جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

أكاديمية كاوست
KAUST ACADEMY

DAY 1

RECON & OSINT

Dr. Ali Hassan
Instructional Professor, CEMSE Division, King Abdullah University of Science and Technology,
Contact: ali.hassan.1@kaust.edu.sa

Site Manager:
Mahmoud Ellouh
Teacher Assistants:
Mohammed Alqurashi
Osama Aldossary
Jumanah Alharbi
Ritaj Alghamdi
Salman Aldhalaan

ACKNOWLEDGEMENT

Some of the material presented here is prepared by:

Dr. Rashid Tahir,
Assistant Professor,
CSFC Department
University of Prince Mugrin, Madinah

WHAT IS RECONNAISSANCE

"Recon is the science of *gathering information* about a target"

- **Profile** a target (a user, a company or any victim) in depth
- Relies heavily on **OSINT**
  - Open-Source Intelligence (publicly available information that can prove to be helpful to the attacker)
    - Collect and analyze everything that's "out there" pertaining to the target
  - Direct communication with the target mostly does not happen
- Used in various **domains**, including cybersecurity, law enforcement, business intelligence, and national security

PHASES OF HACKING

RECONNAISSANCE STAGE

FOOTPRINTING

SCANNING

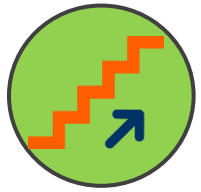
ENUMERATION

Exploitation

OSINT + OTHER TOOLS

Post Exploitation

SYSTEM HACKING



GAINING ACCESS

MAINTAINING ACCESS

COVERING TRACKS & BACKDOORING

TYPES OF RECON

ACTIVE vs PASSIVE

TYPES OF RECON

- **Passive**
  - Relies heavily on OSINT techniques
  - Does not reveal the source of the activity (anonymity)
  - Information can be inaccurate or out-of-date
- **Active**
  - Interact with the system directly (tools communicate with the target)
    - Direct victim profiling via scanning and enumeration-based invasive techniques
  - Information is accurate and up-to-date
  - Can reveal the source of the activity (identity is compromised)

WE WILL SEE BOTH ACTIVE & PASSIVE RECON (OSINT) TOOLS & TECHNIQUES

RECON – ACTIVE & PASSIVE APPROACHES

- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning
- Service Fingerprinting

Some techniques will fall under active while others will be passive recon

RECON – ACTIVE & PASSIVE APPROACHES

- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning
- Service Fingerprinting

RECON: WEB DATA & DOMAIN RECON

- Valuable information on web pages
  - **HTML comments**
    - Sensitive information left there by developers
  - **Website Mirroring & Web Spiders/Crawlers**
    - Technique used to copy publicly available and linked content for offline analysis
  - **Directory Brute Forcing and Forced Browsing**
    - Technique used to discover hidden, restricted and unlinked content on the web server
  - **Google Hacking via Dorks & Advanced Search**
    - Advanced search queries that return very specific data from websites
  - **Email Harvesting**
    - Gathering email addresses on individual victims or potential target in an organization

WEB DATA RECON

1. HTML COMMENTS

HTML COMMENTS – EXAMPLE 1

```html
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>JDBC Server Configuration</title>
</head>
<body>
    <header>
        <h1>JDBC Server Configuration</h1>
    </header>

    <nav>
        <ul>
            <li><a href="#overview">Overview</a></li>
            <li><a href="#settings">Settings</a></li>
            <li><a href="#connection">Connection</a></li>
        </ul>
    </nav>

    <section id="overview">
        <h2>Overview</h2>
        <p>This page contains configuration information for the JDBC server used in our application.</p>
    </section>

    <section id="settings">
        <h2>Settings</h2>
        <p>Configure the JDBC server settings here. Be cautious when calling the server with a large number of arguments.</p>
            <!-- FIXME: calling this with more than 30 args kills the JDBC servers -->
    </section>

    <section id="connection">
        <h2>Connection</h2>
        <p>Specify the connection details for the JDBC server here.</p>
    </section>

    <footer>
        <p>&copy; Rashid Tahir - Ethical Hacking</p>
    </footer>
</body>
</html>
```

HTML COMMENTS – EXAMPLE 2

```html
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <meta name="description" content="Example HTML Page with DB Connection">
    <meta name="author" content="Your Name">
    <title>DB Connection Test Page</title>
</head>
<body>
    <h1>DB Connection Test Page</h1>
    <p>This page is for testing database connections.</p>

    <!-- Use the DB administrator username for testing: f@keU$er -->
    <!-- Use the DB administrator password for testing: f@keP@a$$w0rD -->

    <form action="process_connection.php" method="post">
        <label for="username">Username:</label>
        <input type="text" id="username" name="username" required>
        <br>
        <label for="password">Password:</label>
        <input type="password" id="password" name="password" required>
        <br>
        <input type="submit" value="Connect">
    </form>

    <footer>&copy; Rashid Tahir - Ethical Hacking</footer>
</body>
</html>
```

HTML COMMENTS – EXAMPLE 3

```html
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <meta name="description" content="User Data Table">
    <meta name="author" content="Your Name">
    <title>User Data</title>
    <style>
        /* Add your CSS styles here */
        .table2 {
            display: flex;
            flex-direction: column;
        }
        .col1 {
            font-weight: bold;
            margin-right: 5px;
        }
        .col2 {
            margin-bottom: 10px;
        }
    </style>
</head>
<body>
    <h1>User Data</h1>
    <p>Below is a list of active users:</p>

    <div class="table2">
        <div class="col1">1</div><div class="col2">Mary</div>
        <div class="col1">2</div><div class="col2">Peter</div>
        <div class="col1">3</div><div class="col2">Joe</div>

        <!-- Query: SELECT id, name FROM app.users WHERE active='1' -->
    </div>

    <footer>&copy; Rashid Tahir - Ethical Hacking</footer>
</body>
</html>
```

HTML COMMENTS: IT'S A REAL ISSUE

CVE-ID	
CVE-2007-6197	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The Plumtree portal in BEA AquaLogic Interaction 5.0.2 through 5.0.4 and 6.0.1.218452 allows remote attackers to obtain version numbers and internal hostnames by reading comments in the HTML source of any page.

CVE-ID	
CVE-2007-4072	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Webbler CMS before 3.1.6 provides the full installation path within HTML comments in certain documents, which allows remote attackers to obtain sensitive information by viewing the HTML source, as demonstrated by viewing the source generated from index.php.

CVE-2020-4673 Detail

Description

IBM Workload Automation 9.5 stores sensitive information in HTML comments that could aid in further attacks against the system. IBM X-Force ID: 186286.

CVE-2017-3842 Detail

Description

A vulnerability in the web-based management interface of the Cisco Intrusion Prevention System Device Manager (IDM) could allow an unauthenticated, remote attacker to view sensitive information stored in certain HTML comments. More Information: CSCuh91455. Known Affected Releases: 7.2(1)V7.

CVE-ID	
CVE-2009-2431	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

WordPress 2.7.1 places the username of a post's author in an HTML comment, which allows remote attackers to obtain sensitive information by reading the HTML source.

HTML COMMENTS: CWE - 615

Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

CWE TOP 25 Most Dangerous Software Weaknesses

Home > CWE List > CWE- Individual Dictionary Definition (4.2) ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

CWE-615: Inclusion of Sensitive Information in Source Code Comments

Weakness ID: 615
Abstraction: Variant
Structure: Simple

Status: Incomplete

Presentation Filter: Complete

Description

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

HTML COMMENTS: CWE - 546

Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

Top 25 | Top HW CWE | New to CWE Start here!

Home > CWE List > CWE- Individual Dictionary Definition (4.12) ID Lookup:

Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search

CWE-546: Suspicious Comment

Weakness ID: 546
Abstraction: Variant
Structure: Simple

View customized information: Conceptual | Operational | Mapping Friendly | Complete | Custom

Description

The code contains comments that suggest the presence of bugs, incomplete functionality, or weaknesses.

Extended Description

Many suspicious comments, such as BUG, HACK, FIXME, LATER, LATER2, TODO, in the code indicate missing security functionality and checking. Others indicate code problems that programmers should fix, such as hard-coded variables, error handling, not using stored procedures, and performance issues.

CVE, CVSS, CWE, CPE

CVE-2025-1674 Detail

Description

A lack of input validation allows for out of bounds reads caused by malicious or malformed packets.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Zephyr Project **Base Score:** 8.2 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Hyperlink	Resource
https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-x975-8pgf-qh66	Mitigation, Vendor Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-125	Out-of-bounds Read	NIST, Zephyr Project

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

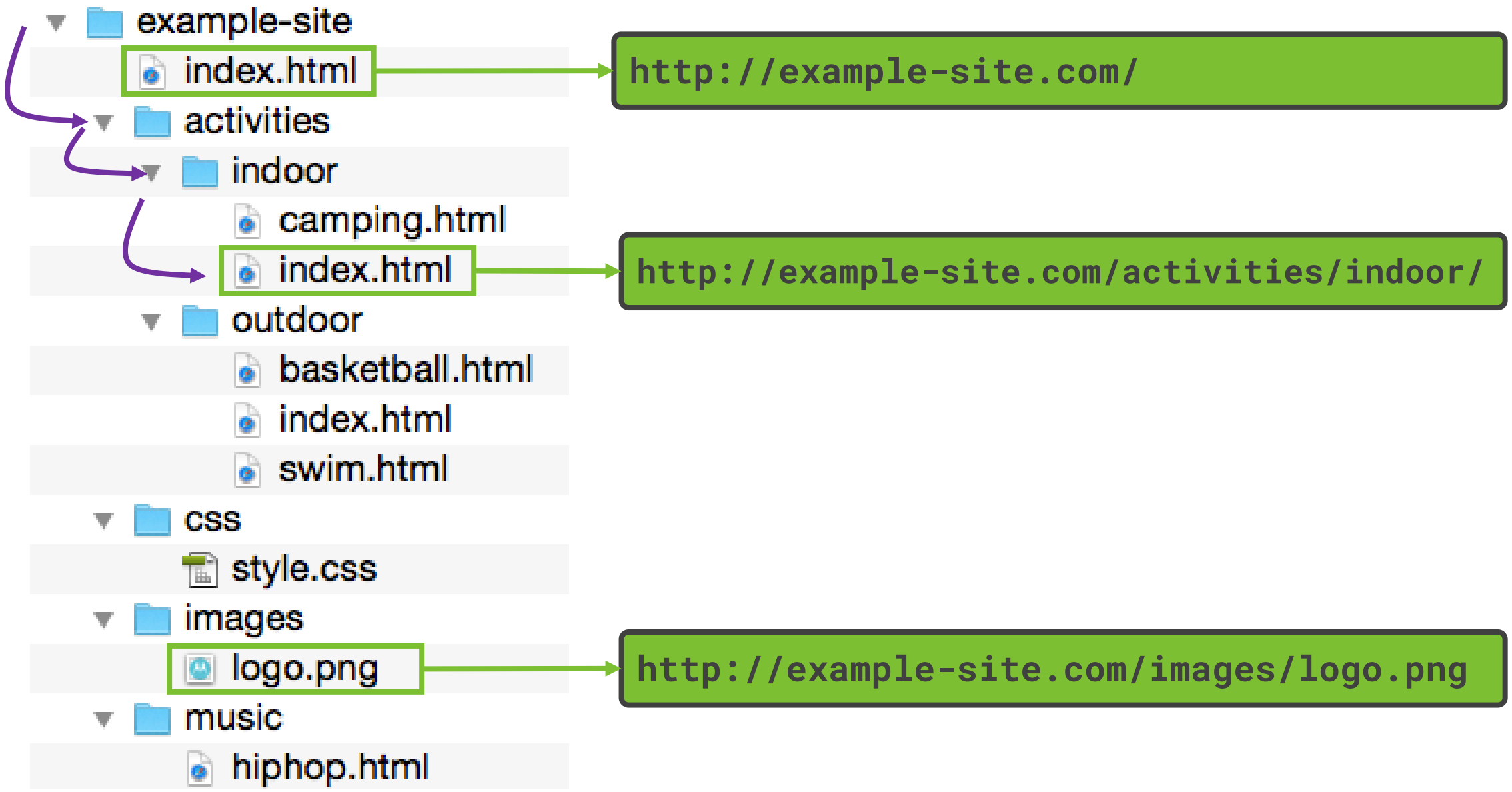
cpe:2.3:o:zephyrproject:zephyr:*:*:*:*:*:*:*:*	**Up to (including)**
Show Matching CPE(s)	**4.0**

