Chapter 05
Information Gathering

Outline

- Open Source Intelligence (OSINT) Gathering
  - ❖Whois Lookups: to find basic information of the target
  - ❖DNS Reconnaissance: to find more machines and IP addresses
  - ❖Searching for Email Addresses: to find who is who
  - ❖Search Engine Reconnaissance (Google-fu): sometimes, surprise!
  - ❖**Recon-ng (Lab03)**
- Port Scanning (from next week)
  - ❖Manual Port Scanning
  - ❖Port Scanning with Nmap (Lab04)
  - ❖Scapy (Lab05)
  - ❖Scanning with Netcat (Week02)

Reconnaissance (information gathering)

- Reconnaissance is "casing the joint"
- Two general types of attackers:
  - Script kiddies – look for low-hanging fruit, and may skip this step
  - Attackers out to get a particular site – this step is extremely important
- Very helpful step for experienced attackers
- **The more time you spend collecting information** on your target, **the more likely you are to be successful** in the later phases

"If I had 6hr to chop down a tree, I'd spend the first hour of them sharpening my axe"
- Abraham Lincoln-

Open Source Intelligence (OSINT) Gathering

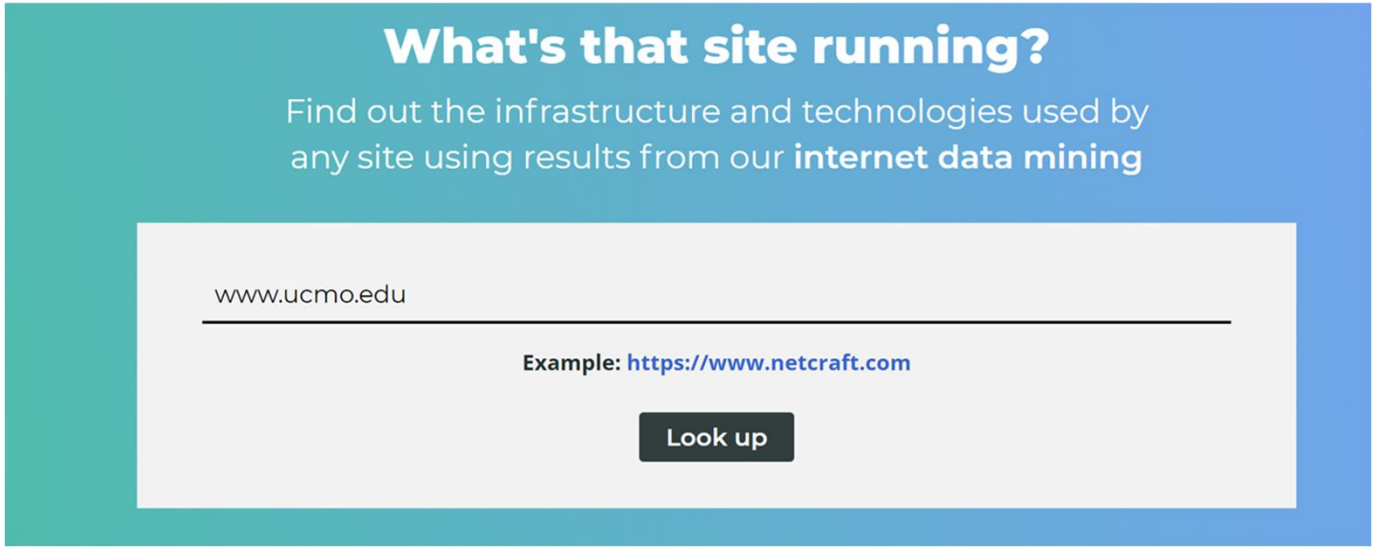
- The success of a pentest often depends on the results of the information-gathering phase
- We will look at a few tools to obtain interesting information from these public sources
- Location Information
  - Satellite images, building layout (badge readers, break areas, security, fencing, etc.)
- Job Information
  - Employees (name, job title, phone number, manager, etc.), indeed, glassdoor?
  - Pictures (badge photos, desk photos, computer photos, etc.)

