# Class Capture The Flag Contest

Silvio Biagioni <sup>1</sup>

 $^{1}$ Department of Information Engineering and Computer Science, University of Trento

May 25, 2017

Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab



## Outline

Who am I?

**DETERLab** 

## Class Capture The Flag

Network Topology

Rounds

Goal

Operational Details

Bank Server Access

Forming Groups

#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

▶ PhD Student

Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

- ▶ PhD Student
- Security Risk Assessment for Attack Surfaceces



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

- ▶ PhD Student
- Security Risk Assessment for Attack Surfaceces



For you Opportunity to apply your skills

Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

- ▶ PhD Student
- Security Risk Assessment for Attack Surfaceces



For you Opportunity to apply your skills For me Improve my research © Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

- ▶ PhD Student
- Security Risk Assessment for Attack Surfaceces



For you Opportunity to apply your skills For me Improve my research © Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

- ▶ PhD Student
- Security Risk Assessment for Attack Surfaceces



For you Opportunity to apply your skills For me Improve my research © Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

PhD Student

Securia Bill Amendment Risk

For At All Needed Information

Link Link to the student's wiki (TBD)

For you Opportunity to apply your skills For me Improve my research © Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

# cyber DEfense Technology Experimental Research (DETERLab)



Information Science Institute (ISI)

Class Capture The Flag Contest

Silvio Biagioni

Who am I?

 $\mathsf{DETERLab}$ 

lass Capture The

# cyber DEfense Technology Experimental Research (DETERLab)



Information Science Institute (ISI)

▶ DETERLab



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

# cyber DEfense Technology Experimental Research (DETERLab)

USC University of Southern California

Information Science Institute (ISI)

▶ DETERI ab



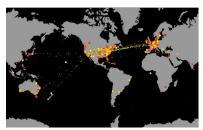


Figure: Global worm DDoS topology on single target

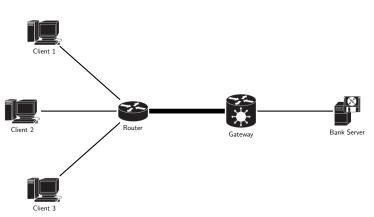
Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

