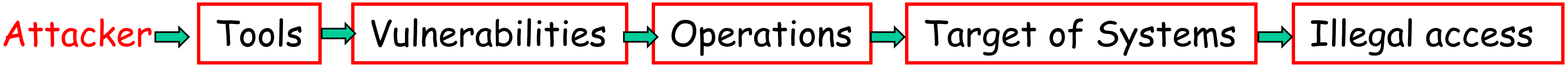
بسم الله الرحمن الرحیم
اثر احسان بهشتی
سنة ۱٤۳٦
۱۳۹٤

Attack Model

General model of attack

- An attacker tries to take control of the target system by using attack tools or exploiting the vulnerabilities of the target system.



Attacker → Tools → Vulnerabilities → Operations → Target of Systems → Illegal access

Attack Phases

- Phase 1: Reconnaissance
- Phase 2: Scanning
- Phase 3: Gaining access
  - Application/OS attacks
  - Network attacks/DoS attacks
- Phase 4: Maintaining access
- Phase 5: Covering tracks and hiding

Recon

- Before bank robber robs a bank…
  - Visit the bank
  - Make friends with an employee (inside info)
  - Study alarm system, vault, security guard’s routine, security cameras placement, etc.
  - Plan arrival and get away
- Most of this is not high tech
- Similar ideas hold for info security

Motivation

Recon helps us make intelligent targeting and attack decisions

- What do we know about the user or organization that will increase our likelihood of success of a phish or SE call?
- Knowledge of the username format and a list of users will make guessing more effective and efficient
- What do we know about the hardware and software that could make lateral movement easier?

Targets

Organization	Goals
	Mergers and Acquisitions
	Projects and Products
	Recent news
Infrastructure	IP Addresses
	Hostnames
	Software & Hardware
Employees	Usernames
	Email addresses
	Breached credentials
	Roles

Types of Shared Data

Intentional Sharing

- URLs and websites
- Project names
- Annual reports
- Press releases
- Job requirements

Unintentional Sharing

- Account information in third-party breaches
- Employees on social media
- File metadata
- Server banners

```
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.29
```

Infrastructure

Learn about the live systems, including software and hardware

- Find IP addresses and subnet ranges
- DNS and host names – these are a must for web attacks
- Listening ports and services
- Determine software and hardware in use

Hostname Information

- Hostnames often indicate their purpose
- For password spraying, look hostnames containing the following:
  - VPN sign-on portals: `vpn`, `access`
  - Citrix StoreFront portals: `ctx`, `citrix`, `storefront`
  - Online email: `mail`, `autodiscover`, `owa`
  - Hostnames containing `login`, `portal`, `sso`, `adfs`, or `remote` are also good targets

Interesting DNS Records

NS	Nameserver record
A	Address record for IPv4 address for a given hostname
AAAA	Quad-A" record for IPv6 address for a given hostname
MX	Mail Exchange record
TXT	Text record
CNAME	Canonical Name record
SOA	Start of Authority record
PTR	Pointer for inverse lookups record
SRV	Service location record

DNS Recorded Example

```
example.com.  3600  IN  NS  ns1.example.com.
example.com.  3600  IN  NS  ns2.example.com.
example.com.  3600  IN  A  93.184.216.34
example.com.  3600  IN  AAAA  2001:0db8:85a3:0000:0000:8a2e:0370:7334
example.com.  3600  IN  MX  10 mail1.example.com.
example.com.  3600  IN  MX  20 mail2.example.com.
example.com.  3600  IN  TXT  "v=spf1 include:_spf.example.com ~all"
www.example.com.  3600  IN  CNAME  example.com.
example.com.  3600  IN  SOA  ns1.example.com. admin.example.com. (
                2024101201 ; serial number
                3600       ; refresh (1 hour)
                600        ; retry (10 minutes)
                1209600    ; expire (2 weeks)
                86400      ; minimum TTL (1 day)
              )
34.216.184.93.in-addr.arpa.  3600  IN  PTR  example.com.
_sip._tcp.example.com.  3600  IN  SRV  10 60 5060 sipserver.example.com.
```

The Dig Command

- The dig command in most Linux can perform zone transfers

```
$ dig @[server] [name] [type]
```

- The type can be ANY, A, MX, and so on; the default is A records
- With a -t flag, we can specify zone transfer

```
$ dig @1.2.3.4 mydomain.com -t AXFR
```

- Use `+norecursive` or `+recursive` (default) to toggle recursion
- Simplify output with `+noall +answer`

