Capstone Project Report

Project Title:

- Create a Report on tools and methods that are used for Reconnaissance (Information Gathering) and describe the uses, functionalities and outcome, also attach the screenshots of the tools to show the.

NAME: **DRASHTI RAMESHBHAI AMIPARA (Linkedin)**

DOMAIN : **CYBERSECURITY &ETHICAL HACKING**

MENTOR : **SURENDRA SINGH(Linkedin)**

PROGRAM : **DIPLOMA**

REPORT DATE: **30-11-2024**

AGENDA

Abstract :

- The goal of this project is to explore and analyze the role of reconnaissance in cybersecurity, focusing on the use of various tools and techniques for information gathering. The project aims to understand how these tools can identify vulnerabilities and misconfigurations in a website's infrastructure by collecting and analyzing data such as domain information, subdomains, technology stacks, and exposed sensitive data. The primary focus is on reconnaissance tools, including passive and active methods, to gather actionable insights about a target website.
- Tools such as Sublist3r, Nmap, Gobuster, and OWASP ZAP will be employed to identify subdomains, open ports, services, hidden directories, and potential vulnerabilities. The expected outcomes include a detailed analysis of the selected website's architecture, insights into potential security flaws, and a list of recommendations for mitigation measures. These recommendations will address identified vulnerabilities to enhance the website's overall security posture. By showcasing proof-of-concept examples and screenshots, the report will demonstrate the tools' effectiveness and emphasize the importance of reconnaissance in proactive cybersecurity defense.

Introduction:

- **Reconnaissance:**
- Reconnaissance in cybersecurity refers to the process of gathering information about a target system, network, or website to identify potential vulnerabilities and entry points. It is the first phase in ethical hacking and penetration testing, serving as a foundation for further exploitation or defense. Reconnaissance can be categorized into passive reconnaissance, where publicly available information is collected without direct interaction, and active reconnaissance, which involves interacting with the target to gather data.
- **Importance of Reconnaissance:**
- Reconnaissance plays a crucial role in securing systems by enabling security professionals to understand the target's digital footprint, uncover vulnerabilities, and implement effective mitigation strategies. It allows for the identification of:
- Misconfigured systems or services
- Exposed sensitive information
- Outdated or vulnerable software versions
- Open ports and services that could be exploited
- By identifying these weaknesses early, organizations can proactively secure their systems and reduce the risk of unauthorized access or data breaches.

- **Selected Website :**

- For this project, the selected website is **[cisco]**, a **[type of website educational portal]**. The website was chosen due to its representative nature in demonstrating real-world reconnaissance techniques and the need to secure sensitive user or business data. By analyzing this website, the project aims to uncover insights into its infrastructure, identify potential security gaps, and recommend measures to strengthen its security posture.

Research:

- Website Details :
  - **Name and URL:**
    - Website Name: Cisco
    - URL: www.cisco.com
  - **Type/Category:**
    - Cisco.com falls under the category of **technology and networking solutions**, specifically offering products and services related to networking, cybersecurity, collaboration, and IT infrastructure.
  - **Popularity Metrics:**
    - Cisco is a globally recognized leader in IT and networking, ranked as one of the top technology companies worldwide. It operates in over 115 countries and generated approximately $57 billion in revenue in 2023.
    - The website is highly visited globally, ranking within the top 1,000 websites in the world, with significant traffic due to its importance to businesses and IT professionals.
    - Cisco holds a dominant position in the **enterprise networking and cybersecurity markets**
    - Statista & Newsroom.
  - **Technology Stack:**
    - Tools for analysis: whois,theHarvester,*Wappalyzer,nmap,amass,nikto* .

Types and Methods:

- Reconnaissance is the process of gathering information about a target system or network to identify vulnerabilities. It is generally divided into two main types: **Passive Reconnaissance** and **Active Reconnaissance**. Each type employs various methods to collect information.

1. Passive Reconnaissance:

- Passive reconnaissance involves gathering information without directly interacting with the target, ensuring that no alerts are triggered.

1.1 Open Source Intelligence (OSINT)

- **Purpose:** Use publicly available data to gather information about the target.
- **Methods and Tools:**
  - **Google Dorking:** Advanced search operators to find sensitive information.
  - **Shodan:** Discover internet-exposed devices and services.
  - **Have I Been Pwned:** Check for leaked credentials associated with the target.
  - **Social Media:** Gather employee names, job titles, or organizational details.

- **1.2 Domain and DNS Reconnaissance**
- **Purpose:** Discover domain information and DNS records.
- **Methods and Tools:**
  - **Whois Lookup:** Obtain domain registration details.
  - **dig and nslookup:** Retrieve DNS records, such as A, MX, and TXT records.
  - **Sublist3r:** Enumerate subdomains.

- **1.3 Metadata Extraction**
- **Purpose:** Collect hidden metadata from documents, images, or media.
- **Methods and Tools:**
  - **FOCA:** Analyze metadata from publicly available documents.
  - **ExifTool:** Extract metadata from images and media files.

- **1.4 Technology Stack Analysis**
- **Purpose:** Identify the technologies and frameworks used by the target website.
- **Tools:**
  - **BuiltWith**
  - **Wappalyzer**
  - **WhatRuns**

2. Active Reconnaissance:

- Active reconnaissance involves directly interacting with the target, increasing the risk of detection but providing more precise data.

- **2.1 Network Scanning**

- **Purpose:** Identify open ports, services, and active hosts.
- **Methods and Tools:**
  - **Nmap:** Scan for open ports and running service.
  - **Masscan:** High-speed network scanning.

- **2.2 Service Enumeration**
  - **Purpose:** Gather details about the services running on open ports.
  - **Methods and Tools:**
    - **Netcat:** Test connectivity and enumerate services on open ports.
    - **Nmap Scripts (NSE):** Automate service detection and vulnerability scans.

    - **2.3 Web Application Reconnaissance**
  - **Purpose:** Explore web servers for vulnerabilities and hidden content.
  - **Methods and Tools:**
    - **Dirb or Gobuster:** Enumerate hidden directories.
    - **Nikto:** Identify web server misconfigurations.

- **2.4 API Reconnaissance**
- **Purpose:** Identify and analyze APIs for exposed sensitive data.
- **Methods and Tools:**
  - **Postman:** Manually test API endpoints.
  - **Burp Suite Repeater:** Modify and resend API requests to analyze responses.
- **3. Social Engineering Reconnaissance**
  - Social engineering involves exploiting human interaction to gather information.
  - **3.1 Techniques**
    - **Phishing:** Sending fake emails to extract credentials or sensitive information.
    - **Impersonation:** Pretending to be an employee or trusted entity to gather details.
    - **Dumpster Diving:** Searching discarded materials for confidential information.

- **4. Reconnaissance Automation**
- Automation tools are used to streamline data collection.
- **4.1 Tools**
  - **Recon-ng:** A modular framework for automating OSINT and reconnaissance tasks.
  - **SpiderFoot:** Automates OSINT for gathering intelligence about domains, IPs, and more.
  - **Amass:** Automates subdomain enumeration and DNS analysis.

Tools and Functionalities ,uses,outcomes,poc :

1: Identify the Target - Cisco.com

- **Objective:** Define the target entity for reconnaissance, focusing on the domain `cisco.com`.
- **Details of the Target:**
  - **Domain Name and ip:**
    - `Cisco.com(72.163.4.185)`
- **Category/Type:**
  - Technology company specializing in networking hardware, software, telecommunications, and cybersecurity.
- **Purpose of Reconnaissance:**
  - To gather publicly available information about `cisco.com`, such as domain details, associated IPs, subdomains, and related services, ensuring ethical and legal compliance.

2: Passive Reconnaissance

- Passive methods collect publicly available information without directly interacting with the target.
- **2.1 WHOIS Lookup Tool:-**
- **a. Tool Overview**
  - **Purpose:**
    - WHOIS lookup tools retrieve domain registration details, including information about the registrant, domain expiry dates, and associated nameservers.
  - **Type:**
    - Passive reconnaissance tool, as it does not interact directly with the target systems but queries publicly available databases.
- **b. Functionalities**
  - **Domain Information:**
    - Retrieves the domain name, registrar, registration, and expiration dates.
  - **Registrant Details:**

    - Provides information about the organization or person registering the domain (unless hidden via WHOIS privacy services).
  - **Nameservers and DNS Info:**
    - Shows nameservers used for hosting and DNS resolution.
  - **Status Flags:**
    - Indicates whether a domain is active, locked, or pending deletion.
  - **IP Mapping (optional):**
    - Links the domain to its current IP address and geolocation (depends on the tool used).
- **C. Uses:**
  - **Cybersecurity Reconnaissance:**
    - Identifies ownership and technical details of a target domain.
  - **Network Troubleshooting:**
    - Helps verify DNS records and expiration dates.
  - **Brand Protection:**
    - Tracks domain usage to identify cybersquatting or domain impersonation.

- **d. How to Use the WHOIS Lookup Tool**
  - **steps: Command-Line WHOIS (Linux/Windows Subsystem for Linux)**
    - Open the terminal.
    - Run the following command:
      - `whois cisco.com`
    - Review the output for registrant details, nameservers, and status.
- **e. Outcome**
  - **Detailed Output Includes:**
    - Domain Registrar: e.g., GoDaddy, Namecheap.
    - Registrant Information: Name, organization (if not private).
    - Domain Status: Active, locked, or pending expiration.
    - Registration and Expiration Dates.
    - Nameservers and DNS details.
  - **Uses in Reconnaissance:**
    - Provides foundational information for further analysis, like identifying additional infrastructure or tracking ownership.

```
┌──(root㉿yash)-[/home/yash]
└─# whois cisco.com
   Domain Name: CISCO.COM
   Registry Domain ID: 4987030_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-04-13T09:39:41Z
   Creation Date: 1987-05-14T04:00:00Z
   Registry Expiry Date: 2025-05-15T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.CISCO.COM
   Name Server: NS2.CISCO.COM
   Name Server: NS3.CISCO.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-20T16:27:53Z <<<
```

