A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report – compass**

**IT21831904 – K.M. Weerasinghe**

Table of Contents

[Scope of the target 3](#_Toc149509735)

[In scope and rewards 3](#_Toc149509736)

[Out of scope 3](#_Toc149509737)

[Reconnaissance 4](#_Toc149509738)

[Subdomain enumeration 4](#_Toc149509739)

[Gathering information about the target 5](#_Toc149509740)

[Virtual host discovery 8](#_Toc149509741)

[Subdomain takeover 9](#_Toc149509742)

[Scanning 10](#_Toc149509743)

[Using Nmap for scanning 10](#_Toc149509744)

[Using final recon for scanning 10](#_Toc149509745)

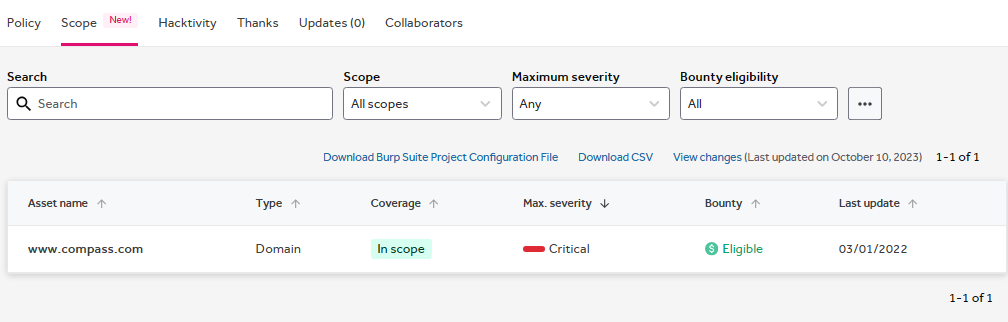
[Vulnerability checking 13](#_Toc149509746)

[Vulnerabilities found using NIKTO 13](#_Toc149509747)

[Vulnerabilities found using rapidscan 14](#_Toc149509748)

