Exercise1a: Google Hacking

1. Choose your organization(s) (or any website that may be of interest) and gather as much information as possible about it using Google and other open web resources.

2. Try organizing the details into the following categories as much as possible:

1) Organizational Structure (who's the boss? Who's the IT guy?)

Chair and CEO: Daryl J. Campbell,   Steven C. Preston

2) Domain names they own.

Goodwill.org

3) IP ranges / Server names they own.

IP ranges: 65.198.25.0 to 65.198.25.255

Server Name: ns10.goodwill.org

IP addresses 65.198.25.0 to 65.198.25.255

65.198.25.0 - 65.198.25.255 is an IP address range owned by Goodwill Industries of Orange County and located in United States - select an address below for more geolocation details

Nameserver ns10.goodwill.org

4) Phone numbers / Addresses.

15810 Indianola Drive Derwood, Maryland (Rockville mailing address), United States 20855

5) Emails and employee names, try to identify the job position of each employee found.

CHAIR LARRY DEJARNETT The LAMAR Group Palm Desert, CA
PRESIDENT AND CEO
JIM GIBBONS Goodwill Industries International Rockville, MD
VICE CHAIR Karla Grazier, CE Discover Goodwill of Southern and Western Colorado Colorado Springs, CO
TREASURER
Joan Y. McCabe Lipotriad, LLC Palm Beach Gardens, FL SECRETARY
Jeffrey Van Doren Jeffrey Van Doren, PLLC Blacksburg, VA BOARD MEMBERS
Michelle Belknap, CE Easter Seals-Goodwill Northern Rocky Mountain Great Falls, MT Tony Bell County of Spartanburg, SC Spartanburg, SC Richard Borer, CE Easter Seals Goodwill Industries Rehabilitation Center North Haven, CT Phillip Boyce Boyce & Associates Saratoga, CA Clark Brekke, CE Goodwill Industries of the Inland Northwest Spokane, WA Diana Burley, Ph.D. Institute for Information Infrastructure Protection The George Washington University Ashburn, VA Debie Coble, CE Goodwill Industries of Michiana South Bend, IN Ned Helms Concord, NH Joanne Hilferty, CE Morgan Memorial Goodwill Industries Boston, MA Larry D. Ishol Deloitte LLP Arlington, VA Brian Itzkowitz, CE Goodwill Industries of Arkansas Little Rock, AR Dale Jenkins Deloitte LLP Covington, LA Ronald Johnson Georgia Institute of Technology Atlanta, GA Michael W. Kempner MWW Group East Rutherford, NJ Steve Lufburrow, CE Goodwill Industries of Houston Houston, TX Robbin “Rob” Morton Morton Resources Inc. Macon, GA Anne Myong Walmart eCommerce San Bruno, CA Akhil Nigam Fidelity Labs Cambridge, MA

Bob Rosinsky, CE Goodwill Manasota Bradenton, FL Lisa Rusyniak, CE Goodwill Industries of the Chesapeake Baltimore, MD Samuel J. Schmitz, CE Goodwill Industries of Northern Illinois and Wisconsin Stateline Area Rockford, IL Michael Sekits Sekits Capital El Segundo, CA Fred Shelfer Jr., CE Goodwill Industries-Big Bend Tallahassee, FL Laura Smith, CE Goodwill Industries of Hawaii Honolulu, HI Deb Testa, CIC Lockton Companies Farmington, CT Frank Talarico Jr., CE Goodwill of Orange County Santa Ana, CA Lorna G. Utley, CE Goodwill Industries of Greater Detroit Detroit, MI Michael Wirth-Davis, DPA CE Goodwill/Easter Seals Minnesota St. Paul, MN EMERITUS DIRECTORS Will A. Courtney Courtney & Courtney Properties Ft. Worth, TX Evelyne Villines Des Moines, IA

(240) 333-5202 or Seth Turner, Director of Government Affairs and Public Policy, at seth.turner@goodwill.org or (240) 333-5508.