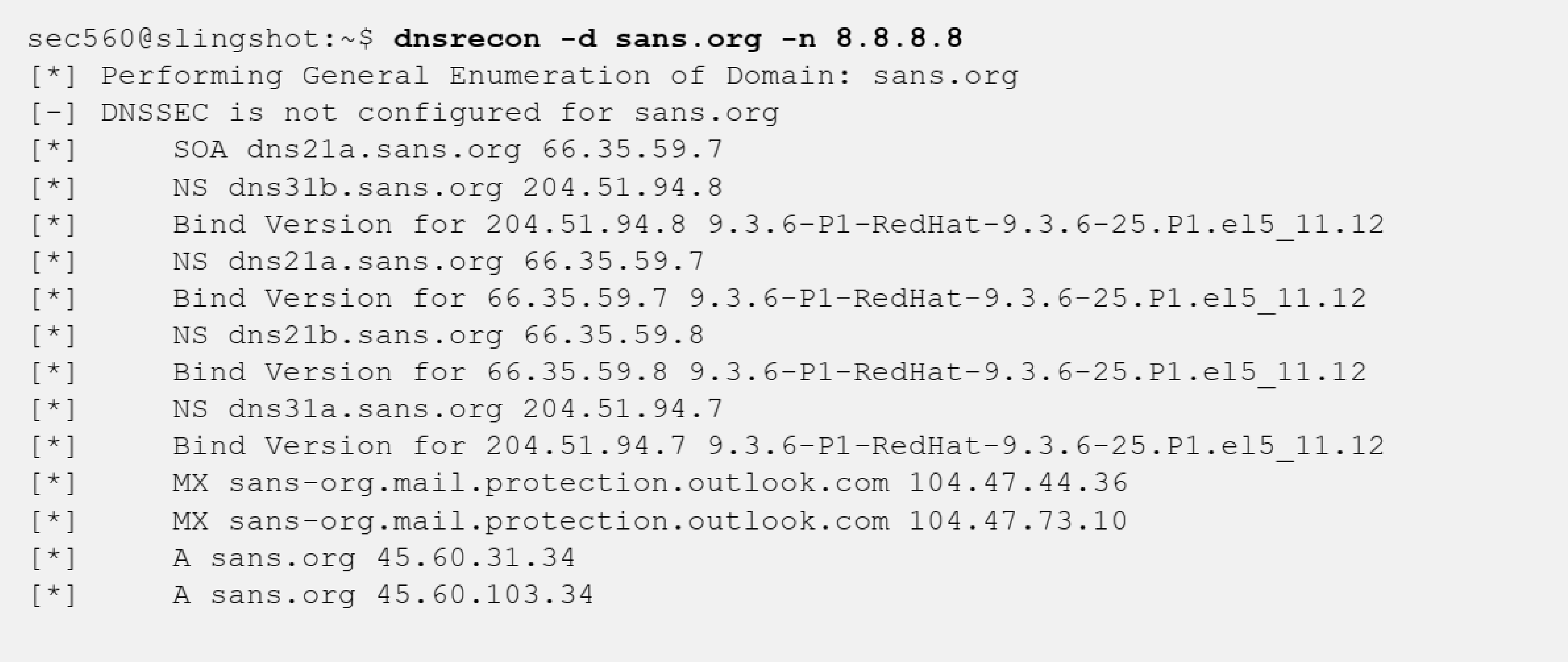
DNSRecon

- Multi-threaded DNS recon tool by Carlos Perez (@darkoperator)
  - Available at https://www.github.com/darkoperator/dnsrecon

```
dnsrecon -d domain.tld -t type
```

```
dnsrecon -d example.com
Zone Transfer Attempt: dnsrecon -d example.com -t axfr
Reverse Lookup: dnsrecon -r 192.168.1.0/24
Brute Force Subdomains: dnsrecon -d example.com -D /path/to/subdomains.txt -t brt
```