# Scope of the target

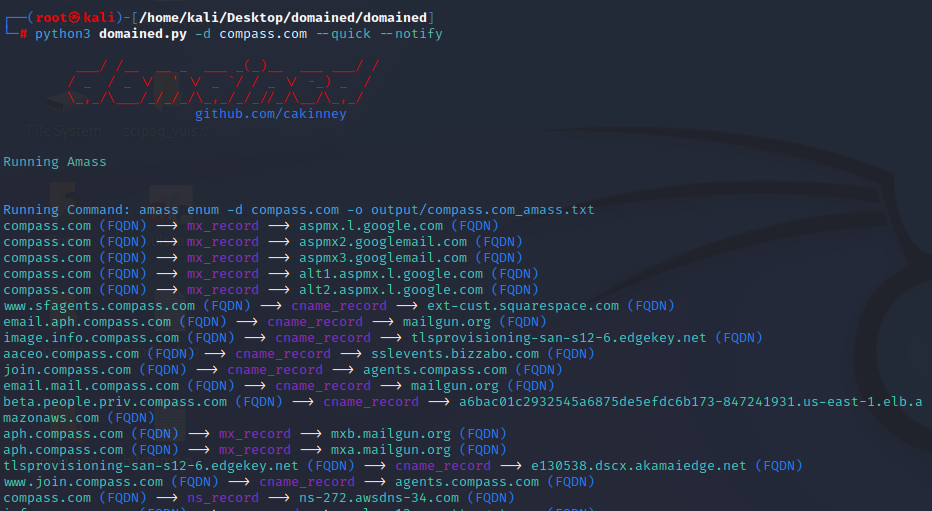
## In scope and rewards



## Out of scope

# Reconnaissance

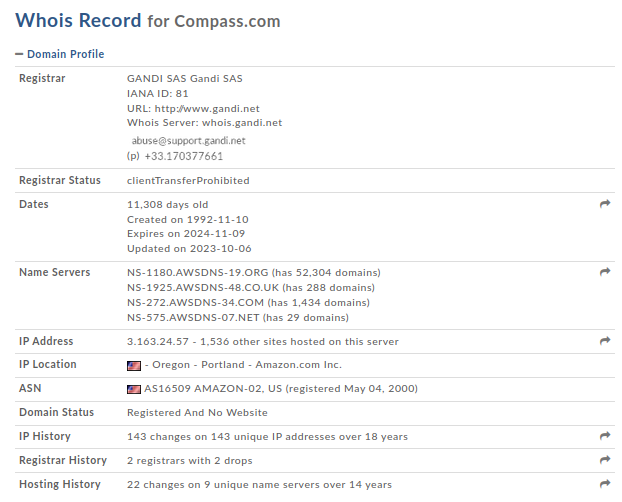
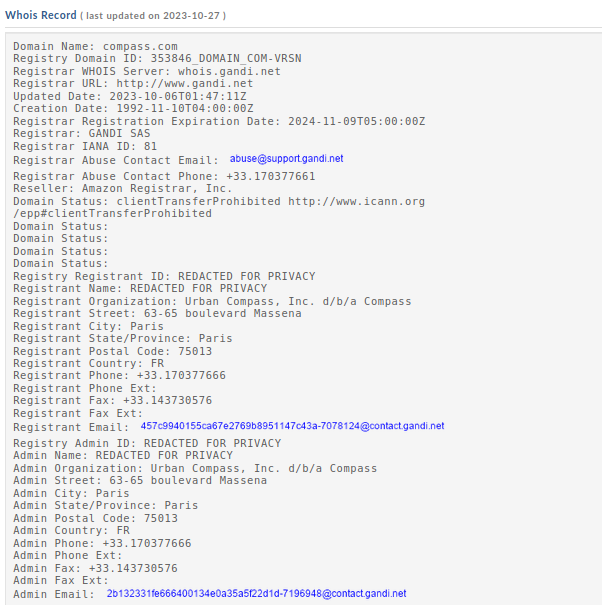
## Subdomain enumeration

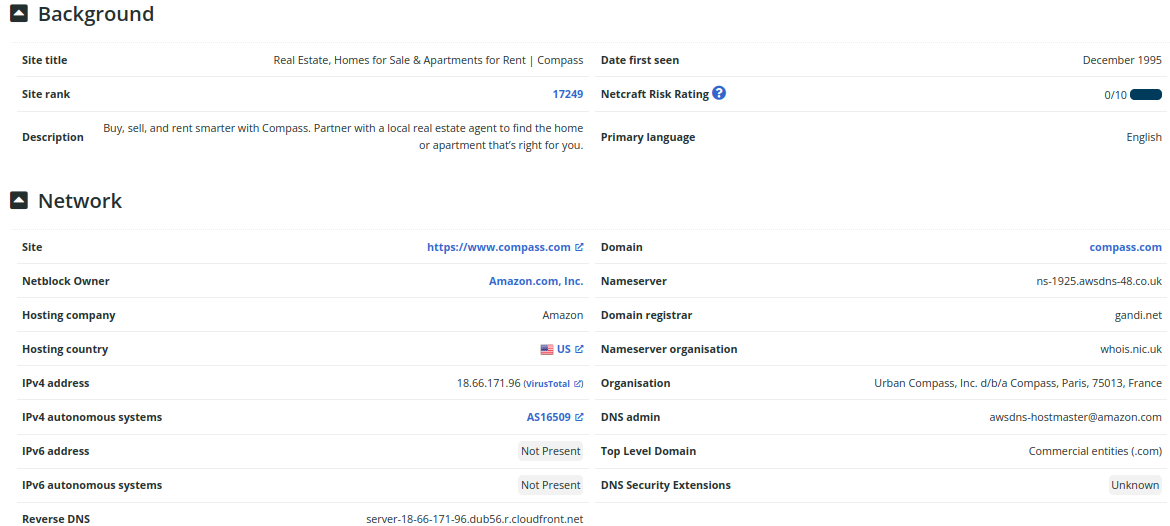
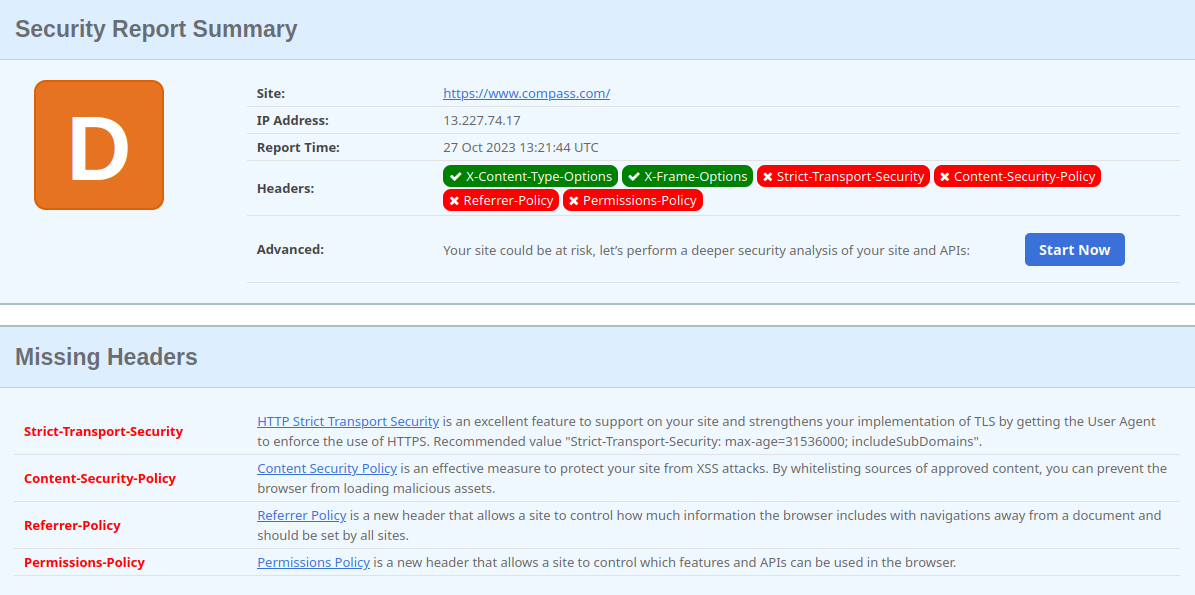
* Using domained.py tools amass and subfinder to do the subdomain enumeration
* └─# python3 domained.py -d compass.com --quick --notify

