OWASP Cape Town Chapter Meeting 1

<Name>Christo Goosen
<Role>Chapter Leader
<Organization>OWASP CPT
<email> christo.goosen@owasp dot org
<phone>

OWASP

<date>2015/06/17

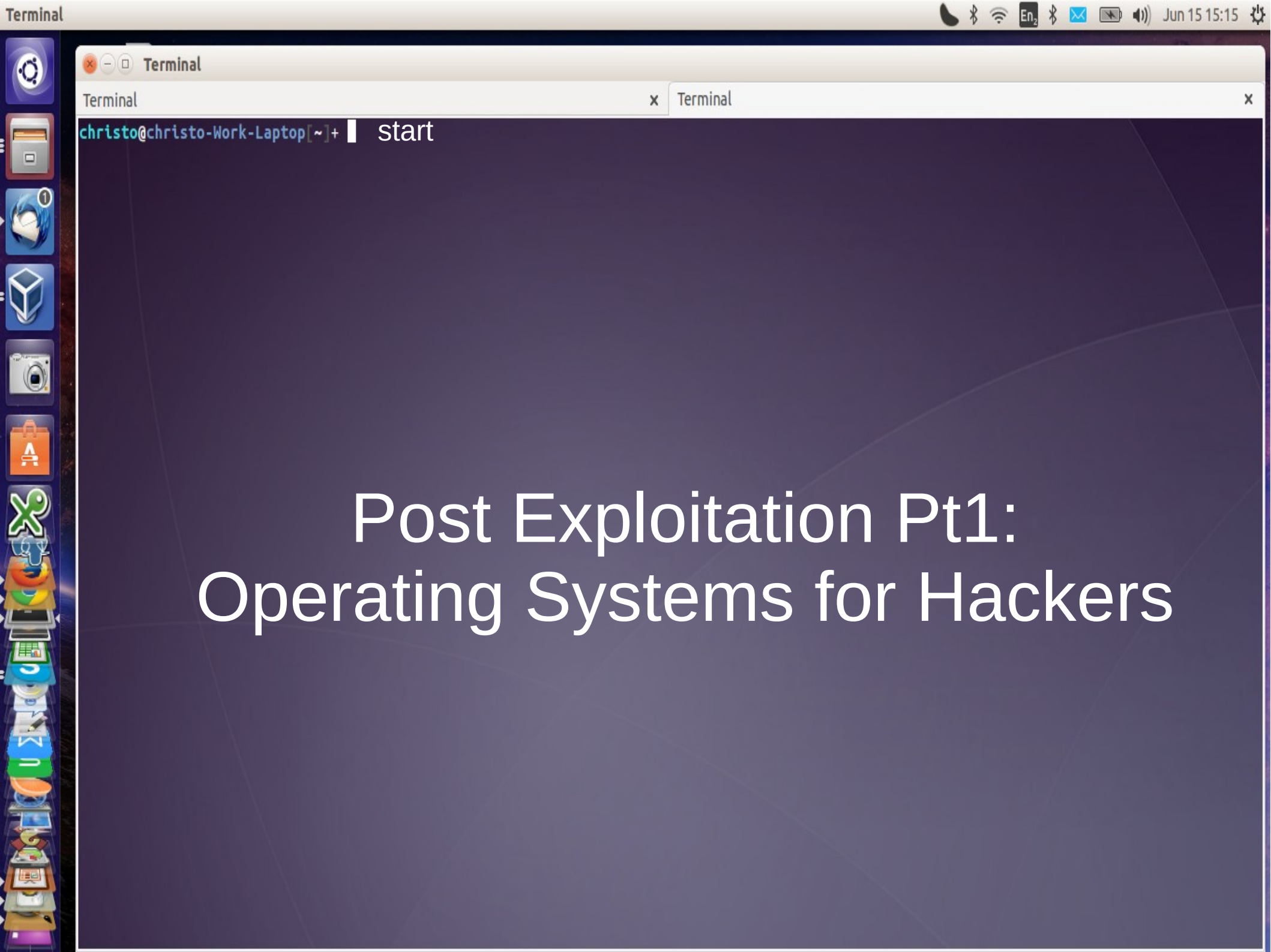
The OWASP Foundation

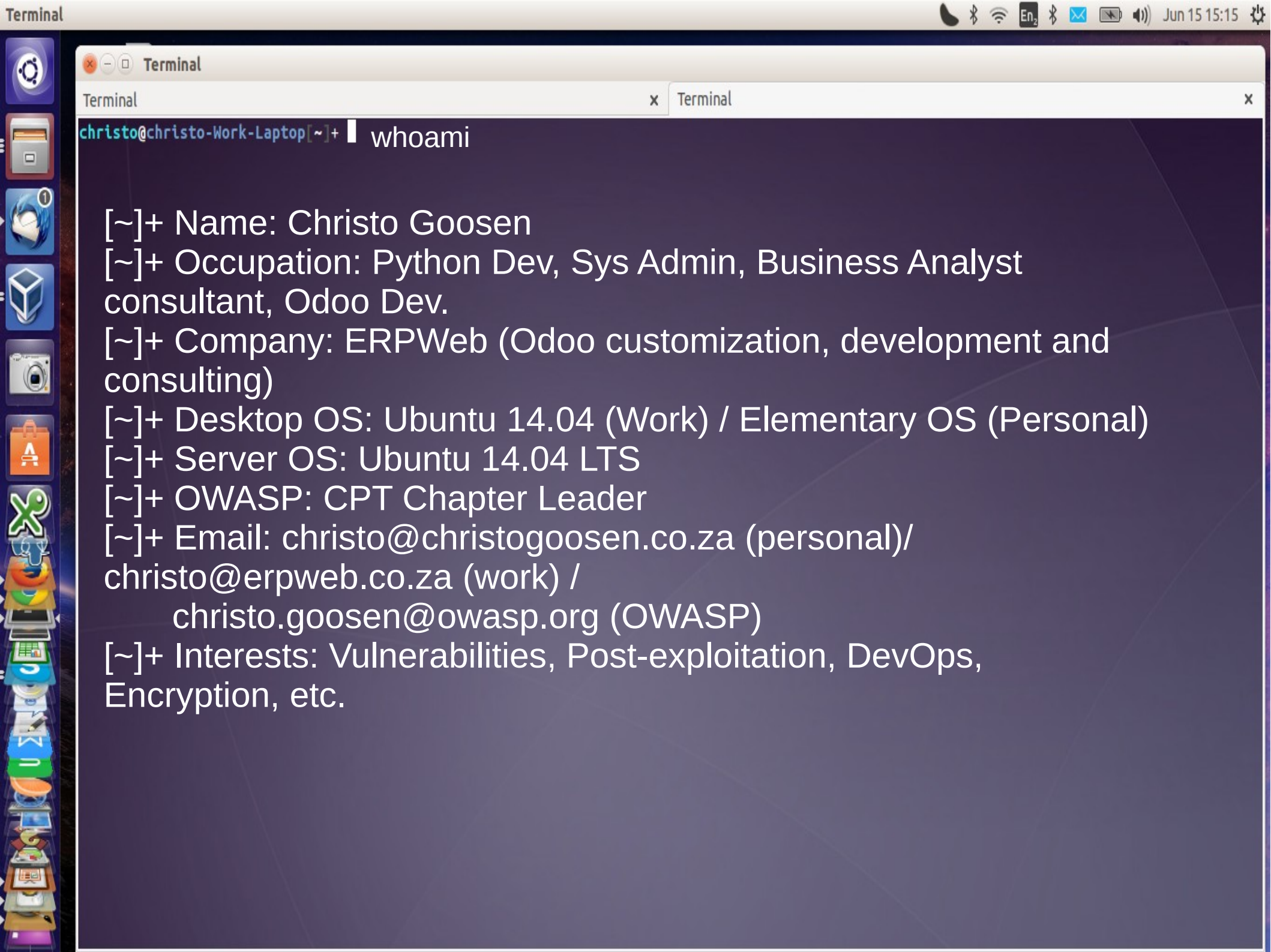
http://www.owasp.org

OWASP

The OWASP Foundation

http://www.owasp.org


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ start
Post Exploitation Pt1:
Operating Systems for Hackers


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ whoami
[~]+ Name: Christo Goosen
[~]+ Occupation: Python Dev, Sys Admin, Business Analyst consultant, Odoo Dev.
[~]+ Company: ERPWeb (Odoo customization, development and consulting)
[~]+ Desktop OS: Ubuntu 14.04 (Work) / Elementary OS (Personal)
[~]+ Server OS: Ubuntu 14.04 LTS
[~]+ OWASP: CPT Chapter Leader
[~]+ Email: christo@christogoosen.co.za (personal)/ christo@erpweb.co.za (work) /
christo.goosen@owasp.org (OWASP)
[~]+ Interests: Vulnerabilities, Post-exploitation, DevOps, Encryption, etc.

