

# Pentesting

---

ITAPP

## Table of content

<b>1. Methodological reporting.....</b>	<b>2</b>
<b>1.1 State of the art.....</b>	<b>4</b>
<b>1.2 Selecting the methodology.....</b>	<b>5</b>
<b>2. Technical report.....</b>	<b>6</b>
<b>2.1 Planning and preparing .....</b>	<b>6</b>
2.1.1 The engagement teams .....	6
2.1.1 Exact dates and times .....	6
2.1.3 Analysis process .....	7
<b>2.2 Assessment .....</b>	<b>7</b>
2.2.1 Information gathering.....	7
<b>3. Conclusions .....</b>	<b>15</b>
<b>4. Bibliography .....</b>	<b>16</b>

## Table of content

Table 1. All machines for the analysis the analysis .....	6
Table 2. All discovered ports in Node1 .....	8
Table 3. All discovered ports in Gateway .....	9
Table 4. All discovered ports in Input.....	10
Table 5. All discovered ports in Prod & Staging.....	11

## Table of illustrations

Illustration 1. Part1 Nmap Scan to Node1 .....	8
Illustration 2. Part2 Nmap Scan to Node1 .....	9
Illustration 3. Part1 Nmap Scan to Gateway.....	10
Illustration 4. Part1 Nmap Scan to Node1 .....	11
Illustration 5. Part1 Nmap Scan to Staging & Prod .....	12
Illustration 6. Part2 Nmap Scan to Staging & Prod .....	12
Illustration 7. Part3 Nmap Scan to Staging & Prod .....	12
Illustration 8. Part4 Nmap Scan to Staging & Prod .....	12
Illustration 9. Django App .....	13
Illustration 10. Django Discovery .....	13
Illustration 11. Vulnerability detection.....	14

## 1. Methodological reporting

In this section of the different methodologies offered today and will proceed to select one.

### 1.1 State of the art

There are many proposed methodologies that describe how a security report should be written and how to perform a security audit. This section will describe four proposed methodologies and will select one that will be used to perform the audits.

- **OSSTMM:** Open source security testing methodology manual. This methodology analyses, from many points of view, how an audit must be performed as well as defining the sections that should be included on a report. Some of the sections that the report should include are the following: Information security, process security, internet technologies security, communications security, wireless security and physical security.
- **ISSAF:** Information systems security assessment framework. The ISSAF methodology is no longer maintained and might be outdated but describe in three steps how the audit must be done. It also describes witch tools to use for specific penetration testing steps. The three steps are:
  - **Planning and preparing:** This step consists on describing the phases needed to obtain some basic initial information and establishes which test to perform.
  - **Assessment:** This step describes which penetration testing tools to use to penetrate the target. It also includes an analysis of different important aspects of an audit such as a network analysis, the host analysis and so on.
  - **Reporting and cleaning:** This last step covers how the communication outputs should be used to share the results of the audit. The most common channel is through a written report. It also describes how to remove the artifacts created to penetrate the system.
- **OWASP:** Open web application security project. This is not a methodology. It is even bigger than that. OWASP is a project that focuses on identifying web security vulnerabilities. Their most famous guide is called “OWASP top 10” that describes those vulnerabilities.
- **PTES:** Penetration testing execution standard. This standard consists of seven sections covering everything related to pentesting. It covers the information

gathering, also defines the threats models as well as analyzing the vulnerabilities and exploits. Also, it allows to fine grain detailed methodology. In other words, if the report needs to be very precise and detailed, this methodology has the possibility to expand some aspects and vice versa.

## 1.2 Selecting the methodology

The methodology that will be used on this report focuses on the ISSAF. This decision has been taken because it sums up in short but concise steps or phases how the audit must be performed as well as proposing pen test tools. This methodology will be mixed with a pure pentesting report to have a better crafted report.

As described earlier, this methodology is divided into three main sections. The first one will be used to establish the objective of the report, as well as describing some of the provided information. The second section will describe how the security audit and pentest has been done detailing specific steps and results. The last step will conclude the audit briefly describing the main security vulnerabilities of each machine as well as proposing some security improvements to harden each host.

The final formal report might not include all the sections described by ISSAF as it might not be possible to obtain some information due to the nature of the scenario we are trying to emulate.

## 2. Technical report

This section will cover all aspects of planning and report preparation.

### 2.1 Planning and preparing

First, it is advisable to define the teams you will be working on.