A screenshot of a computer

Description automatically generated

## Gathering information about the target

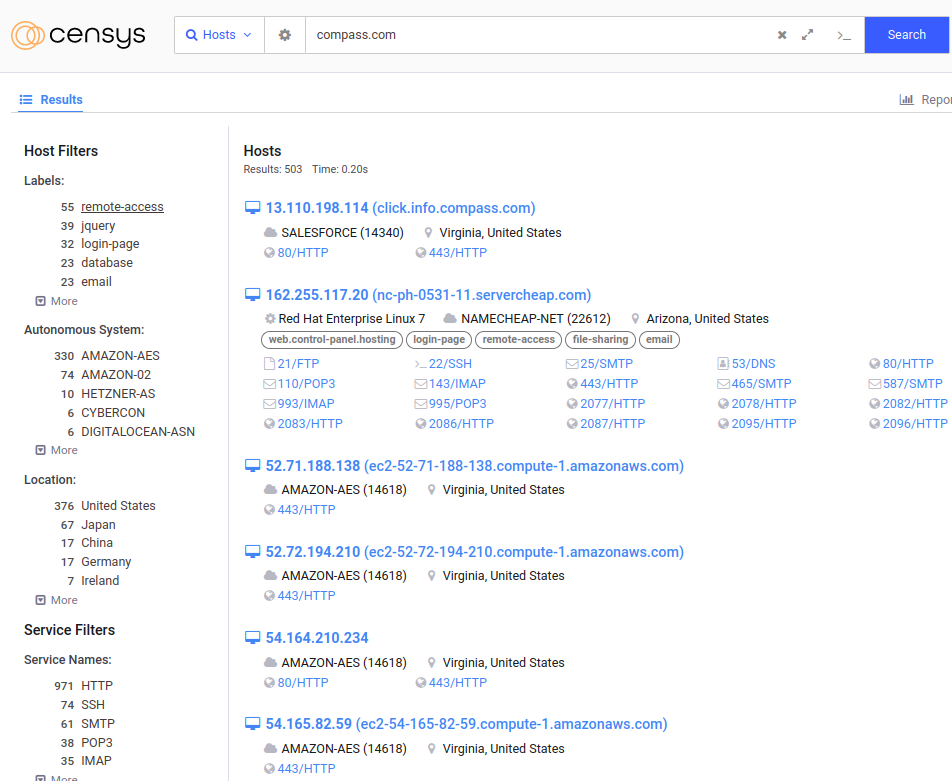
* Domain profile and whois records
  + Domain profile
  + Whois records
  + A screenshot of a computer

