A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report –**

**IT21831904 – K.M. Weerasinghe**

Table of Contents

[Scope of the target 3](#_Toc149248773)

[In scope and rewards 3](#_Toc149248774)

[Out of scope 3](#_Toc149248775)

[Reconnaissance 4](#_Toc149248776)

[Subdomain enumeration 4](#_Toc149248777)

[Gathering information about the target 5](#_Toc149248778)

[Virtual host discovery 6](#_Toc149248779)

[Subdomain takeover 7](#_Toc149248780)

[Scanning 8](#_Toc149248781)

[Using Nmap for scanning 8](#_Toc149248782)

[Using final recon for scanning 8](#_Toc149248783)

[Vulnerability checking 9](#_Toc149248784)

[Vulnerabilities found using NIKTO 9](#_Toc149248785)

[Vulnerabilities found using rapidscan 10](#_Toc149248786)

# Scope of the target

A screenshot of a computer

Description automatically generated

## In scope and rewards

A screenshot of a computer

Description automatically generated

## Out of scope

A screenshot of a computer

Description automatically generated

# Reconnaissance

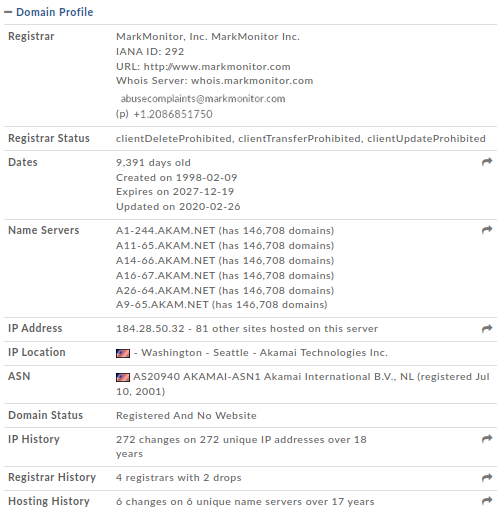
## Subdomain enumeration

* Using domained.py tools amass and subfinder to do the subdomain enumeration
* A screenshot of a computer

  Description automatically generatedA computer screen shot of a program

  Description automatically generated└─# python3 domained.py -d trip.com --quick –notify
* Total subdomains found using sublister is 250

## Gathering information about the target

* A screenshot of a computer screen

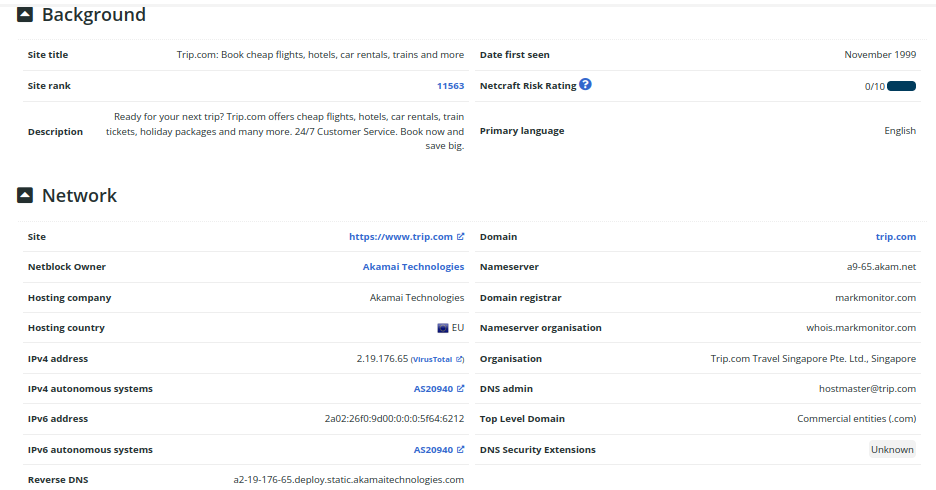
  Description automatically generatedwhois record

The email address of the administrator and other information (address, phone, etc) is available publicly. An attacker may use these information to leverage an attack. This may not be used to carry out a direct attack as this is not a vulnerability. However, an attacker makes use of these data to build information about the target.