https://nvd.nist.gov/
https://www.cve.org/
https://cwe.mitre.org/
https://nvd.nist.gov/products/cpe

2. WEBSITE MIRRORING & CRAWLING

STRUCTURE OF A WEBSITE: DIRECTORIES & FILES

- A typical website has the following files/contents
  - HTML files
  - CSS files
  - Font files
  - JavaScript files
  - Image or media files
  - Many others…
- This content is distributed into various folders/directories and subfolders/subdirectories



Each resource on the webserver can be accessed via a unique URL

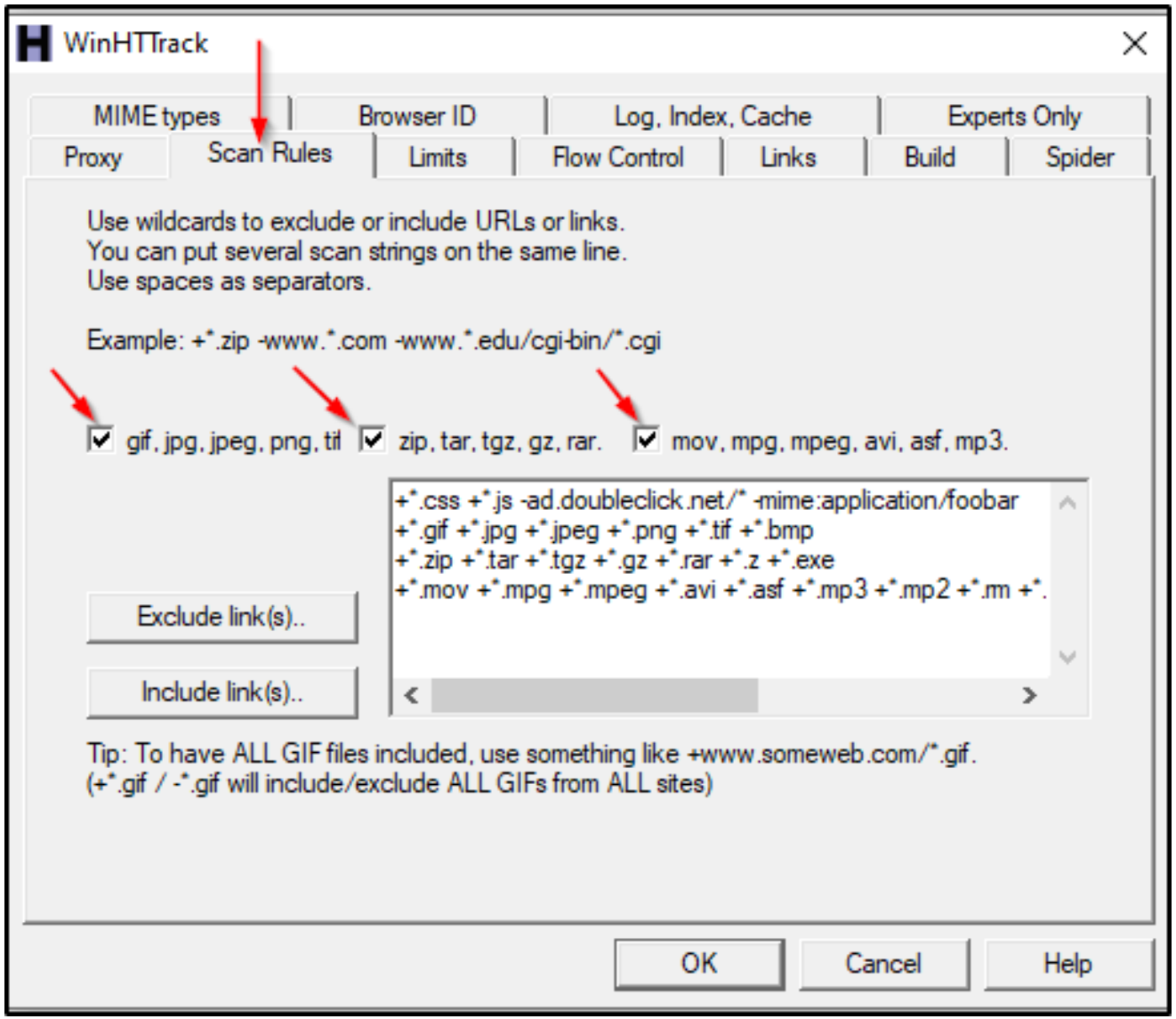
WEBSITE MIRRORING: HOW DOES IT WORK?

- Site Ripping
  - **Download** the **entire website** to your local machine for offline browsing
    - Retrieves the content that is **publicly available** or **linked** on the site
    - Does not look for hidden directories or content (no brute force or dictionaries are used)
    - Tools follow/explore links/references on the main page and then sub-pages
  - Much **easier** to **parse** and **analyze** the website for useful information
    - No further interaction with the live site (no need to send repeated requests for content)
- Many tools exist
  - PageNest
  - BlackWidow
  - HTTrack

WEBSITE MIRRORING: HOW DOES IT WORK?

- Web Spider or Crawler
  - Visit website **homepage** and **follow/open links** to **sub-pages** recursively
    - Content needs to be publicly accessible for this
  - Downloads relevant content in an **automated fashion** matching pre-defined search criteria
    - Regular expressions
    - Certain file extensions (like JPG or PNG)
    - Metadata of Office (Word, PowerPoint, Excel) & PDF documents

HTTRACK



Downloads the entire website

METAGOOFIL

```
root@kali-20  :~# metagoofil -d sans.org -t doc,pdf -l 20 -n 10 -o sans -f html

*****************************************************
*     /\/\    ___| |_ __ _  __ _  ___   ___  / _(_) | *
*    /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | | *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | | *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_| *
*                           |___/                     *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*****************************************************

[-] Starting online search...

[-] Searching for doc files, with a limit of 20
        Searching 100 results...
Results: 5 files found
Starting to download 10 of them:
```

Downloads specific data/metadata from a target website

METAGOOFIL

Usernames harvested

Software list harvested

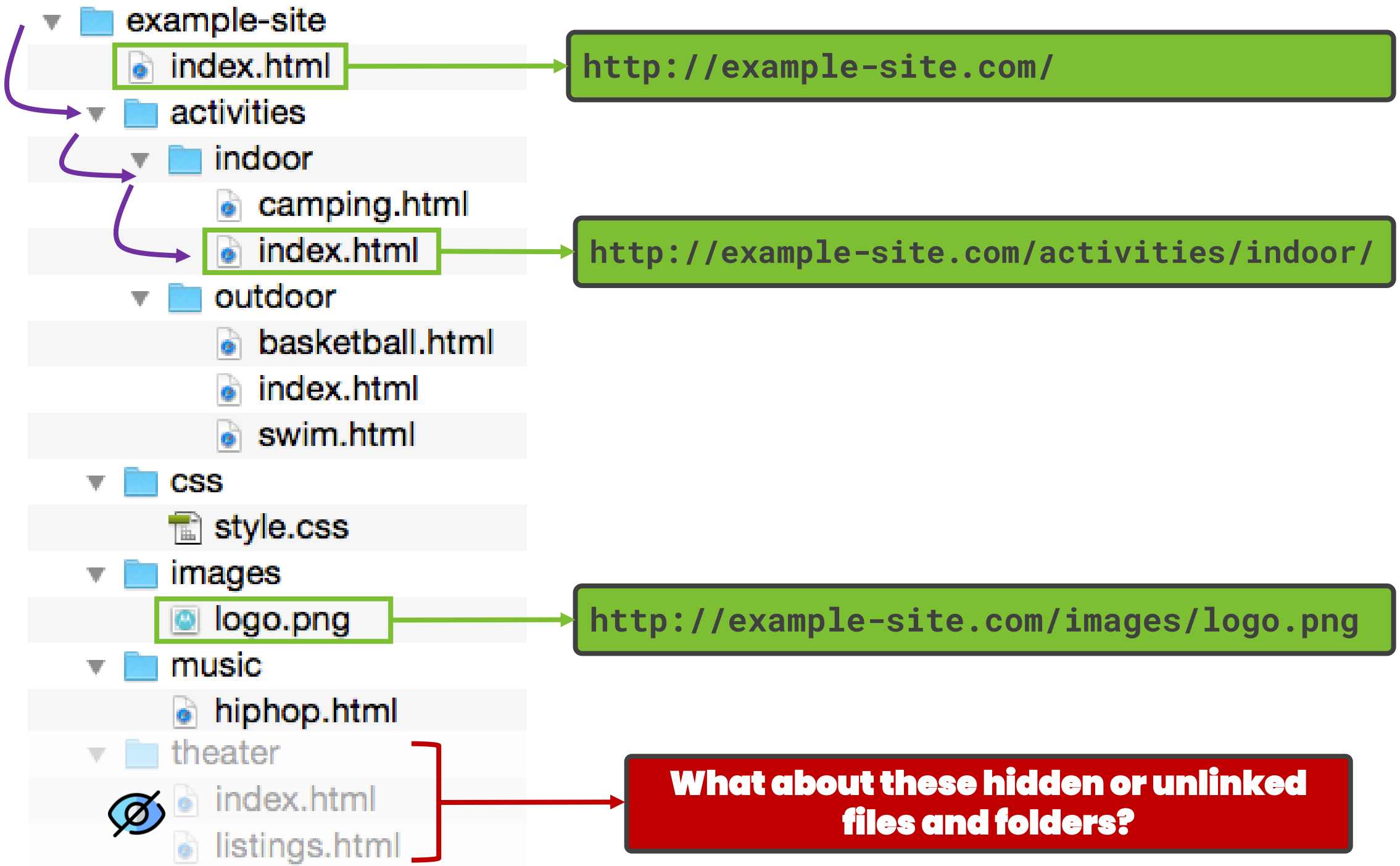
Email IDs harvested

```
[+] List of users found:
--------------------------
Dean Farrington
aswanger
Kyle Wilhoit
Lynn
Brian
Edward

[+] List of software found:
-----------------------------
Microsoft Office Word
Adobe PDF Library 11.0
Adobe InDesign CC 2014 (Windows)
Adobe PDF Library 10.0.1
Adobe InDesign CS6 (Windows)
Acrobat Distiller 6.0 (Windows)
PScript5.dll Version 5.2
www.adlibsys.com:3135-W2KP
Hex Quiz.doc - Microsoft Word
Mac OS X 10.5.6 Quartz PDFContext
Microsoft Word

[+] List of paths and servers found:
---------------------------------------
 Normal.dot

[+] List of e-mails found:
----------------------------
tson@sans
BCorreia@sans
DGilbertson@sans.orgBrian
BCorreia@sans.orgDoDD
BCorreia@sans.orgDoD
8140@sans.org
BCorreia@sans.orgGIAC
BCorreia@sans.orgAbout
BCorreia@sans.orgSANS
symantec_intelligence@symantec.com
webmaster@sans.org.
```

