A blue and orange logo

Description automatically generated

**IE2062 – Web Security**

**Year 2, Semester 2**

**Scanning report – etsy.com**

**It21831904 – K.M. Weerasinghe**

Table of Contents

[Scope and Guidelines 3](#_Toc149219204)

[Reconnaissance 4](#_Toc149219205)

[Subdomain enumeration 4](#_Toc149219206)

[Gathering information about the target 5](#_Toc149219207)

[Virtual host discovery 7](#_Toc149219208)

[Subdomain takeover 8](#_Toc149219209)

[Scanning 9](#_Toc149219210)

[Using finalrecon for scanning 9](#_Toc149219211)

[using Nmap to scan for open ports. 9](#_Toc149219212)

[Vulnerability checking 10](#_Toc149219213)

[Vulnerability found using Nikto. 10](#_Toc149219214)

[Vulnerabilities found using rapidscan 11](#_Toc149219215)

# Scope and Guidelines

A screenshot of a computer

Description automatically generated

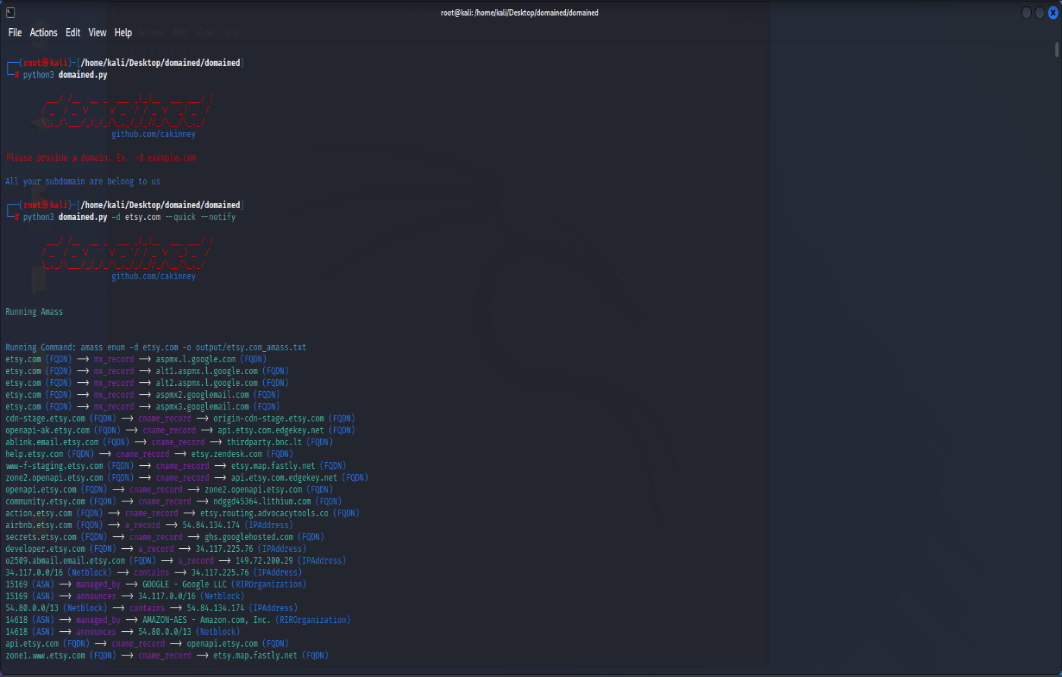
A screenshot of a computer

Description automatically generated

# Reconnaissance

## Subdomain enumeration

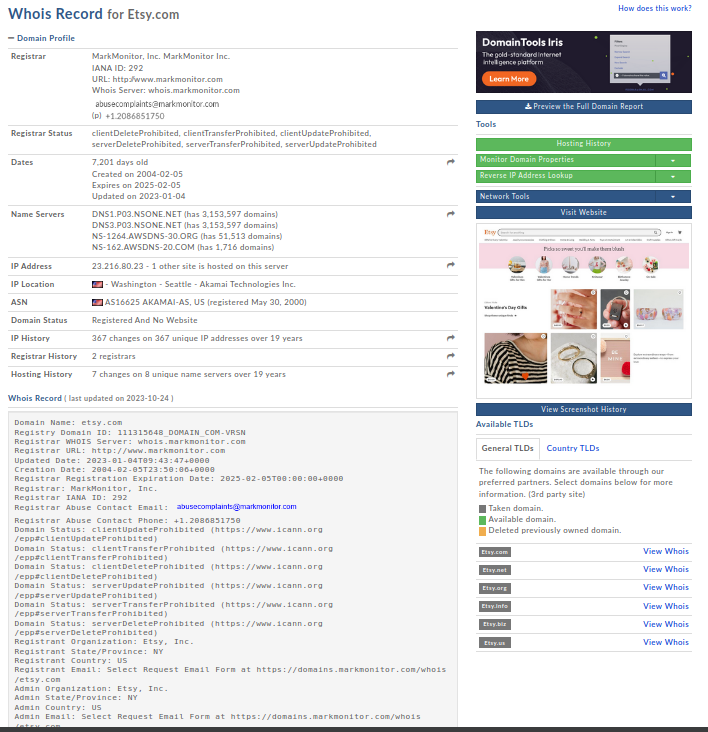
* Using amass and subfinder to do the subdomain enumeration using domained.py.
* ─# python3 domained.py -d etsy.com --quick --notify the output is saved in a txt folder

