UNIVERSITÀ DEGLI STUDI DI SALERNO

Department of Information and Electrical Engineering and applied Mathematics

Master's Degree in Computer Engineering

DESIGN AND APPLICATION OF A SECURITY ASSESSMENT AND HARDENING METHODOLOGY FOR VIRTUAL ENVIRONMENTS

First Supervisor
Prof. Vincenzo Carletti
Second Supervisor
Prof. Pasquale Foggia

Candidate
Enrico Maria Di Mauro
Identification Number
0622701706

Academic Year 2022/2023

Problem description

Design a methodology for

OSSTMM

Security assessment

Hardening

State of the art

Data & Information security

=

Crucial challenge

- Systems complexity
- Sensitive data

- Resources
- Skills

State of the art

Contribution

- Structurality
- Generalizability
- Iterativity
- Replicability & Coherence

Proposed solution

- Knowledge level
- Goals of the activity

Proposed solution

- Preparatory actions

Proposed solution

- Comprehensive &
  Detailed investigation

Proposed solution

- Obtain access
- Privilege escalation

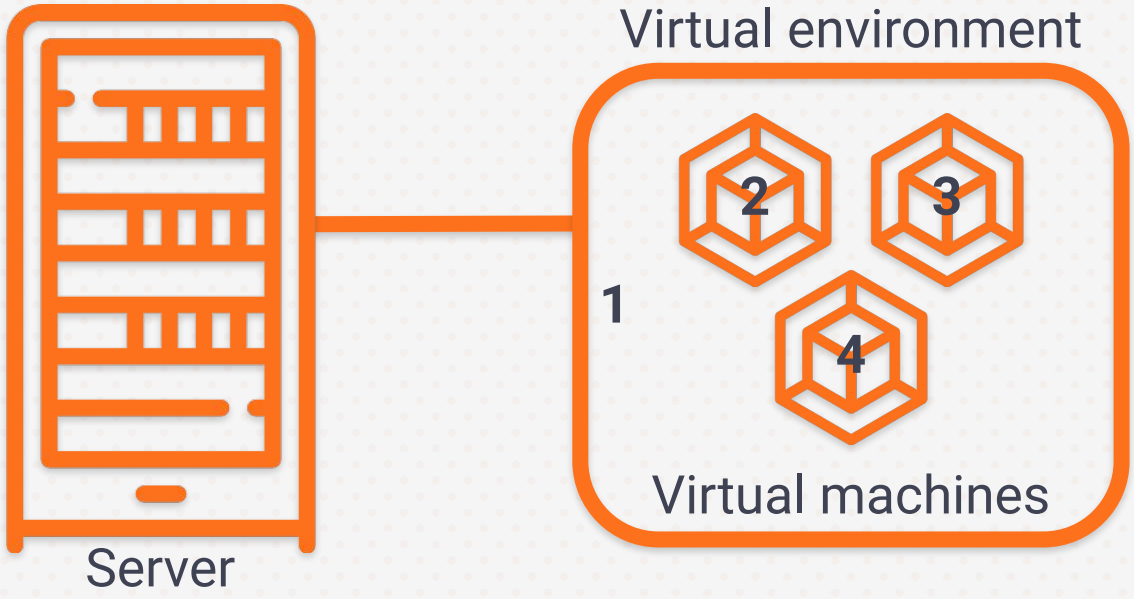
Proposed solution

- Risk level
- Risk Assessment Value (RAV)

Proposed solution

- Defense practices are implemented

Real-world setup



Real-world setup

Proxmox

Robotcup

Docenti

Repository-GitLab

- SSH
- HTTP
- HTTPS

Vulnerability report

CVE	Vulnerability source	Potential impact (CVSS)	Exploit likelihood (EPSS)	Expected consequence

Risk analysis

Severity	Impact
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10

Severity	Likelihood (%)
Impossible	0.00
Less probable	0.01 - 39.99
Probable	40 - 69.99
High probable	70 - 89.99
Sure	90 - 100

