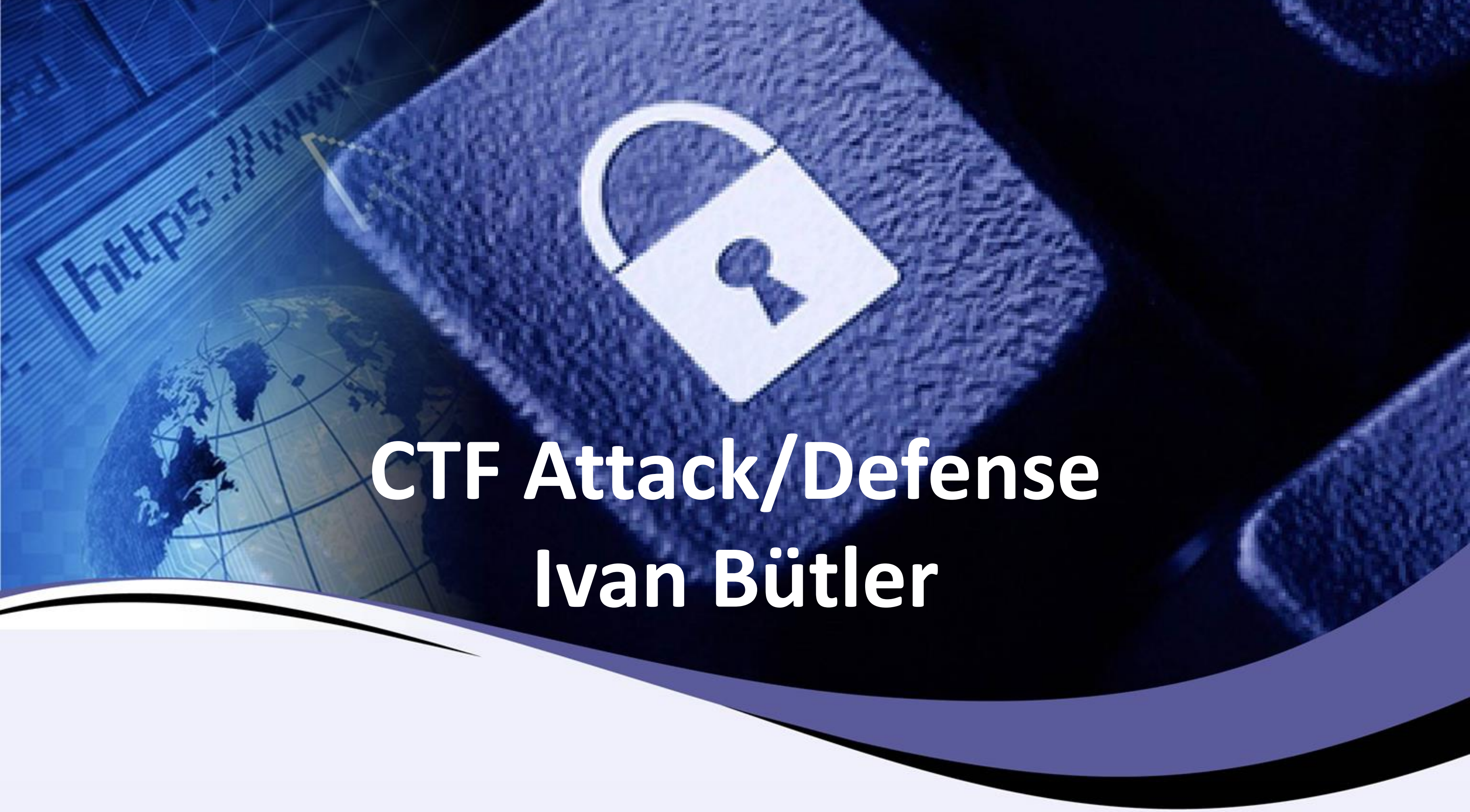


CTF Attack/Defense
Ivan Bütler

https://www.owasp.org/index.php/OWASP_University_Challenge

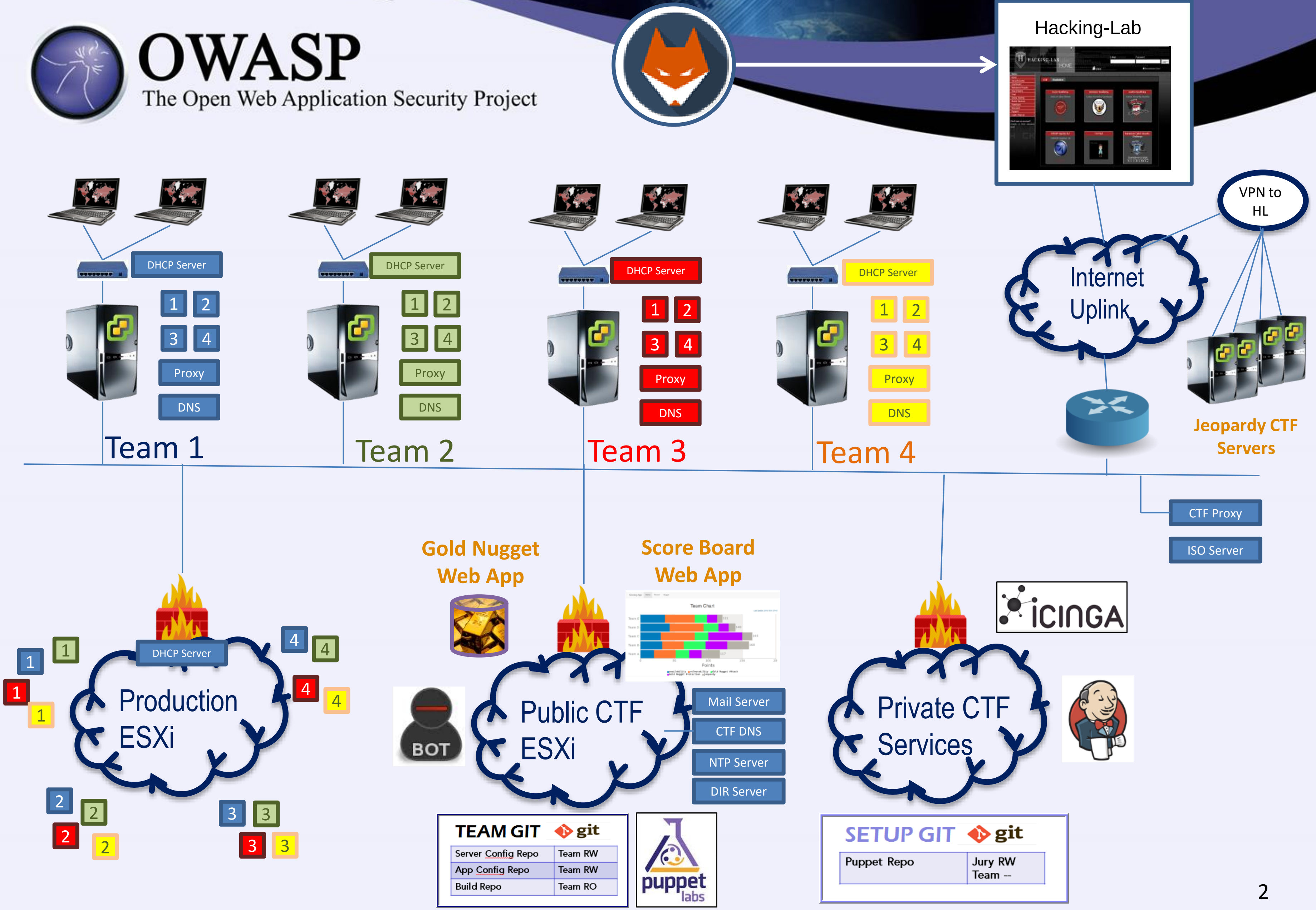
OWASP
The Open Web Application Security Project

ivan.buetler@owasp.org

CTF Architecture

OWASP
The Open Web Application Security Project

Mobile CTF App



Hacking-Lab

VPN to HL

Internet Uplink

Jeopardy CTF Servers

DHCP Server
1 2
3 4
Proxy
DNS
Team 1

DHCP Server
1 2
3 4
Proxy
DNS
Team 2

DHCP Server
1 2
3 4
Proxy
DNS
Team 3

DHCP Server
1 2
3 4
Proxy
DNS
Team 4

CTF Proxy

ISO Server

Gold Nugget Web App

Score Board Web App

DHCP Server

Production ESXi

BOT

Public CTF ESXi

Mail Server

CTF DNS

NTP Server

DIR Server

Private CTF Services

ICINGA

TEAM GIT git

Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

puppet labs

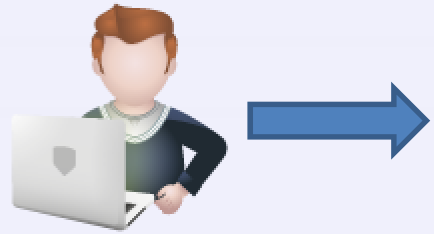
SETUP GIT git

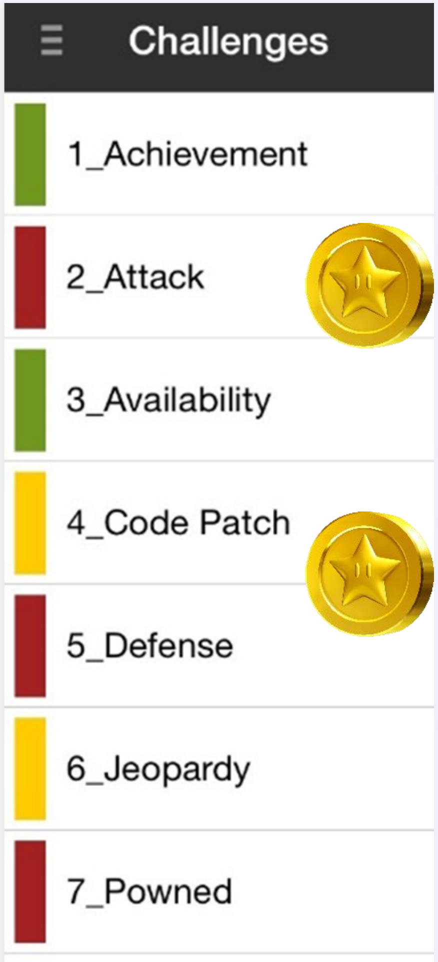
Puppet Repo	Jury RW Team --

CTF Tasks

OWASP
The Open Web Application Security Project

CTF Tasks





☰ Challenges

- 🟩 1_Achievement
- 🟥 2_Attack
- 🟩 3_Availability
- 🟨 4_Code Patch
- 🟥 5_Defense
- 🟨 6_Jeopardy
- 🟥 7_Powned

Setup and maintain a service like DNS, Proxy, E-Mail, Apache, WordPress, …

Hack in other CTF team servers and services and steal the gold nugget (EXPLOITATION)

Keep own services up and running (IT OPS)

Fix vulnerable software & services (IT DEV)

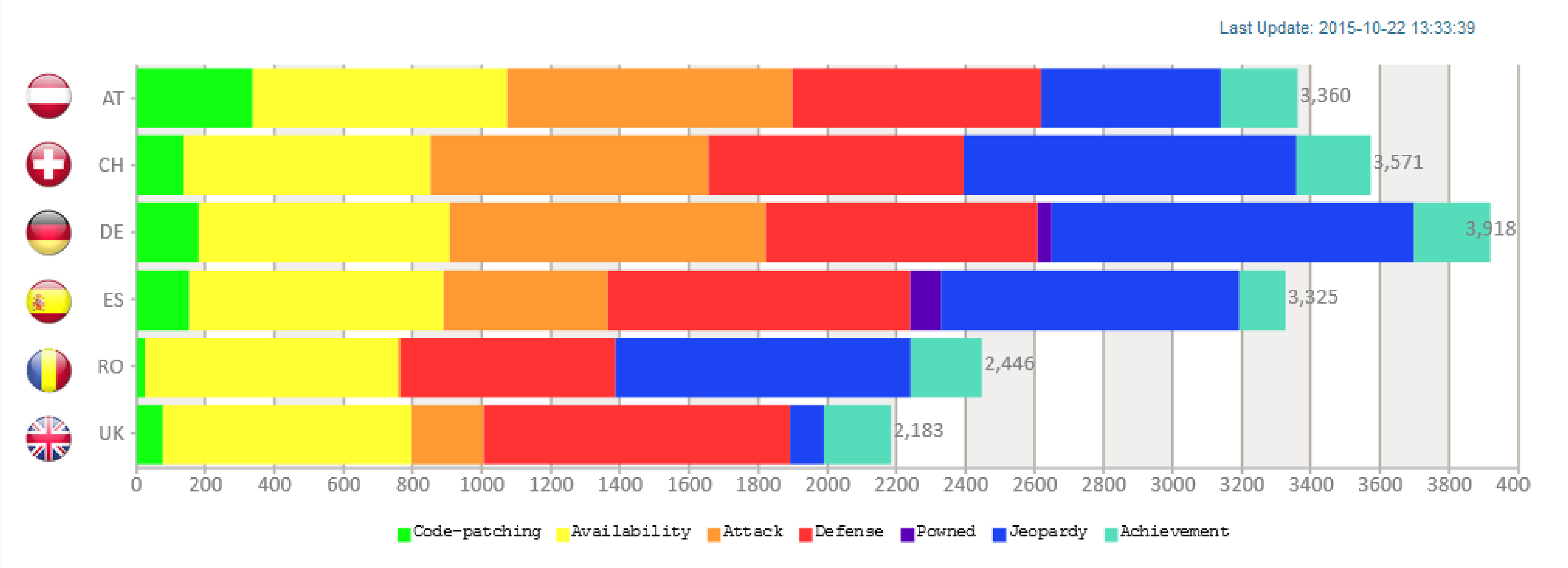
Safe guard own gold nuggets

Solving jeopardy challenges

Own a device/server and prove the attack by leaving a special gold nugget, known as evidence nugget (0-day)

