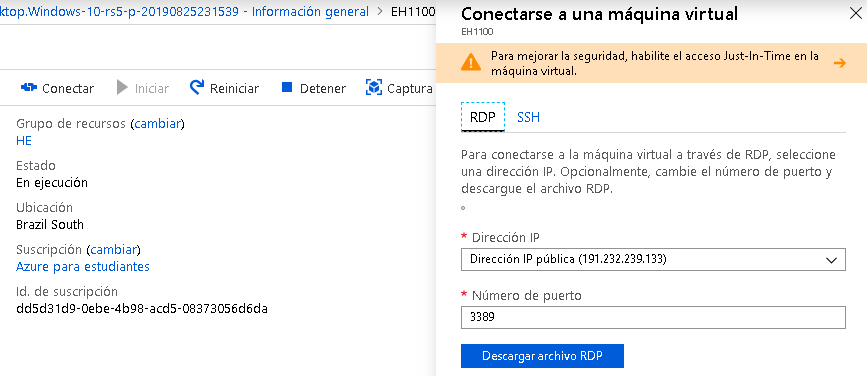


1. **After** the virtual machine is created, you may select “Go to the resource” and you should see the following image:

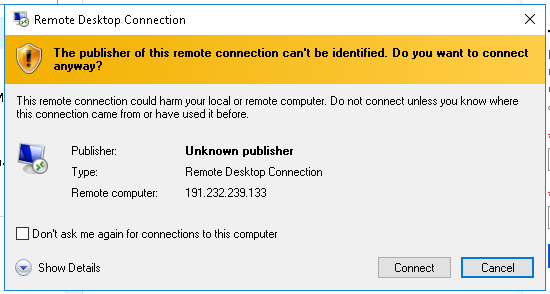


|  |
| --- |
| **Task:** Include in the report the screenshot of your windows virtual machine deployed in Azure that include the public IP and the date of execution |

1. Then, you can connect to the virtual machine through the bottom “Connect” (Conectar), and download the RDP file:

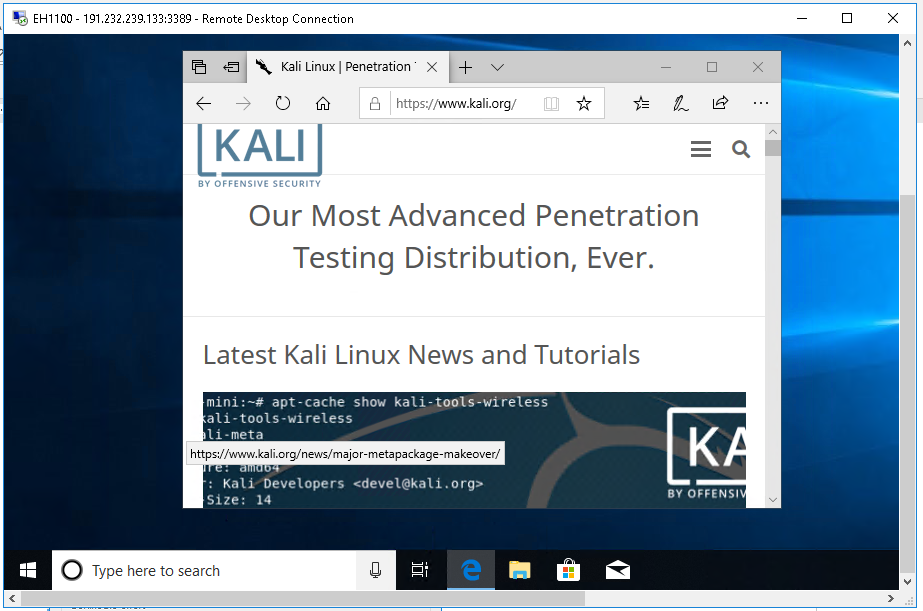


1. In Windows you can make double click on the file to open a remote session to the virtual machine.



|  |  |
| --- | --- |
|  |  |

Then you have a Windows Virtual Machine to achieve your mission:



**Now, execute all the following steps from the Windows Virtual Machine that you have just created in the previous procedure.**

1. **Footprinting concepts**

Footprinting

* **Definition:** It is to gather public information about the target to identify the ways to make an intrusion.
* **The main output of a footprinting:** A blueprint with the security profile of the target containing for example: Organization information, Network information, System information.