DNSRecon Usage

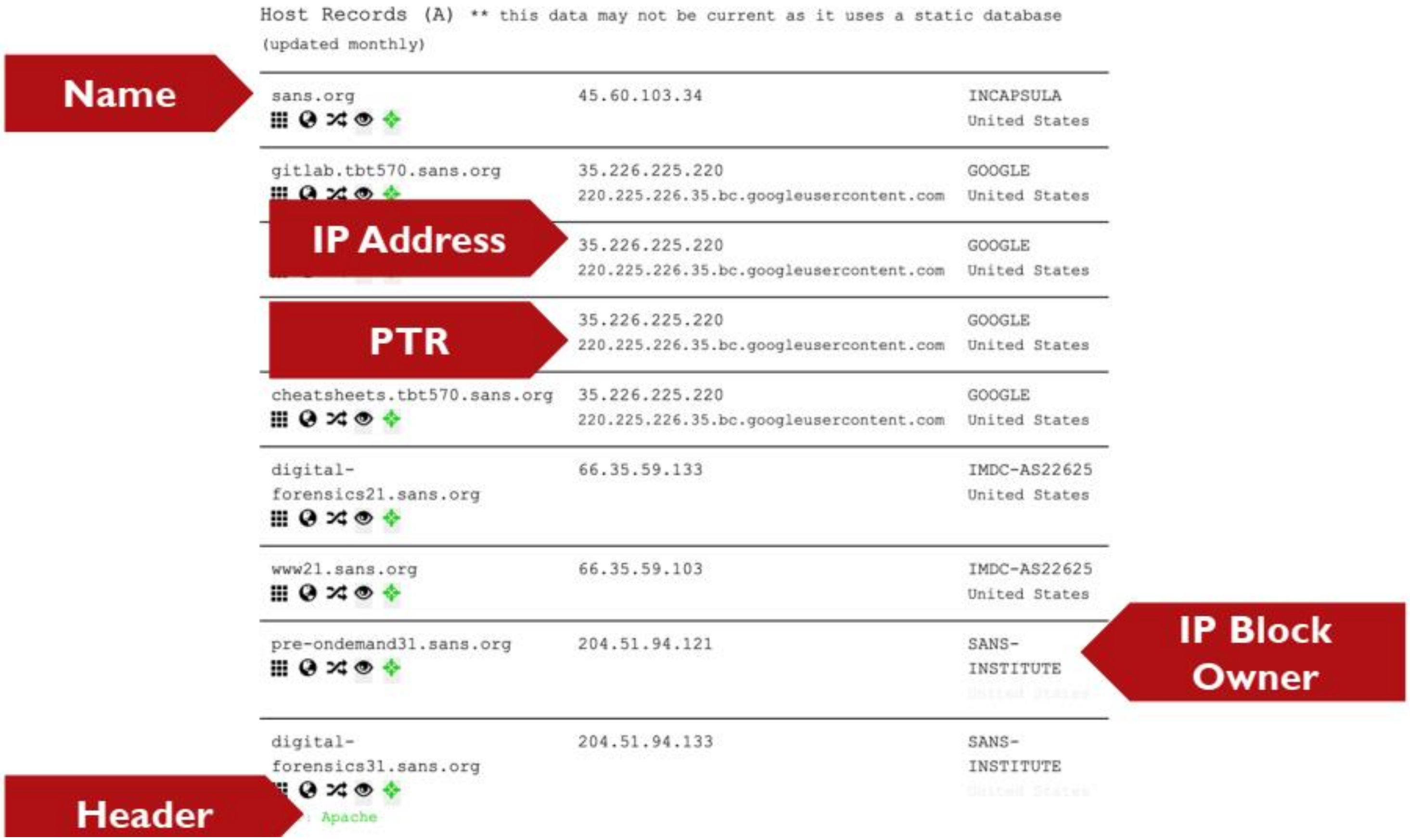


```
sec560@slingshot:~$ dnsrecon -d sans.org -n 8.8.8.8
[*] Performing General Enumeration of Domain: sans.org
[-] DNSSEC is not configured for sans.org
[*]     SOA dns21a.sans.org 66.35.59.7
[*]     NS dns31b.sans.org 204.51.94.8
[*]     Bind Version for 204.51.94.8 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.12
[*]     NS dns21a.sans.org 66.35.59.7
[*]     Bind Version for 66.35.59.7 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.12
[*]     NS dns21b.sans.org 66.35.59.8
[*]     Bind Version for 66.35.59.8 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.12
[*]     NS dns31a.sans.org 204.51.94.7
[*]     Bind Version for 204.51.94.7 9.3.6-P1-RedHat-9.3.6-25.P1.el5_11.12
[*]     MX sans-org.mail.protection.outlook.com 104.47.44.36
[*]     MX sans-org.mail.protection.outlook.com 104.47.73.10
[*]     A sans.org 45.60.31.34
[*]     A sans.org 45.60.103.34
```

DNSDumpster (1)

- Provides a list of DNS A records for a given domain
  - Free version provides up to 100 A records.
  - The paid version of dnsdumpster at hackertarget.com provides the full list as well as additional services
- MX and TXT records disclose cloud email services and spam/malware filters
- Autonomous System Numbers (ASNs) can have the target’s name
  - ASNs with the target’s name provide proof of in-scope hosts
  - Can lead to additional domain name discovery
- DNSDumpster is located at https://dnsdumpster.com

DNSDumpster (2)



Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

sans.org	45.60.103.34	INCAPSULA United States
gitlab.tbt570.sans.org	35.226.225.220 220.225.226.35.bc.googleusercontent.com	GOOGLE United States
	35.226.225.220 220.225.226.35.bc.googleusercontent.com	GOOGLE United States
	35.226.225.220 220.225.226.35.bc.googleusercontent.com	GOOGLE United States
cheatsheets.tbt570.sans.org	35.226.225.220 220.225.226.35.bc.googleusercontent.com	GOOGLE United States
digital-forensics21.sans.org	66.35.59.133	IMDC-AS22625 United States
www21.sans.org	66.35.59.103	IMDC-AS22625 United States
pre-ondemand31.sans.org	204.51.94.121	SANS-INSTITUTE United States
digital-forensics31.sans.org : Apache	204.51.94.133	SANS-INSTITUTE United States