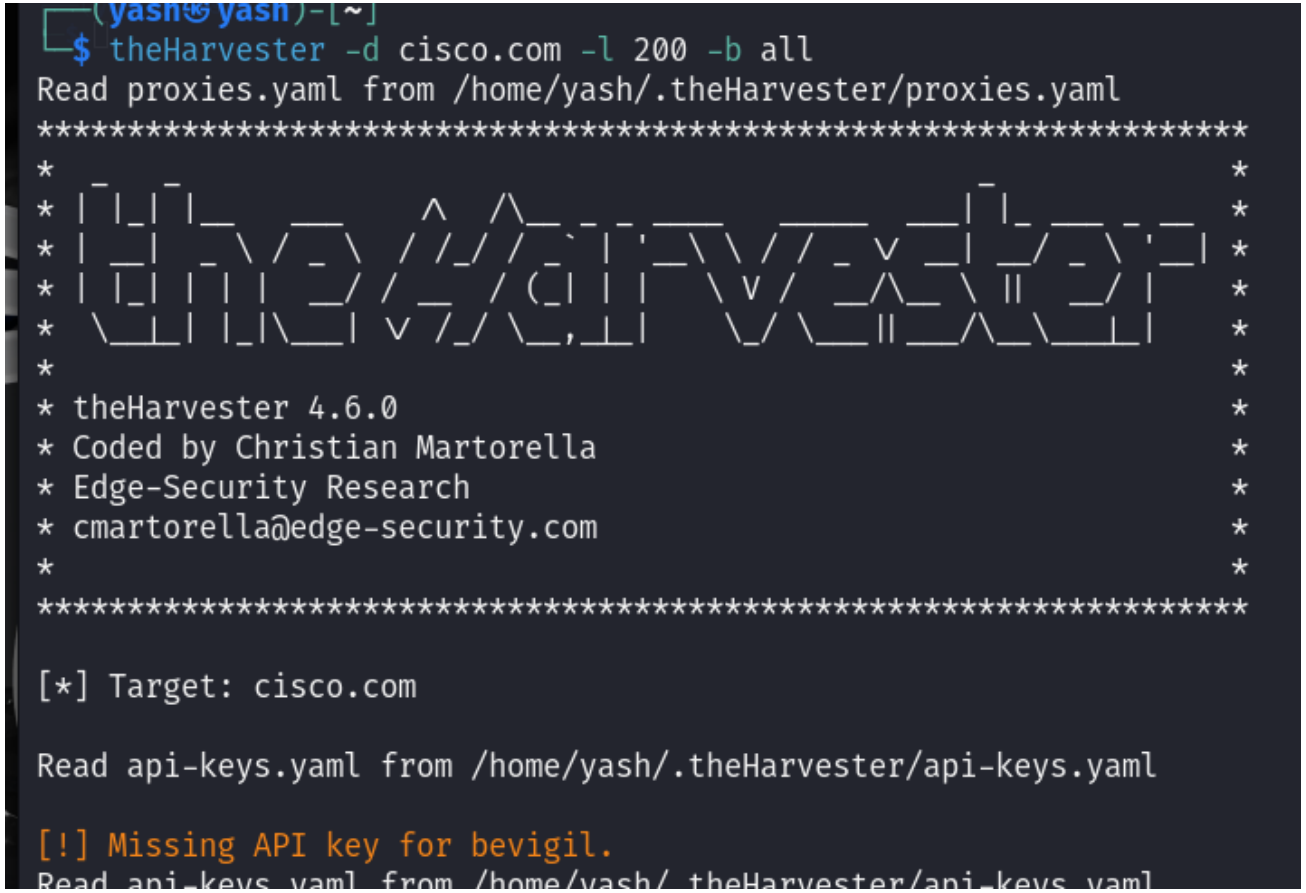
- **2.2 TheHarvester tool:-**
  - **a.Overview**
    - **TheHarvester** is a popular OSINT (Open Source Intelligence)tool designed to gather information about a target from public sources. It is widely used for reconnaissance during penetration testing to identify potential attack vectors.
  - **b.Functionalities**
    - TheHarvester gathers the following information:
      - **Emails:** Identifies email addresses associated with a domain.
      - **Subdomains:** Detects subdomains linked to the target domain.
      - **IP Addresses:** Discovers associated IP ranges.
      - **URLs:** Finds relevant URLs or endpoints.
      - **ASNs (Autonomous System Numbers):** Lists network-related data.
      - **Social Media Information:** Collects data from platforms, depending on the source.
  - **C.Uses**
    - **Step 1: Installation**
      - Ensure you have Python installed on your system.
    - Install TheHarvester using the command:

- `git clone https://github.com/laramies/theHarvester.git`
- `cd theHarvester`
- `python3 -m pip install -r requirements.txt`

- Run the tool:
  - `python3 theHarvester.py`

- **Step 2: Basic Command**
  - To run TheHarvester against a target domain Gathering emails and subdomains from all.
    - **`theharvester -d cisco.com -l 100 -b all`**
      - **`-d`**: Specifies the target domain.
      - **`-l`**: Sets the limit of results to retrieve.
      - **`-b`**: Defines the search engine or source (e.g., Google, Bing ,all etc.).
  - Collecting data from Bing:
    - **`theharvester -d example.com -l 100 -b bing`**

- **d. Outcome:**
  - **Email Discovery:**
    - Emails can indicate employees or departments
      - (e.g., admin@cisco.com).
  - **Subdomain Enumeration:**
    - Subdomains may reveal development or testing Environments
    - (e.g., dev.cisco.com).
    - **Network Blocks (ASNs or CIDR Ranges):**
    - Provides Autonomous System Numbers (ASNs) or IP ranges associated with the domain.



- **Associated Domains**
  - Other domains linked to the target.
  - Associated domains: cisco.net, cisco.org, cisco-shop.com
- **Public Source Data**
  - Information extracted from public sources like LinkedIn, Google, Bing, and others.
  - Provides employee details, public records, or additional intelligence.
  - Useful for social engineering or further reconnaissance.
  - LinkedIn data: - John Doe (CISO) - john.doe@cisco.com

- **e.Poc:**
  - file:///C:/kalilinux/output.xml

- **2.3 Wappalyzer:**
  - **a.Overview**
    - **Wappalyzer** is a browser extension and web tool that identifies the technology stack used by a website. It is widely used for reconnaissance, competitive analysis, and learning about technologies.
  - **b.Functionalities of Wappalyzer**
    - **Technology Detection:**
      - Identifies front-end frameworks (e.g., React, Angular).
      - Recognizes backend technologies (e.g., PHP, Python).
      - Detects Content Management Systems (CMS) like WordPress or Drupal.
      - Shows analytics platforms (e.g., Google Analytics).
    - **Categorization:**
      - Groups technologies by category (e.g., programming languages, web servers, CDNs).
    - **Ease of Access:**
      - Operates as a browser extension for quick results during website browsing.
    - **Use Cases:**

- Gathering information during reconnaissance.
- Competitive analysis of websites.
- Learning about trending technologies in use.

- **C.Uses:**
  - **Step 1: Installation**
    - **Browser Extension:**
      - Visit the Wappalyzer website.
      - Install the extension for your browser (Chrome, Firefox, or Edge).
  - **Step 2: Analyze a Website**
    - Open your browser and navigate to the target website (e.g., `example.com`).
    - Click on the Wappalyzer icon in the browser toolbar.
    - Review the detected technologies categorized in a dropdown list.
  - **Step 3: Generate Reports**
    - Optional: Use the Wappalyzer dashboard to save or export results for multiple sites.

- **d. Outcome :**
  - **Detailed Technology List:**
    - Wappalyzer provides a categorized breakdown of the detected technologies, such as:
  - **Web Server:** Apache, Nginx.
  - **CMS:** WordPress, Joomla.
  - **Frontend Frameworks:** Bootstrap, React.
  - **Programming Languages:** PHP, Python.
  - **Analytics Tools:** Google Analytics, Hotjar.

- **e. poc:**

  - https://sitereport.netcraft.com/?url=https://www.cisco.com

- ## 3: Active Reconnaissance
- Active methods interact directly with the target to gather information.
- ### 3.1 Nmap tool :
  - Nmap is a widely used open-source tool for network discovery and security auditing. It helps security professionals and system administrators assess network infrastructure, identify vulnerabilities, and monitor system health.
  - **a.Overview**
    - Nmap is a powerful open-source network scanning tool used for discovering hosts, services, and vulnerabilities in a network. It is widely used in cybersecurity for reconnaissance and vulnerability assessment.
  - **b.Uses :**
    - **Network Discovery**
      - Identify live hosts in a network.
      - Map the topology of a network.

- **Port Scanning**
  - Determine which ports are open, closed, or filtered.
  - Identify services running on open ports.
- **Service Enumeration**
  - Gather details about the software running on open ports, including version numbers.
- **Operating System Detection**
  - Identify the operating system of a host using fingerprinting.
- **Vulnerability Scanning**
  - Detect common vulnerabilities using built-in scripts.
- **Firewall and Security Policy Testing**
  - Evaluate the effectiveness of firewall configurations by simulating various traffic patterns.
- **Penetration Testing Preparation**
  - Gather initial data about the network to assist in ethical hacking or penetration testing.
- **Monitoring Network Changes**
  - Track changes in a network setup or detect unauthorized devices.