* A screenshot of a report

  Description automatically generatedsecurity header check

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.
  +  netcraft scan to gather background, network, and certificate information

A screenshot of a computer

Description automatically generated

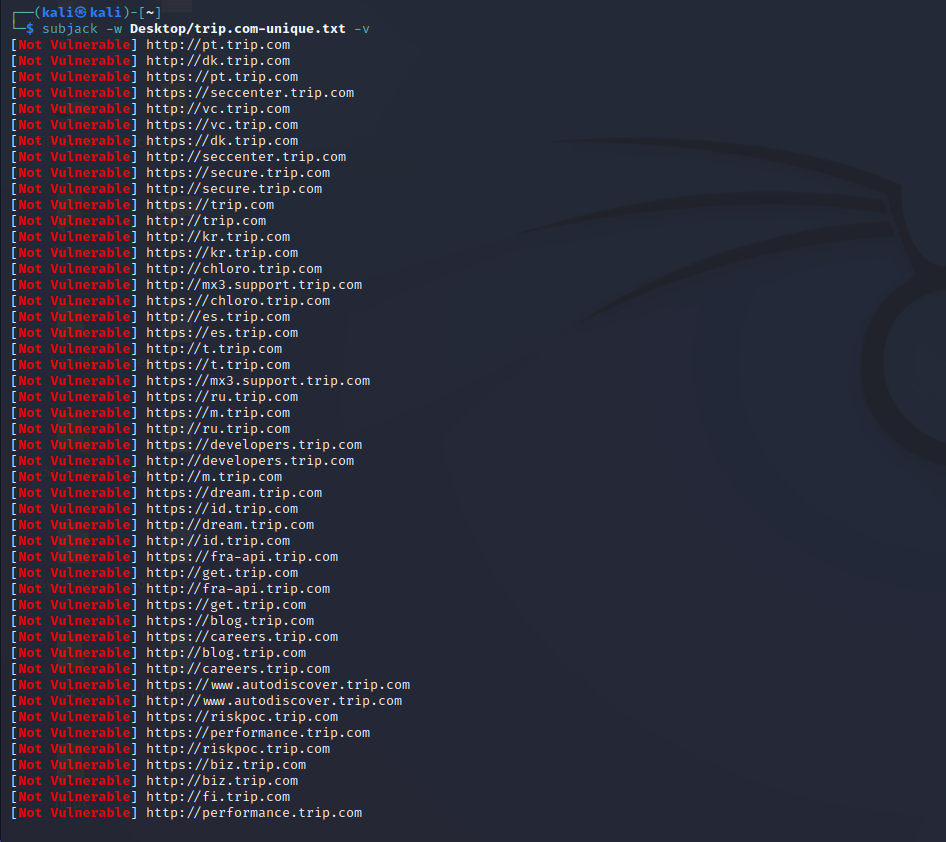
## Virtual host discovery

A screenshot of a computer

Description automatically generated

## Subdomain takeover

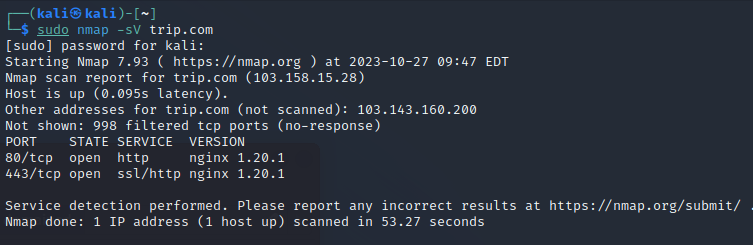
* None of the previously found 250 subdomains were vulnerable to takeover
* └─$ subjack -w Desktop/trip.com-unique.txt -v