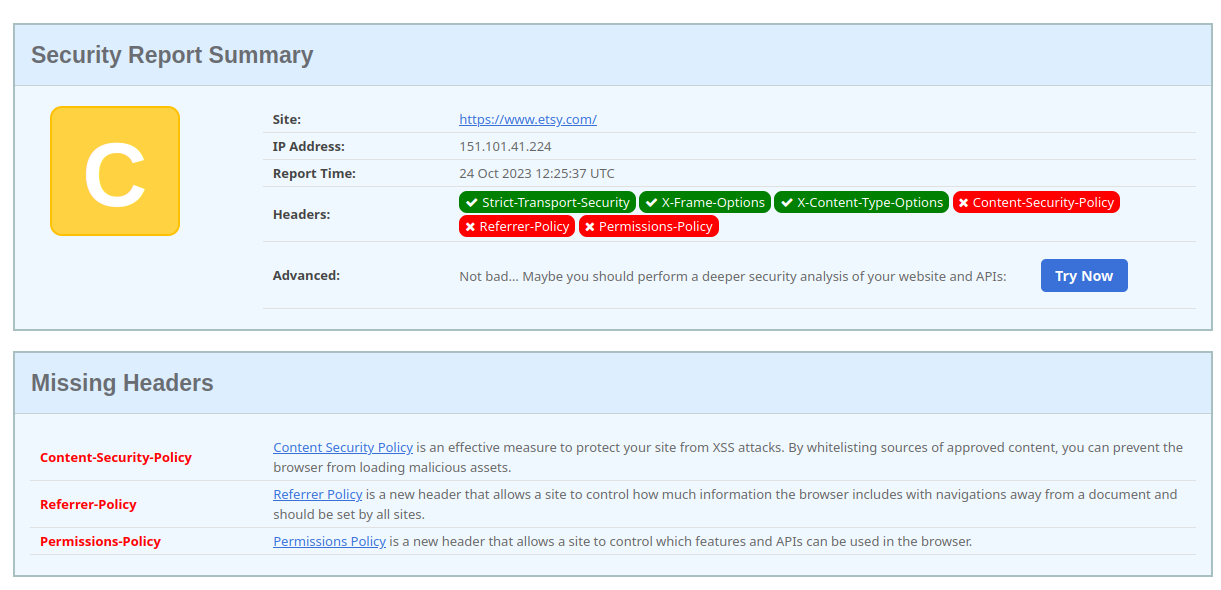


A screenshot of a computer

Description automatically generated

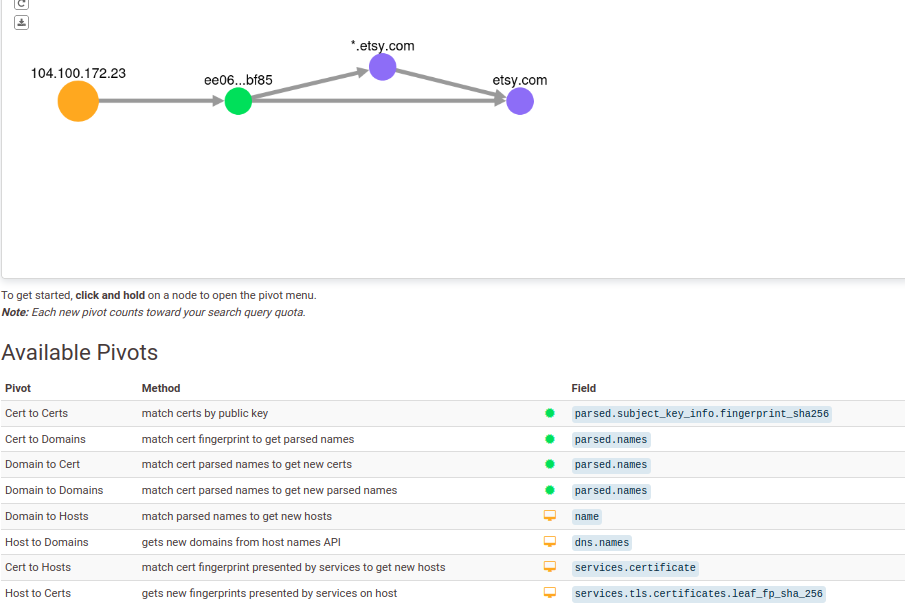
## Gathering information about the target

* ***Whois*** record for the etsy.com
* Using this website <https://whois.domaintools.com/etsy.com> finding information about the domain
* **A screenshot of a computer

