

Cifrado de Hill

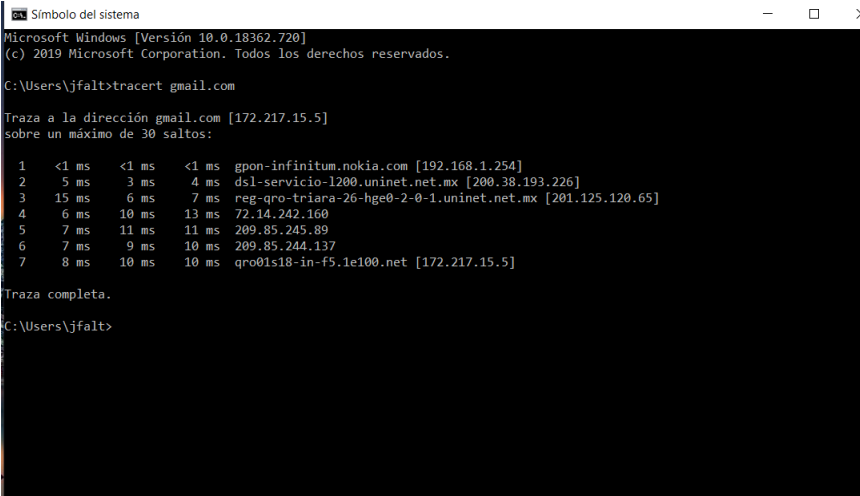
Proyecto1

Altamirano Vázquez Jesús Fernando
Sánchez Sarmiento Eric
Rubí Rojas Tania Michelle

18 de marzo del 2020

1. Traceroute

traceroute nos permite seguir la pista de los paquetes que vienen desde un host (punto de red). Cuando ejecutamos el comando traceroute (tracert en windows) obtenemos una aproximación de la latencia de red de esos paquetes, lo que es una estimación de la distancia a la que están los extremos de la comunicación.



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.18362.720]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\jfalt>tracert gmail.com

Traza a la dirección gmail.com [172.217.15.5]
sobre un máximo de 30 saltos:

 1  <1 ms  <1 ms  <1 ms  gpon-infinity.nokia.com [192.168.1.254]
 2  5 ms   3 ms   4 ms   dcl-servicio-1200.uninet.net.mx [200.38.193.226]
 3  15 ms  6 ms   7 ms   reg-qro-triara-26-hge0-2-0-1.uninet.net.mx [201.125.120.65]
 4  6 ms   10 ms  13 ms  72.14.242.160
 5  7 ms   11 ms  11 ms  209.85.245.89
 6  7 ms   9 ms   10 ms  209.85.244.137
 7  8 ms   10 ms  10 ms  qro01s18-in-f5.1e100.net [172.217.15.5]

Traza completa.

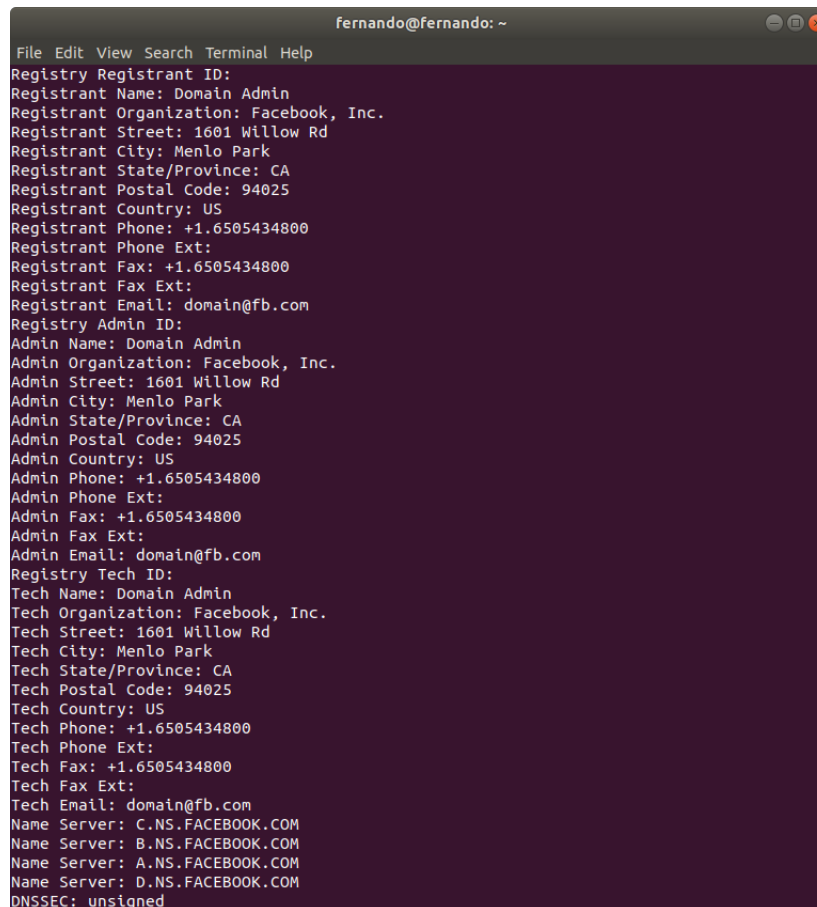
C:\Users\jfalt>
```

Figura 1: traceroute

2. Whois

whois es un protocolo de transmisión TCP que se utiliza para efectuar consultas en una base de datos, y que contiene gran información acerca de diferentes

dominios registrados. También sirve como intermediario entre la ICANN, la cual es la compañía encargada de la asignación de nombres y números en internet, y los registradores de dominios.

A terminal window titled 'fernando@fernando: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal displays the output of a 'whois' command, showing registration details for a domain owned by Facebook, Inc. in Menlo Park, CA. The output includes Registry and Admin information, contact details, and DNS server information.

