

# Who's Hacking Who?

From Russia with Love



*Hackers - 1995*

D. Barry<sup>1</sup>   L.Bol<sup>1</sup>

<sup>1</sup>Computer Science Society  
University of Hertfordshire

October, 2016

# Table of Contents

- 1 Introduction
- 2 Aims
- 3 History
- 4 Environment
- 5 Conclusion

# Credentials



Intro

Aims

History

Env

End

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

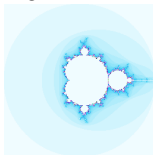
# Previous Projects



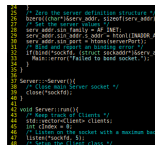
RoboCup - *Football playing robots*



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

Intro

Aims

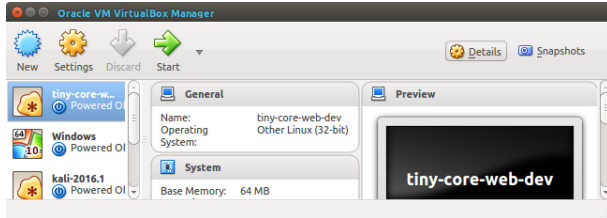
History

Env

End

- <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:

```
tiny-core-web-dev [Running] - Oracle VM VirtualBox
( ' > )
/) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
(/-__-_-\)   www.tinycorelinux.net

tc@box:~$ floppy0: no floppy controllers found
work still pending
pcnet32 0000:00:03.0 eth0: link up, 100Mbps, full-duplex
_
```

# Running

```
1 tc@box:~$ sudo -s
2 root@box:/home/tc#
3
```

Listing 1: Root Access

```
1 root@box:/home/tc# cd /mnt/sda1/home/tc
2 root@box:/mnt/sda1/home/tc#
3
```

Listing 2: Saveable Location

```
1 root@box:/home/tc# ash setup.sh
2
```

Listing 3: Setup Network

# Test Virtual Machine

```
1 tc@box:~$ sudo -s
2 root@box:/home/tc#
3
```

Listing 4: Root Access

```
1 root@box:/home/tc# ifconfig eth0 192.168.1.100 netmask
    255.255.255.0 broadcast 192.168.1.255 up
2
```

Listing 5: Setup Netork

Both machines should now be able to ping one another.

# Basics of Linux

Intro

Aims

History

Env

End

- `'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

`'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/](http://www.theregister.co.uk/2015/12/07/janet_under_persistent_ddos_attack/), 2016.