#### 2.1.1 The engagement teams

The audit team had a meeting with ITAPP as they have requested our services to audit some of their computers located on a specific network. They asked to report back a detailed formal report to know the vulnerabilities of each host.

The project consists of a series of virtual machines which are hosted on different clouds (AWS & GCloud):

Machine name	DNS Address	IP Address
Node1	node1.itapp.eus	107.20.134.105
Node2	node2.itapp.eus	184.73.123.0
Node3	node3.itapp.eus	23.23.100.62
Gateway	gateway.itapp.eus	18.205.222.127
Input	input.itapp.eus	34.234.191.180
Staging	staging.itapp.eus	34.120.32.18
Production	prod.itapp.eus	34.120.57.230

Table 1. All machines for the analysis the analysis

If any complication arises during the evaluation process, the audit team will contact Enaitz Ezpeleta, the responsible of the audited company either by email or in person.

#### 2.1.1 Exact dates and times

The audit starts the 1st of June until the 6th of the same month. During that time, the machines will be running to carry out our security audit. The formal report is expected to be delivered to the client the 8th of June.

### 2.1.3 Analysis process

The security audit team has defined to test each host with the following methodology to pentest each machine and try to discover which vulnerabilities are located on those machines.

Normally in this type of analysis a pre-process steps should be followed in order to discovery IP addresses, Networks, etc. However, as we are testing our own machines this step has been omitted and directly perform the vulnerability scan with the OpenVas tool.

- **OpenVas** is a full-featured vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
- **OpenVas Alternatives:** Some alternatives to Openvas have been considered, such as Nessus, Qualys or Burp Suit, but due to the experience with it in some subjects, his user-friendliness and the limited time available, it has not been possible to use an alternative.

As will be explained in the following sections, the use of Nmap has been required as an extra tool in order to discover extra information about the analyzed machines.

## 2.2 Assessment

This section will consist of a collection of information, identification of possible vulnerabilities.

Openvas has a huge amount of possibilities and options in order to discover vulnerabilities in your machines, providing a different point of view allowing you to analyze whether your deployed applications have optimal security.

### 2.2.1 Information gathering

Let's start with the analysis of our different machines, discovering the vulnerable ports they have, the version of the service hosted on each of them and finally which vulnerabilities have been discovered and how to fix them.



### 2.2.1.1. Node 1

The Node 1 machine is dedicated to the collection and transmission of data, so it only has installed the NiFi software and those necessary for the transmission of data such as ElasticSearch and Hadoop.

The opened ports that have been discovered with Openvas are the following:

PORT	SOFTWARE
8080	NiFi UI
9200	ElasticSearch (REST)
9300	ElasticSearch (Node Communication)
9870	WebUI-Hadoop
9000	HADOOP
7077	Spark Standalone Master (RPC)
8580	Spark Standalone Master (Web UI)

Table 2. All discovered ports in Node1

As we can see there some opened ports that correspond to the previously mentioned software. With OpenVas was really impossible to discover more information about the version of any of the services running on that ports.

For that reason, an extra tool has been used in order to gain more info about our machines as an external auditories, Nmap.

A complete scan has been done with the following command:

```
$ nmap -T4 -A -v -O -sV 34.234.191.180
```

```

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 65:7c:a1:52:a2:e6:95:02:cb:8b:0a:71:34:7e:d7:82 (ECDSA)
|_  256 bb:18:87:34:19:fd:61:89:c7:50:62:ba:b7:f8:24:49 (ED25519)
25/tcp    filtered smtp
110/tcp   filtered pop3
1026/tcp  open  LSA-or-nterm?
1580/tcp  filtered tn-tl-r1
2200/tcp  filtered ici
7443/tcp  filtered oracleas-https
8080/tcp  open  http         Jetty 9.4.11.v20180605
|_ http-favicon: Unknown favicon MD5: C35857838974EAADE88EB7AF897E1F26
|_ http-methods:
|_   Supported Methods: GET HEAD POST
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-server-header: Jetty(9.4.11.v20180605)
|_ http-title: NiFi
8443/tcp  open  ssl/https-alt
    
```