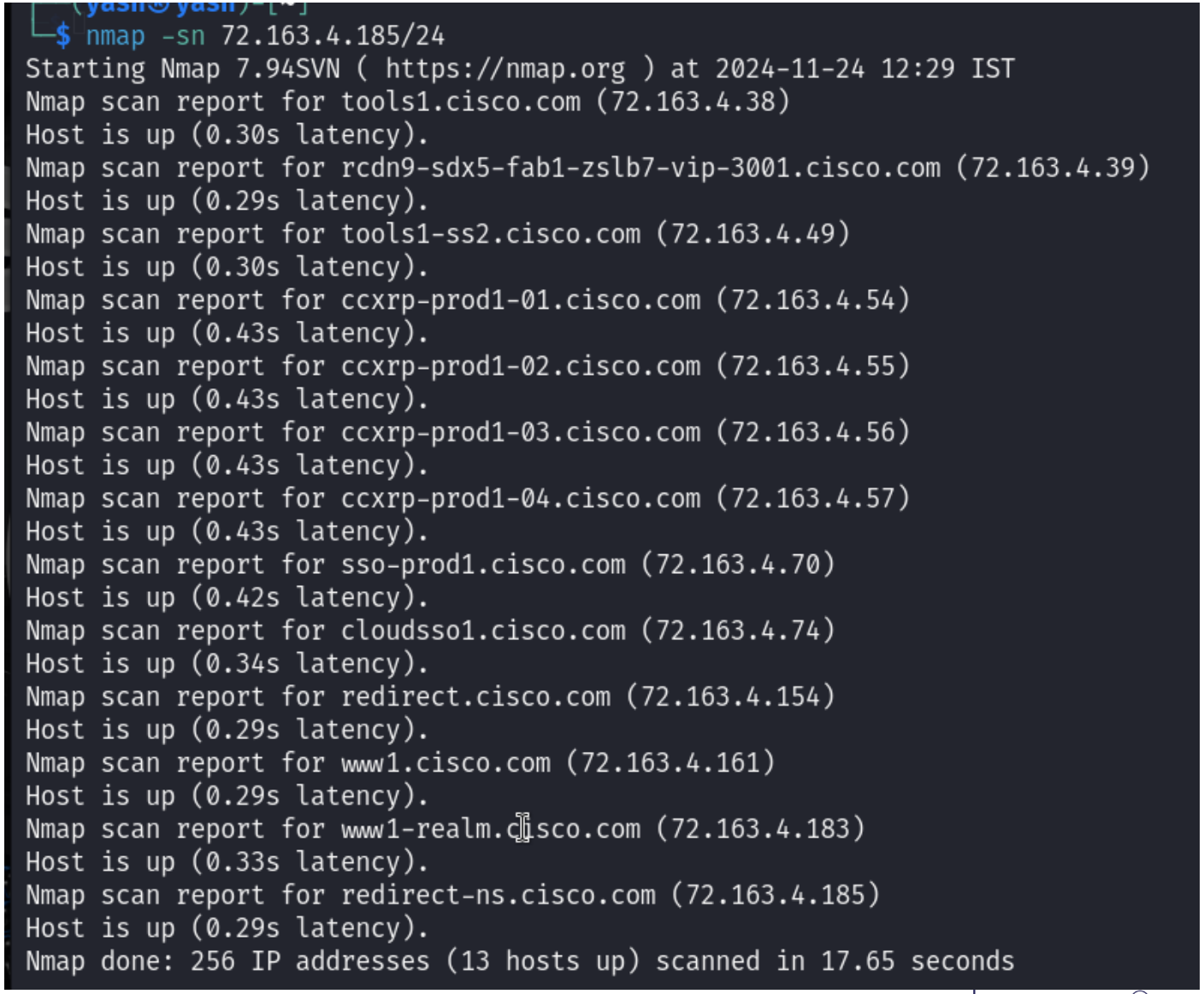
- **C.Functionalities**
  - **1. Host Discovery**
    - **Purpose:** Determine which systems are online in a network.
    - **Key Options:**
      - `-sn`: Performs a ping scan without port scanning.
      - `-Pn`: Skips ping checks and assumes all hosts are live.
  - **2. Port Scanning**
    - **Purpose:** Identify open ports and their state (open, closed, or filtered).
    - **Key Options:**
      - `-sS`: Performs a stealth SYN scan.
      - `-sT`: Conducts a full TCP connect scan.
      - `-p`: Specifies the port range to scan (e.g., `-p 1-65535`)
  - **.3. Service Version Detection**
    - **Purpose:** Determine the version of services running on open ports.
    - **Key Options:**
      - `-sV`: Enables service version detection.

- **4.Operating System Detection**
  - **Purpose:** Identify the operating system of a host.
  - **Key Options:**
    - `-O`: Enables OS detection based on response patterns.
- **5. Aggressive Scan**
  - **Purpose:** Combines multiple functionalities like OS detection, service enumeration, and traceroute.
  - **Key Options:**
    - `-A`: Enables aggressive scanning.
- **6.Script Scanning (NSE – Nmap Scripting Engine)**
  - **Purpose:** Run scripts to detect vulnerabilities, brute force login credentials, or perform other advanced tasks.
  - **Key Options:**
    - `--script`: Specifies a script or category (e.g., `vuln`, `http`, `ssl`).
    - Example:
    - `nmap --script vuln <target_IP>`

- **7. Network Topology Mapping**
  - **Purpose:** Visualize the structure of a network.
  - **Key Options:**
    - `-traceroute`: Traces the path packets take to the target.
- **8. Custom Timing Options**
  - **Purpose:** Adjust scanning speed to balance stealth and efficiency.
  - **Key Options:**
    - `-T0` to `-T5`: From the slowest (paranoid) to the fastest (aggressive).

- **d.Outcomes:**
  - **Open Ports**: Helps prioritize ports to secure or monitor.
  - **Services and Versions**: Identifies outdated software for patching.
  - **Operating System**: Determines system compatibility and potential vulnerabilities.
  - **Firewall Rules**: Detects security gaps in filtering mechanisms.
  - **Exposed Systems**: Identifies devices that should not be public-facing.

- **Poc:**
- **1.Discover Live Hosts**
  - nmap -sn 72.163.4.185/24
    - *Discovers live hosts in the specified subnet.*



- **2.Aggressive Scan**
  - nmap -A 72.163.4.185
    - *Performs OS detection, version detection, script scanning, and traceroute*

```
└─$ nmap -A cisco.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 23:24 IST
Nmap scan report for cisco.com (72.163.4.185)
Host is up (0.44s latency).
Other addresses for cisco.com (not scanned): 2001:420:1101:1::185
rDNS record for 72.163.4.185: redirect-ns.cisco.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http?
|_http-title: Did not follow redirect to https://cisco.com/
443/tcp open  ssl/https
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=www.cisco.com/organizationName=Cisco Systems In
ProvinceName=California/countryName=US
| Subject Alternative Name: DNS:cisco.com, DNS:www.cisco.com, DNS:www1.cisco.co
2.cisco.com, DNS:www3.cisco.com, DNS:www-01.cisco.com, DNS:www-02.cisco.com, DN
cisco.com, DNS:www1-ss2.cisco.com, DNS:www2-ss1.cisco.com, DNS:www3-ss1.cisco.c
w3-ss2.cisco.com, DNS:www.static-cisco.com, DNS:redirect-ns.cisco.com, DNS:cisc
isco.com, DNS:www.mediafiles-cisco.com
| Not valid before: 2024-09-08T14:05:00
|_Not valid after:  2025-09-08T14:04:00
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://www.cisco.com/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|   HTTPOptions:
|     HTTP/1.1 302 Found
|     Location: https://www.cisco.com/
|_    Connection: close
```

```
|     HTTP/1.1 302 Found
|     Location: https://www.cisco.com/
|_    Connection: close
| http-title: Access Denied
|_Requested resource was https://www.cisco.com/
|_ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please su
bmit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=11/24%Time=674227C8%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,4B,"HTTP/1\.1\x20302\x20Found\r\nLocation:\x20https:/
SF:/www\.cisco\.com/\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,4B,"H
SF:TTP/1\.1\x20302\x20Found\r\nLocation:\x20https://www\.cisco\.com/\r\nCo
SF:nnection:\x20close\r\n\r\n")%r(FourOhFourRequest,6E,"HTTP/1\.1\x20302\x
SF:20Found\r\nLocation:\x20https://www\.cisco\.com/nice%20ports%2C/Tri%6Ei
SF:ty\.txt%2ebak\r\nConnection:\x20close\r\n\r\n");
```

3.Scan Specific Ports

- nmap -p 22,80 72.163.4.185

- *Scans for SSH, HTTP services on a target.*

```
└─$ nmap -p 22,80 72.163.4.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 12:34 IST
Nmap scan report for redirect-ns.cisco.com (72.163.4.185)
Host is up (0.31s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
80/tcp open     http
```

- # 4. Subdomain Enumeration:
  - ## 4.1 amass tool:
    - **a.Overview**
      - **Amass** is an open-source tool developed by OWASP for advanced reconnaissance and information gathering. It specializes in **subdomain enumeration** and mapping an organization's attack surface. Amass aggregates data from multiple sources, making it highly effective for large-scale asset discovery.
  - **b.Functionalities**
    - **Subdomain Enumeration:**
      - Discovers subdomains using public sources, search engines, and APIs.
    - **DNS Enumeration:**
      - Performs DNS record lookups (A, AAAA, CNAME, TXT, etc.).
    - **Passive Reconnaissance:**
      - Gathers data from passive sources like SSL certificates and domain registration records.
    - **Active Reconnaissance:**
      - Uses techniques like DNS zone transfers and brute-forcing.

- **Graph Visualization:**
  - Maps relationships between domains, IPs, and organizations.
- **Integration with APIs:**
  - Supports multiple APIs such as VirusTotal, Shodan, and Censys to enhance discovery.
- **Output Formats:**
  - Generates results in various formats (JSON, text) for integration with other tools.

- **C.Usage:**
  - **Step 1: Install Amass**
    - Install Amass via package managers or GitHub:
      - Debian/Ubuntu:
        - `sudo apt install amass`
        -
    - From Source:

      - `git clone https://github.com/owasp-amass/amass.git`
      - `cd amass`
      - `go install ./...`

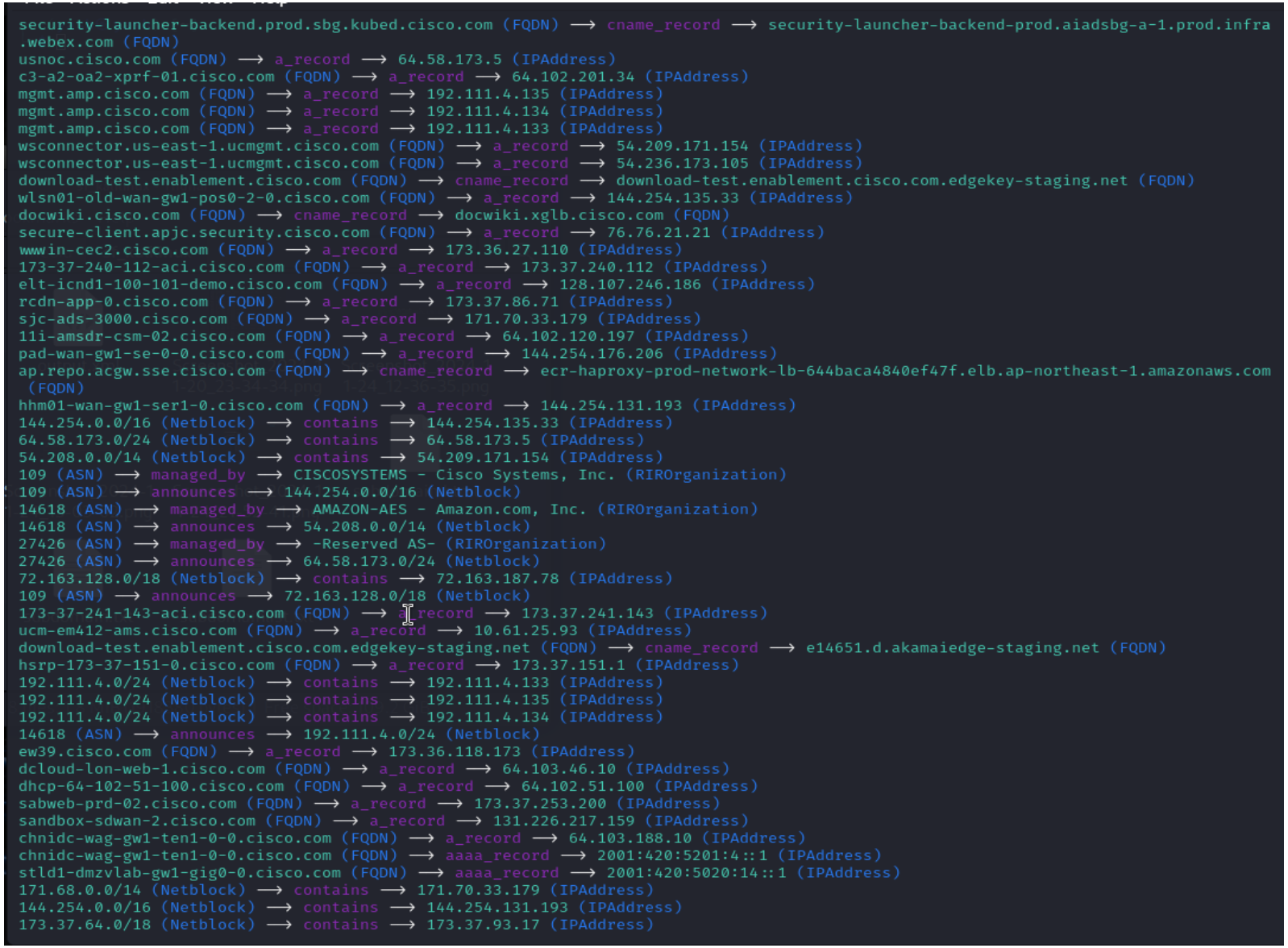
- **Step :2. Run Basic Commands**
  - **Simple Subdomain Enumeration:**
    - `amass enum -d example.com`
      - This command passively discovers subdomains.
  - **Active Reconnaissance:**
    - Use brute-forcing for active discovery:
      - `amass enum -d example.com -brute`
  - **Output to a File:**
    - Save results for later analysis:
      - `amass enum -d example.com -o subdomains.txt`
  - **Use Specific Sources:**
    - Limit search to specific APIs or sources:
      - `amass enum -d example.com -src`