Importance of OSINT Research

- **Open-Source Intelligence** (OSINT)
  - We can gather a significant amount of data **without ever sending a single packet to the target** (which tools?)
  - It is important to know the difference between **which tools do and which tools do not touch the target**
- Types of recon
  - **Active recon**: interact directly with the target, homepage copy? (target may record our info)
  - **Passive recon**: information available on the web (no direct interaction with the target, or directly with expected manner)
- Two main goals in this phase
  - We need to gather **as much information as possible** about the target
  - We need to **sort through all the information gathered** and create a <u>list of attackable IP addresses or URLs</u>

Netcraft

- Website technology information
- https://sitereport.netcraft.com/



Builtwith Technology (builtwith.com)

- Website technology information

Find out what websites are
Built With

ucmo.edu | Lookup

Whatweb

- Recognizes web technologies, CMS (content management system), etc.

```
┌──(kali㉿kali)-[/tmp]
└─$ whatweb https://www.umkc.edu
https://www.umkc.edu [200 OK] Bootstrap, Country[UNITED STATES][US], Frame, Google-Analytics[Universal][UA-54827
23-17,UA-5482723-2,UA-89352600-1], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[134.193.116.82], JQuery, Microsoft-
IIS[10.0], Open-Graph-Protocol, Script[text/x-handlebar-template], Strict-Transport-Security[max-age=31536000],
Title[Home | University of Missouri - Kansas City][Title element contains newline(s)!], UncommonHeaders[access-c
ontrol-allow-origin,x-content-type-options], X-Frame-Options[SAMEORIGIN], X-Powered-By[ASP.NET]
```

```
┌──(kali㉿kali)-[~]
└─$ whatweb https://www.ucmo.edu
ERROR Opening: https://www.ucmo.edu - SSL_connect returned=1 errno=0 peeraddr=153.91
.1.10:443 state=error: unsafe legacy renegotiation disabled
```

*This error happens when OpenSSL 3 to connect to a server which does not support it.

Whois Lookups

- First, look up the target at ICANN to determine the registrar
  - https://lookup.icann.org/
  - Operated by Internet Corporation for Assigned Names and Numbers (ICANN)
  - You get basic info from here

- Then (or), go to registrar's whois database to get detailed records
  - https://www.whois.com/whois
  - Whois server uses tcp port 43

ICANN Lookup

Domain Name Registration Data Lookup

Enter a domain name

Frequently Asked Questions (FAQ)

microsoft.com

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN Privacy Policy, and agree to abide by the website Terms of Service and the Domain Name Registration Data Lookup Terms of Use.

Nameservers:
NS1-205.AZURE-DNS.COM
NS2-205.AZURE-DNS.NET
NS3-205.AZURE-DNS.ORG
NS4-205.AZURE-DNS.INFO

Dates

Registry Expiration: 2021-05-03 04:00:00 UTC

Created: 1991-05-02 04:00:00 UTC

Registrar Information

Name: MarkMonitor Inc.

IANA ID: 292

Abuse contact email: abusecomplaints@markmonitor.com

Abuse contact phone: +1.2083895770

Whois Lookups

- All domain registrars keep records of the domains they host
- When registering a domain name, the registrar requests:
  - ❖Postal addresses, phone numbers, name of points of contact, IP addresses of your authoritative domain name servers
- # whois bulbsecurity.com
  - ❖Domain privacy offers private registration, hiding your personal details in the Whois information for the domains you own

Registrant Contact	
Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd

- # whois ucmo.edu
  - ❖What do you see?

Whois (https://www.whois.com/whois/)

```
--------------------------------------------------------------

Domain Name: UCMO.EDU

Registrant:
        University of Central Missouri
        Ward Edwards 0101
        Warrensburg, MO 64093
        United States of America

Administrative Contact:
        Jim Graham
        University of Central Missouri
        Ward Edwards 0101
        Warrensburg, MO 64093
        United States of America
        +1.6605434279
        graham@ucmo.edu

Technical Contact:
        Alan Cline
        University of Central Missouri
        Ward Edwards 0400
        Warrensburg, MO 64093
        United States of America
        +1.6605438539
        hostmaster@ucmo.edu

Name Servers:
        NS2.UCMO.EDU
        NS1.UCMO.EDU

Domain record activated:    08-Dec-2006
Domain record last updated: 26-Sep-2018
Domain expires:             31-Jul-2019
```

Whois Lookups – cont'd

- How do attackers use this information?
  - ❖Contact names: Social engineering, duping users via the telephone into giving up useful information
  - ❖Telephone numbers: War dialing, finding unsecure modems to infiltrate an internal network
  - ❖Postal addresses: War driving, finding unsecure wireless access points to attack
  - ❖IP addresses: Scanning, looking for openings in the target

IP Address Assignment Lookup

- Several **regional internet registries (RIRs)** offer whois database that store information about IP address block assignment
- Not all organizations have their own IP address blocks. Many get them from their ISP
- You may get
  - ❖Actual assignment of the address blocks
  - ❖Nothing at all
  - ❖A huge address space most likely from the ISP

- **We want to find IP addresses from this slide**

Regional Internet Registries (RIRs)

- Attackers look for IP address assignments in these geographic whois databases
- ARIN (American Registry of Internet Numbers)
  - ❖www.arin.net
- RIPE NCC (Reseaux IP Europeans Network Coordination Centre)
  - ❖www.ripe.net
- APNIC (Asia Pacific Network Information Centre)
  - ❖www.apnic.net
- LACNIC (Latin American and Caribbean NIC)
  - ❖www.lacnic.net
- AFRINIC (Africa's NIC)
  - ❖www.afrinic.net

