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 Tasks

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 Application
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 Nuggets are digitally signed strings. The gold nugget app is issuing them. The gold nugget app knows, who owns which gold nugget
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.
OWASP
The Open Web Application Security Project

CTF Architecture

Mobile CTF App

Hacking-Lab

Internet
Uplink

VPN to
HL

Jeopardy CTF
Servers

CTF Proxy

ISO Server

Team 1

Team 2

Team 3

Team 4

Gold Nugget
Web App

Score Board
Web App

Public CTF
ESXi

Private CTF
Services

Team GIT

Puppet Repo

Jury RW

Team RO

Hacking-Lab

CTF Proxy

ISO Server

VP to
HL

Jeopardy CTF
Servers

CTF Architecture
• 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

<table>
<thead>
<tr>
<th>Challenges</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Achievement</td>
<td></td>
</tr>
<tr>
<td>2. Attack</td>
<td>Stealing Gold Nugget</td>
</tr>
<tr>
<td>3. Availability</td>
<td></td>
</tr>
<tr>
<td>4. Code Patch</td>
<td></td>
</tr>
<tr>
<td>5. Defense</td>
<td></td>
</tr>
<tr>
<td>6. Jeopardy</td>
<td></td>
</tr>
<tr>
<td>7. Powned</td>
<td></td>
</tr>
</tbody>
</table>
• 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
Scoring per Time Unit

OWASP
The Open Web Application Security Project

Gold Nugget
Web App

ATTACK/DEFENSE

team 2 is requesting an new gold nugget

the previous gold nugget becomes invalid

penalty period

team 2

team 3

team 2

team 3

3' 3' 3' 3' 3'

13
Fixing Vulnerable Apps

<table>
<thead>
<tr>
<th>Challenges</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1_Achievement</td>
<td></td>
</tr>
<tr>
<td>2_Attack</td>
<td>Stealing Gold Nugget</td>
</tr>
<tr>
<td>3_Availability</td>
<td></td>
</tr>
<tr>
<td>4_Code Patch</td>
<td>Fix vulnerable software &amp; services</td>
</tr>
<tr>
<td>5_Defense</td>
<td>Safe guard own gold nuggets</td>
</tr>
<tr>
<td>6_Jeopardy</td>
<td></td>
</tr>
<tr>
<td>7_Powned</td>
<td></td>
</tr>
</tbody>
</table>
Fixing vulnerable apps

OWASP
The Open Web Application Security Project

- Team 1
- Team 2
- Team 3
- Team 4

Gold Nugget Web App
Public CTF ESXi
Score Board Web App
Private CTF Services

Internet Uplink
VPN to HL

Jeopardy CTF Servers
CTF Proxy
ISO Server

Production ESXi
Gold Nugget
Web App
Public CTF ESXi
Score Board
Web App
Private CTF
Services

Team GIT
Server Config Repo
App Config Repo
Build Repo

<table>
<thead>
<tr>
<th>SETUP GIT</th>
<th>git</th>
</tr>
</thead>
<tbody>
<tr>
<td>Puppet Repo</td>
<td>Jury RW</td>
</tr>
</tbody>
</table>

Fixing vulnerable apps
Teams have access to the source code of the vulnerable apps.

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

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

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

get nugget ()

Gold Nugget Web App

Team 1

Team 2

Team 3

Team 4

read-only

read-write

git hook triggers new Jenkins build

git hook triggers installation on PROD

git hook triggers installation on DEV

Production

ESXi

Team 1 Build - RO

Team 2 Build - RD

Team 3 Build - RO

Team 4 Build - RO

Team 1 App - RW

Team 2 App - RW

Team 3 App - RW

Team 4 App - RW

Team 1

Team 2

Team 3

Team 4

DHCP Server

Proxy

DNS

DHCP Server

Proxy

DNS

DHCP Server

Proxy

DNS

DHCP Server

Proxy

DNS
teamgit.hacking-lab.com
source repo

commit

triggers

build
build repo

build commits:
- log file
- app (if ok)
# Jeopardy Challenges

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1_Achievement</td>
<td>Stealing Gold Nugget</td>
</tr>
<tr>
<td>2_Attack</td>
<td>Fix vulnerable software &amp; services</td>
</tr>
<tr>
<td>3_Availability</td>
<td>Safe guard own gold nuggets</td>
</tr>
<tr>
<td>4_Code Patch</td>
<td>Solving jeopardy challenges</td>
</tr>
<tr>
<td>5_Defense</td>
<td></td>
</tr>
<tr>
<td>6_Jeopardy</td>
<td></td>
</tr>
<tr>
<td>7_Powned</td>
<td></td>
</tr>
</tbody>
</table>
• 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
Mission 1
Crypto solved by team 3

Mission 2
Stegano solved by team 2

Mission 2
Crypto solved by team 3
• Jeopardy type 1: Secret flag
• Jeopardy type 1: Solution Message / File
Achievements

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1_Achievement</td>
<td>Setup and maintain a service</td>
</tr>
<tr>
<td>2_Attack</td>
<td>Stealing Gold Nugget</td>
</tr>
<tr>
<td>3_Availability</td>
<td>Fix vulnerable software &amp; services</td>
</tr>
<tr>
<td>4_Code Patch</td>
<td>Safe guard own gold nuggets</td>
</tr>
<tr>
<td>5_Defense</td>
<td>Solving jeopardy challenges</td>
</tr>
<tr>
<td>6_Jeopardy</td>
<td></td>
</tr>
<tr>
<td>7_Powned</td>
<td></td>
</tr>
</tbody>
</table>
• 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
<table>
<thead>
<tr>
<th>Challenges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1_Achievement</td>
<td>Setup and maintain a service</td>
</tr>
<tr>
<td>2_Attack</td>
<td>Stealing Gold Nugget</td>
</tr>
<tr>
<td>3_Availability</td>
<td></td>
</tr>
<tr>
<td>4_Code Patch</td>
<td>Fix vulnerable software &amp; services</td>
</tr>
<tr>
<td>5_Defense</td>
<td>Safe guard own gold nuggets</td>
</tr>
<tr>
<td>6_Jeopardy</td>
<td>Solving jeopardy challenges</td>
</tr>
<tr>
<td>7_Powned</td>
<td>Own a device/server</td>
</tr>
</tbody>
</table>
• 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
team 3 found a 0-day exploit and left an evidence nugget on the server.
Availability

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1_Achievement</td>
<td>Setup and maintain a service</td>
</tr>
<tr>
<td>2_Attack</td>
<td>Stealing Gold Nugget</td>
</tr>
<tr>
<td>3_Availability</td>
<td>Keep own services up and running</td>
</tr>
<tr>
<td>4_Code Patch</td>
<td>Fix vulnerable software &amp; services</td>
</tr>
<tr>
<td>5_Defense</td>
<td>Safe guard own gold nuggets</td>
</tr>
<tr>
<td>6_Jeopardy</td>
<td>Solving jeopardy challenges</td>
</tr>
<tr>
<td>7_Powned</td>
<td>Own a device/server</td>
</tr>
</tbody>
</table>
one service from team 3 is not available  

team 3 fixed the problem, everything ok

---

Scoring per Time Unit
CTF Scoring
Thank You!

ivan.buetler@owasp.org

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