Pentest report - 192.99.54.66

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **192.99.54.66** using Python modules. The objective of this assessment is to provide a brief overview of the security posture of the target and identify potential vulnerabilities that could be exploited by attackers.

The main objective of the assessment was to identify vulnerabilities that could be used by attackers to compromise the confidentiality, integrity, or availability of the target. Python modules are used to automate the scanning process and identify potential vulnerabilities in the target.

Date: 2024-05-06 12:30

Target : 192.99.54.66

Type: vulnerability scanner

II. DNS Request

Check your domain name or the API website (https://networkcalc.com/api/)

III. Data about HTTP/HTTPS certificate

Error. Check your domain name or the API website (https://networkcalc.com/api/)

IV. NMAP scan

Port	Service	Version
22	ssh	7.2p2 Ubuntu 4ubuntu2.10
80	http	2.4.18
2222	ssh	7.2p2 Ubuntu 4ubuntu2.10
8080	http-proxy	

V. Nikto scan

Web server : Apache/2.4.18 (Ubuntu)

The server supports compression.

Version of software might be found in the following header Server : 2.4.18

Target URL don't use any redirection

Target URL isn't protected by a basic HTTP authentication

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

The X-XSS-Protection header is not defined.

The X-Content-Type-Options header is not set.

VI. Potential vulnerabilities

Port : 22, Service: ssh, Version: 7.2p2 Ubuntu 4ubuntu2.10

- CVE-2012-1577
- CVE-2015-8325
- CVE-2016-6515
- CVE-2016-1000
- CVE-2016-1001
- CVE-2023-3578
- CVE-2016-8858

VII. Exploit find

Exploits found for CVE-2016-6515:

-- ---------------------------- Exploit Title | Path -- ---------------------------- OpenSSH 7.2 - Denial of Service | linux/dos/40888.py -- ---------------------------- Shellcodes: No Results

Exploits found for CVE-2016-1000:

-- ---------------------------- Exploit Title | Path -- ---------------------------- Adobe Flash - Sprite Creation Use-After-Fr | windows/dos/39610.txt Joomla! Component Huge-IT Portfolio Galler | php/webapps/42597.txt Joomla! Component Huge-IT Portfolio Galler | php/webapps/42598.txt Joomla! Component Huge-IT Video Gallery 1. | php/webapps/42596.txt OpenSSH < 7.4 - agent Protocol Arbitrary L | linux/remote/40963.txt -- ---------------------------- Shellcodes: No Results

Exploits found for CVE-2022-3181:

-- ---------------------------- Exploit Title | Path -- ---------------------------- pfBlockerNG 2.1.4_26 - Remote Code Executi | php/webapps/51032.py -- ---------------------------- Shellcodes: No Results

Exploits found for CVE-2021-4479:

-- ---------------------------- Exploit Title | Path -- ---------------------------- Apache 2.4.x - Buffer Overflow | multiple/webapps/51193.py -- ---------------------------- Shellcodes: No Results

Exploits found for CVE-2019-0211:

-- ---------------------------- Exploit Title | Path -- ---------------------------- Apache 2.4.17 < 2.4.38 - 'apache2ctl grace | linux/local/46676.php

```
----------------------------------------- ------------------------------ Shellcodes: No
Results
```

Exploits found for CVE-2016-1001:

```
----------------------------------------- ------------------------------ Exploit Title | Path
----------------------------------------- ------------------------------ Adobe Flash - Zlib
Codec Heap Overflow | windows/dos/39609.txt OpenSSH < 7.4 -
'UsePrivilegeSeparation Di | linux/local/40962.txt
----------------------------------------- ------------------------------ Shellcodes: No
Results
```

VIII. Recommendations

Keep your systems up-to-date with the latest security patches and updates for all software and services running on your domain or IP address. Vulnerabilities are often discovered and patched by vendors, so it's important to stay current with updates to minimize risk.

We also recommend reviewing the list of links provided in this report, which point to known exploits and vulnerabilities affecting various services. These links can provide additional information and guidance on how to mitigate these specific security risks for your domain or IP address.

By following these recommendations and staying vigilant against emerging security threats, you can help protect your systems and data from unauthorized access and exploitation.