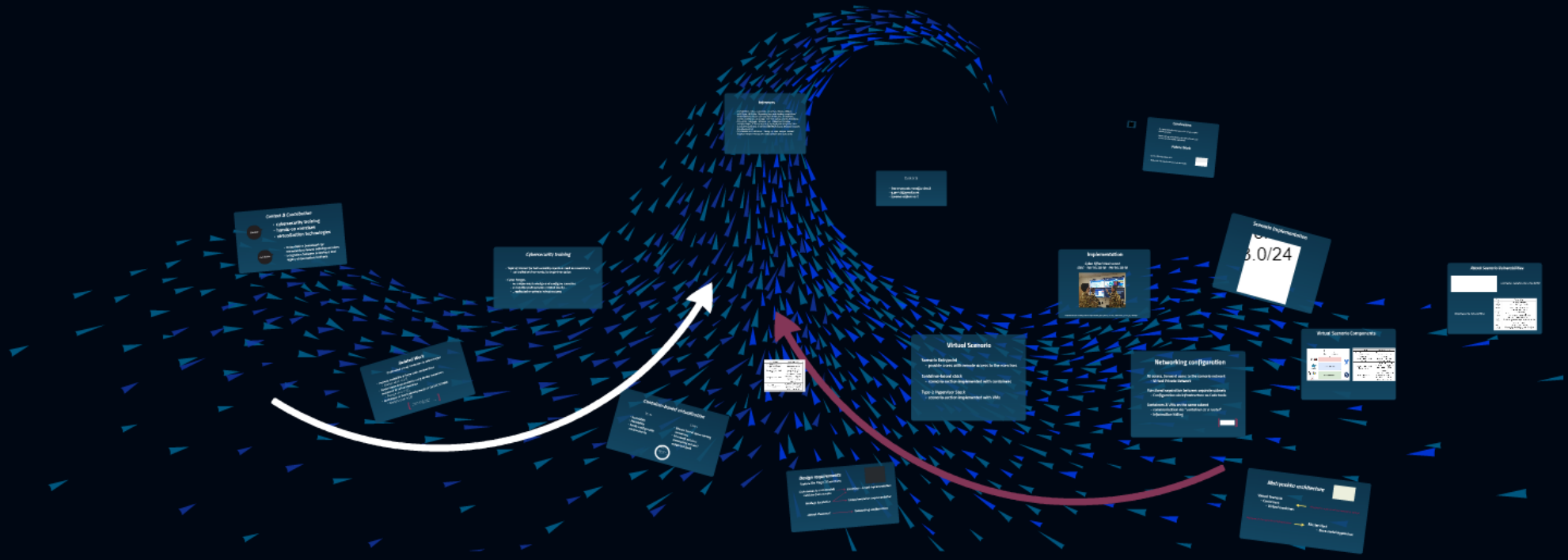
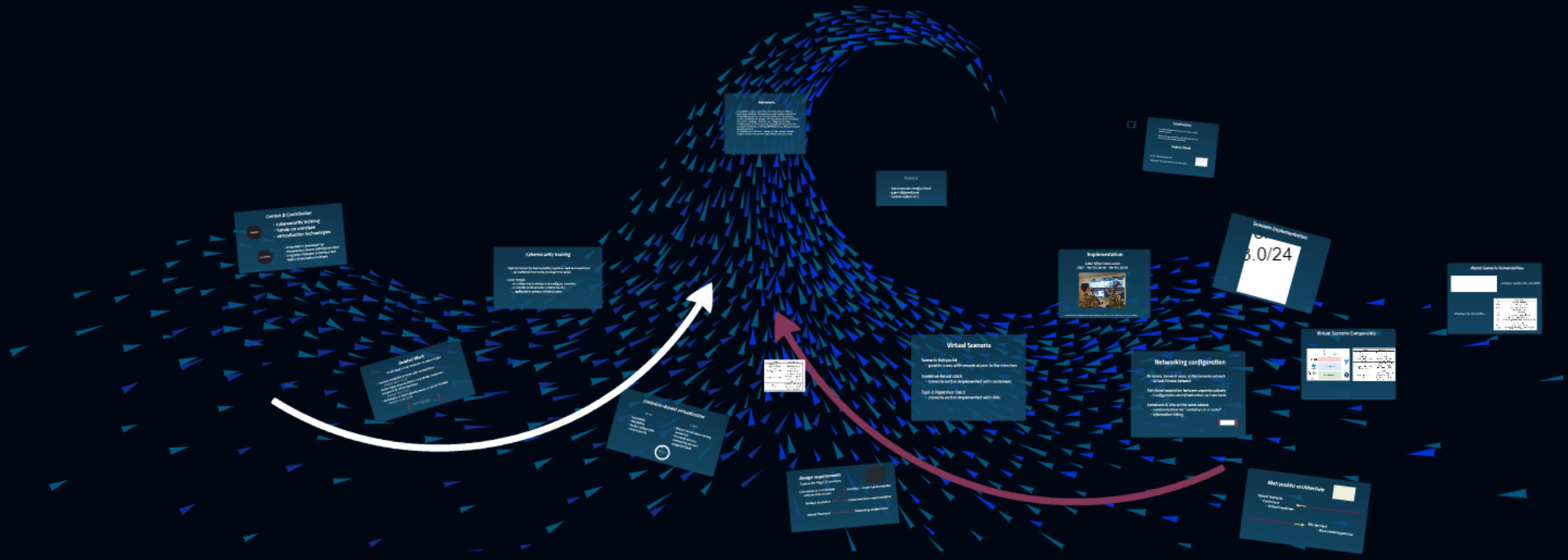


