Name: ____ Student ID:_______________

You will need:
Kali (VM)
CySCA2014inaBox (VM)
Windows 95 (VM)
A computer with internet access

COS30015 Internet Security

Lab 4 (week 4) Denial of Service attacks

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

1. Start the *Kali with local network* VM.
   Start the *CYSCA2014InABox with local network* VM.

2. On Kali, start **Wireshark**

3. On CYSCA2014InABox, log in:
User: **`user`**
Password: **`CYSCA2014user`**

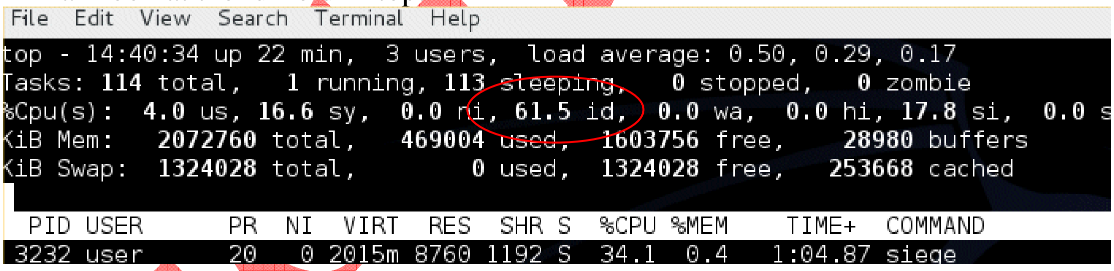
Top monitors the CPU load used by the top 15 programs running in the VM.

4. On Kali, log in: (other)
User: **`root`**
Password: **`toor`**

Run top:

```
top
```

In Kali look at the id field in top:



```
top - 14:40:34 up 22 min,  3 users,  load average: 0.50, 0.29, 0.17
Tasks: 114 total,   1 running, 113 sleeping,   0 stopped,   0 zombie
%Cpu(s):  4.0 us, 16.6 sy,  0.0 ni, 61.5 id,  0.0 wa,  0.0 hi, 17.8 si,  0.0 s
KiB Mem:   2072760 total,   469004 used,  1603756 free,    28980 buffers
KiB Swap:  1324028 total,        0 used,  1324028 free,   253668 cached

  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+  COMMAND
 3232 user      20   0 2015m 8760 1192 S  34.1  0.4   1:04.87 siege
```

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 / Kali linux / 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.

What is the value of CYSCA'a TOP id?

Over 99%

Swap over to Kali.

Name: ____ Student ID:______________

What is the value of Kali's TOP id?

Over 99%

In the Kali console for siege, type this:

```
siege --concurrent=250 192.168.100.210
```

What is the value of Kali's TOP id?

60-70%

What is the value of CYSCA'S TOP id?

0 - 35%

A large number of processes have appeared in the CYSCA Top list.
which application to they belong to?

Apache2

On the host PC, look up
"siege stress test".

What does siege do?

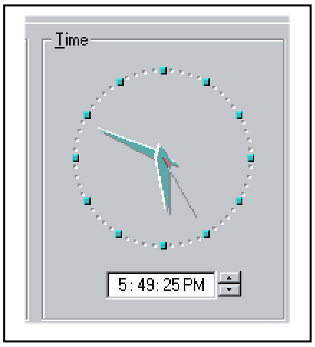
http load testing.

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

DDOS

6. Download and run the ***Windows95 with local network*** virtual machine.

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
```

Name: ______________________________________ Student ID:______________

What is the target IP address?

Look for the IP you haven't seen before

192.168.100.211

To confirm that it is *win95*,

```
    nmap -O 192.168.100.x
```

x is the final octet of the IP address.

What is nmap's guess? Windows NT4 SP3

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

Try using jolt:
Download ***jolt.c*** from Blackboard.
Drag it onto the Kali desktop
In a spare console, *cd* to the desktop

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.*

```
cd Desktop
```

Compile it:

```
gcc -o jolt jolt.c
```

Run it:

```
    ./jolt 192.168.100.x 192.168.100.x 100
```

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

Is Win95 running?

No. the clock stopped

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

7. HOIC, LOIC, xOIC

Look up the *Low Orbit Ion Cannon*.

What is it? DDOS attack tool for web sites

How many versions are there?

Original C#, java, LOIC++

Why is it so popular with script kiddies?

Easy to use – click and attack

What about the High Orbit Ion Cannon?

Easy to use – more powerful – attacks multiple resources on the same target web site

What techniques mitigate or stop DDOS attacks?

Blackholing, DDOS mitigation cloud services