Scoring

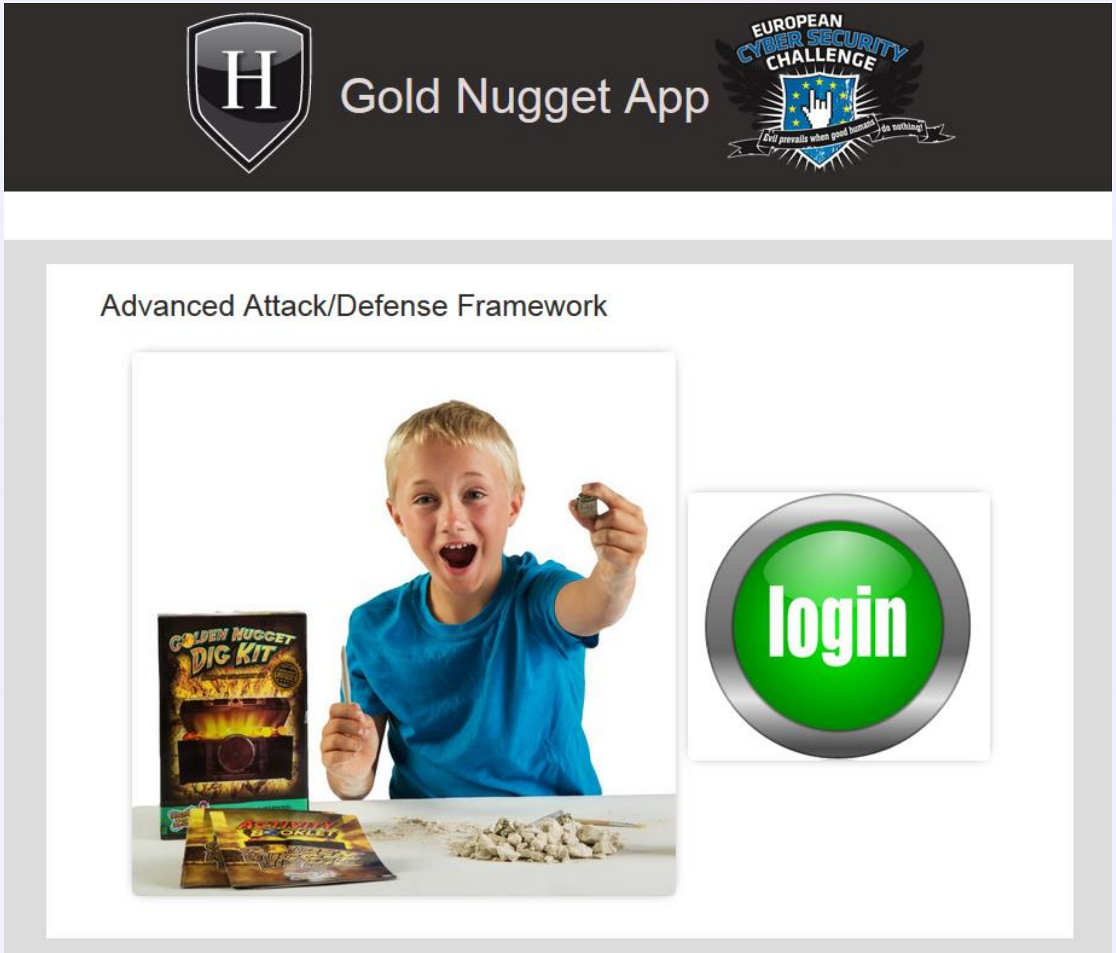
- Scoring Application



The CTF Glue

CTF players must find/hack/disclose a string, known as gold nugget, from the 'vulnerable' services of the other teams

The purpose of the gold nugget is to claim points for a successful attack



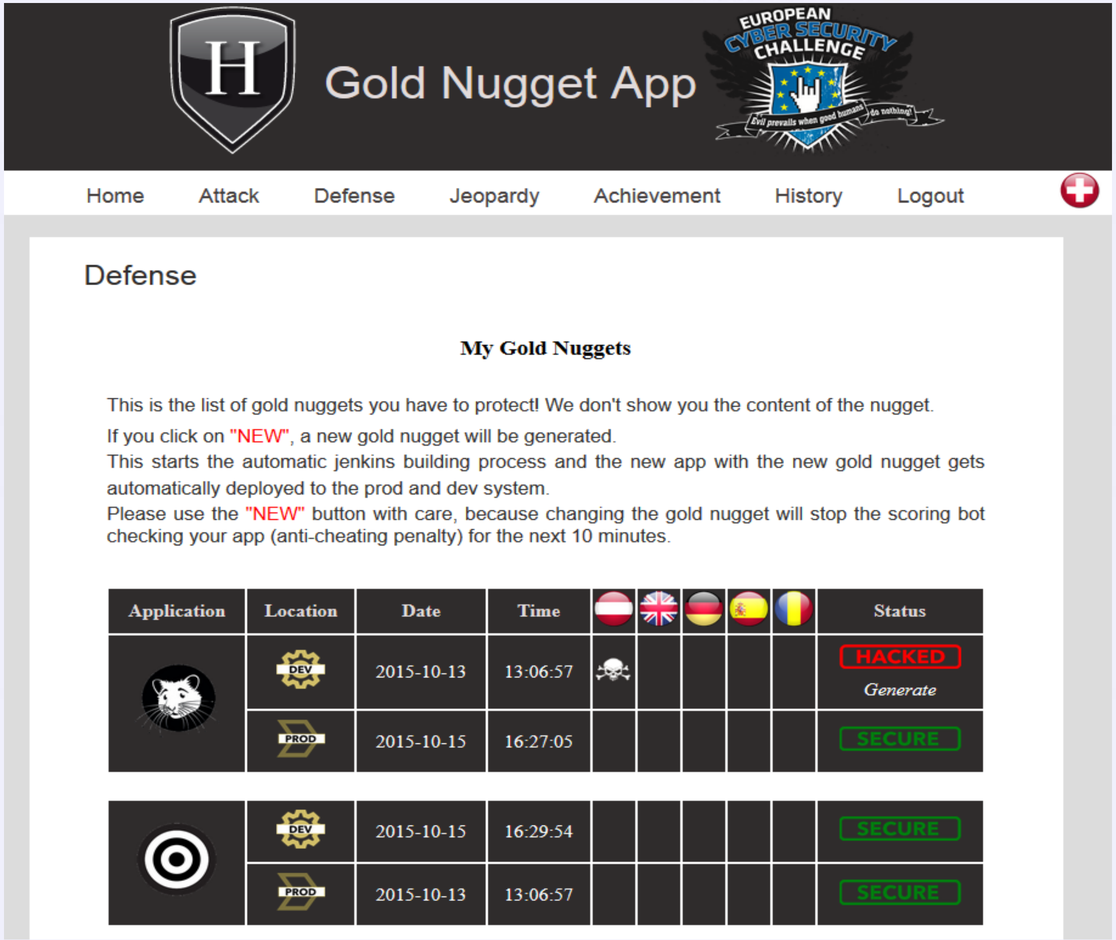
Gold Nugget App

Advanced Attack/Defense Framework

H
EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!
GOLDEN NUGGET DIG KIT
login

The CTF Glue Gold Nuggets

Gold Nuggets are digitally signed strings. The gold nugget app is issuing them. The gold nugget app knows, who owns which gold nugget


H
Gold Nugget App
EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!
Home
Attack
Defense
Jeopardy
Achievement
History
Logout

Defense

My Gold Nuggets

This is the list of gold nuggets you have to protect! We don't show you the content of the nugget.

If you click on "NEW", a new gold nugget will be generated.
This starts the automatic jenkins building process and the new app with the new gold nugget gets automatically deployed to the prod and dev system.
Please use the "NEW" button with care, because changing the gold nugget will stop the scoring bot checking your app (anti-cheating penalty) for the next 10 minutes.

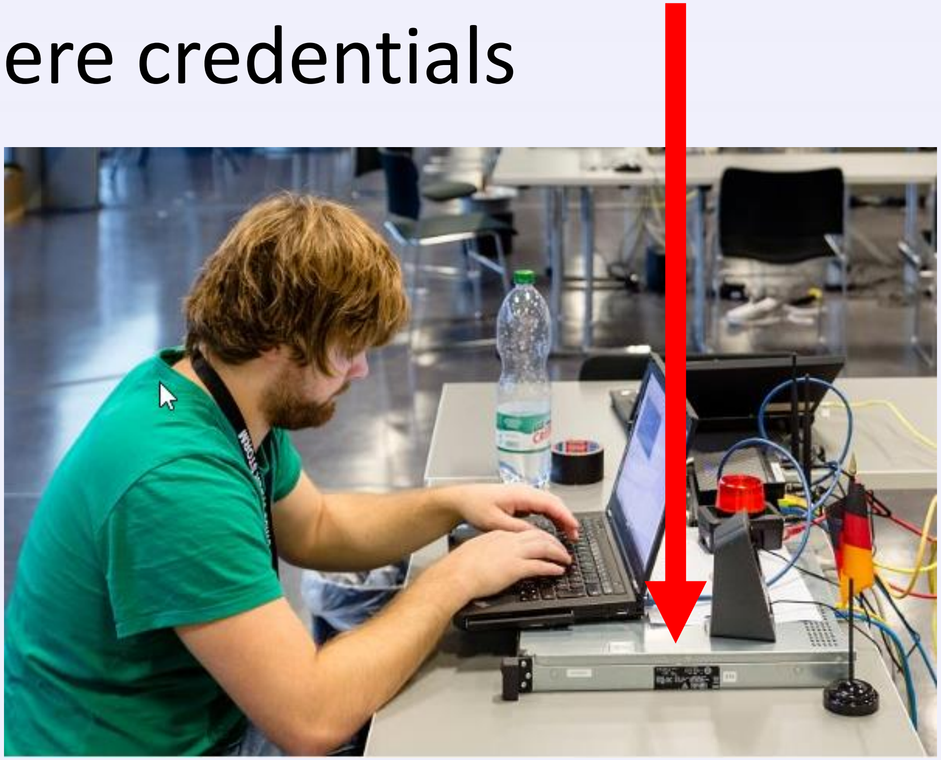
Application	Location	Date	Time						Status
	DEV	2015-10-13	13:06:57	☠					HACKED Generate
	PROD	2015-10-15	16:27:05						SECURE
	DEV	2015-10-15	16:29:54						SECURE
	PROD	2015-10-13	13:06:57						SECURE

Team ESX = DEV SYSTEM

OWASP
The Open Web Application Security Project

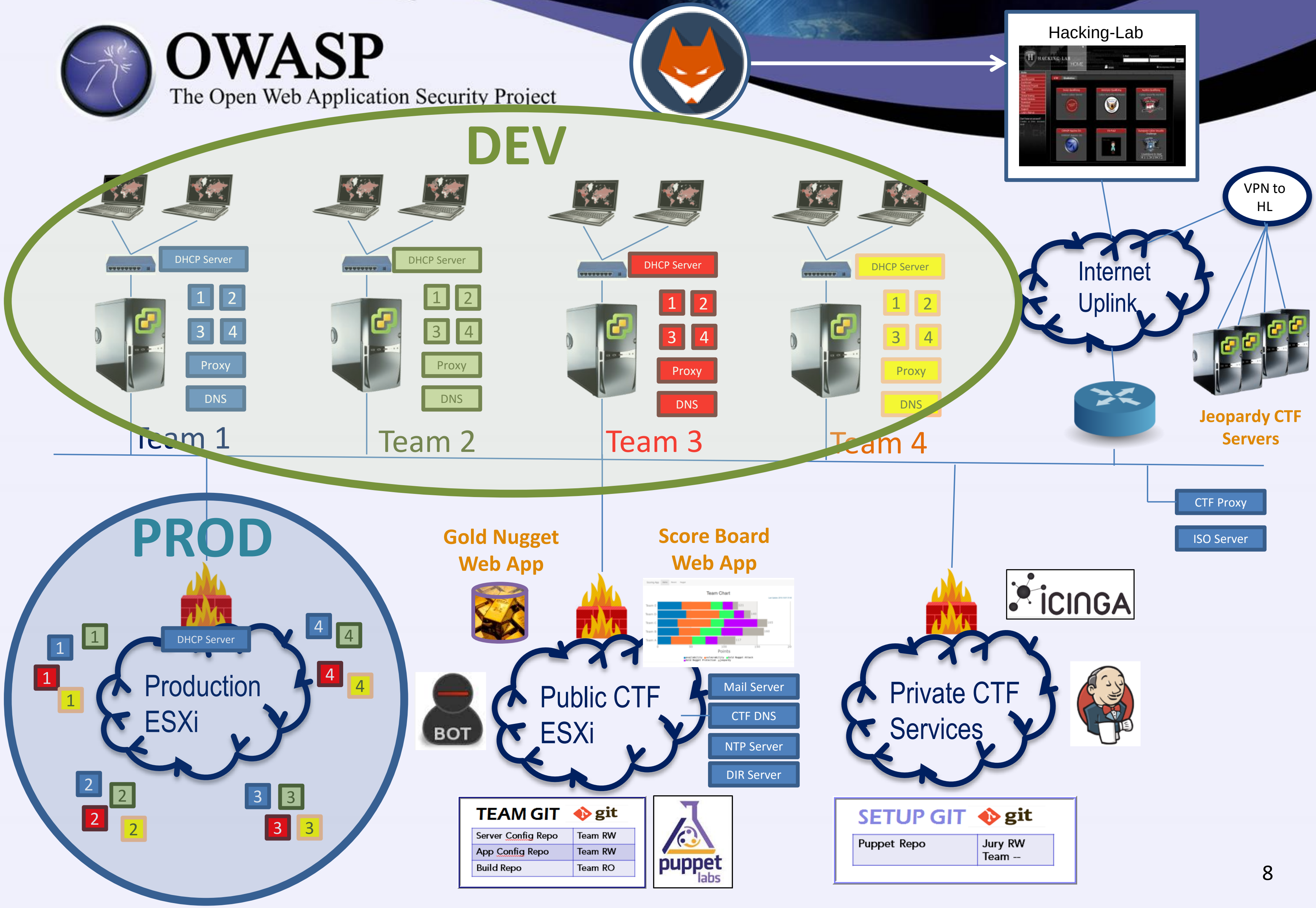
- Every CTF team gets a physical server (ESXi) and the proper vSphere credentials