Whois Lookup

```
root@kali:~# whois 153.91.1.51
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '153.0.0.0 - 153.255.255.255'

% Abuse contact for '153.0.0.0 - 153.255.255.255' is 'helpdesk@apnic.net'

inetnum:        153.0.0.0 - 153.255.255.255
netname:        ERX-NETBLOCK
descr:          Early registration addresses
remarks:        -------------------------------------------------------
remarks:        Important:
remarks:
remarks:        Networks in this range were allocated by InterNIC
remarks:        prior to the formation of Regional Internet
remarks:        Registries (RIRs): AfriNIC, APNIC, ARIN, LACNIC and RIPE NCC.
remarks:
remarks:        Address ranges from this historical space have now
remarks:        been transferred to the appropriate RIR database.remarks:
remarks:        If your search has returned this record, it means the
remarks:        address range is not administered by APNIC.
remarks:
remarks:        Instead, please search one of the following databases:
remarks:
remarks:        - AfriNIC (Africa)
remarks:        website: http://www.afrinic.net/
remarks:        command line: whois.afrinic.net
remarks:
```

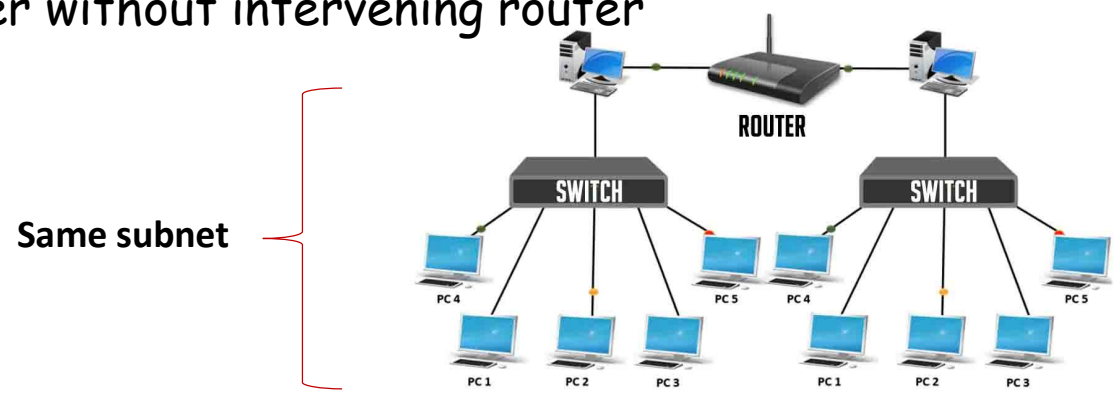
Whois Lookup - Netrange

```
root@kali:~# whois -h whois.arin.net 153.91.1.51

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.
#


NetRange:       153.91.0.0 - 153.91.255.255
CIDR:           153.91.0.0/16
NetName:        CMSU-NET
NetHandle:      NET-153-91-0-0-1
Parent:         APNIC-ERX-153 (NET-153-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   University of Central Missouri (CMSU)
RegDate:        1991-09-22
Updated:        2008-08-12
Ref:            https://rdap.arin.net/registry/ip/153.91.0.0


OrgName:        University of Central Missouri
OrgId:          CMSU
Address:        Ward Edwards 0101
City:           Warrensburg
StateProv:      MO
PostalCode:     64093
Country:        US
RegDate:        1991-09-22
Updated:        2011-10-19
Ref:            https://rdap.arin.net/registry/entity/CMSU
```

Subnets & CIDR notation

- Each IP address has
  - subnet part - high order bits
  - host part - low order bits

- What's a subnet ?
  - device interfaces with same subnet part of IP address
  - can physically reach each other without intervening router



Classless Inter-Domain Routing (CIDR)

- Subnet portion of address of arbitrary length
- Address format: a.b.c.d/x, where x is the number of bits in subnet portion of address

IP Address

Dotted decimal 192.168. 2. 15/24

Binary 11000000 . 10101000 . 00000010. 00001111

Network Address. **24**bit (subnet part)