    Description automatically generatednetcraft scan to gather background, network, and certificate information
  + security header checking

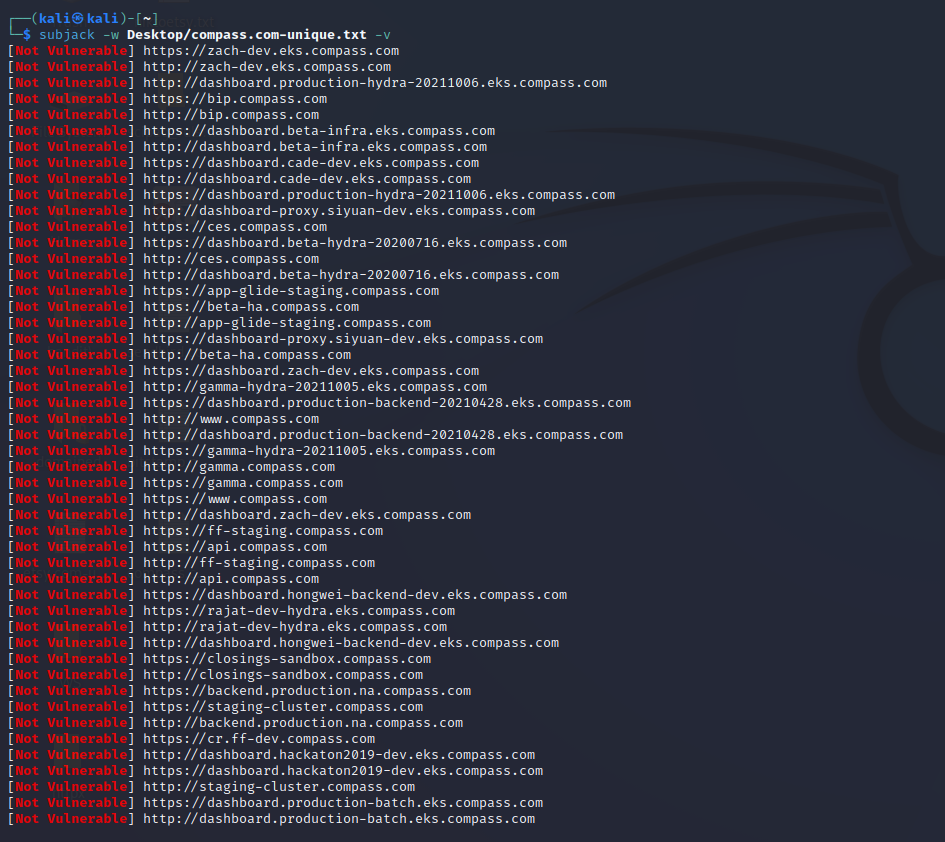
missing headers - Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.

* + Strict-Transport-Security
    - HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
  + Content-Security-Policy
    - Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
  + Referrer-Policy
    - Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
  + Permissions-Policy
    - Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