This data has been extracted from doc & pdf files on sans website

QUESTION

CAN WEBSERVERS HAVE HIDDEN OR UNLINKED CONTENT AS WELL?


example-site
index.html
http://example-site.com/
activities
indoor
camping.html
index.html
http://example-site.com/activities/indoor/
outdoor
basketball.html
index.html
swim.html
css
style.css
images
logo.png
http://example-site.com/images/logo.png
music
hiphop.html
theater
index.html
listings.html
What about these hidden or unlinked files and folders?

WEB DATA RECON

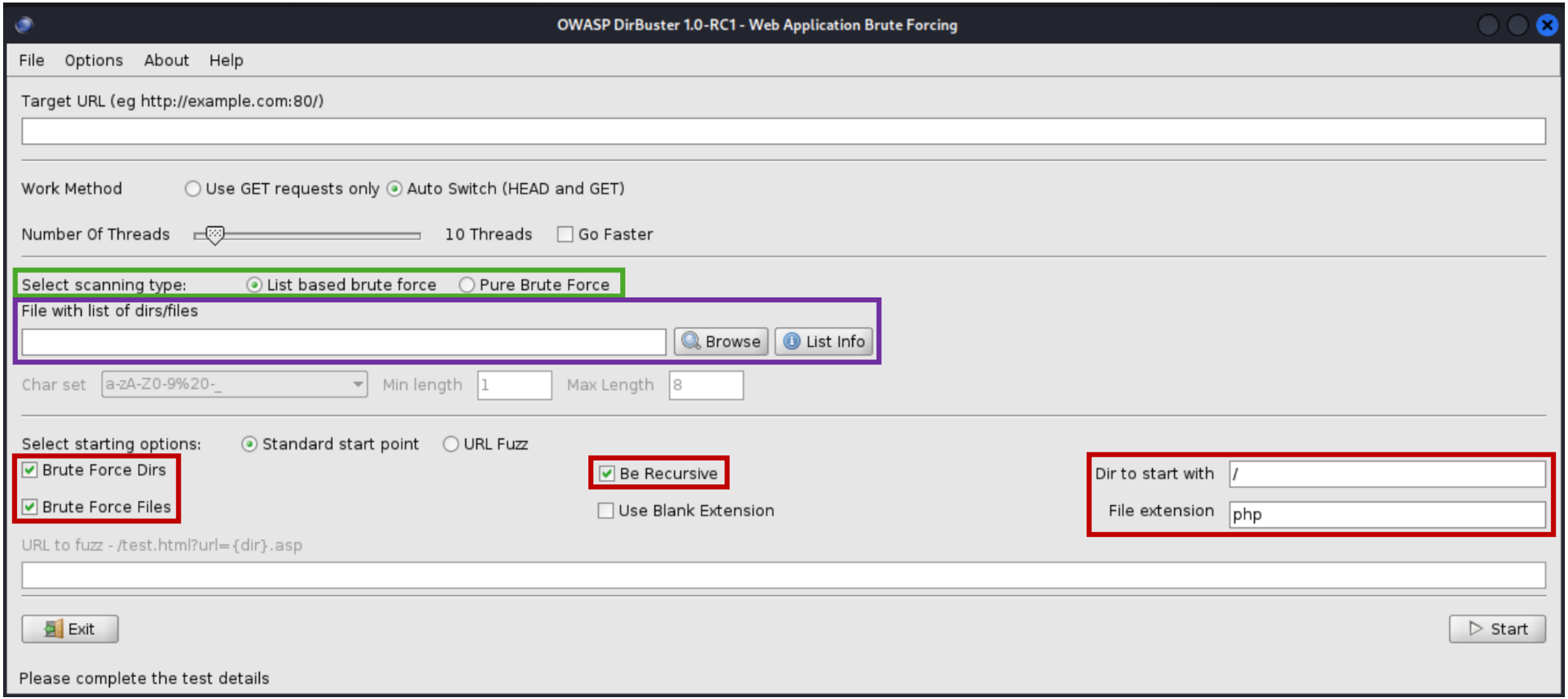
3. DIRECTORY BRUTE FORCING & FORCED BROWSING

DIRECTORY BRUTE FORCING: WHAT IS IT?

- **Systematically** trying different directory and file names to see if they exist on the server
  - Used for accessing **hidden**, **restricted** or **unlinked** content on a website
  - Often a **contextually relevant** list of common directory and file names (**dictionary**) is used
  - For instance, for a university web server, the potential entries in the dictionary could be:
    - Academics
    - Grades
    - Registrar
    - Student Affairs
    - Courses
  - Another option to discover content is to attempt all possible combinations (**brute forcing**)
    - A → Z
    - 0 → 9
    - Combinations of alphabets and digits to cover the entire space of possible directory and file names

TOO TEDIUS & LABORIOUS TO DO THIS MANUALLY!

DIRECTORY BRUTE FORCING



DIRECTORY BRUTE FORCING: MORE TOOLS

- Lots of Web Content Scanners
  - BurpSmartBuster (plug-in for Burp Suite)
  - Dirsearch
  - DIRB (available in Kali with built-in dictionaries)
  - Cansina (available with BlackArch Linux) – Good one!
  - Meg (does not overwhelm the servers)
  - Wfuzz (available in Kali with much more functionality)
  - Gobuster

FORCED BROWSING: WHAT IS IT?

- Directory brute forcing is a **resource-intensive activity** (aggressive)
  - May **trigger security alerts** on the target server
- Instead, strategically **manipulate URLs** to take advantage of vulnerabilities in the application's input validation or authorization mechanisms
  - Attackers attempt to navigate to directories or resources that should be protected but are not due to **flawed security configurations** (improper access control)
  - Targeted approach which is more **stealthy**
  - Feroxbuster is useful for forced browsing
    - Uses brute forcing as well as wordlists (dictionaries)

FEROXBUSTER

FORCED BROWSING: WHAT IS IT?

Date

www.example.com/users/calendar.php/user1/20240715

User ID
(Predictable)

- Allows user1 to check their online calendar
  - No authentication is performed
  - What if we change the username or date in the URL?

www.example.com/users/calendar.php/user2/20240715

- Attacker can easily guess the username and date to gain unauthorized access to other users' calendar

4. GOOGLE HACKING VIA DORKS & ADVANCED SEARCH

GOOGLE DORKS: SEARCH ENGINES

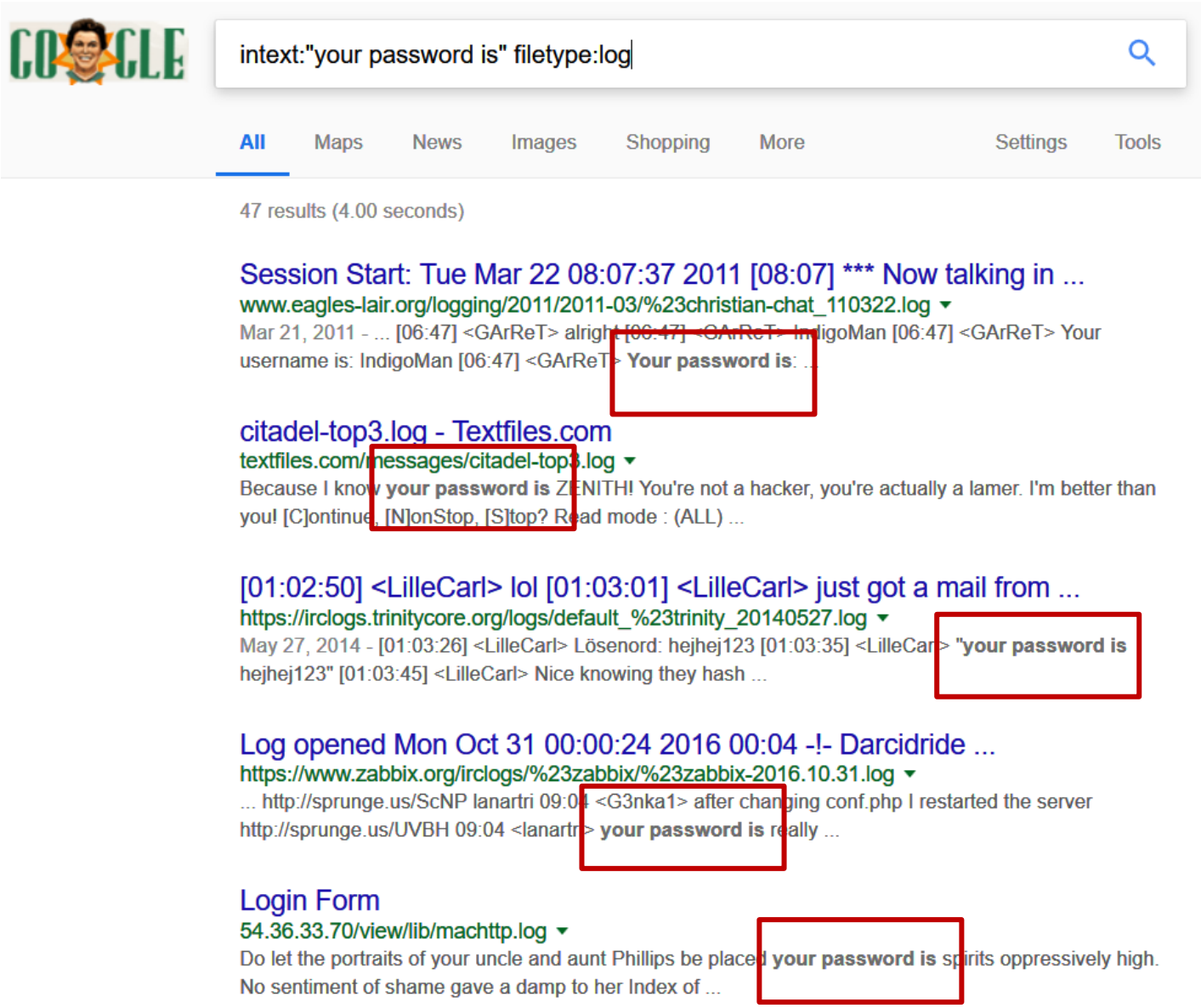
- Advanced Google queries and operators
  - **cache:** Display results from pages stored in Google cache
  - **link:** Display results with links to the specified page
  - **related:** Display similar results
  - **site:** Display results from the queried website only
  - **intitle:** Display results that have searched keywords in title
  - **inurl:** Display results that have searched keywords in the URL