# Scanning

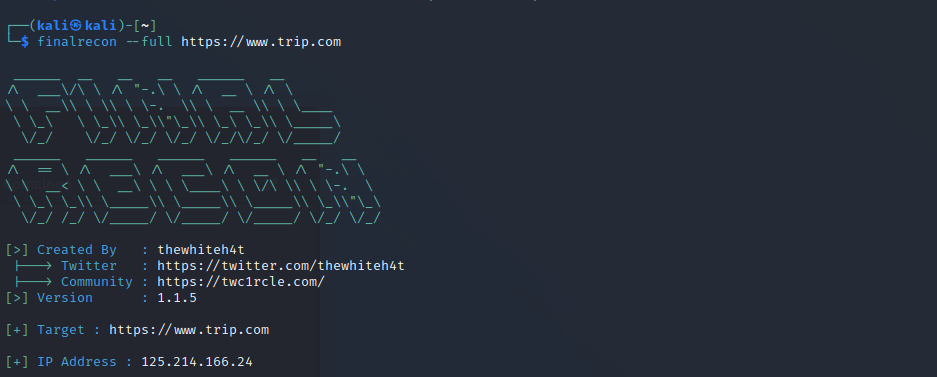
## Using Nmap for scanning

* └─$ sudo nmap -sV trip.com



## Using final recon for scanning

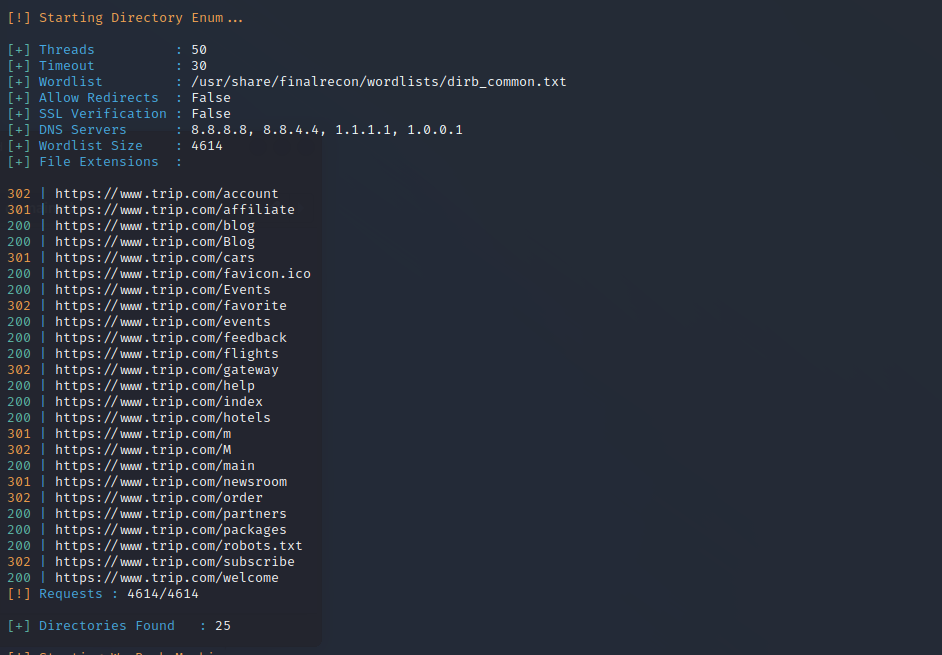
* └─$ finalrecon --full https://www.trip.com