- The ESXi is pre-configured with several pre-installed VM’s



- The team ESXi is named as “**DEV**” system

CTF Architecture



OWASP

The Open Web Application Security Project

Mobile CTF App

Hacking-Lab

VPN to HL

Internet Uplink

Jeopardy CTF Servers

CTF Proxy

ISO Server

DEV

Team 1: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 2: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 3: DHCP Server, 1, 2, 3, 4, Proxy, DNS

Team 4: DHCP Server, 1, 2, 3, 4, Proxy, DNS

PROD

DHCP Server

Production ESXi

1 1 1 1 2 2 2 2 3 3 3 3 4 4 4 4

Gold Nugget Web App

Score Board Web App

BOT

Public CTF ESXi

Mail Server

CTF DNS

NTP Server

DIR Server

Private CTF Services

ICINGA

TEAM GIT git

Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

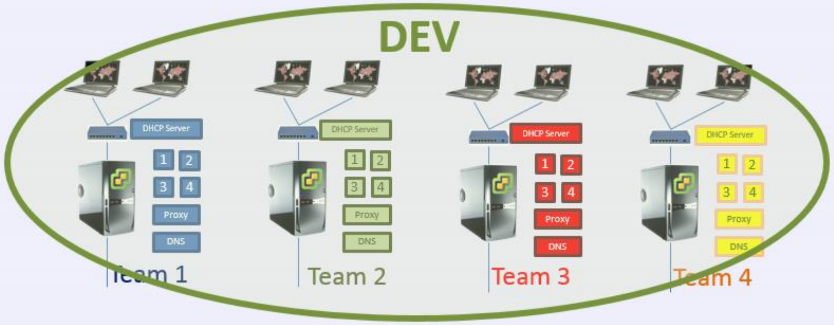
puppet labs

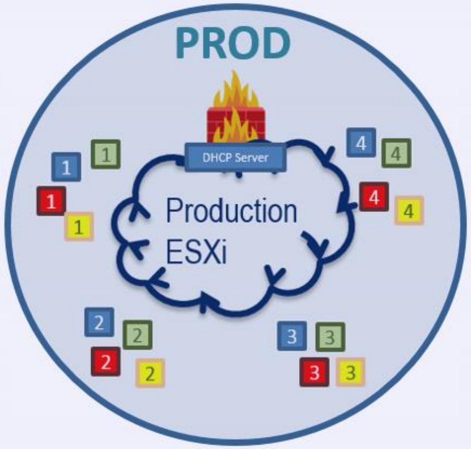
SETUP GIT git

Puppet Repo	Jury RW Team --

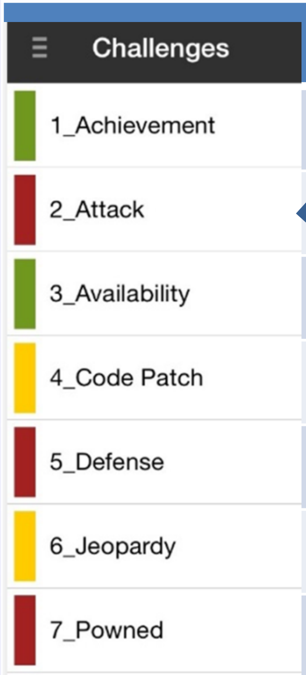
Production ESXi

- The apps on **DEV** is ‘equal’ or ‘identical’ as on **PROD**
- On **DEV**, teams have root access (SSH)
- On **PROD** teams do *NOT* have root or interactive access





Attacking



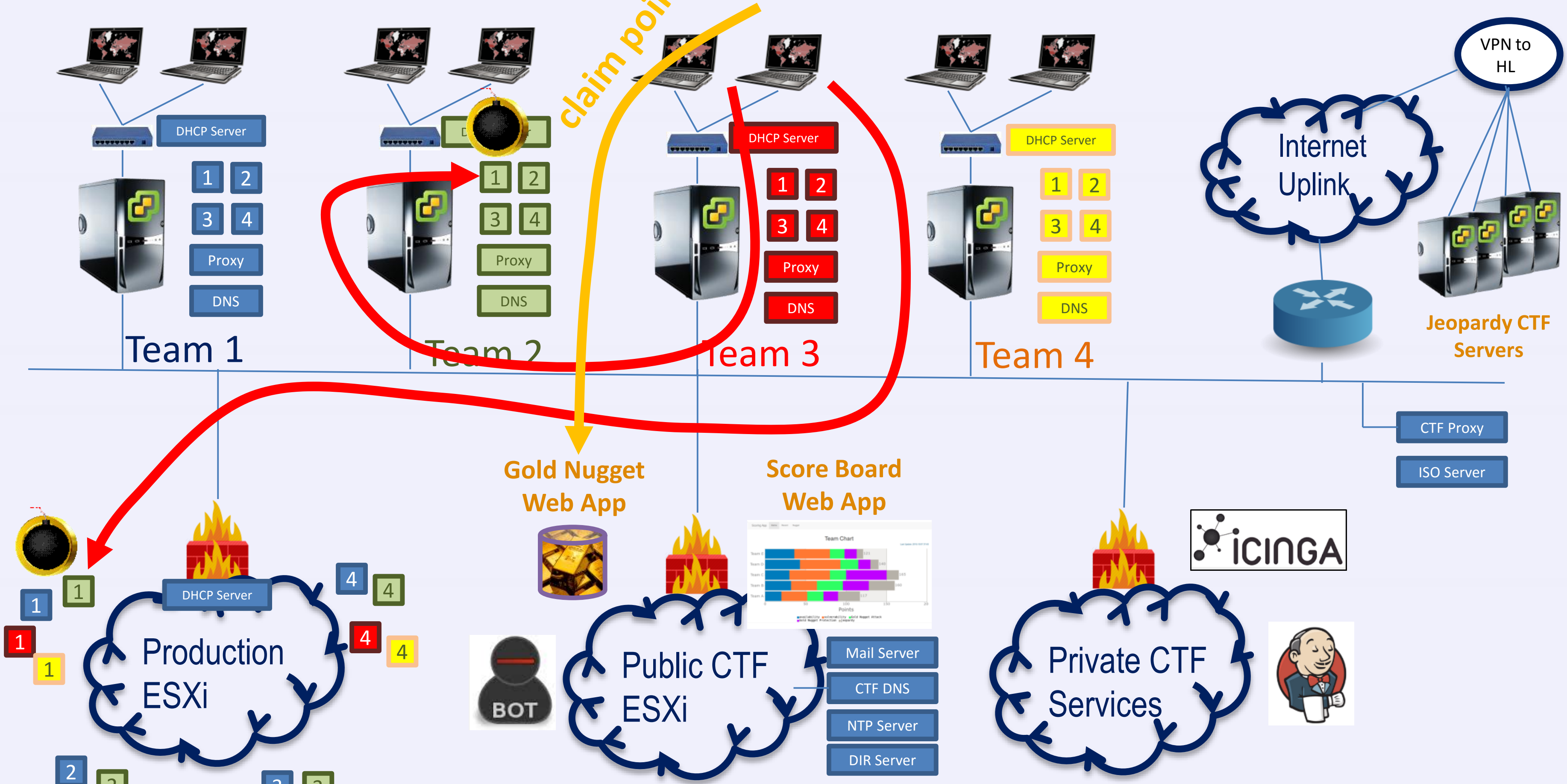
☰ Challenges	
🟩 1_Achievement	
🟥 2_Attack ⇦	Stealing Gold Nugget
🟩 3_Availability	
🟨 4_Code Patch	
🟥 5_Defense	
🟨 6_Jeopardy	
🟥 7_Powned	

Attacking

- Every team is allowed to attack other teams on the **DEV** or **PROD** environment
- On success, the attacking team discloses the gold nugget from the victim team
- The gold nugget is different in **DEV** and **PROD** for any team and app (every gold nugget is unique)
- The gold nugget must be used to claim points using the gold nugget app

Attacking

OWASP
The Open Web Application Security Project



TEAM GIT git

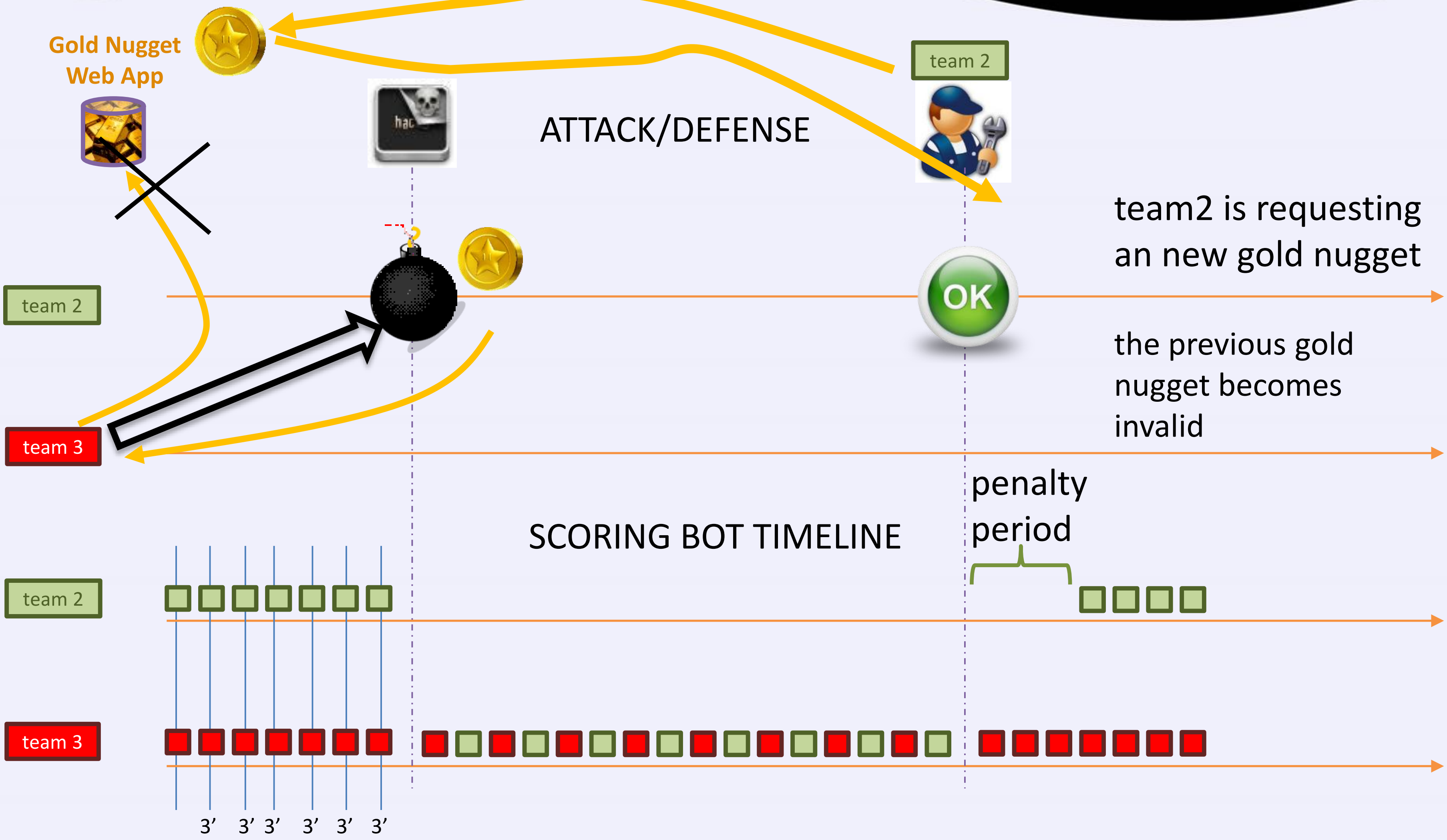
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

puppet labs

SETUP GIT git

Puppet Repo	Jury RW Team --

Scoring per Time Unit



Gold Nugget Web App

team 2

ATTACK/DEFENSE

team2 is requesting an new gold nugget

team 2

team 3

the previous gold nugget becomes invalid

penalty period

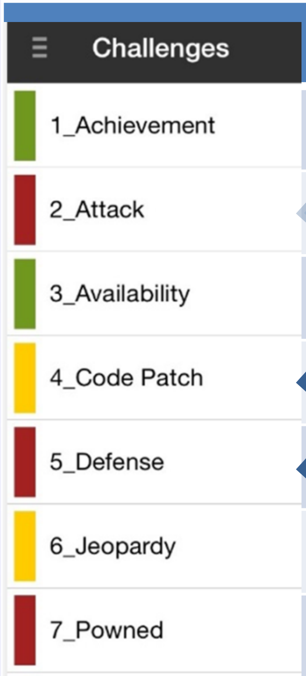
SCORING BOT TIMELINE

team 2

team 3

3’ 3’ 3’ 3’ 3’ 3’