Illustration 1. Part1 Nmap Scan to Node1

```

9000/tcp open  hadoop-ipc      Hadoop IPC
fingerprint-strings:
  GetRequest:
    HTTP/1.1 404 Not Found
    Content-type: text/plain
    looks like you are making an HTTP request to a Hadoop IPC port. This is not the correct port for the web interface on this d
aemon.
9090/tcp open  tcpwrapped
9200/tcp open  http             Elasticsearch REST API 7.6.2 (name: node1; cluster: es-cluster; Lucene 8.4.0)
  _http-favicon: Unknown favicon MD5: 61778FB75B498E0BB356223ED76FFE43
  _http-methods:
    Supported Methods: DELETE GET HEAD OPTIONS
    Potentially risky methods: DELETE
  _http-title: Site doesn't have a title (application/json; charset=UTF-8).
    
```

*Illustration 2. Part2 Nmap Scan to Node1*

As you can see the concrete version of the software was not achieved through the analysis (that's because they are well secured), so we recommend reading the following articles with the most common vulnerabilities of the installed software:

- [Nifi](#)
- [Hadoop](#)
- [ElasticSearch](#)

In addition to contemplating these vulnerabilities, it is advisable to keep the software always updated to the latest version in order to cover possible security gaps that may arise.

#### 2.2.1.2. Node 2&3

As in the case of nodes 2 and 3 they contain the same versions of the software of node 1 (together they form a cluster) we see unnecessary to make an exhaustive analysis of these machines since the results will be the same.

#### 2.2.1.3. Gateway

The Gateway machine is dedicated to the transmission of data, as a intermediary between the Input Machine and the Cloud, so it only has installed the NiFi software.

PORT	SOFTWARE
8080	NiFi UI

*Table 3. All discovered ports in Gateway*

OpenVas was really impossible to discover more information about the version of any of the services running on that ports.

For that reason, an extra tool has been used in order to gain more info about our machines as an external audit, Nmap.

A complete scan has been done with the following command:

```
nmap -T4 -A -v -O -sV 34.234.191.180
```

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 59:87:8c:2e:45:3f:b7:b9:97:e5:f9:e8:78:93:2f:a0 (RSA)
  256 a8:d8:a2:ec:27:f0:3a:55:f1:66:f8:6b:09:de:8a:6e (ECDSA)
  256 3a:6e:a4:18:01:7e:c8:53:37:cb:45:7c:e4:23:6b:df (ED25519)
8080/tcp  open  http      Jetty 9.4.11.v20180605
_http-favicon: Unknown favicon MD5: C35857838974EAADE88EB7AF897E1F26
_http-methods:
  Supported Methods: GET HEAD POST
_http-open-proxy: Proxy might be redirecting requests
_http-server-header: Jetty(9.4.11.v20180605)
_http-title: NiFi
Device type: bridge|general purpose|router
Running (JUST GUESSING): Oracle Virtualbox (94%), QEMU (91%), Cisco IOS 12.X (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:cisco:5300_router cpe:/o:cisco:ios:12.1
Aggressive OS guesses: Oracle Virtualbox (94%), QEMU user mode network gateway (91%), Cisco 5300 router (IOS 12.1) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=30 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

*Illustration 3. Part1 Nmap Scan to Gateway.*

As we have said on the previous machine, its recommendable to take a look on the common vulnerabilities of the software and to try to have the software updated.

#### 2.2.1.4. Input

The Input machine is dedicated to capture the data and transmit it to the gateway machine, so it only has installed the NiFi software.

PORT	SOFTWARE
8080	NiFi UI

*Table 4. All discovered ports in Input*

OpenVas was really impossible to discover more information about the version of any of the services running on that ports.

For that reason, an extra tool has been used in order to gain more info about our machines as an external audit, Nmap.

A complete scan has been done with the following command:

```
nmap -T4 -A -v -O -sV 34.234.191.180
```

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 7a:c4:b0:a2:88:61:2e:e7:69:cd:aa:37:8b:bb:84:a8 (RSA)
  256 1d:0a:f1:4d:d6:66:33:53:30:2c:ba:c9:14:f0:0c:2f (ECDSA)
  256 5b:b1:94:30:34:40:56:49:e1:21:cc:d6:88:e0:01:d4 (ED25519)
8080/tcp  open  http      Jetty 9.4.11.v20180605
_http-favicon: Unknown favicon MD5: C35857838974EAADE88EB7AF897E1F26
_http-methods:
  Supported Methods: GET HEAD
_http-open-proxy: Proxy might be redirecting requests
_http-server-header: Jetty(9.4.11.v20180605)
_http-title: NiFi
Device type: general purpose|bridge
Running (JUST GUESSING): QEMU (97%), Oracle Virtualbox (95%)
OS CPE: cpe:/a:qemu:qemu cpe:/o:oracle:virtualbox
Aggressive OS guesses: QEMU user mode network gateway (97%), Oracle Virtualbox (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=30 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
    