Capturing flags in a dynamically deployed microservices-based heterogeneous environment

F. Caturano, G. Perrone, S.P. Romano

University Federico II of Napoli

Prezi

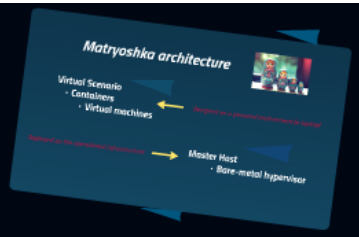


Capturing flags in a dynamically deployed microservices-based heterogeneous environment

F. Caturano, G. Perrone, S.P. Romano

University Federico II of Napoli

Prezi

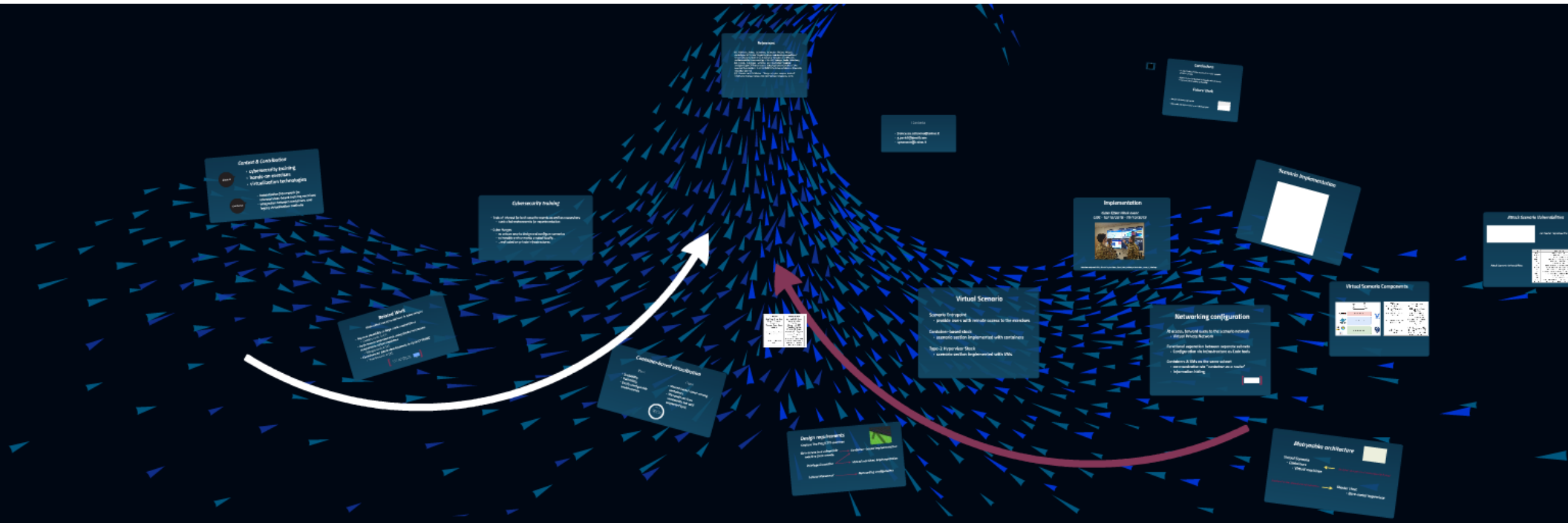


s in a dynamically deployed ed heterogeneous environment

F. Caturano, G. Perrone, S.P. Romano

University Federico II of Napoli

Prezi



Capturing flags in a dynamically deployed microservices-based heterogeneous environment

F. Caturano, G. Perrone, S.P. Romano

University Federico II of Napoli

Prezi

Context & Contribution

Context

- cybersecurity training
- hands-on exercises
- virtualization technologies

Contribution

- instantiation framework for microservices-based training exercises
- integration between containers and legacy virtualization methods

Prezi

Cybersecurity training

- Topic of interest for both security experts as well as researchers
  - controlled environments for experimentation
- Cyber Ranges
  - no unique way to design and configure scenarios
  - vulnerable environments created locally...
  - ...replicated on private infrastructures

Prezi

Container-based virtualization

Pros

- **Scalability**
- **Portability**
- **Easily configurable environments**

Cons

- **Shared kernel space among containers**
- **Microsoft services community not well supported (yet)**

