Design and Developement of a Cyber Range

Alexandru Mocanu

Università Degli Studi di Torino
Dipartimento di Informatica

February 14, 2020

Outline

Cyber Range

È un ambiente virtuale usato da professionisti, e non, per testare:

- Affidabilità
- Sicurezza
- Prestazioni

di infrastrutture e sistemi IT.

CTF - Capture the Flag

È un gioco di **hacking** dove team (o singoli) cercano **vulnerabilità** in sistemi e software messi a disposizione dagli organizzatori della competizione al fine di sfruttarle e di collezionare le varie **flag** nascoste sul sistema bersaglio.

Tipologie CTF

Ci sono vari tipi di Capture the Flag, i più famosi sono:

- Jeopardy
- Attack/Defense
- Boot2Root

CTF - Jeopardy

I CTF di tipo Jeopardy sono probabilmente i più popolari, dato che si adattano bene a competizioni online.
In questo formato:

- diverse *challenge*, ognuna con un singolo *flag*

CTF - Jeopardy

I CTF di tipo Jeopardy sono probabilmente i più popolari, dato che si adattano bene a competizioni online.
In questo formato:

- diverse *challenge*, ognuna con un singolo *flag*
- **punteggio**: a seconda della difficoltà della singola *challenge*

CTF - Jeopardy

I CTF di tipo Jeopardy sono probabilmente i più popolari, dato che si adattano bene a competizioni online.
In questo formato:

- diverse *challenge*, ognuna con un singolo *flag*
- **punteggio**: a seconda della difficoltà della singola *challenge*
- **vincitore**: chi totalizza il punteggio maggiore

CTF - Jeopardy

I CTF di tipo Jeopardy sono probabilmente i più popolari, dato che si adattano bene a competizioni online.
In questo formato:

- diverse *challenge*, ognuna con un singolo *flag*
- **punteggio**: a seconda della difficoltà della singola *challenge*
- **vincitore**: chi totalizza il punteggio maggiore
- **durata**: a tempo

CTF - Jeopardy

I CTF di tipo Jeopardy sono probabilmente i più popolari, dato che si adattano bene a competizioni online.
In questo formato:

- diverse *challenge*, ognuna con un singolo *flag*
- **punteggio**: a seconda della difficoltà della singola *challenge*
- **vincitore**: chi totalizza il punteggio maggiore
- **durata**: a tempo

Generalmente con questo tipo di formato i partecipanti formano squadre, le quali assegnano una challenge a uno o più membri della squadra, per velocizzare la risoluzione delle challenge e la conquista delle flag.

CTF - Attack/Defense

Il formato Attack/Defense prevede che gli organizzatori forniscano ai giocatori (principalmente squadre) una o più macchine virtuali.

CTF - Attack/Defense

Il formato Attack/Defense prevede che gli organizzatori forniscano ai giocatori (principalmente squadre) una o più macchine virtuali.

I giocatori quindi avranno un doppio ruolo:

CTF - Attack/Defense

Il formato Attack/Defense prevede che gli organizzatori forniscano ai giocatori (principalmente squadre) una o più macchine virtuali.

I giocatori quindi avranno un doppio ruolo:

- **difendere** i servizi esposti sulla propria macchina virtuale

CTF - Attack/Defense

Il formato Attack/Defense prevede che gli organizzatori forniscano ai giocatori (principalmente squadre) una o più macchine virtuali.

I giocatori quindi avranno un doppio ruolo:

- **difendere** i servizi esposti sulla propria macchina virtuale
- **attaccare** i servizi dei team concorrenti

CTF - Attack/Defense

Il formato Attack/Defense prevede che gli organizzatori forniscano ai giocatori (principalmente squadre) una o più macchine virtuali.

I giocatori quindi avranno un doppio ruolo:

- **difendere** i servizi esposti sulla propria macchina virtuale
- **attaccare** i servizi dei team concorrenti

Si guadagna un **punteggio** per ogni flag conquistato.

CTF - Attack/Defense

Il formato Attack/Defense prevede che gli organizzatori forniscano ai giocatori (principalmente squadre) una o più macchine virtuali.

I giocatori quindi avranno un doppio ruolo:

- **difendere** i servizi esposti sulla propria macchina virtuale
- **attaccare** i servizi dei team concorrenti

Si guadagna un **punteggio** per ogni flag conquistato.

Generalmente sono eventi *offline* e con un limite di tempo.