```
Registry Registrant ID:  
Registrant Name: Domain Admin  
Registrant Organization: Facebook, Inc.  
Registrant Street: 1601 Willow Rd  
Registrant City: Menlo Park  
Registrant State/Province: CA  
Registrant Postal Code: 94025  
Registrant Country: US  
Registrant Phone: +1.6505434800  
Registrant Phone Ext:  
Registrant Fax: +1.6505434800  
Registrant Fax Ext:  
Registrant Email: domain@fb.com  
Registry Admin ID:  
Admin Name: Domain Admin  
Admin Organization: Facebook, Inc.  
Admin Street: 1601 Willow Rd  
Admin City: Menlo Park  
Admin State/Province: CA  
Admin Postal Code: 94025  
Admin Country: US  
Admin Phone: +1.6505434800  
Admin Phone Ext:  
Admin Fax: +1.6505434800  
Admin Fax Ext:  
Admin Email: domain@fb.com  
Registry Tech ID:  
Tech Name: Domain Admin  
Tech Organization: Facebook, Inc.  
Tech Street: 1601 Willow Rd  
Tech City: Menlo Park  
Tech State/Province: CA  
Tech Postal Code: 94025  
Tech Country: US  
Tech Phone: +1.6505434800  
Tech Phone Ext:  
Tech Fax: +1.6505434800  
Tech Fax Ext:  
Tech Email: domain@fb.com  
Name Server: C.NS.FACEBOOK.COM  
Name Server: B.NS.FACEBOOK.COM  
Name Server: A.NS.FACEBOOK.COM  
Name Server: D.NS.FACEBOOK.COM  
DNSSEC: unsigned
```

Figura 2: whois

3. Nslookup

nslookup es una herramienta de línea de comandos, cuya función básica es encontrar la dirección IP de un equipo determinado o realizar una búsqueda de el nombre de dominio de una determinada dirección IP.

```
fernando@fernando: ~  
File Edit View Search Terminal Help  
(base) fernando@fernando:~$ nslookup google.com  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   google.com  
Address: 172.217.15.14  
Name:   google.com  
Address: 2607:f8b0:4012:80a::200e  
(base) fernando@fernando:~$
```

Figura 3: nslookup

4. Google Hacking

Google Hacking cuenta con distintas herramientas para el "hacking" de información (la cual puede llegar a ser muy sensible) de distintos sitios web, entre sus herramientas estan intitle, inurl, site y filetype, haremos muestra del uso de esta última.

En la siguiente imagen mostraremos distintos sitios web, en donde algunos de ellos nos obsequian información delicada, en este caso esquemas de base de datos.

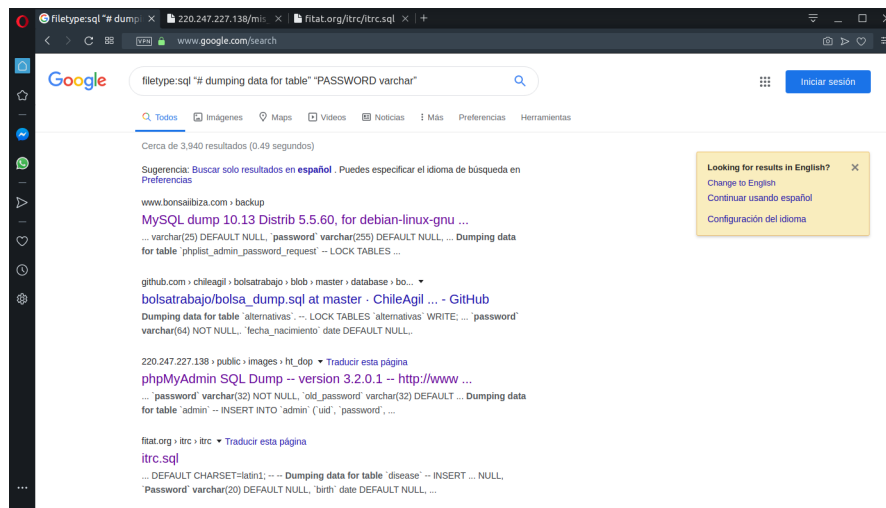


Figura 4: Sitios vulnerables

La siguiente imagen hace muestra parcial de uno de los esquemas vulnerables.

