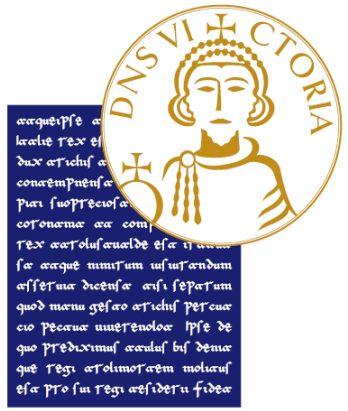
University of Sannio
Department of Engineering



Vulnerability Assessment and Penetration Testing

Arnaldo Sgueglia

CIA

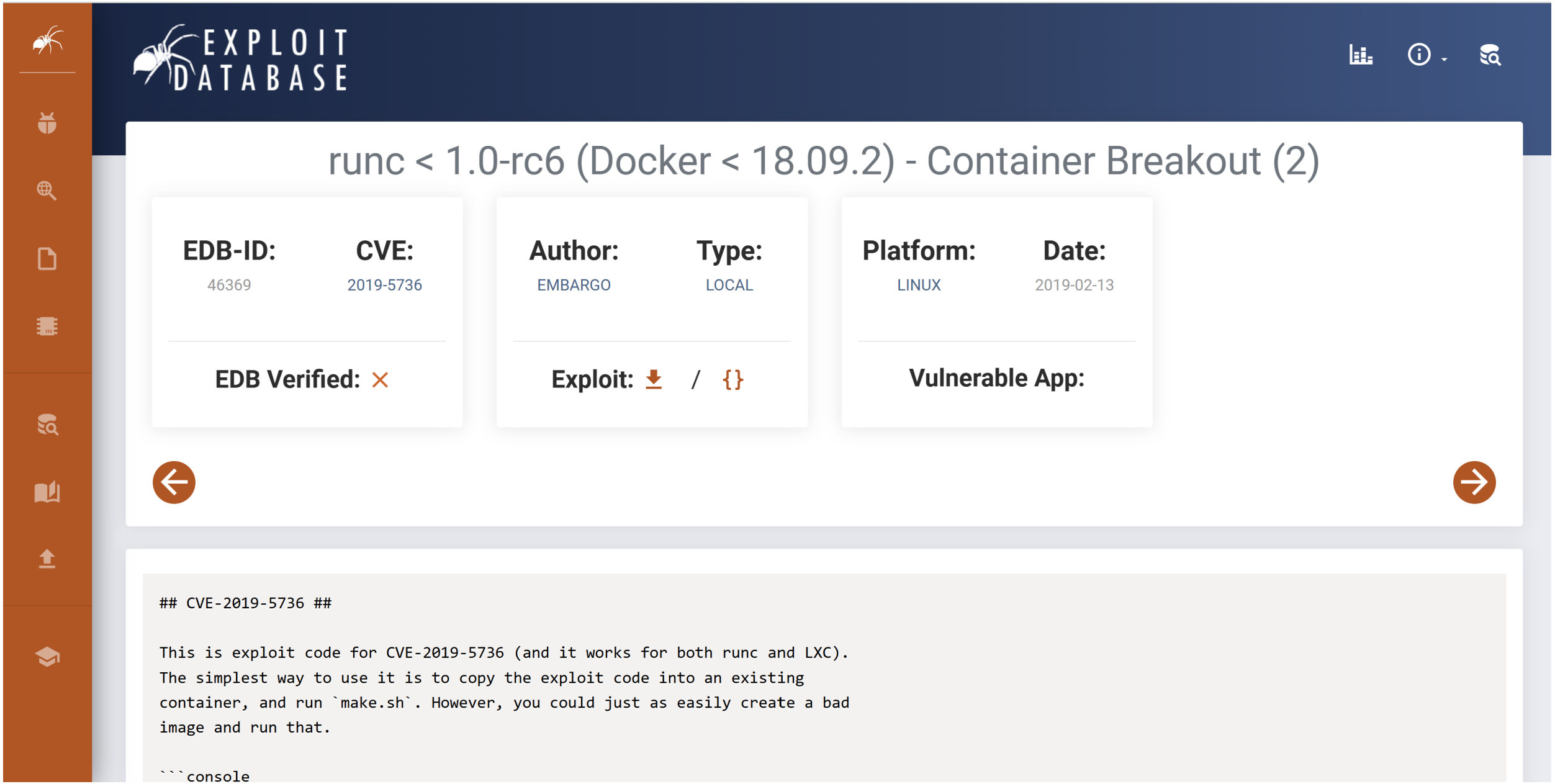
- **Confidentiality**: restrict access to information and resources to authorized person only;

- **Integrity**: verify the correctness, consistency and reliability of information and resources;

- **Availability**: ensure that information and computer resources are accessible when users request for them.