Prezi

Solution

- Hybrid virtual scenarios
- Integration between containers and virtual machines
    - Infrastructure as Code (IaC) as glue

Prezi

Related Work

Underrated use of containers in cyber ranges

- ***Improve scalability in large scale competitions***
  - Childers et al. in [1]
- ***Performance improvements using Docker containers compared to virtual machines***
  - Alangot et al. in [2]
- ***Containers as future developments in Cyris/CYTRONE***
  - Chandra et al. in [3]

Prezi

ure developments in Cyris

in [3]

Docker Security Playground

A microservices-based framework for the implementation of attack scenarios in virtualized network infrastructures

IPTComm 2017

Prezi

Design requirements

Capture The Flag (CTF) exercises

Gain access to a vulnerable machine from remote → *Container - based implementation*

Privilege Escalation → *Virtual machines implementation*

Lateral Movement → *Networking configuration*

Prezi

Matryoshka architecture

Virtual Scenario

- **Containers**
  - **Virtual machines**

← *Designed on a personal environment (a laptop)*

Deployed on the operational infrastructure →

Master Host

- **Bare-metal hypervisor**

Prezi

Virtual Scenario

Scenario Entrypoint

- provide users with remote access to the exercises

Container-based stack

- scenario section implemented with containers

Type-2 Hypervisor Stack

- scenario section implemented with VMs

Prezi

Networking configuration

At access, forward users to the scenario network

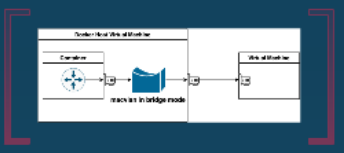
- Virtual Private Network

Functional separation between separate subnets

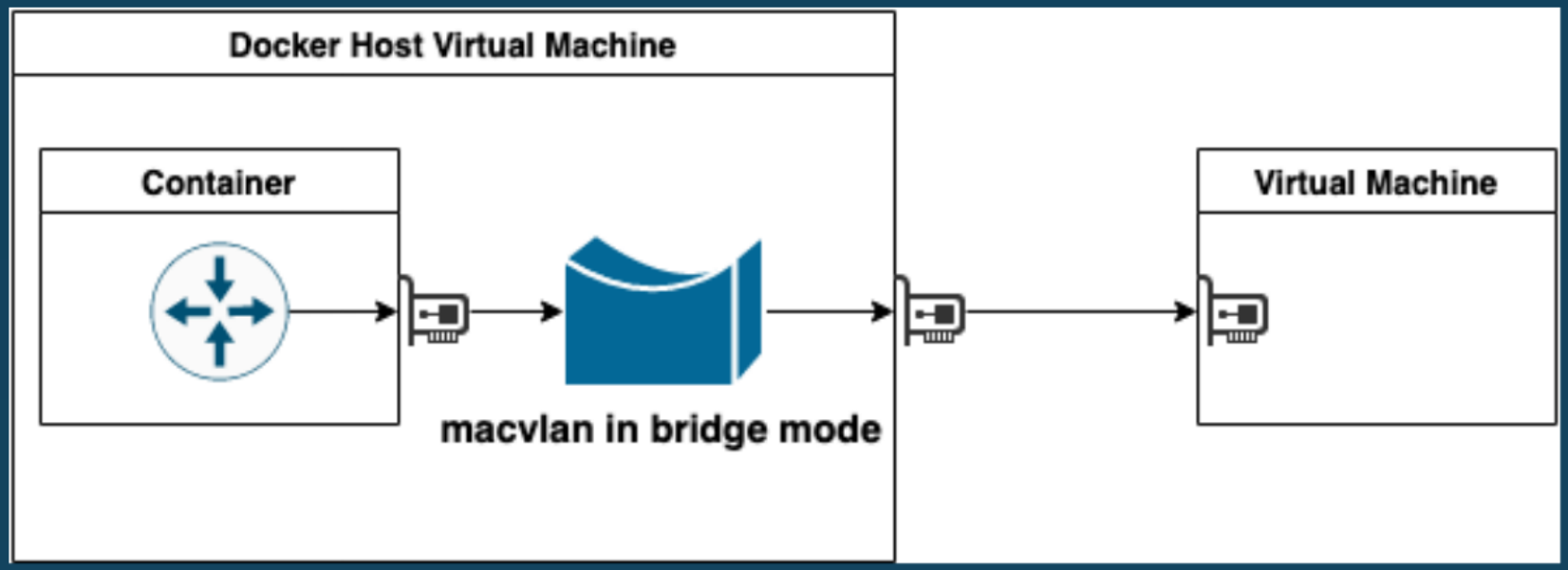
- Configuration via Infrastructure as Code tools