Name

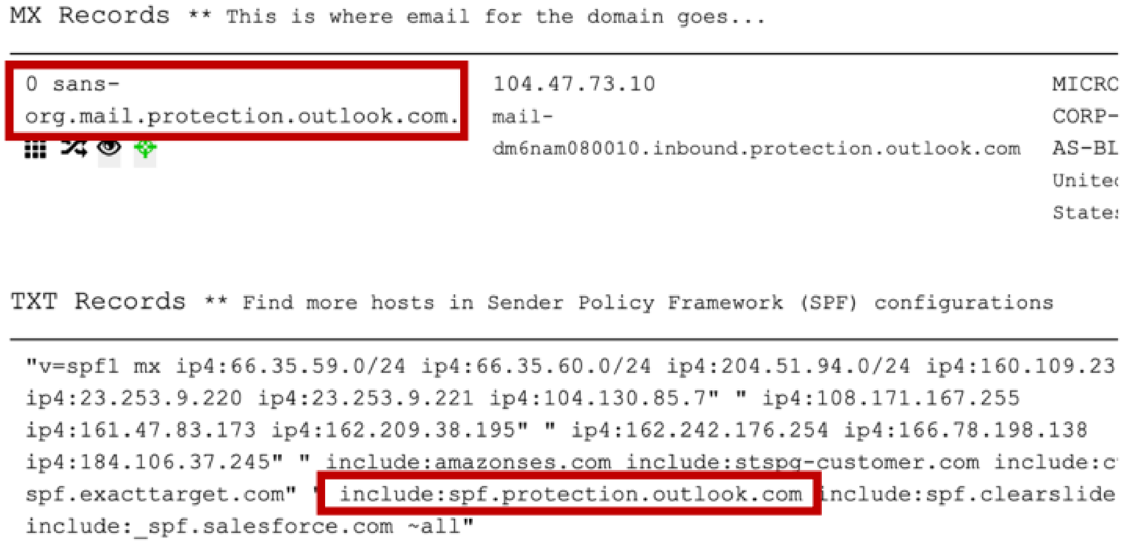
IP Address

PTR

IP Block Owner

Header

DNSDumpster (3)

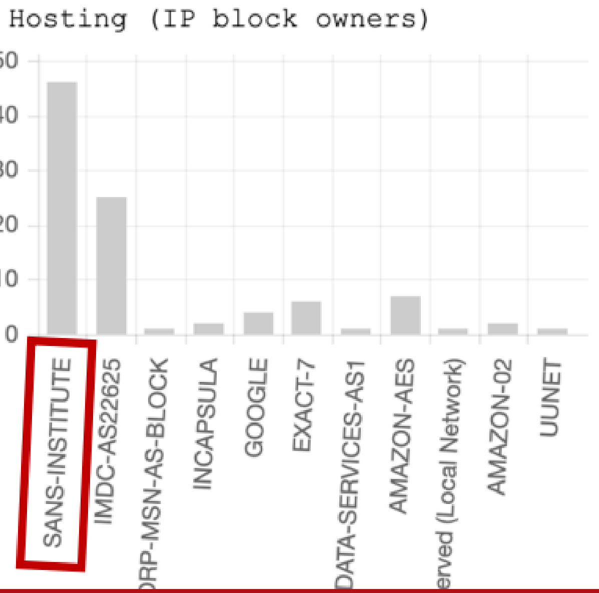


```
MX Records ** This is where email for the domain goes...

0 sans-                                  104.47.73.10                                  MICRO
org.mail.protection.outlook.com.         mail-                                         CORP-
                                         dm6nam080010.inbound.protection.outlook.com   AS-BL
                                                                                       Unite
                                                                                       State

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"v=spf1 mx ip4:66.35.59.0/24 ip4:66.35.60.0/24 ip4:204.51.94.0/24 ip4:160.109.23
ip4:23.253.9.220 ip4:23.253.9.221 ip4:104.130.85.7" " ip4:108.171.167.255
ip4:161.47.83.173 ip4:162.209.38.195" " ip4:162.242.176.254 ip4:166.78.198.138
ip4:184.106.37.245" " include:amazonses.com include:stspg-customer.com include:c
spf.exacttarget.com" " include:spf.protection.outlook.com include:spf.clearslide
include:_spf.salesforce.com ~all"
```



Hosting (IP block owners)

Email Hosted in Office 365 (Cloud Attacks)

Block owner containing "SANS" (possible more targets)

IP Address Assignment WHOIS Databases

Query the registries for IP ranges to find additional targets

- Regional Internet Registries (RIRs) offer Whois databases that store information about IP address block assignments
- Provide a company or domain name, and they tell you if there is an address range officially assigned to it
  - IPv4 and IPv6 address assignment and CIDR block
  - Autonomous System (AS) number assignment
  - DNS information
- Many orgs get addresses from their ISP (not self owned)
- Results may vary. You may get:
  - Actual addresses assignment
  - Nothing at all
  - A huge address space, far bigger than that allotted to this one organization (you are likely seeing whole ISP)

