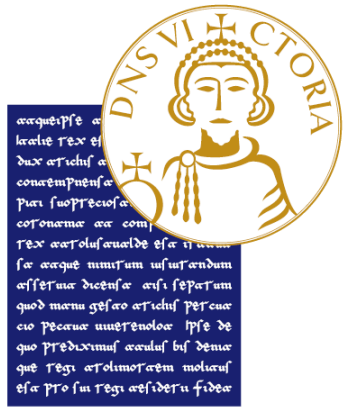
University of Sannio
Department of Engineering



Vulnerability Assessment and Penetration Testing

Arnaldo Sgueglia

CIA

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

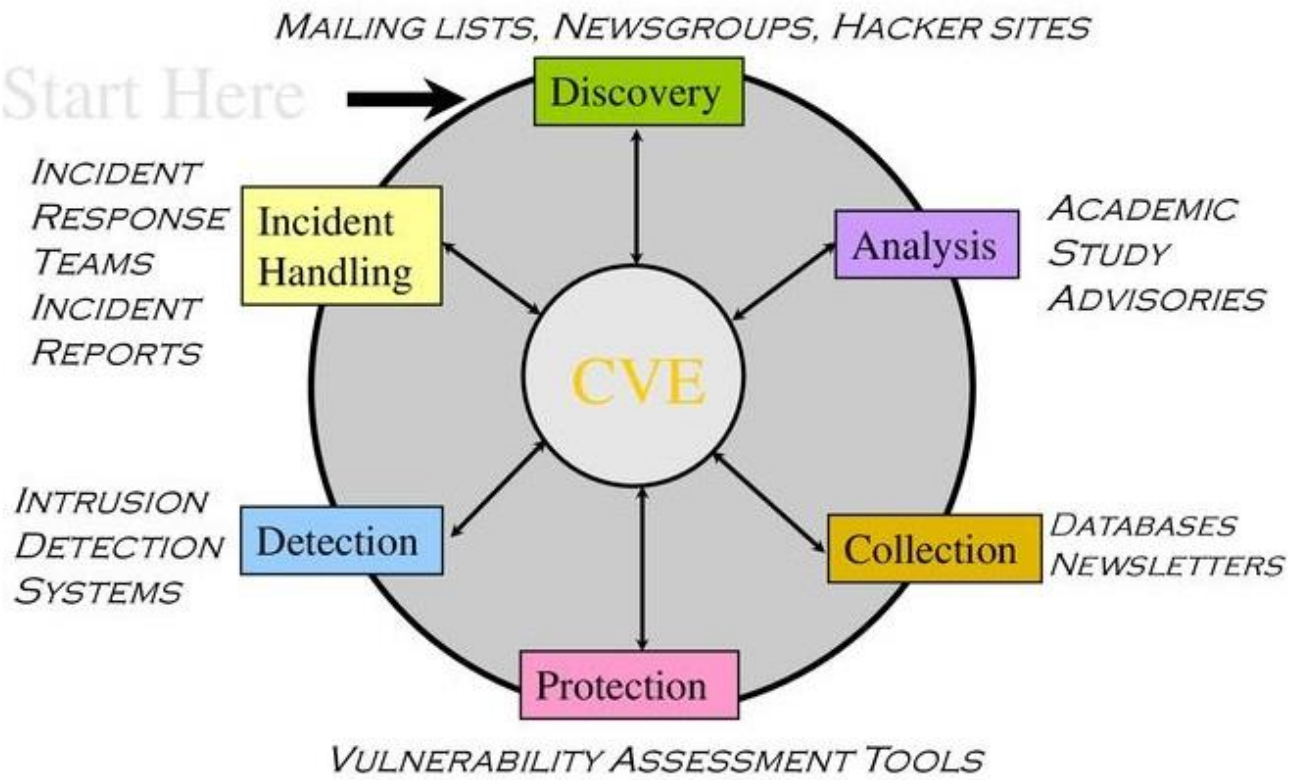
- **Integrity**: verify the correctness, consistency and reliability of information and resources;

- **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.

