Corso di Sicurezza delle Reti e dei Sistemi Software *aa 2015/16*

Universita' degli Studi del Sannio

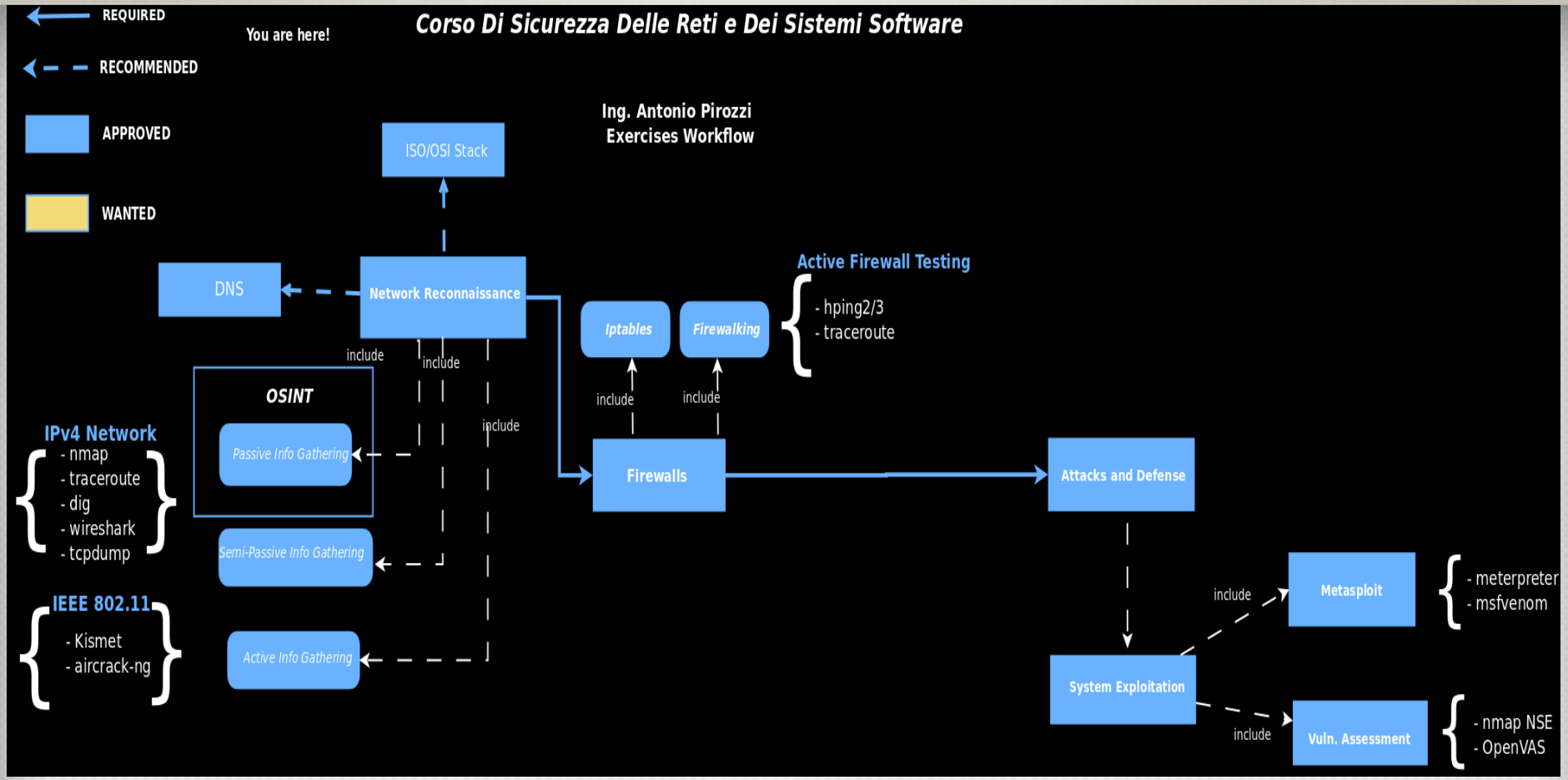
Ing. Antonio Pirozzi

Hacking *toolZ*

- **OpenVAS** (Open Vulnerability Assessment System) :NESSUS fork
- **NESSUS**
- **Nexpose**
- **Nmap NSE scripts**
- **Metasploit framework**
- **nikto**
- **Nmap VULNscan**