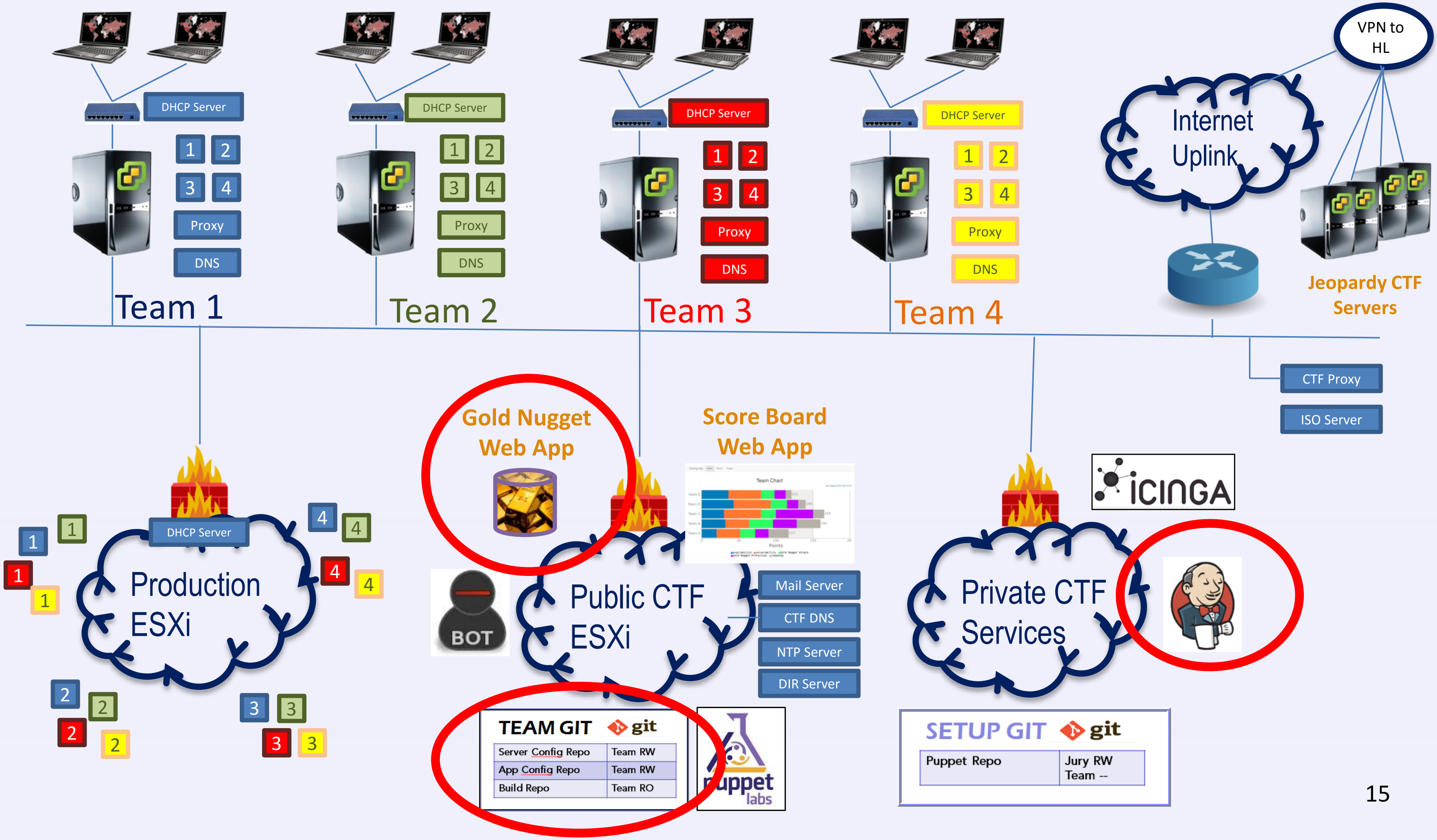
Fixing Vulnerable Apps



☰ Challenges		
🟩 1_Achievement		
🟥 2_Attack	⇦	Stealing Gold Nugget
🟩 3_Availability		
🟨 4_Code Patch	⇦	Fix vulnerable software & services
🟥 5_Defense	⇦	Safe guard own gold nuggets
🟨 6_Jeopardy		
🟥 7_Powned		

Fixing vulnerable apps

OWASP
The Open Web Application Security Project



VPN to HL

Internet Uplink

Jeopardy CTF Servers

DHCP Server
1 2
3 4
Proxy
DNS
Team 1

DHCP Server
1 2
3 4
Proxy
DNS
Team 2

DHCP Server
1 2
3 4
Proxy
DNS
Team 3

DHCP Server
1 2
3 4
Proxy
DNS
Team 4

CTF Proxy
ISO Server

Production ESXi
DHCP Server
1 1 1 1
2 2 2 2
3 3 3 3
4 4 4 4

Gold Nugget Web App

Score Board Web App

BOT

Public CTF ESXi

Mail Server
CTF DNS
NTP Server
DIR Server

iCINGA

Private CTF Services

TEAM GIT git

Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

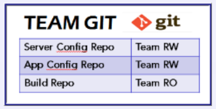
puppet labs

SETUP GIT git

Puppet Repo	Jury RW Team --

Fixing vulnerable apps

- Teams have access to the source code of the vulnerable apps



TEAM GIT git

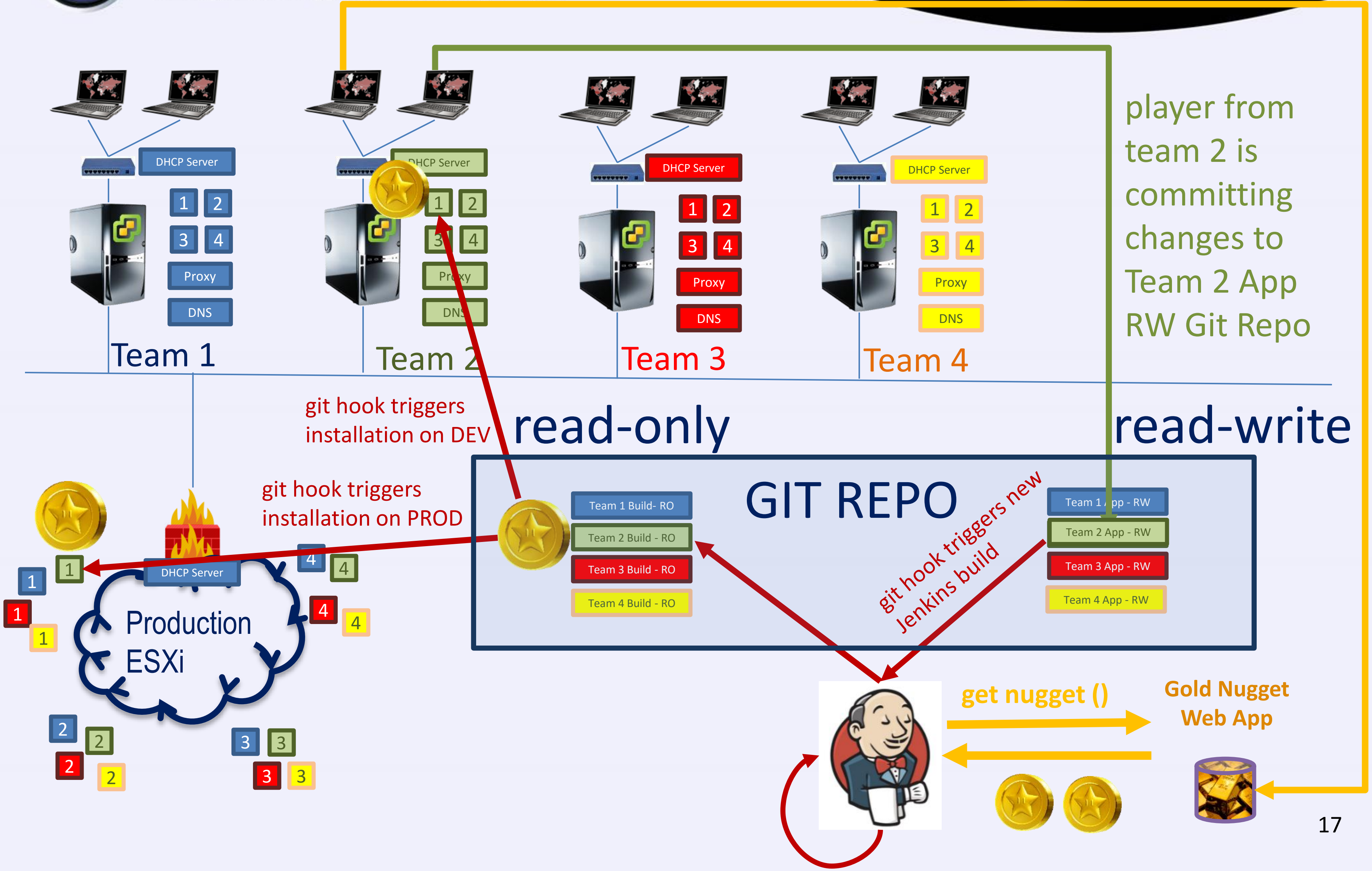
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

- Teams must fix the vulnerabilities and commit changes to the source code repository = GIT
- The Jenkins-based building infrastructure is building the new release of the app
- The Jenkins-based building infrastructure is packaging the current team's gold nugget into the new release
- The building infrastructure is automatically deploying the new app to DEV and PROD

Fixing vulnerable apps

OWASP
The Open Web Application Security Project

player is issueing a new gold nugget for App 01 of team 2



player from team 2 is committing changes to Team 2 App RW Git Repo

Team 1
DHCP Server
1 2 3 4
Proxy
DNS

Team 2
DHCP Server
1 2 3 4
Proxy
DNS

Team 3
DHCP Server
1 2 3 4
Proxy
DNS

Team 4
DHCP Server
1 2 3 4
Proxy
DNS

git hook triggers installation on DEV

git hook triggers installation on PROD

read-only

read-write

GIT REPO

Team 1 Build- RO
Team 2 Build - RO
Team 3 Build - RO
Team 4 Build - RO

Team 1 App - RW
Team 2 App - RW
Team 3 App - RW
Team 4 App - RW

git hook triggers new Jenkins build

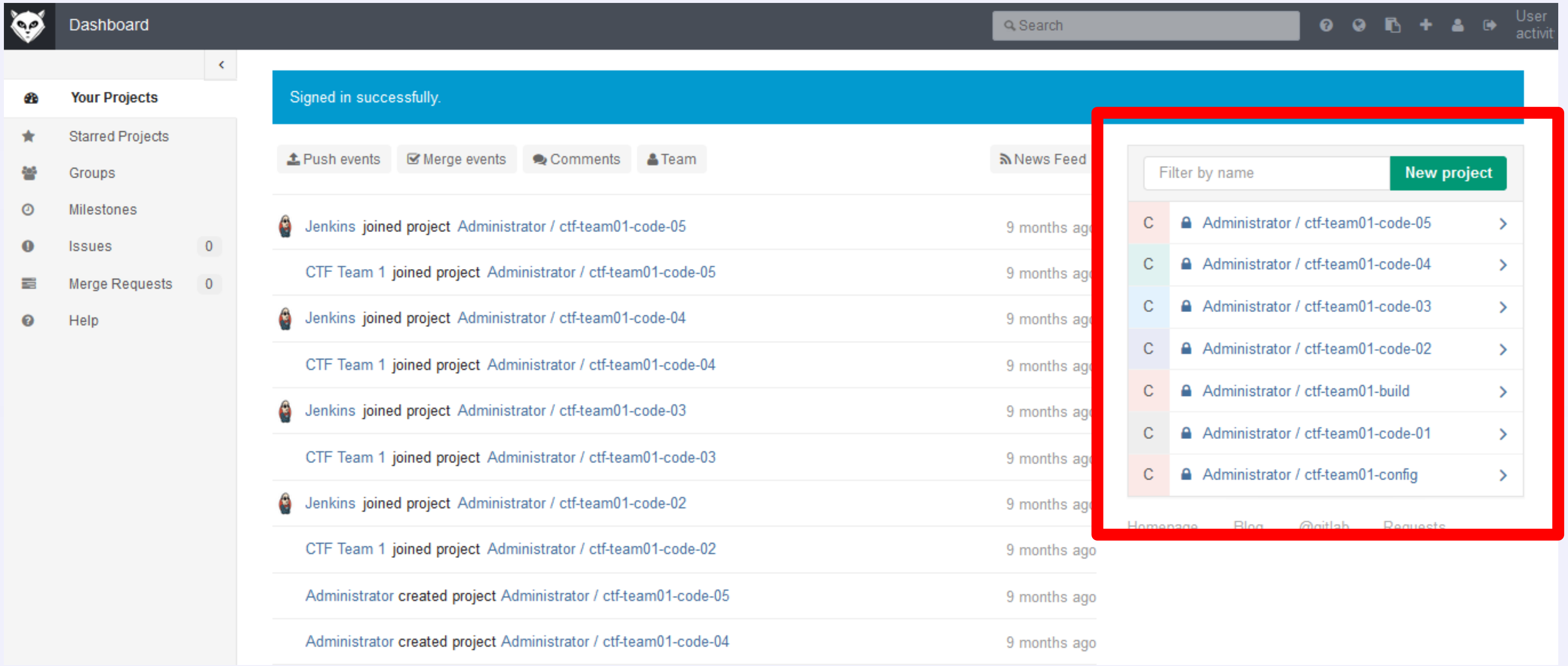
DHCP Server

Production ESXi

get nugget ()

Gold Nugget Web App

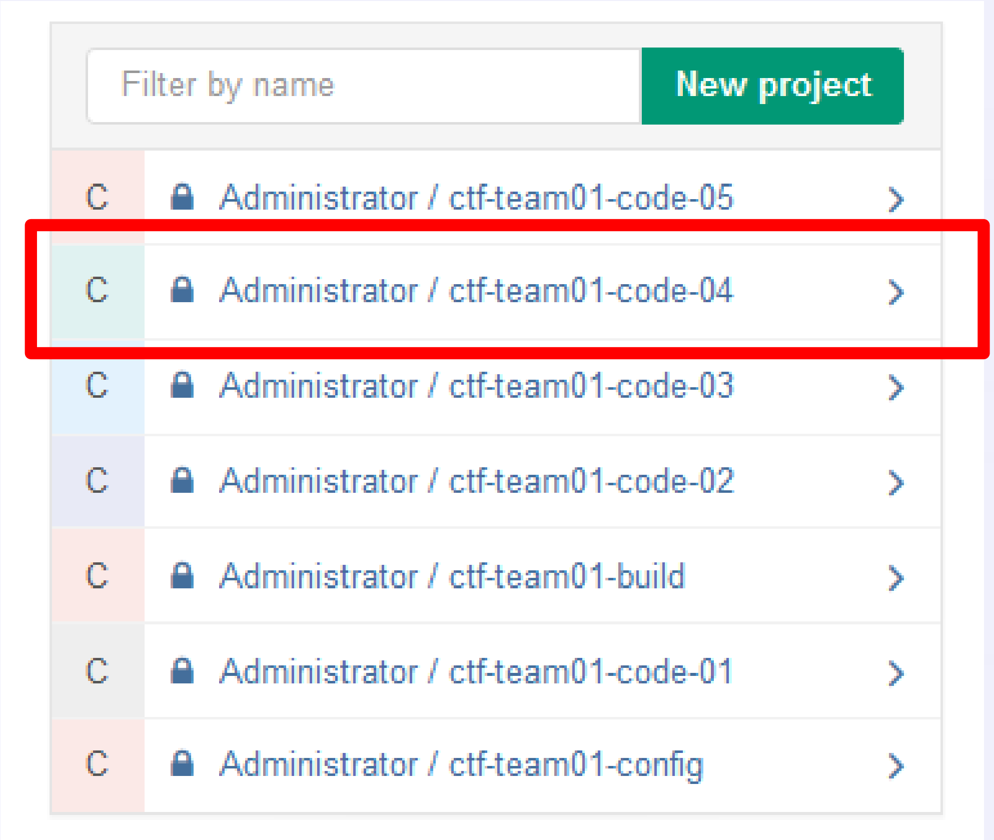
teamgit.hacking-lab.com



Signed in successfully.