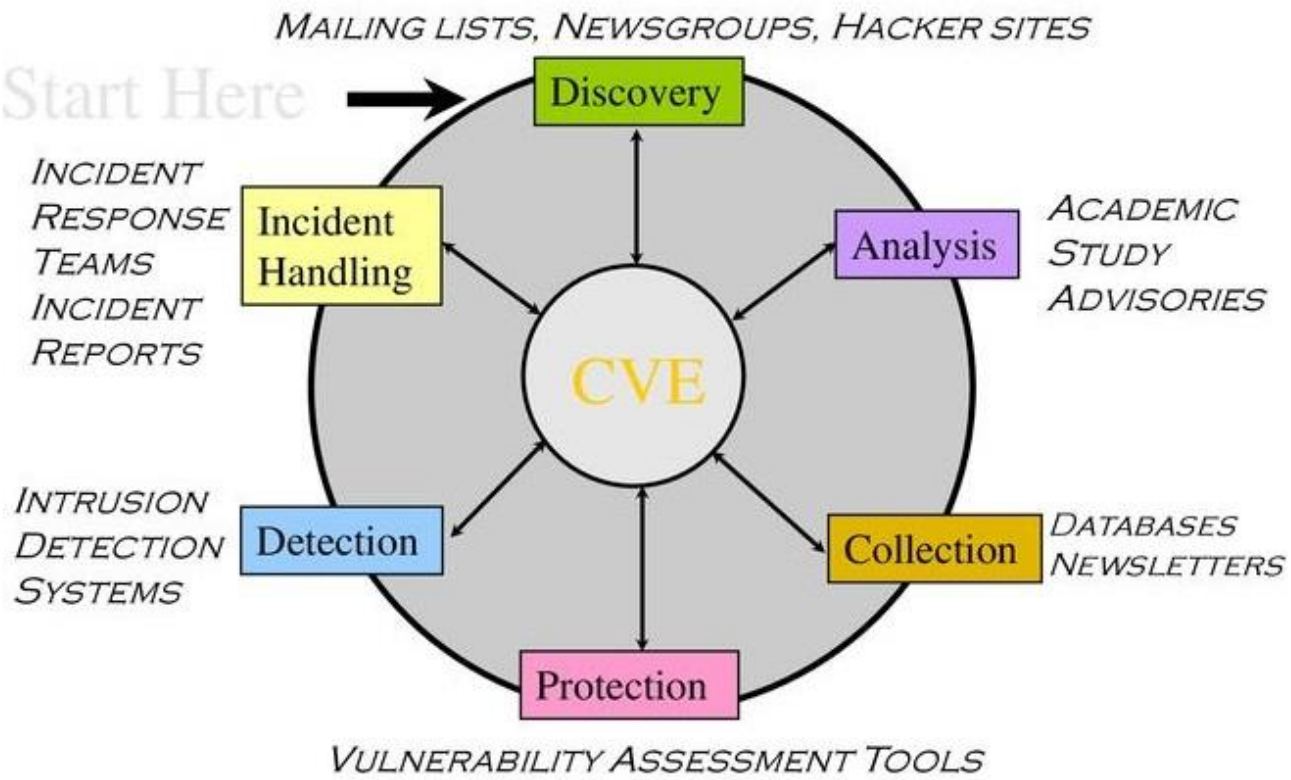
Software vulnerability

- A **software bug** generate an abnormal system behavior;
- A bug is considered a **software vulnerability** if it impacts CIA (Confidentiality, Integrity, Availability) properties;
- An **exploit** refers to a set of instructions useful to access a software system through a software vulnerability.


EXPLOIT DATABASE
runc < 1.0-rc6 (Docker < 18.09.2) - Container Breakout (2)
EDB-ID:
46369
CVE:
2019-5736
Author:
EMBARGO
Type:
LOCAL
Platform:
LINUX
Date:
2019-02-13
EDB Verified:
Exploit:
/
{}
Vulnerable App:
CVE-2019-5736
This is exploit code for CVE-2019-5736 (and it works for both runc and LXC).
The simplest way to use it is to copy the exploit code into an existing
container, and run `make.sh`. However, you could just as easily create a bad
image and run that.
```console

Exploit-DB
```

Vulnerability life-cycle



Zero day vulnerability

Common Vulnerabilities and Exposure (CVE)

- A **Common Vulnerabilities and Exposure** (**CVE**) is a list of common identifiers for publicly known cyber security vulnerabilities

- The **Common Vulnerability Scoring System** (**CVSS**) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVE approval process

- Board member submits raw information to **MITRE**;
- Submissions are grouped, refined, and proposed back to the Board as candidates (CNA-YYYY-NNNN);
- Board reviews and votes on candidates (Accepted, Reserved, Disputed, Rejected);
- If approved, the candidate becomes a **CVE ID** (published on CVE web site).

CVE Identifier

- CVE identifier number (CVE-YYYY-NNNN):
  - YYYY: year when the vulnerability was discovered and made public;
  - NNNN: progressive number based on the number of CVE released in that year.

- Brief description of the security vulnerability or exposure:
  - Typically written by CVE Numbering Authorities (CNAs), MITRE's CVE Content Team, or individuals requesting a CVE ID

Threat and Risk

- A **threat** is a function of an attacker's **capability** in launching an attack and the **impact** that the attack has on the system;

- **Risk** is a function of the **probability** that an organization will remain **impacted** in an attack;

Qualitative and Quantitative risk evaluation

Quantitative risk evaluation

- Classify threat as low, medium or high;
- Give a quantitative weight to a particular event that affect the system.

