# Who's Hacking Who?

## From Russia with Love

*Hackers - 1995*

D. Barry[1] L.Bol[1]

[1]Computer Science Society
University of Hertforshire

October, 2016

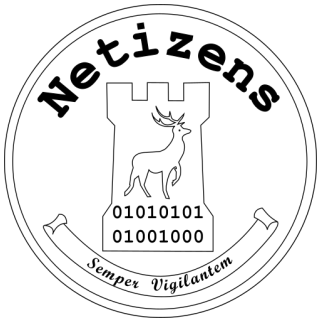
# Table of Contents

# Credentials

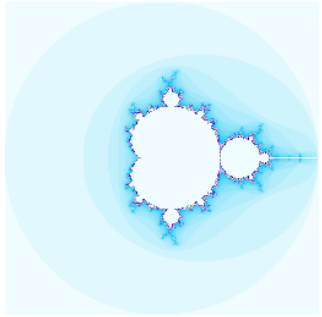
| | Daniel Barry | Lukasz Bol |
|---|---|---|
| |  |  |
| From | Essex, UK | Lodz, Poland |
| Study | MSc | BSc (3rd Year) |
| Society | Mentor | Chair |
| Speciality | AI | IoT |
| University | (Past) Student Rep | (Past) Student Rep |
| | PAL Leader | PAL Leader |
| | Student Proctor | Student Proctor |
| Work Exp | Visteon | Self-employed DJ |

# Previous Projects

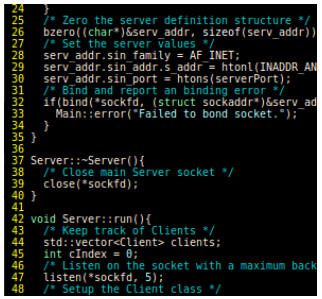
RoboCup - *Football playing robots*




Netizens - *UH hacking group*



General Programming - *Too much to mention!*




PAL & Proctoring - *Mentoring students*

# Aims Over Time

- [ ] Why are people hacking?
- [ ] What hacking is going on?
- [ ] Who is hacking?

# Aims Today

- [ ] Learn about hacking
- [ ] Setup a development environment
- [ ] Introduction to the tools
- [ ] Build a monitoring program

# Why Hack?

Financial

Power

Information

Relationships

# Targets of Hacking


DYN [1]


OVH [2]


WikiLeaks [3]


JANET [4]

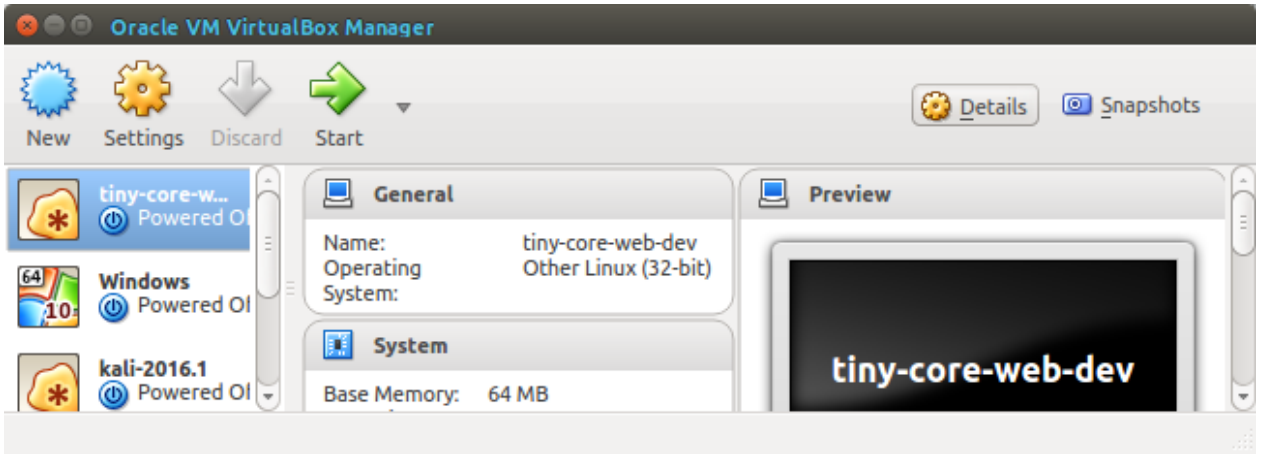
# Attacks on Servers

- (D)DoS - (Distributed) Denial of Service
- Privilege Escalation
- Database Injection
- Exploits (Metasploit and CVEs)
- And many, many others