Containers & VMs on the same subnet

- communication via "*container as a router*"
- information hiding



Prezi


Docker Host Virtual Machine
Container
Virtual Machine
macvlan in bridge mode

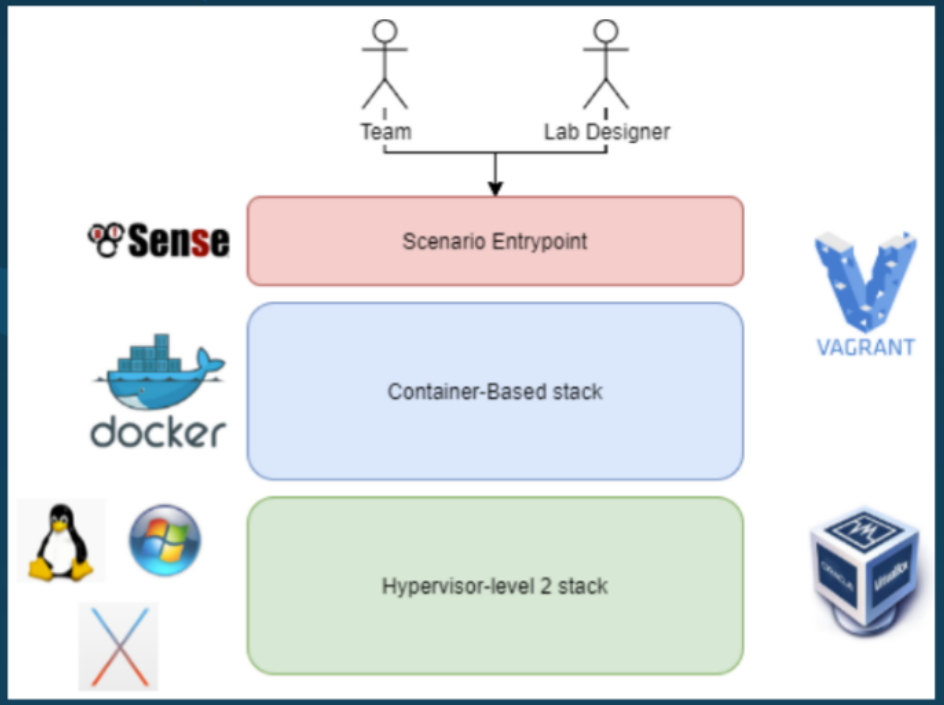
Prezi

Implementation

Cyber Effect Week event
CIOC - 10/10/2018 - 19/10/2018

http://www.difesa.it/SMD_/Eventi/Pagine/Cyber_Effect_Week_attivita_addestrativa_presso_il_CIOC.aspx

Virtual Scenario Components



VS Element	Implementation
Bare-Metal Hypervisor	Vmware ESXi Server
Hyper-V Scenario Entrypoint	PfSense Virtualbox Machine
Container-Based Stack Machine	Ubuntu 18.04 LTS Virtualbox Machine
Container-Based Stack Environment	10 vulnerable Docker containers, 3 vulnerable networks, 1 public network, 1 internal network
Level-2 Hypervisor stack	1 Windows Server 2008 (Domain Controller), 2 Windows 7, 1 Ubuntu Xenial 16.04 64 bits

Prezi

Attack Scenario Vulnerabilities

ID	Vulnerability Type	Can use Docker?
WAV	Web Application Vulnerabilities	Y
LAV	Linux-based Application Vulnerabilities	Y
SPEV	Privilege Escalation through services running with high privileges	Y
LUPEV	Linux-based User space privilege escalation	Y
MPEV	Privilege Escalation through Misconfiguration	Y
LMV	Linux Misconfiguration Vulnerabilities	Y
SV	Service Vulnerabilities	Y
NLAV	Non Linux-based Application Vulnerabilities	N
NLRV	Non Linux-based Remote Vulnerabilities	N
LKV	Linux Kernel-level Vulnerabilities	N
NLPEV	Non Linux-based Privilege Escalation Vulnerabilities	N

Can Docker reproduce the vulnerability?

Attack Scenario Vulnerabilities

Type	Vulnerability
WAV	KikChat - LFI / RCE
MPEV	passwd file World-Writable
LAV	LFI - Local File Inclusion
SPEV	Mysql UDF running as root
LAV	Wordpress Vulnerability
LUPEV	vim with bit suid
LAV	Buffer overflow in custom application
MPEV	Same password for separate users
LAV	Shellshock on User-Agent header
LAV	Bruteforce attack against a vulnerable service
SPEV	Local Webserver with root privileges
LAV	CVE-2017-5645
LKV	Dirty-Cow vulnerability
NLAV	Windows FtpShell Client Buffer Overflow
NLPEV	Pass the Hash / SMB Relay via XSS

Prezi

Attack Scenario Vulnerabilities

ID	Vulnerability Type	Can use Docker?
WAV	Web Application Vulnerabilities	Y
LAV	Linux-based Application Vulnerabilities	Y
SPEV	Privilege Escalation through services running with high privileges	Y
LUPEV	Linux-based User space privilege escalation	Y
MPEV	Privilege Escalation through Misconfiguration	Y
LMV	Linux Misconfiguration Vulnerabilities	Y
SV	Service Vulnerabilities	Y
NLAV	Non Linux-based Application Vulnerabilities	N
NLRV	Non Linux-based Remote Vulnerabilities	N
LKV	Linux Kernel-level Vulnerabilities	N
NLPEV	Non Linux-based Privilege Escalation Vulnerabilities	N

Can Docker reproduce the vulnerability?