Host Address, **8**bit

CIDR & Subnet Mask

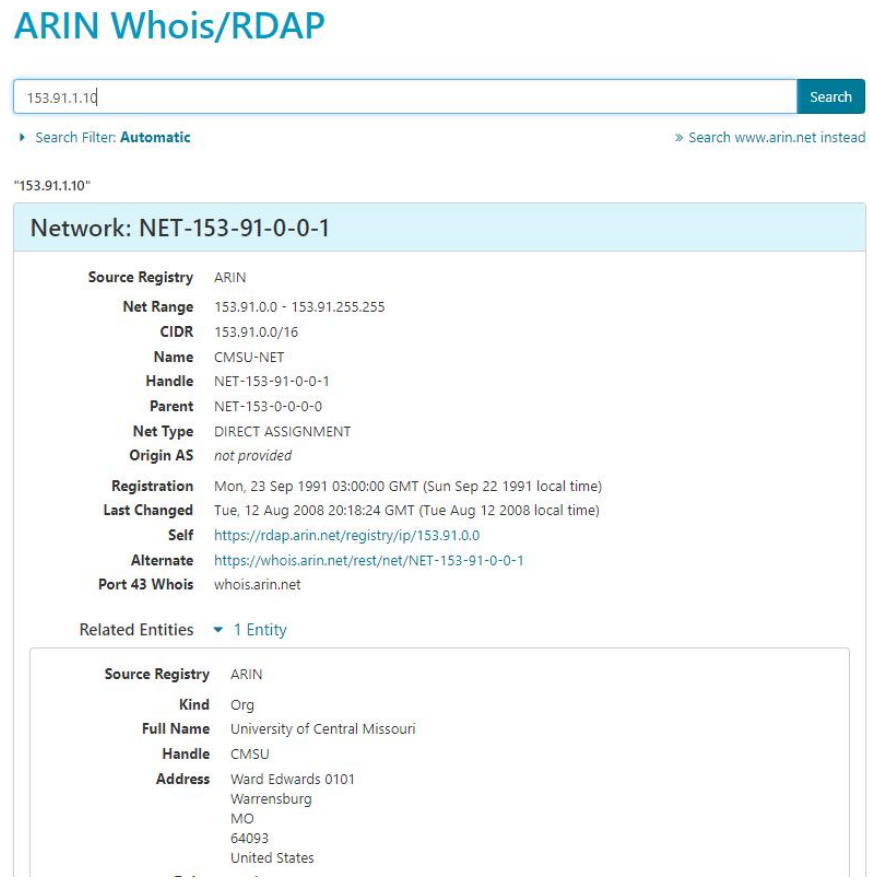
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ucmo.local
   Link-local IPv6 Address . . . . . : fe80::2df9:f035:763d:2000%5
   IPv4 Address. . . . . . . . . . . : 153.91.107.220
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 153.91.111.254
```

- 255.255.248.0 – 11111111.11111111.11111000.00000000
- 153.91.107.220 – 10010111.01011011.01101011.11011100

- Address range
- 10010111.01011011.01101000.00000000 - 153.91.104.0
- 10010111.01011011.01101111.11111111 – 153.91.111.255

ARIN IP Lookup

- https://search.arin.net/rdap/?query=153.91.1
  10



Whois Recon Defenses

- Preparation:
  - ❖Just live with it – That's just the way the Internet is
  - ❖Use organization name or title with real e-mail and phone number
  - ❖Be wary of anonymous registration agents
    - Network Solutions and Go Daddy offer private registration for an extra US $9.99 per year
    - General Data Protection Regulation (GDPR) may affect the information to be included in the whois database
    - Incident handlers depend on being able to use whois info to contact each other!
- Identification:
  - ❖You can't really tell someone has looked you up

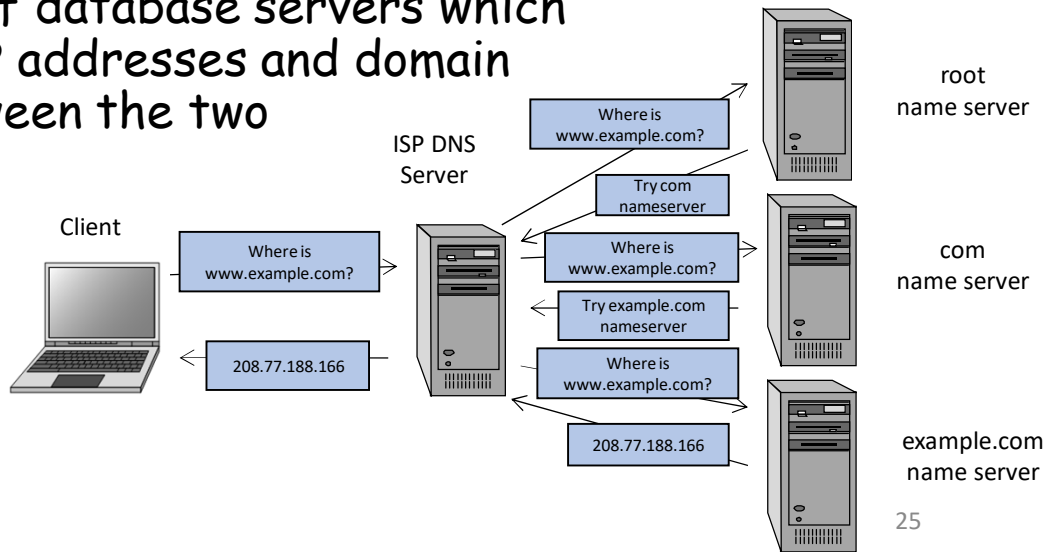
DNS Reconnaissance

- Use DNS servers to learn more about a domain
- Available tools
  - nslookup
  - host
  - dig
  - Zone transfers

DNS Server & Name Server

- DNS (Domain Name Service) is a **system** which maintains a relationship between Internet Protocol (IP) addresses and domain names

- DNS is actually comprised of a set of database servers which maintain the relationship between IP addresses and domain names and facilitate the lookup between the two



Querying DNS Servers

- At the end of the whois information, we have **a list of target's DNS servers**
- We want all kinds of DNS records which include
  - NS: nameserver record
  - A: IPv4 address for a given hostname
  - AAAA: IPv6 address for a given hostname
  - CNAME: canonical name record
  - HINFO: host information record
  - MX: mail exchange record
  - SOA: start of authority record, which indicates that a server is authoritative for that DNS zone (set of records)
  - TXT: text record
  - PTR: pointer for inverse lookups record
  - RP: responsible person record
  - SRV: service location record

DNS Records

DNS: Distributed db storing resource records (RR)

RR format: **(name, value, type, ttl)**

type=A

- **name** is hostname
- **value** is IP address

type=NS

- **name** is domain (e.g., foo.com)
- **value** is hostname of authoritative name server for this domain

type=CNAME

- **name** is alias name for some "canonical" (the real) name
- **www.ibm.com** is really **servereast.backup2.ibm.com**
- **value** is canonical name

type=MX

- **value** is name of mailserver associated with **name**

DNS Recon – Nslookup

- The **nslookup** command is included in Windows and Linux
  - nslookup = name server lookup
- Can type the whole command in one line
  - # nslookup www.bulbsecurity.com
- Or type nslookup to invoke the interactive mode
  - # nslookup
    > set type=mx
    > ucmo.edu
  - Type exit to exit

Using nslookup Interactively

- Within nslookup interactive mode, we can
  - ❖Resolve an individual name or IP address
    - > [name or IP_addr]
  - ❖Use a different DNS server
    - > server [serverIPaddr or name]
  - ❖Indicate which record we are interested in (pull address record by default)
    - > set type=MX
  - ❖Perform a **zone transfer** of all records for a given domain (Windows nslookup)
    - > ls –d [target_domain]
  - ❖Store zone transfer out in a file
    - > ls –d [target_domain] [> filename]

Zone Transfer Using Nslookup

Administrator: Command Prompt - nslookup