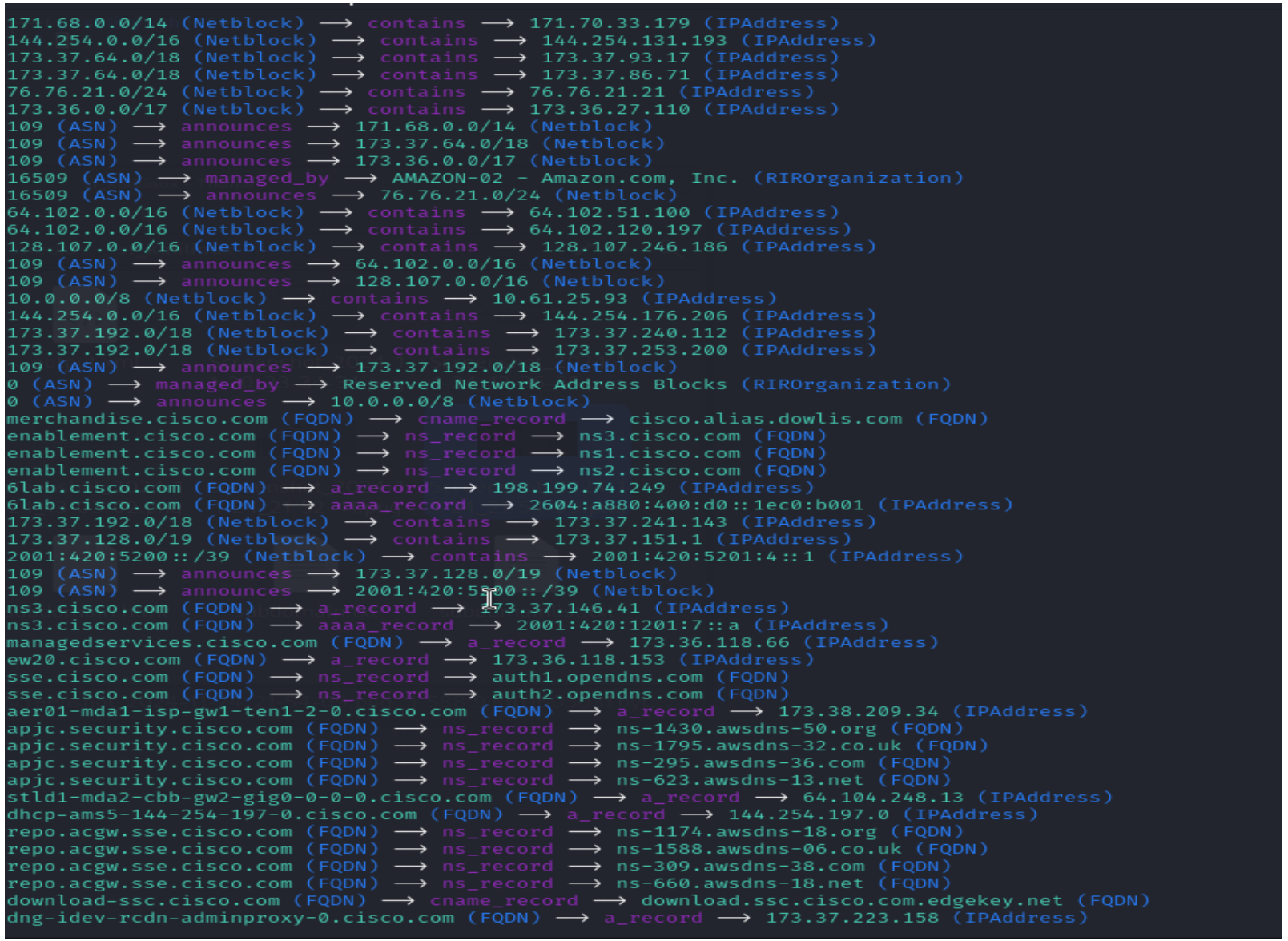
- **d. Outcome:**
  - **Sample Output**
    - Running the basic command `amass enum -d cisco.com -o subdomain.txt` produces results like:
      - `[cisco.com] Subdomain enumeration`
      - `www.cisco.com`
      - `mail.cisco.com`
      - `blog.cisco.com`
      -
  - **Detailed Results**
    - Output may include:
      - Subdomains and associated IP addresses.
      - DNS records (CNAME, MX, TXT).
      - Vulnerabilities or misconfigurations.

- **e. poc:**

```
$ amass -h
```

```
                                                                  v4.2.0
                                                OWASP Amass Project - @owaspamass
                                        In-depth Attack Surface Mapping and Asset Discovery

Usage: amass intel|enum [options]

  -h     Show the program usage message
  -help
         Show the program usage message
  -version
         Print the version number of this Amass binary


Subcommands:

         amass intel - Discover targets for enumerations
         amass enum  - Perform enumerations and network mapping

The user's guide can be found here:
https://github.com/owasp-amass/amass/blob/master/doc/user_guide.md

An example configuration file can be found here:
https://github.com/owasp-amass/amass/blob/master/examples/config.yaml

The Amass tutorial can be found here:
https://github.com/owasp-amass/amass/blob/master/doc/tutorial.md

┌──(yash㉿yash)-[~]
└─$ amass enum -d cisco.com -o subdomain.txt
cisco.com (FQDN) --> ns_record --> ns3.cisco.com (FQDN)
cisco.com (FQDN) --> ns_record --> ns2.cisco.com (FQDN)
cisco.com (FQDN) --> ns_record --> ns1.cisco.com (FQDN)
cisco.com (FQDN) --> mx_record --> rcdn-mx-01.cisco.com (FQDN)
cisco.com (FQDN) --> mx_record --> alln-mx-01.cisco.com (FQDN)
cisco.com (FQDN) --> mx_record --> aer-mx-01.cisco.com (FQDN)
appsara-prod01.cisco.com (FQDN) --> a_record --> 173.37.93.17 (IPAddress)
wsconnector.na.ucmgmt.cisco.com (FQDN) --> cname_record --> wsconnector.us-east-1.ucmgmt.cisco.com (FQDN)
```





