Ethical Hacking Webinar

Footprinting & Reconnaissance

1

- Paul Ulasien
  - Marana, AZ
  - Training and Cyber Security consultant – 17 years
  - Modern Classroom Certified Trainer MCCT - 2020
  - Security+ - 2008
  - Cyber Security Analyst CySA+ - 2017/2021
  - Cyber Security Analytics Professional CSAP - 2021

2

Did You Know

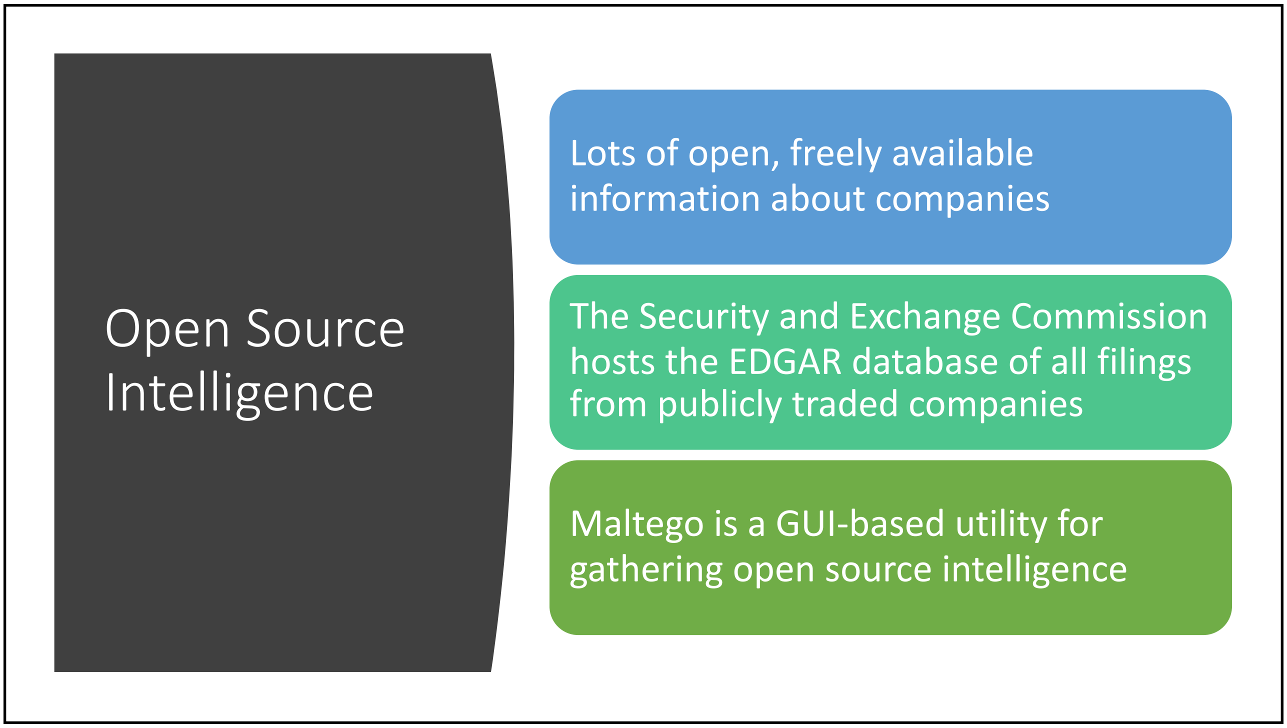
- 23 million people still use “123456” or “password” as their password(s)
- There are some estimates of roughly **46 billion devices** being connected to the Internet by 2021.
- In 2016 - 95 percent of breached records came from one of three industries: Government, retail, or technology.
- Since 2013 estimates of records stolen through breaches are approximately 3,900,000 per day, 159,000 per hour, 2,700 per minute and 44 every second of every day.

