Design and Developement of a Cyber Range

Alexandru Mocanu

Università Degli Studi di Torino
Dipartimento di Informatica

February 17, 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

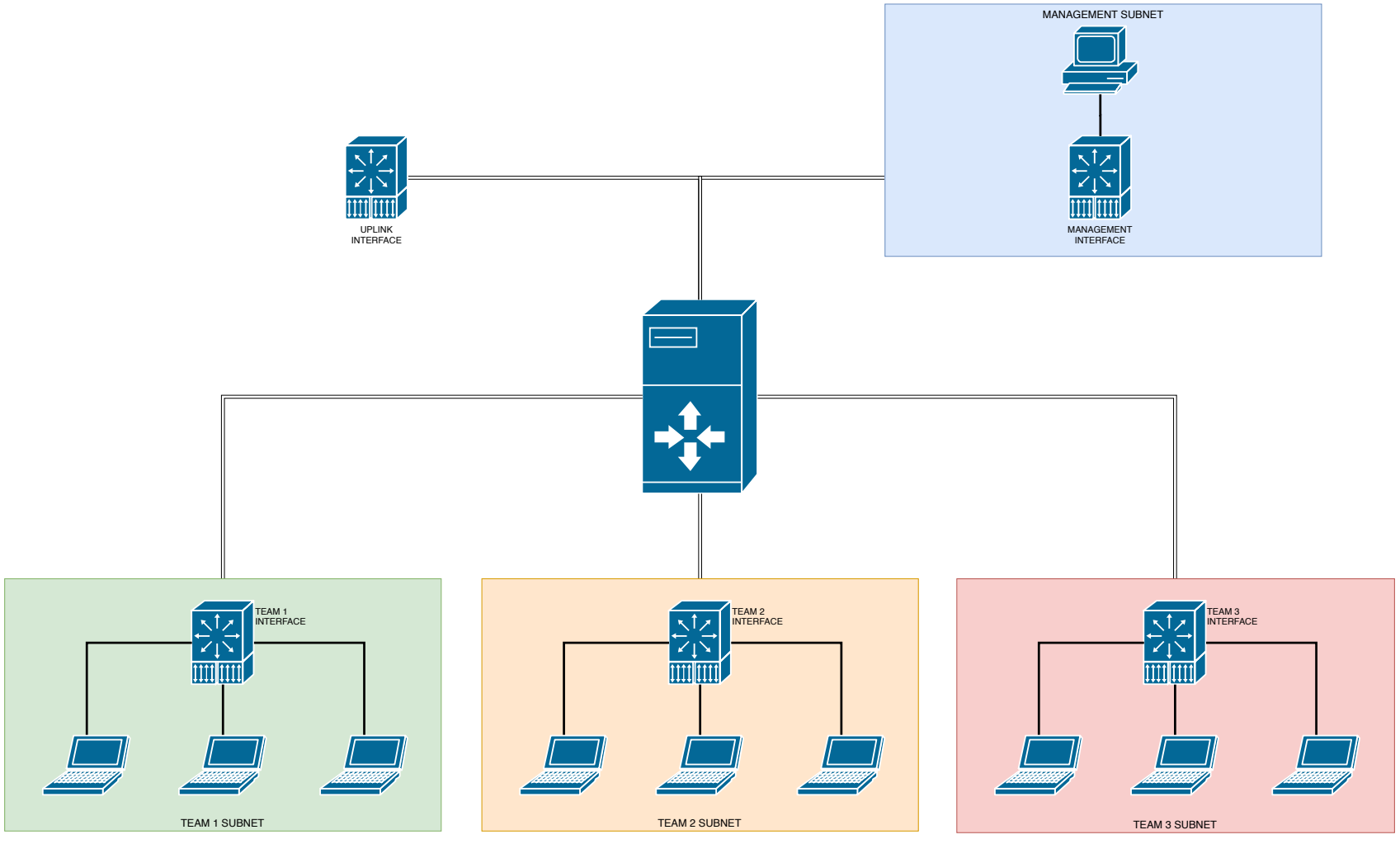
Consiste l'installazione di una *macchina virtuale* e lo scopo è di trovare e sfruttarne le vulnerabilità che permettano di avere l'accetto root alla stessa.

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

Software

- iptables

Software

- iptables
- netplan

Software

- iptables
- netplan
- script python

Software

- iptables
- netplan
- script python
- script bash

Definizione

Iptables è un potente firewall integrato nel kernel Linux. Permette di definire, tramite regole, il filtraggio, la manipolazione dei pacchetti ed il NAT.

È strutturato in **tabelle**, ognuna contiene le proprie **catene** che possono, anche, essere definite dall'utente.

Ogni catena è una *lista di regole* che specificano l'**azione** da intraprendere con i pacchetti che corrispondono alla regole.

Quest'*azione* corrisponde al **target**.

TARGETS

Una regola di firewall specifica il criterio di selezione dei pacchetti ed il **target**.