Vulnerability life-cycle



CVE (Common Vulnerabilities and Exposure)

- A **CVE** (**Common Vulnerabilities and Exposure**) 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

Zero day vulnerability

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

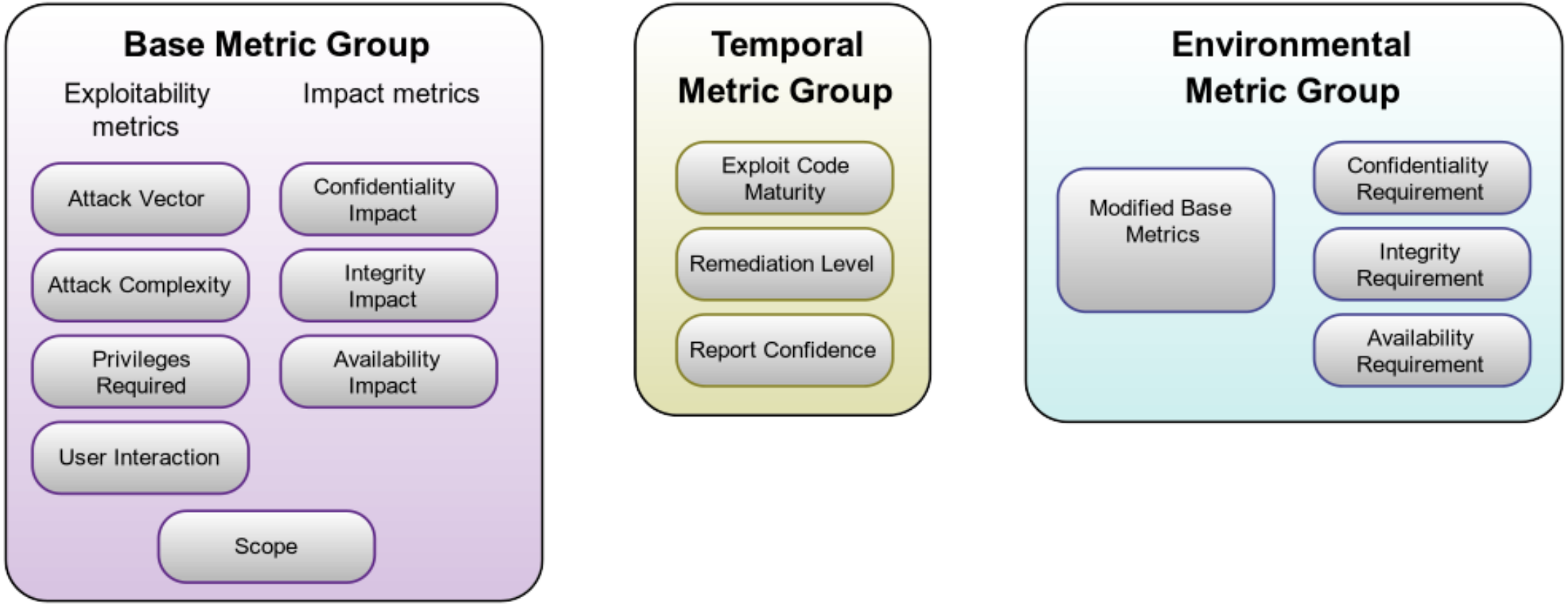
Quantitative risk evaluation

- 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 Score System



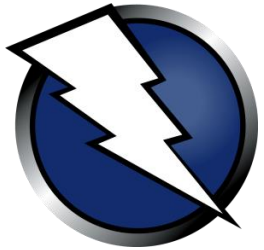
Vulnerability assessment

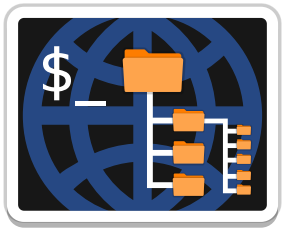
"The **Vulnerability assessment** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system"