3

Agenda

- Open Source Intelligence
- Footprinting
- Web site intelligence
- Technical intelligence

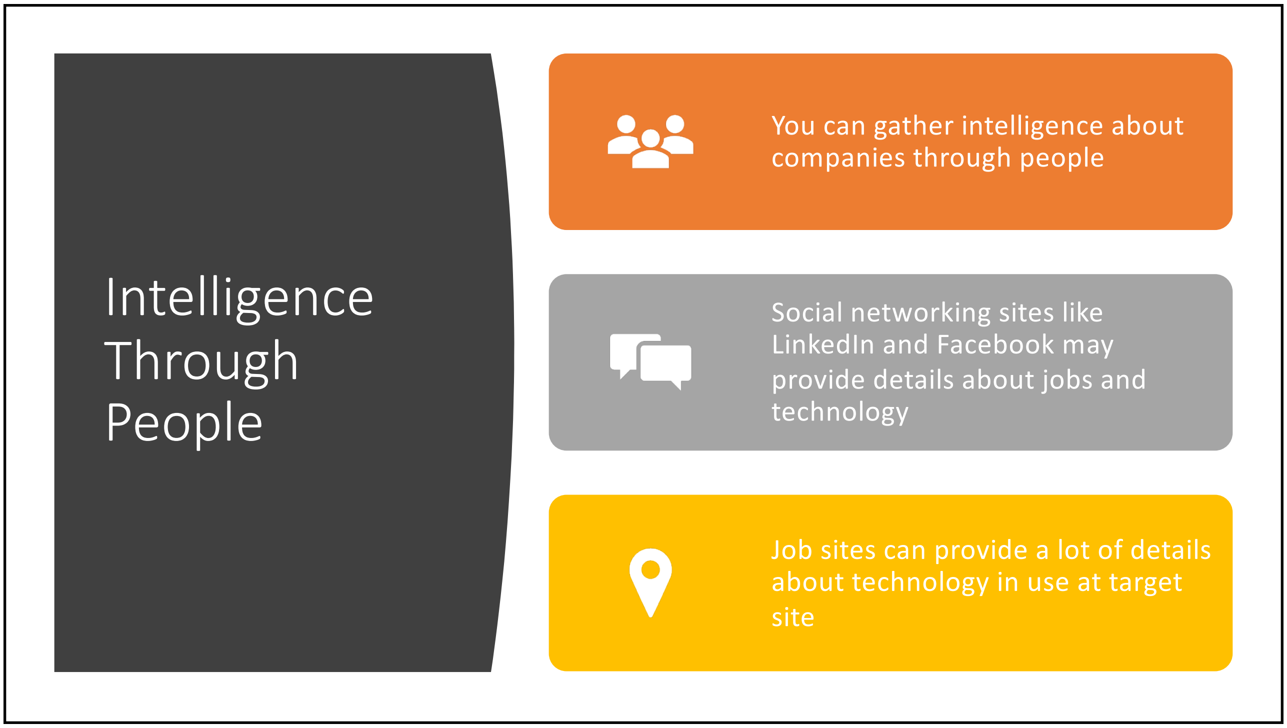
4



Open Source Intelligence

- Lots of open, freely available information about companies
- The Security and Exchange Commission hosts the EDGAR database of all filings from publicly traded companies
- Maltego is a GUI-based utility for gathering open source intelligence