https://n0where.net/nmap-vulnerability-scanner-vulscan/

Exercises workflow



VA(PT) → System Exploitation

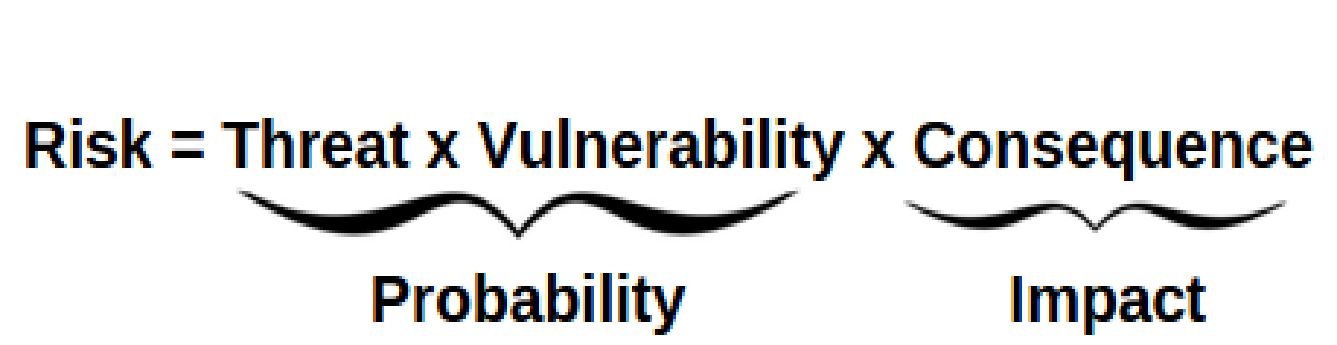
how damaging a flaw could be in a real attack

Find every flaws in the system

VAPT provides a detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks

Risk mgmt

Risk can be quantified using the risk equation:



Greater is the Threat..

more likely the system could be attacked

More vulnerable is the system

Greater the probability the system could be compromised.

What is a..

Vulnerability Assessment :

Is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Cit. wikipedia

CVSS (actually v3) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

three metric groups, the Base, Temporal, and Environmental

Don’t just rely on vulnerability counts to understand your exposure to threats and exploits

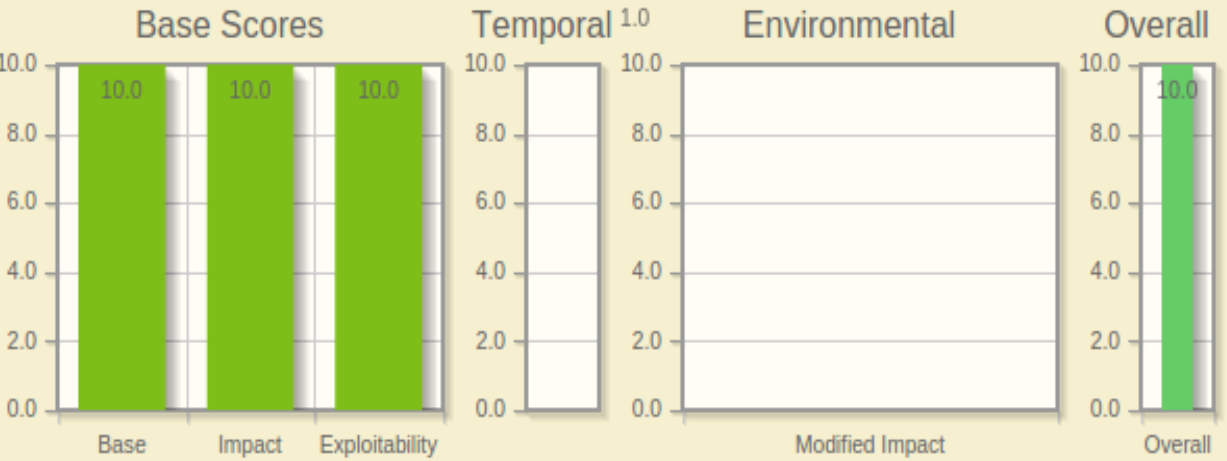
Prioritize risks

OWASP_RISK_RATING_Methodology

#Step 1: Identifying a Risk
#Step 2: Factors for Estimating Likelihood
#Step 3: Factors for Estimating Impact
#Step 4: Determining Severity of the Risk
#Step 5: Deciding What to Fix
#Step 6: Customizing Your Risk Rating Model

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

CVSS..an example



CVSS Base Score	**10**
Impact Subscore	10
Exploitability Subscore	10
CVSS Temporal Score	**Not Defined**
CVSS Environmental Score	**Not Defined**
Modified Impact Subscore	0
Overall CVSS Score	**10**

Show Equations

CVSS v2 Vector (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Local (AV:L)	Adjacent Network (AV:A)	Network (AV:N)

Access Complexity (AC)*

High (AC:H)	Medium (AC:M)	Low (AC:L)

Authentication (Au)*

Multiple (Au:M)	Single (Au:S)	None (Au:N)

* - All base metrics are required to generate a base score.

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Partial (C:P)	Complete (C:C)

Integrity Impact (I)*

None (I:N)	Partial (I:P)	Complete (I:C)

Availability Impact (A)*

None (A:N)	Partial (A:P)	Complete (A:C)

Risk evaluation for Compliance Requirements

PCI DSS v3.0 Req. 11.2.1: quarterly internal scans and rescans until all 'high risk' vulnerabilities are resolved.

PCI DSS v3.0 Req. 11.2.2 : requires quarterly external scans and rescans until no vulnerabilities exist that are scored 4.0 or higher by the CVSS.

PCI DSS v3.0 Req. 11.2.3 : requires internal and external scanning, and rescanning, after any significant change to the network.

Cite:

Risk rankings should be based on industry best practices as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score,and/or the classification by the vendor, and/or type of systems affected.