Attack Scenario Vulnerabilities

Type	Vulnerability
WAV	KikChat - LFI / RCE
MPEV	passwd file World-Writable
LAV	LFI - Local File Inclusion
SPEV	Mysql UDF running as root
LAV	Wordpress Vulnerability
LUPEV	vim with bit suid
LAV	Buffer overflow in custom application
MPEV	Same password for separate users
LAV	Shellshock on User-Agent header
LAV	Bruteforce attack against a vulnerable service

Prezi

ID	Vulnerability Type	Can use Docker?
WAV	Web Application Vulnerabilities	Y
LAV	Linux-based Application Vulnerabilities	Y
SPEV	Privilege Escalation through services running with high privileges	Y
LUPEV	Linux-based User space privilege escalation	Y
MPEV	Privilege Escalation through Misconfiguration	Y
LMV	Linux Misconfiguration Vulnerabilities	Y
SV	Service Vulnerabilities	Y
NLAV	Non Linux-based Application Vulnerabilities	N
NLRV	Non Linux-based Remote Vulnerabilities	N
LKV	Linux Kernel-level Vulnerabilities	N
NLPEV	Non Linux-based Privilege Escalation Vulnerabilities	N

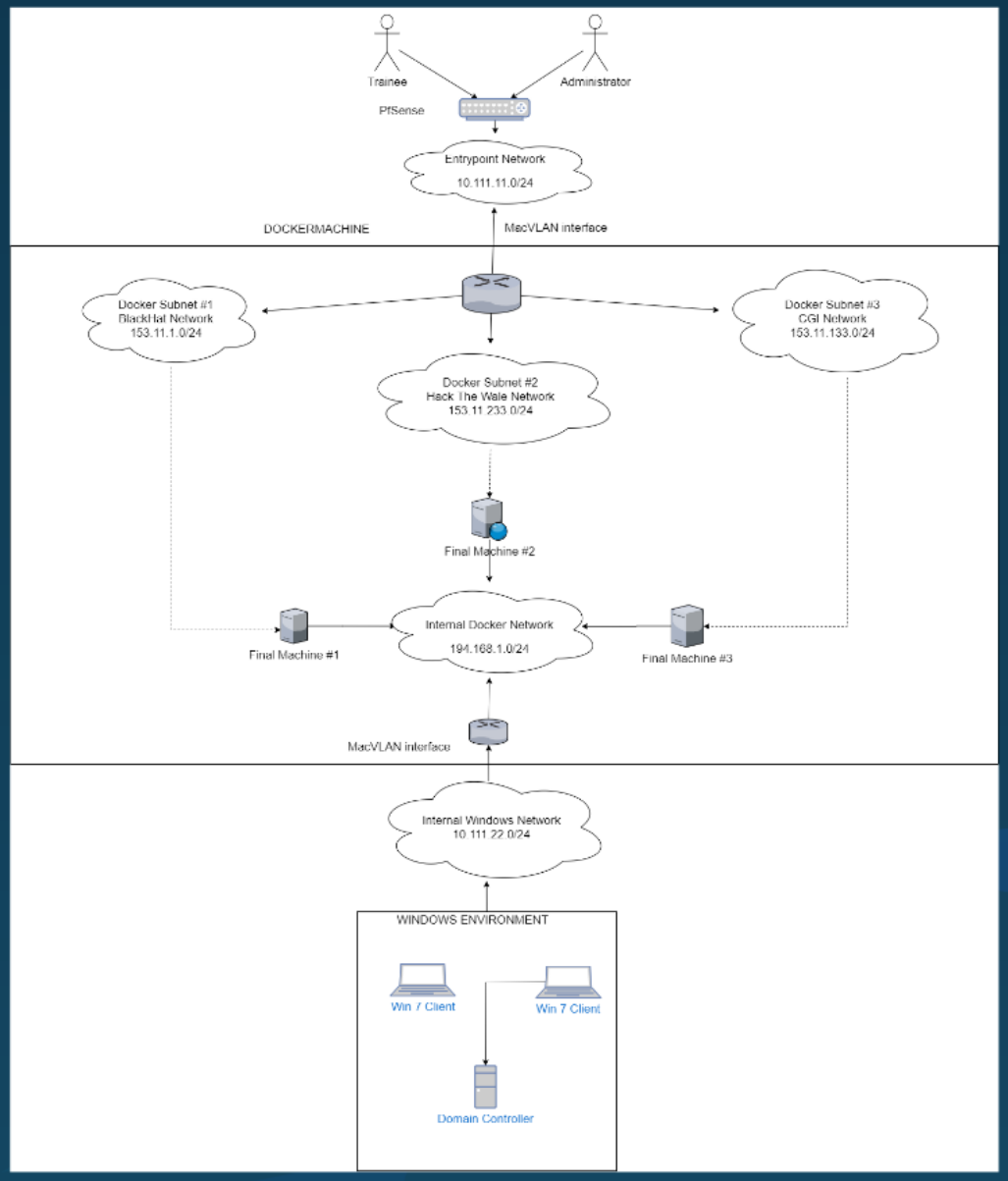
Can Docker reproduce the vulnerability?

