Pentest report - 161.35.72.192

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **161.35.72.192** 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: 2024-05-08 21:49
Target : 161.35.72.192
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: 161.35.72.192
port: 443

Certificate

protocol: https:
hostname: 161.35.72.192
port: 443
issued_to: derridas-test.webrecorder.net
issued_by: R3
valid_from: 2024-01-31T14:32:52.000Z
valid_to: 2024-04-30T14:32:51.000Z
alternate_names: ['DNS:derridas-test.webrecorder.net', 'DNS:dev.webrecorder.net', 'DNS:kiwix-dev.webrecorder.net']
serial_number: 043C48154EC0B19B46D6A21C3C243AF2D6D6
fingerprint: EE:B2:42:3F:DE:1D:D9:66:A4:FF:CD:6A:F0:F9:E5:2F:67:23:3A:F0
raw:

-----BEGIN CERTIFICATE-----
MIIFODCCBCCgAwIBAgISBDxIFU7AsZtG1qIcPCQ68tbWMA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yNDAxMzExNDMyNTJaFw0yNDA0MzAxNDMyNTFaMCgxJjAkBgNVBAMT

```
HWRlcnJpZGFzLXRlc3Qud2VicmVjb3JkZXIubmV0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA0GgQ5/Z3zPeNaGtRA0I7wx72baOOglRLVP58qmX/
JfBw
nnqDCGyqdFglVGRdaqnmnVKGNkb9c9+uk2v6BXpfUp2YYXmzyXtb9FraLNqU89/
w 0V9e4CYTGDPv6oljM/iYhXRA3oBf/
+AZFZ4KS0oALADrFkp91vn9Mlpz6DRBkWG1
5ID2izTzjbuD91fo8K86PQrT0pYF/wA/MeGvmXYXEPMn0A0DkCeUqr/
yVIzsr3bI MBv3bcYcRgskT4ohkIgMBijC8BA3x/f/+SjCAnZmojmBtM3ugPH7b/
hILlFk3UWS
LHb0L1YGOkeZyaoRL7ZXcIlj62qet7FDirzo7og92wIDAQABo4ICUDCCAkwwDgYD
VR0PAQH/
BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBgNV
HRMBAf8EAjAAMB0GA1UdDgQWBBR9i9BnjzX3wFPT9VK72mX74dnpHjAfBgNVHSME
GDAWgBQULrMXt1hWy65QCUDmH6+dixTCxjBVBggrBgEFBQcBAQRJMEcwIQYIKwYB
BQUHMAGGFWh0dHA6Ly9yMy5vLmxlbmNyLm9yZzAiBggrBgEFBQcwAoYWaHR0cDov
L3IzLmkubGVuY3Iub3JnLzBYBgNVHREEUTBPgh1kZXJyaWRhcy10ZXN0LndlYnJl
Y29yZGVyLm5ldIITZGV2LndlYnJlY29yZGVyLm5ldIIZa2l3aXgtZGV2LndlYnJl
Y29yZGVyLm5ldDATBgNVHSAEDDAKMAgGBmeBDAECATCCAQUGCisGAQQB1nkCBAIE
gfYEgfMA8QB3ADtTd3U+LbmAToswWwb+QDtn2E/D9Me9AA0tcm/
h+tQXAAABjWAm
zsAAAAQDAEgwRgIhALUYJh5RtmUf96bfj3AJjgSs8nActqUOaJNZ+ZeX99jlAiEA
z+lZo0qi4TenrexsX0Ik4NZFC+wN4b9/LkWMEDJVkOIAdgB2/4g/
Crb7lVHCYcz1
h7o0tKTNuyncaEIKn+ZnTFo6dAAAAY1gJs+IAAAEAwBHMEUCIGZCJ6+agvpv2dPi
OSTvUne4KxZhrd4u9WCTFKHt7bbYAiEA8OPGDTcnnlUgmT/
PZN5JglJ+1Z8bGjNc
hMh9S+cfMKkwDQYJKoZIhvcNAQELBQADggEBAAj6VOZIHXalYE8O44NLoDBVy7Tg
8/
fETpQW7u6YqRzLf+xnULc67Wi0TdTl1g8RY8QbxJCZKM9fr8yFejLPm62VvqTC
q0a2EEUamRjR77xSDrO9+xiz02iBSCESG/
Nzi7FTozTGL6DMK7lgAymdS7lY1F1y
MQmQ6o8wjGU3P5SJu3bCezPKKYP8z+91J4dh8McqyYe+uwHUEotrCeq8gUD1o8Rr
WGaAC7l6cMS5sbsupZH9Va4WcXabNw2GqC03mvHcdghNkUmx2G9zvUJOxfM3mK1Z
sFXTbG0lJgu9/nEH83KKqr7wqWciYTNUyE4p3Kn4rgI7xXT0dxZX42BkWcU=
-----END CERTIFICATE-----
```

IV. NMAP scan

Port	Service	Version
22	ssh	7.6p1 Ubuntu 4ubuntu0.7
80	http	1.14.0
443	http	1.14.0

V. Nikto scan

Web server : nginx/1.14.0 (Ubuntu)
The server doesn't support compression.
Version of software might be found in the following header Server : 1.14.0
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

CVE ID	Description	Score
CVE-2012-1577	lib/libc/stdlib/random.c in OpenBSD returns 0 when seeded with 0.	9.8
CVE-2018-1684	IBM WebSphere MQ 8.0 through 9.1 is vulnerable to a error with MQTT topic string publishing that can cause a denial of service attack. IBM X-Force ID: 145456.	6.5
CVE-2018-1684	IBM WebSphere MQ 8.0 through 9.1 is vulnerable to a error with MQTT topic string publishing that can cause a denial of service attack. IBM X-Force ID: 145456.	6.5

VII. Exploit find

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.