Terminal

Jun 15 15:15

Terminal

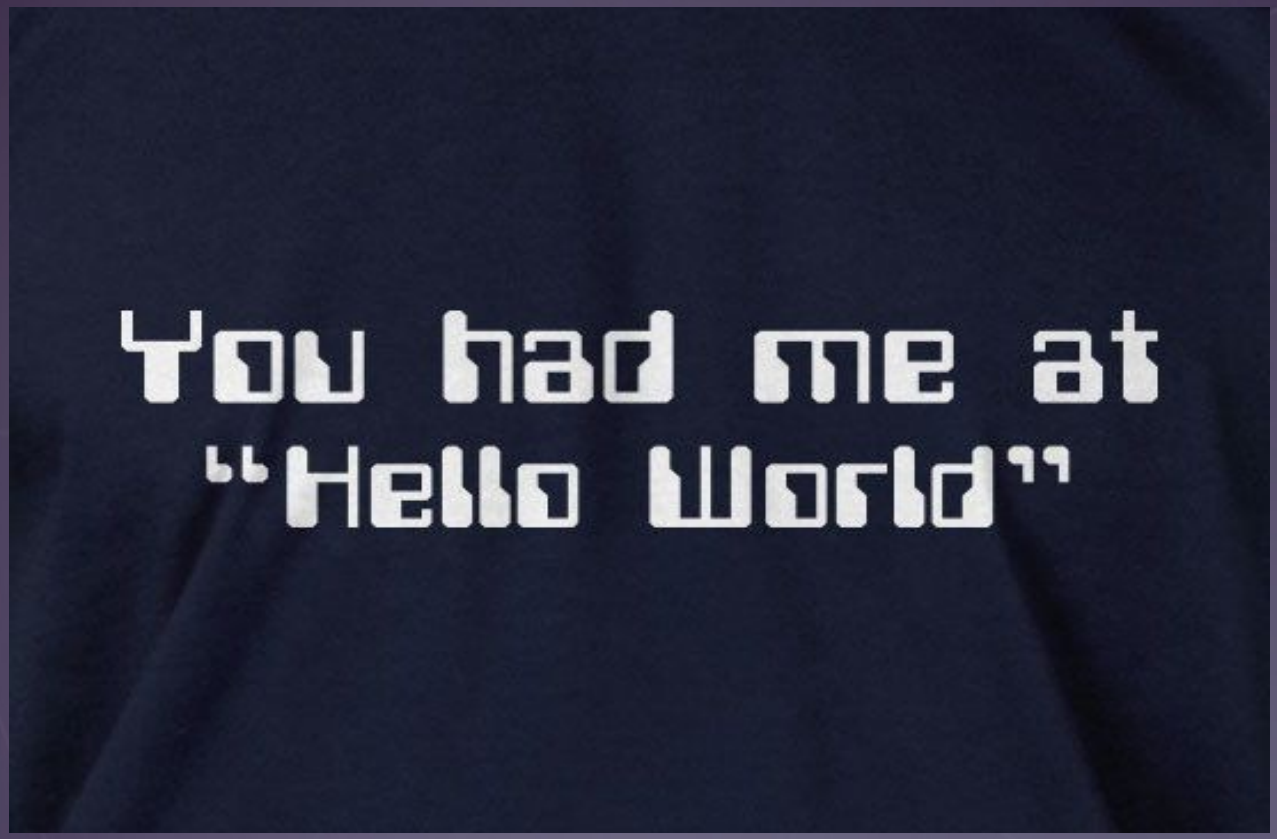
Terminal

Terminal

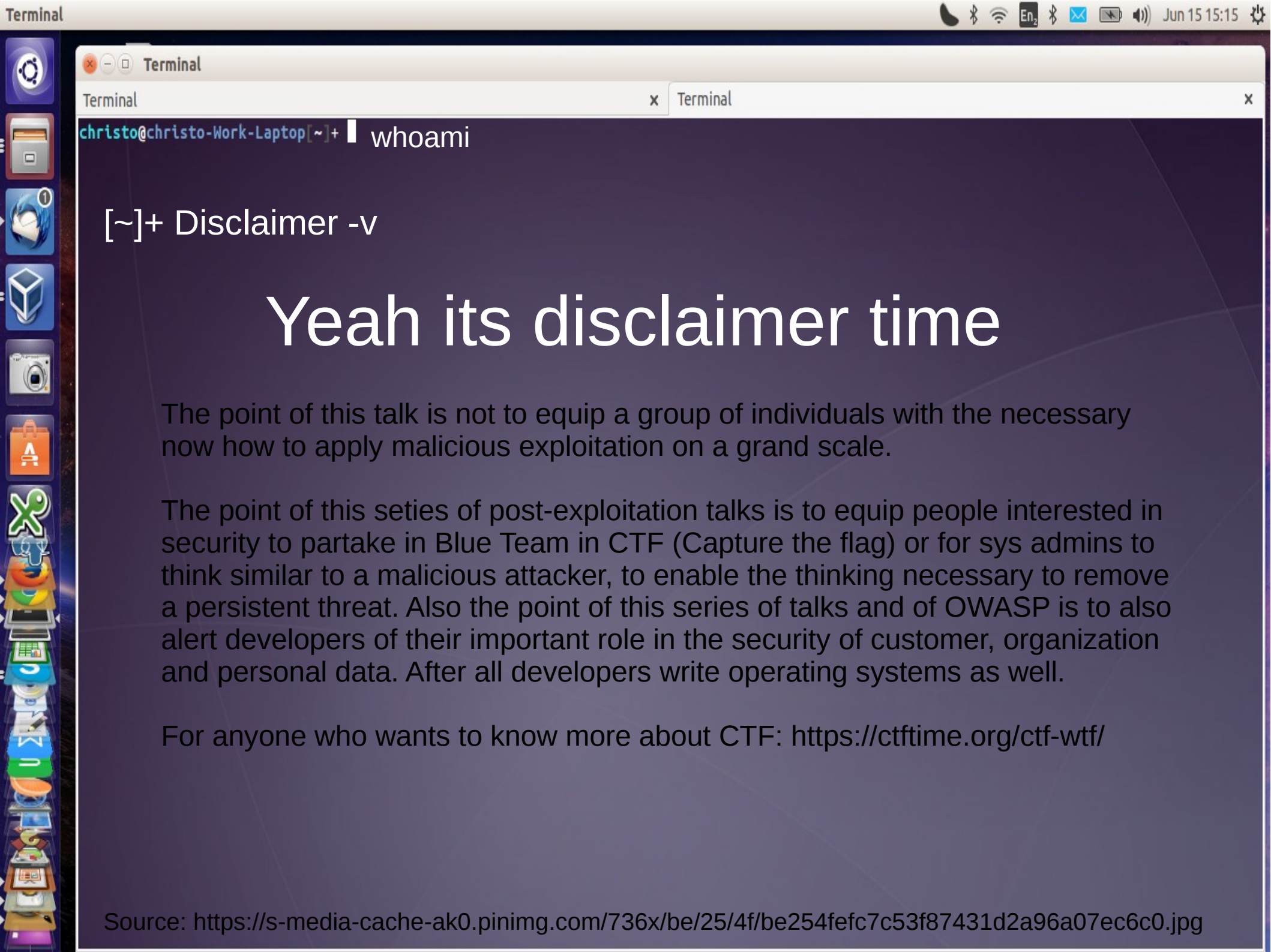
christo@christo-Work-Laptop[~]+ whoami

[~]+ Disclaimer -v

Yeah its disclaimer time



Source: https://s-media-cache-ak0.pinimg.com/736x/be/25/4f/be254fefc7c53f87431d2a96a07ec6c0.jpg