Qualitative risk evaluation

- Provide more accurate refelction of an organization's risk;
- Their potential impact;
- Maps a cost, a monetary loss, to a particular risk exposure.

Common Vulnerability Scoring System (CVSS-SIG)

- Calculator
- Specification Document
- **User Guide**
- Examples
- Frequently Asked Questions
- CVSS v4.0 Documentation & Resources
- CVSS v3.1 Archive
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

Common Vulnerability Scoring System version 4.0: User Guide

Also available in PDF format .

Document Version: 1.0

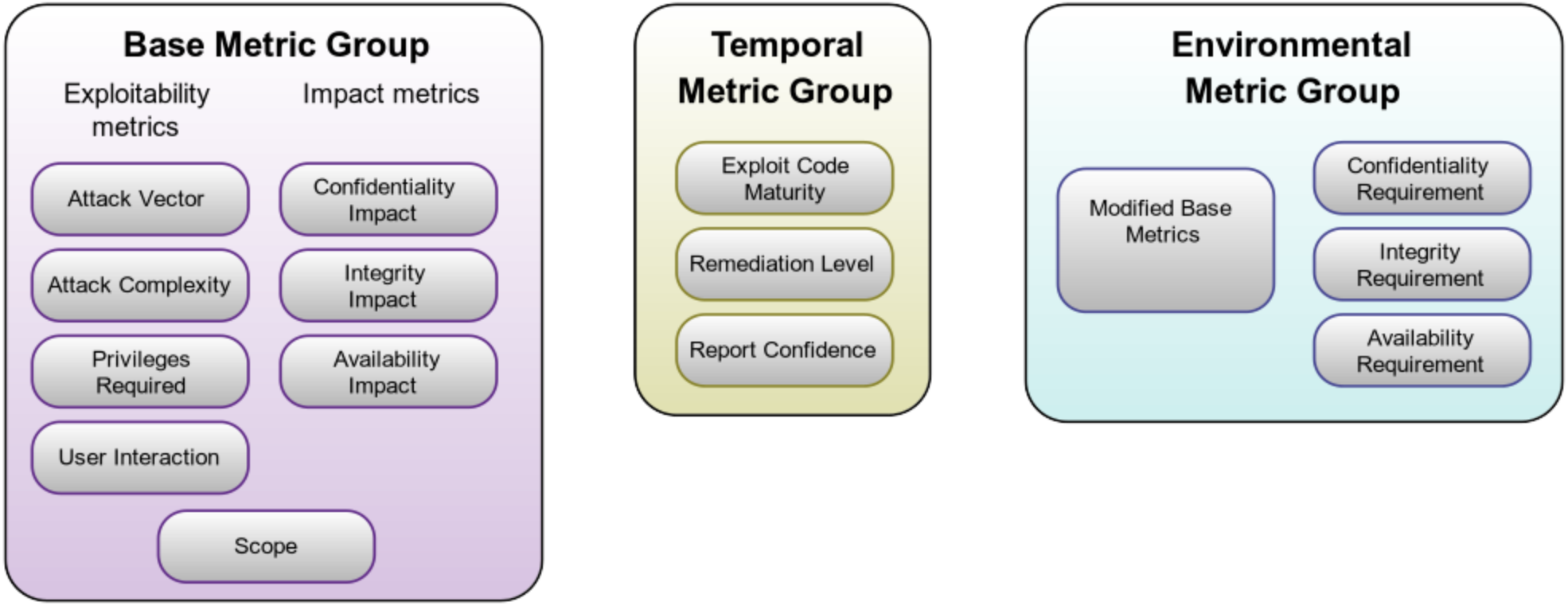
The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Threat group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10. To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations. Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. A CVSS vector string consists of a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 4.0.

The most current CVSS resources can be found at https://www.first.org/cvss/

CVSS is owned and managed by FIRST Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help

Table of Contents

Common Vulnerability Score System



Base Score: 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

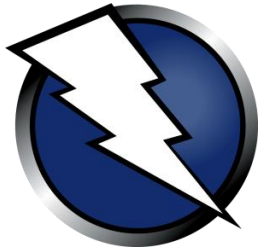
Vulnerability assessment

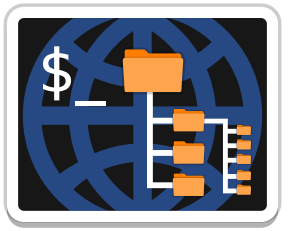
"The **Vulnerability assessment** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system"

Phases:

- Information gathering;
- Vulnerability analysis (automated or manual);
- Reporting;
- Risk mitigation or elimination.