Phases:

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

Vulnerability Assessment Tools





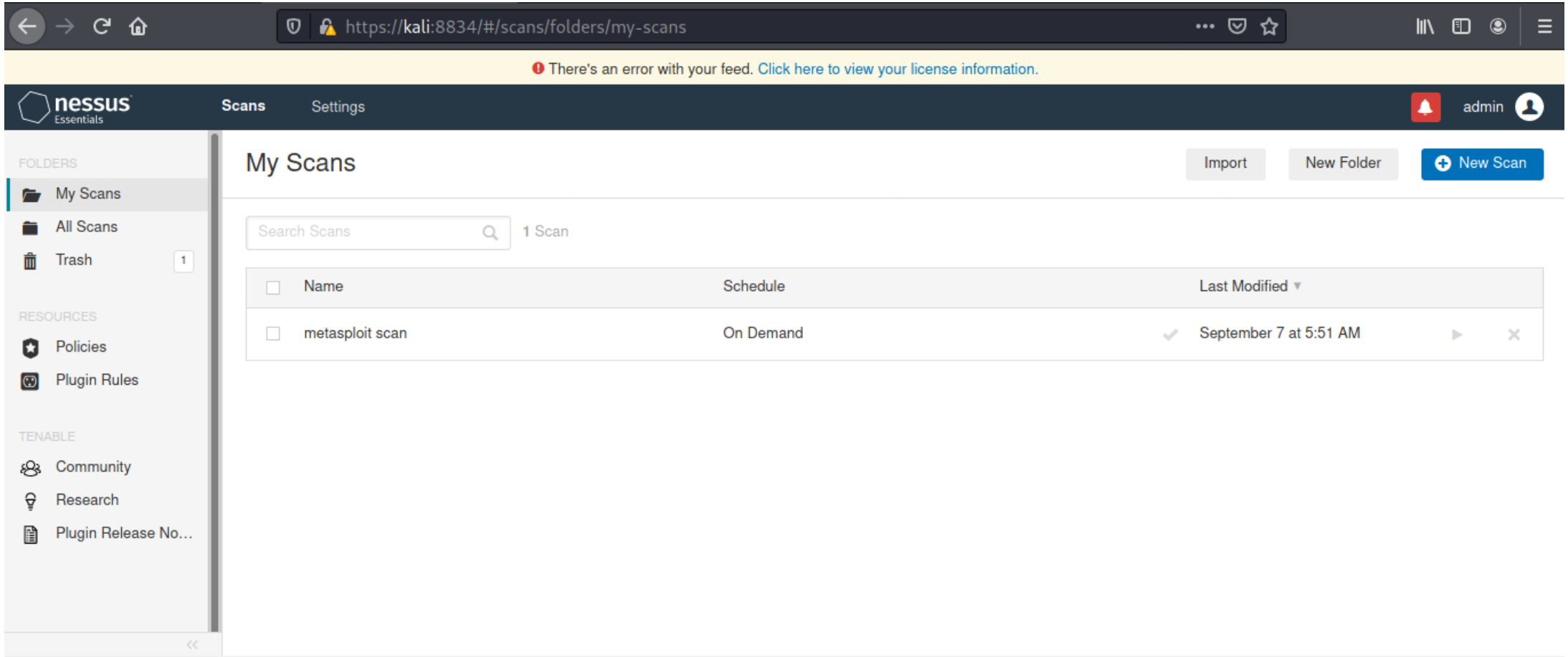
Information gathering - Netdiscover

- 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

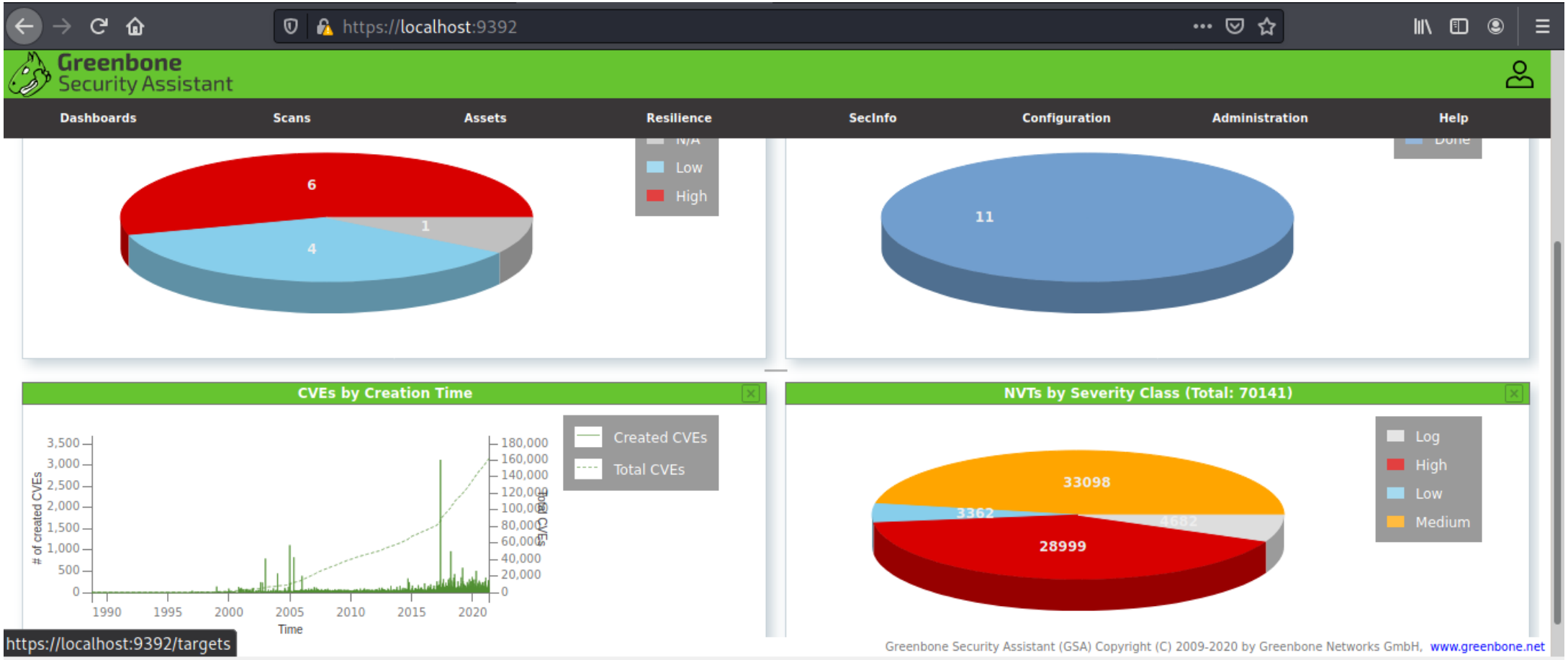
- Nmap (Network Mapper) is a free and open-source network scanner;
- Used to discover hosts and services on a computer network by sending packets and analizing the responses;
- Provides several features for probing computer networks, including host discovery and service and operating system detection;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

