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 11:35

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: 2024-05-03T11:30:27.000Z
valid_to: 2025-05-03T11:30:27.000Z
alternate_names:
['DNS:a2a9dc71561127fb41bd78735b500384.d240589cab282d04584cc3d6ba9cfbe1
serial_number: FD443814F1C7EA98A9BFE231CF19286F
fingerprint: 5E:DA:23:F6:CE:E8:11:35:6C:AE:CE:94:37:5F:51:83:EB:19:2D:A9
raw:

```
-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIRAP1EOBTxx+qYqb/
iMc8ZKG8wDQYJKoZIhvcNAQELBQAw
HzEdMBsGA1UEAxMUVFJBRUZJSyBERUZBVUxUIENFUlQwHhcNMjQwNTAzMTEz
WhcNMjUwNTAzMTEzMDI3WjAfMR0wGwYDVQQDExRUUkFFRklLIERFRkFVTFQg
VDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM8y40ZaS2lDaytxPj4H
Hf15lPwcCDxlwiEmdwopPQ5j9N8RLOtraU7V2lLNgC/
149V8Y3WbT1n8eCtUGHKL 06SdQg/5cPrAbEwV4t4UH/
B2cXXdnbRfuBzTEMJRKVZo2+BKQdszdX9hu35uA8pc
MAekoWi3UvtvcaesQaJr47A1nY8ddrYIbBTMf/i2OvruQEb4I3/r1ak/
S6Vn6pz3
ZzLD4CBGbTMcX6JaoLic8QpoE1WlVm+JYP0lyi24f0VrFW+Cw/
5aq3TNIDZXLyYJ
LV9m1garDUyBOXdim50BGXPRwjXm9+wai7xVfjjw627Lw8y6ljaQUiiN5RtWEmHN
xm8CAwEAAaOBlDCBkTAOBgNVHQ8BAf8EBAMCA7gwEwYDVR0lBAwwCgYIKwYBE
AwEwDAYDVR0TAQH/
BAIwADBcBgNVHREEVTBTglFhMmE5ZGM3MTU2MTEyN2ZiNDFi
ZDc4NzM1YjUwMDM4NC5kMjQwNTg5Y2FiMjgyZDA0NTg0Y2MzZDZiYTljZmJlMS5
cmFlZmlrLmRlZmF1bHQwDQYJKoZIhvcNAQELBQADggEBACgVYzTU8ZteY6jmvb59
QDdEIraEtnAMd7+fcjiZGR7brR6dWdD0eOQ54t/
Kcs4LuGbV1edlwpCHbp7ONaln NymKiwM2jN89nNUB/
F9qGNeLbzM5zL8Bo42MrVMlWfScE19UFvQhWMlzqyhY8oCO w/
iDHazDFO0/
Kbt1EtvqjmDtPjJ0QX31jRYhH9m2IfXmPHiuKJ7Yopx5PoTMM2UE
6/38Pb/d7oEQVKkYq9FVP+WwJD/
c32FLK7pkLARgqFuY1Xbupo65BrCUww2qss6N
H41DcsMWN3SG6XJBWka/BC/A4yzebP1Ezhk1mVHovPCU/
WWbqLQiEggpZGJ4m1Iz i9I= -----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

Service: http, Version:

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

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.