Vulnerability Assessment Tools





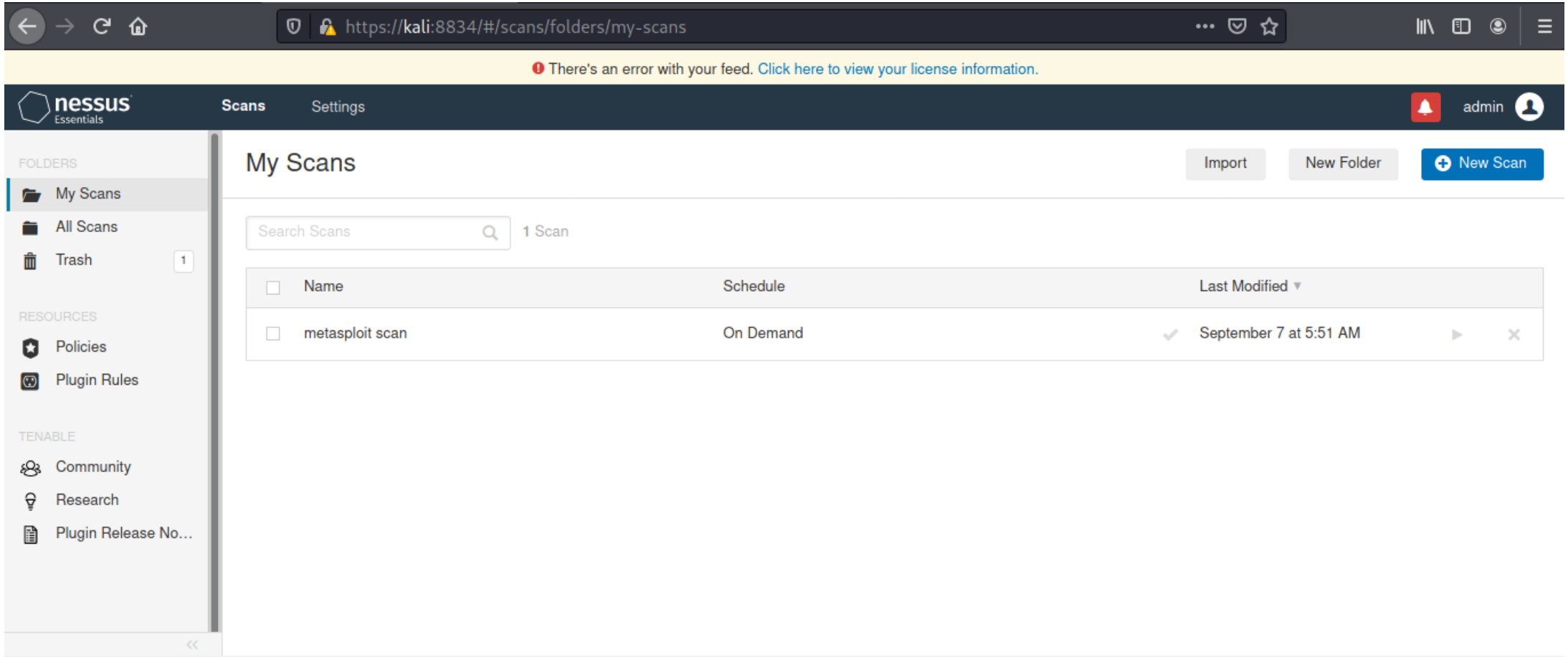
Information gathering - Netdiscover

- Netdiscover is an active/passive address reconnaissance tool;
- Can passively detect online hosts, or search for them, by actively sending ARP requests;
- Also be used to inspect your network ARP traffic, or find network addresses using auto scan mode, which will scan for common local networks.