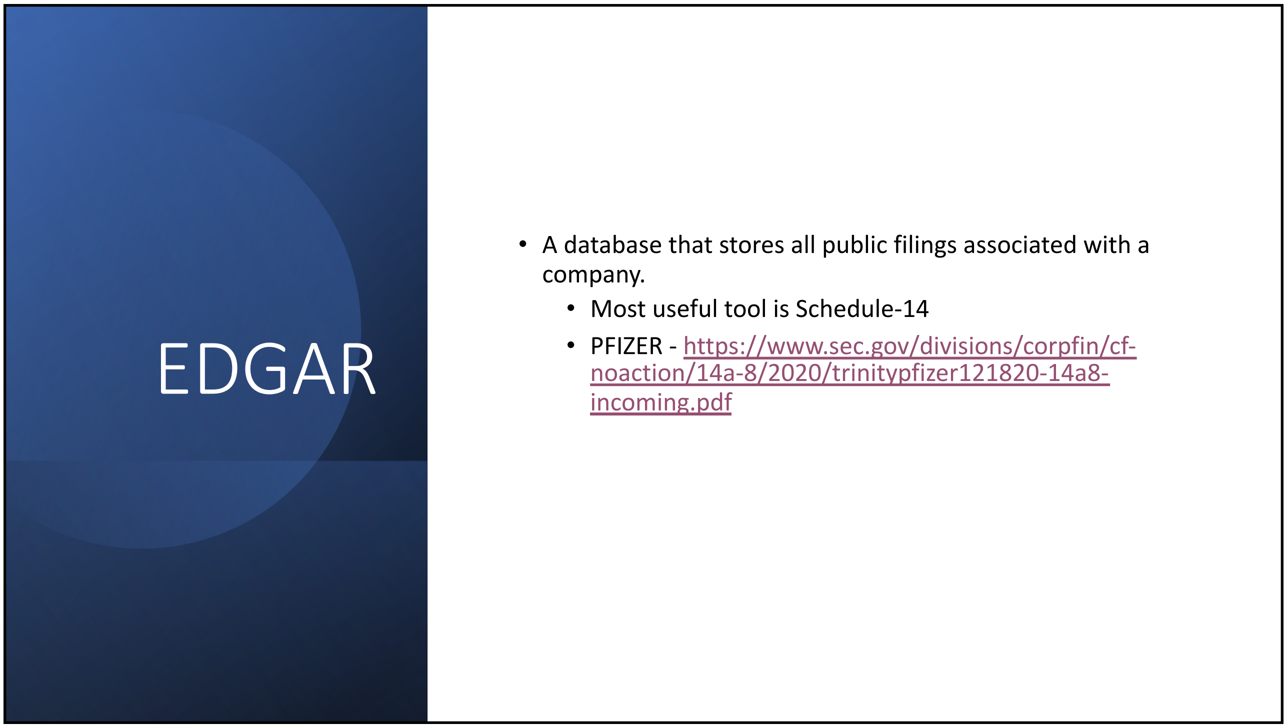
5



Intelligence Through People

- You can gather intelligence about companies through people
- Social networking sites like LinkedIn and Facebook may provide details about jobs and technology
- Job sites can provide a lot of details about technology in use at target site