ARIN
American Registry for Internet Numbers

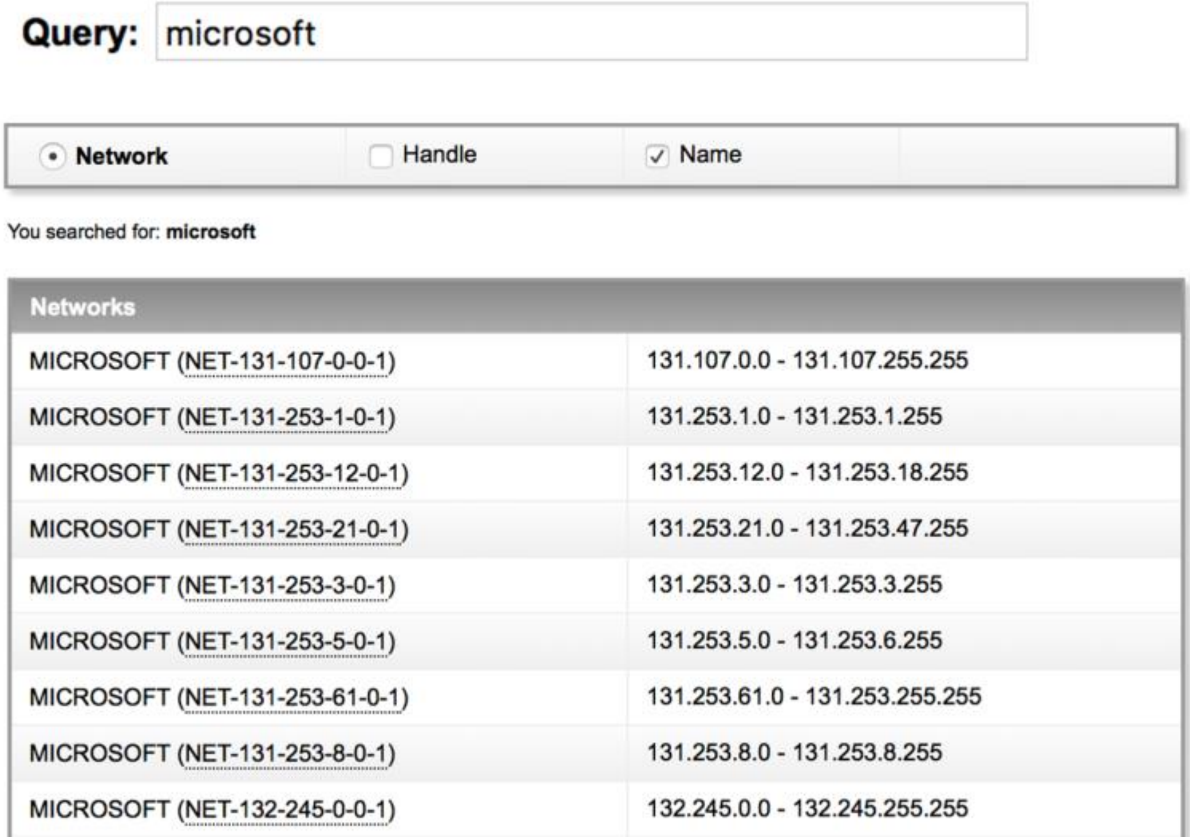
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