Information gathering - Nmap

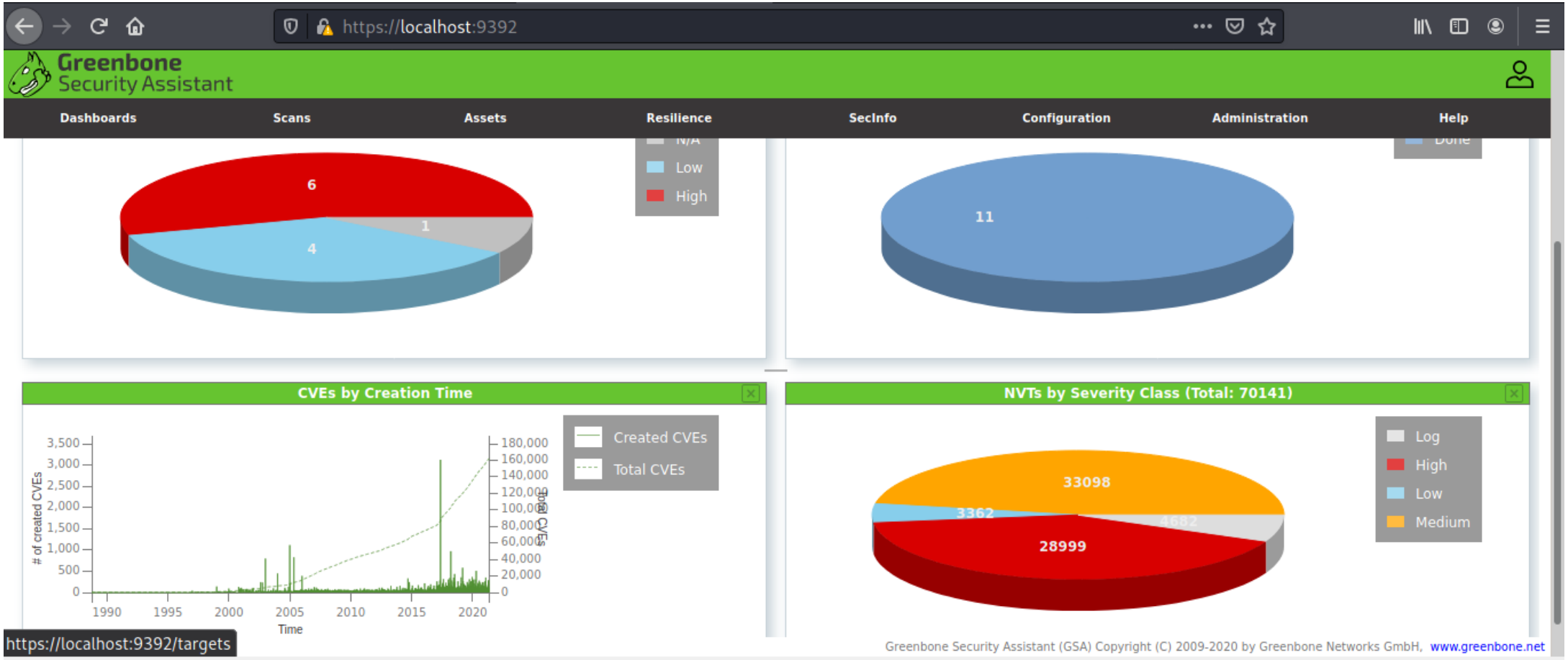
- Nmap (Network Mapper) is a free and open-source network scanner;
- Used to discover hosts and services on a computer network by sending packets and analizing the responses;
- Provides several features for probing computer networks, including host discovery and service and operating system detection;
- Extensible feature set with many scripts that provide more advanced services detection, vulnerability detection and other features.