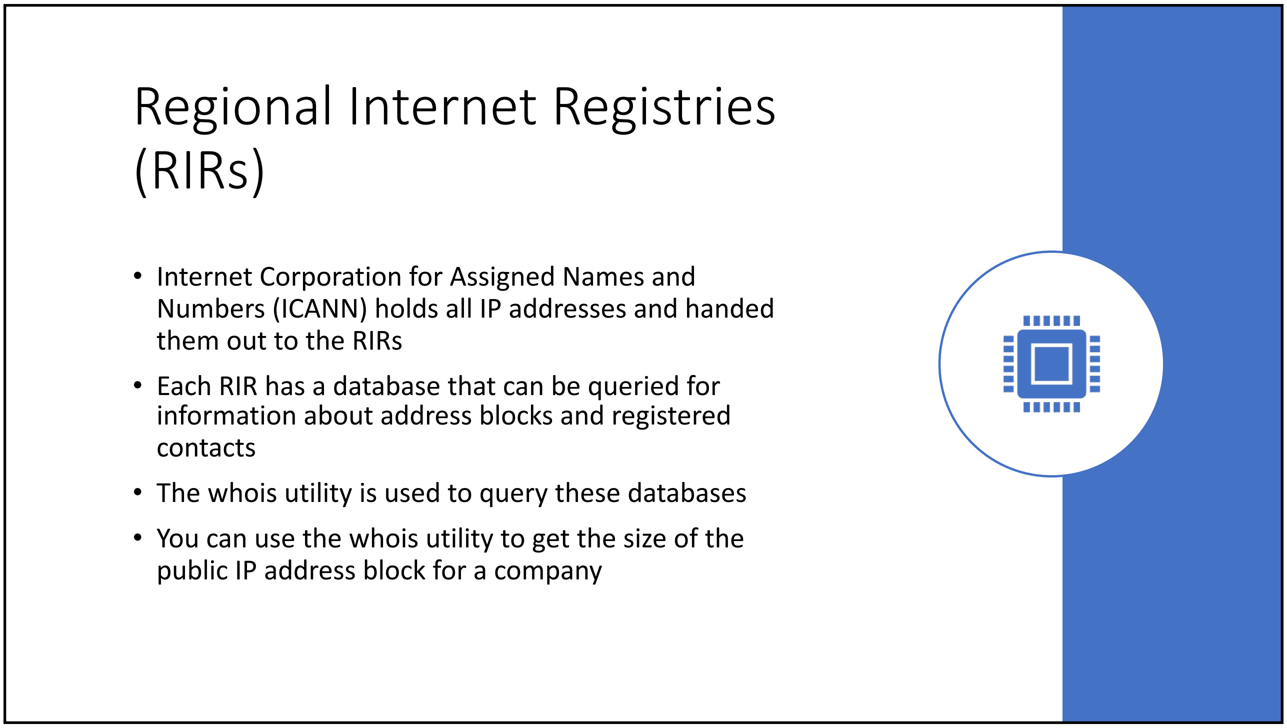
6



EDGAR

- A database that stores all public filings associated with a company.
  - Most useful tool is Schedule-14
  - PFIZER - https://www.sec.gov/divisions/corpfin/cf-noaction/14a-8/2020/trinitypfizer121820-14a8-incoming.pdf

7



Regional Internet Registries (RIRs)

- Internet Corporation for Assigned Names and Numbers (ICANN) holds all IP addresses and handed them out to the RIRs
- Each RIR has a database that can be queried for information about address blocks and registered contacts
- The whois utility is used to query these databases
- You can use the whois utility to get the size of the public IP address block for a company

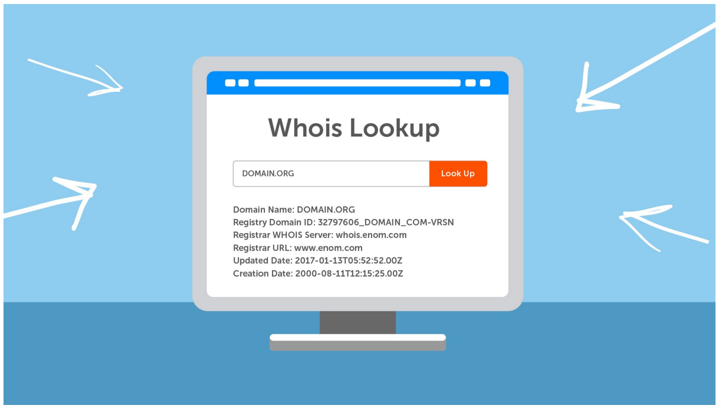
8

What are the RIRs

- American Registry for Internet Numbers (ARIN)
- Réseaux IP Européens Network Coordination Centre (RIPE)
- Africa Network Information Center (AfriNIC)
- Latin American Network Information Center (LATNIC)
- Asia Pacific Network Information Center (APNIC)