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ whoami
[~]+ Disclaimer -v
Yeah its disclaimer time
The point of this talk is not to equip a group of individuals with the necessary now how to apply malicious exploitation on a grand scale.
The point of this seties of post-exploitation talks is to equip people interested in security to partake in Blue Team in CTF (Capture the flag) or for sys admins to think similar to a malicious attacker, to enable the thinking necessary to remove a persistent threat. Also the point of this series of talks and of OWASP is to also alert developers of their important role in the security of customer, organization and personal data. After all developers write operating systems as well.
For anyone who wants to know more about CTF: https://ctftime.org/ctf-wtf/
Source: https://s-media-cache-ak0.pinimg.com/736x/be/25/4f/be254fefc7c53f87431d2a96a07ec6c0.jpg

Terminal

Jun 15 15:15

Terminal

Terminal

Terminal

christo@christo-Work-Laptop[~]+ whoami

[~]+ lifeline -h

Potential lifelines or protection

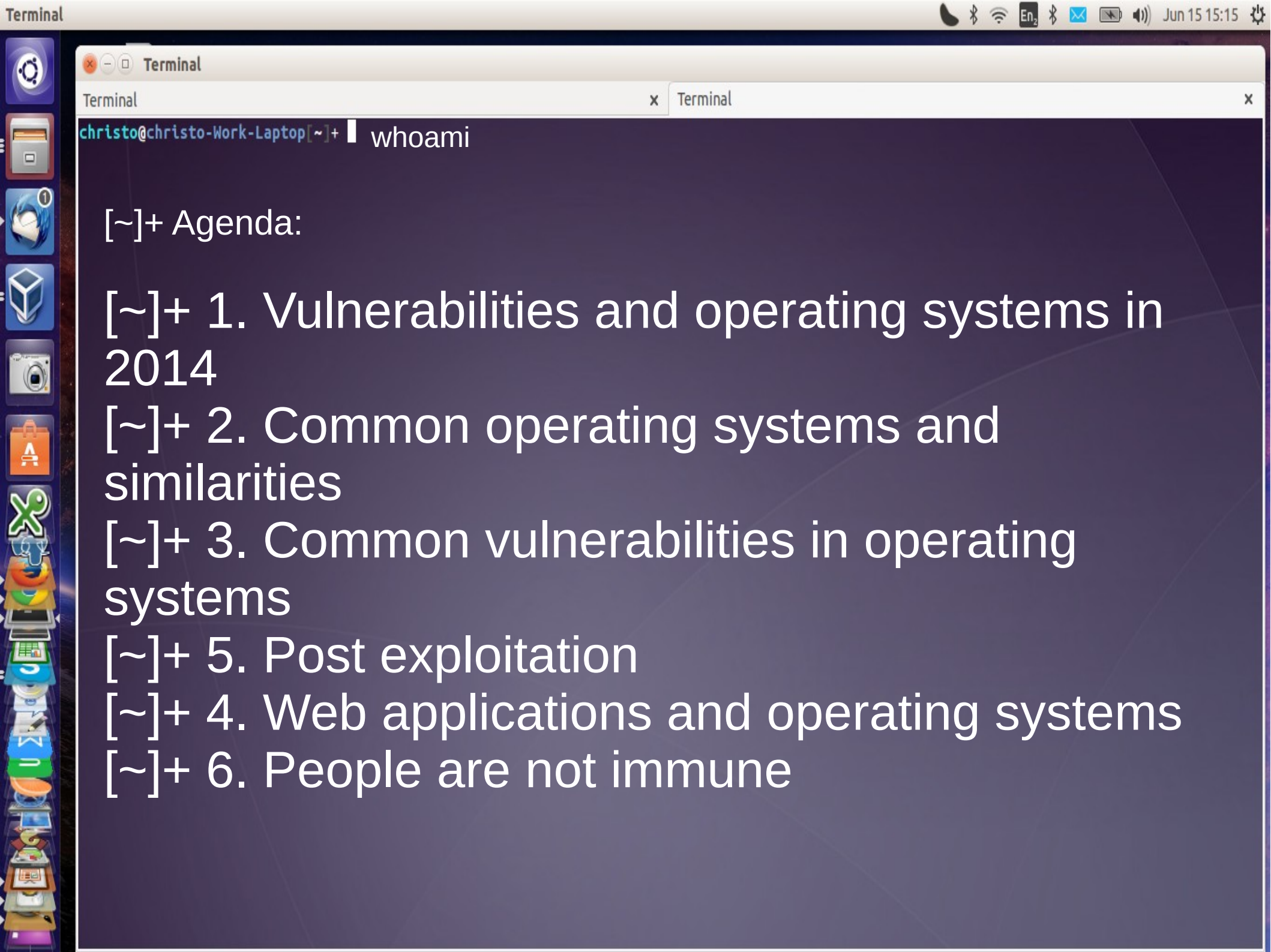
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