```
filetypesql "# dump" x 220.247.227.138/mis x Fitat.org/itrc/itrc.sql x +
220.247.227.138/mis_external/public/images/ht_dop.sql

-- phpMyAdmin SQL Dump
-- version 3.2.0.1
-- http://www.phpmyadmin.net
--
-- Host: localhost
-- Generation Time: Aug 20, 2010 at 03:53 AM
-- Server version: 5.1.36
-- PHP Version: 5.3.0

SET SQL_MODE="NO_AUTO_VALUE_ON_ZERO";

--
-- Database: 'ht_dop'
--
--
-- Table structure for table 'admin'
--
DROP TABLE IF EXISTS `admin`;
CREATE TABLE IF NOT EXISTS `admin` (
  `uid` varchar(20) NOT NULL,
  `password` varchar(32) NOT NULL,
  `old_password` varchar(32) DEFAULT NULL,
  `admin_level` varchar(10) NOT NULL,
  `mobile` varchar(10) NOT NULL,
  `status` int(2) NOT NULL DEFAULT '0',
  `online` binary(1) NOT NULL DEFAULT '0',
  `last_login` datetime DEFAULT NULL,
  `created_by` varchar(20) NOT NULL,
  `created_on` datetime NOT NULL,
  `mod_by` varchar(20) DEFAULT NULL,
  `mod_on` datetime DEFAULT NULL,
  ENGINE=InnoDB DEFAULT CHARSET=latin1;
--
-- Dumping data for table 'admin'
--
INSERT INTO `admin` (`uid`, `password`, `old_password`, `admin_level`, `mobile`, `status`, `online`, `last_login`, `created_by`, `created_on`, `mod_by`, `mod_on`)
VALUES
('administrator', '202cb962ac59075b964b07152d234b70', NULL, 'L0002', '0777459969', 0, '0', NULL, '-', '0000-00-00 00:00:00', NULL, NULL);
```

Figura 5: Esquema de una base de datos

Al igual que podemos obtener acceso a (en este caso) esquemas de bases de datos, también podemos acceder a, por ejemplo, cámaras. En la siguiente imagen mostraremos distintas IP's, las cuales muestran algunas cámaras accesibles, esto con ayuda de shodan.io .

The screenshot shows the Shodan.io search results for the query "linux upnp avtech country:ID". The interface includes a search bar, navigation tabs (Exploits, Maps, Download Results, Create Report), and a summary of results (20,763 total results). The results are categorized by top countries (Indonesia), top cities (Medan, Jakarta, Bandung, Surabaya, Tangerang), top services (HTTP, Andromouse, Qconn, Kerberos, NAS Web Interfaces), and top organizations (PT Telkom Indonesia, FirstMedia, Biznet Networks, PT. Eka Mas Republik). The detailed view shows three specific results, each with a login status, IP address, location, and technical details like HTTP status, date, server, connection, last modified, content type, ETag, and content length.

IP Address	Location	Service	Status	Date	Server	Connection	Last Modified	Content Type	ETag	Content Length
110.137.24.32	Indonesia, Medan	PT Telkom Indonesia	HTTP/1.1 200 OK	Thu, 19 Mar 2020 09:22:33 GMT	Linux/2.x UPnP/1.0 Avtech/1.0	close	Tue, 13 Dec 2016 05:40:55 GMT	text/html	372-15850-1481687655	15850
110.137.24.151	Indonesia, Jakarta Pusat	PT. Eka Mas Republik	HTTP/1.1 200 OK	Thu, 19 Mar 2020 09:30:42 GMT	Linux/2.x UPnP/1.0 Avtech/1.0	close	Mon, 07 Mar 2016 09:15:17 GMT	text/html	387-16695-1457342117	16695
110.137.24.151	Indonesia, Medan	PT Telkom Indonesia	HTTP/1.1 200 OK	Thu, 19 Mar 2020 09:08:46 GMT	Linux/2.x UPnP/1.0 Avtech/1.0	close	Tue, 13 Dec 2016 05:40:55 GMT	text/html	372-15850-1481687655	15850

Figura 6: Shodan.io: Cámaras vulnerables