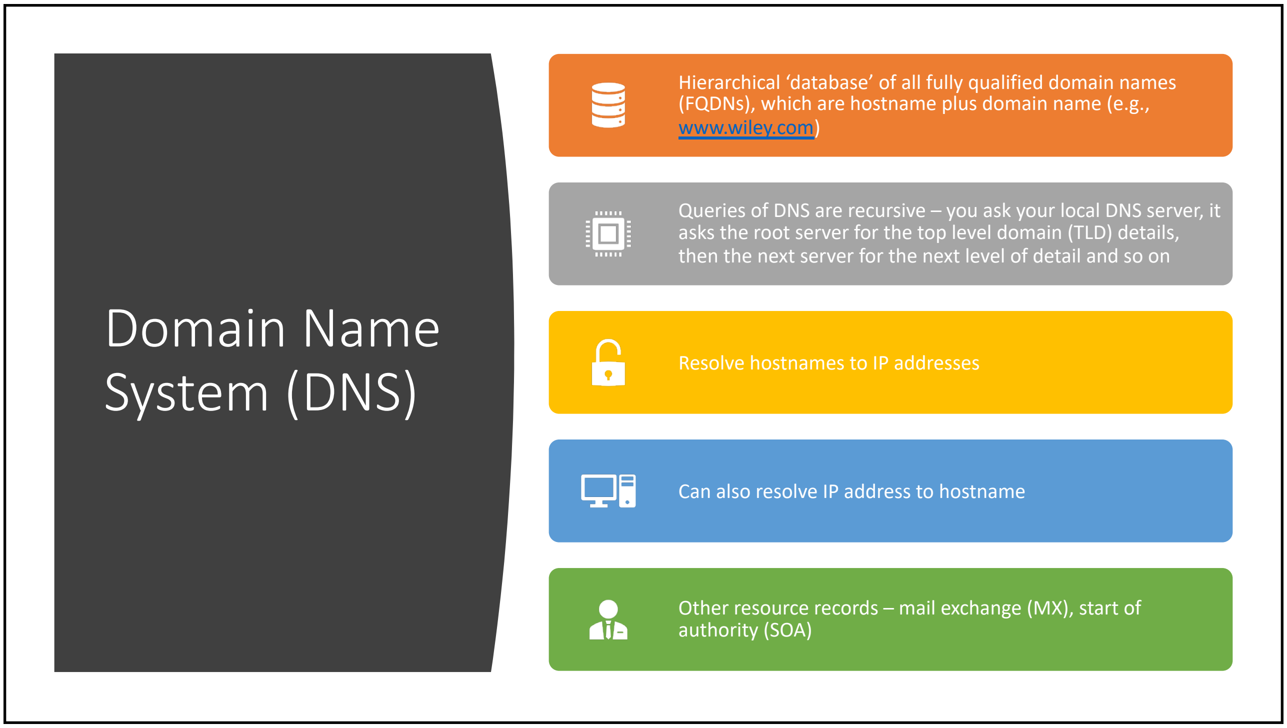
9

WHOIS



Domain Name: DOMAIN.ORG
Registry Domain ID: 32797606_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: www.enom.com
Updated Date: 2017-01-13T05:52:52.00Z
Creation Date: 2000-08-11T12:15:25.00Z