Jenkins joined project Administrator / ctf-team01-code-05 9 months ago
CTF Team 1 joined project Administrator / ctf-team01-code-05 9 months ago
Jenkins joined project Administrator / ctf-team01-code-04 9 months ago
CTF Team 1 joined project Administrator / ctf-team01-code-04 9 months ago
Jenkins joined project Administrator / ctf-team01-code-03 9 months ago
CTF Team 1 joined project Administrator / ctf-team01-code-03 9 months ago
Jenkins joined project Administrator / ctf-team01-code-02 9 months ago
CTF Team 1 joined project Administrator / ctf-team01-code-02 9 months ago
Administrator created project Administrator / ctf-team01-code-05 9 months ago
Administrator created project Administrator / ctf-team01-code-04 9 months ago

C Administrator / ctf-team01-code-05
C Administrator / ctf-team01-code-04
C Administrator / ctf-team01-code-03
C Administrator / ctf-team01-code-02
C Administrator / ctf-team01-build
C Administrator / ctf-team01-code-01
C Administrator / ctf-team01-config



C Administrator / ctf-team01-code-05

C Administrator / ctf-team01-code-04

C Administrator / ctf-team01-code-03

C Administrator / ctf-team01-code-02

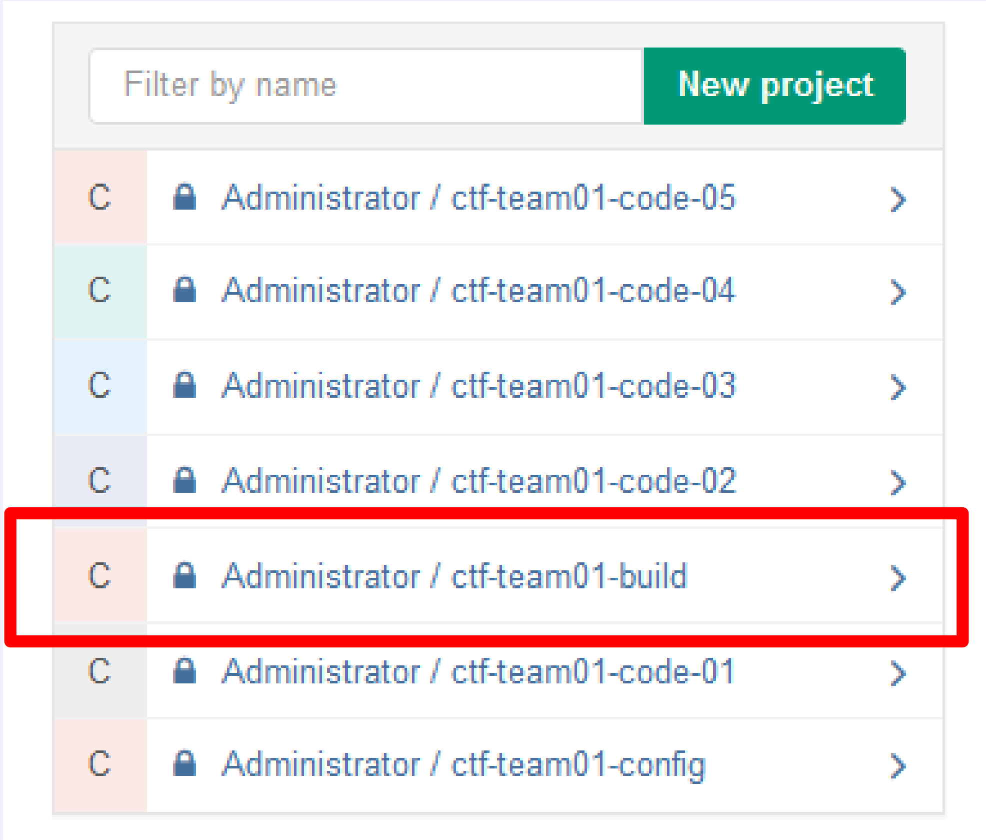
C Administrator / ctf-team01-build

C Administrator / ctf-team01-code-01

C Administrator / ctf-team01-config

source repo

commit
triggers
build



C 🔒 Administrator / ctf-team01-code-05 ›

C 🔒 Administrator / ctf-team01-code-04 ›

C 🔒 Administrator / ctf-team01-code-03 ›

C 🔒 Administrator / ctf-team01-code-02 ›

C 🔒 Administrator / ctf-team01-build ›

C 🔒 Administrator / ctf-team01-code-01 ›

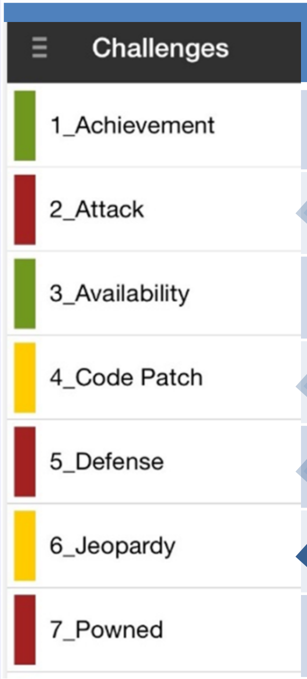
C 🔒 Administrator / ctf-team01-config ›

build repo

build commits:

- log file
- app (if ok)

Jeopardy Challenges

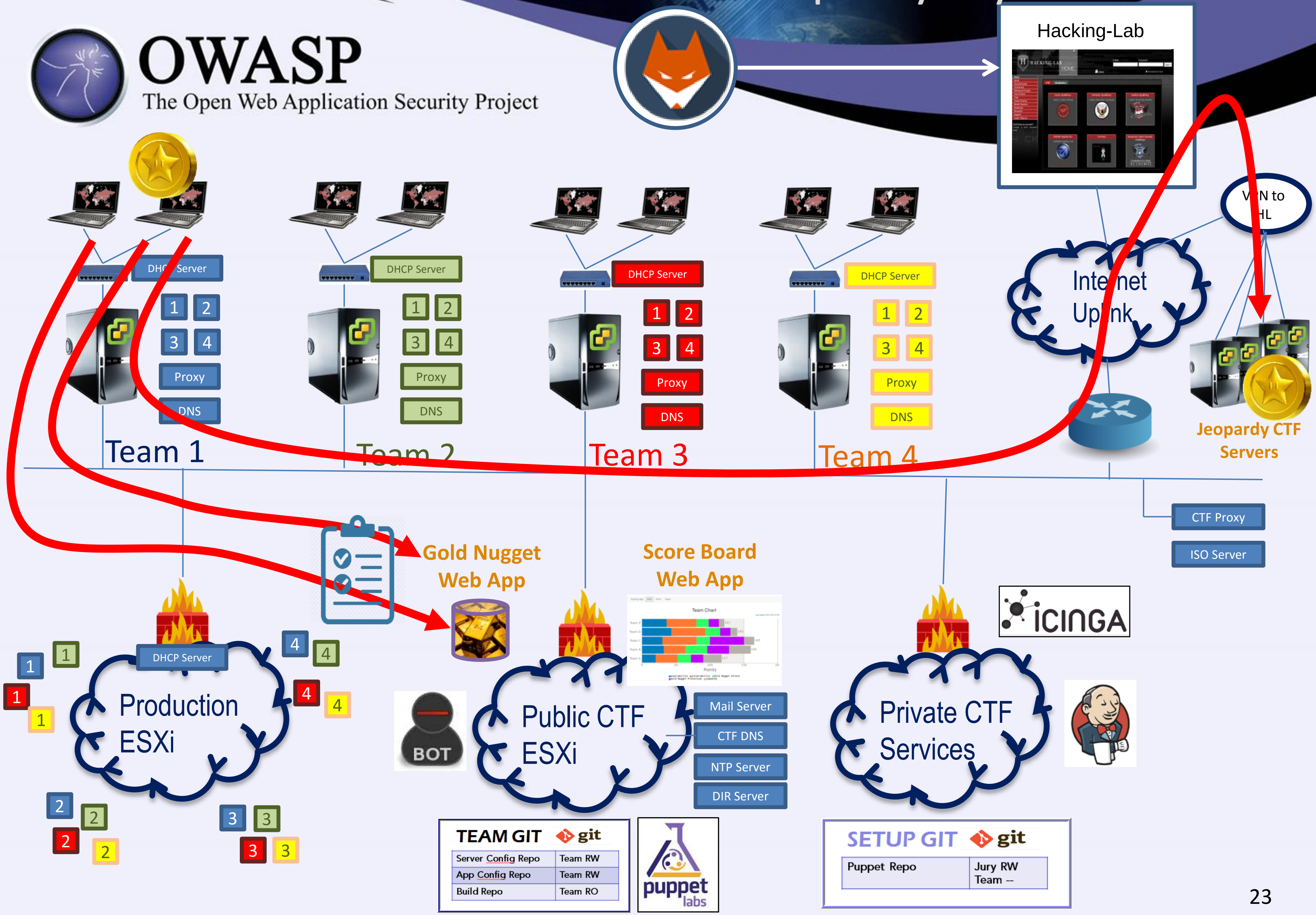


☰ Challenges		
🟩 1_Achievement		
🟥 2_Attack	⇦	Stealing Gold Nugget
🟩 3_Availability		
🟨 4_Code Patch	⇦	Fix vulnerable software & services
🟥 5_Defense	⇦	Safe guard own gold nuggets
🟨 6_Jeopardy	⇦	Solving jeopardy challenges
🟥 7_Powned		

Jeopardy-style CTF

- Jeopardy-style CTFs have a couple of tasks in range of categories. For example, Web, Reverse Engineering, Crypto, Binary, Forensics, …
- Gold Nugget app is introducing the task (mission)
- Teams gain points for every solved task
- More points for more complicated tasks
- Teams are not fighting against each others
- The earlier a team solves the challenge, the more points they get

Jeopardy-style CTF



TEAM GIT git

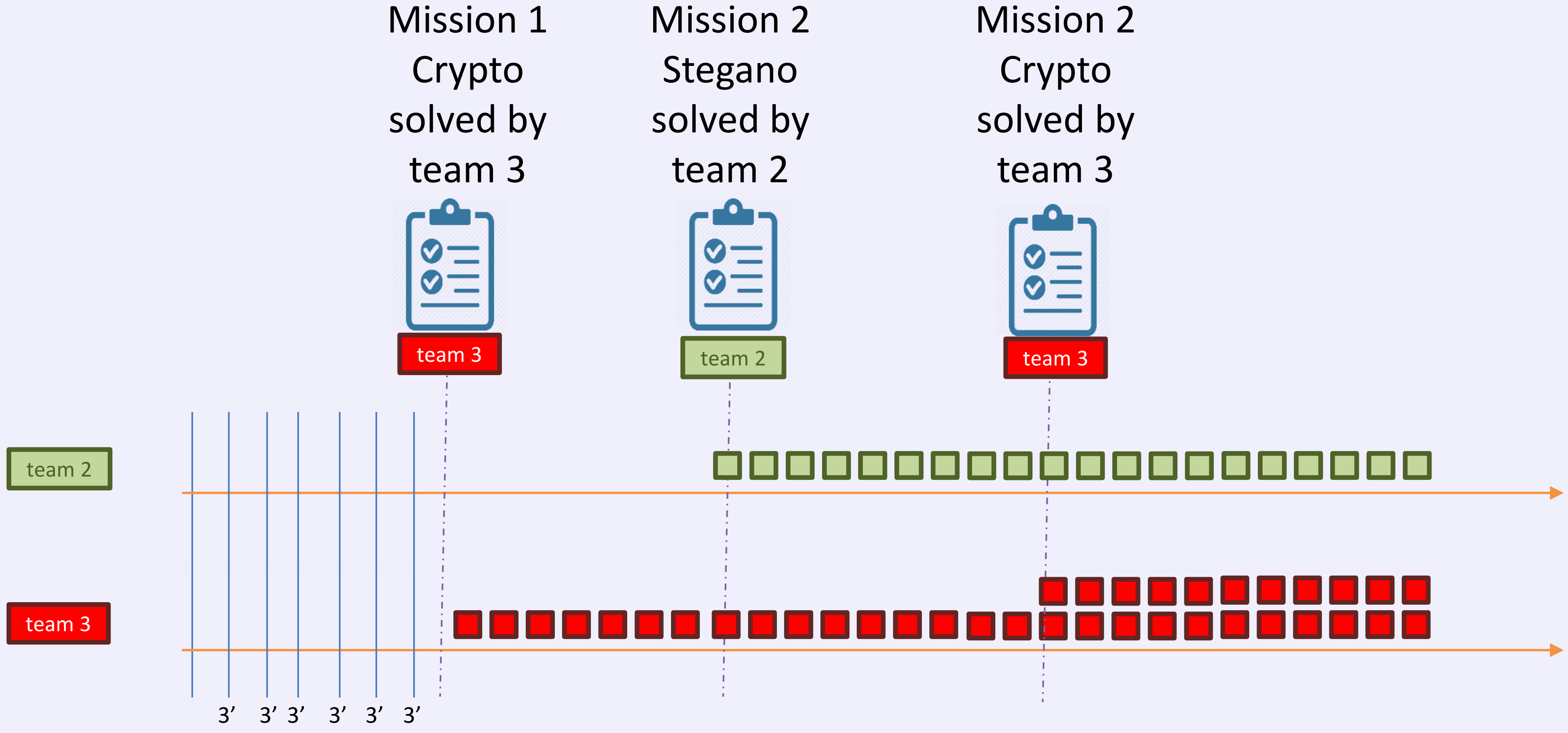
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