Vulnerability scanning - Nessus

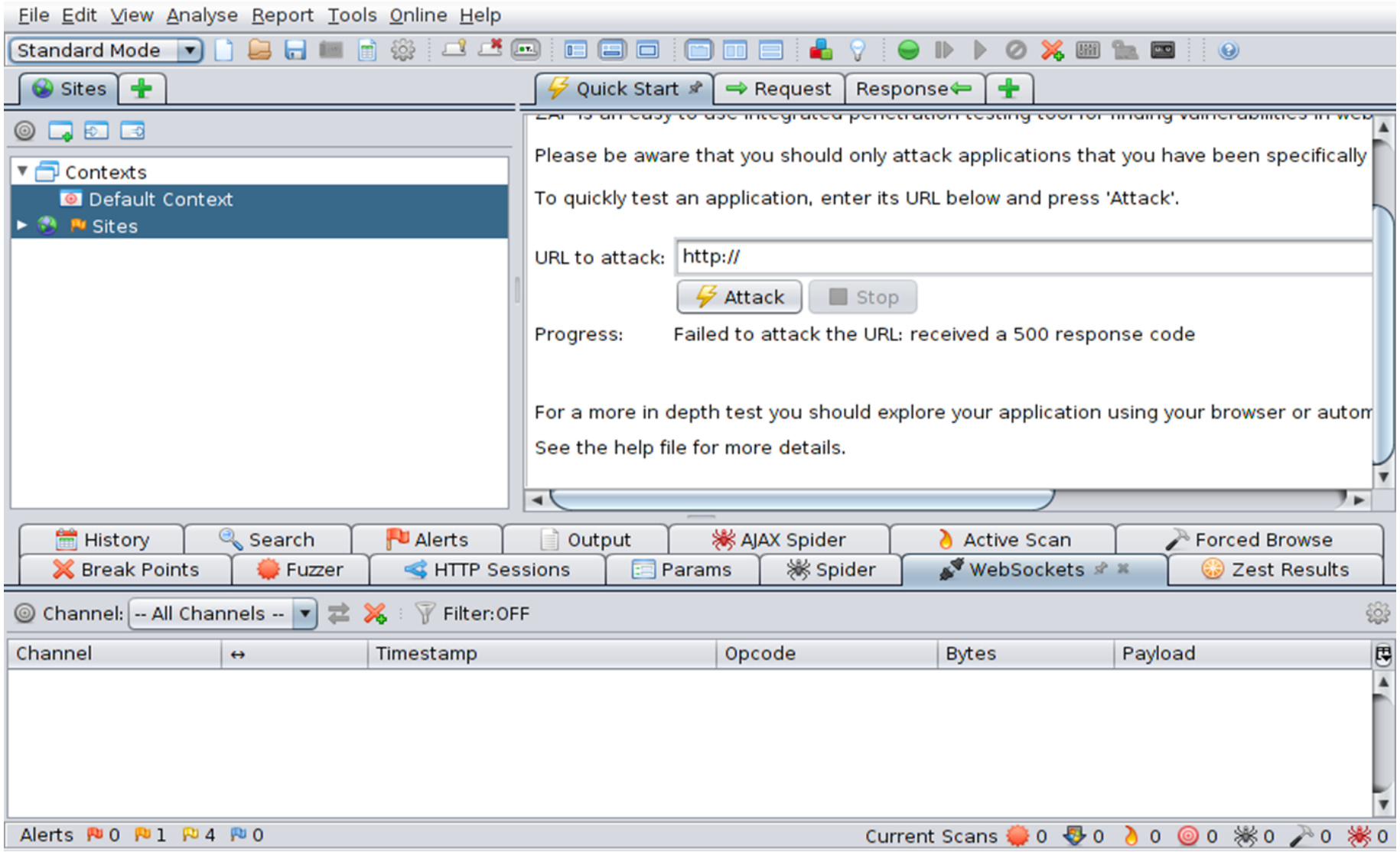


Vulnerability scanning - OpenVAS

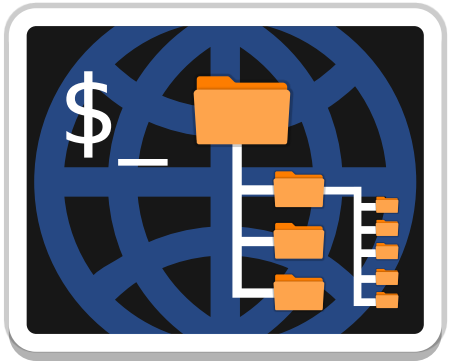
OpenVAS
Open Vulnerability Assessment Scanner



Vulnerability scanning – OWASP ZAP



Vulnerability scanning - Dirb



- DIRB is a Web Content Scanner and it looks for existing (and/or hidden) Web Objects;

- It basically works by launching a dictionary based attack against a web server and analyzing the responses;

- It comes with a set of preconfigured attack wordlists for easy usage and you can use your custom wordlists too.

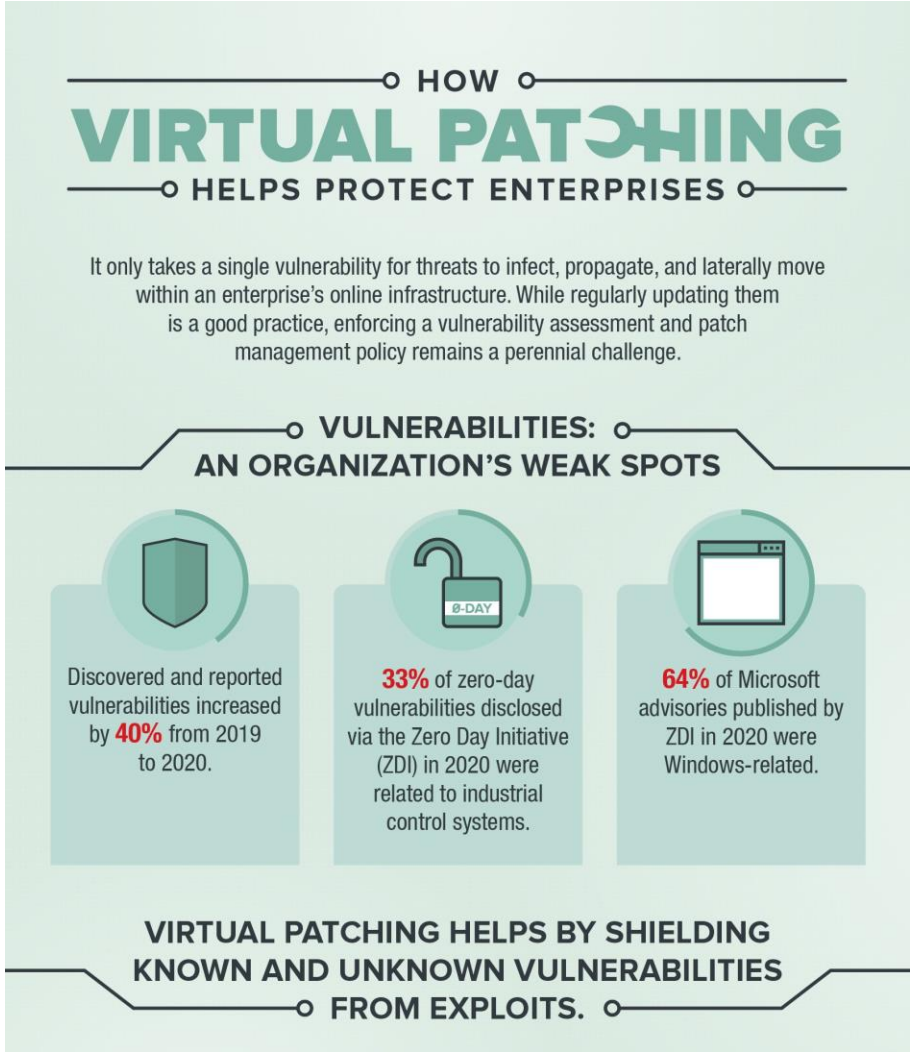
Reporting

- Analyze the previous collected information;
- Create a detailed report based on the analyzed information.

Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	CentOS 6 / 7 : openssl (CE…	CentOS Local Security Checks	1
CRITICAL	CentOS 7 : glibc (CESA-201…	CentOS Local Security Checks	1
HIGH	CentOS 7 : graphite2 (CESA…	CentOS Local Security Checks	1
HIGH	CentOS 7 : kernel (CESA-20…	CentOS Local Security Checks	1
HIGH	CentOS 7 : mariadb (CESA-…	CentOS Local Security Checks	1
MEDIUM	CentOS 5 / 6 / 7 : bind (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : ipa / libldb / li…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : libssh2 (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : nss-util (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : samba (CES…	CentOS Local Security Checks	1

Risk mitigation or elimination

- Analize the previous final report;
- According to the risk analysis decide to patch or not a vulnerability.



Vulnerability assessment vs Penetration Testing

A **Vulnerability Assessment** is the way to find as many flaws as possible and make a prioritized list of remediation items.

- List Oriented
- Do not differentiate between flaws that can be exploited to cause damage and those that cannot.

A **Penetration Test** is an intrusive test, simulating real threat scenario and it is designed to evaluate also the defense measures in place.

- Goal oriented
- A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system

Types of Penetration Test

- Network service test;
- Client-side test;
- Web App Pen Test;
- Wireless Pen Test;
- Social Engineering Test;
- Physical Security Test;
- Cryptanalysis Attack.

Testing Methodologies

- Pen Testing Execution Standard (PTES);
- Open Source Security Testing Methodology (OSSTMM);
- Open Web Application Security Project (OWASP).

PTES

Step 1
- Pre-engagement

Step 2
- Intelligent gathering

Step 3
- Threat modeling

Step 4
- Vulnerability analysis

Step 5
- Exploitation

Step 6
- Post-exploitation

Step 7
- Reporting

Malicious Attackers go further:

- Mantaining access with backdoord;
- Covering tracks.

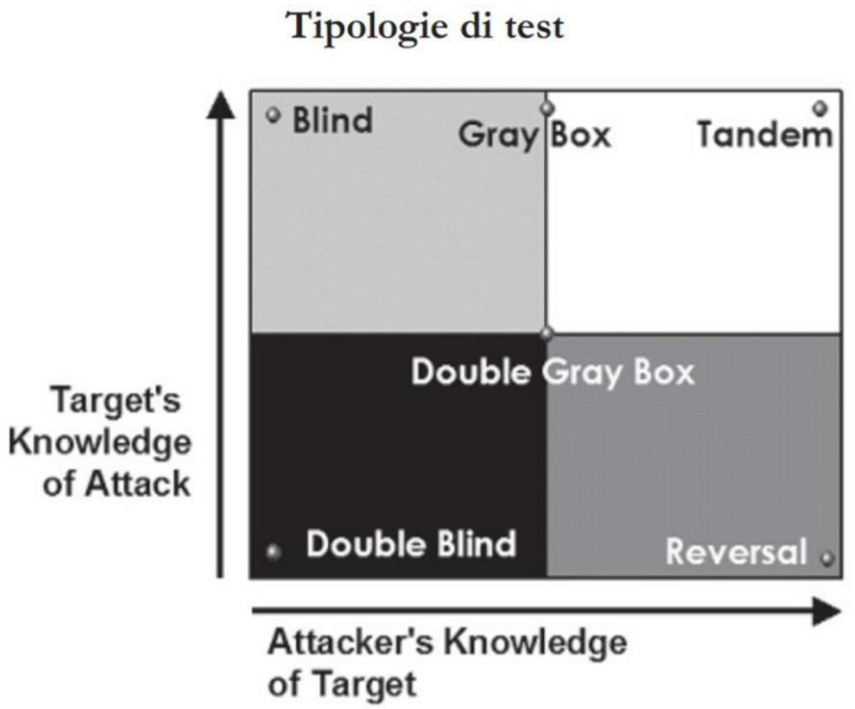
OSSTMM

- OSSTMM provide a scientific methodology for the accurate characterization of operational security (OpSec) through examination and correlation of test results in a consistent and reliable way;

- Scope: provide specific descriptions for operational security tests over all operational channel, which include Human, Physical, Wireless, and Data network, over any vector, and the description of derived metrics;

- Written by Pete Herzog and distributed by ISECOM;

- Includes numeros information gathering templates.