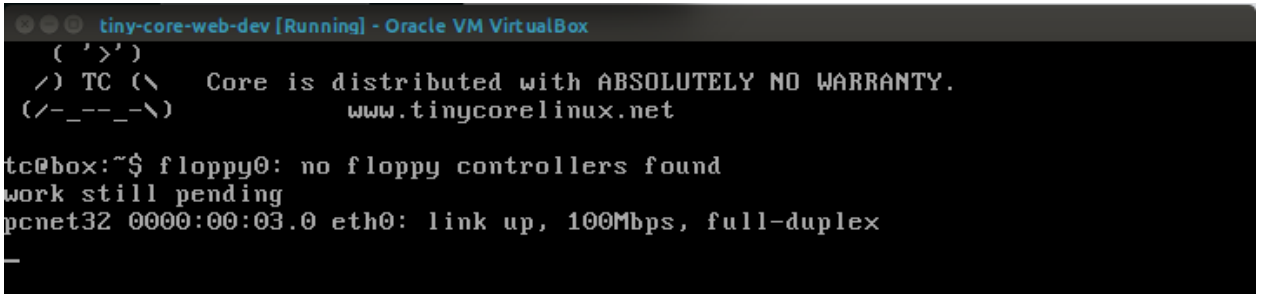
# Download

- https://www.virtualbox.org/wiki/Downloads
- http://coffeespace.org.uk/downloads/tiny-core-web-dev.zip
- http://coffeespace.org.uk/downloads/tiny-core-web-test.zip
- http://coffeespace.org.uk/downloads/Core-7.2.iso

# Dev Virtual Machine




And if run:



# Running

```
tc@box:~$ sudo -s
root@box:/home/tc#
```

Listing 1: Root Access

```
root@box:/home/tc# cd /mnt/sda1/home/tc
root@box:/mnt/sda1/home/tc#
```

Listing 2: Saveable Location

```
root@box:/home/tc# ash setup.sh
```

Listing 3: Setup Network

# Test Virtual Machine

```
tc@box:~$ sudo -s
root@box:/home/tc#

```

Listing 4: Root Access

```
root@box:/home/tc# ifconfig eth0 192.168.1.100 netmask
    255.255.255.0 broadcast 192.168.1.255 up

```

Listing 5: Setup Netork

Both machines should now be able to ping one another.

# Basics of Linux

- '`cd [DIRECTORY]`' - "Change Directory"
- '`nano [FILE]`' - Simple text editor
- '`tce-ab`' - Search for packages
- '`tce-load -wi [PACKAGE]`' - Install a package
- '`[CMD] --help`' - Produces help for a command
- '`[CMD] > [FILE]`' - Save output of command to file

# Tools

‘`tcpdump port [NUM] and '(tcp-syn|tcp-ack)!=0'`’

- What is TCP, SYN and ACK?
- What is a port and which is interesting?

# Advanced

For those of you who want a challenge:

- [ ] Setup a web server (Nginx, Apache, etc)
- [ ] Search logs for interesting cases (directory traverse)
- [ ] Interesting ports to watch
- [ ] Honey trapping connected users

# Achievements

- [X] Learn about hacking
- [X] Setup a development environment
- [X] Introduction to the tools
- [?] Build a monitoring program

# Wrapping Up

Any questions?

# References

[1] Paganini, P. "150,000 IoT Devices behind the 1Tbps DDoS attack on OVH", URL: http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html?, 2016.

[2] York, K. "Dyn Statement on 10/21/2016 DDoS Attack", URL: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/, 2016.

[3] WikiLeaks. "WikiLeaks", URL: https://www.wikileaks.org/, 2016.

[4] Martin, A. "UK research network Janet under ongoing and persistent DDoS attack", URL: http://www.theregister.co.uk/2015/12/07/janet_under_persistent_ddos_attack/, 2016.