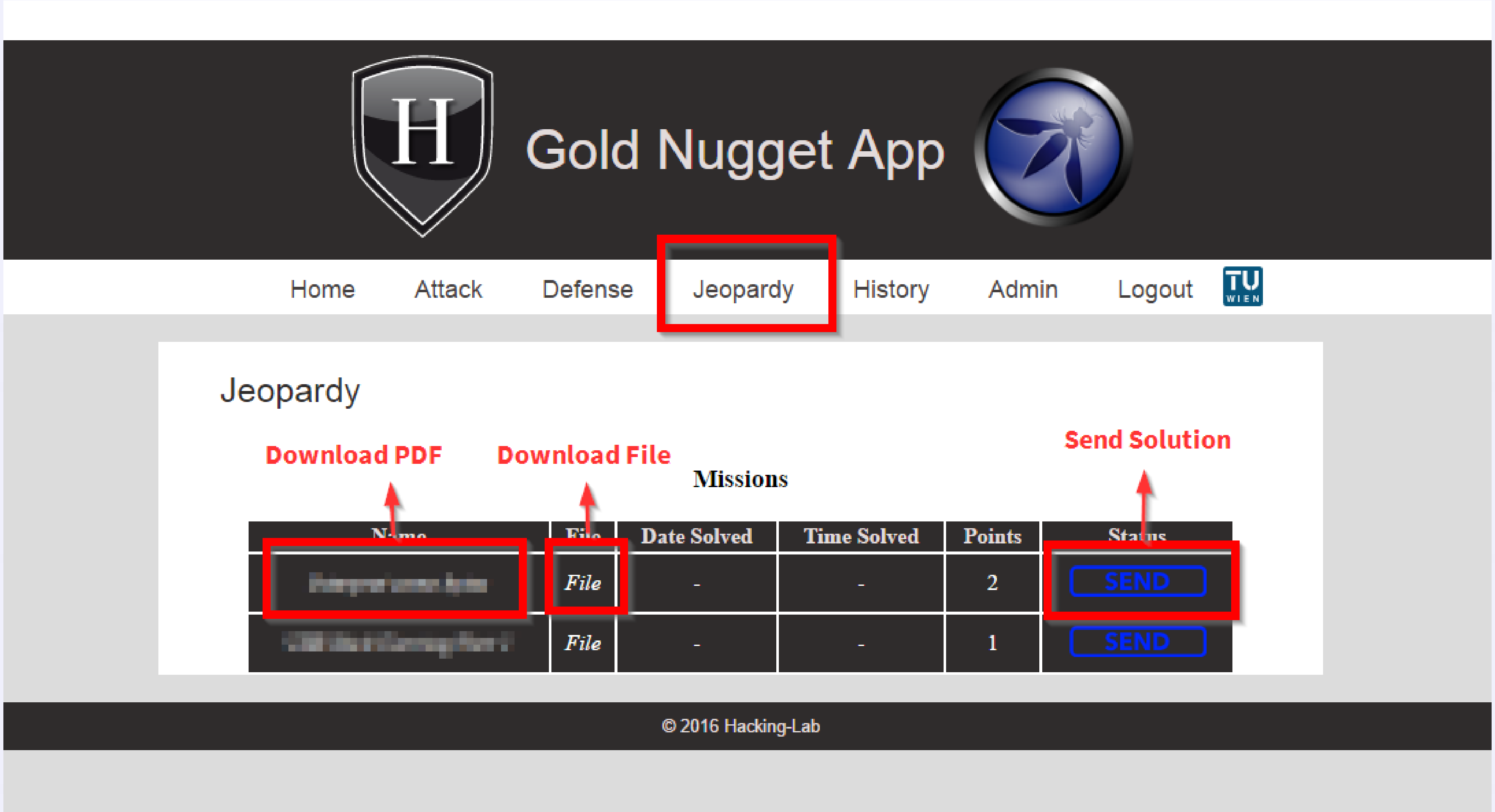
SETUP GIT git

Puppet Repo	Jury RW Team --

Scoring per Time Unit

OWASP
The Open Web Application Security Project





Jeopardy

Download PDF

Download File

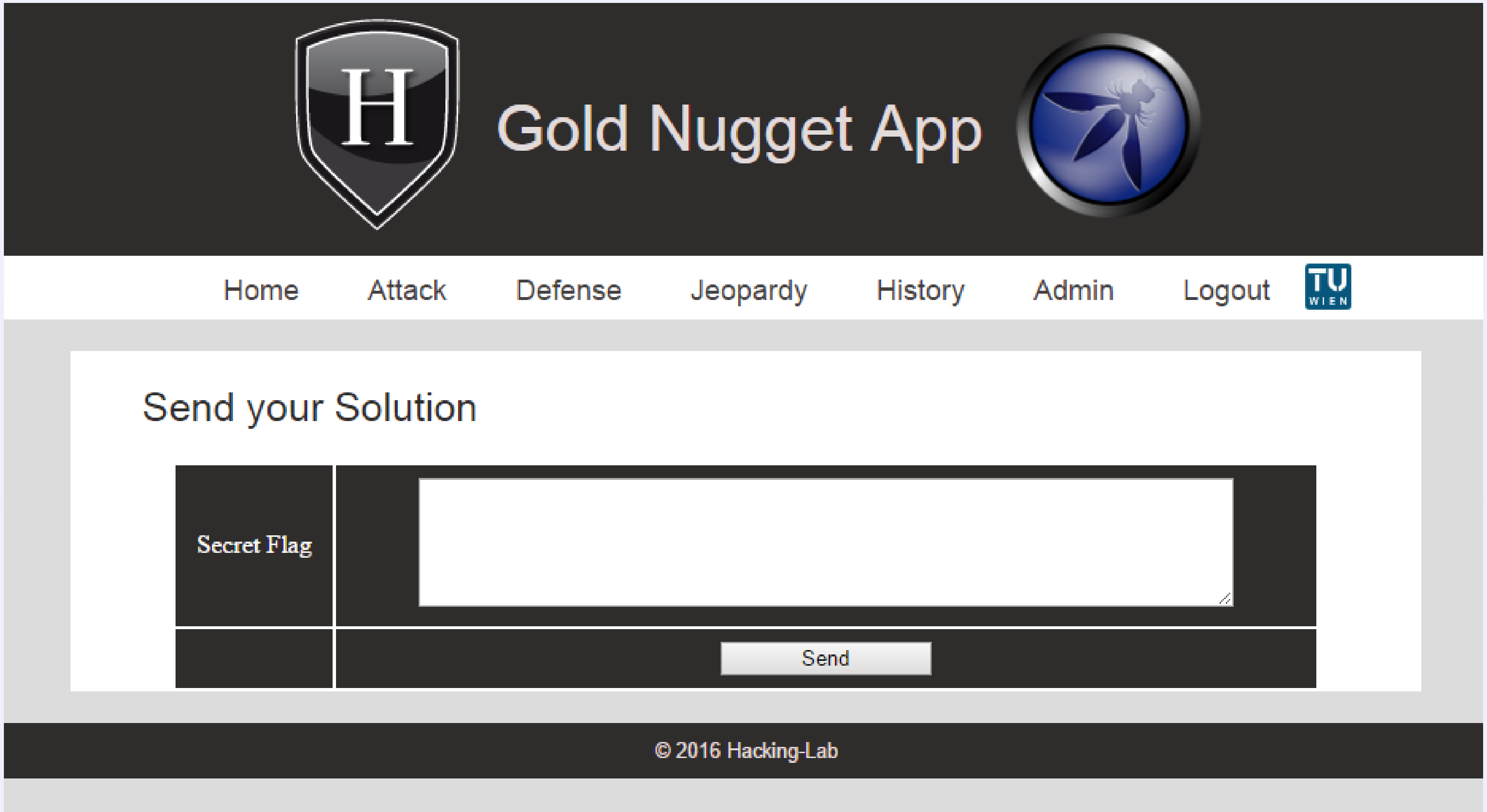
Send Solution

Missions

Name	File	Date Solved	Time Solved	Points	Status
[redacted]	*File*	-	-	2	SEND
[redacted]	*File*	-	-	1	SEND

© 2016 Hacking-Lab

- Jeopardy type 1: Secret flag



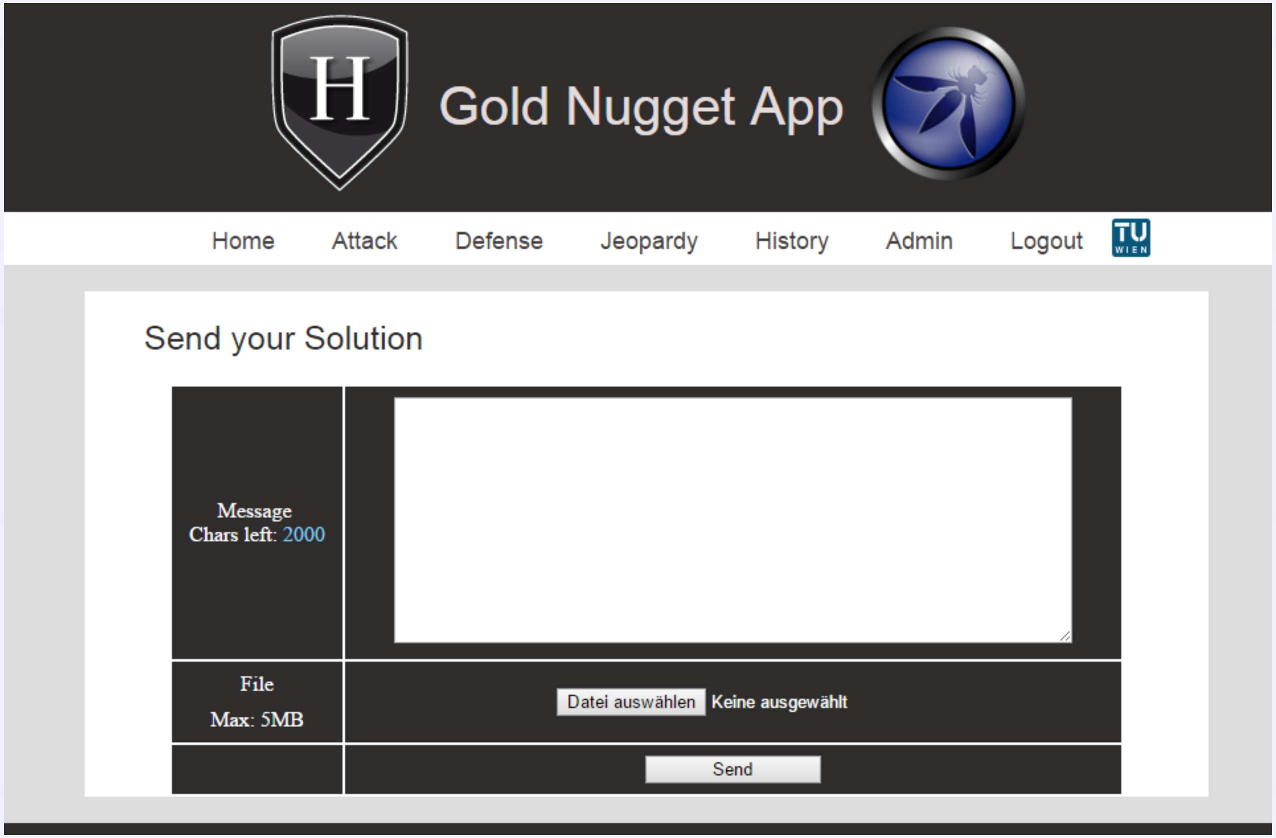
Gold Nugget App

Send your Solution

Secret Flag

© 2016 Hacking-Lab

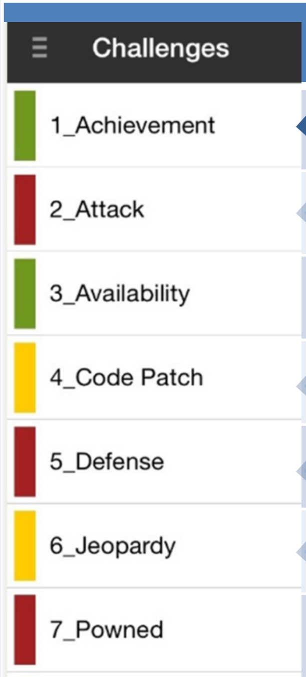
- Jeopardy type 1: Solution Message / File