BIA BOSTON INSTITUTE OF ANALYTICS ®

```
dng-idev-rcdn-adminproxy-0.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.223.158 (IPAddress)
dhcp-64-100-67-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.100.67.0 (IPAddress)
171.68.0.0/14 (Netblock) ⟶ contains ⟶ 171.71.241.105 (IPAddress)
64.102.0.0/16 (Netblock) ⟶ contains ⟶ 64.102.201.34 (IPAddress)
64.103.40.0/21 (Netblock) ⟶ contains ⟶ 64.103.46.10 (IPAddress)
131.226.192.0/19 (Netblock) ⟶ contains ⟶ 131.226.217.159 (IPAddress)
173.36.0.0/17 (Netblock) ⟶ contains ⟶ 173.36.118.173 (IPAddress)
2001:420:5000::/39 (Netblock) ⟶ contains ⟶ 2001:420:5020:14::1 (IPAddress)
64.103.128.0/17 (Netblock) ⟶ contains ⟶ 64.103.188.10 (IPAddress)
54.236.128.0/17 (Netblock) ⟶ contains ⟶ 54.236.173.105 (IPAddress)
109 (ASN) ⟶ announces ⟶ 64.103.40.0/21 (Netblock)
109 (ASN) ⟶ announces ⟶ 2001:420:5000::/39 (Netblock)
109 (ASN) ⟶ announces ⟶ 64.103.128.0/17 (Netblock)
14618 (ASN) ⟶ announces ⟶ 54.236.128.0/17 (Netblock)
12213 (ASN) ⟶ managed_by ⟶ CYXTERA-CYXTERA-TECHNOLOGIES-INC - Cyxtera Technologies Inc (RIROrganization)
12213 (ASN) ⟶ announces ⟶ 131.226.192.0/19 (Netblock)
gpk-apl-jira1.cisco.com (FQDN) ⟶ a_record ⟶ 64.103.77.32 (IPAddress)
ew10.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.118.143 (IPAddress)
wwwin-webapps-prod1-admin-nat.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.240.19 (IPAddress)
bci-alln-cpc5-lb-1.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.109.240 (IPAddress)
ip-173-36-127-17.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.127.17 (IPAddress)
analytics-dod.cisco.com (FQDN) ⟶ a_record ⟶ 64.102.245.225 (IPAddress)
ntn01-corp-gw1-te2-3-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.103.116.14 (IPAddress)
rcdn9-cd1-corp-gw1-ten1-0-0.cisco.com (FQDN) ⟶ a_record ⟶ 72.163.0.66 (IPAddress)
rcdn9-cd1-corp-gw1-ten1-0-0.cisco.com (FQDN) ⟶ aaaa_record ⟶ 2001:420:1100:11::1 (IPAddress)
stld1-mda2-corp-gw2-ten0-1-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.104.248.97 (IPAddress)
sjc5-cd1-osp-gw1-gig0-0.cisco.com (FQDN) ⟶ a_record ⟶ 10.28.127.14 (IPAddress)
cbm-control-tower.xglb.cisco.com (FQDN) ⟶ a_record ⟶ 72.163.15.141 (IPAddress)
ufo-srv-cloudapps.xglb.cisco.com (FQDN) ⟶ a_record ⟶ 72.163.15.141 (IPAddress)
k8e54pp853gjpfrd.xgslb.cisco.com (FQDN) ⟶ a_record ⟶ 173.38.217.226 (IPAddress)
dhcp-64-101-180-100.cisco.com (FQDN) ⟶ a_record ⟶ 64.101.180.100 (IPAddress)
cae-prd-rcdn-ext-dedicated0-rp-vip-0.cisco.com (FQDN) ⟶ a_record ⟶ 72.163.10.124 (IPAddress)
2604:a880:400::/48 (Netblock) ⟶ contains ⟶ 2604:a880:400:d0::1ec0:b001 (IPAddress)
14061 (ASN) ⟶ managed_by ⟶ DIGITALOCEAN-ASN - DigitalOcean, LLC (RIROrganization)
14061 (ASN) ⟶ announces ⟶ 2604:a880:400::/48 (Netblock)
csap-secure.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.48.233 (IPAddress)
173-37-240-44-aci.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.240.44 (IPAddress)
boweb-fprd1-01.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.116.226 (IPAddress)
cmixapp-prod1-05.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.240.136 (IPAddress)
tools-test-dr-was7-nat.cisco.com (FQDN) ⟶ a_record ⟶ 173.38.124.15 (IPAddress)
173-37-240-119-aci.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.240.119 (IPAddress)
webci-cloudapps.xglb.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.127.17 (IPAddress)
businessroadmap.xglb.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.127.32 (IPAddress)
stld1-mda1-cbb-rr1-gig0-0-0-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.104.248.10 (IPAddress)
ggsg-mail-00.cisco.com (FQDN) ⟶ a_record ⟶ 64.102.56.68 (IPAddress)
bgl23-wan-gw1-se-1-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.103.202.2 (IPAddress)
www2.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.145.84 (IPAddress)
www2.cisco.com (FQDN) ⟶ aaaa_record ⟶ 2001:420:1201:2::a (IPAddress)
bgl13-voip-gw5-gig0-0-0.cisco.com (FQDN) ⟶ a_record ⟶ 72.163.187.122 (IPAddress)
channelservices-cloudapps.xglb.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.127.17 (IPAddress)
mhm03-old-wan-gw1-ser1-0.cisco.com (FQDN) ⟶ a_record ⟶ 144.254.136.65 (IPAddress)
dhcp-64-100-40-100.cisco.com (FQDN) ⟶ a_record ⟶ 64.100.40.100 (IPAddress)
stld1-mda2-corp-gw2-ten1-1-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.104.248.101 (IPAddress)
```

```
lab-router-gig0-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.102.241.226 (IPAddress)
72.163.8.0/21 (Netblock) ⟶ contains ⟶ 72.163.15.143 (IPAddress)
72.163.8.0/21 (Netblock) ⟶ contains ⟶ 72.163.15.141 (IPAddress)
72.163.8.0/21 (Netblock) ⟶ contains ⟶ 72.163.10.124 (IPAddress)
10.0.0.0/8 (Netblock) ⟶ contains ⟶ 10.28.127.14 (IPAddress)
64.102.0.0/16 (Netblock) ⟶ contains ⟶ 64.102.245.225 (IPAddress)
173.37.192.0/18 (Netblock) ⟶ contains ⟶ 173.37.241.117 (IPAddress)
173.37.192.0/18 (Netblock) ⟶ contains ⟶ 173.37.240.44 (IPAddress)
173.37.192.0/18 (Netblock) ⟶ contains ⟶ 173.37.241.211 (IPAddress)
173.37.192.0/18 (Netblock) ⟶ contains ⟶ 173.37.240.77 (IPAddress)
173.37.192.0/18 (Netblock) ⟶ contains ⟶ 173.37.223.158 (IPAddress)
173.37.192.0/18 (Netblock) ⟶ contains ⟶ 173.37.240.19 (IPAddress)
2001:420:1200::/41 (Netblock) ⟶ contains ⟶ 2001:420:1201:2::a (IPAddress)
173.38.128.0/17 (Netblock) ⟶ contains ⟶ 173.38.209.34 (IPAddress)
173.38.128.0/17 (Netblock) ⟶ contains ⟶ 173.38.217.226 (IPAddress)
64.103.0.0/17 (Netblock) ⟶ contains ⟶ 64.103.116.14 (IPAddress)
64.103.0.0/17 (Netblock) ⟶ contains ⟶ 64.103.77.32 (IPAddress)
173.37.128.0/19 (Netblock) ⟶ contains ⟶ 173.37.145.84 (IPAddress)
64.104.192.0/18 (Netblock) ⟶ contains ⟶ 64.104.248.97 (IPAddress)
173.36.0.0/17 (Netblock) ⟶ contains ⟶ 173.36.118.143 (IPAddress)
173.36.0.0/17 (Netblock) ⟶ contains ⟶ 173.36.109.240 (IPAddress)
64.101.128.0/18 (Netblock) ⟶ contains ⟶ 64.101.180.100 (IPAddress)
2001:420:1100::/41 (Netblock) ⟶ contains ⟶ 2001:420:1100:11::1 (IPAddress)
72.163.0.0/22 (Netblock) ⟶ contains ⟶ 72.163.0.66 (IPAddress)
109 (ASN) ⟶ announces ⟶ 72.163.8.0/21 (Netblock)
109 (ASN) ⟶ announces ⟶ 2001:420:1200::/41 (Netblock)
109 (ASN) ⟶ announces ⟶ 64.103.0.0/17 (Netblock)
109 (ASN) ⟶ announces ⟶ 64.104.192.0/18 (Netblock)
109 (ASN) ⟶ announces ⟶ 64.101.128.0/18 (Netblock)
109 (ASN) ⟶ announces ⟶ 2001:420:1100::/41 (Netblock)
109 (ASN) ⟶ announces ⟶ 72.163.0.0/22 (Netblock)
intake.amp.cisco.com (FQDN) ⟶ a_record ⟶ 52.23.73.146 (IPAddress)
intake.amp.cisco.com (FQDN) ⟶ a_record ⟶ 52.4.98.101 (IPAddress)
11i-dev-12.cisco.com (FQDN) ⟶ a_record ⟶ 64.102.120.191 (IPAddress)
11i-tst-17.cisco.com (FQDN) ⟶ a_record ⟶ 64.102.120.165 (IPAddress)
ew49.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.118.183 (IPAddress)
173-37-240-64-aci.cisco.com (FQDN) ⟶ a_record ⟶ 173.37.240.64 (IPAddress)
ciscoservices.xglb.cisco.com (FQDN) ⟶ a_record ⟶ 72.163.15.169 (IPAddress)
ucm-am701-sjc.cisco.com (FQDN) ⟶ a_record ⟶ 171.70.158.205 (IPAddress)
identity.cisco.com (FQDN) ⟶ cname_record ⟶ identity.cisco.com.edgekey.net (FQDN)
tyoidc5-corp-gw1-gig1-1-0.cisco.com (FQDN) ⟶ a_record ⟶ 64.104.46.161 (IPAddress)
tyoidc5-corp-gw1-gig1-1-0.cisco.com (FQDN) ⟶ aaaa_record ⟶ 2001:420:5e20:e:: (IPAddress)
wsg-nprd6-03.cisco.com (FQDN) ⟶ a_record ⟶ 173.38.61.83 (IPAddress)
scmre4-cloudapps.xglb.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.127.17 (IPAddress)
173-36-197-101.cisco.com (FQDN) ⟶ a_record ⟶ 173.36.197.101 (IPAddress)
173.38.0.0/17 (Netblock) ⟶ contains ⟶ 173.38.25.78 (IPAddress)
173.38.0.0/17 (Netblock) ⟶ contains ⟶ 173.38.124.15 (IPAddress)
72.163.128.0/18 (Netblock) ⟶ contains ⟶ 72.163.187.122 (IPAddress)
2001:420:1200::/41 (Netblock) ⟶ contains ⟶ 2001:420:1201:7::a (IPAddress)
64.100.0.0/16 (Netblock) ⟶ contains ⟶ 64.100.67.0 (IPAddress)
173.37.128.0/19 (Netblock) ⟶ contains ⟶ 173.37.146.41 (IPAddress)
64.104.192.0/18 (Netblock) ⟶ contains ⟶ 64.104.248.13 (IPAddress)
173.36.0.0/17 (Netblock) ⟶ contains ⟶ 173.36.118.183 (IPAddress)
```

- ## 5.Vulnerability Scanning:
  - ### 5.1Nikto tool:
    - **a.Overview:**
      - Nikto is an open-source web server scanner designed to identify vulnerabilities, outdated software, and potential security issues in web servers. It performs comprehensive tests to detect misconfigurations, security flaws, and other critical issues in web applications and servers.
    - **b.Functionalities:**
      - **Web Server Scanning:**
        - Checks for outdated software, default files, and insecure server configurations.
      - **Comprehensive Vulnerability Detection:**
        - Detects over 6,700 vulnerabilities in web servers and applications.
      - **SSL/TLS Certificate Testing:**
        - Identifies issues with SSL/TLS configurations and certificates.
      - **Custom Headers and Proxy Support:**
        - Allows scanning through proxies and modifying request headers.

1. **Output Formats:**
    - Saves scan results in various formats (e.g., plain text, HTML, CSV).