Risk analysis

	None	Low	Medium	High	Critical
Impossible	Inexistent	Inexistent	Inexistent	Inexistent	Inexistent
Less probable	Inexistent	Slight	Slight	Normal	Great
Probable	Inexistent	Slight	Normal	Great	Catastrophic
High probable	Inexistent	Normal	Great	Catastrophic	Catastrophic
Sure	Inexistent	Great	Catastrophic	Catastrophic	Catastrophic

RAV

OSSTMM

Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC	
Visibility	4
Access	2
Trust	0
Total (Porosity)	6

CONTROLS		
Class A		Missing
Authentication	2	4
Indemnification	0	6
Resilience	2	4
Subjugation	0	6
Continuity	0	6
Total Class A	4	26

Class B		Missing
Non-Repudiation	2	4
Confidentiality	1	5
Privacy	0	6
Integrity	1	5
Alarm	2	4
Total Class B	6	24

		True Missing
All Controls Total	10	50
Whole Coverage	16,67%	83,33%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	590	9,333333	5506,666667
Weaknesses	7	5,333333	37,333333
Concerns	0	5,000000	0,000000
Exposures	0	100,333333	0,000000
Anomalies	0	99,500000	0,000000
Total # Limitations	597		5544,0000

OPSEC	7,722143
True Controls	4,017304
Full Controls	4,017304
True Coverage A	13,33%
True Coverage B	20,00%
Total True Coverage	16,67%
Limitations	32,991514
Security Δ	-36,70
True Protection	63,30