Attack Scenario Vulnerabilities

Type	Vulnerability
WAV	KikChat - LFI / RCE
MPEV	passwd file World-Writable
LAV	LFI - Local File Inclusion
SPEV	Mysql UDF running as root
LAV	Wordpress Vulnerability
LUPEV	vim with bit suid
LAV	Buffer overflow in custom application
MPEV	Same password for separate users
LAV	Shellshock on User-Agent header
LAV	Bruteforce attack against a vulnerable service
SPEV	Local Webserver with root privileges
LAV	CVE-2017-5645
LKV	Dirty-Cow vulnerability
NLAV	Windows FtpShell Client Buffer Overflow
NLPEV	Pass the Hash / SMB Relay via XSS

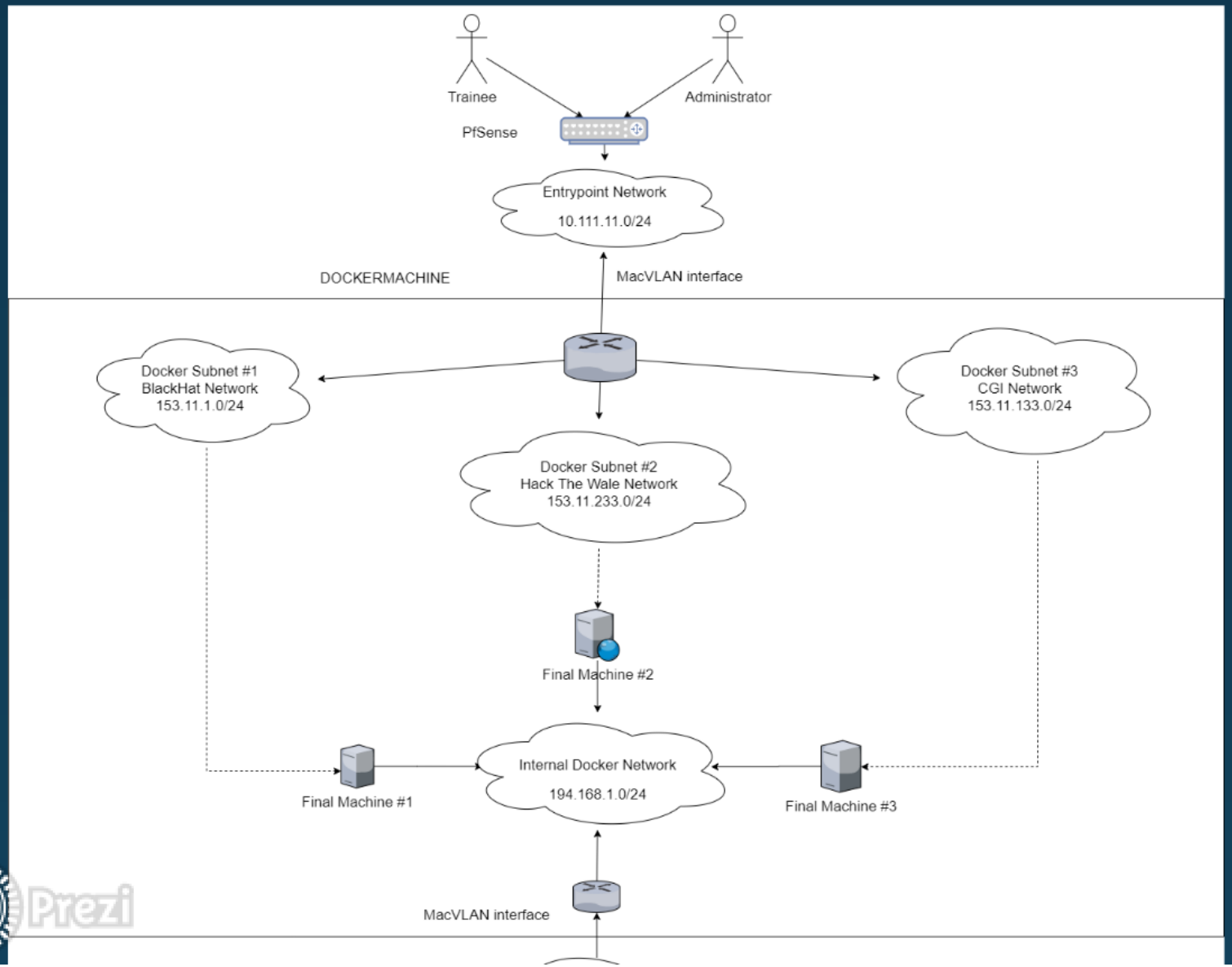
Prezi

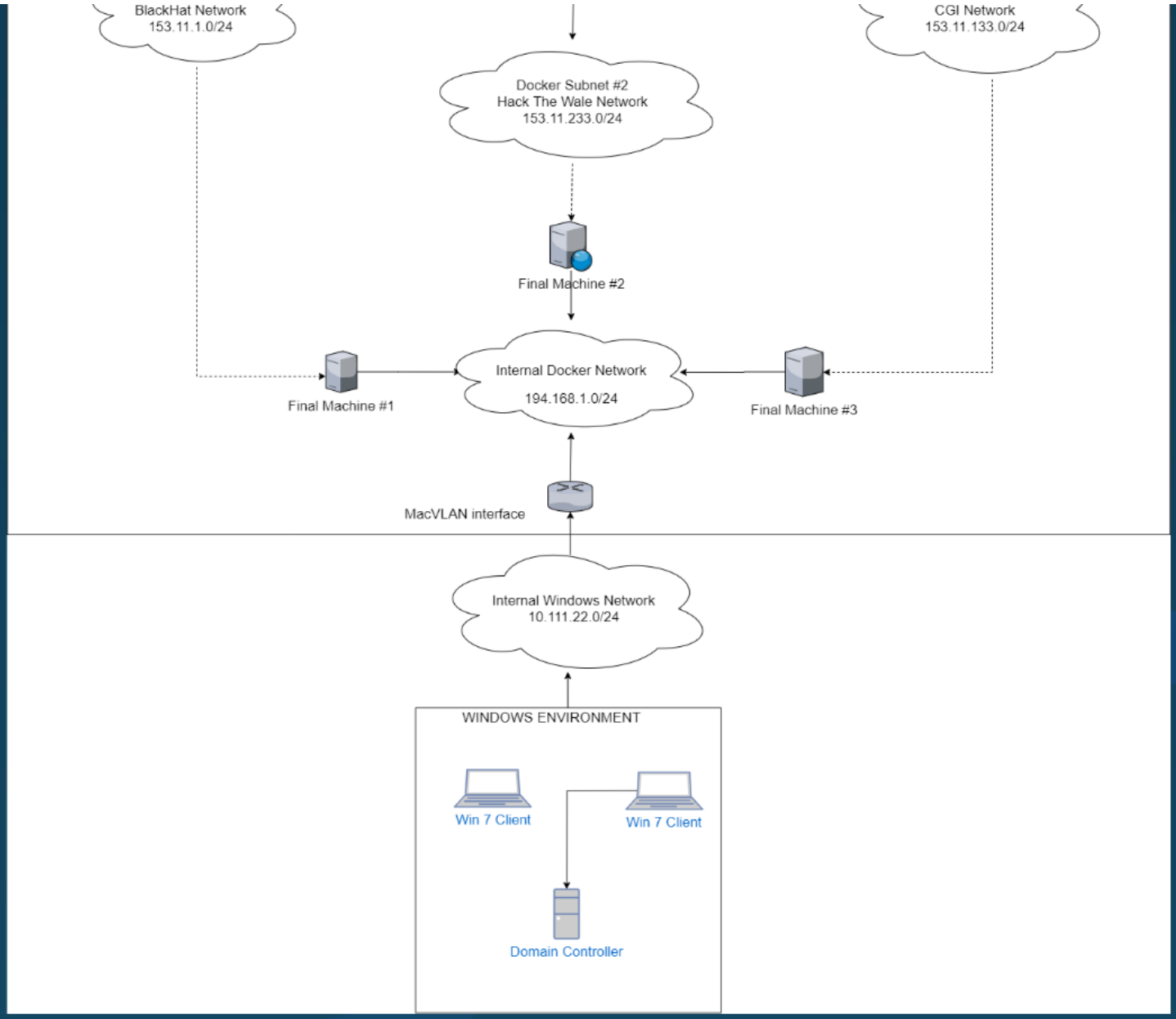
Scenario Implementation



Prezi

Scenario Implementation




BlackHat Network
153.11.1.0/24
CGI Network
153.11.133.0/24
Docker Subnet #2
Hack The Wale Network
153.11.233.0/24
Final Machine #2
Internal Docker Network
194.168.1.0/24
Final Machine #1
Final Machine #3
MacVLAN interface
Internal Windows Network
10.111.22.0/24
WINDOWS ENVIRONMENT
Win 7 Client
Win 7 Client
Domain Controller