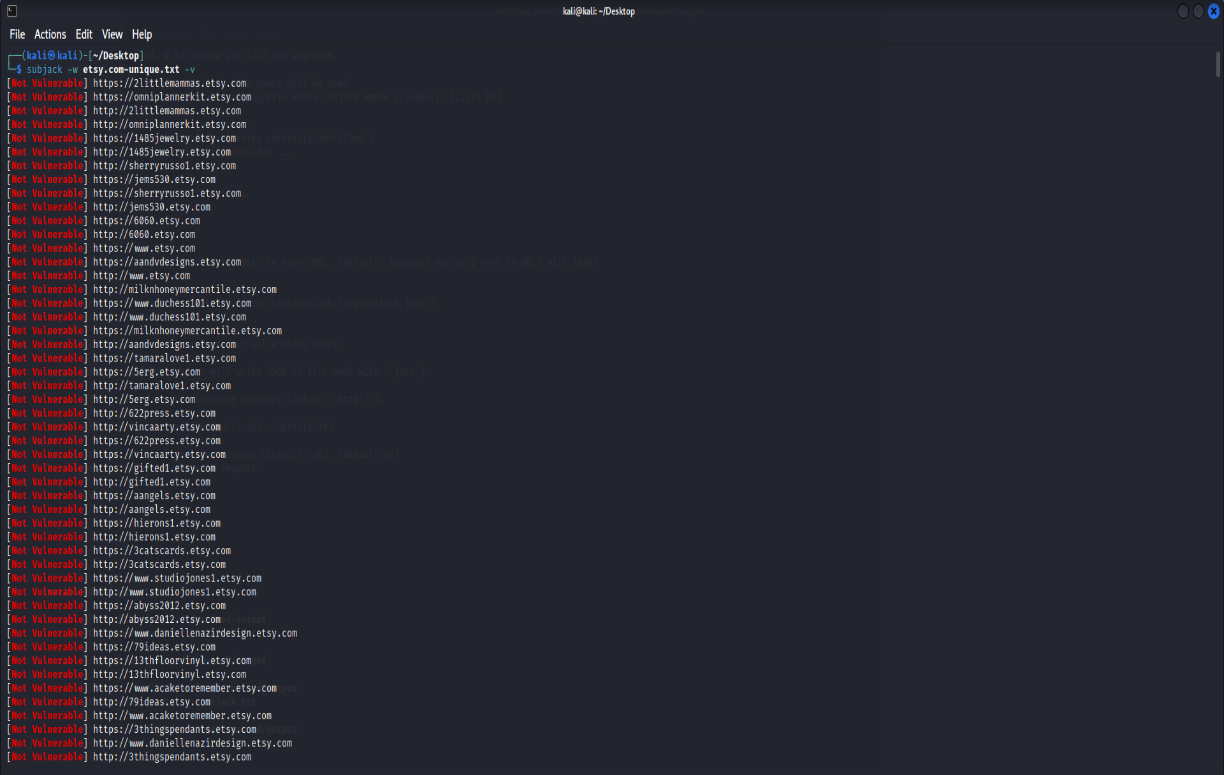
  Description automatically generatedNetcraft** scan to find more information about the website.
* checking for Security headers using **securityheaders.com**
* Missing header found,
  + Content - Security-Policy Content Security Policy is an effective measure to protect your site from XSS attacks. By 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