Se il pacchetto non corrisponde → verrà esaminata la regola successiva.
Se il pacchetto corrisponde → verrà intrapresa l'azione definita dal *target*, che può essere:

- ACCEPT
- DROP
- RETURN
- catena definita dall'utente

CHAINS

TABLES

Ci sono 5 tabelle indipendenti:

filter defr

TABLES

Ci sono 5 tabelle indipendenti:

filter defr

nat

TABLES

Ci sono 5 tabelle indipendenti:

filter defr

nat

mangle

TABLES

Ci sono 5 tabelle indipendenti:

filter defr

nat

mangle

raw

TABLES

Ci sono 5 tabelle indipendenti:

filter defr

nat

mangle

raw

security

Obiettivi Fase 1

- Isolamento dei Team

Obiettivi Fase 1

- Isolamento dei Team
- Solo Management e Virtual Router possono iniziare una connessione verso gli altri

Obiettivi Fase 1

- Isolamento dei Team
- Solo Management e Virtual Router possono iniziare una connessione verso gli altri
- Solo Management e Virtual Router possono connettersi all'esterno, attraverso l'UPLINK

Obiettivi Fase 1

- Isolamento dei Team
- Solo Management e Virtual Router possono iniziare una connessione verso gli altri
- Solo Management e Virtual Router possono connettersi all'esterno, attraverso l'UPLINK
- LOG dei pacchetti entranti e dei pacchetti inoltrati

Regole specifiche per il Virtual Router

Connessione all'esterno attraverso UPLINK

```
$ iptables -P OUTPUT ACCEPT

$ iptables -P INPUT DROP

$ iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per il Virtual Router

Ricevere connessioni da MANAGEMENT (qualsiasi tipo)

```
$ iptables -P INPUT DROP

$ iptables -A INPUT -i $MANAGEMENT_INTERFACE -j ACCEPT

$ iptables -P OUTPUT ACCEPT
```

Regole specifiche per il Virtual Router

Connessioni ai TEAM e ricezione risposta

```
$ iptables -P OUTPUT ACCEPT
```

```
$ iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per il Virtual Router

Connessione loopback

```
$ iptables -P OUTPUT ACCEPT

$ iptables -A INPUT -i lo -j ACCEPT
```

Regole specifiche per il Virtual Router

Blocco connessioni dall'esterno e dai TEAM (se non iniziate da VR)

```
$ iptables -P INPUT DROP

$ iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per il Management

Connessione all'esterno attraverso UPLINK

```
$ iptables -P FORWARD DROP

$ iptables -t nat -A POSTROUTING -o $UPLINK -j MASQUERADE

$ iptables -A FORWARD -i $MANAGEMENT_INTERFACE -j ACCEPT

$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per il Management

Connessione al VIRTUAL ROUTER

```
$ iptables -P INPUT DROP

$ iptables -A INPUT -i $MANAGEMENT_INTERFACE -j ACCEPT

$ iptables -P OUTPUT ACCEPT
```

Regole specifiche per il Management

Connessione ai TEAM

```
$ iptables -P FORWARD DROP

$ iptables -A FORWARD -i $MANAGEMENT_INTERFACE -j ACCEPT

$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per il Management

Blocco connessioni dall'esterno e dai TEAM (se non iniziate da MANAGEMENT)

```
$ iptables -P INPUT DROP

$ iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per i Team

Rispondere a connessioni iniziate da MANAGEMENT

```
$ iptables -P FORWARD DROP
```

```
$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per i Team

Rispondere a connessioni iniziate da VR

```
$ iptables -P INPUT DROP
```

```
$ iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per i Team

Blocco inizio connessioni verso:

- MANAGEMENT

```
$ iptables -P FORWARD DROP
```

- VIRTUAL ROUTER

```
$ iptables -P INPUT DROP
```

- altri TEAM

```
$ iptables -P FORWARD DROP
```

- esterno tramite UPLINK

```
$ iptables -P FORWARD DROP
```

Regole per il LOG

LOG dei pacchetti entranti

```
$ iptables -N LOGGING

$ iptables -A INPUT -j LOGGING

$ iptables -A LOGGING -m limit --limit $LOGLIMIT -j LOG --log-prefix
        "COMPETITION-LOG: " --log-level 4
```

Regole per il LOG

LOG dei pacchetti inoltrati

```
$ iptables -N LOGGING

$ iptables -A LOGGING -m limit --limit $LOGLIMIT -j LOG --log-prefix
      "COMPETITION-LOG: " --log-level 4

$ iptables -A FORWARD -j LOGGING
```

Obiettivi Fase 2

- Solo Management e Virtual Router possono iniziare una connessione verso chiunque

Obiettivi Fase 2

- Solo Management e Virtual Router possono iniziare una connessione verso chiunque
- Solo Management e Virtual Router possono connettersi all'esterno, attraverso l'UPLINK