Vulnerability scanning - Nessus

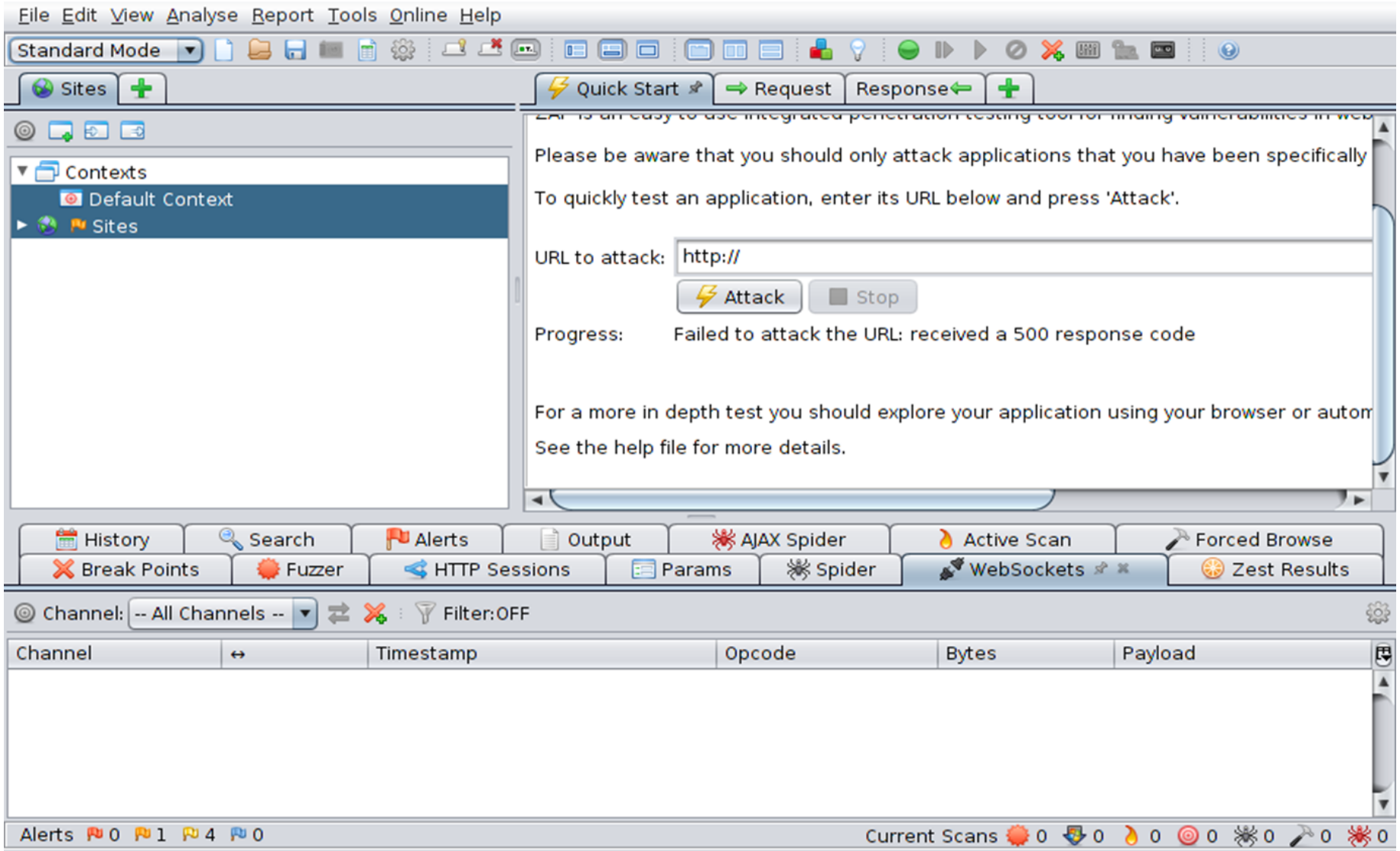


Vulnerability scanning - OpenVAS

OpenVAS
Open Vulnerability Assessment Scanner



Vulnerability scanning – OWASP ZAP



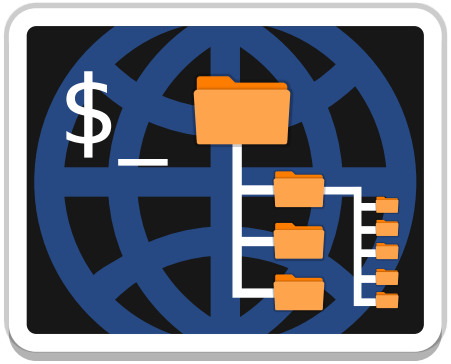
Vulnerability scanning - GoBuster

- Gobuster is a tool used to brute-force URIs including directories and files as well as DNS subdomains;

- It comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists;

- Among the feature found URIs (directories and files) in web sites and DNS subdomains (with wildcard support).