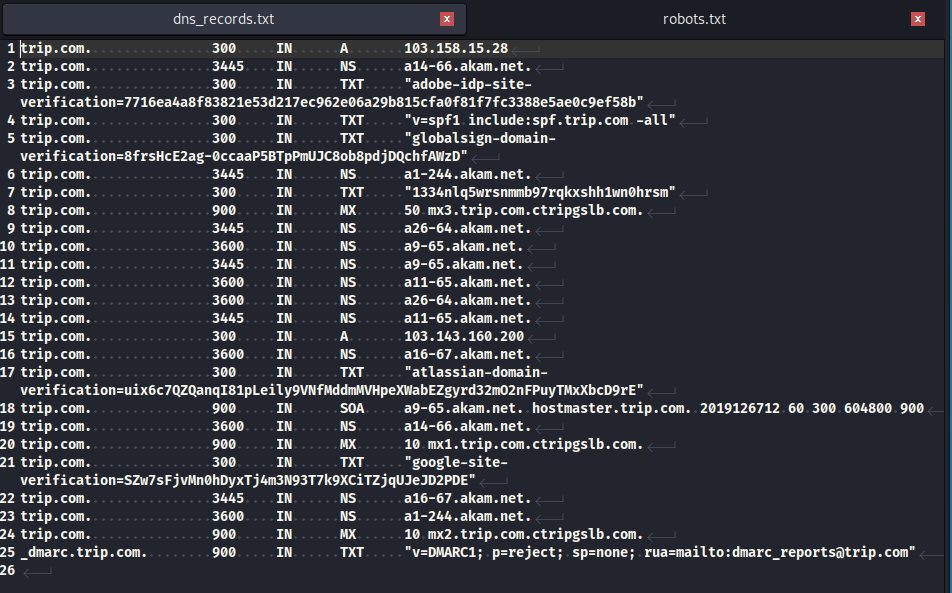


Information gathered using crawlers

A blue screen with red text

Description automatically generated

Directories enumeration

DNS records found

# Vulnerability checking

## Vulnerabilities found using NIKTO

└─$ nikto -h trip.com

- Nikto v2.1.6

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

+ Target IP: 103.143.160.200

+ Target Hostname: trip.com

+ Target Port: 80

+ Message: Multiple IP addresses found: 103.143.160.200, 103.158.15.28

+ Start Time: 2023-10-27 09:51:20 (GMT-4)

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

+ Server: No banner retrieved

+ 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

+ 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://www.trip.com/

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

+ Server banner has changed from '' to 'nginx/1.20.1' which may suggest a WAF, load balancer or proxy is in place

+ 7786 requests: 1 error(s) and 3 item(s) reported on remote host

+ End Time: 2023-10-27 10:23:11 (GMT-4) (1911 seconds)

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

+ 1 host(s) tested

## Alternative scan with tuning using nikto

└─$ nikto tuning 9 -h trip.com -p 80,443

- Nikto v2.1.6

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

+ Target IP: 103.158.15.28

+ Target Hostname: trip.com

+ Target Port: 80

+ Message: Multiple IP addresses found: 103.158.15.28, 103.143.160.200

+ Start Time: 2023-10-27 14:47:56 (GMT-4)

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

+ Server: No banner retrieved

+ 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

+ 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://www.trip.com/

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

+ Server banner has changed from '' to 'nginx/1.20.1' which may suggest a WAF, load balancer or proxy is in place

+ 7786 requests: 0 error(s) and 3 item(s) reported on remote host

+ End Time: 2023-10-27 15:08:51 (GMT-4) (1255 seconds)

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

+ Target IP: 103.158.15.28

+ Target Hostname: trip.com

+ Target Port: 443

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

+ SSL Info: Subject: /C=SG/ST=Singapore/L=Singapore/O=TRIP.COM TRAVEL SINGAPORE PTE. LTD./CN=\*.trip.com

Ciphers: TLS\_AES\_256\_GCM\_SHA384

Issuer: /C=BE/O=GlobalSign nv-sa/CN=GlobalSign RSA OV SSL CA 2018

+ Message: Multiple IP addresses found: 103.158.15.28, 103.143.160.200

+ Start Time: 2023-10-27 15:08:51 (GMT-4)

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

+ Server: No banner retrieved

+ 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

+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

+ The site uses SSL and Expect-CT header is not present.

+ 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://www.trip.com/

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

+ Server banner has changed from '' to 'nginx/1.20.1' which may suggest a WAF, load balancer or proxy is in place

+ Server is using a wildcard certificate: \*.trip.com

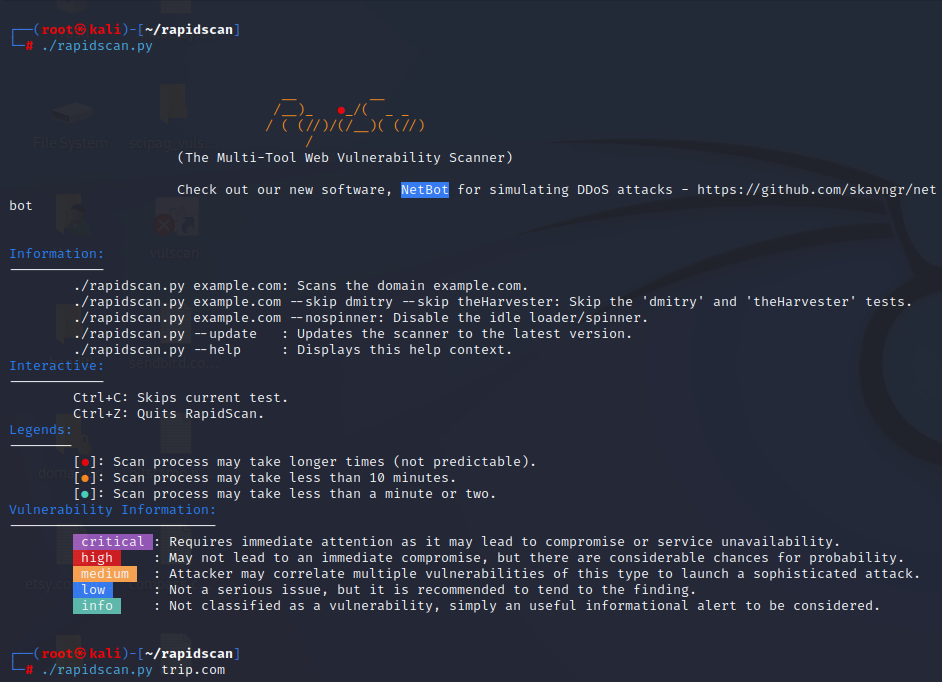
+ 15808 requests: 0 error(s) and 6 item(s) reported on remote host