Lauren Lawson Media Relations Manager (240) 333-5266 lauren.lawson@goodwill.org

Seth Turner Director of Government Affairs and Public Policy (240) 333-5508 seth.turner@goodwill.org

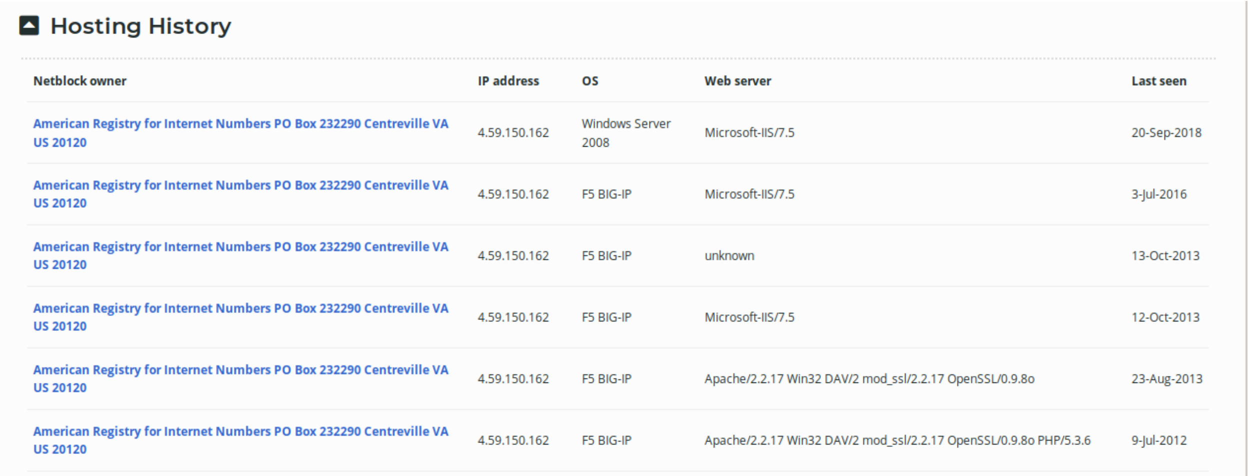
Laura Walling Director of Advocacy and Legislative Affairs (240) 333-5378 laura.walling@goodwill.org

6) Rogue / leaked information (PDFs, XLS, PPT etc) found via Google.

Goodwill Industries International Inc. FY 2010-2011 Budget Comparison Chart
https://www.goodwill.org/wp-content/uploads/2011/01/Budget_Comparison_WIA.pdf
Goodwill Industries International Exhibits Vendors
http://marketplace.goodwill.org/media/Goodwill_Industries_International_Past_Exhibits_Vendors_2015.pdf
GOODWILL INDUSTRIES INTERNATIONAL 2018 ANNUAL REPORT
https://www.goodwill.org/wp-content/uploads/2019/08/2018-Annual-Report_web.pdf
Audited Consolidating Financial Statements, Supplementary Information, and Reports Required by Government Auditing Standards and the Uniform Guidance

https://www.goodwill.org/wp-content/uploads/2019/11/GII-2018-Final-AFS.pdf

7) Use Netcraft to identify the web server versions of the organization, if they exist.



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
American Registry for Internet Numbers PO Box 232290 Centreville VA US 20120	4.59.150.162	Windows Server 2008	Microsoft-IIS/7.5	20-Sep-2018
American Registry for Internet Numbers PO Box 232290 Centreville VA US 20120	4.59.150.162	F5 BIG-IP	Microsoft-IIS/7.5	3-Jul-2016
American Registry for Internet Numbers PO Box 232290 Centreville VA US 20120	4.59.150.162	F5 BIG-IP	unknown	13-Oct-2013
American Registry for Internet Numbers PO Box 232290 Centreville VA US 20120	4.59.150.162	F5 BIG-IP	Microsoft-IIS/7.5	12-Oct-2013
American Registry for Internet Numbers PO Box 232290 Centreville VA US 20120	4.59.150.162	F5 BIG-IP	Apache/2.2.17 Win32 DAV/2 mod_ssl/2.2.17 OpenSSL/0.9.8o	23-Aug-2013
American Registry for Internet Numbers PO Box 232290 Centreville VA US 20120	4.59.150.162	F5 BIG-IP	Apache/2.2.17 Win32 DAV/2 mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.6	9-Jul-2012

8) Any other interesting information you may find relevant.

