DeceptiConf - Pentest report - 20.7.1.11

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **20.7.1.11** 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: 2024-05-03 11:21

Target : 20.7.1.11

Type: vulnerability scanner

II. DNS Request

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

III. Data about HTTP/HTTPS certificate

Metadata

protocol: https:
hostname: 20.7.1.11
port: 443

Certificate

protocol: https:
hostname: 20.7.1.11
port: 443
issued_to: TRAEFIK DEFAULT CERT
issued_by: TRAEFIK DEFAULT CERT
valid_from: 2024-05-03T11:15:27.000Z
valid_to: 2025-05-03T11:15:27.000Z
alternate_names: ['DNS:574fa308ae4c73c3c9cd91dbc62240ba.6f37a3b3667ac8bf2e70dbafc8198cd0.traefik.default']
serial_number: CC01AC71A26E82E4604681F3A6FBF29F

fingerprint: 92:AB:73:67:AF:D5:4E:43:DF:6E:CE:40:7B:74:37:EC:
21:82:9E:4C
raw:
-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIRAMwBrHGiboLkYEaB86b78p8wDQYJKoZIhvcNAQELBQA
HzEdMBsGA1UEAxMUVFJBRUZJSyBERUZBVUxUIENFUlQwHhcNMjQwNTAzMTI
WhcNMjUwNTAzMTExNTI3WjAfMR0wGwYDVQQDExRUUkFFRklIERFRkFVTFQ
VDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANeyUCd8sC4/
iKkwp2j1
NSNphxQw3Scw5gJJGKJJbu6UcTUiRKSTjfMwj9XONjnFrHZedw4ODgZXmRVTeB1
NTFOiLB9mFpF9HsqKNHfF5ZVFpuTK5GNWGMFPfCrq0WH5hPWPBzQsnazz1gW
HJVjFtstDkgdoFB+LPDOowB/ZtXE8KYEjmBJANcJ8MBy3N/
s3pBjaDh9GfqfLmK+
Hr06rKolpWxMc1NejXzOMRuVQYfLAND4FNyLqeml0Gw4X9vCP3vAUZKrlKL7GG
g/C/
t3ML0NiyZwAD4Iq9vCqUHkSMV6f4eKz4RMsCsS50UHrQt7V1p1NST4jyropR
VV8CAwEAAaOBlDCBkTAOBgNVHQ8BAf8EBAMCA7gwEwYDVR0lBAwwCgYIKwY
AwEwDAYDVR0TAQH/
BAIwADBcBgNVHREEVTBTglE1NzRmYTMwOGFlNGM3M2MzYzlj
ZDkxZGJjNjIyNDBiYS42ZjM3YTNiMzY2N2FjOGJmMmU3MGRiYWZjODE5OGNkM
cmFlZmlrLmRlZmF1bHQwDQYJKoZIhvcNAQELBQADggEBAKrOvIcL6GEsg4xaSq
zfB2X/yKTcteCxKbFjhUgYE9sazCkO/J8H/
BCb33QcGZkSnZVZo5jkuP5MbJ/hUX chTFOi/
t632BDq4Z4ufetQ4Au230TxRkcEQmD/
SRtO3r9PdW6fnhPuRyN8FHnD2W s1LMk4z6dLoFMa+xMn7Oiq5/
P8rzwnvtaIKttoNAVKG/jtsYLOTa8plTfVJPw4jx
PNNq9Js96kGoHIRdTA4H7QxWwr1e/
t08KyKwYBupJ98U+q+N1fxeVjSYE+nYEEQZ
spZHH49suhiu2G+b1k+si9eoUc/
z8KE+LAriEF+cNBNXRSKRmWryGtehcnFGBMdV 2kI= -----END
CERTIFICATE-----

IV. NMAP scan

[['20.7.1.11', 80, 'http', ''], ['20.7.1.11', 443, 'http', '']]

V. Nikto scan

The server doesn't support compression.

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.

VI. Potential vulnerabilities

CVE associated with http

Service: http, Version:

- CVE-2018-19790
- CVE-2023-34062
- CVE-2021-31618
- CVE-2023-45288
- CVE-2016-4423
- CVE-2021-3007
- CVE-2003-1307
- CVE-2024-2653
- CVE-2013-4407
- CVE-2015-2308
- CVE-2007-6420
- CVE-2023-44487

VII. Exploit find

Exploit find result goes here

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.