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.

Vulnerability scanning - Nikto

Nikto is a pluggable web server and scanner written in Perl that perform fast security or informational checks

Features:

- Easily updatable CSV-format checks database
- Output reports in plain text or HTML
- Available HTTP versions automatic switching
- Generic as well as specific server software checks
- SSL support (through libnet-ssleay-perl)
- Proxy support (with authentication)
- Cookies support

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.

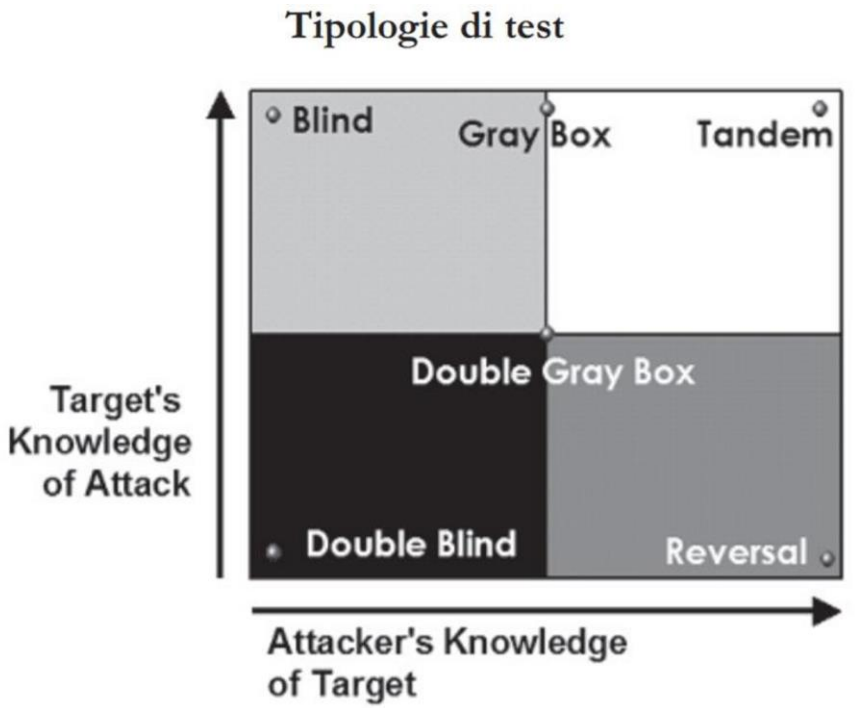
OSSTMM

- 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;

