Class Capture The
Flag
Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The
Flag

Class Capture The Flag Contest

Silvio Biagioni [1]

[1]Department of Information Engineering and Computer Science,
University of Trento

May 27, 2017

Outline

Class Capture The
Flag
Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The
Flag

Who am I

- ▶ PhD Student

Who am I

Class Capture The
Flag
Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The
Flag

- ▶ PhD Student
- ▶ Security Risk Assessment
  for Attack Surfaceces

Who am I

Class Capture The
Flag
Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The
Flag

- ▶ PhD Student
- ▶ Security Risk Assessment for Attack Surfaceces

For you Opportunity to apply your skills

Who am I

- ▶ PhD Student
- ▶ Security Risk Assessment for Attack Surfaceces

For you Opportunity to apply your skills

For me Improve my research ☺

Who am I

Class Capture The
Flag
Contest

Silvio Biagioni

Who am I?

DETERLab

Class Capture The
Flag

- PhD Student
- Security Risk Assessment
  for At

All Needed Information

Link to the user guide: (▸ Link)

For y

For me Improve my research ☺

cyber DEfense Technology Experimental Research (DETERLab)

►

Information Science
Institute (ISI)

cyber DEfense Technology Experimental Research (DETERLab)

- USC University of Southern California

  Information Science Institute (ISI)
- DETERLab

cyber DEfense Technology Experimental Research (DETERLab)

- USC University of Southern California

  Information Science Institute (ISI)
- DETERLab
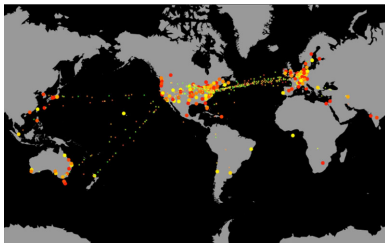
Figure: Global worm DDoS topology on single target

Network Topology

Client 1

Client 2

Router

Gateway

Bank Server

Client 3

Network Topology

Network Topology

Network Topology

Attack Team

- This is yours
- You can do whatever

Client 1

Client 2

Router

Gateway

Bank Server

- Simulate a Good Client
- Should not be disturbed...

Client 3

Automatic Client

Network Topology

Class Capture The
Flag
Contest

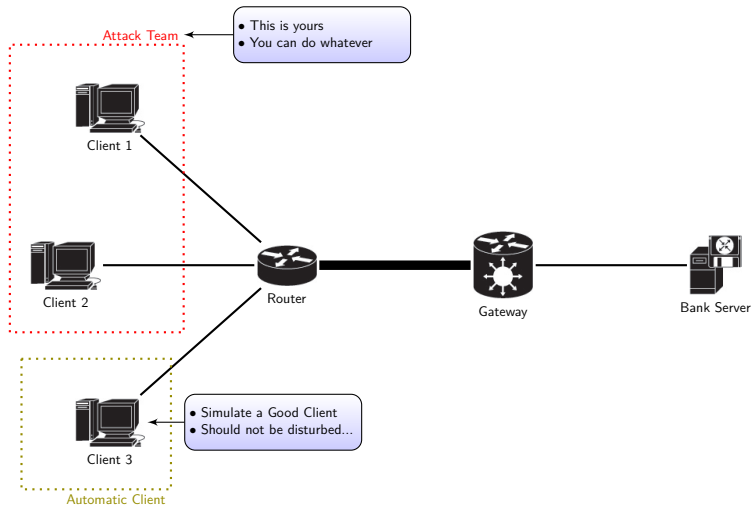Silvio Biagioni

Who am I?