## Virtual host discovery

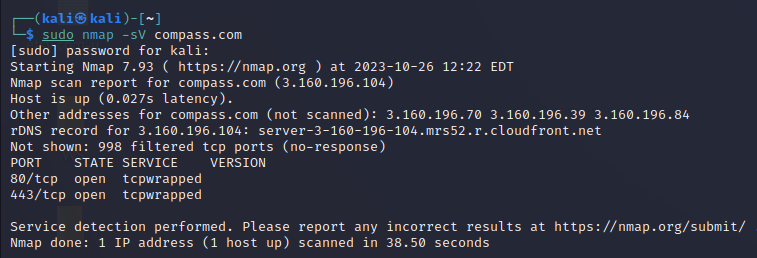


## Subdomain takeover

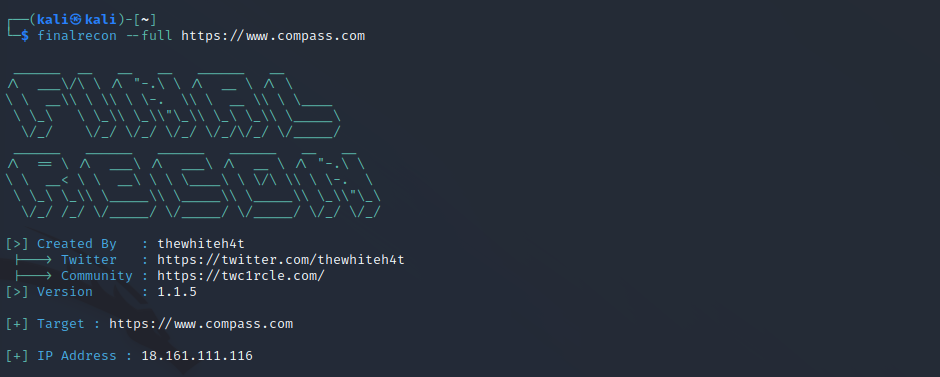
* Identifying if any of the found subdomains from the previous scans are vulnerable to takeover
* └─$ subjack -w Desktop/compass.com-unique.txt -v
* No vulnerable subdomains were found
* All subdomains appear to be secure
* No issues were identified in the subdomain analysis