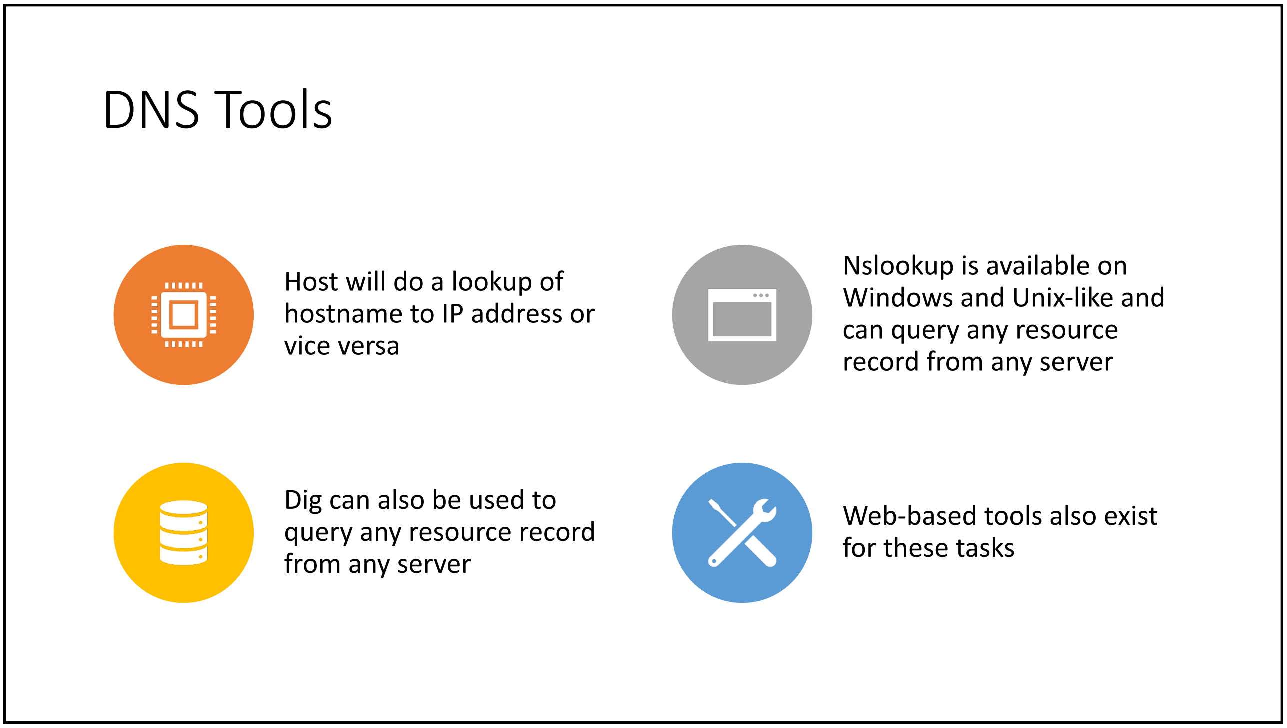
10



Domain Name System (DNS)

- Hierarchical 'database' of all fully qualified domain names (FQDNs), which are hostname plus domain name (e.g., www.wiley.com)
- Queries of DNS are recursive – you ask your local DNS server, it asks the root server for the top level domain (TLD) details, then the next server for the next level of detail and so on
- Resolve hostnames to IP addresses
- Can also resolve IP address to hostname
- Other resource records – mail exchange (MX), start of authority (SOA)

11



DNS Tools

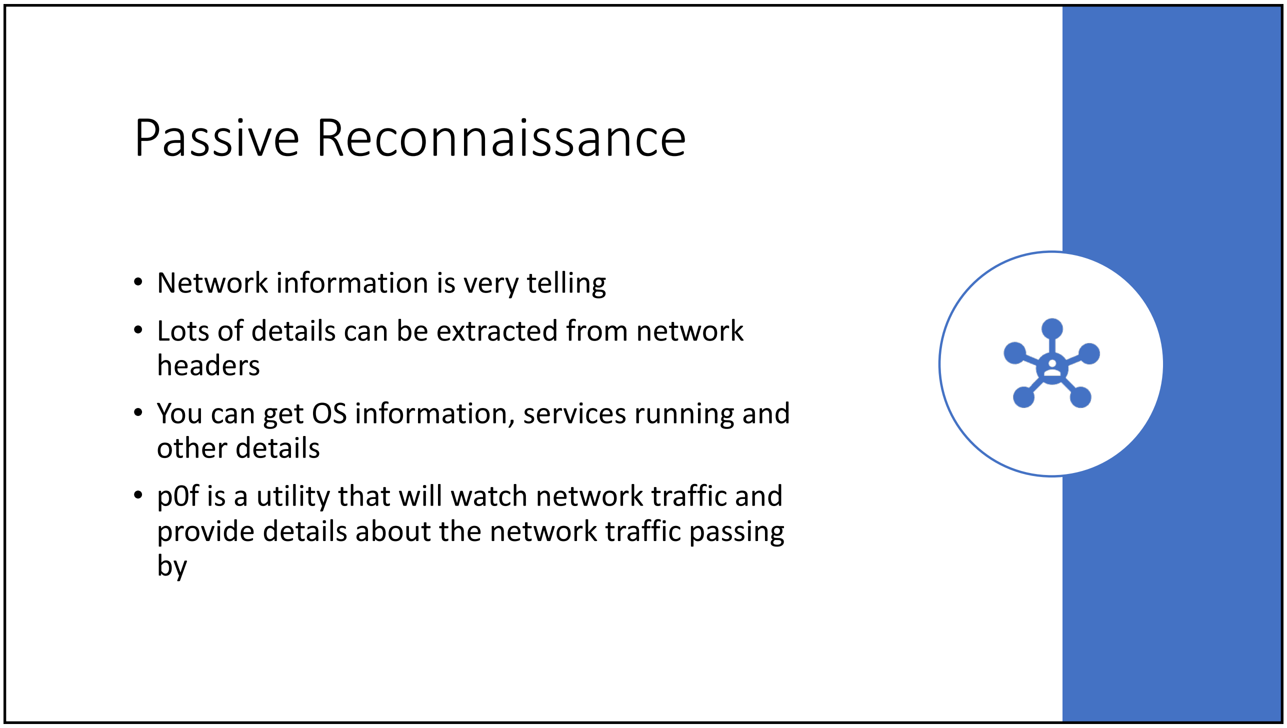
- Host will do a lookup of hostname to IP address or vice versa
- Nslookup is available on Windows and Unix-like and can query any resource record from any server
- Dig can also be used to query any resource record from any server
- Web-based tools also exist for these tasks