DETERLab

Class Capture The
Flag

Network Topology
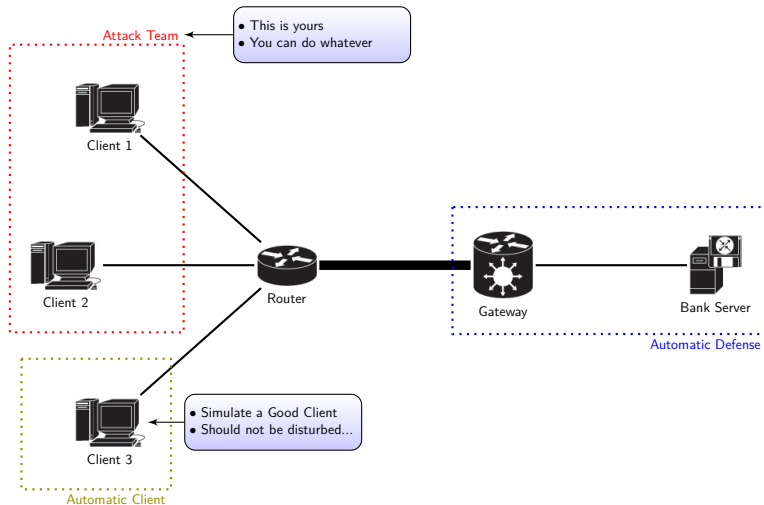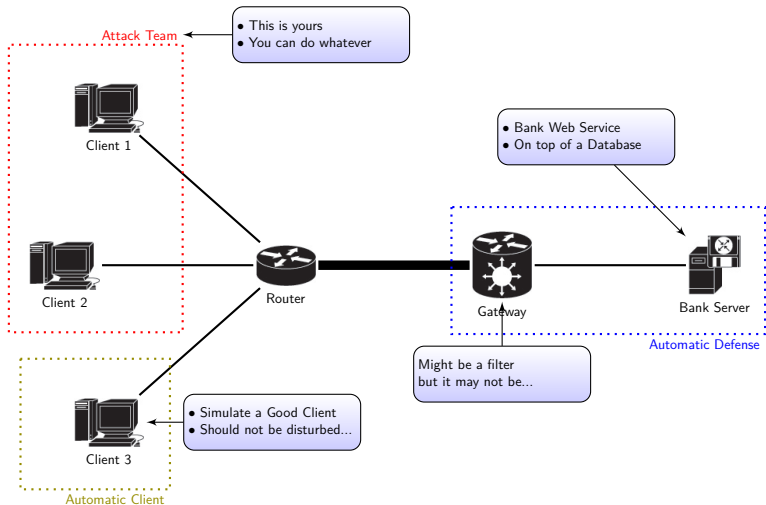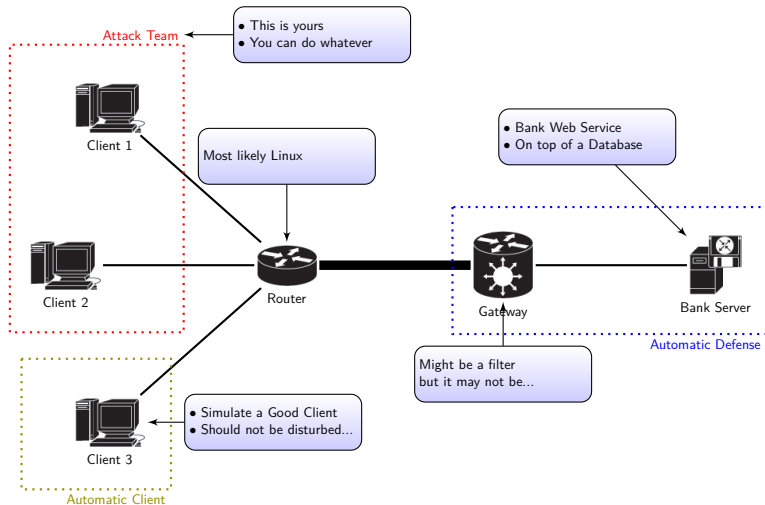
Rounds

Goal

Operational Details

Forming Groups

Network Topology

Network Topology

Attack Team

- This is yours
- You can do whatever

Client 1

Most likely Linux

- Bank Web Service
- On top of a Database

Client 2

Router

Gateway

Bank Server

Automatic Defense

Might be a filter but it may not be...

- Simulate a Good Client
- Should not be disturbed...

Client 3

Automatic Client

Rounds

Rounds

1. Questionnaire

Rounds

1. Questionnaire
   - ▶ Web Admin

Rounds

1. Questionnaire
   - Web Admin
   - Sys/Network Admin

Rounds

1. Questionnaire
   - Web Admin
   - Sys/Network Admin
   - Security

Rounds

1. Questionnaire
   - Web Admin
   - Sys/Network Admin
   - Security
2. 1 Day to compromise
   a Level 0 config
   (super-vulnerable)

Rounds

1. Questionnaire
   - Web Admin
   - Sys/Network Admin
   - Security
2. 1 Day to compromise
   a Level 0 config
   (super-vulnerable)
3. 5 Days to compromise
   a Level 1 config
   (hardening OS, Server)

Rounds

1. Questionnaire
   - Web Admin
   - Sys/Network Admin
   - Security
2. 1 Day to compromise a Level 0 config (super-vulnerable)
3. 5 Days to compromise a Level 1 config (hardening OS, Server)
4. 5 Days to compromise a Level 2 config

Goal

Goal

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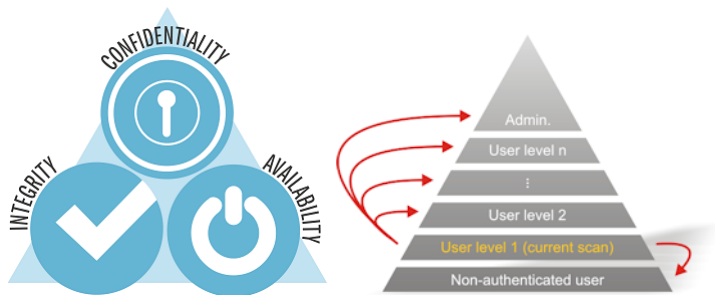 Integrity Modify Bank Accounts
  Availability Provoke a DoS