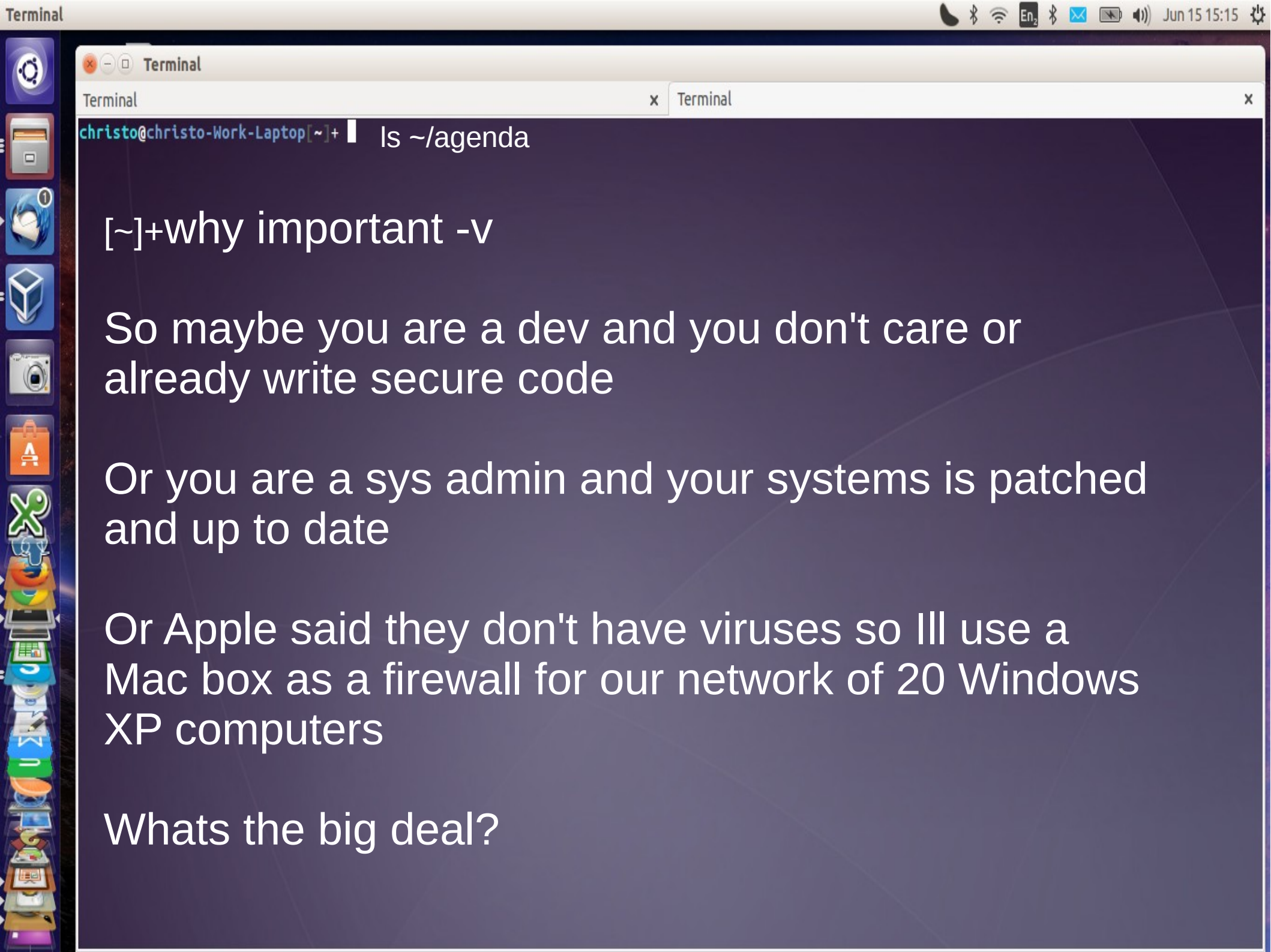
RIGHT2KNOW

vbox

Tails
theamnesicincognitolivesystem

TorProject.org


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ whoami
[~]+ Agenda:
[~]+ 1. Vulnerabilities and operating systems in 2014
[~]+ 2. Common operating systems and similarities
[~]+ 3. Common vulnerabilities in operating systems
[~]+ 5. Post exploitation
[~]+ 4. Web applications and operating systems
[~]+ 6. People are not immune


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ ls ~/agenda
[~]+why important -v
So maybe you are a dev and you don't care or already write secure code
Or you are a sys admin and your systems is patched and up to date
Or Apple said they don't have viruses so Ill use a Mac box as a firewall for our network of 20 Windows XP computers
Whats the big deal?

Terminal

Jun 15 15:15

Terminal

Terminal

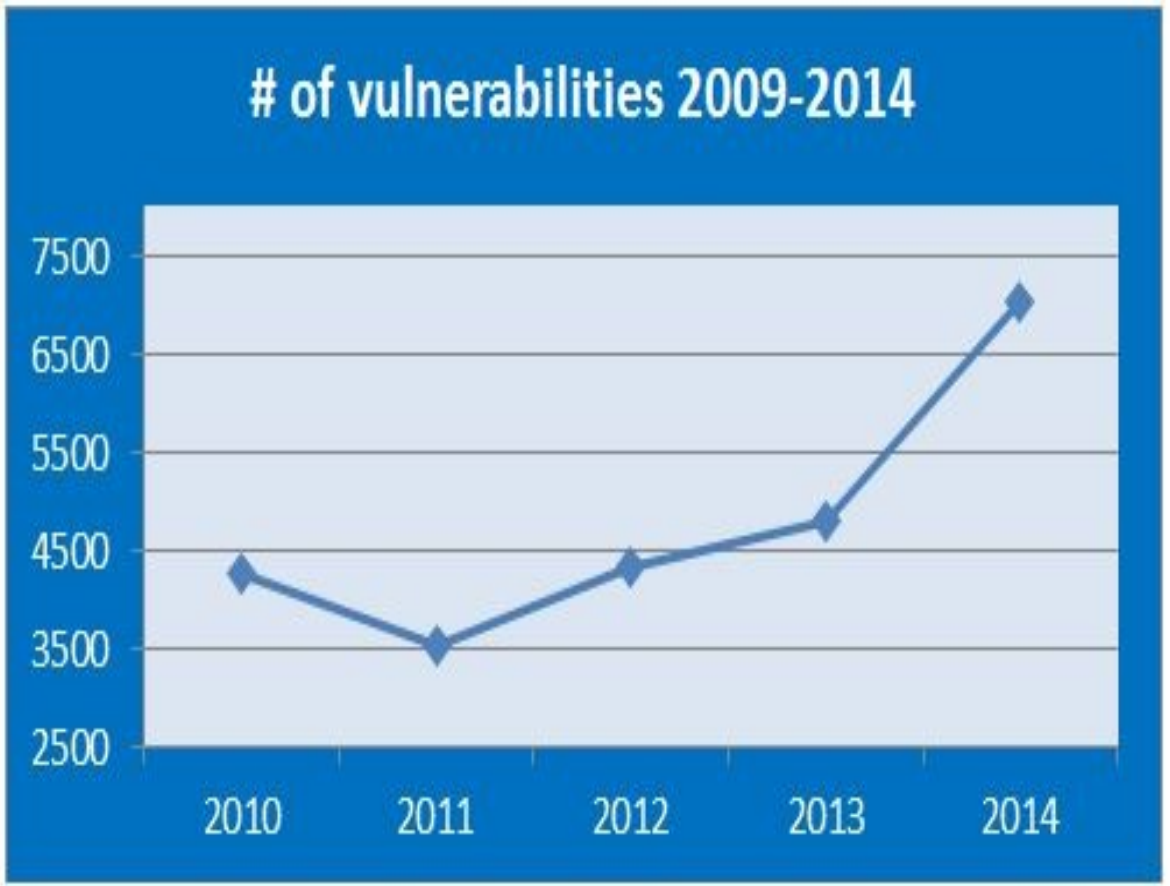
Terminal

christo@christo-Work-Laptop[~]+ statistics

[~]+ Vulnerabilities of 2014:

Some statistics:

Year	# of vulnerabilities
2010	4,258
2011	3,532
2012	4,347
2013	4,794
2014	7,038



Source: http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/

Terminal

Jun 15 15:15

Terminal

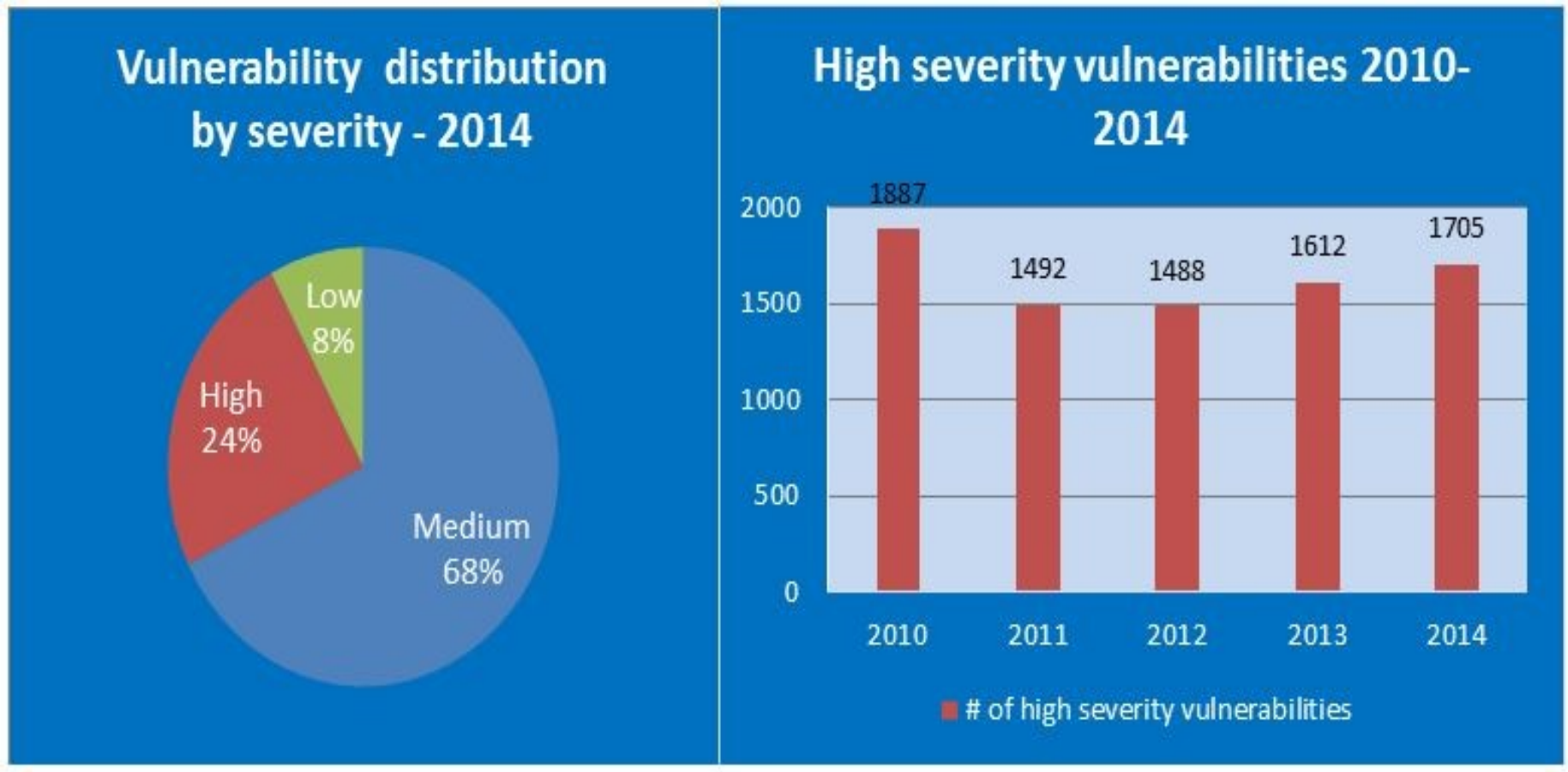
Terminal

Terminal

christo@christo-Work-Laptop[~]+ pretty_graphs

[~]+ Vulnerabilities of 2014:

Severity of the vulnerabilities



Source: http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/

Terminal

Jun 15 15:15

Terminal

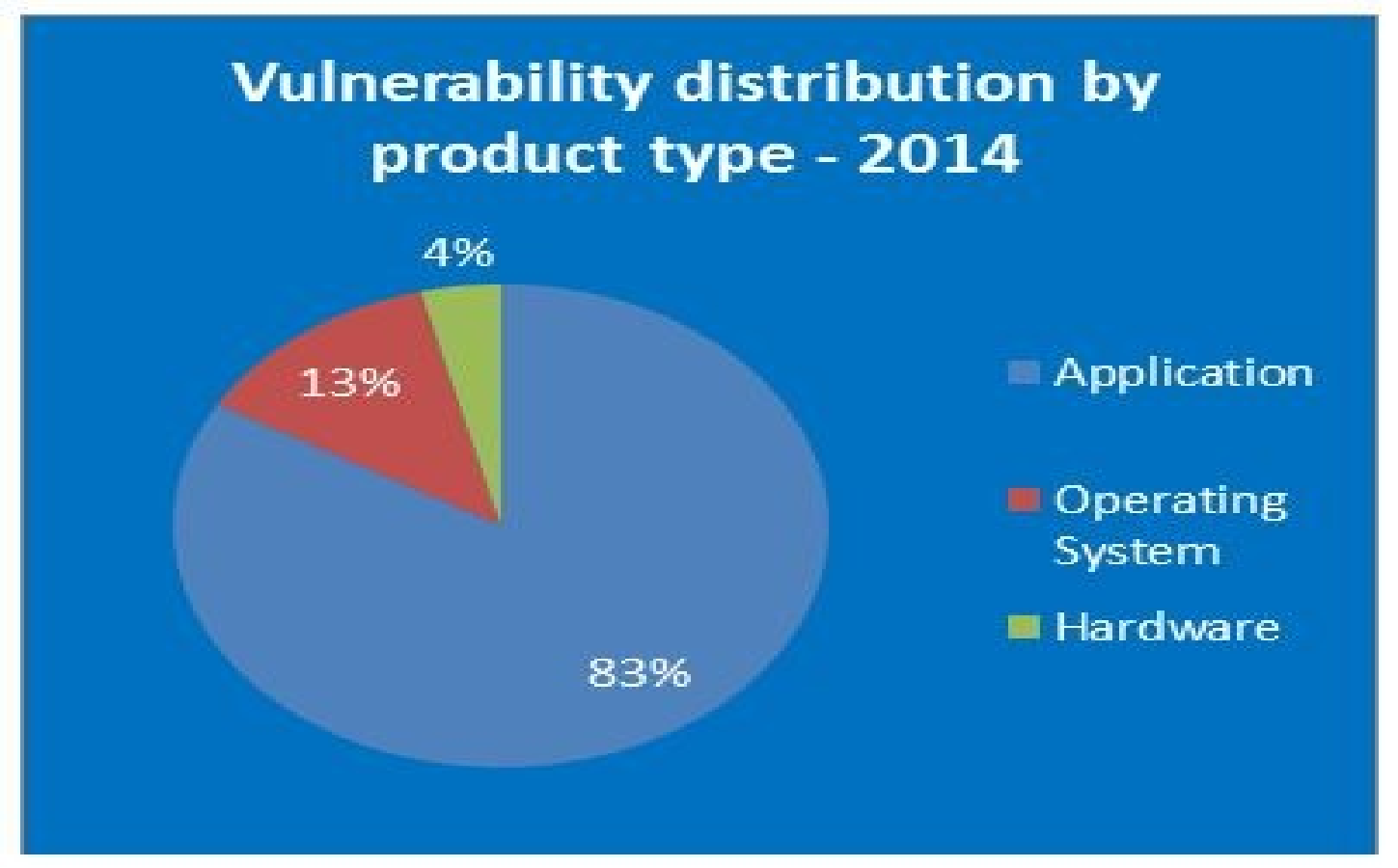
Terminal

Terminal

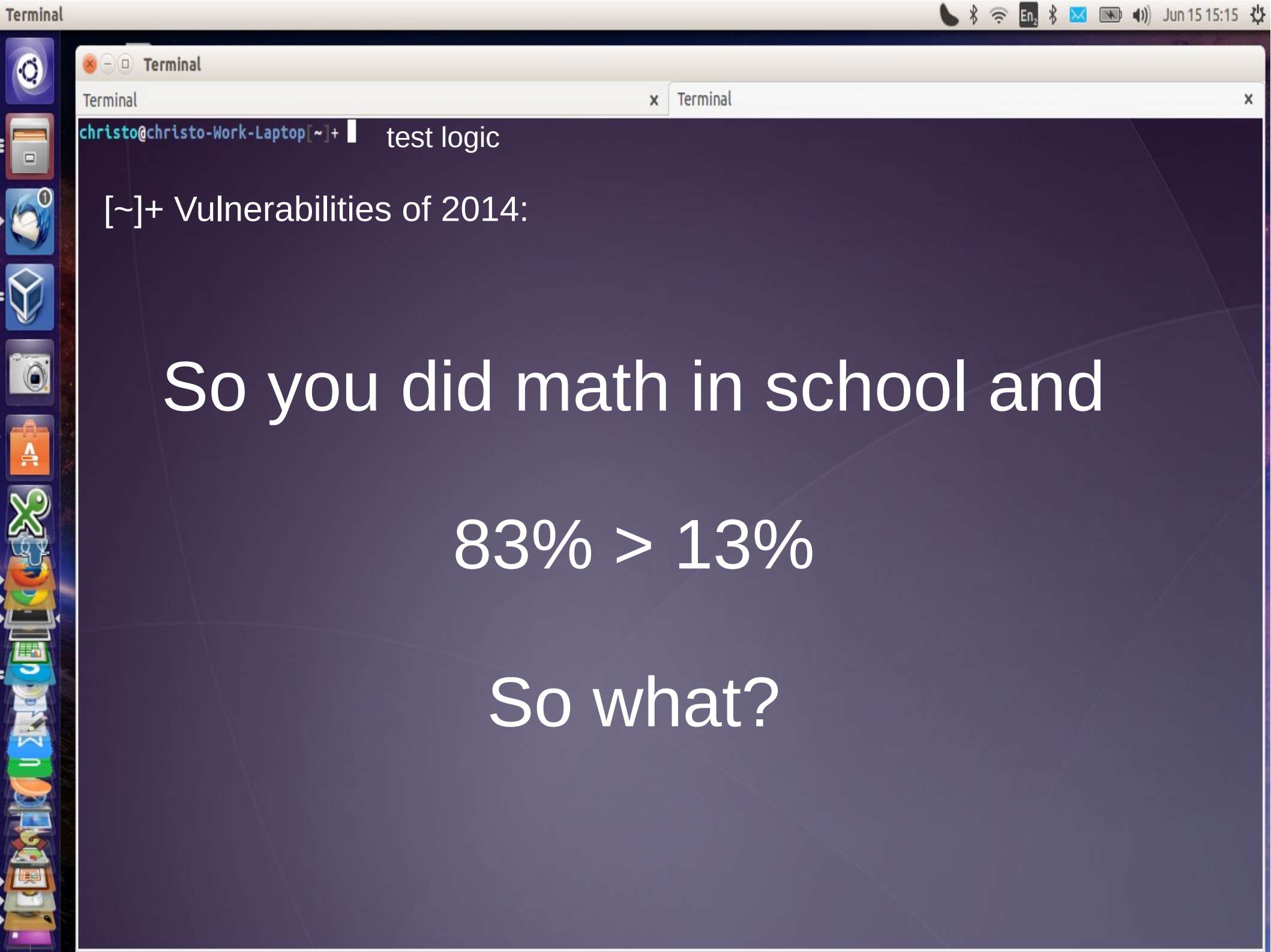
christo@christo-Work-Laptop[~]+ piechart

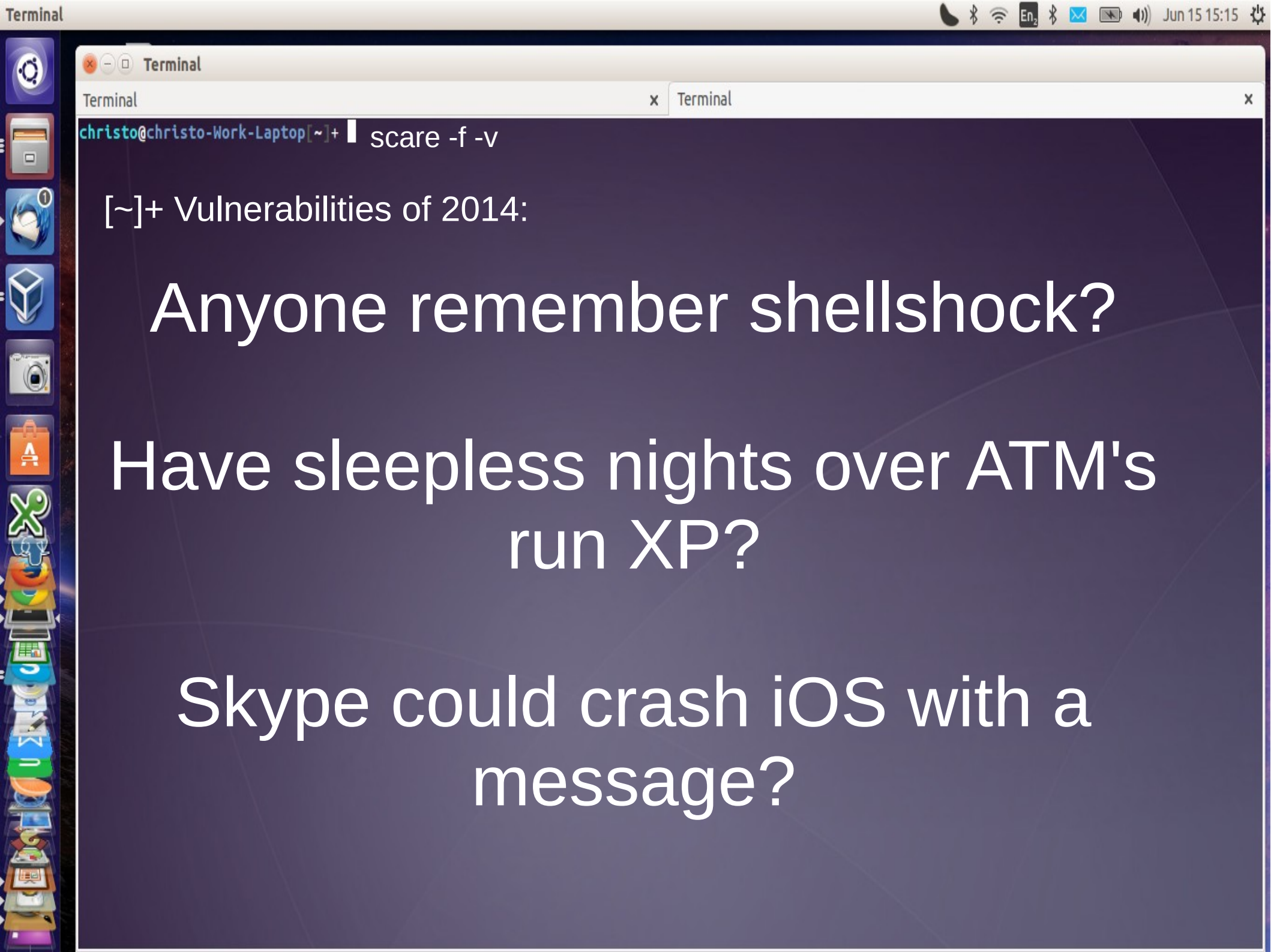
[~]+ Vulnerabilities of 2014:

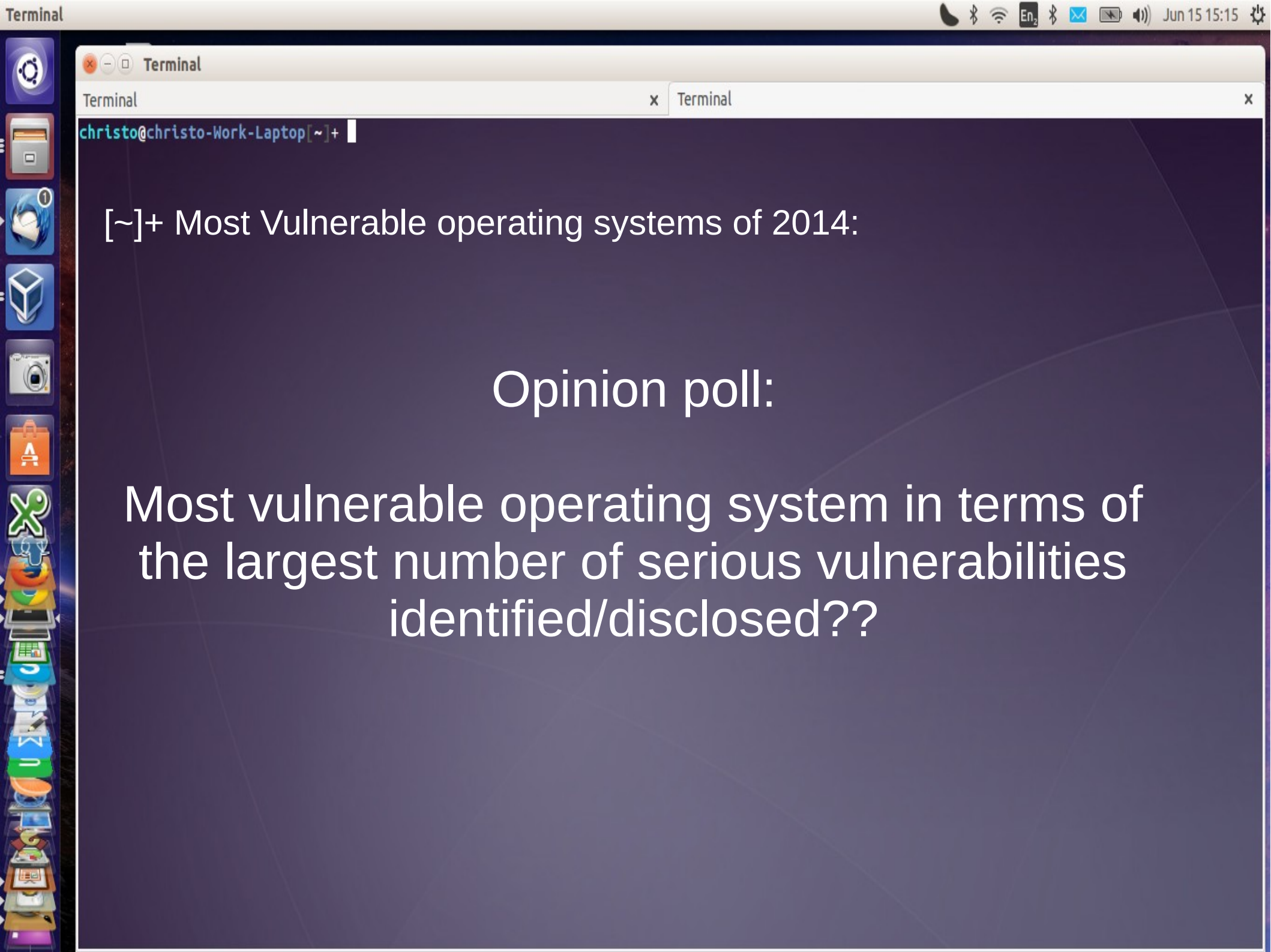
Distribution of the vulnerabilities

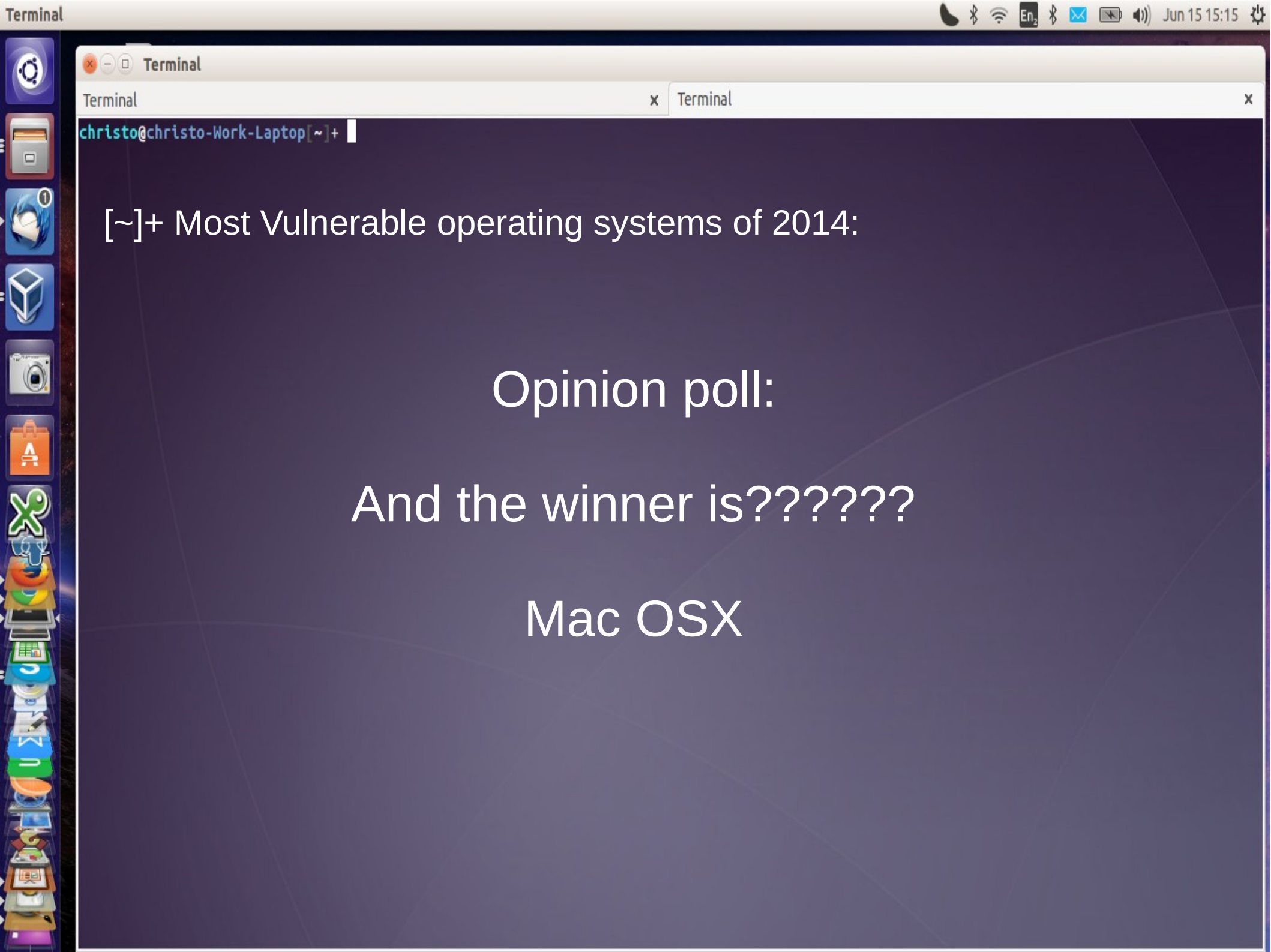


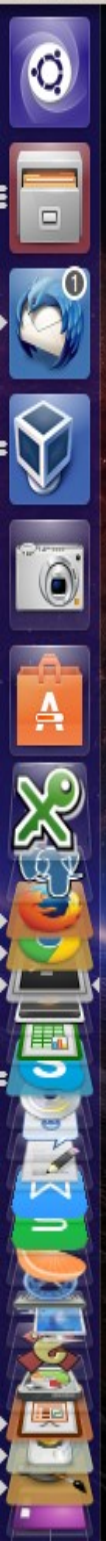
Source: http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ test logic
[~]+ Vulnerabilities of 2014:
So you did math in school and
83% > 13%
So what?


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ scare -f -v
[~]+ Vulnerabilities of 2014:
Anyone remember shellshock?
Have sleepless nights over ATM's run XP?
Skype could crash iOS with a message?


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Most Vulnerable operating systems of 2014:
Opinion poll:
Most vulnerable operating system in terms of the largest number of serious vulnerabilities identified/disclosed??