Similarly, try Google Advanced Search!

https://www.recordedfuture.com/threat-intelligence-101/threat-analysis-techniques/google-dorks

https://www.exploit-db.com/google-hacking-database

GOOGLE DORK: intext:"your password is" filetype:log



Returns log files indexed on the web containing the phrase "your password is"

GOOGLE DORK 1: intext:"aws_access_key_id" | intext:"aws_secret_access_key" filetype:json | filetype:yaml

Finds exposed cloud service credentials for Amazon Web Services (AWS)

GOOGLE DORK 2: site:github.com "BEGIN OPENSSH PRIVATE KEY"

Finds OpenSSH private keys on Github

GOOGLE DORK 3: intitle:"Webcam" inurl:WebCam.htm

Let's try this one

Shows homepage of indexed webcams on the Web

Google

intitle:"Webcam" inurl:WebCam.htm

All | Shopping | Images | Videos | Short videos | Forums | Web | More | Tools

Lees-McRae College
https://www.lmc.edu › webcam

Lees-McRae Webcam

Lees-McRae Webcam. BACK to Top. Lees-McRae College. 191 Main Street. Banner Elk
828.898.5241 · Facebook.Instagram. Helpful Links; Campus Safety ...

Home | CERN
https://laser-caltech.web.cern.ch › webcam

webcam

Snapshops from pt5. WebCAM Cessy · Control Room DP2-2 webcam · lhc-webcams.ht

National Park Service (.gov)
https://www.nps.gov › liho › learn › photosmultimedia 28

Lincoln Home Webcam

Jan 31, 2024 — The home grew and changed with the Lincoln family to become the tw
with green shutters visible today. View the Lincoln home and historic area ...

UNICO Hotel Collection
https://www.unicohotelcollection.com › riviera-maya

Live Webcam at Riviera Maya | UNICO 20˚87˚

Webcam Live From UNICO 20°87° Take a look at our best spots directly from paradise. We are waiting for you!

LHC Compact Muon Solenoid Experiment Webcams

There are currently two webcams online

- **Camera 7:** looking at the Underground Experimental Cavern from the Saleve side.
- **Camera 8:** looking out of the window of the 1st Floor of the SCX building that houses the CMS Control room.

GOOGLE HACKING DATABASE (GHDB)

EXPLOIT DATABASE

Google Hacking Database

Filters | Reset All

Show 120

Quick Search

Date Added	Dork	Category	Author
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	Google Dork Submisson For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"	Vulnerable Servers	Kishoreram

5. EMAIL HARVESTING

(NOT RESTRICTED TO WEB PAGES)

EMAIL HARVESTING: HOW DOES IT WORK?

- **Email Harvest**
  - » Gathering emails of potential victims
  - » **Step 1:** Guess email IDs because companies have a pattern
    - ali.hassan.1@kaust.edu.sa (first initial followed by a dot and the last name)
    - Do this for as many users as possible (dictionaries of common names, employee lists, brute force, etc.)
  - » **Step 2:** Send email on the guessed email ID
  - » **Step 3:** Analyze the response of the SMTP server
    - If email is accepted, add to the database of harvested email IDs
    - If email is rejected, discard it (*Delivery Status Notification msg*)

EMAIL HARVESTING: OTHER OPTIONS

- **Spider or Crawler Scans**
  - Use web crawlers and spiders to go **search** through the entire **website**, **forums**, **blogs**, etc., for email addresses
- **Search Engines**
  - Use Google and other search engines to return all email addresses having a certain **suffix,** such as “@kaust.edu.sa”
- **Email Address Lookup Services**
  - Hunter.io - https://hunter.io/
  - Phonebook.cz - https://phonebook.cz/
  - VoilaNorbert - https://www.voilanorbert.com/

EMAIL HARVESTING

```
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...
        Searching 200 results...
[-] Searching in Exalead..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...
        Searching 200 results...
        Searching 250 results...


[+] Emails found:
------------------
36180135@upm.edu.sa
Admission.bc@upm.edu.sa
Admission.gc@upm.edu.sa
Hack@upm.edu.sa
abstracts@kfupm.edu.sa
eahmed@ccse.kfupm.edu.sa
m.arahman@upm.edu.sa
onaizi@kfupm.edu.sa
pixel-1517763088166131-web-@upm.edu.sa
pixel-1517763093538293-web-@upm.edu.sa
pixel-1517763099112281-web-@upm.edu.sa
pixel-1517763107276905-web-@upm.edu.sa
r.ghazouani@upm.edu.sa
s.adwan@upm.edu.sa
tarek@ccse.kfupm.edu.sa
umjohar@kfupm.edu.sa
```

False Positive

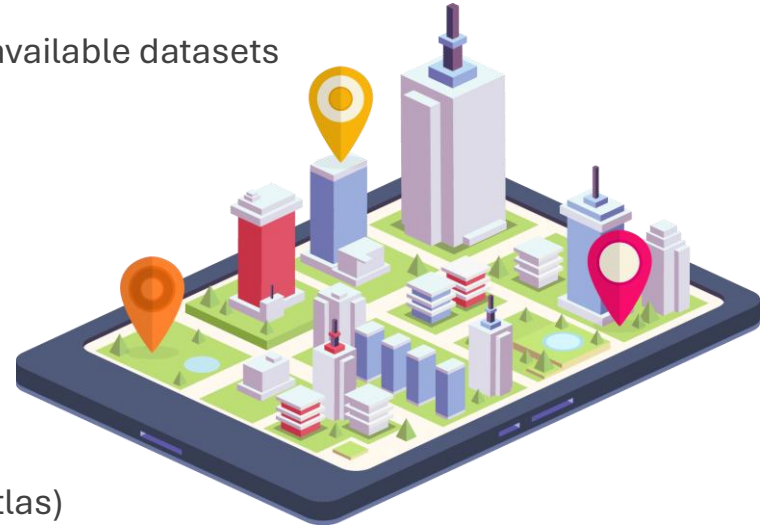
theHarvester -d upm.edu.sa -b all -l 200

RECON & OSINT

- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning
- Service Fingerprinting

RECON: LOCATION DETAILS

- **Google Maps & Google Earth**
  - Used to plot data points and cross-reference with know landmarks, addresses, or publicly available datasets
- **OpenStreetMap (OSM) Geographic DB & Wikimapia**
  - Queryable open-source database with loads of features (geographic encyclopedia)
- **Quantum Geographic Info System (QGIS)**
  - Perform detailed spatial analysis and visualization
- **World Imagery Wayback**
  - A digital archive of different versions of World Imagery created over time (online historical atlas)
- **IP Geolocation Services**
  - Translates IP addresses to the corresponding physical location of a system
- **Social Networking Sites**
  - Users share geolocation tags or hashtags; movement patterns of users can be inferred if they post frequently
- **Shodan**
  - Seach engine for Internet-connected devices that can also provide geographic location based on IP information
- **Maltego**
  - A data mining tool used to connect location data with other OSINT findings



ACQUIRING LOCATION: EASY WAY

جامعة الأمير مقرن بن عبد العزيز
University of Prince Mugrin

University Of Prince Mugrin
FPH5+XV6,
Al Aqool, Medina 42241,
Saudi Arabia
Get Direction

University Of Prince Mugrin
FPH5+XV6,
Al Aqool, Medina 42241,
Saudi Arabia
Get Direction

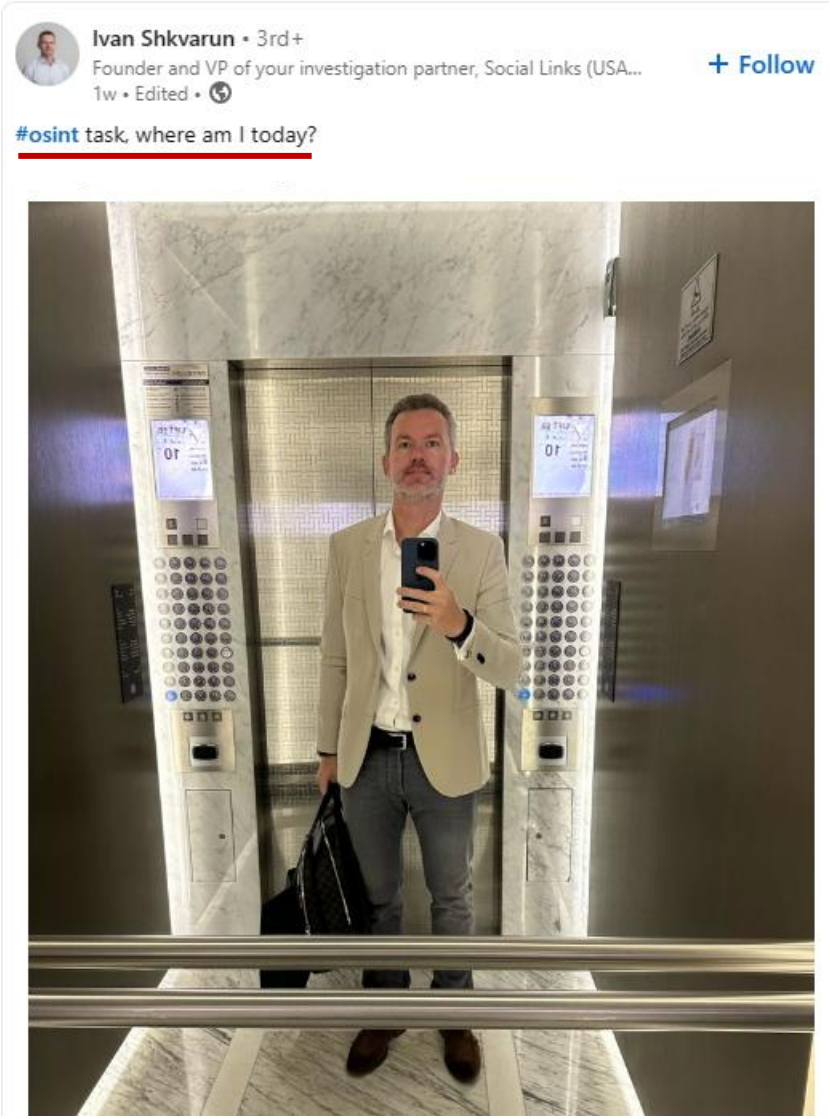
GET IT FROM THE WEBSITE EASILY!!