AFRINIC

APNIC

lacnic

Sample ARIN Lookups: Network



Query: microsoft

● **Network** □ Handle ☑ Name

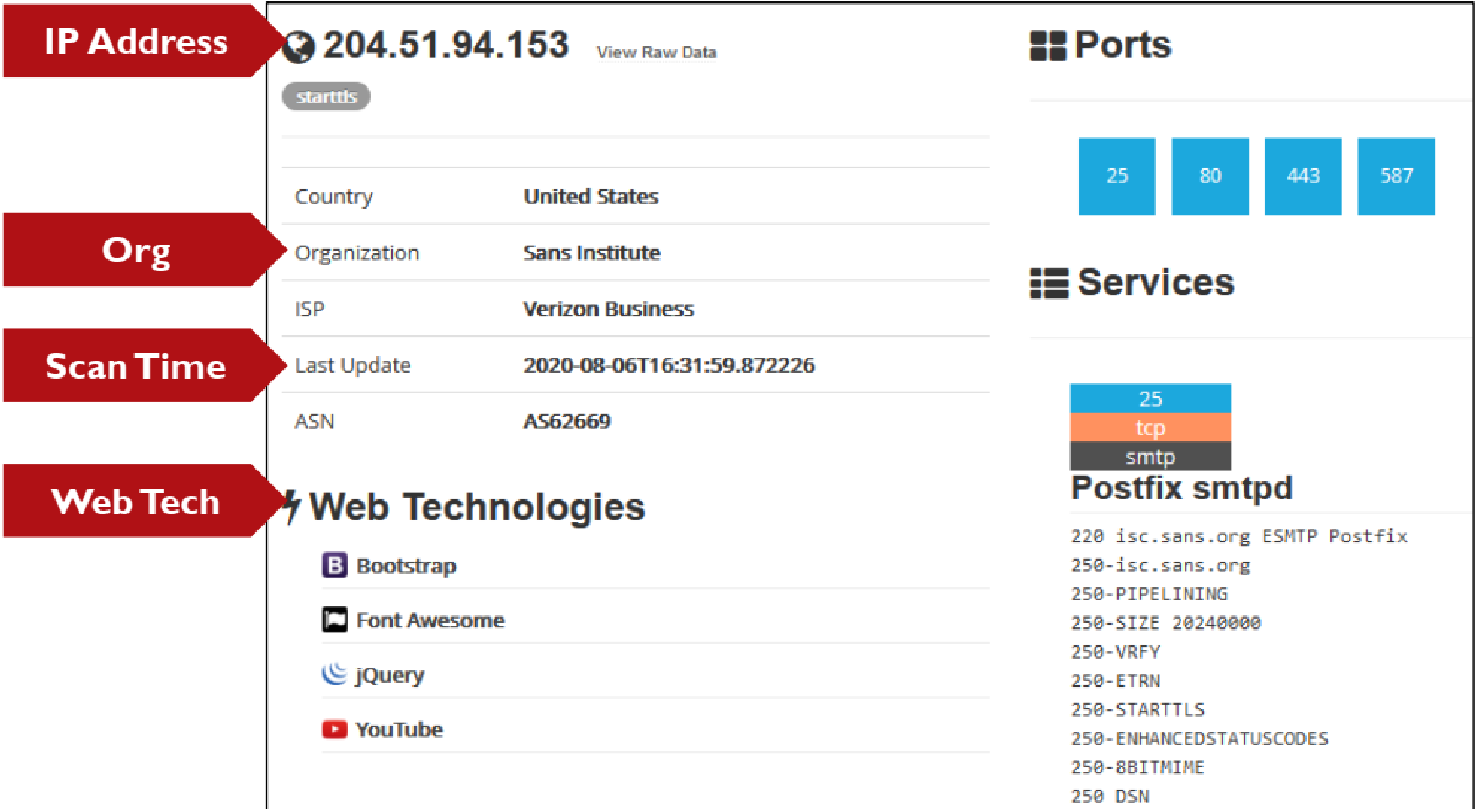
You searched for: **microsoft**

Networks	
MICROSOFT (NET-131-107-0-0-1)	131.107.0.0 - 131.107.255.255
MICROSOFT (NET-131-253-1-0-1)	131.253.1.0 - 131.253.1.255
MICROSOFT (NET-131-253-12-0-1)	131.253.12.0 - 131.253.18.255
MICROSOFT (NET-131-253-21-0-1)	131.253.21.0 - 131.253.47.255
MICROSOFT (NET-131-253-3-0-1)	131.253.3.0 - 131.253.3.255
MICROSOFT (NET-131-253-5-0-1)	131.253.5.0 - 131.253.6.255
MICROSOFT (NET-131-253-61-0-1)	131.253.61.0 - 131.253.255.255
MICROSOFT (NET-131-253-8-0-1)	131.253.8.0 - 131.253.8.255
MICROSOFT (NET-132-245-0-0-1)	132.245.0.0 - 132.245.255.255

Shodan

- Regularly scans available services and ports on hosts connected to the internet
  - Port Scan results without accessing the target
- SSL Certificate Information
  - SSL certificate can reveal additional subdomains
  - Expired certificates can create social engineering scenarios
- IP Address Geolocation
  - Helps with verifying in-scope hosts when dealing with netblocks

Shodan Search for isc.sans.org



204.51.94.153 View Raw Data

starttls

Country	United States
Organization	Sans Institute
ISP	Verizon Business
Last Update	2020-08-06T16:31:59.872226
ASN	AS62669