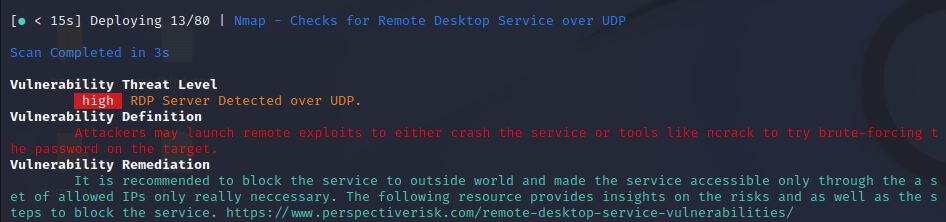
+ End Time: 2023-10-28 01:54:42 (GMT-4) (38751 seconds)

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

+ 2 host(s) tested

## Vulnerabilities found using rapidscan



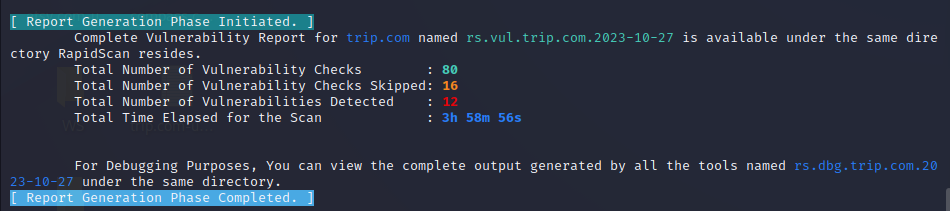
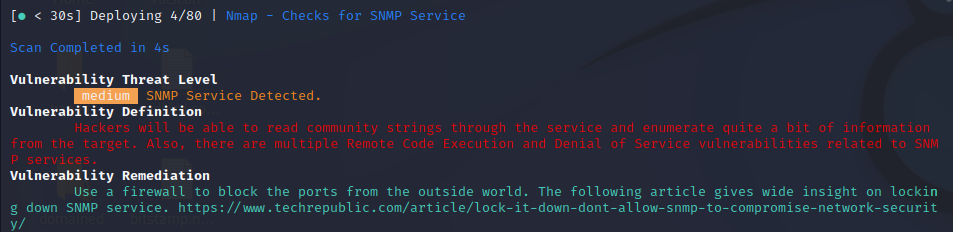
1. Vulnerability title – RDP server detected over UDP

* 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 - Secure client-initiated renegotiation vulnerability

* Vulnerability threat level
  + Medium
* Vulnerability description
  + This vulnerability, otherwise known as a Plain-Text Injection attack, allows Man-in-the-Middle (MiTM) attackers to insert data into HTTPS sessions, and potentially other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context.
* Affected components.
  + Secure client renegotiation that supports TLS or SSL protocols
* Proposed mitigation or fix
  + Disable Secure Client Initiated Renegotiation
  + Use strict certificate validation.

1.  Vulnerability title – SNMP service detected

* Vulnerability threat level
  + Medium
* Vulnerability description
  + Attackers will be able to read the community strings through the service and enumerate quite a bit of information from the target
  + Also there are multiple remote code execution and denial of service vulnerabilities related to SNMP services.
* Affected components
  + SNMP service
* Proposed mitigation or fix
  + Use a firewall to block the ports from the outside world