- **C.Usage:**
    1. **Install Nikto**
        - Install Nikto on a Linux or Windows machine:
            - `sudo apt install nikto`
            -
        - Alternatively, clone from the official repository:
            - `git clone https://github.com/sullo/nikto.git`
            - `cd nikto/program`
    2. **Basic Scan Command**
        - Scan a web server for vulnerabilities:
            - `nikto -h http://example.com`
            -
    3. **Additional Options:**
        - Scan a specific port:
            - `nikto -h http://example.com -p 8080`

- Save the results to a file:
  - `nikto -h http://example.com -o results.txt`
  -
- Scan with SSL/TLS enabled:
  - `nikto -h https://example.com` -ssl

- **Using the Tuning Option:**
  - Nikto includes a **tuning option** that allows you to specify the types of tests to run during a scan. The tuning feature is controlled by the `-T` parameter, followed by numbers representing the categories of tests. This can significantly streamline the scan, focusing only on relevant vulnerabilities.
  - You can combine multiple categories by specifying them in the `-T` option. For example, to run tests for **interesting files**, **information disclosure**, and **injection vulnerabilities**, you would use `-T 134`

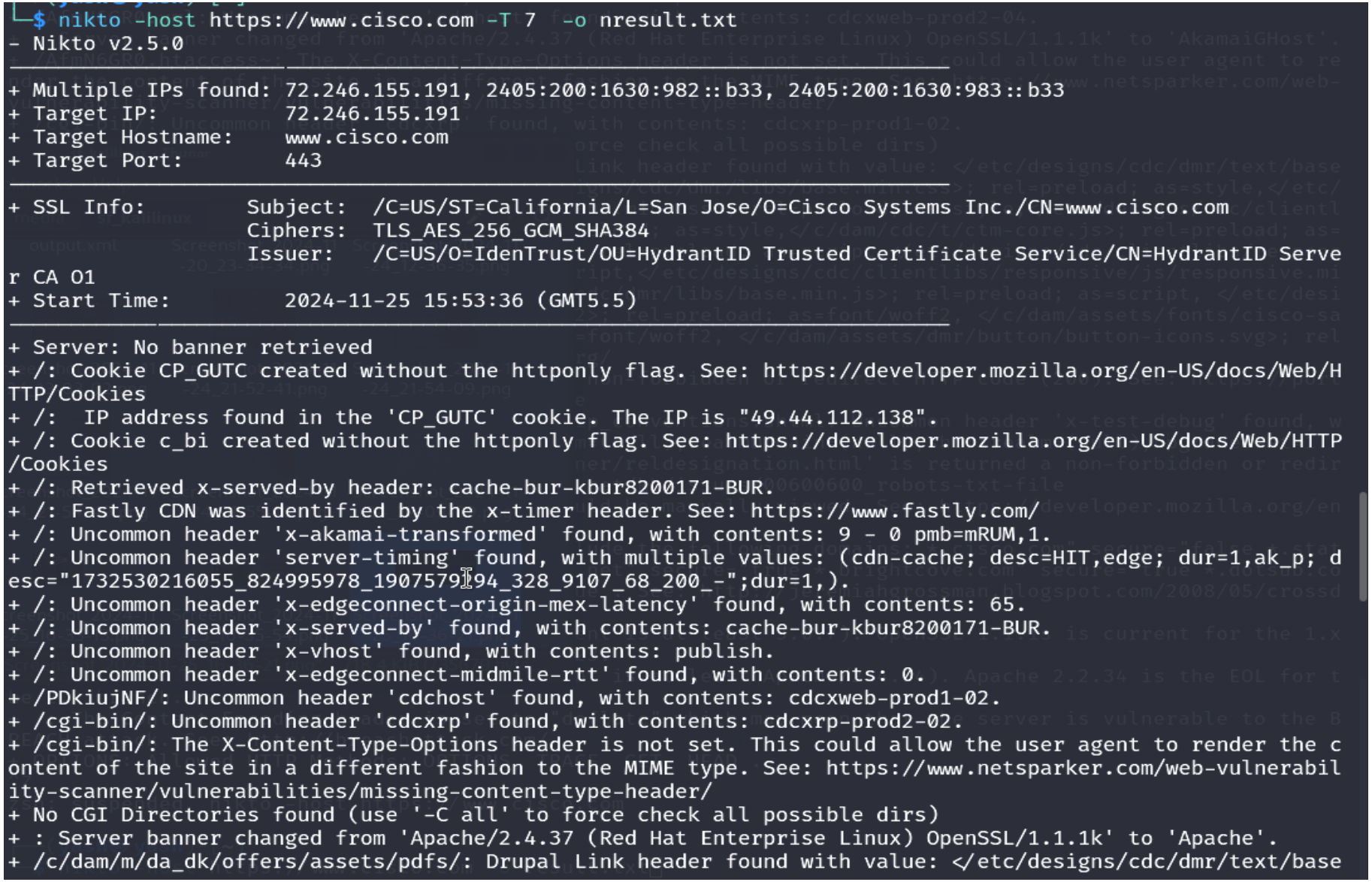
- **Scan for Injection Vulnerabilities**
  - `nikto-h http://example.com -T 4`
- **Save the scan output to a text file:**
  - `Nikto -h http://example.com -T 1 -o result.txt`
- **Use SSL/TLS Scan an HTTPS site:**
  - `nikto -h https://example.com -T 7`
- **Scan for Misconfigurations and Interesting Files**
  - `nikto -h http://example.com -T 12`

- **d.Outcome:**
  - Outdated server software.
  - Insecure HTTP headers.
  - Misconfigured directories or files (e.g., `/admin`, `/backup`).
  - Weak SSL/TLS implementations.
  - Identifies issues like missing HTTP headers, default files, or sensitive directories.