Web Technologies

- Bootstrap
- Font Awesome
- jQuery
- YouTube

Ports

25 80 443 587

Services

25
tcp
smtp

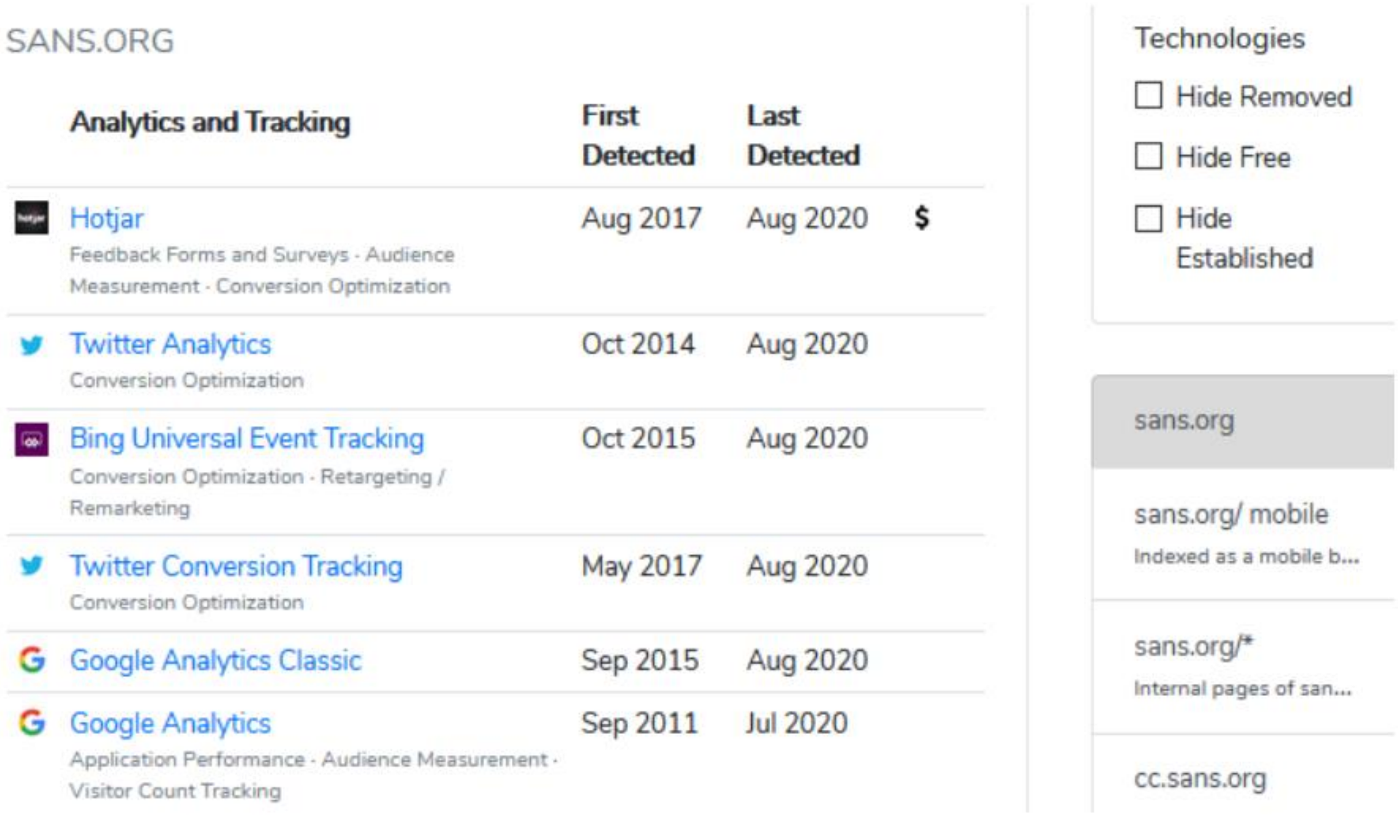
Postfix smtpd

```
220 isc.sans.org ESMTP Postfix
250-isc.sans.org
250-PIPELINING
250-SIZE 20240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

BuiltWith (1)

- BuiltWith.com compiles lists of technologies used in web server and software frameworks for target web services
  - List is broken down by the subdomain where the technology was observed, when the technology was first observed, and the last recorded time the technology was in use
- Maintains lists of related websites
  - Related site list contains domains directly related to the target domain
  - Also contains IP address history of each related domain

BuiltWith (2)



SANS.ORG

Analytics and Tracking	First Detected	Last Detected	
Hotjar Feedback Forms and Surveys · Audience Measurement · Conversion Optimization	Aug 2017	Aug 2020	$
Twitter Analytics Conversion Optimization	Oct 2014	Aug 2020	
Bing Universal Event Tracking Conversion Optimization · Retargeting / Remarketing	Oct 2015	Aug 2020	
Twitter Conversion Tracking Conversion Optimization	May 2017	Aug 2020	
Google Analytics Classic	Sep 2015	Aug 2020	
Google Analytics Application Performance · Audience Measurement · Visitor Count Tracking	Sep 2011	Jul 2020	

Technologies

☐ Hide Removed

☐ Hide Free

☐ Hide Established

sans.org

sans.org/ mobile
Indexed as a mobile b...

sans.org/*
Internal pages of san...

cc.sans.org

Useful Google Search Directives: Sites and Links

`site:` – Searches only within the given domain

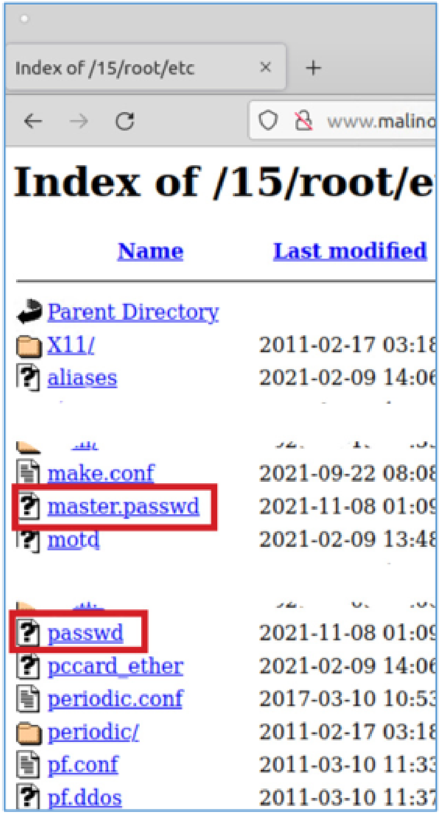
- Example: `site:sans.org "web app"`
- Find pages with the phrase "web app" that are on sans.org

`intitle:` – Page title matches search criteria

- Example: `intitle:index.of passwd`
- Finds indexed web directories with the word "passwd" in the directory listing, possibly an /etc/passwd file

`inurl:` – URL matches the search criteria

- Example: `inurl:viewtopic.php`