```
C:\windows\system32>nslookup
Default Server:  ghana.ucmo.edu
Address:  153.91.3.203

> server nsztm1.digi.ninja
Default Server:  nsztm1.digi.ninja
Address:  81.4.108.41

> set type=all
> ls -d zonetransfer.me
[nsztm1.digi.ninja]
 zonetransfer.me.               SOA    nsztm1.digi.ninja robin.digi.ninja. (2017042001 172800 900 1209600 3600)
 zonetransfer.me.               HINFO  Casio fx-700G  Windows XP
 zonetransfer.me.               TXT            "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"

 zonetransfer.me.               MX     0    ASPMX.L.GOOGLE.COM
 zonetransfer.me.               MX     10   ALT1.ASPMX.L.GOOGLE.COM
 zonetransfer.me.               MX     10   ALT2.ASPMX.L.GOOGLE.COM
 zonetransfer.me.               MX     20   ASPMX2.GOOGLEMAIL.COM
 zonetransfer.me.               MX     20   ASPMX3.GOOGLEMAIL.COM
 zonetransfer.me.               MX     20   ASPMX4.GOOGLEMAIL.COM
 zonetransfer.me.               MX     20   ASPMX5.GOOGLEMAIL.COM
 zonetransfer.me.               A      5.196.105.14
 zonetransfer.me.               NS     nsztm1.digi.ninja
 zonetransfer.me.               NS     nsztm2.digi.ninja
 _sip._tcp                      SRV    priority=0, weight=0, port=5060, www.zonetransfer.me
 14.105.196.5.IN-ADDR.ARPA      PTR    www.zonetransfer.me
 asfdbauthdns                   AFSDB  1    asfdbbox.zonetransfer.me
 asfdbbox                       A      127.0.0.1
 asfdbvolume                    AFSDB  1    asfdbbox.zonetransfer.me
```

DNS Cache Snooping