OSSTMM

- **BLIND:** does not require any prior knowledge about the target system. But the target is informed before the test execution;

- **DOUBLE BLIND:** does not require any knowledge about the target system nor is the target informed before the test execution;

- **GRAY BOX:** limited knowledge about the target system are available and the target is also informed before the test is executed;

- **DOUBLE GRAY BOX:** works in a similar way to gray box testing, except that the time frame is defined and there are no channels and vectors being tested;

- **TANDEM:** minimum knowledge to assess the target system are available and the target is also notified in advance before the test is executed;

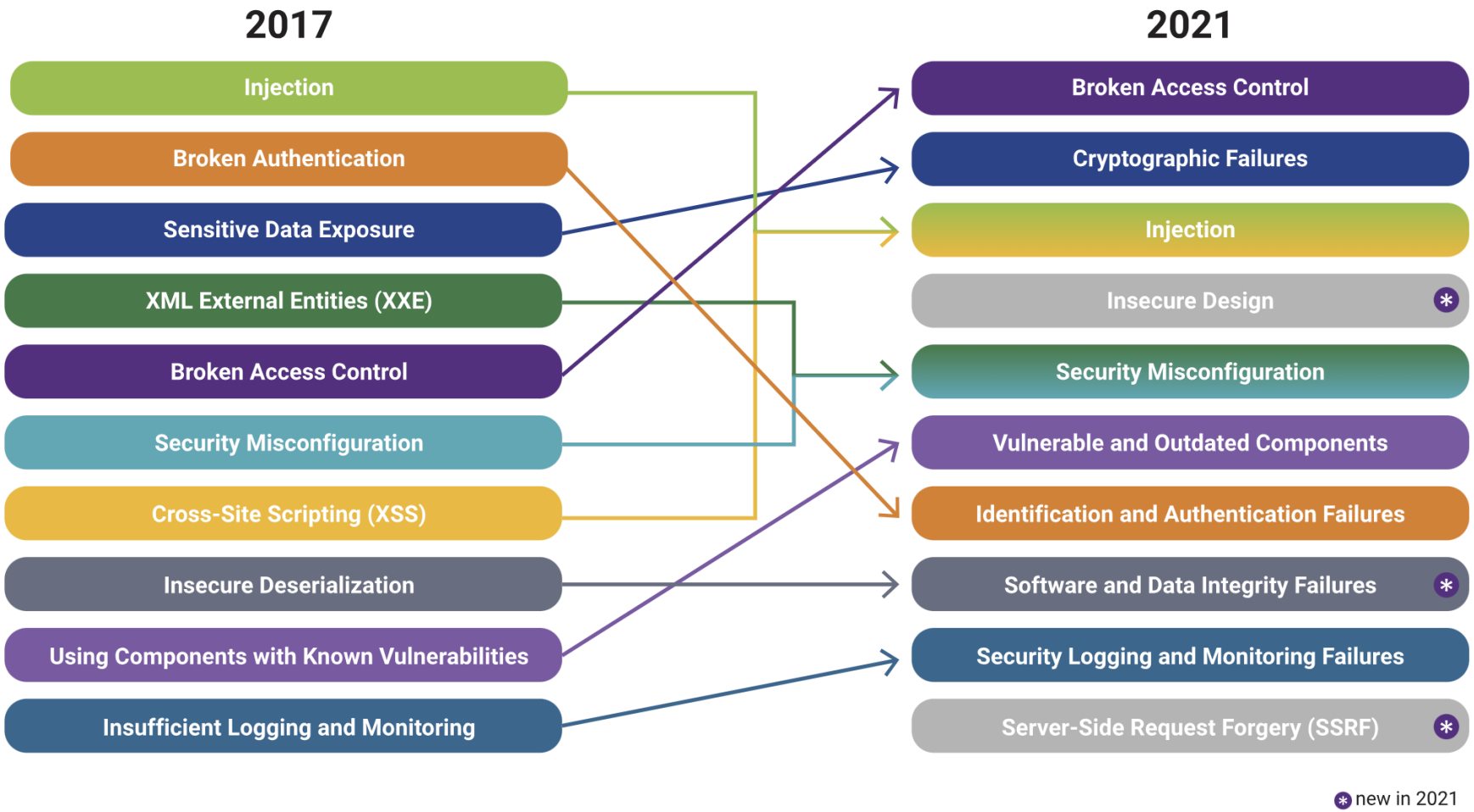
- **REVERSAL**: full knowledge about the target system are available and the target will never be informed of how and when the test will be conducted.

Owasp Testing Guide v.4.0

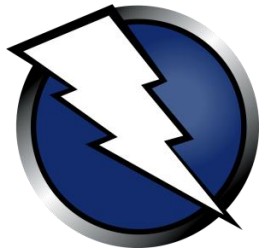
- Information gathering;
- Configuration and deployment management testing;
- Identity management testing;
- Authentication testing;
- Authorization testing;
- Session management testing;
- Input validation testing;
- Testing for error handling;
- Testing for weak cryptography;
- Business Logic testing;
- Client side testing.
- API testing

Owasp Testing Guide v.4.2

Owasp Top 10 2021



Penetration Testing Tools



Exploitation – Metasploit

- Metasploit Framework is an open source penetration testing tool;

- The main components are called modules that provide additional functionality;

- There are six total modules: exploits, payloads, auxiliary, nops, posts, and encoders. We will just focus on exploits and payloads.

Exploitation – Hydra

- Hydra is a parallelized login cracker which supports numerous protocols to attack;

- The main components are called modules that provide additional functionality;

- This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

DEMO