# Scanning

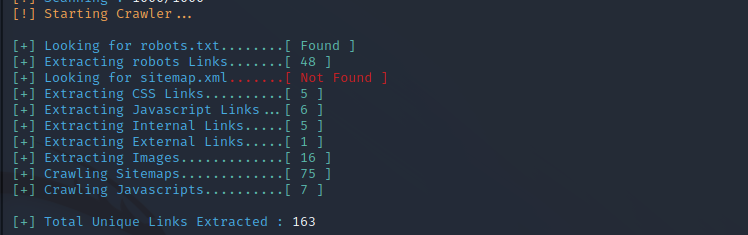
## Using Nmap for scanning

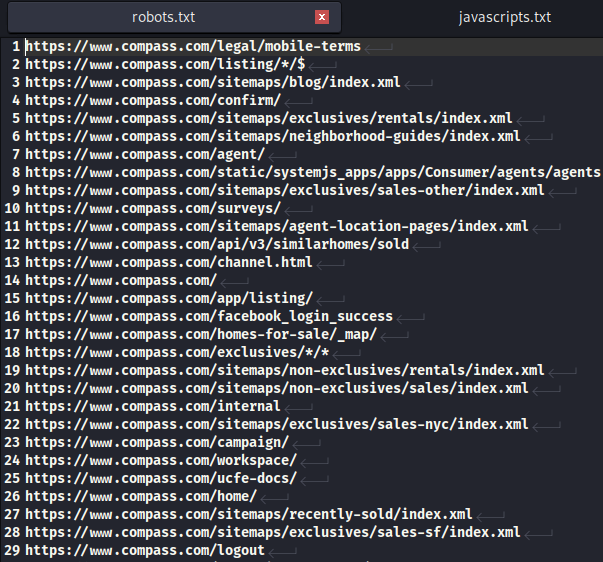


## Using final recon for scanning

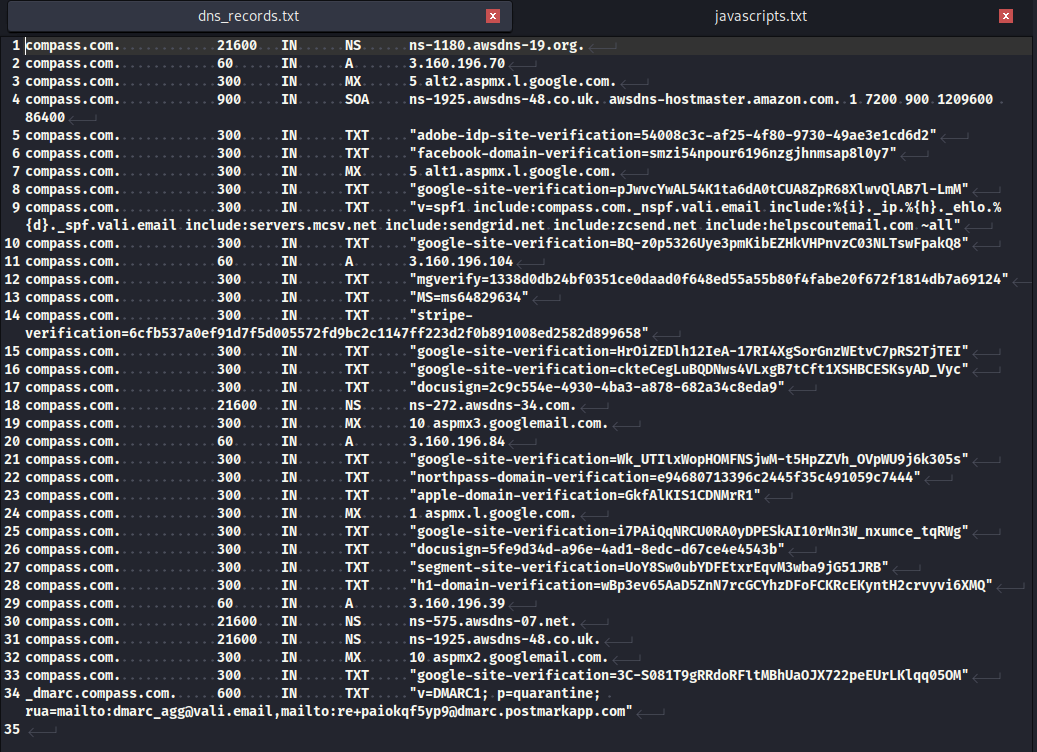


Information gathered using crawlers



Robots.txt files found

DNS records found



* How DNS records could be used
  + DNS hijacking, which is a type of DNS attack in which DNS queries are incorrectly resolved to unexpectedly redirect users to malicious sites
  + DNS tunneling: Attackers can use DNS records to tunnel traffic to and from their own servers. This can be used to bypass network security controls, such as firewalls and web application firewalls.
  + DNS amplification attacks: Attackers can use DNS records to launch DNS amplification attacks against the bug bounty program's website or other infrastructure. This can be done by sending large DNS requests to the bug bounty program's DNS servers. If the attack is successful, it can overwhelm the servers and cause the website to become unavailable.

# Vulnerability checking

## Vulnerabilities found using NIKTO

* NIKTO scan to check for vulnerabilities
  + └─$ nikto -h compass.com

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 3.160.196.104

+ Target Hostname: compass.com

+ Target Port: 80

+ Message: Multiple IP addresses found: 3.160.196.104, 3.160.196.84, 3.160.196.39, 3.160.196.70

+ Start Time: 2023-10-26 12:56:15 (GMT-4)

---------------------------------------------------------------------------

+ Server: CloudFront

+ Retrieved via header: 1.1 bc6de7d15bcc2ecdbff00d480028457c.cloudfront.net (CloudFront)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ Uncommon header 'x-amz-cf-pop' found, with contents: MRS52-P6

+ Uncommon header 'x-cache' found, with contents: Redirect from cloudfront

+ Uncommon header 'x-amz-cf-id' found, with contents: m-NgaTxmFAUrK04eU\_D3im6PqaLUbAgTayjLxMt0h4HNDuiYLjUX1Q==

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Root page / redirects to: https://compass.com/

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress

+ Scan terminated: 13 error(s) and 7 item(s) reported on remote host

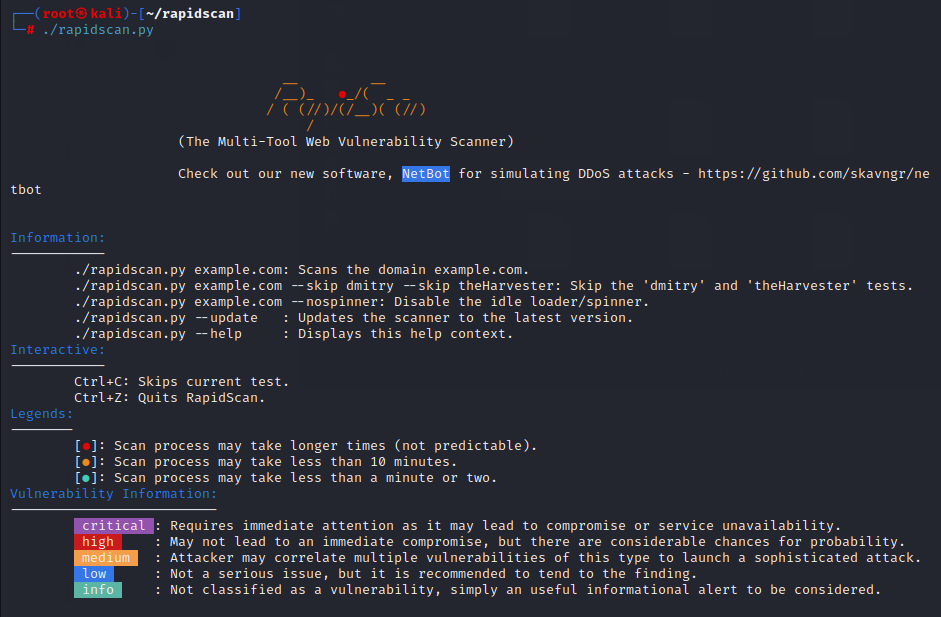
+ End Time: 2023-10-26 13:10:16 (GMT-4) (841 seconds)