```
root@slingshot: ~
File  Edit  View  Search  Terminal  Help
root@slingshot:~# nslookup
> set norecurse
> www.counterhack.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
*** Can't find www.counterhack.com: No answer
> set recurse
> www.counterhack.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.counterhack.com     canonical name = counterhack.com.
Name:   counterhack.com
Address: 204.51.94.79
> set norecurse
> www.counterhack.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.counterhack.com     canonical name = counterhack.com.
Name:   counterhack.com
Address: 204.51.94.79
>
```

1) For now, there is no record for the address in DNS cache

2) The recursive query result come into DNS cache record

3) Now, we can check out the data in DNS cache
: by using this technique, we can figure out the pages the users are visiting that specific website

DNS Zone Transfer in Windows

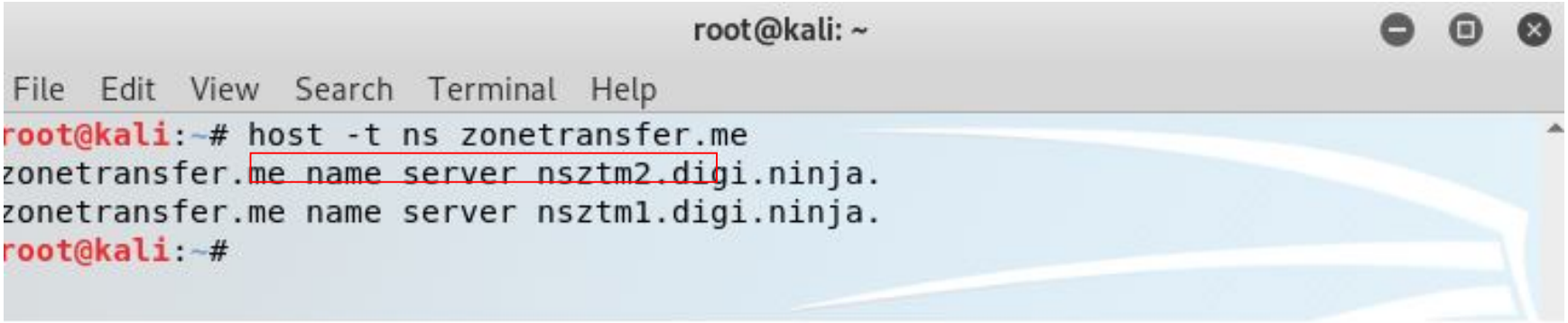
- By dumping all records from your DNS servers, an attacker can determine which machines are accessible on the Internet
- DNS zone transfers are carried over TCP port 53, whereas most DNS queries and responses rely on UDP port 53.
- # tcpdump -nn port 53, and host <authoritative_server_IP>

```
C:\WINDOWS\system32>nslookup
Default Server:  ghana.ucmo.edu
Address:  153.91.3.203

> set type=all
> ls -d ucmo.edu
[ghana.ucmo.edu]
*** Can't list domain ucmo.edu: Query refused
The DNS server refused to transfer the zone ucmo.edu to your computer. If this
is incorrect, check the zone transfer security settings for ucmo.edu on the DNS
server at IP address 153.91.3.203.
```

* Zone transfer works when there is misconfiguration on DNS server

DNS Recon – host

- The command **host** shows all the DNS servers for the given domain name
  - ❖# host -t ns zonetransfer.me



DNS Recon – Zone Transfers

- DNS zone transfers allow name servers to replicate all the entries about a domain
- Zone transfer
  - ❖# **host** -l zonetransfer.me nsztm1.digi.ninja
  - ❖# **host** -t axfr zonetransfer.me nsztm1.digi.ninja

  → There are pages and pages of DNS entries for zonetransfer.me, which gives us a good idea of where to start in looking for vulnerabilities for our pentest
- Seems like many organizations maintain a good posture for this

DNS Zone Transfer In Linux

- The **nslookup** command in modern Linuxes cannot perform a zone transfer
- Use **dig** command instead or **host** command as shown in previous slide
- dig @[DNS_Server] [target_domain] [type]
- The type can be ANY, A, MX, etc. The default is A records
- With a –t flag, we can specify zone transfer
    - ❖Full zone transfer: -t AXFR
    - ❖Incremental zone transfer: -t IXFR=N
    - ❖# dig @nsztm1.digi.ninja zonetransfer.me -t AXFR

Zone Transfer Example