- Finds a script used in phpBB (a history of significant flaws)

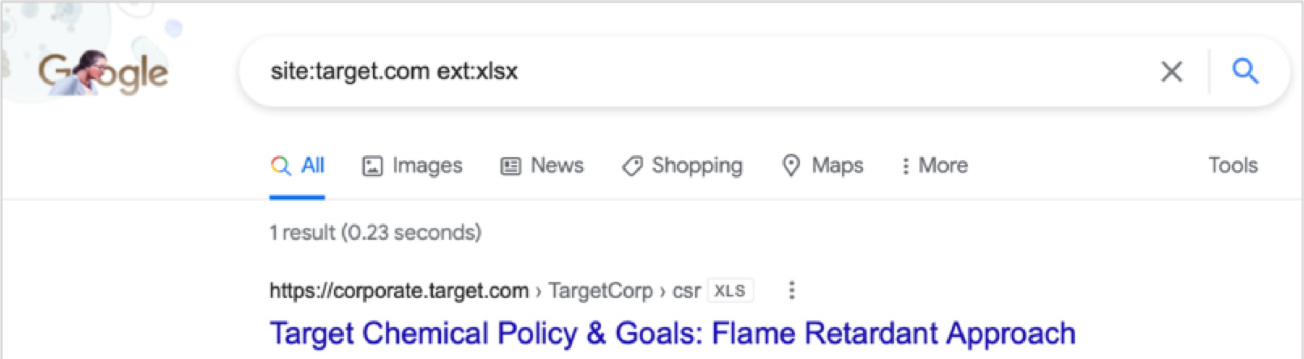


Index of /15/root/e

Name	Last modified
Parent Directory	
X11/	2011-02-17 03:18
aliases	2021-02-09 14:06
make.conf	2021-09-22 08:08
master.passwd	2021-11-08 01:09
motd	2021-02-09 13:48
passwd	2021-11-08 01:09
pccard_ether	2021-02-09 14:06
periodic.conf	2017-03-10 10:53
periodic/	2011-02-17 03:18
pf.conf	2011-03-10 11:33
pf.ddos	2011-03-10 11:37

Searching for File Types

- Google identifies hundreds of different file types as it scours the internet, such as .pdf, .doc[x], .xls[x], .ppt[x], .cgi, .php, .asp, and many others
- "filetype:" and "ext:" directives search for only a specific kind of file
- Also, note that Google sometimes mistakes a given file type
- Combine with "site:" to restrict to your scope



site:target.com ext:xlsx

1 result (0.23 seconds)

https://corporate.target.com › TargetCorp › csr XLS

Target Chemical Policy & Goals: Flame Retardant Approach

Inventory of Discoverable Flaws via Google

- Johnny Long created a huge inventory of Google searches to find vulnerable systems: the Google Hacking Database, with each search called a "Google dork"
- The folks at Exploit-DB took it over and now operate it at: https://www.exploit-db.com/google-hacking-database
- More than 1,000 entries in this database in the following categories:
  - Advisories and vulnerabilities
  - Error messages
  - Files containing juicy info
  - Files containing passwords
  - Files containing usernames
  - Footholds
  - Login portals
  - Network or vuln data
  - Sensitive directories
  - Sensitive online shopping info
  - Online devices
  - Vulnerable files
  - Vulnerable servers
  - Web server version detection

Some Interesting Samples from the GHDB

SQL Injection	`inurl:".php?id=" "You have an error in your SQL syntax"`
Bash History	`intitle:"index of" ./bash_history`
Login pages	`inurl:/login.asp "Configuration and Management"`
Admin SQL Files	`intext:admin ext:sql inurl:admin`

Add `site:yourtarget.com` to restrict results to your target organization