Obiettivi Fase 2

- Solo Management e Virtual Router possono iniziare una connessione verso chiunque
- Solo Management e Virtual Router possono connettersi all'esterno, attraverso l'UPLINK
- Team possono comunicare tra loro

Obiettivi Fase 2

- Solo Management e Virtual Router possono iniziare una connessione verso chiunque
- Solo Management e Virtual Router possono connettersi all'esterno, attraverso l'UPLINK
- Team possono comunicare tra loro
- Team non possono iniziare connessioni verso MANAGEMENT e VIRTUAL ROUTER
- LOG dei pacchetti entranti e dei pacchetti inoltrati

Regole specifiche per il Virtual Router

Le regole rimangono le stesse della FASE 1

Regole specifiche per il Management

Connessione all'esterno attraverso UPLINK

```
$ iptables -P FORWARD ACCEPT
```

Regole specifiche per il Management

Connessione al VIRTUAL ROUTER

```
$ iptables -P INPUT DROP

$ iptables -A INPUT -i $MANAGEMENT_INTERFACE -j ACCEPT

$ iptables -P OUTPUT ACCEPT
```

Regole specifiche per il Management

Connessione ai TEAM

```
$ iptables -P FORWARD ACCEPT

$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per il Management

Blocco connessioni dall'esterno e dai TEAM (se non iniziate da MANAGEMENT)

```
$ iptables -P FORWARD ACCEPT

$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT

$ iptables -A FORWARD -o $MANAGEMENT_INTERFACE -j DROP
```

Regole specifiche per i Team

Rispondere a connessioni iniziate da MANAGEMENT

```
$ iptables -P FORWARD ACCEPT

$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED -j ACCEPT

$ iptables -A FORWARD -o $MANAGEMENT_INTERFACE -j DROP
```

Regole specifiche per i Team

Rispondere a connessioni iniziate da VR

```
$ iptables -P INPUT DROP
```

```
$ iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Regole specifiche per i Team

Connessioni verso altri TEAM

```
$ iptables -P FORWARD ACCEPT
```

Regole specifiche per i Team

Blocco inizio connessioni verso:

- MANAGEMENT

```
$ iptables -P FORWARD ACCEPT

$ iptables -A FORWARD -o $MANAGEMENT_INTERFACE -j DROP
```

- VIRTUAL ROUTER

```
$ iptables -P INPUT DROP
```

- esterno tramite UPLINK

```
$ iptables -P FORWARD ACCEPT

$ iptables -A FORWARD -o $UPLINK -j DROP
```

Regole per il LOG

Le regole sono le stesse della FASE 1

NAT

Il NAT, ovvero *Network Address Translation*, conosciuto anche come **network masquerading**, è una tecnica che consiste nel modificare gli **indirizzi IP** contenuti negli **header** dei pacchetti in transito su un sistema che agisce da **router** all'interno di una comunicazione tra due o più *host*.

NAT

Il NAT, ovvero *Network Address Translation*, conosciuto anche come **network masquerading**, è una tecnica che consiste nel modificare gli **indirizzi IP** contenuti negli **header** dei pacchetti in transito su un sistema che agisce da **router** all'interno di una comunicazione tra due o più *host*.

Nel nostro caso verrà mascherato l'indirizzo sorgente del pacchetto.

MASQUERADING

Lo script è stato ideato per permettere quattro situazioni di *masquerading*:

- Un indirizzo unico per tutti i TEAM

MASQUERADING

Lo script è stato ideato per permettere quattro situazioni di *masquerading*:

- Un indirizzo unico per tutti i TEAM, che può essere:
  - definito dall'amministratore di gara

MASQUERADING

Lo script è stato ideato per permettere quattro situazioni di *masquerading*:

- Un indirizzo unico per tutti i TEAM, che può essere:
  - definito dall'amministratore di gara
  - generato in modo casuale

MASQUERADING

Lo script è stato ideato per permettere quattro situazioni di *masquerading*:

- Un indirizzo unico per tutti i TEAM, che può essere:
  - definito dall'amministratore di gara
  - generato in modo casuale
- Indirizzi diversi per tutti i TEAM

MASQUERADING

Lo script è stato ideato per permettere quattro situazioni di *masquerading*:

- Un indirizzo unico per tutti i TEAM, che può essere:
  - definito dall'amministratore di gara
  - generato in modo casuale
- Indirizzi diversi per tutti i TEAM, che possono essere:
  - definiti dall'amministratore di gara

MASQUERADING

Lo script è stato ideato per permettere quattro situazioni di *masquerading*:

- Un indirizzo unico per tutti i TEAM, che può essere:
  - definito dall'amministratore di gara
  - generato in modo casuale
- Indirizzi diversi per tutti i TEAM, che possono essere:
  - definiti dall'amministratore di gara
  - generati in modo casuale

Regole per il Masquerading

La regola per il **masquerading** è strutturata in questo modo:

```
$ iptables -t nat -A POSTROUTING -o $interface -j SNAT
        --to-source $MASQUERADING_ADDRESS
```