FINDING LOCATION CAN BE TRICKY

- Even if users don't explicitly share their location, **background** or **minor details** can provide intelligence:
  - Landmarks (Eiffel Tower, Burj Khalifa, road signs)
  - Shadows and time of day (can help estimate time zone)
  - License plates, billboards, or street signs for geographic hints
- **Reverse image search** can match an image to a known place or location
  - Use **AI services** to enhance image quality
- Explore **video reviews** and **vlogs** on YouTube for certain locations to look for clues and information

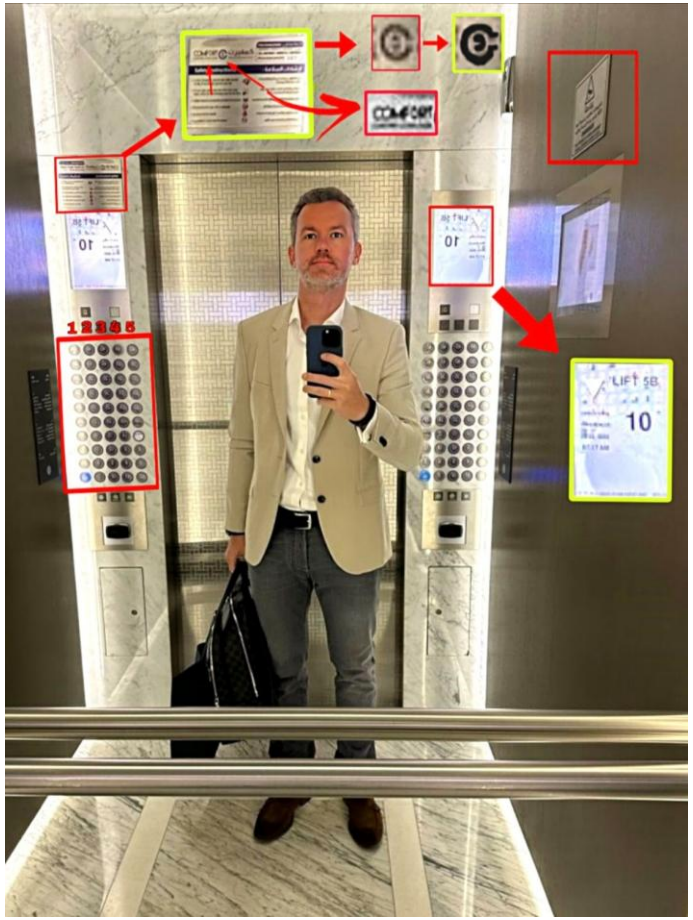
LET’S SEE A COUPLE OF EXAMPLES OF LOCATION RECON

ACQUIRING LOCATION: HARD WAY



OPEN CHALLENGE TO FIND LOCATION!

ACQUIRING LOCATION: HARD WAY

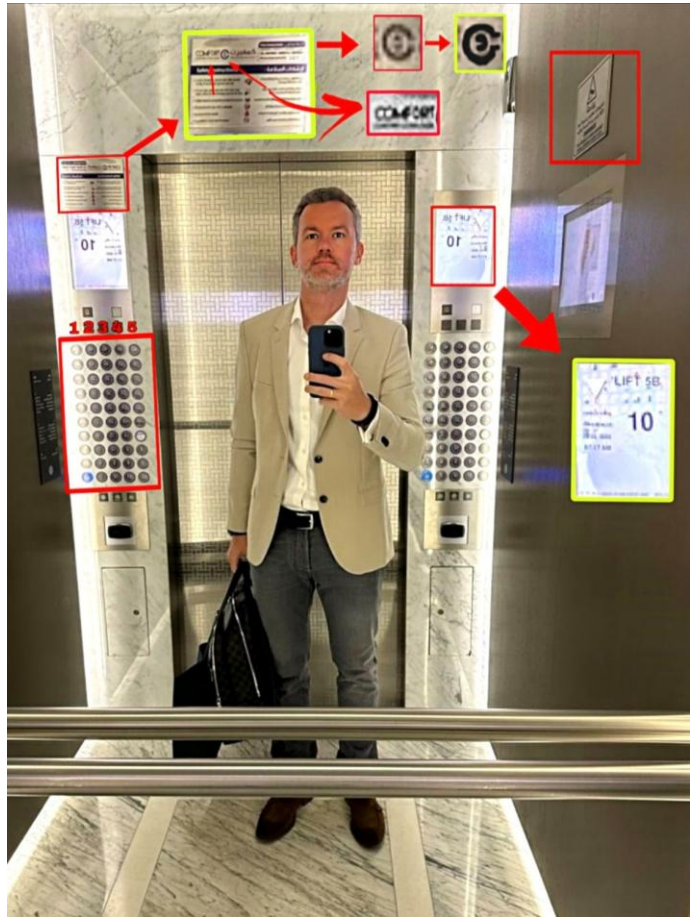


STEP 1:
Enhance the image using **remini.ai**

STEP 2:
Count number of buttons on the elevator panel. Roughly 55 so building must be around 45-50 floors

STEP 3:
Search for cybersecurity conferences on the day the challenge was made. Found 3 but the venue was a building with only 4 floors (confirmed using **Google Earth** and **Google Street View**)

ACQUIRING LOCATION: HARD WAY



STEP 4:
Notice a small rectangular notice above the elevator screen

STEP 5:
Crop it and enhance using remini.ai. Found the logo of the elevator company called "Comfort Elevators"

STEP 6:
Google the company and find their website (www.comfortelevators.com) with the same logo as in the notice. Website shows that all their customers are from Qatar including some hotels

ACQUIRING LOCATION: HARD WAY

STEP 7:
Start searching about the hotels that use elevators by Comfort Elevators company

STEP 8:
One by one, look at the website of each hotel. On the third attempt, discover that hotel "Pulman Doha West Bay" has some pictures on their website that match the given picture

STEP 9:
Search "Pulman Doha West Bay" on YouTube and find a video of a vlogger showing the exact elevator as in the picture hence, confirming the location and the exact floor (shown in the screen panel but flipped as image was taken in a mirror).

RECON & OSINT

- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning
- Service Fingerprinting

RECON: EMPLOYEE INFORMATION

- Lots of **people-based search engines** out there:
  - Pipl, snitch.name, That'sThem, Intelius, myLife, etc.
- Provide the following information:
  - Biodata (name, age, address, sex etc.)
  - Emails
  - Social media presence
  - Friends
  - Preferences/Interests
  - Marital status
  - Education
  - Court records
  - Credit history
  - And much more

pipl

Rashid.tahir.khan@gmail.com | Location (optional)

LOGIN

Search By

Email Rashid.tahir.khan@gn

+ MORE OPTIONS

Sponsored Links

R

Rashid Tahir (rashid.tahir.khan@gmail.com)

38 years old

SPONSORED:

Online Photos | Personal Info | Contact Info | Social Profiles

CAREER:	Research Intern at Microsoft (2013-2013)
EDUCATION:	PhD, Computer Science from University of Illinois at Urbana-Champaign (2011-2016)
PHONES:	847-480-7497 , 253-572-9639
ADDITIONAL NAME:	Rashid Khan
PLACES:	3624 Torrey Pines Parkway, Northbrook, Illinois Redmond, Washington

rashid.tahir.khan@gmail.com, Rashid Tahir, Pakistan, Illinois, ...

linkedin.com/in/rashid-tahir-92343b17

Professional Profile | Networking | LinkedIn

INTELIUS

CUSTOMER SUPPORT

LOGIN

People Search | Reverse Phone Lookup | Criminal & Traffic Records Search | Background Check | Public Records Search | Reverse Address Lookup

ENJOY UNLIMITED SEARCHES!

Look Up Anyone!

Enter a Name Below to Get Started Now. Access Information Instantly!

NAME | PHONE | ADDRESS

FIRST NAME: Rashid

LAST NAME: Tahir

CITY: Enter City

STATE: Select State

SEARCH

mylife™

JOIN NOW LOG IN

Check Anyone's Reputation or Just Get in Touch

View Background Checks, Contact Details, Personal Reviews, Reputation Scores & More

Search for Anyone or Yourself or Automatically Check All Your Friends

Enter any name

This is Me

Search

Have a Promo Code? Click Here

mylife™

Christine | Davis | City or Zip

Join Now | Log In

My Profile | Friends & Relatives | Neighbors | Classmates | Singles

We Found 100 Results for Christine Davis

Christine M Davis, 56
San Antonio, TX, 78220-1104

AKA: Christine M Chris Chris M

Places Lived: San Antonio, TX

ALERT: Court Records Found

View Reputation Profile

This is me - View My Report

Christine M Davis, 86
Redwood City, CA, 94065-1268

AKA: Chris

Places Lived: San Carlos, CA Redwood City, CA

View Reputation Profile

This is me - View My Report

Christine Davis, 74
Blackfoot, ID, 83221-5732

AKA: Chris

Places Lived: Blackfoot, ID Mesquite, NV

View Reputation Profile

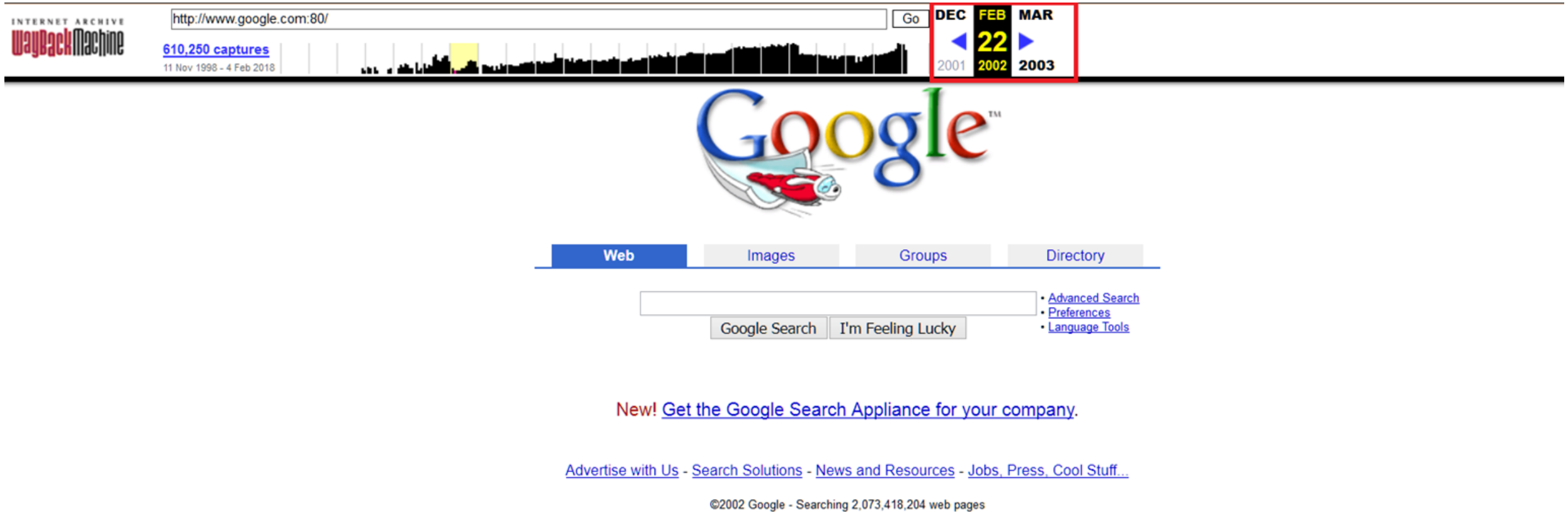
This is me - View My Report

RECON & OSINT

- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning
- Service Fingerprinting