* A screenshot of a computer

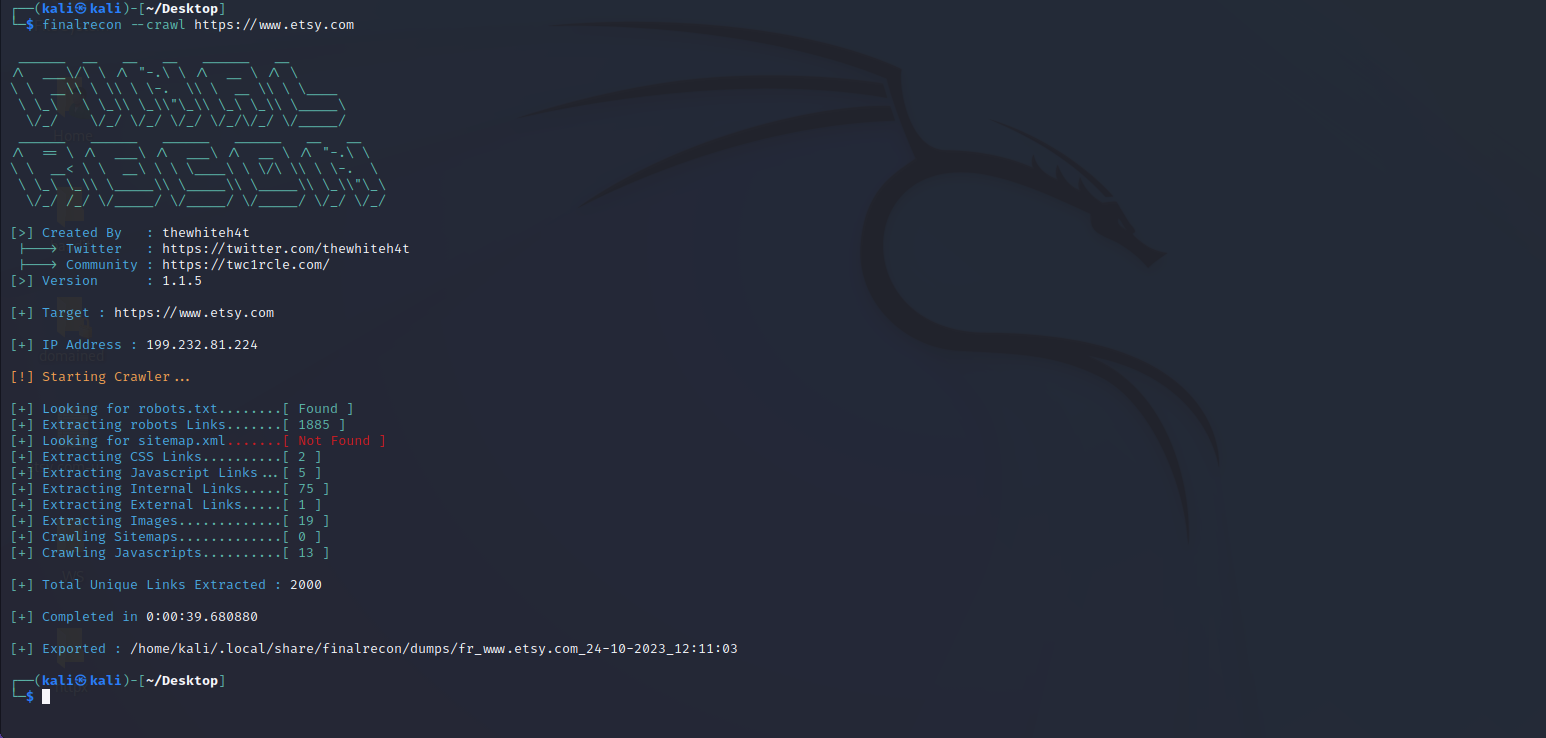
  Description automatically generatedUsing censys.com to find virtual hosts.
* SSL/TLS certificates were found to be appropriately configured without any evident weaknesses or misconfigurations.
* DNS records did not reveal any additional attack vectors or improperly configured subdomains.
* Sensitive data, such as databases, was not identified as publicly accessible through the Censys scan.