CTF - Boot2Root

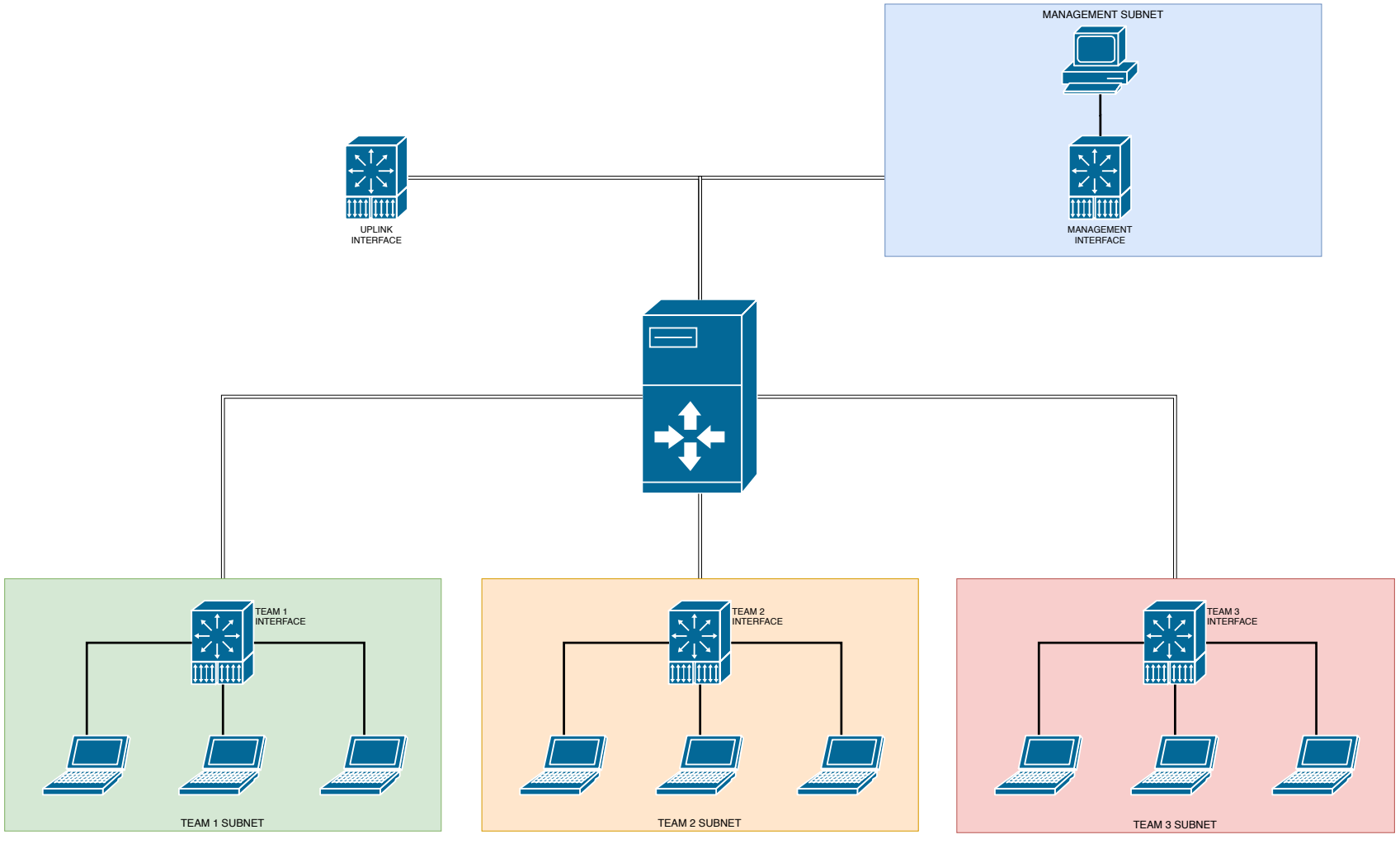
Consiste l'installazione di una *macchina virtuale* e lo scopo è di trovare e sfruttarne le vulnerabilità che permettano di avere l'accetto root alla stessa.

CTF - Boot2Root

Consiste l'installazione di una *macchina virtuale* e lo scopo è di trovare e sfruttarne le vulnerabilità che permettano di avere l'accetto root alla stessa.

Questo formato di CTF è principalmente preferito da singoli che vogliono esercitarsi a sfruttare vulnerabilità in uno scenario semi-reale, ma non preclude la possibilità di creare un team.

Scenario


MANAGEMENT SUBNET
UPLINK INTERFACE
MANAGEMENT INTERFACE
TEAM 1 INTERFACE
TEAM 2 INTERFACE
TEAM 3 INTERFACE
TEAM 1 SUBNET
TEAM 2 SUBNET
TEAM 3 SUBNET

Obiettivi Fase 1

Regole specifiche per il Virtual Router

- aa

Regole specifiche per il Management

- aaa

Regole specifiche per i Team

- aaa

Obiettivi Fase 2

Regole specifiche per il Virtual Router

- aa

Regole specifiche per il Management

- aa

Regole specifiche per i Team

- aa

Software

- iptables
- netplan
- python