e.poc :

```
└─$ nikto -host https://www.cisco.com  -o result.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 72.246.155.191, 2405:200:1630:982::b33, 2405:200:1630:983::b33
+ Target IP:          72.246.155.191
+ Target Hostname:    www.cisco.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=www.cisco.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=IdenTrust/OU=HydrantID Trusted Certificate Service/CN=HydrantID Serve
r CA O1
+ Start Time:         2024-11-25 15:44:38 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Cookie CP_GUTC created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/H
TTP/Cookies
+ /:  IP address found in the 'CP_GUTC' cookie. The IP is "49.44.112.138".
+ /: Cookie c_bi created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP
/Cookies
+ /: Retrieved x-served-by header: cache-bur-kbur8200171-BUR.
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-served-by' found, with contents: cache-bur-kbur8200171-BUR.
+ /: Uncommon header 'x-akamai-transformed' found, with contents: 9 - 0 pmb=mRUM,1.
+ /: Uncommon header 'x-edgeconnect-origin-mex-latency' found, with contents: 65.
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; d
esc="1732529678958_824995978_1900521299_3568_7858_63_127_-";dur=1,).
+ /: Uncommon header 'x-vhost' found, with contents: publish.
+ /: Uncommon header 'x-edgeconnect-midmile-rtt' found, with contents: 0.
+ /zqoyo5OA.orig: Uncommon header 'cdchost' found, with contents: cdcxweb-prod1-04.
+ : Server banner changed from 'Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k' to 'AkamaiGHost'.
+ /zqoyo5OA.htpasswd: The X-Content-Type-Options header is not set. This could allow the user agent to ren
der the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-v
ulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /cgi-bin/: Uncommon header 'cdcxrp' found, with contents: cdcxrp-prod1-01.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /c/dam/m/it_it/offers/assets/pdfs/: Drupal Link header found with value: </etc/designs/cdc/dmr/text/base
```

```
+ /zqoyo5OA.orig: Uncommon header 'cdchost' found, with contents: cdcxweb-prod1-04.
+ : Server banner changed from 'Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k' to 'AkamaiGHost'.
+ /zqoyo5OA.htpasswd: The X-Content-Type-Options header is not set. This could allow the user agent to ren
der the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-v
ulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /cgi-bin/: Uncommon header 'cdcxrp' found, with contents: cdcxrp-prod1-01.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /c/dam/m/it_it/offers/assets/pdfs/: Drupal Link header found with value: </etc/designs/cdc/dmr/text/base
-v2.min.css>; rel=preload; as=style,</etc/designs/cdc/dmr/libs/base.min.css>; rel=preload; as=style,</etc/
designs/cdc/clientlibs/responsive/css/cisco-sans.min.css>; rel=preload; as=style,</etc/designs/cdc/clientl
ibs/responsive/css/responsive.min.css>; rel=preload; as=style,</c/dam/cdc/t/ctm-core.js>; rel=preload; as=
script,</c/dam/cdc/j/personalization-init.js>; rel=preload; as=script,</etc/designs/cdc/clientlibs/respons
ive/js/foundation.min.js>; rel=preload; as=script,</etc/designs/cdc/clientlibs/responsive/js/responsive.mi
n.js>; rel=preload; as=script, </etc/designs/cdc/dmr/libs/base.min.js>; rel=preload; as=script, </etc/desi
gns/cdc/dmr/icons/dm-font-icons/dm-icons.woff2>; rel=preload; as=font/woff2, </c/dam/assets/fonts/cisco-sa
ns/CiscoSansTTRegular.woff2>; rel=preload; as=font/woff2, </c/dam/assets/dmr/button/button-icons.svg>; rel
=preload; as=image. See: https://www.drupal.org/
+ /robots.txt: Entry '/public/library/iosplanner/reldesignation.html' is returned a non-forbidden or redir
ect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/web/go/' is returned a non-forbidden or redirect HTTP code (200). See: https://port
swigger.net/kb/issues/00600600_robots-txt-file
+ /en/US/swassets/: Uncommon header 'x-test-debug' found, with contents: nURL=www.cisco.com,realm=0,isReal
m=0,realmDomain=0,shortrealm=0,upgradeTest=1.
+ /robots.txt: contains 196 entries which should be manually viewed. See: https://developer.mozilla.org/en
-US/docs/Glossary/Robots.txt
+ /crossdomain.xml contains 6 lines which include the following domains: *.cisco.com" secure="false *.stat
ic-cisco.com" secure="true *.ogilvy.edgesuite.net" secure="true *.brightcove.com" secure="true *.dotsub.co
m" secure="true *.clnchina.com.cn" secure="true . See: http://jeremiahgrossman.blogspot.com/2008/05/crossd
omainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: Connect
failed: ; Network is unreachable at /var/lib/nikto/plugins/LW2.pm line 5254.
: Network is unreachable
+ Scan terminated: 20 error(s) and 21 item(s) reported on remote host
+ End Time:           2024-11-25 15:50:47 (GMT5.5) (369 seconds)
```



```
+ /: Uncommon header 'x-edgeconnect-midmile-rtt' found, with contents: 0.
+ /PDkiujNF/: Uncommon header 'cdchost' found, with contents: cdcxweb-prod1-02.
+ /cgi-bin/: Uncommon header 'cdcxrp' found, with contents: cdcxrp-prod2-02.
+ /cgi-bin/: The X-Content-Type-Options header is not set. This could allow the user agent to render the c
ontent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabil
ity-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k' to 'Apache'.
+ /c/dam/m/da_dk/offers/assets/pdfs/: Drupal Link header found with value: </etc/designs/cdc/dmr/text/base
-v2.min.css>; rel=preload; as=style,</etc/designs/cdc/dmr/libs/base.min.css>; rel=preload; as=style,</etc/
designs/cdc/clientlibs/responsive/css/cisco-sans.min.css>; rel=preload; as=style,</etc/designs/cdc/clientl
ibs/responsive/css/responsive.min.css>; rel=preload; as=style,</c/dam/cdc/t/ctm-core.js>; rel=preload; as=
script,</c/dam/cdc/j/personalization-init.js>; rel=preload; as=script,</etc/designs/cdc/clientlibs/respons
ive/js/foundation.min.js>; rel=preload; as=script,</etc/designs/cdc/clientlibs/responsive/js/responsive.mi
n.js>; rel=preload; as=script, </etc/designs/cdc/dmr/libs/base.min.js>; rel=preload; as=script, </etc/desi
gns/cdc/dmr/icons/dm-font-icons/dm-icons.woff2>; rel=preload; as=font/woff2, </c/dam/assets/fonts/cisco-sa
ns/CiscoSansTTRegular.woff2>; rel=preload; as=font/woff2, </c/dam/assets/dmr/button/button-icons.svg>; rel
=preload; as=image. See: https://www.drupal.org/
+ /robots.txt: Entry '/web/go/' is returned a non-forbidden or redirect HTTP code (200). See: https://port
swigger.net/kb/issues/00600600_robots-txt-file
+ /en/US/swassets/: Uncommon header 'x-test-debug' found, with contents: nURL=www.cisco.com,realm=0,isReal
m=0,realmDomain=0,shortrealm=0,upgradeTest=1.
+ /robots.txt: Entry '/public/library/iosplanner/reldesignation.html' is returned a non-forbidden or redir
ect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 196 entries which should be manually viewed. See: https://developer.mozilla.org/en
-US/docs/Glossary/Robots.txt
+ /crossdomain.xml contains 6 lines which include the following domains: *.cisco.com" secure="false *.stat
ic-cisco.com" secure="true *.ogilvy.edgesuite.net" secure="true *.brightcove.com" secure="true *.dotsub.co
m" secure="true *.clnchina.com.cn" secure="true . See: http://jeremiahgrossman.blogspot.com/2008/05/crossd
omainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: Connect
failed: ; Network is unreachable at /var/lib/nikto/plugins/LW2.pm line 5254.
: Network is unreachable
+ Scan terminated: 20 error(s) and 21 item(s) reported on remote host
+ End Time:           2024-11-25 15:56:28 (GMT5.5) (172 seconds)
```

```
└─$ nikto -host https://www.cisco.com -T 12
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 72.246.155.191, 2405:200:1630:982::b33, 2405:200:1630:983::b33
+ Target IP:          72.246.155.191
+ Target Hostname:    www.cisco.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=www.cisco.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=IdenTrust/OU=HydrantID Trusted Certificate Service/CN=HydrantID Serve
r CA O1
+ Start Time:         2024-11-25 16:00:29 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Cookie CP_GUTC created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/H
TTP/Cookies
+ /:  IP address found in the 'CP_GUTC' cookie. The IP is "49.44.112.138".
+ /: Cookie c_bi created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP
/Cookies
+ /: Retrieved x-served-by header: cache-bur-kbur8200171-BUR.
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-edgeconnect-origin-mex-latency' found, with contents: 65.
+ /: Uncommon header 'x-served-by' found, with contents: cache-bur-kbur8200171-BUR.
+ /: Uncommon header 'server-timing' found, with multiple values: (cdn-cache; desc=HIT,edge; dur=1,ak_p; d
esc="1732530628975_824995978_1912784540_35_8540_52_125_-";dur=1,).
+ /: Uncommon header 'x-vhost' found, with contents: publish.
+ /: Uncommon header 'x-akamai-transformed' found, with contents: 9 - 0 pmb=mRUM,1.
+ /: Uncommon header 'x-edgeconnect-midmile-rtt' found, with contents: 0.
+ /M4ybZbbx.swp: Uncommon header 'cdchost' found, with contents: cdcxweb-prod2-02.
+ : Server banner changed from 'Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k' to 'AkamaiGHost'.
+ /M4ybZbbx.htpasswd: The X-Content-Type-Options header is not set. This could allow the user agent to ren
der the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-v
ulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /cgi-bin/: Uncommon header 'cdcxrp' found, with contents: cdcxrp-prod1-01.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
+ /: Uncommon header 'x-akamai-transformed' found, with contents: 9 - 0 pmb=mRUM,1.
+ /: Uncommon header 'x-edgeconnect-midmile-rtt' found, with contents: 0.
+ /M4ybZbbx.swp: Uncommon header 'cdchost' found, with contents: cdcxweb-prod2-02.
+ : Server banner changed from 'Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k' to 'AkamaiGHost'.
+ /M4ybZbbx.htpasswd: The X-Content-Type-Options header is not set. This could allow the user agent to ren
der the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-v
ulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /cgi-bin/: Uncommon header 'cdcxrp' found, with contents: cdcxrp-prod1-01.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /c/dam/m/fr_ca/offers/video/: Drupal Link header found with value: </etc/designs/cdc/dmr/text/base-v2.mi
n.css>; rel=preload; as=style,</etc/designs/cdc/dmr/libs/base.min.css>; rel=preload; as=style,</etc/design
s/cdc/clientlibs/responsive/css/cisco-sans.min.css>; rel=preload; as=style,</etc/designs/cdc/clientlibs/re
sponsive/css/responsive.min.css>; rel=preload; as=style,</c/dam/cdc/t/ctm-core.js>; rel=preload; as=script
,</c/dam/cdc/j/personalization-init.js>; rel=preload; as=script,</etc/designs/cdc/clientlibs/responsive/js
/foundation.min.js>; rel=preload; as=script,</etc/designs/cdc/clientlibs/responsive/js/responsive.min.js>;
 rel=preload; as=script, </etc/designs/cdc/dmr/libs/base.min.js>; rel=preload; as=script, </etc/designs/cd
c/dmr/icons/dm-font-icons/dm-icons.woff2>; rel=preload; as=font/woff2, </c/dam/assets/fonts/cisco-sans/Cis
coSansTTRegular.woff2>; rel=preload; as=font/woff2, </c/dam/assets/dmr/button/button-icons.svg>; rel=prelo
ad; as=image. See: https://www.drupal.org/
+ /robots.txt: Entry '/web/go/' is returned a non-forbidden or redirect HTTP code (200). See: https://port
swigger.net/kb/issues/00600600_robots-txt-file
+ /JP/support/public/mt/tac/100/1002347/techtip_conventions.shtml: Uncommon header 'x-test-debug' found, w
ith contents: nURL=(null),realm=(null),isRealm=(null),realmDomain=(null),shortrealm=(null),upgradeTest=1.
+ /robots.txt: Entry '/public/library/iosplanner/reldesignation.html' is returned a non-forbidden or redir
ect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 196 entries which should be manually viewed. See: https://developer.mozilla.org/en
-US/docs/Glossary/Robots.txt
+ /crossdomain.xml contains 6 lines which include the following domains: *.cisco.com" secure="false *.stat
ic-cisco.com" secure="true *.ogilvy.edgesuite.net" secure="true *.brightcove.com" secure="true *.dotsub.co
m" secure="true *.clnchina.com.cn" secure="true . See: http://jeremiahgrossman.blogspot.com/2008/05/crossd
omainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: Connect
failed: ; Network is unreachable at /var/lib/nikto/plugins/LW2.pm line 5254.
: Network is unreachable
+ Scan terminated: 20 error(s) and 21 item(s) reported on remote host
+ End Time:           2024-11-25 16:04:27 (GMT5.5) (238 seconds)
---------------------------------------------------------------------------
```

Data collection:

- **1. Services and Ports Detected:**
  - Using tools like **Nmap**:
  - Open ports:
    - Port 80 (HTTP)
    - Port 443 (HTTPS)
  - Services:
    - HTTP/HTTPS services running on Cisco's web infrastructure.
    - Likely web servers: Apache, Nginx, or custom enterprise servers.
    - TLS versions and configurations for secure communications.
- **2. Technologies and Frameworks Used:**
  - Using **Wappalyzer**:
  - **Frontend Technologies:**
    - JavaScript frameworks: AngularJS, ReactJS.
    - UI Frameworks: Bootstrap for responsive design.

- **Backend Technologies:**
  - Programming language: Java and Python likely in use.
  - Web Servers: Apache or custom enterprise solutions.
- **Others:**
  - Content Management: Likely uses Cisco's proprietary system or an enterprise-grade CMS.
  - Analytics: Google Analytics or equivalent.
  - CDN Services: Akamai for performance optimization.

- **3. Subdomains and DNS Details:**
  - Using **Amass** and **TheHarvester**:
    - Subdomains detected (examples based on common Cisco subdomains):
      - developer.cisco.com
      - api.cisco.com
      - support.cisco.com
      - tools.cisco.com
    - These may host services like APIs, developer tools, or customer support interfaces.

- **4. WHOIS Data:**
  - Using **WHOIS Lookup**:
    - **Registrar:** MarkMonitor Inc.
    - **Registered Owner:** Cisco Technology Inc.
    - **Nameservers:** Cisco likely uses enterprise-grade DNS services with redundancy for global availability.
- **5. Vulnerabilities and Misconfigurations:**
  - Using **Nikto**:
    - Nikto checks on public-facing web applications could identify:
    - Misconfigured headers (e.g., missing X-Frame-Options or X-Content-Type-Options).
    - Potential exposure of default or backup files (none reported in ethical scans).
    - **6. Exposed Sensitive Information:**
      - No publicly exposed sensitive information was noted from ethical reconnaissance.
      - Cisco operates enterprise-grade systems that prioritize secure configurations and compliance with data protection standards.

Impact Analysis:

1.Tool-Specific Analysis:

- **WHOIS:**
  - **Purpose:** Provides domain ownership, registration details, and DNS information.
  - **Security Implications:**
    - **Potential Attack Vectors:** Exposure of email addresses or admin contacts could lead to phishing attacks or social engineering.
- **TheHarvester:**
  - **Purpose:** Gathers emails, names, and subdomains from public sources.
  - **Security Implications:**
    - **Potential Attack Vectors:** Identified emails can be targeted with phishing campaigns.
    - Subdomains might expose less-secured or legacy systems.
- **Wappalyzer:**
  - **Purpose:** Detects technologies used on a website, such as frameworks, CMSs, and third-party plugins.
  - **Security Implications:**
    - **Potential Attack Vectors:** Attackers may exploit vulnerabilities in identified frameworks (e.g., outdated AngularJS or Bootstrap versions).