RECON: ARCHIVED INFORMATION

- Wayback Machine is a digital archive (collection) of the Web
- Useful tool for various reconnaissance scenarios
  - **Uncovering Deleted Information:**
    - Archived versions can help recover sensitive information that has been removed from websites
  - **Tracking Website Evolution:**
    - By examining how a website has changed over time, attackers can identify the security patterns and plan accordingly
  - **Discovering Deprecated APIs and Endpoints:**
    - In API reconnaissance, Wayback Machine can help identify endpoints or functionalities that were once publicly accessible but have since been deprecated or hidden



Snapshot of www.google.com from 2002

RECON & OSINT

- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning
- Service Fingerprinting

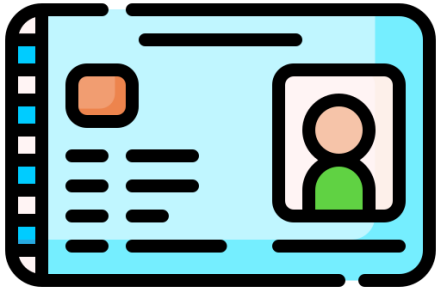
RECON: SOCIAL NETWORKING SITES

Treasure trove of information!

Very fine-grained information available here

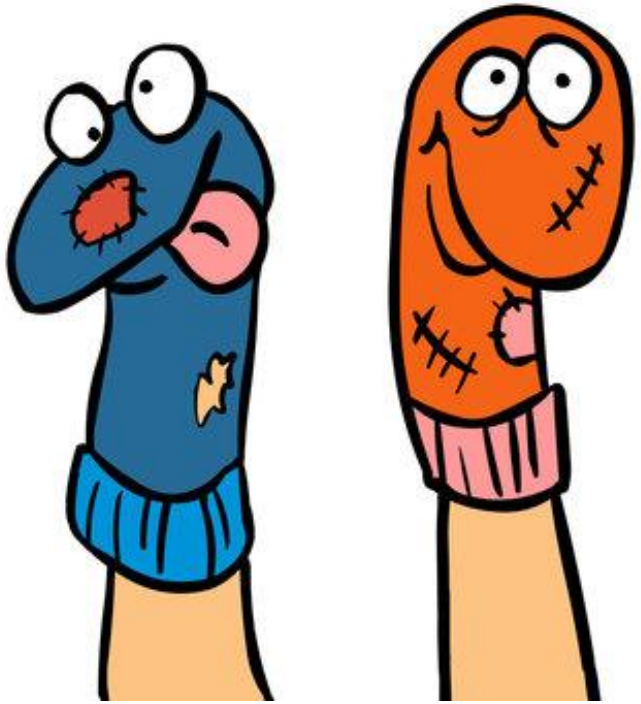
RECON: SOCIAL MEDIA INTELLIGENCE

- Profile information
- Photos and videos
- Friend and connection lists
- Status updates and posts
- Groups and communities
- Check-ins and locations
- Likes and interactions



RECON: SOCIAL MEDIA INTELLIGENCE

- Impersonation, **Sock Puppets**, and **Sybil Identities**:
  - Assume identity of someone the target knows or trusts or someone they could easily learn to trust
  - A fake online identity or persona is called a sock puppet or sybil identity
    - E.g., a male attacker joining a female-only WhatsApp group by pretending to be a female
  - Hides true identity of the attacker while simultaneously tricking the victim into revealing sensitive information



RECON & OSINT

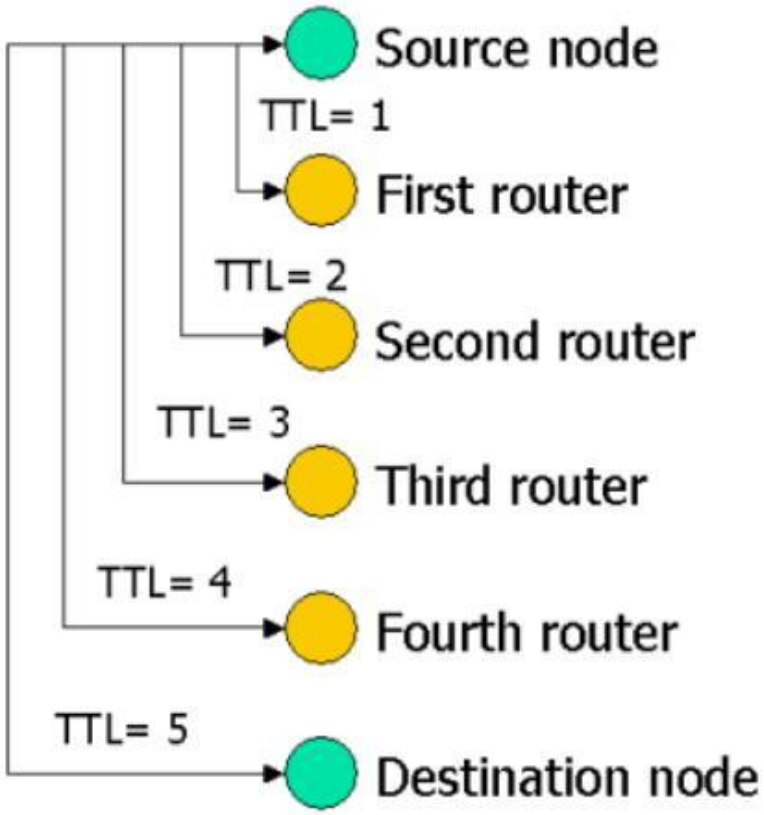
- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning (Network Recon or Scouting)
- Service Fingerprinting

NETWORK RECON:

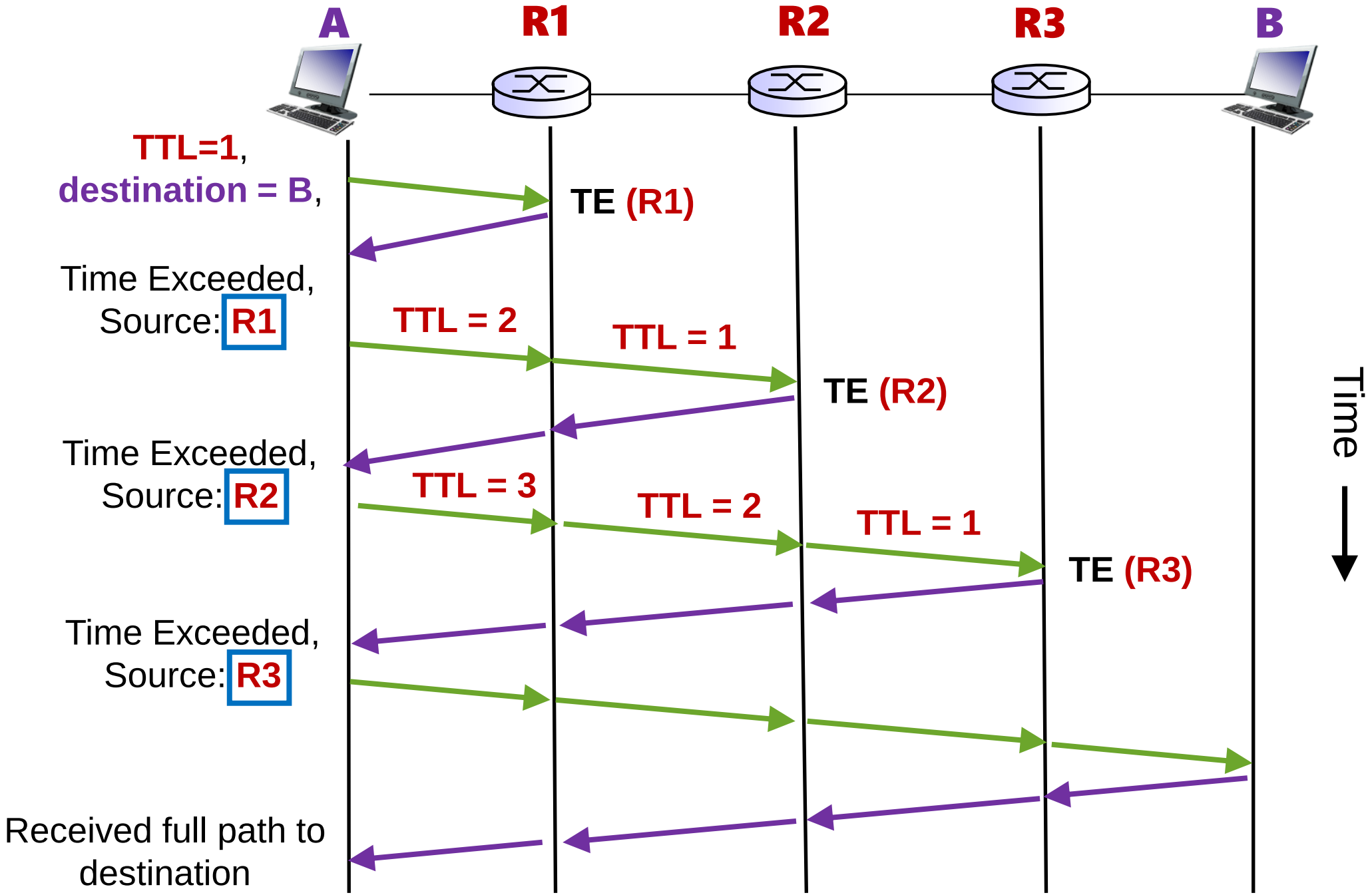
TOPOLOGY MAPPING

TOPOLOGY MAPPING: TRACEROUTING

- Trace the route to a host
- Direct interaction with the victim
- How ‘traceroute’ works:
  - » Send packet with TTL 1
  - » First router will receive and drop the packet
  - » Send packet with TTL 2
  - » Second router will receive and drop
  - » Send until max number of hops