Prezi

Conclusions

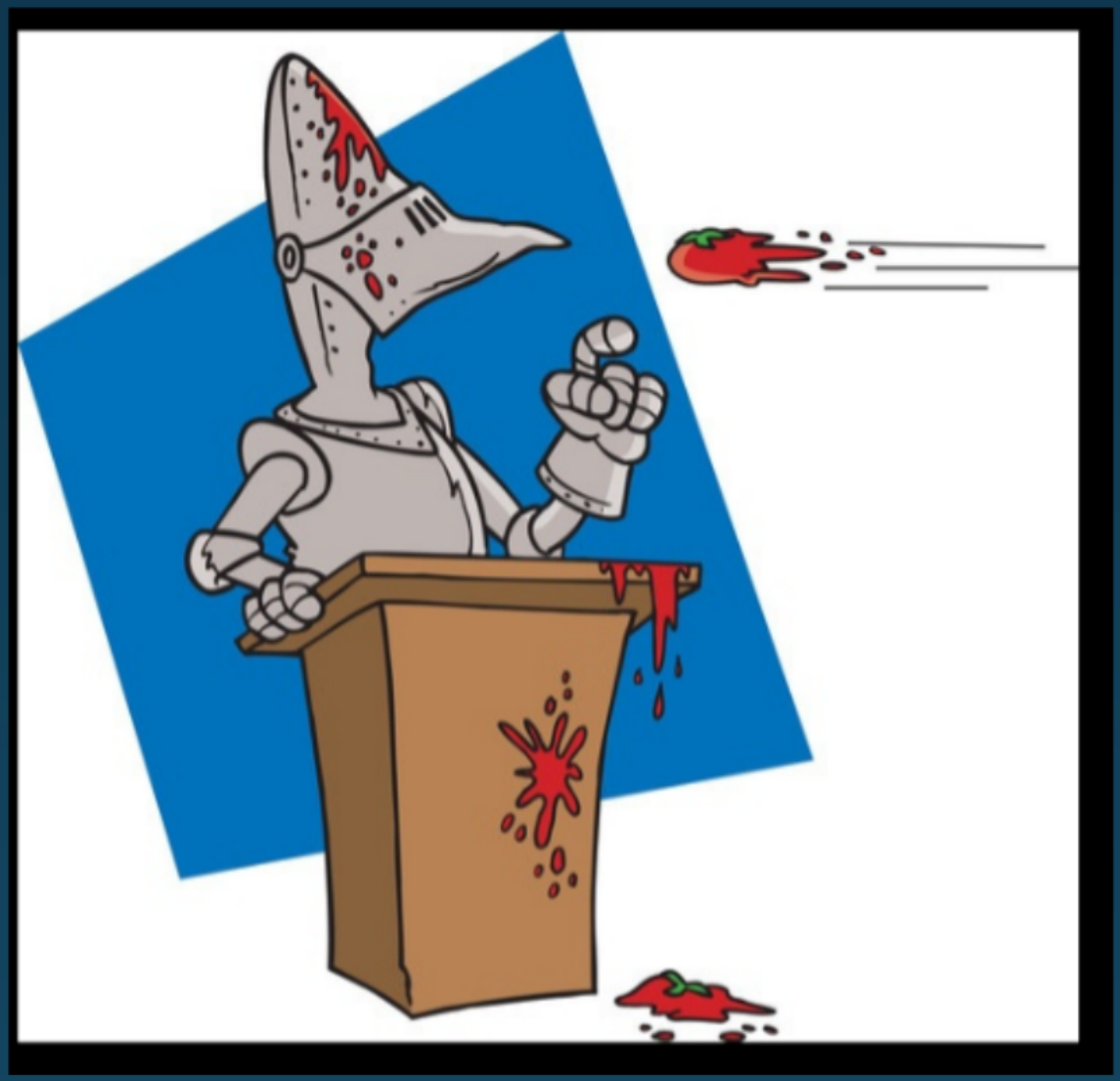
- *An hybrid virtualization approach to create complex attack-scenarios*
- *Obtain OS-level virtualization benefits without losing in terms of vulnerability replicability*

Future Work

- *Docker Windows Exploration*
- *Vulnerable lab Infrastructure as Code descriptor*

Prezi

Questions?



Prezi

References

- [1]. N.Childers, B.Boe, L.Cavallaro, L.Cavedon, M.Cova, M.Egele, andG.Vigna, 2010, July. "Organizing large scale hacking competitions." InInternational Conference on Detection of Intrusions and Malware, andVulnerability Assessment (pp. 132-152). Springer, Berlin, Heidelberg.
- [2]. A.S.Raj, B.Alangot, S.Prabhu and K.Achuthan."Scalable andLightweight CTF Infrastructures Using Application Containers" (Pre-recorded Presentation). In 2016 USENIX Workshop on Advances inSecurity Education (ASE 16)
- [3]. Chandra and P.K.Mishra. "Design of cyber warfare testbed". InSoftware Engineering (pp. 249 256). Springer, Singapore, 2019.

Prezi

Contacts

- francesco.caturano@unina.it
- g.per45@gmail.com
- spromano@unina.it

Prezi