## Subdomain takeover

* Using the previously found subdomains checking if any of the subdomains are vulnerable using the subjack tool.
* └─$ subjack -w etsy.com-unique.txt -v
* Subjack scan for Etsy Bug Bounty: No vulnerable subdomains found.
* The subdomain scan yielded no security vulnerabilities.
* All subdomains appeared to be secure.
* No issues were identified in the subdomain analysis for the Etsy bug bounty program.

# Scanning

## Using finalrecon for scanning

* Using crawlers from finalrecon to check vulnerabilities.
* Robots.txt files found.
* robots.txt file is a standard in web development that instructs web crawlers and search engine bots which parts of a website should not be crawled or indexed.
* The robots.txt file may disclose directories or pages that the website owner intends to keep hidden, potentially revealing sensitive data or unsecured sections of the site.
* The information could be used for attacker’s advantage.
* The robotos.txt file doesn’t mean there is a vulnerability but it the information it has could be used for attacks.

## A close up of a screen Description automatically generatedusing Nmap to scan for open ports.

# Vulnerability checking

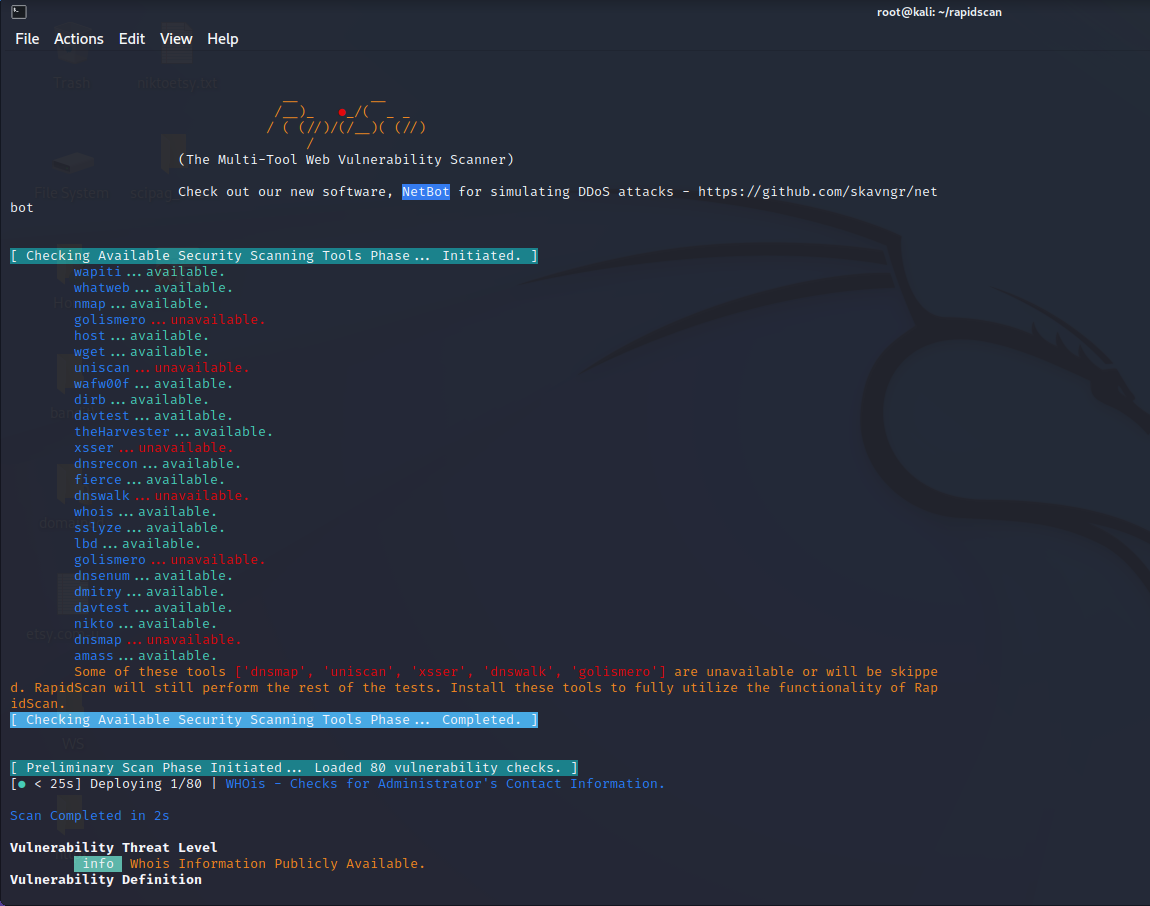