Goal

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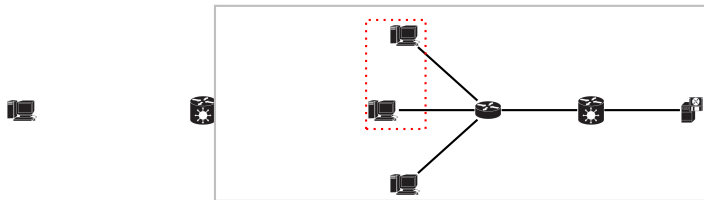 Availability Provoke a DoS
- Privilege Escalation

Operational Details
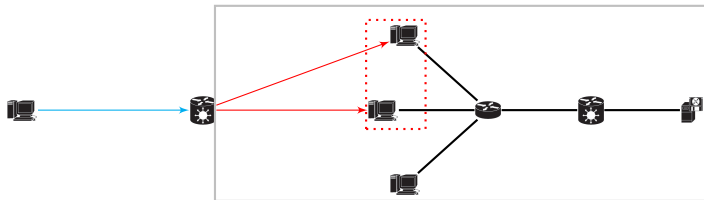## Client Access

Operational Details
Client Access

▶ ssh unitn9ab@users.deterlab.net

Operational Details

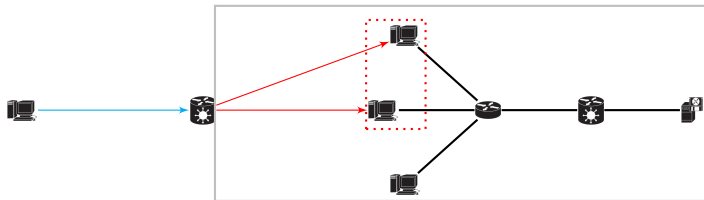## Client Access

- ▶ ssh unitn9ab@users.deterlab.net
- ▶ ssh client1.exp1.ExperCCTF1.isi.deterlab.net
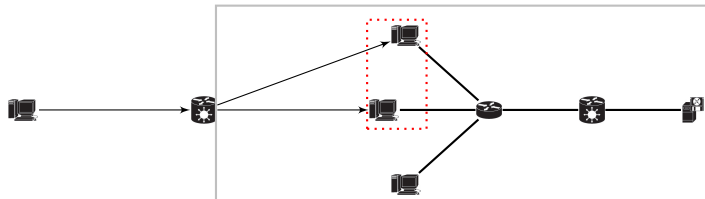
Operational Details
Client Access

- ▶ ssh unitn9ab@users.deterlab.net
- ▶ ssh client1.exp1.ExperCCTF1.isi.deterlab.net
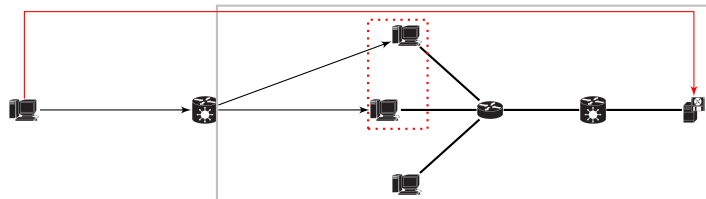   - ▶ same for the other nodes (for you, not yet...)

Operational Details

Bank Server Access
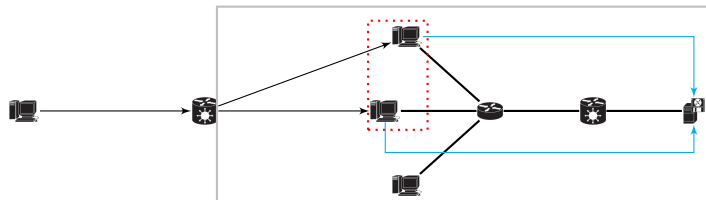
Operational Details
Bank Server Access

- ▶ Local Browser
  - ▶ ssh -L 8080:pc184:80 unitn9ab@users.isi.deterlab.net

Operational Details
Bank Server Access

- ▶ Local Browser
  - ▶ ssh -L 8080:pc184:80 unitn9ab@users.isi.deterlab.net
- ▶ Command Line Browser
  - ▶ lynx server.exp1.expercctf1.isi.deterlab.net/index.html

Forming Groups

Forming Groups

- For each Team 2-3 people

Forming Groups

- For each Team 2-3 people
- Email me (members in CC)

Thanks for your Attention!