- We know the identity of each router from the ICMP response message


A
R1
R2
R3
B
TTL=1,
destination = B,
TE (R1)
Time Exceeded,
Source: R1
TTL = 2
TTL = 1
TE (R2)
Time Exceeded,
Source: R2
TTL = 3
TTL = 2
TTL = 1
TE (R3)
Time Exceeded,
Source: R3
Received full path to
destination
Time

```
                                    tracert upm.edu.sa

Tracing route to upm.edu.sa [160.153.129.41]
over a maximum of 30 hops:

                    2 ms     2 ms  www.huaweimobilewifi.com [192.16
                    *        *     Request timed out.
                   73 ms    52 ms  10.80.133.2
                    *        *     Request timed out.
                   38 ms    70 ms  10.81.131.21
   ms              59 ms    58 ms  tw202-static240.tw1.com [110.93.202.240]
  7                68 ms    79 ms  110.93.253.208
  8   160 ms      149 ms   173 ms  be4932.ccr22.mrs01.atlas.cogentco.com [149.14.12
5.89]
  9   171 ms      169 ms   166 ms  be3093.ccr42.par01.atlas.cogentco.com [130.117.5
0.165]
                  163 ms   316 ms  prs-b2-link.telia.net [213.248.86.169]
                  248 ms   309 ms  prs-bb3-link.telia.net [62.115.122.4]
                  190 ms   175 ms  adm-bb3-link.telia.net [213.155.136.20]
                  182 ms   234 ms  adm-b2-link.telia.net [62.11
                  324 ms   312 ms  godaddy-ic-305669-adm-b2.c.t
 15                313 ms   244 ms  po64.bbsa0201-01.bbn.mgmt.am
6]
 16   235 ms        *     172 ms  10.241.131.197
 17   224 ms      478 ms   302 ms  10.240.67.1
 18   197 ms      258 ms   239 ms  10.240.64.0
 19   493 ms        *      237 ms  10.240.64.25
 20   491 ms      321 ms   406 ms  ip-160-153-129-41.ip.secureserver.net [160.153.1
29.41]

Trace complete.
```

Each node is pinged three times

ICMP is probably disabled

No response received

Identity of the router

NETWORK RECON:

PORT SCANNING

SERVICES/APPS REQUIRE PORTS

- Services/Apps run on a **specific port(s)** over a particular protocol
  - **FTP → 21** **(TCP)**
  - **SSH → 22** **(TCP)**
  - **DNS → 53** **(TCP, UDP)**
- Vulnerable service software allows hackers to break into a system
  - Unpatched Web server software
  - Buggy DNS server software
  - Etc..
- Hence, an important step in reconnaissance is to discover which ports are open

ENTER PORT SCANNING

TCP & UDP PORT SCANNING

TIME TO REVISIT THE FLAGS!

TCP FLAGS AKA CONTROL BITS

There are a total of 9 TCP flags

URG	ACK	PSH
RST	SYN	FIN
NS	CWR	ECE

RFC 793:

Unexpected or invalid flag based on the current state of the connection

Any TCP segment with an out-of-state flag sent to an open port is discarded, whereas segments sent to closed ports should be handled with a RST in response.
(except the ACK flag – more on that later)

NOW THAT WE KNOW
RFC793 AND THE TCP FLAGS,

LET'S SCAN LIKE A BOSS!

PORT SCANNING – TCP

Sending packets to TCP ports to determine open ports

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan

Some Common TCP Scans

PORT SCANNING – TCP

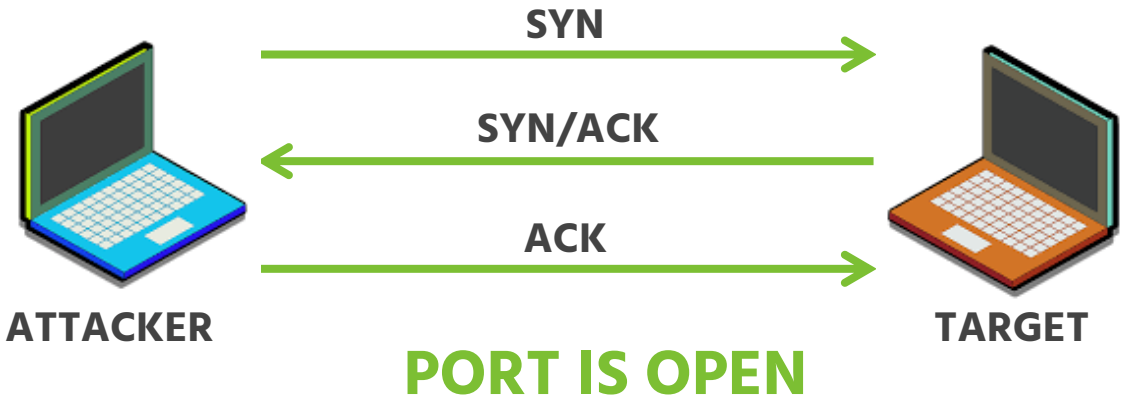
Sending packets to TCP ports to determine open ports

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan

Some Common TCP Scans

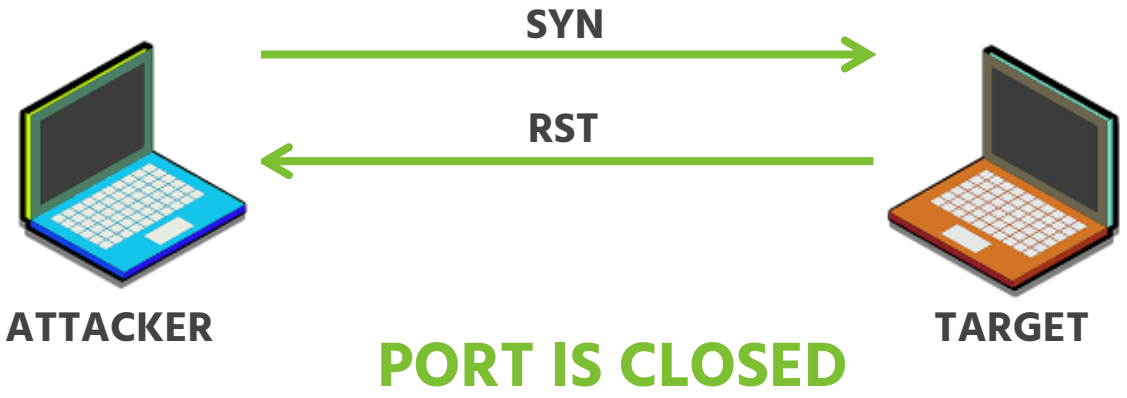
TCP CONNECT SCAN (VANILLA SCAN) – OPEN STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



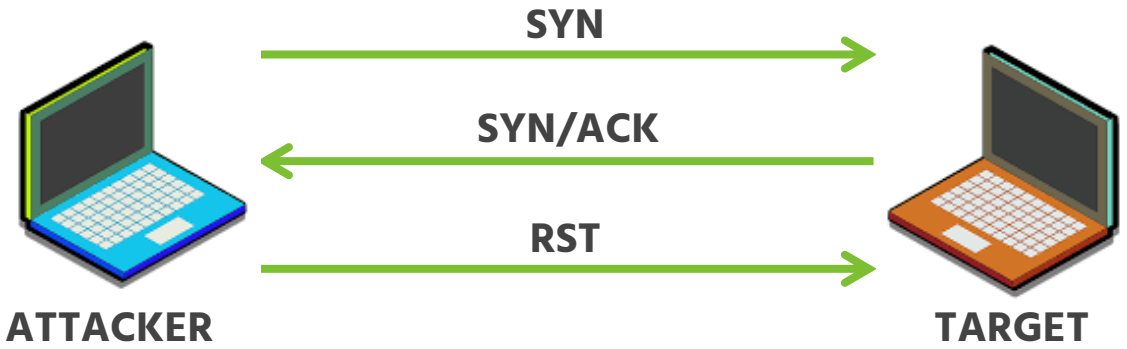
TCP CONNECT SCAN (VANILLA SCAN) – CLOSE STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



TCP SYN SCAN – OPEN STATE

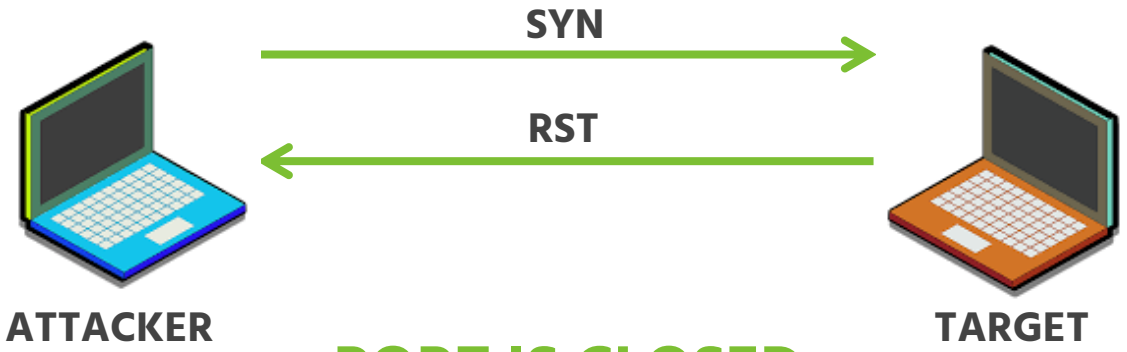
TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



PORT IS OPEN

TCP SYN SCAN – CLOSE STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



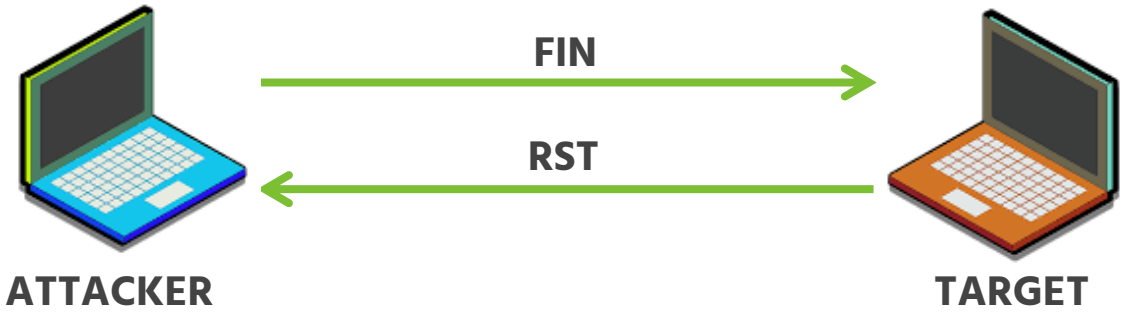
PORT IS CLOSED

(BEHAVIOR IS SIMILAR TO CONNECT SCAN)

TILL NOW WE WERE CERTAIN ABOUT A PORT BEING OPEN OR CLOSE

TCP FIN SCAN – CLOSE STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



PORT IS CLOSED

TCP FIN SCAN – OPEN STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan

PORT IS OPEN

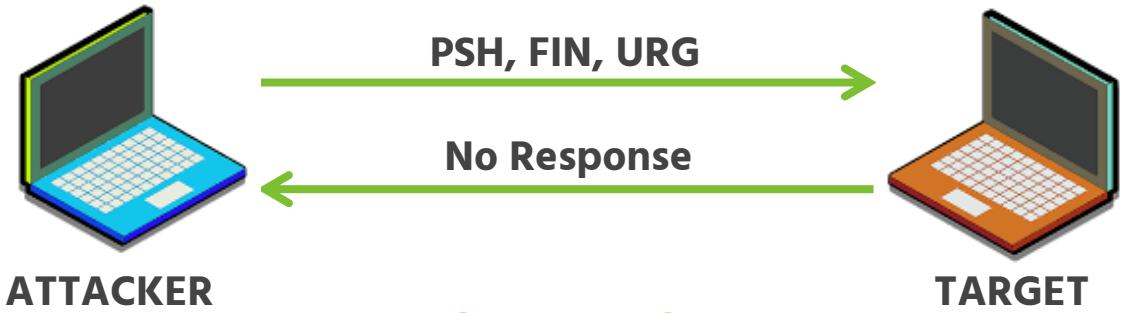
(may be)

TCP XMAS SCAN – CLOSE STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan

TCP XMAS SCAN – OPEN STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



PORT IS OPEN

(may be)

WHAT IF NONE OF THE FLAGS IS SET?