Send your Solution

Message Chars left: 2000	
File Max: 5MB	Datei auswählen Keine ausgewählt
	Send

Achievements



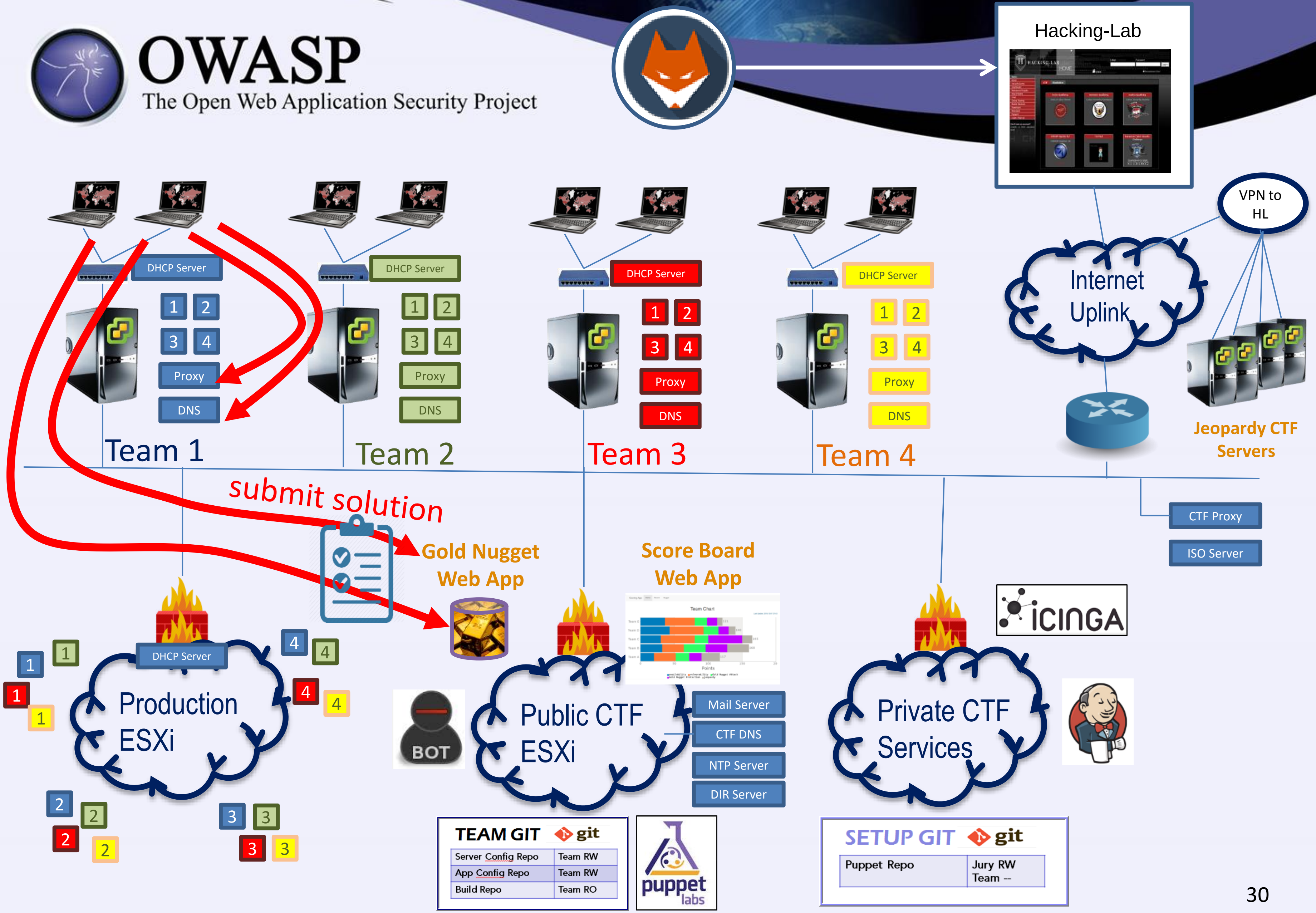
☰ Challenges	
🟩 1_Achievement	Setup and maintain a service
🟥 2_Attack	Stealing Gold Nugget
🟩 3_Availability	
🟨 4_Code Patch	Fix vulnerable software & services
🟥 5_Defense	Safe guard own gold nuggets
🟨 6_Jeopardy	Solving jeopardy challenges
🟥 7_Powned	

Achievements

- Technical Achievements
  - – Teams must setup and maintain services
  - – DNS, Proxy, Apache, NodeJS, AngularJS, …
- Non-Technical Achievements (Management)
  - – Write press release
  - – Announce news
  - – Create crisis organization during CTF game
  - – Presentation / Talk

Achievements

OWASP
The Open Web Application Security Project



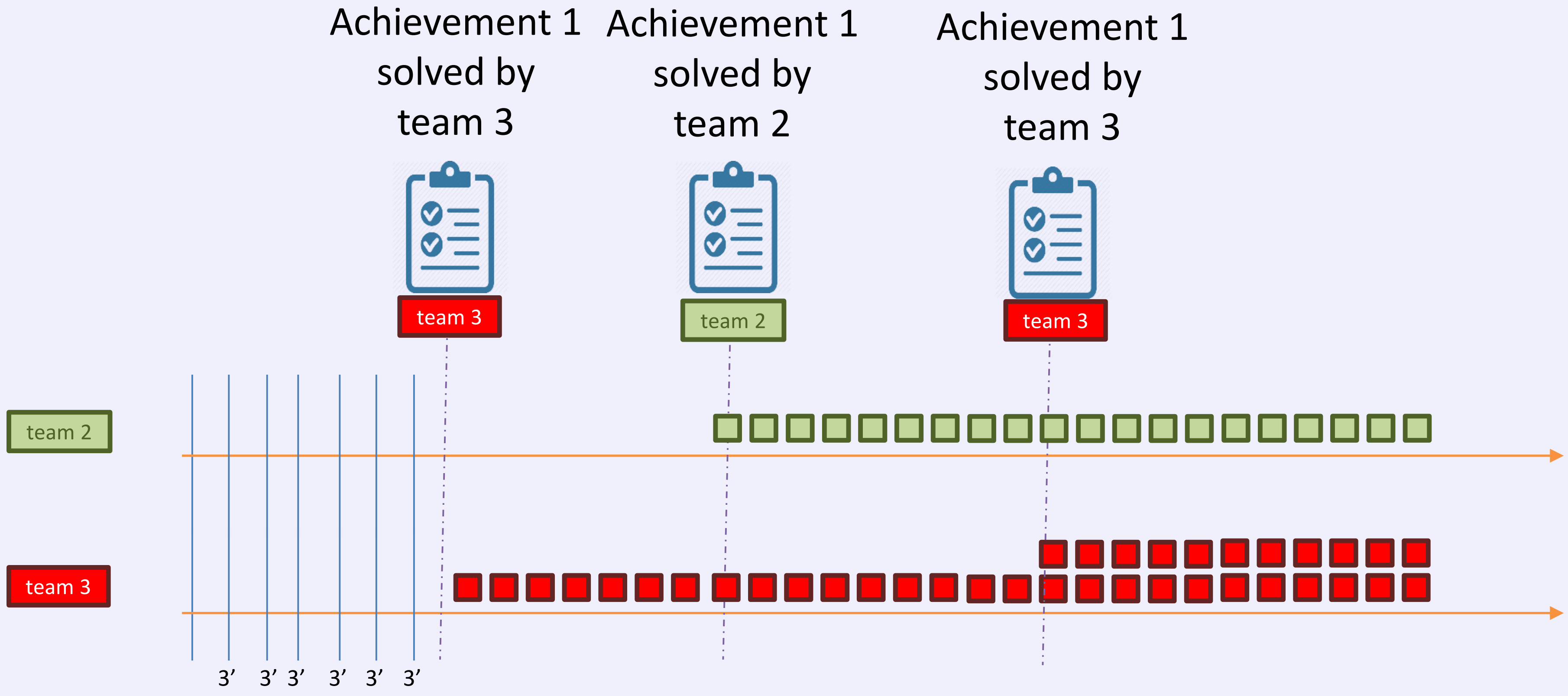
TEAM GIT git

Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

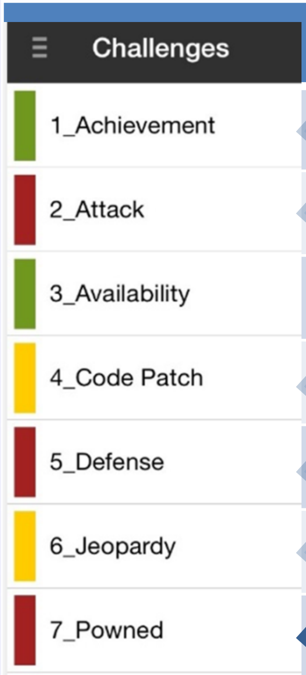
SETUP GIT git

Puppet Repo	Jury RW Team --

Scoring per Time Unit


Achievement 1 solved by team 3
Achievement 1 solved by team 2
Achievement 1 solved by team 3
team 3
team 2
team 3
team 2
team 3
3’
3’
3’
3’
3’
3’

Pown’ed



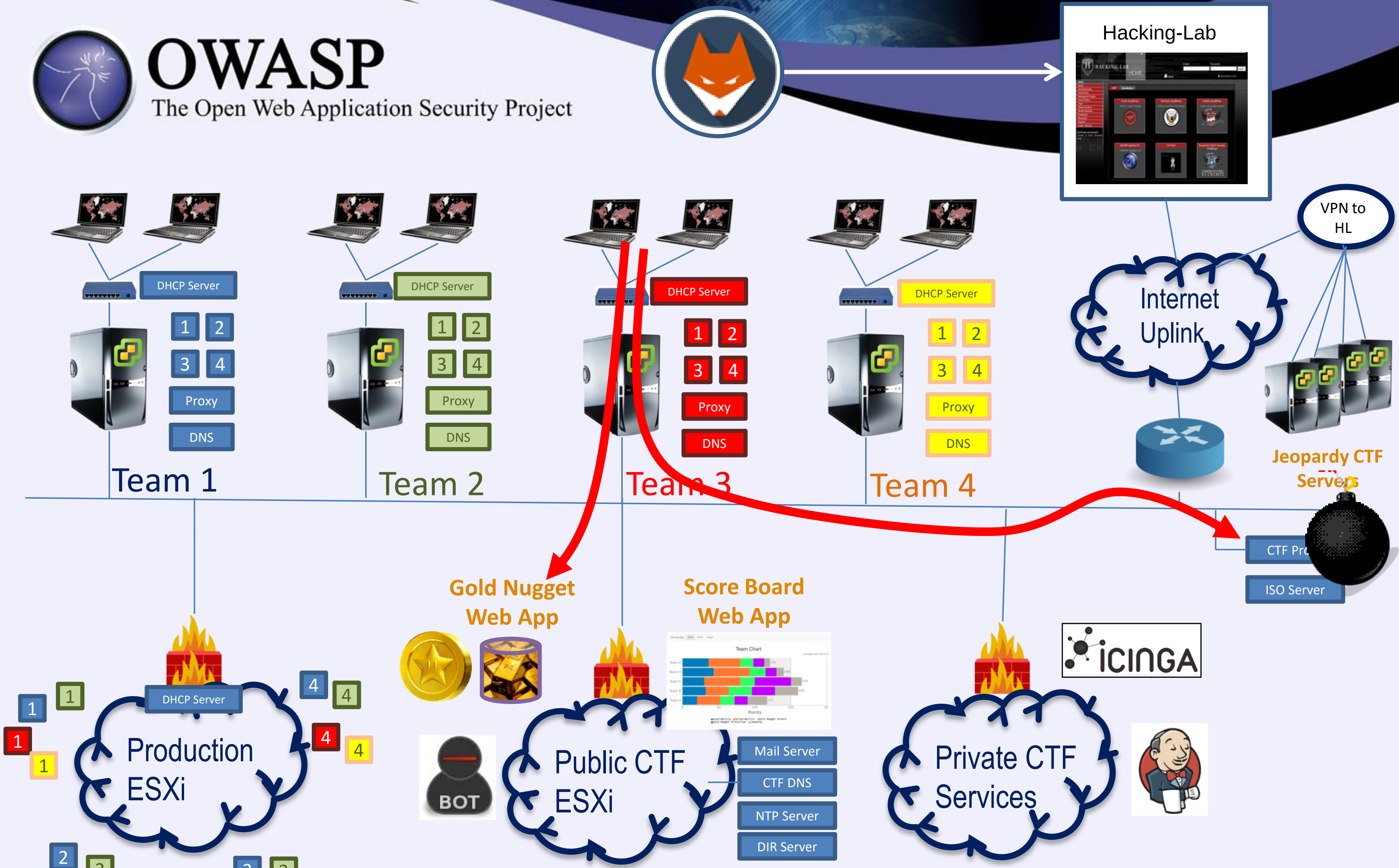
☰ Challenges	
🟩 1_Achievement	Setup and maintain a service
🟥 2_Attack	Stealing Gold Nugget
🟩 3_Availability	
🟨 4_Code Patch	Fix vulnerable software & services
🟥 5_Defense	Safe guard own gold nuggets
🟨 6_Jeopardy	Solving jeopardy challenges
🟥 7_Powned	Own a device/server

Pown'ed

- Teams may find vulnerabilities that are not known to the CTF jury
- If a team could hack such a service, then the team could get a special gold nugget and leave it on the hacked server as 'evidence'
- This special gold nugget is defined as the "evidence gold nugget"
- Teams can request such an evidence gold nugget from the gold nugget app, but only one at a time until it's being verified by the jury