ass Capture The



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

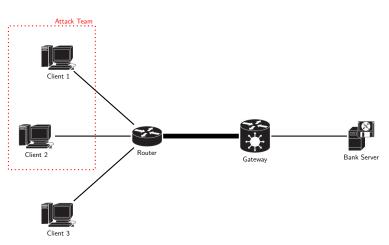
Class Capture The

Network Topology

Round

perational Det

ank Server A



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

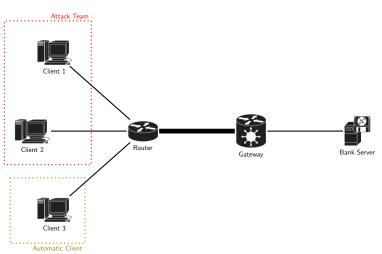
Class Capture The

Network Topology

Rounds Goal

Operational Det

sank Server Acce



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLah

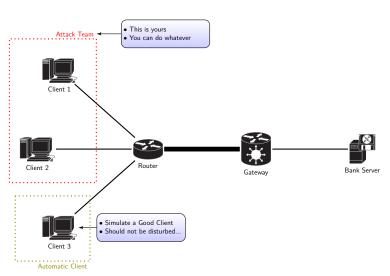
Class Capture The

Network Topology

Rounds Goal

Operational Deta

Dalik Jerver Acces



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

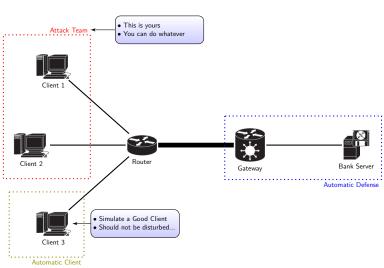
Class Capture The

Network Topology

Rounds

Operational Deta

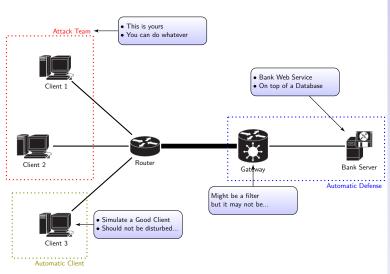
- - -



#### Class Capture The Flag Contest

Silvio Biagioni

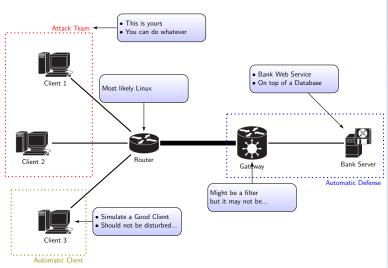
Network Topology



#### Class Capture The Flag Contest

Silvio Biagioni

Network Topology



#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The

Network Topology

Rounds

Operational Deta

Forming Crouns

Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

Class Capture The Flag

etwork Topology

Rounds

0----

ink Server Acce

1. Questionnaire on Web Application Security



#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

Class Capture The Flag

Network Topology

Rounds Goal

> erational Details nk Server Access

- 1. Questionnaire on Web Application Security
  - ▶ SQL injection



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

Class Capture The Flag

Network Topology

Rounds Goal

erational Details

- 1. Questionnaire on Web Application Security
  - ► SQL injection
  - XSS



#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

Class Capture The Flag

Network Topology

Rounds Goal

> perational Details ink Server Access rming Groups

- 1. Questionnaire on Web Application Security
  - ▶ SQL injection
  - XSS
  - HTTP misconfigurations



Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The Flag

Rounds Rounds

Goal

perational Details ink Server Access rming Groups

- 1. Questionnaire on Web Application Security
  - ▶ SQL injection
  - XSS
  - HTTP misconfigurations
- 1 Day to compromise a Level 0 config (super-vulnerable)





#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The Flag

Network Topology Rounds

Sank Server Acce

- 1. Questionnaire on Web Application Security
  - ▶ SQL injection
  - XSS
  - HTTP misconfigurations
- 1 Day to compromise a Level 0 config (super-vulnerable)
- 5 Days to compromise a Level 1 config (hardening OS, Server)





Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The Flag

Network Topology Rounds

Operational Detai

- Questionnaire on Web Application Security
  - ► SQL injection
  - XSS
  - HTTP misconfigurations
- 1 Day to compromise a Level 0 config (super-vulnerable)
- 5 Days to compromise a Level 1 config (hardening OS, Server)
- 4. 5 Days to compromise a Level 2 config





Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLED

Flag

Network Topology Rounds

Operational Detail

Bank Server Acce

## Goal

Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The Flag

Network Topology

Goal

perational Detai ank Server Acces

## Goal

 Confidentiality Exfiltrate all Data on Bank Accounts Integrity Modify Bank Accounts Availability Provoke a DoS



#### Class Capture The Flag Contest

Silvio Biagioni

Who am I

**DETERLab** 

Class Capture The

twork Topology

Goal

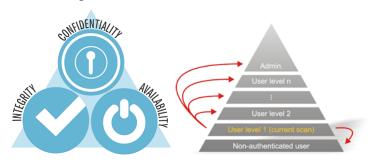
erational De

nk Server Access

## Goal

 Confidentiality Exfiltrate all Data on Bank Accounts Integrity Modify Bank Accounts Availability Provoke a DoS

▶ Privilege Escalation



#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

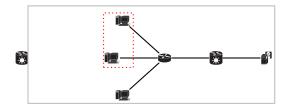
Class Capture The

Network Topology

Goal

perational Detai

Bank Server Access



#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

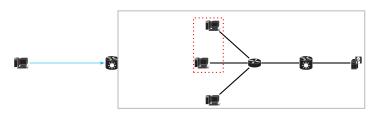
DETERLab

Class Capture The

Network Topology

Goal

Operational Details



► ssh unitn9ab@users.deterlab.net

#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

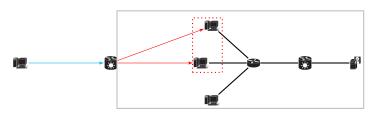
Class Capture The

Network Topology

Goal

Operational Details

Bank Server Access
Forming Groups



- ► ssh unitn9ab@users.deterlab.net
- ssh client1.exp1.ExperCCTF1.isi.deterlab.net

#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

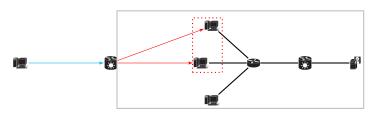
Class Capture The

Network Topology

Goal

Operational Details

Bank Server Access



- ► ssh\_unitn9ab@users.deterlab.net
- ssh client1.exp1.ExperCCTF1.isi.deterlab.net
  - same for the other nodes (for you, not yet...)

#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The

Network Topology

Goal

Operational Details

## Bank Server Access

to GUI or not GUI... waiting Jelena

#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The Flag

Network Topology

Goal

Operational Details

Bank Server Access

# Forming Groups

- my contact
- how many people per group

#### Class Capture The Flag Contest

Silvio Biagioni

# Thanks for your Attention!



#### Class Capture The Flag Contest

Silvio Biagioni

Who am I?

**DETERLab** 

Class Capture The Flag

Network Topology Rounds

perational Details