Information Technologies Security

Assignment

Looking for vulnerabilities in large networks

Author: Adam Žilla

ID: 92177

Contents

[Assignment clarification 3](#_Toc54189381)

[CVE-2020-11969 3](#_Toc54189382)

[CWE-287 3](#_Toc54189383)

[Nmap 3](#_Toc54189384)

[NSE 3](#_Toc54189385)

[Python 3](#_Toc54189386)

[Shodan 3](#_Toc54189387)

[Detection 3](#_Toc54189388)

[Code snippets 3](#_Toc54189389)

[Bibliography 5](#_Toc54189390)

# Assignment clarification

The specific task in my assignment is to look for and choose some recent CVE. Next part is to implement a simple Python script with use of NSE scripting language or some more advanced scanner like Shodan or so, in edge case I can use Metasploit framework, for detecting vulnerable devices in specified IP range.

# CVE-2020-11969

I have been looking for vulnerability I can detect via network. I chose CVE-2020-11969. Short description of this vulnerability is the following. If Apache TomEE is configured to use the embedded ActiveMQ broker, and the broker URI includes the useJMX=true parameter, a JMX port is opened on TCP port 1099, which does not include authentication. This affects Apache TomEE 8.0.0-M1 - 8.0.1, Apache TomEE 7.1.0 - 7.1.2, Apache TomEE 7.0.0-M1 - 7.0.7, Apache TomEE 1.0.0 - 1.7.5. (1)

# CWE-287

As stated in mitre Common Weakness Enumeration database, above mentioned CVE is type of Improper Authentication. IT means that an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct. (2)

# Nmap

## NSE

# Python

# Shodan

# Detection

# Code snippets

# Bibliography

1. **NIST. [Online] https://nvd.nist.gov/vuln/detail/CVE-2020-11969#vulnCurrentDescriptionTitle.**

**2. Mitre. *cve.* [Online] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11969.**