```

Illustration 4. Part1 Nmap Scan to Node1

As we have said on the previous machine, its recommendable to take a look on the common vulnerabilities of the software and to try to have the software updated.

### 2.2.1.1. Staging & Production

These two machines will be analyzed together since both have the same characteristics.

In the case of staging, it is the machine on which a pre-production version is deployed in order to check if there are any last bugs before putting it in front of the public.

In the case of the production machine, it is the machine that faces the public.

Therefore, both of them contain different software necessary for the correct functioning, such as the web server.

The open ports are the following:

PORT	SOFTWARE
443	Web Server Django

Table 5. All discovered ports in Prod & Staging

OpenVas was really impossible to discover more information about the version of any of the services running on that ports.

For that reason, an extra tool has been used in order to gain more info about our machines as an external audit, Nmap.

A complete scan has been done with the following command:

```
nmap -T4 -A -v -O -sV 34.234.191.180
```

```

PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
43/tcp    open  tcpwrapped
80/tcp    open  http
|_fingerprint-strings:
|_DNSVersionBindReqTCP:
|_HTTP/1.0 400 Bad Request
|_Content-Length: 54
|_Content-Type: text/html; charset=UTF-8
|_Date: Thu, 04 Jun 2020 11:02:27 GMT
|_<html><title>Error 400 (Bad Request)!!1</title></html>
|_FourOhFourRequest:
|_HTTP/1.0 404 Not Found
|_Date: Thu, 04 Jun 2020 11:02:18 GMT
|_Content-Length: 21
|_Content-Type: text/plain; charset=utf-8
|_Via: 1.1 google
|_Alt-Svc: clear
|_default backend - 404
|_GetRequest:
|_HTTP/1.0 404 Not Found
|_Content-Type: text/html; charset=UTF-8
|_Referrer-Policy: no-referrer
|_Content-Length: 1561
|_Date: Thu, 04 Jun 2020 11:02:09 GMT

```

Illustration 5. Part1 Nmap Scan to Staging & Prod

```

m/images/branding/googlelogo/1x
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
110/tcp   open  tcpwrapped
143/tcp   open  tcpwrapped
443/tcp   open  ssl/https
|_fingerprint-strings:
|_FourOhFourRequest:
|_HTTP/1.0 404 Not Found
|_Date: Thu, 04 Jun 2020 11:02:18 GMT
|_Content-Length: 21
|_Content-Type: text/plain; charset=utf-8
|_Via: 1.1 google
|_Alt-Svc: clear
|_default backend - 404
|_GetRequest:
|_HTTP/1.0 404 Not Found
|_Content-Type: text/html; charset=UTF-8
|_Referrer-Policy: no-referrer
|_Content-Length: 1561
|_Date: Thu, 04 Jun 2020 11:02:09 GMT

```

Illustration 6. Part2 Nmap Scan to Staging & Prod

```

|_http/1.1
465/tcp   open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 465
587/tcp   open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 587
700/tcp   open  tcpwrapped
993/tcp   open  tcpwrapped
995/tcp   open  tcpwrapped
3389/tcp  open  tcpwrapped
5222/tcp  open  tcpwrapped

```

Illustration 7. Part3 Nmap Scan to Staging & Prod

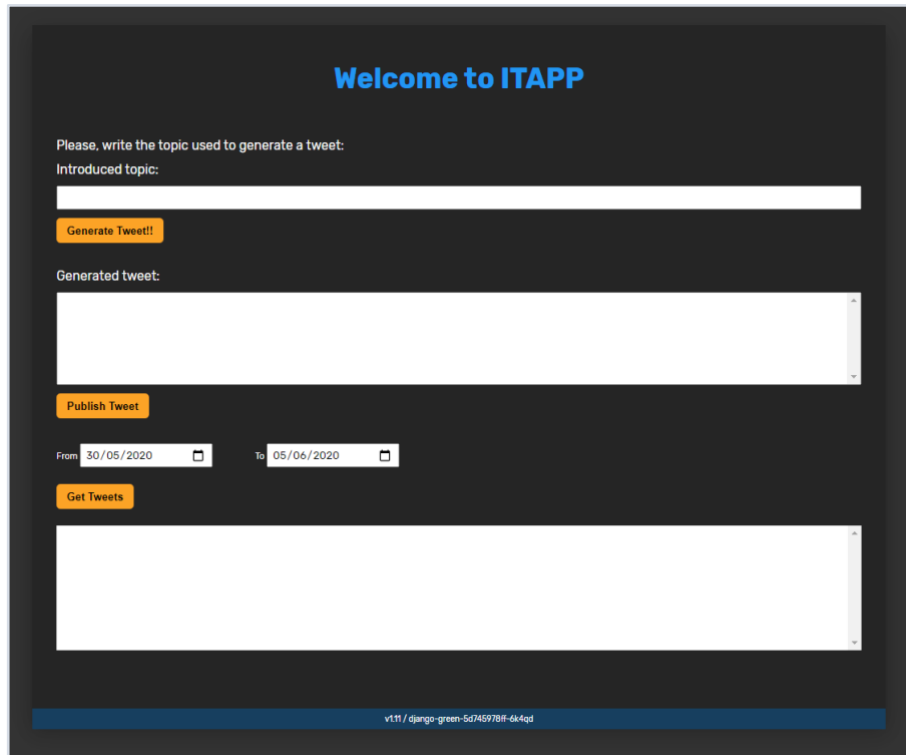
```