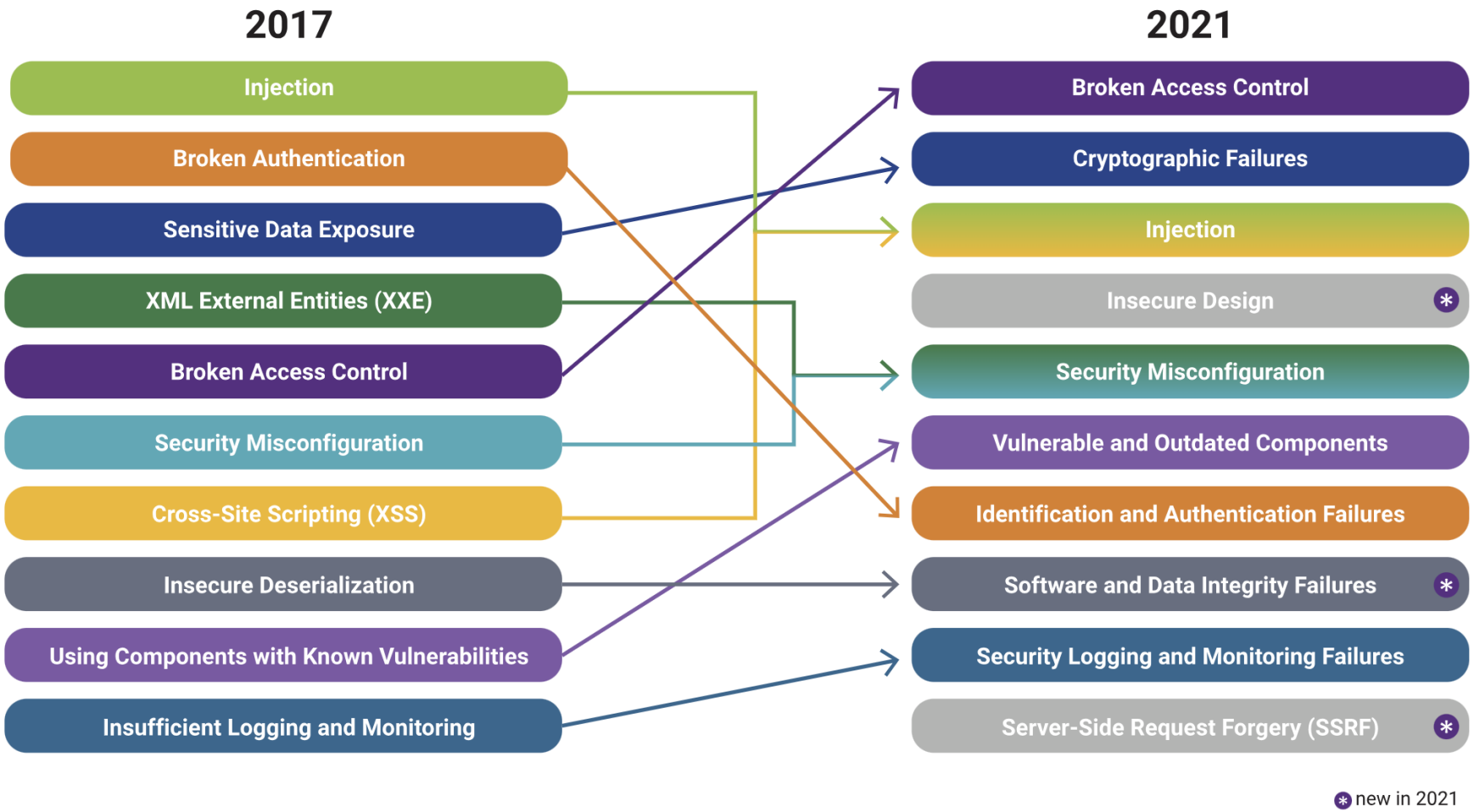
- **TANDEM:** minimum knowledge to assess the target system are available and the target is also notified in advance before the test is executed;

- **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.

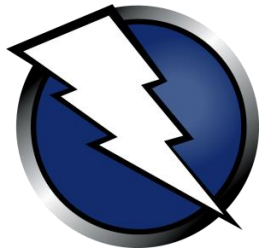
Owasp Testing Guide v.4.0

- 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 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

USB rubber ducky

```
Keyboard.begin();
Keyboard.press(KEY_LEFT_GUI);
Keyboard.press('r');
Keyboard.releaseAll();
Keyboard.print("notepad");
Keyboard.press(KEY_RETURN);
Keyboard.releaseAll();
Keyboard.print("You have been pawned!");
```

OMG cable

GUI r

DELAY 1000

STRING notepad

DELAY 1000

ENTER

DELAY 1000

STRING Have been hacked!!