Actual Security: 64,2157 ravs

Relevant discoveries

External threats

Pros

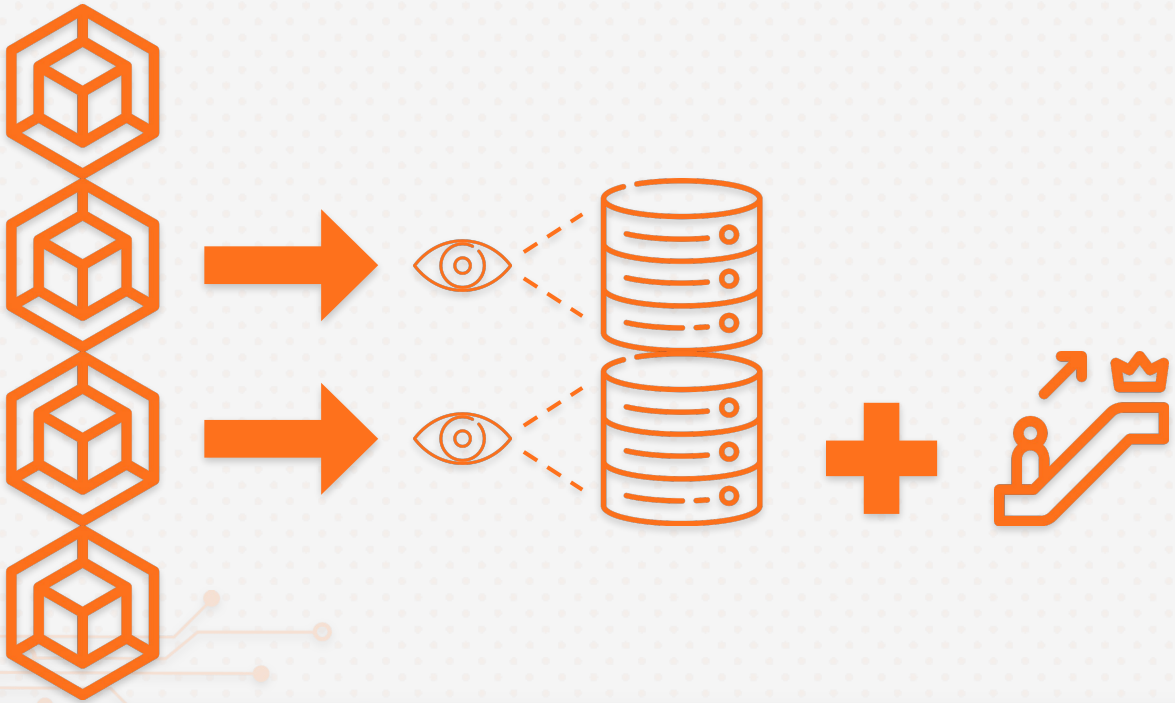
- No usable exploits
- No brute force

Cons

- No firewalls
- No secure configurations
- Outdated elements

Relevant discoveries

Internal threats



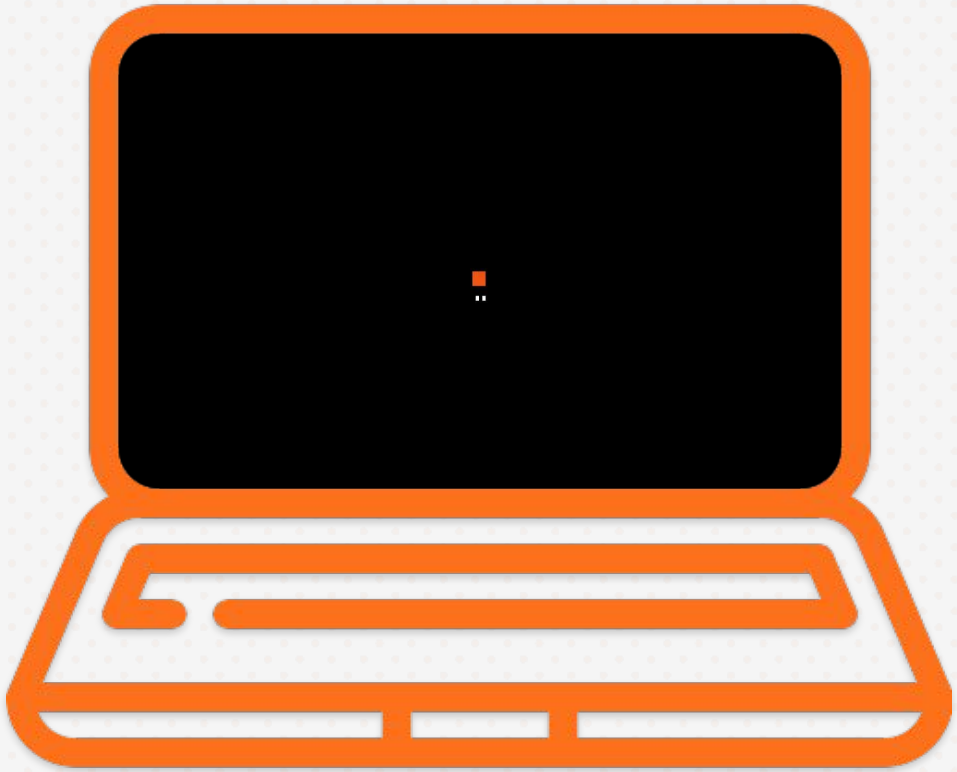
Results evaluation

	Old RAV	New RAV	
100	69.62	72.65	~5%
	64.21	71.33	~11%
	56.51	67.47	~20%
	63.24	71.56	~13%

Results evaluation

- Designed methodology validated
- Design choices consistent with the goals
- Characteristics satisfy the needs of cybersecurity

Demo video



UNIVERSITÀ DEGLI STUDI DI SALERNO

Department of Information and Electrical Engineering and applied Mathematics

THANK YOU
FOR THE ATTENTION

First Supervisor
Prof. Vincenzo Carletti
Second Supervisor
Prof. Pasquale Foggia

Academic Year 2022/2023

Candidate
Enrico Maria Di Mauro
Identification Number
0622701706