```
root@kali:~# dig @nsztm1.digi.ninja zonetransfer.me -t AXFR

; <<>> DiG 9.11.4-P2-3-Debian <<>> @nsztm1.digi.ninja zonetransfer.me -t AXFR
; (1 server found)
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2017042001 172800 900 1209600 3600
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       5.196.105.14
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN   AFSDB   1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200  IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN    AFSDB   1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A      202.14.81.230
cmdexec.zonetransfer.me. 300    IN      TXT     "; ls"
contact.zonetransfer.me. 2592000 IN     TXT     "Remember to call or email Pippa on +44 123 4567890 or pippa@zonetransfer.me when making DNS changes"
dc-office.zonetransfer.me. 7200 IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201  IN      AAAA    dead:beaf::
dr.zonetransfer.me.     300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10000m 10m
DZC.zonetransfer.me.    7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.  2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me.  7200    IN      A       74.125.206.26
home.zonetransfer.me.   7200    IN      A       127.0.0.1
Info.zonetransfer.me.   7200    IN      TXT     "ZoneTransfer.me service provided by Robin Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php for more informat
ion."
internal.zonetransfer.me. 300   IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me. 300   IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me. 300     IN      A       81.4.108.41
intns2.zonetransfer.me. 300     IN      A       167.88.42.94
office.zonetransfer.me. 7200    IN      A       4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA    2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.    7200    IN      A       207.46.197.32
robinwood.zonetransfer.me. 302  IN      TXT     "Robin Wood"
rp.zonetransfer.me.     321     IN      RP      robin.zonetransfer.me. robinwood.zonetransfer.me.
```

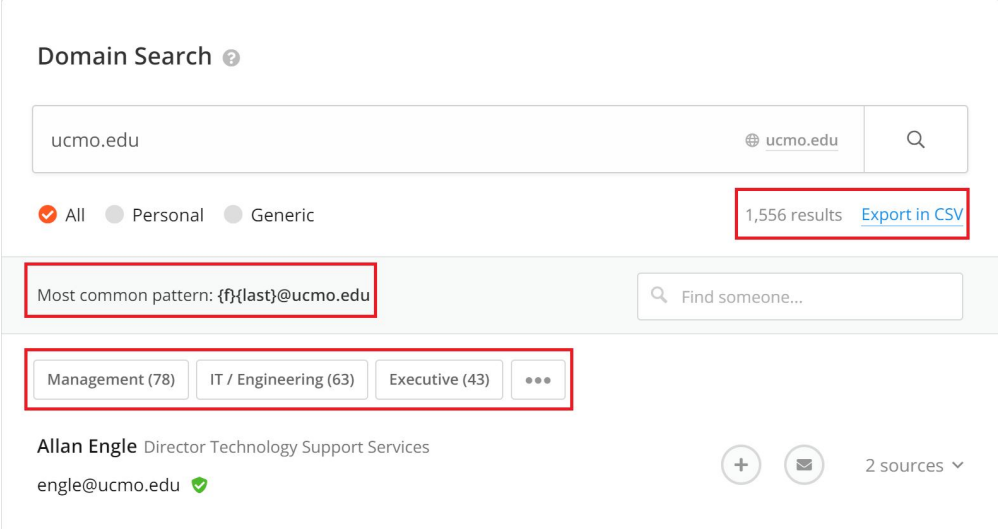
nouse pointer inside or press Ctrl+G.

Another Tool - dnsenum

```
root@kali:~# dnsenum zonetransfer.me
dnsenum VERSION:1.2.6

-----   zonetransfer.me   -----


Host's addresses:
__________________

zonetransfer.me.                         5        IN    A        5.196.105.14


Wildcard detection using: irzslactxjrs
______________________________________

irzslactxjrs.zonetransfer.me.            5        IN    A        23.217.138.110
irzslactxjrs.zonetransfer.me.            5        IN    A        23.202.231.169


!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 Wildcards detected, all subdomains will point to the same IP address
 Omitting results containing 23.217.138.110, 23.202.231.169.
 Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Name Servers:
_____________

nsztm2.digi.ninja.                       5        IN    A        34.225.33.2
nsztm1.digi.ninja.                       5        IN    A        81.4.108.41