1)The chairman and CEO both changed on 2017

2)For the POS, they are using the Retail Control Systems

Exercise 1b: Use Google hacking to extract some sensitive doc from any website

Showed in 1(6)

How to use the POS system inside Goddwill:
http://marketplace.goodwill.org/webinars/2011_RCS_Presentation_09192012.pdf

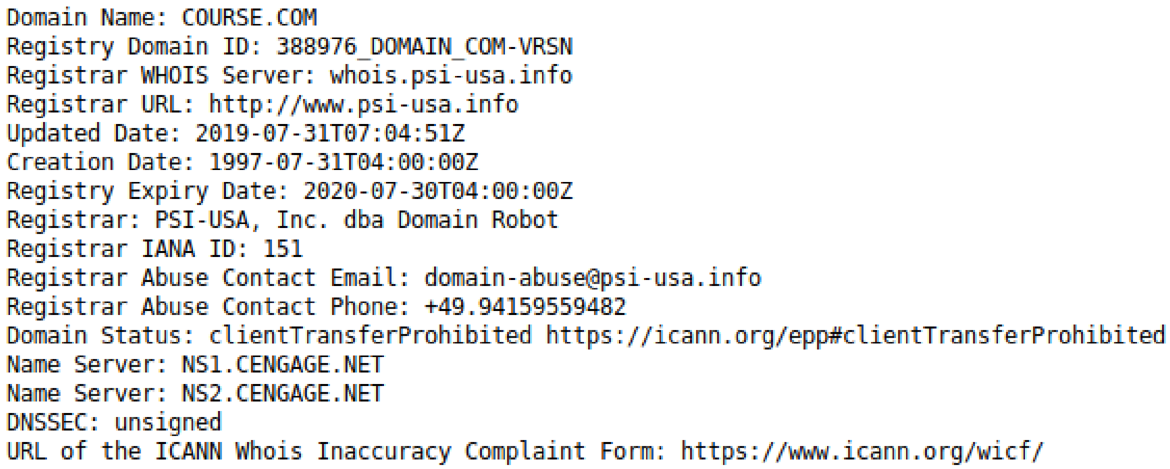
Exercise 2: Gathering WHOIS Information with Windows/Linux WHOIS is a service that allows you to look up people's names on a remote server. Whenever you need to find out more about a domain name, such as its IP address, who the administrative contact is or other information, you can use the WHOIS utility to determine points of contact (POCs), domain owners, and name servers. Many servers respond to TCP queries on port 43 in a manner roughly analogous to the DDN NIC WHOIS service described in RFC 954. Using a Web Browser

1. Open the site: www.internic.net

2. Click Whois in the list of options

3. In the Whois text box, enter the following domain: course.com

4. Record the registrar for this domain name:



```
Domain Name: COURSE.COM
Registry Domain ID: 388976_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.psi-usa.info
Registrar URL: http://www.psi-usa.info
Updated Date: 2019-07-31T07:04:51Z
Creation Date: 1997-07-31T04:00:00Z
Registry Expiry Date: 2020-07-30T04:00:00Z
Registrar: PSI-USA, Inc. dba Domain Robot
Registrar IANA ID: 151
Registrar Abuse Contact Email: domain-abuse@psi-usa.info
Registrar Abuse Contact Phone: +49.94159559482
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.CENGAGE.NET
Name Server: NS2.CENGAGE.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Whois.psi-usa.info

5. Record the primary and secondary name servers for this domain name:

Name Server: NS1.CENGAGE.NET

Name Server: NS2.CENGAGE.NET

6. What other useful information can you determine from this output?

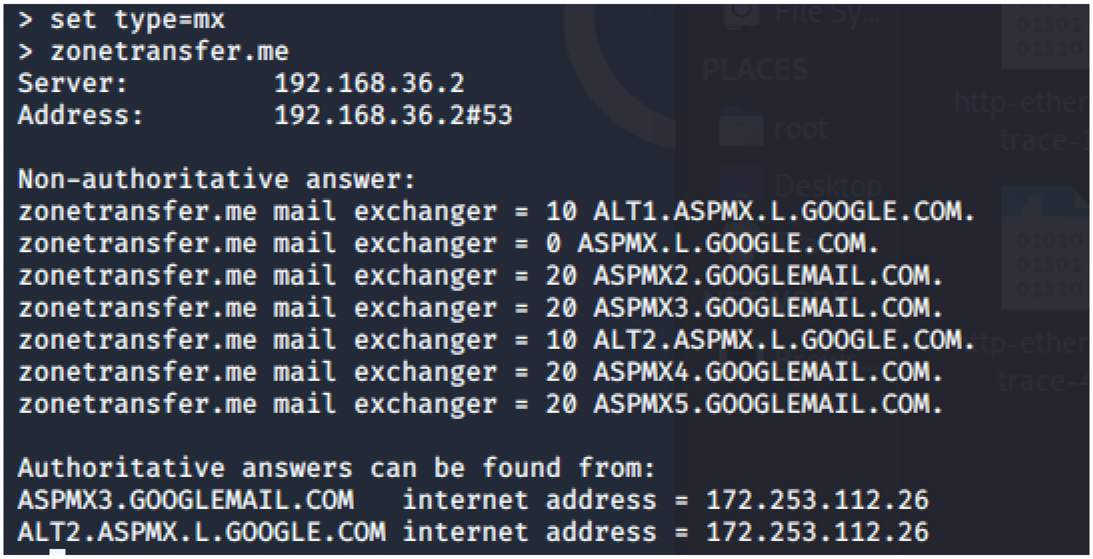
The registrar email: doman-abuse@psi-usa.indo

The registrar phone: +49.94159559482

Exercise3: DNS Reconnaissance

For this website zonetransfer.me or any other site of your choide, enumerate the following information using DNS reconnaissance: (Repeat exercise for all the tools discussed in class – nslookup, dig and fierce.)

- Their MX servers.

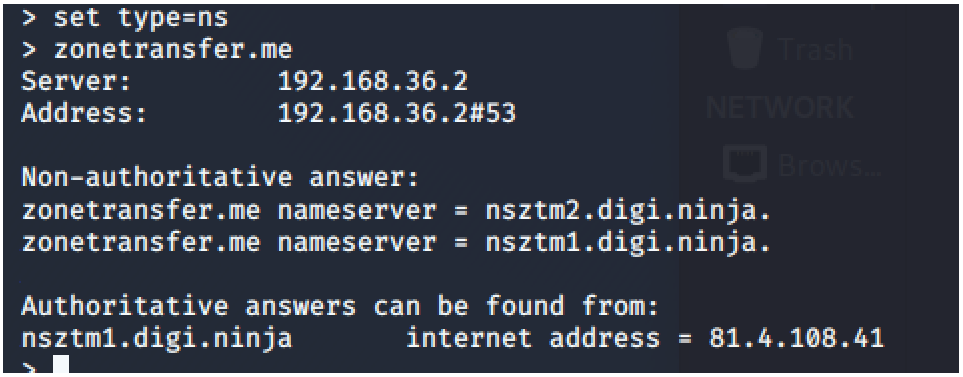