Pown'ed

OWASP
The Open Web Application Security Project



TEAM GIT git

Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

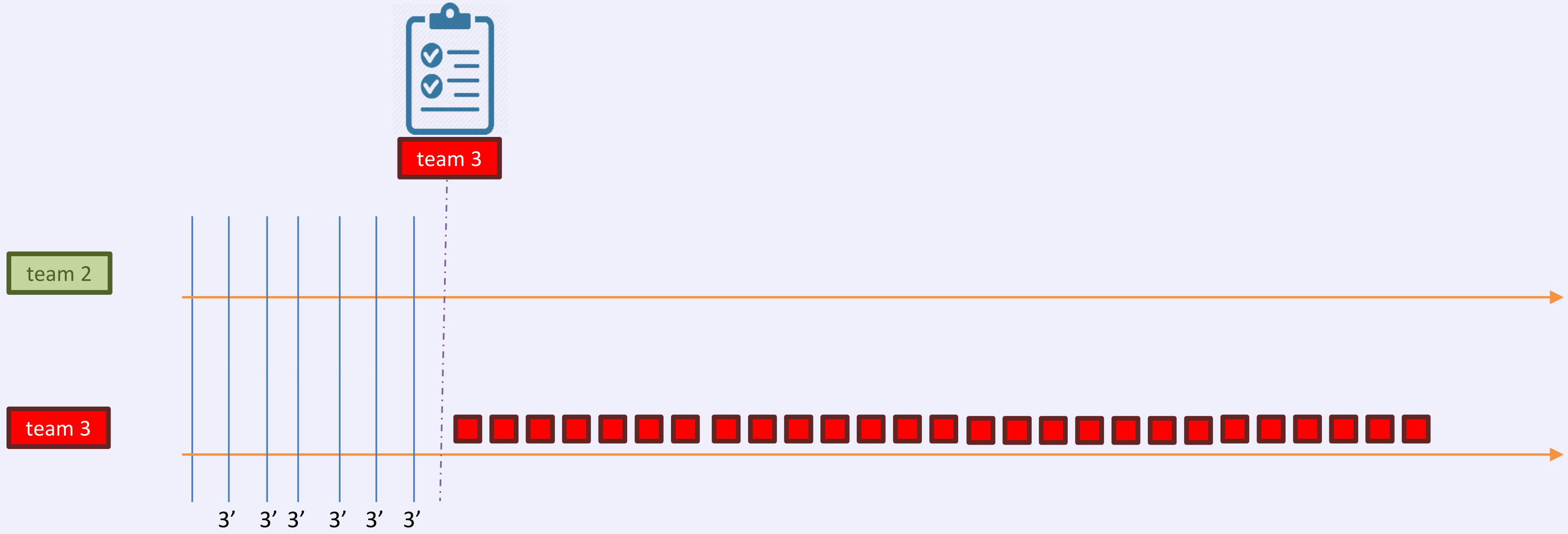
puppet labs

SETUP GIT git

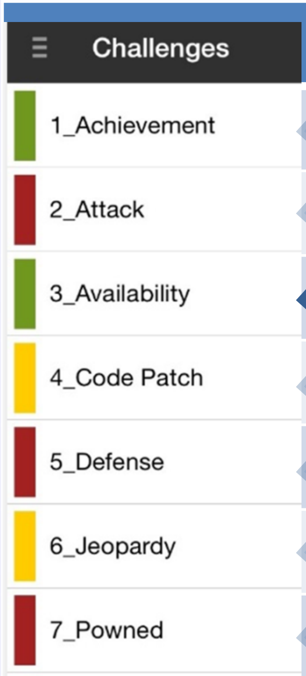
Puppet Repo	Jury RW Team --

Scoring per Time Unit

team 3 found a 0-day exploit and left an evidence nugget on the server



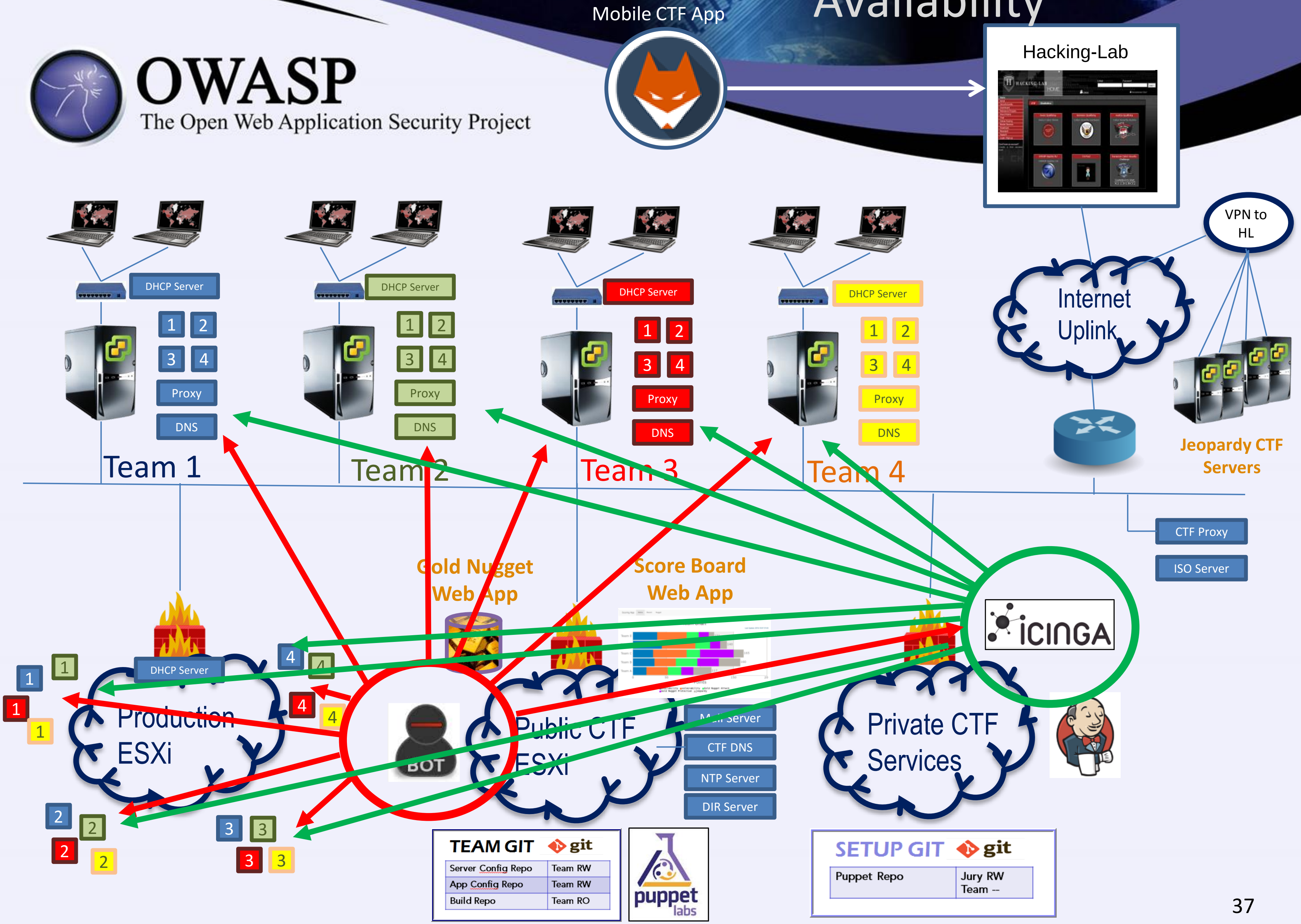
Availability



☰ Challenges	
🟩 1_Achievement	Setup and maintain a service
🟥 2_Attack	Stealing Gold Nugget
🟩 3_Availability	Keep own services up and running
🟨 4_Code Patch	Fix vulnerable software & services
🟥 5_Defense	Safe guard own gold nuggets
🟨 6_Jeopardy	Solving jeopardy challenges
🟥 7_Powned	Own a device/server

Availability

OWASP
The Open Web Application Security Project



TEAM GIT git

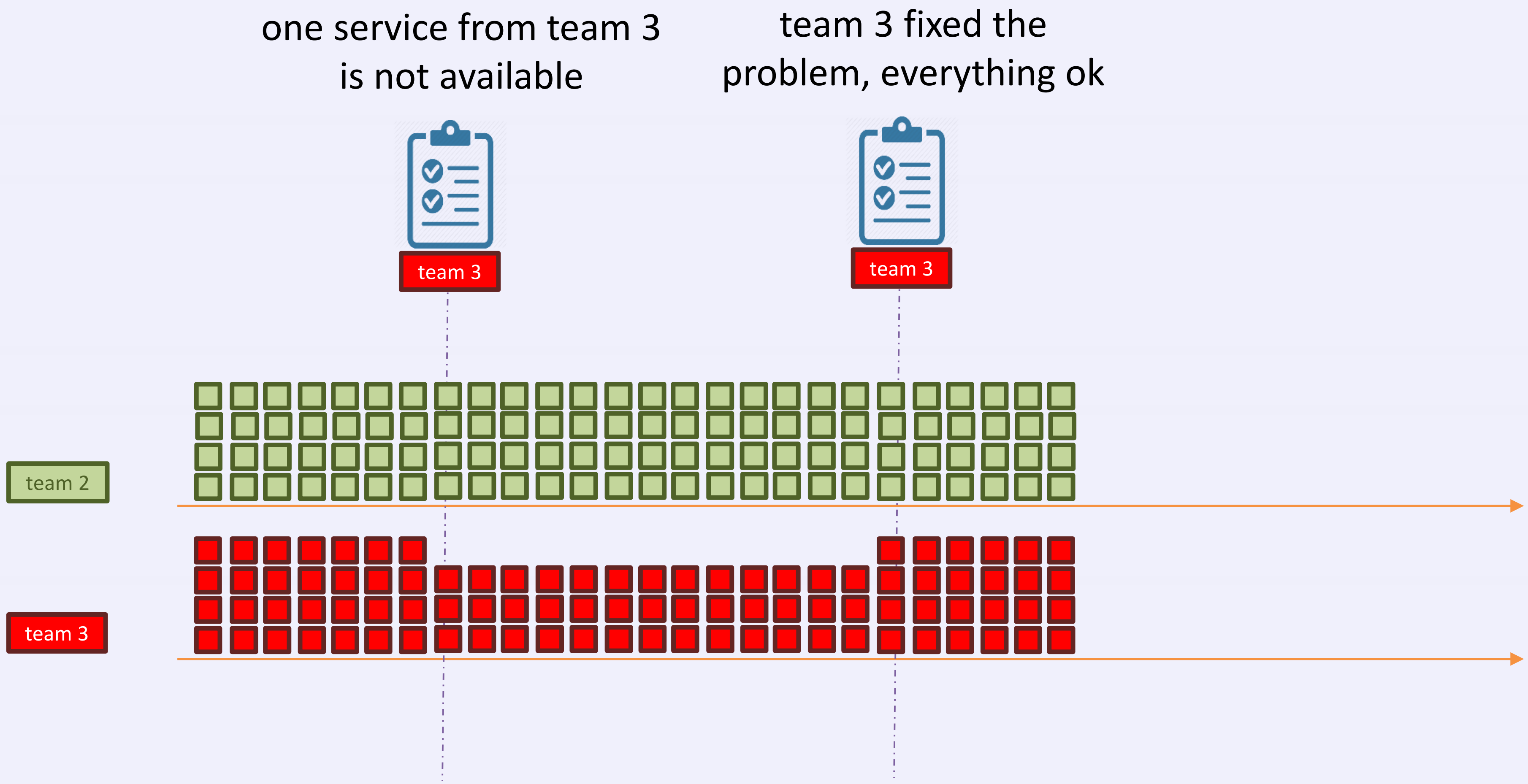
Server Config Repo	Team RW
App Config Repo	Team RW
Build Repo	Team RO

SETUP GIT git

Puppet Repo	Jury RW Team --

Scoring per Time Unit

OWASP
The Open Web Application Security Project

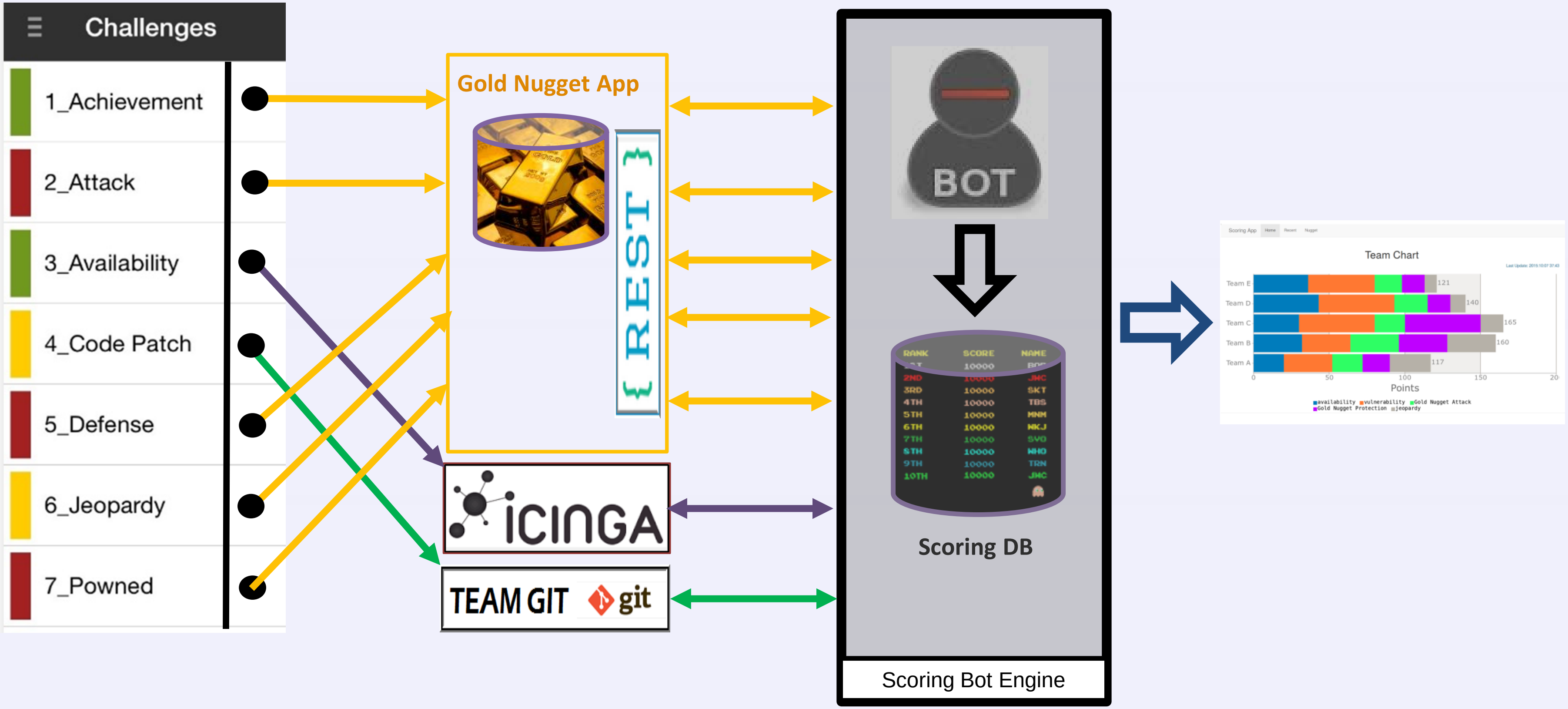

one service from team 3 is not available
team 3 fixed the problem, everything ok
team 3
team 3
team 2
team 3

CTF Scoring

CTF Scoring

OWASP

The Open Web Application Security Project



ECSC Award Ceremony 2015

OWASP
The Open Web Application Security Project

Thank You!

ivan.buetler@owasp.org

https://www.owasp.org/index.php/OWASP_University_Challenge