12

People

- Whois
- yourdomain.com

13



Passive Reconnaissance

- Network information is very telling
- Lots of details can be extracted from network headers
- You can get OS information, services running and other details
- p0f is a utility that will watch network traffic and provide details about the network traffic passing by

14

Web Site Intelligence

BROWSING WEB SITES CAN REVEAL A LOT ABOUT THE TECHNOLOGY RUNNING

WAPPALYZER HTTPS://WWW.WAPPALYZER.COM/LOOKUP/WWW.PAULULASIEN.COM/

HTTP HEADERS CAN REVEAL SERVER TYPE AND VERSION

OTHER HEADERS CAN PROVIDE TECHNOLOGY DETAILS (E.G., PHP, JAVA, .NET, ETC)

SOURCE CODE CAN PROVIDE FRAMEWORKS AND LIBRARIES IN USE (E.G., SPRING, STRUTS, ETC)

BROWSER PLUGINS CAN BE USED TO GATHER ANALYZE ALL THIS INFORMATION (E.G., WAPPALYZER)

15

Google Hacking

- **Keywords** that can be used to narrow search results
- Boolean logic – “apache server” AND “vulnerabilities”
- Site specific – site:apache.org tomcat
- Specific locations in the content – inurl:, intext:, intitle:, allinurl:, allintext:, allintitle:
- Specific filetypes – filetype:pdf site:Microsoft.com windows

16

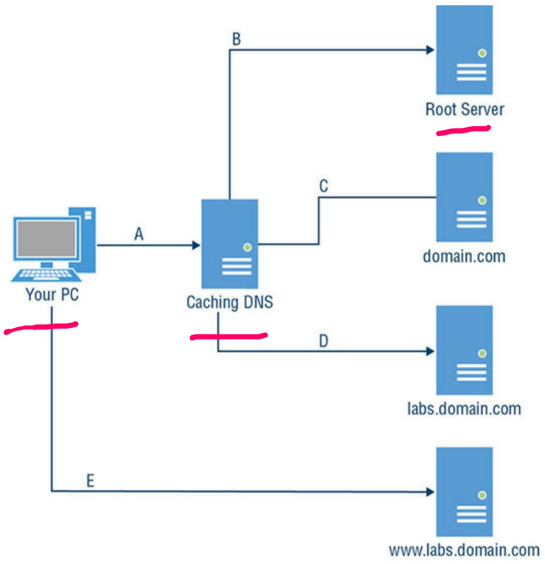
Social Networking

- Facebook
- LinkedIn
- Twitter
- Github.com

17

DNS

Host
nslookup
dig
axfr
dnsrecon
(kali)



18

Internet of Things (IoT)

- B ~~Millions~~ of devices around the world
- Limited functionality, non-standard input/output capabilities (no keyboard, no monitor, etc)
- Web site thingful.net has a database of IoT devices
- Web site shodan.io also has a database of IoT devices

19

Summary

- Intelligence can be gathered from many directions including social networking sites
- RIRs can provide details about IP address ranges belonging to a company and the people who manage those IP addresses at the company
- DNS provides IP addresses from hostnames
- Google Hacking is the use of keywords to narrow search results
- IoT devices can be found using sites like Thingful and Shodan

20

Try it!!

- Gather as much OSINT as you can about yourself or your organization
- Use any or a combination of:
  - ping
  - WHOIS
  - dig
  - traceroute / tracert

21