Mail (MX) Servers:
__________________

ASPMX2.GOOGLEMAIL.COM.                   5        IN    A        173.194.209.27
ASPMX3.GOOGLEMAIL.COM.                   5        IN    A        142.250.96.27
```

Searching for Email Addresses

- One excellent way to find usernames is by looking for email addresses on the Internet
- theHarvester – a python tool
  - ❖Automate searching Google, Bing, PGP, LinkedIn, and others for email addresses
  - ❖# theHarvester –d ucmo.edu –b all
- https://hunter.io/domain-search



Useful Google Search Directives

- The "site:" directive
  - ❖Searches only within the given domain
  - ❖Example: site:ucmo.edu jobs
- The "link:" directive
  - ❖Shows all sites linked to a given site
  - ❖Example: link:www.bulbsecurity.com
- The "intitle:" directive
  - ❖Shows pages whose title matches the search criteria
  - ❖Example: intitle:index.of passwd

Useful Google Search Directives

- The "inurl:" directive
  - Shows pages whose URL matches the search criteria
  - Example: inurl:viewtopic.php

- The "filetype:"directive searches for only a specific kind of file
  - Same effect as the "ext:" directive
  - site:ucmo.edu filetype:ppt
  - site:ucmo.edu ppt

Google's Cache and Wayback

- One more directive: cache
  - cache:www.ucmo.edu
  - Brings up the cached version of the page

- The wayback machine at www.archive.org
  - An even more thorough view, with multiple images over time
  - Cached pages from billions of web pages for the last several years

Additional Search Tips

- Google search is case-insensitive
- Search for a literal string using double quotes ("")
  - "your search keywords"
- Add minus (-) to search term to exclude pages with a given word to maximize effectiveness of resulting hits
  - E.g., site:ucmo.edu –www.ucmo.edu

Searching for File types

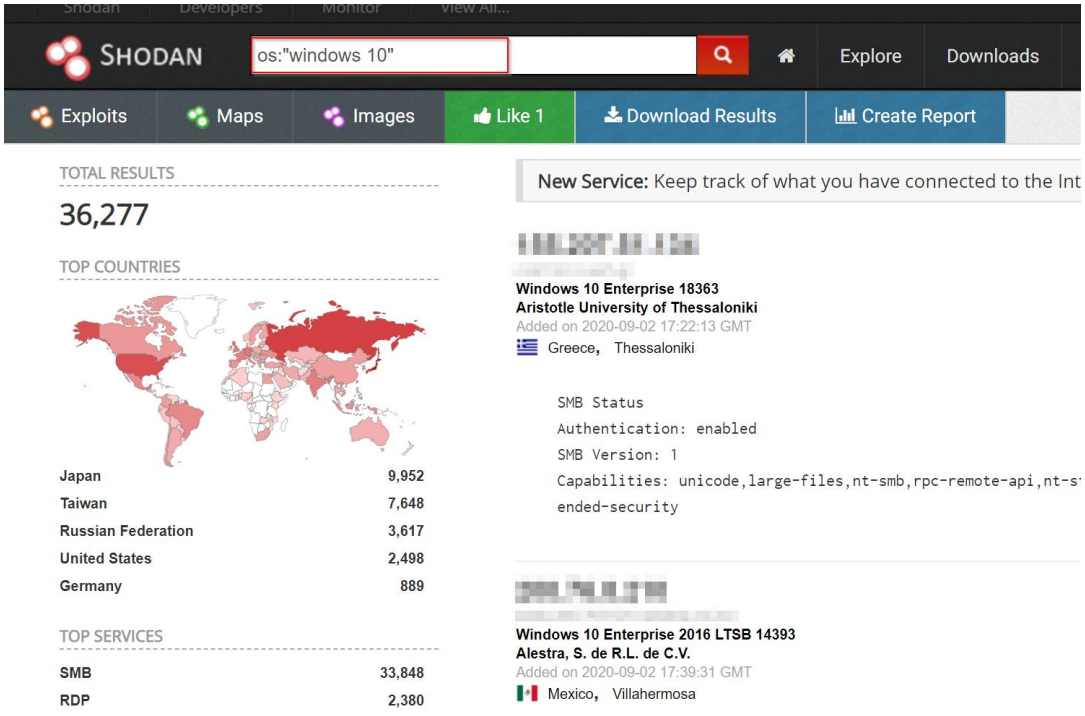
- Search for specific file types on a target domain
- asp, jsp, php, cgi, and others → These types of files indicate active web content, and may be vulnerable
- xlsx and pptx → Organizations sometimes don't even realize that they've left an Excel spreadsheet or PowerPoint presentation on their website
- Other miscellaneous file types suited to that target

Google Hacking Database (GHDB)

- Google Hacking Database
  - https://www.exploit-db.com/google-hacking-database
- Shell history files in interesting domains
  - site:site_name intitle:index.of bash_history
- Robots.txt file
  - Robots.txt disallow filetype:txt
- Nessus scan results
  - intitle:"Nessus Scan Report" "This file was generated by Nessus"

Reconnaissance Using Shodan

- Shodan is the world's first search engine for Internet-connected devices (IoT)



Basic Search Filters

- **city**: find devices in a particular city
- **country**: find devices in a particular country
- **geo**: you can pass it coordinates
- **hostname**: find values that match the hostname
- **net**: search based on an IP or /x CIDR
- **os**: search based on operating system
- **port**: find particular ports that are open
- **before/after**: find results within a timeframe

Recon-ng

- Recon-ng is written in Python by Tim Tomes
- Several dozen different recon **module**, organized into groups
- Stores information in a database which can be used for analysis and exporting
- "Tab" auto completes to simplify command typing
- Can run bash commands at the Recon-ng prompt
  - [recon-ng] > shell ifconfig