TCP NULL SCAN – CLOSE STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan

PORT IS CLOSED

TCP NULL SCAN – OPEN STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan

PORT IS OPEN

(may be)

FILTERED vs UNFILTERED TARGETS

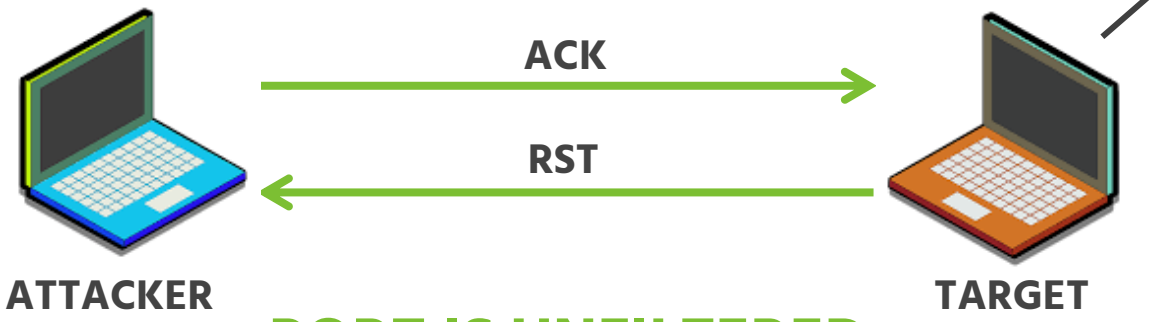
ACCOMMODATING FOR FIREWALLS

RFC 793:

For the ACK flag, out-of-state segments sent to an open/listening port or to closed ports should both be handled with a RST in response.

TCP ACK SCAN – UNFILTERED STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



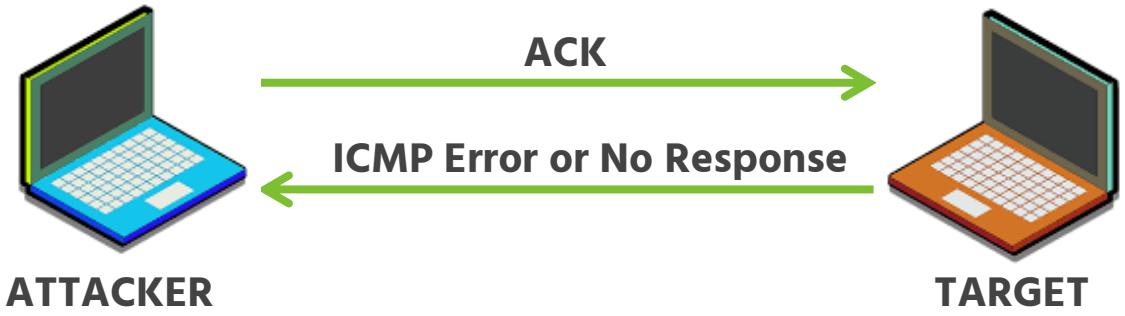
What we do know is that there is no firewall preventing us from getting to the machine or firewall allows ACK packets

PORT IS UNFILTERED

(Not sure if port is open or close as behaviour is same in both cases)

TCP ACK SCAN – FILTERED STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan



PORT IS FILTERED

(behind a firewall or ACL)

TCP ACK SCAN – UNFILTERED STATE

TCP Connect Scan	TCP SYN Scan	TCP FIN Scan	TCP XMAS Scan	TCP NULL Scan	TCP ACK Scan

TO CHECK IF PORT IS FILTERED OR UNFILTERED

USEFUL FOR MAPPING FIREWALL RULES

NOT USEFUL ALONE
OFTEN COMBINED WITH SYN SCAN

WHAT ABOUT UDP?

PORT SCANNING – UDP

Sending packets to UDP ports to determine open ports

UDP Empty Packet Scan	UDP Application Data Scan

Two Common UDP Scans

PORT SCANNING – UDP

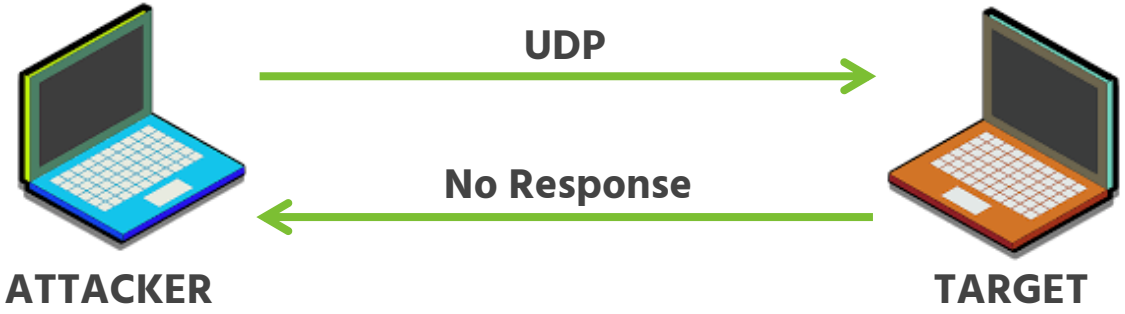
Sending packets to UDP ports to determine open ports

UDP Empty Packet Scan	UDP Application Data Scan

Two Common UDP Scans

UDP EMPTY PACKET SCAN – OPEN STATE

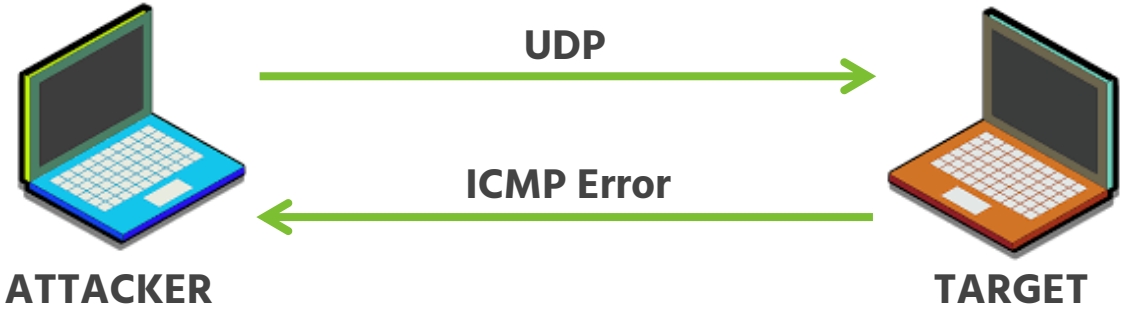
UDP Empty Packet Scan	UDP Application Data Scan



PORT IS OPEN

UDP EMPTY PACKET SCAN – CLOSE STATE

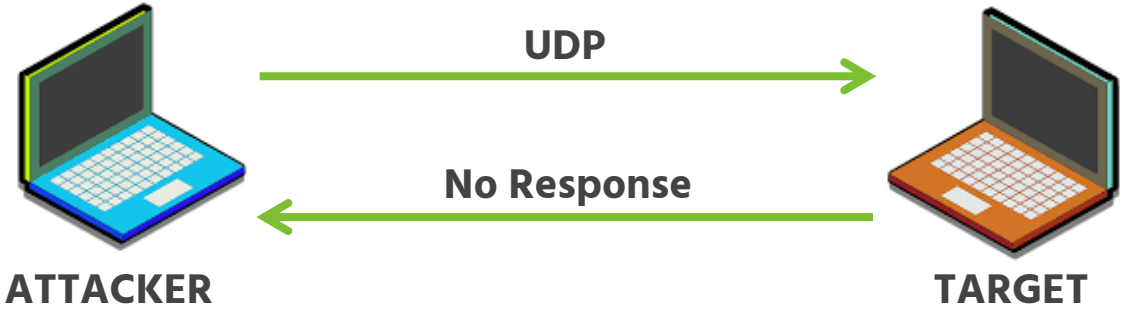
UDP Empty Packet Scan	UDP Application Data Scan



PORT IS CLOSED

UDP APPLICATION DATA SCAN – OPEN STATE

UDP Empty Packet Scan	UDP Application Data Scan

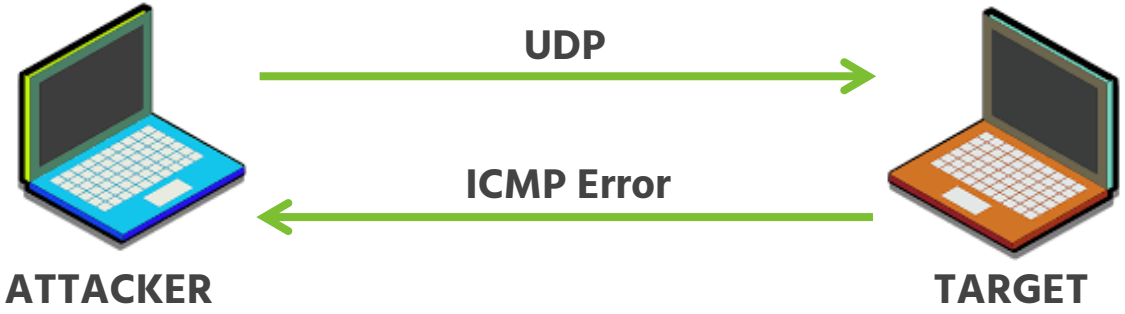


PORT IS OPEN

(Dummy payload is added)

UDP APPLICATION DATA SCAN – CLOSE STATE

UDP Empty Packet Scan	UDP Application Data Scan



PORT IS CLOSED

(Dummy payload is added)

RECON & OSINT

- Web Data & Domain Recon (e.g., www.kaust.edu.sa)
- Location Recon (geolocation, GPS coordinates, geotags, etc.)
- Employee Information (name, email, sex, age, preferences, etc.)
- Recon of Archived or Cached Data (Internet archives, SE caches, etc.)
- Social Media Intelligence (SOCMINT)
- Topology Mapping & Port Scanning
- Service Fingerprinting – For another time!!

QUESTIONS!