```
> set type=mx
> zonetransfer.me
Server:         192.168.36.2
Address:        192.168.36.2#53

Non-authoritative answer:
zonetransfer.me mail exchanger = 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail exchanger = 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me mail exchanger = 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me mail exchanger = 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me mail exchanger = 10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me mail exchanger = 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me mail exchanger = 20 ASPMX5.GOOGLEMAIL.COM.

Authoritative answers can be found from:
ASPMX3.GOOGLEMAIL.COM   internet address = 172.253.112.26
ALT2.ASPMX.L.GOOGLE.COM internet address = 172.253.112.26
```

- Their NS Servers.

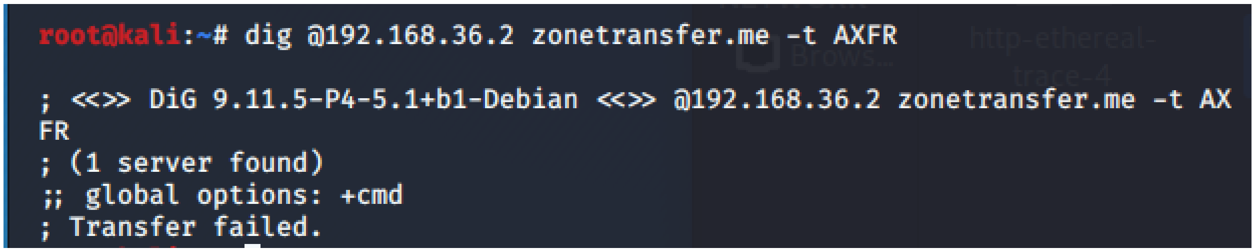


```
> set type=ns
> zonetransfer.me
Server:         192.168.36.2
Address:        192.168.36.2#53

Non-authoritative answer:
zonetransfer.me nameserver = nsztm2.digi.ninja.
zonetransfer.me nameserver = nsztm1.digi.ninja.

Authoritative answers can be found from:
nsztm1.digi.ninja       internet address = 81.4.108.41
>
```

- Additional hostnames on their IP range(s).



```
root@kali:~# dig @192.168.36.2 zonetransfer.me -t AXFR

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @192.168.36.2 zonetransfer.me -t AX
FR
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

- DNS zone transfer possible?

NO, transfer failed