---------------------------------------------------------------------------

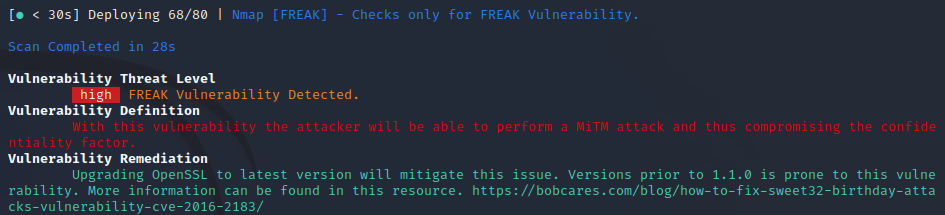
+ 1 host(s) tested

* Vulnerability title – X-XSS header not found
* Vulnerability description - This vulnerability pertains to the absence of the X-XSS-Protection header in the target web server's response. This absence makes older web browsers vulnerable to Reflected Cross-Site Scripting (XSS) attacks, which can allow malicious code to be executed within a user's browser context
* Proposed mitigation or fix - To mitigate this vulnerability, the web server should be configured to include the X-XSS-Protection header in its responses. This header can be set to enable the browser's built-in XSS protection mechanisms. Additionally, it's essential to keep web browsers updated to the latest versions with improved security features

## Vulnerabilities found using rapidscan

* Commands for the full rapidscan
* └─# ./rapidscan.py
* └─# ./rapidscan.py compass.com

1. Vulnerability title – freak vulnerability detected



* Vulnerability threat level
  + high
* Vulnerability description
  + Attacker will be able to perform a MiM attack and it could compromise the confidentiality
* Proposed mitigation or fix
  + Upgrading OpenSSL to latest version
* Affected components
  + mitigate this vulnerability, it is recommended to upgrade OpenSSL to the latest version, which should include fixes for the FREAK vulnerability. Additionally, ensure that affected systems no longer support export-grade cryptography, as this is often the root cause of vulnerability.

1. A screen shot of a computer program

   Description automatically generatedVulnerability title – vulnerable to slowloris denial of service

* Vulnerability threat level
  + Critical
* Vulnerability description
  + This attack works by opening multiple simultaneous connections to the web server and it keeps them alive as long as possible by continuously sending partial HTTP requests, which never get completed. They easily slip through IDS by sending partial requests.
* Affected components
  + affects web servers, could include a wide range if web server software’s
* Impact assessment
  + it can effectively deny legitimate users access to the targeted web server, disrupt services, and potentially lead to significant downtime.
* How an attack could be carried out
  + Establish multiple simultaneous connections to the target web server.
  + Keep these connections open by sending partial HTTP requests that are never completed.
  + Continuously maintain these connections to exhaust server resources.
* Proposed mitigation or fix –
  + Implementation of rate limiting to limit the number of concurrent connections from a single Ip address.
  + Implementing intrusion detection and prevention systems
  + Distribute traffic across multiple servers to reduce the impact of these type of attacks

1. A screenshot of a computer

   Description automatically generatedVulnerability title – RDP server detected over UDP.

* Vulnerability threat level
  + High
* Vulnerability description
  + Attacker may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password of the target.
* Impact assessment
  + The vulnerability has a high threat level, as it can lead to service disruptions or unauthorized access.
* Proposed mitigation or fix
  + It is recommended that to block the service outside world and make the service accessible only through the set of allowed IPs only necessary to prevent potential exploits.

1. A screen shot of a computer

   Description automatically generatedvulnerability title – open files found with uniscan

* vulnerability threat level
  + medium
* A screen shot of a computer

  Description automatically generatedvulnerability description
  + attackers may find considerable amount of information from those files there is even chance attacker may get access to critical information from these files
* Impact assessment
  + potential exposure of sensitive information.
* Proposed mitigation or fix
  + Implement proper access controls, review and secure sensitive files, and restrict access to unauthorized users.
  + Block or restrict access to these files unless necessary