5432/tcp  open  tcpwrapped
5900/tcp  open  tcpwrapped
5901/tcp  open  tcpwrapped
8080/tcp  open  http-proxy
|_fingerprint-strings:
|_GetRequest:
|_HTTP/1.0 404 Not Found
|_Content-Type: text/html; charset=UTF-8
|_Referrer-Policy: no-referrer
|_Content-Length: 1561
|_Date: Thu, 04 Jun 2020 11:02:09 GMT

```

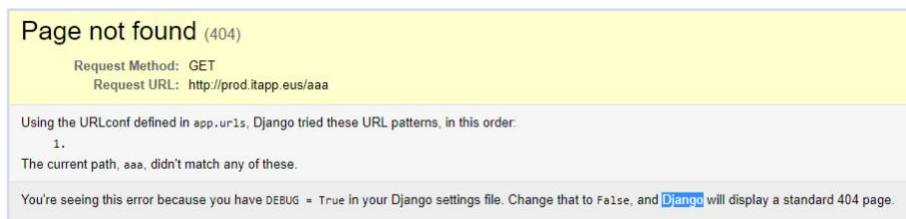
Illustration 8. Part4 Nmap Scan to Staging & Prod

As we can see the only port available is the one from the web application and if we try to access there, we achieve the following:



*Illustration 9. Django App*

If we put some random path in the browser, we can find the following:



*Illustration 10. Django Discovery*

We can see that the application is using Django, but we don't know the concrete version. For that reason, we cannot take a look on concrete vulnerabilities so it advisable to take a look on [this list](#) and keep the software of the system updated.

### SSL/TLS Vulnerability

During the report written so far there is no mention of any specific vulnerability discovered through Nmap or OpenVas because the obtained results have been quite limited, in fact only one type of vulnerability has been reported: *SSL/TLS Vulnerable Cipher Suites for HTTPS*.

```
Vulnerability Detection Result  
  
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:  
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)  
  
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:  
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)  
  
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:  
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

*Illustration 11. Vulnerability detection*

Our machines are using TLSv1.X protocol that accepted some vulnerable cipher suites which can be dangerous in some situations.

To solve this type of vulnerability is highly recommend change the configuration to not accept the listed cipher suites anymore.

### 3. Conclusions

This report has covered many steps in order to audit our machines. First some security methodologies were analyzed, and the decision was taken to use the ISSAF approach as it was the methodology that structured in three simple stages the auditing process.

From the point of view of vulnerabilities found, and as a general advice to protect the audited machines, it is recommended to use the latest possible version of the software used as they might have corrected some security vulnerabilities (of course newer releases might have new vulnerabilities, so if the new version is stable and doesn't have publicly known vulnerabilities, it is highly advised to upgrade or migrate the current services).

This audit revealed some of the flaws of the machine, and in some cases, proposed some advices to solve or to avoid being exploited using publicly known vulnerabilities.



#### **4. Bibliography**

<https://www.openvas.org/>

<https://www.g2.com/products/openvas/competitors/alternatives>

<https://community.greenbone.net/t/openvas-vulnerability-sweet32/1211/4>

<https://nmap.org/book/zenmap-scanning.html>

<https://www.kali.org/tutorials/configuring-and-tuning-openvas-in-kali-linux/>