Types:

* **Passive**: Without direct interaction with the target. Examples:
  + Find information in search engines
  + Find TLD (Top-Level-Domains) and subdomain of a target
  + Find out physical location
  + Find out about people related with the target using social networks
  + Ask financial services
  + Find out infrastructure details through job sites
  + Ask groups, forums, blogs
  + Find out operating systems
  + Consult internet archives
  + Perform intelligence
  + Monitor website traffic
  + Track reputation
* **Active**: With direct interaction with the target
  + Querying name servers of the target
  + Extract metadata of published documents
  + Gather website information through web spidering and mirroring
  + Use an email tracking
  + Whois lookup
  + DNS information
  + Tracerroute analysis
  + Social Engineering

1. **Footprinting through Search Engines and Advanced Google Hacking**

* Search by the name of the target in major search engines: Google, Bing, Yahoo, Ask, Aol, Baidu, DuckDuckGo.
* Use advanced search at

<https://www.google.com/advanced_search>

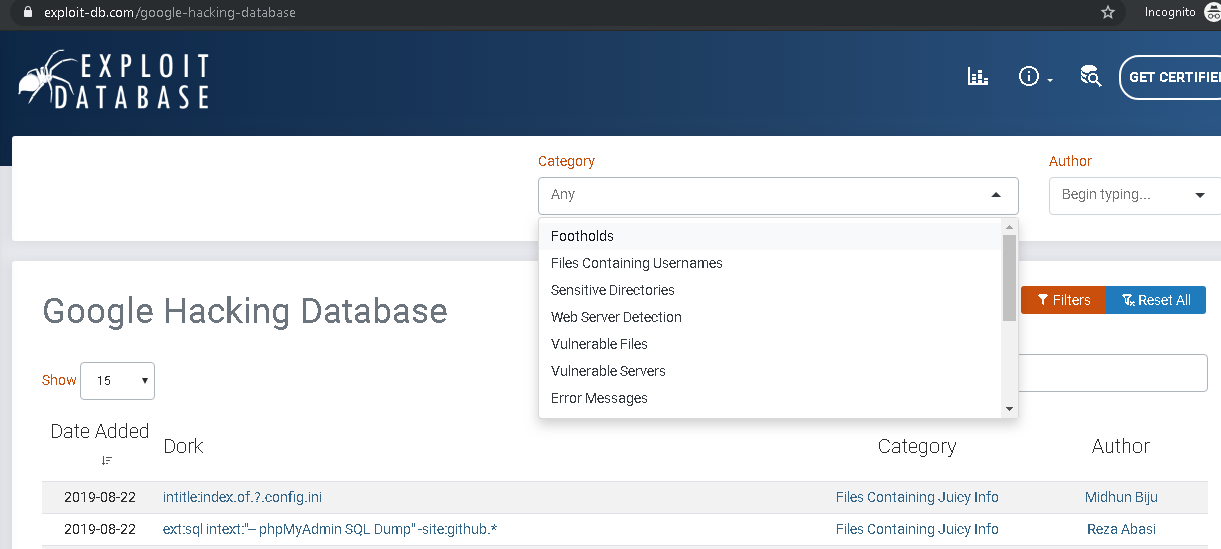
* Use advanced image search at

<https://www.google.com/advanced_image_search>

* Use Google Hacking Techniques: cache, link, related, info, site, allintitle, intitle, allinurl, inurl, location, etc. More info:

<http://www.googleguide.com/advanced_operators_reference.html>

* Connect to Google Hacking Database through this link: <https://www.exploit-db.com/google-hacking-database>



Explore the different categories available in GHDB (Google Hacking Database). Try specially the following queries:

* 1. Category: Footholds:
     + intitle:"FCKeditor - Uploaders Tests"
     + inurl:/phpmyadmin/index.php?db=
  2. Category: Files containing username
     + inurl:admin inurl:userlist
  3. Category: sensitive directories
     + type:mil inurl:ftp ext:pdf | ps
  4. Category: Web server detection
     + inurl:phpinfo.php intext:build 2600
  5. Category: vulnerable files
     + allinurl:forcedownload.php?file=
  6. Category: Vulnerable servers
     + inurl:"/user/register" "Powered by Drupal" -CAPTCHA -"Access denied"
  7. Category: Error messages
     + intext:"Access denied for" intitle:"Shopping cart"
  8. Category: Files Containing Juicy Info
     + site:https://docs.google.com/spreadsheets edit
  9. Category: Files -Containing Passwords
     + inurl:users.json "username"
  10. Category: Sensitive Online Shopping Info
      + inurl:midicart.mdb
      + intext:"Dumping data for table `orders`"
  11. Category: Network or Vulnerability data
      + inurl:nagios/cgi-bin/status.cgi
  12. Category: Pages Containing Login Portals
      + inurl:/admin/index.php
  13. Category: Various Online Devices
      + inurl:app/kibana intext:Loading Kibana
      + allintitle:"3cx phone system management console"
  14. Category: Advisories and Vulnerabilities
      + site:connect.garmin.com inurl:"/modern/profile/"
      + intext:"Powered by 74cms v5.0.1"

|  |
| --- |
| **Task:** Create a section in your report that contains:   * The results of the use of footprinting through Search Engines * At least one result for any 7 categories of the Google Hacking Database * **Most important answer of this section:** Explain how the information that you have just found in this section can be useful to perform an attack.   **Note:** Important data is sensitive files, error message with sensitive information, files with passwords, logon portals, network logs, software version information, web app source code, information about employees, or any information from the target that can be usable. |

1. **Footprinting through Web Services and Social Networking Sites**

* Identify all the subdomains (for example: empleados.urosario.edu.co, biblioteca.urosario.edu.co, campus.urosario.edu.co, etc) of the target using:
  + <https://www.netcraft.com/>
  + Use the “Sublist3r” script to identify all the subdomains of the target: <https://github.com/aboul3la/Sublist3r>

|  |  |
| --- | --- |
|  |  |

* Identify the location of the target using
  + <https://www.google.com/map>
  + <https://wikimapia.org/>
  + <https://maps.yahoo.com/b>
  + <https://www.bing.com/maps/>
* Find people working on the target using webpages like:
  + [www.facebook.com](http://www.facebook.com)



* + [www.intelius.com](http://www.intelius.com)
  + [www.beenverified.com](http://www.beenverified.com)
  + <https://www.spokeo.com/>
* Run InSpy script for linkedin
  + <https://www.leapsecurity.io/blog/linkedin-enumeration-inspy/>
* Job sites:
  + <https://www.linkedin.com/jobs/>
  + [www.elempleo.com](http://www.elempleo.com)
  + [www.indeed.com](http://www.indeed.com)
* Search operative systems
  + <https://www.shodan.io/search?query=bogota>
  + <https://www.netcraft.com>
  + <https://censys.io/ipv4/201.234.181.59>

|  |
| --- |
| **Task:** Create a section in your report that contains:   * Information obtained from Web services and Social Networking Sites related to target employees or people related with the target, which can be useful for a future attack. * Execute the code of sublist3r.py, identify the subdomains of the target, and test if some of them work. * **Most important answer of this section:** Explain how the information that you have just found in this section can be useful to perform an attack. |

1. **Website Footprinting**

Identify important data of the target using website footprinting techniques like:

* Data extractor: Names, Extract emails, contact details, phones, fax, URLs from files from different types
  + <http://www.spadixbd.com/elink/index.htm> (Install on your windows virtual machine)
  + <http://www.webextractor.com/download.htm> (Install on your windows virtual machine)
* Mirroring websites using:
  + <http://www.httrack.com/> (Install on your windows virtual machine)
  + <http://www.spadixbd.com/rafabot/index.htm> (Install on your windows virtual machine)
  + <https://archive.org/> (Identify interesting information of the target that can be obtained from previous webpage snapshots)
* Extract metadata from the public files of the target
  + <https://www.elevenpaths.com/labstools/foca/index.html>

|  |
| --- |
| **Task:** Create a section in your report that contains:   * Names, Extract emails, contact details, phones, fax or urls obtained from **spadixbd** OR **webextractor**. * Metadata of the target obtained from FOCA. * **Target directory structure** obtained from a mirroring of the target website using HTTRACK * **Most important answer of this section:** Explain how the information that you have just found in this section can be useful to perform an attack. |