**COS30015 Internet Security**

You will need:

Kali (VM)

CySCA2014inaBox (VM)

Windows 95

A computer with internet access

### Lab 4 (week 4) Denial of Service attacks

In this lab you will perform some simple attacks while   
observing their effects.

1. Start *Kali*.

Start *CYSCA2014InABox*.

2. On Kali, start **Wireshark**

3. On CYSCA2014InABox, log in:

User: **user**

Password: **CYSCA2014user**

Top monitors the CPU load used by the top 15 programs running in the VM.

4. On Kali, log in: (other)

User: **root**

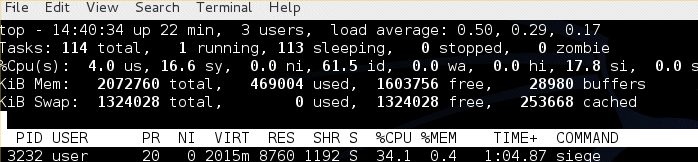
Password: **toor**

Run top:

**top**

In Kali look at the id field in top:

*Kali TOP id (IDLE %) field during a* **siege** *attack*



It should be close to 100 (i.e. 100% idle)

From the menu we will launch a DDOS attack:

***Applications / Vulnerability Analysis / Stress Testing / Network Stress Testing / siege***

A new console appears, with the help for siege.

Before you start the attack, watch the output of TOP in CYSCA2014InABox.

*99.0%*

***What is the value of CYSCA'a TOP id?***

Swap over to Kali.

***What is the value of Kali's TOP id?***

*99.9%*

In the Kali console for siege, type this:

**siege --concurrent=250 192.168.100.210**

*75.4%*

***What is the value of Kali's TOP id?***

*0.0%*

***What is the value of CYSCA'S TOP id?***

A large number of processes have appeared in the CYSCA Top list.

*Network services / apache2*

***which application to they belong to?***

On the host PC, look up

“siege stress test”.

***What does siege do?***

Stress testing and benchmarking tool designed to simulate a large number of users interacting with a web server.

***What would happen if 10,000 computers used siege on a computer at the same time?***

*Overwhelm the server, leading to DoS*

5. Run ***Windows95***.



Double-click on the clock so that you can see the clock   
face with the second hand (moving).

Use ***nmap*** to find the IP address of the win95 machine:

**nmap –sP 192.168.100.0/24**

***What is the target IP address?***

***Look for the IP you haven't seen before***

*192.168.100.211*

***x is the final octet of the IP address.***

To confirm that it is *win95*,

**nmap –O 192.168.100**.x

***NMAP matches the behaviour of the TCP/IP stack. Sometimes the guess matches a previous version.***

***What is nmap's guess?***

*All open*

Try using jolt:

***This can be tricky. Try to shrink the VM a bit and then drag* jolt.c *to an empty part of the desktop. Alternatively transfer by USB drive.***

Download ***jolt.c*** from Canvas.

Drag it onto the Kali desktop

In a spare console, *cd* to the desktop

**cd Desktop**

Compile it:

***You can monitor the network traffic using wireshark running on the Kali machine, even though Kali is not being attacked.***

**gcc –o jolt jolt.c**

Run it:

**./jolt 192.168.100.x 192.168.100.x 100**

***Is Win95 running?***

*unresponsive*

**Shutdown the VMs.**

**Kali: 'q' will stop top. type in poweroff**

**Win95 – use the VMPlayer menu to close it.**

**CYSCA: 'q' to stop top. sudo poweroff**

**followed by CYSCA2014user //the user password**

**6. HOIC, LOIC, xOIC**

Look up the *Low Orbit Ion Cannon*.

*Network stress testing tool commonly used for launching DoS attack*

***What is it?***

***How many versions are there?***

*Two main versions*

***Why is it so popular with script kiddies?***

*Easy to use and used in high-profile hacktivist*

***What about the High Orbit Ion Cannon?***

*Updated version of LOIC, designed to generate more powerful attacks by targeting multiple websites simultaneously.*

***What techniques mitigate or stop DDOS attacks?***

*Traffic filtering, Load balancing, rate limiting, CDN usage, anycast routing.*