## Vulnerability found using Nikto.

* Some missing headers and uncommon headers found. Missing X-XSS headers.
  + vulnerability title
    - X-XSS protection is not present
  + Vulnerability threat level
    - medium
  + Vulnerability description
    - Older browsers might be prone to reflected XSS attacks
  + Proposed mitigation or fix
    - Upgrade the older browsers.

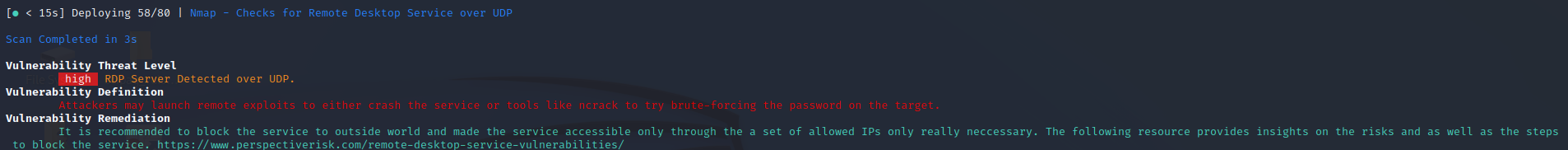
## Vulnerabilities found using rapidscan

* Using rapidscan a multi-tool vulnerability scanner to check for vulnerabilities.

1. A screen shot of a computer

   Description automatically generatedVulnerability Title - who is information publicly available.
   * Vulnerability threat level
     + info
   * Vulnerability description
     + 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.
   * Impact assessment
     + Depending on the usage of the public data that have been gathered and used the impact would be different.
   * Proposed mitigations or fix
     + Review the publicly available data and remove any information that doesn’t have to be public.
     + Adding access controls to prevent misuse of public information.
2. A screen shot of a computer error

   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.
3. 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.