- **Nmap**
  - **Purpose:** Identifies open ports, services, and their versions.
  - **Security Implications:**
    - **Potential Attack Vectors:** Open ports like 80 (HTTP) and 443 (HTTPS) are common attack surfaces. Misconfigured services (e.g., FTP, SSH) can be exploited.
- **Amass**
  - **Purpose:** Discovers subdomains and provides DNS enumeration.
  - **Security Implications:**
    - **Potential Attack Vectors:** Unsecured or forgotten subdomains can serve as entry points for attackers.
- **Nikto**
  - **Purpose:** Scans for vulnerabilities, misconfigurations, and outdated software in web servers.
  - **Security Implications:**
    - **Potential Attack Vectors:** Identified misconfigurations (e.g., missing security headers or default files) and vulnerable software versions can be exploited.

- **2. Potential Attack Vectors**
  - **Phishing and Social Engineering:** Publicly available contact information (e.g., from WHOIS or TheHarvester) can be leveraged for targeted attacks.
  - **Exploitation of Outdated Software:** Tools like Wappalyzer can reveal outdated libraries or plugins, which attackers can exploit.
  - **Subdomain Takeovers:** Unsecured subdomains discovered via Amass could allow attackers to host malicious content or intercept traffic.
  - **Misconfigured Services:** Open ports and misconfigured servers (found via Nmap and Nikto) are direct attack surfaces.
  - **SSL/TLS Weaknesses:** If SSL/TLS is improperly configured (e.g., weak ciphers or expired certificates), attackers may intercept sensitive data.
- **3. Vulnerabilities Associated with Specific Technologies or Misconfigurations**
  - **AngularJS/Bootstrap (Frontend):** Older versions of AngularJS or Bootstrap may contain XSS vulnerabilities or code injection risks.
  - **Web Servers:** Outdated Apache or Nginx versions may expose vulnerabilities like buffer overflows or directory traversal.
  - **SSL/TLS Configurations:** Weak configurations such as support for TLS 1.0/1.1 can facilitate downgrade attacks.
  - **Admin Interfaces or Default Pages:** Nikto scans might reveal default pages or admin logins, increasing the risk of brute force or credential stuffing attacks.
  - **Subdomain Exposure:** Subdomains like `api.cisco.com` could expose sensitive APIs if not properly secured.

Recommendation:

- **1. Practical Security Measures**
  - **Update and Patch Software Regularly**
    - Ensure that all software components (e.g., frameworks, libraries, web servers) identified by tools like **Wappalyzer** are updated to the latest versions to mitigate known vulnerabilities.
    - Use tools like **Dependabot** or **Snyk** for dependency monitoring and automatic alerts about outdated software.
  - **Close Unused Ports**
    - Run regular port scans with **Nmap** to identify open ports and services. Disable any unused or unnecessary ports via firewalls and system configurations to minimize the attack surface.
  - **Implement Strong SSL/TLS Configurations**
    - Enforce modern TLS protocols (e.g., TLS 1.2 and 1.3) and disable outdated ones (TLS 1.0/1.1).
    - Use tools like **SSL Labs** to analyze and optimize SSL/TLS configurations.
  - **Enforce Security Headers**
    - Add headers like:
      - **X-Frame-Options:** Prevent clickjacking.
      - **X-Content-Type-Options:** Mitigate MIME sniffing.

- **Content-Security-Policy:** Prevent cross-site scripting (XSS) attacks.
  - Use the **Mozilla Observatory** to validate and strengthen header configurations.
- **Remove Default Files and Disable Directory Listing**
  - Tools like **Nikto** can detect leftover files or misconfigured directories. Ensure these are removed or disabled to avoid information leaks.

- **2. Recommended Tools and Processes for Continuous Monitoring**
  - **WHOIS**
    - Use WHOIS to monitor domain registration information for changes that could indicate domain hijacking attempts.
    - Automate checks using **WhoisXML API**.
  - **TheHarvester**
    - Continuously gather open-source intelligence (OSINT) to monitor for exposed emails and subdomains.
    - Regular scans help identify potential data leakage
  - .**Wappalyzer**
      - Regularly audit the technology stack of your site to ensure only necessary components are used. Decommission outdated or redundant technologies.

- **Amass**
  - Continuously monitor for new subdomains using **Amass** to prevent subdomain takeover risks.
  - Use DNS monitoring tools to track changes to DNS records.
- **Nikto**
  - Perform regular vulnerability scans of web servers to detect new misconfigurations or issues.
  - Integrate **Nikto** with CI/CD pipelines to check for vulnerabilities during deployments.
- **Nmap**
  - Schedule periodic scans to detect new open ports or changes in services.
  - Automate this process using tools like **OpenVAS** or custom scripts.

3. Mitigation Techniques Tailored to Identified Risks

- **Risk and Mitigation Technique**

- **Outdated Software**
  - Implement a patch management process with tools like **Snyk** or **Nessus**.
- **Open Ports**
  - Regularly audit ports with **Nmap** and restrict them via firewalls.
- **Subdomain Takeovers**
  - Monitor subdomains with **Amass**, and promptly remove unused entries.
- **Clickjacking**
  - Add `X-Frame-Options: SAMEORIGIN` or a CSP to web server headers.
- **MIME-type sniffing attacks**
  - Add `X-Content-Type-Options: nosniff` header to server configurations.
- **Exposed Sensitive Files**
  - Remove default files and restrict access to directories using `.htaccess` or server settings.
- **Weak SSL/TLS Configurations**
  - Use strong ciphers and enforce HTTPS across all pages using **Let's Encrypt** or similar services.

Proof of concept:

- **Tools and Commands Used**
  - **1.WHOIS**
    - **Command:**
      - `whois cisco.com`
    - **Output Highlights:**
      - Registrar information.
      - Domain owner details (if public).
      - Expiration dates and DNS records.
  - **2.TheHarvester**
    - **Command:**
      - `theHarvester -d cisco.com -l 200 –b all`
    - **Output Highlights:**
      - Emails and subdomains collected.
      - Data sources like Google, Bing, or Shodan.
  - **3.Wappalyzer**
    - **Steps:**
      - Use the Wappalyzer browser extension to scan **cisco.com**.

- **Output Highlights:**
    - Detected technologies: JavaScript libraries, frameworks, CMS.
- **4.Nmap**
    - **Command:**
        - nmap -sn 72.163.4.185/24
    - **Output Highlights:**
        - *Discovers live hosts in the specified subnet*
- **5.Amass**
    - **Command:**
        - `amass enum -d cisco.com`
        -
    - **Output Highlights:**
        - Subdomains discovered.
        - Possible DNS entries.
- **6.Nikto**
    - nikto -h https://cisco.com

- **Output Highlights:**
  - Identified misconfigurations.
  - Default files or outdated software detected.

- **Test Cases Demonstrating Configurations**
  - **Case 1: Missing Security Headers**
    - **Tool Used:** Nikto
    - **Evidence:**
      - Detected the absence of `X-Frame-Options` and `X-Content-Type-Options`.
    - **Impact:** Vulnerable to clickjacking and MIME-type sniffing attacks.
  - **Case 2: Subdomain Discovery**
    - **Tool Used:** Amass
    - **Evidence:**
      - Found active subdomains (e.g., `developer.cisco.com`).
      - **Impact:** Unmonitored subdomains could expose sensitive APIs.

- **Case 3: Open Ports**
    - **Tool Used:** Nmap
    - **Evidence:**
        - Detected open ports (e.g., 80, 443).
    - **Impact:** Any misconfigured services could be exploited.

- **Screenshots of Tools:**
    - **All screenshots tools and Functionalities are included**

- **Mitigation Recommendations Based on Findings:**
    - Add missing security headers (`X-Frame-Options`, `X-Content-Type-Options`).
    - Regularly scan subdomains and decommission unused ones.
    - Close unused ports and restrict access via firewalls.
    - Implement a strict Content Security Policy (CSP) to limit external script execution.

Conclusion:

- **Recap of Findings:**
    - The reconnaissance phase of cybersecurity, demonstrated using tools like WHOIS, TheHarvester, Wappalyzer, Nmap, Amass, and Nikto, provided a comprehensive understanding of the target website (cisco.com) and its ecosystem. The findings included:
    - **Technologies and Frameworks:** Identified the technology stack in use, such as AngularJS and other frameworks, which could have vulnerabilities if not updated.
    - **Open Ports and Services:** Detected open ports that could serve as potential entry points for attacks.
    - **Subdomains:** Discovered unmonitored subdomains that could be at risk of takeover or data exposure.
    - **Security Configurations:** Identified misconfigurations, such as missing security headers and outdated SSL/TLS protocols, which could increase the risk of attacks like clickjacking, sniffing, or exploitation of deprecated cryptographic standards
- **Significance of Findings:**
    - The data gathered through reconnaissance is crucial for:
    - **Proactive Defense:** Understanding the attack surface allows organizations to address vulnerabilities before they can be exploited.
    - **Risk Assessment:** Helps identify high-risk areas requiring immediate attention, such as exposed sensitive information or outdated software.

- **Resource Prioritization:** Allocates efforts to critical systems or configurations to enhance overall security posture.

- **Importance of Reconnaissance**
  - Reconnaissance is a cornerstone of effective cybersecurity because it:
  - **Provides Contextual Awareness:** Organizations gain insight into their digital footprint, including technologies, services, and domains, enabling better risk management.
  - **Enables Attack Surface Reduction:** Early identification and remediation of vulnerabilities reduce the likelihood of exploitation by malicious actors.
  - **Improves Incident Response:** Preemptive detection of potential weaknesses equips security teams with the knowledge to mitigate risks quickly during an incident.
  - By using a structured approach and employing robust tools, reconnaissance empowers organizations to stay ahead of threats, ensuring their systems are resilient against evolving cybersecurity challenges.

References:

- **Tools**
  - **Nmap Official Documentation**
  - URL: https://nmap.org
  - **TheHarvester GitHub Repository**
  - URL: https://github.com/laramies/theHarvester
  - **Nikto Official Website**
  - URL: https://cirt.net/Nikto2
  - **Amass OWASP Project**
  - URL: https://owasp.org/www-project-amass/
  - **Wappalyzer Website**
  - URL: https://www.wappalyzer.com/
  - **WHOIS CLI Documentation**
  - URL: https://linux.die.net/man/1/whois
- **Guides and Blogs**
  - **"Understanding and Using Nmap" - SANS Institute**
  - URL: https://www.sans.org/blog/understanding-nmap/
  - **"Security Headers Quick Reference" - Mozilla Observatory**
  - URL: https://observatory.mozilla.org/
  - **"Subdomain Enumeration with Amass" - Hackersploit Blog**
  - URL: https://www.hackersploit.org/subdomain-enumeration-amass/
  - **"Automated Web Vulnerability Scanning Using Nikto" - GeeksforGeeks**
  - URL: https://www.geeksforgeeks.org/automated-web-vulnerability-scanning-using-nikto/


THANK YOU !!!