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Most Vulnerable operating systems of 2014:
Opinion poll:
And the winner is??????
Mac OSX



Terminal

Terminal x Terminal x

```
christo@christo-Work-Laptop[~]+
```

[~]+ Most Vulnerable operating systems of 2014:

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

Terminal

Terminal

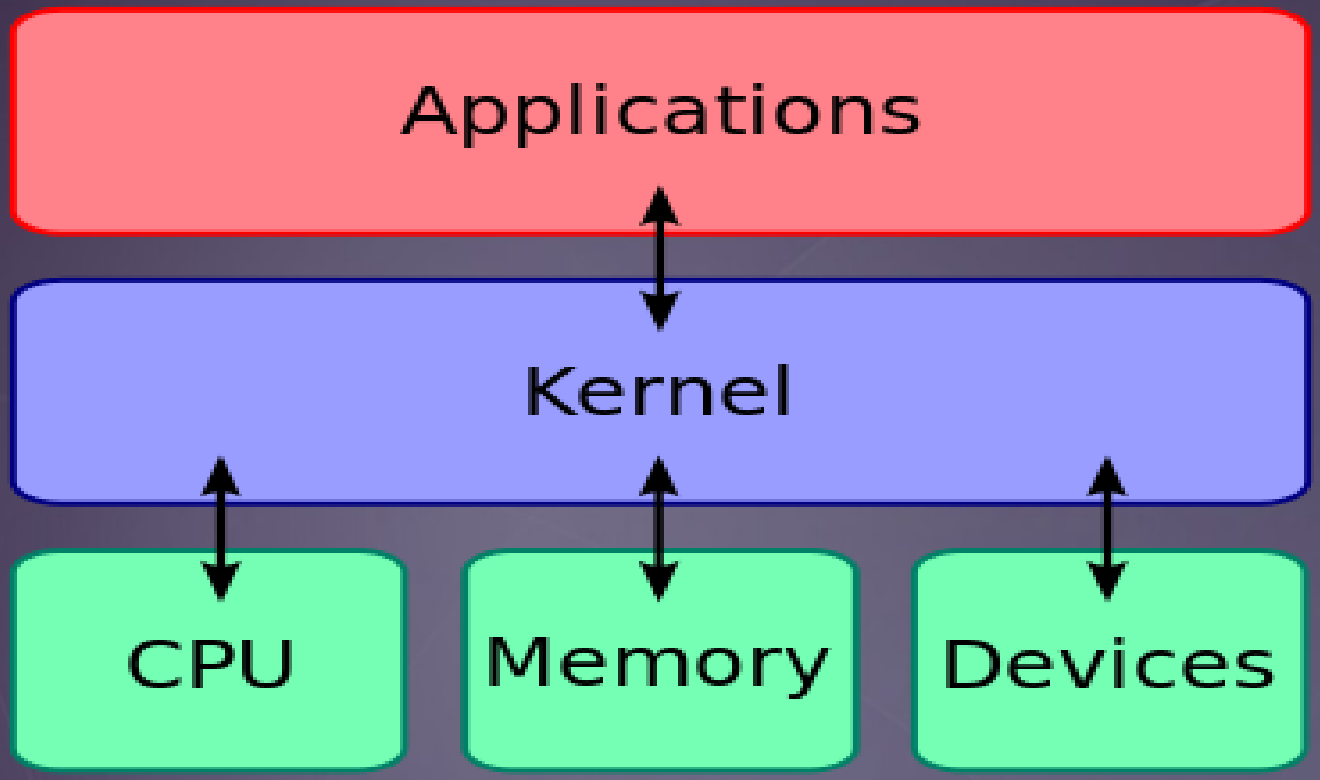
Terminal

Terminal

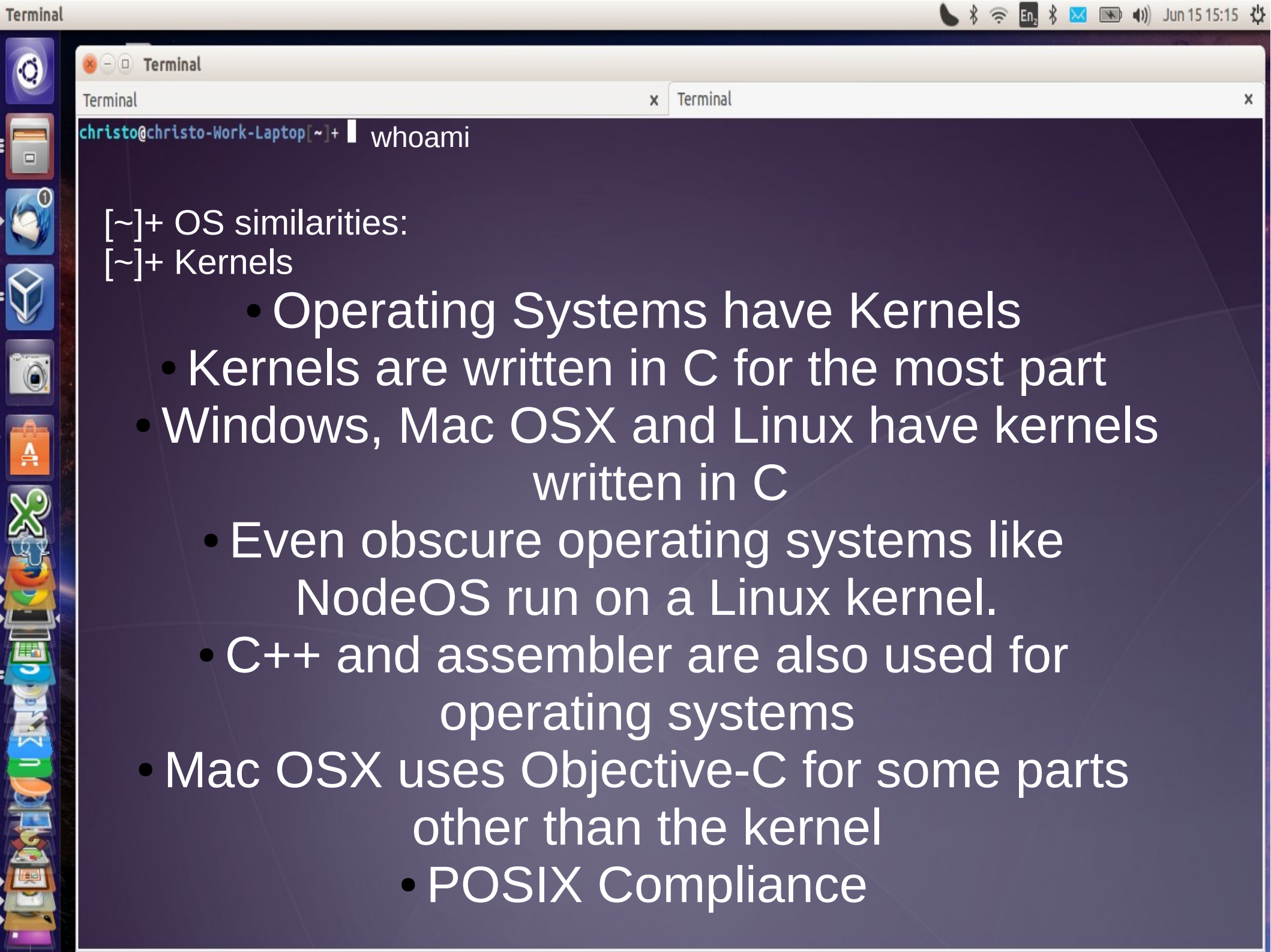
christo@christo-Work-Laptop[~]+ Uname -r

[~]+ Common operating systems:

- Kernels



Source: https://en.wikipedia.org/wiki/Kernel_%28operating_system%29#/media/File:Kernel_Layout.svg


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+ whoami
[~]+ OS similarities:
[~]+ Kernels
• Operating Systems have Kernels
• Kernels are written in C for the most part
• Windows, Mac OSX and Linux have kernels written in C
• Even obscure operating systems like NodeOS run on a Linux kernel.
• C++ and assembler are also used for operating systems
• Mac OSX uses Objective-C for some parts other than the kernel
• POSIX Compliance

Terminal

Jun 15 15:15

Terminal

Terminal

Terminal

christo@christo-Work-Laptop[~]+ whoami

[~]+ OS similarities:
[~]+ Kernels

OS	ASM	C	C++	Java	C#	Other
Microsoft Windows	○	○ →	●			
Linux		●				
Apple MacOS		●	●			Objective-C
Sun Solaris		●				
HP-UX		●				
Google Chrome OS		●	●			
Apple IOS		●	●			Objective-C
Google Android		●	○	●		
RIM BlackBerry OS 4.x			●			
Amazon Kindle OS		●				

Source: http://www.lextrait.com/vincent/implementations.html

Terminal

Jun 15 15:15

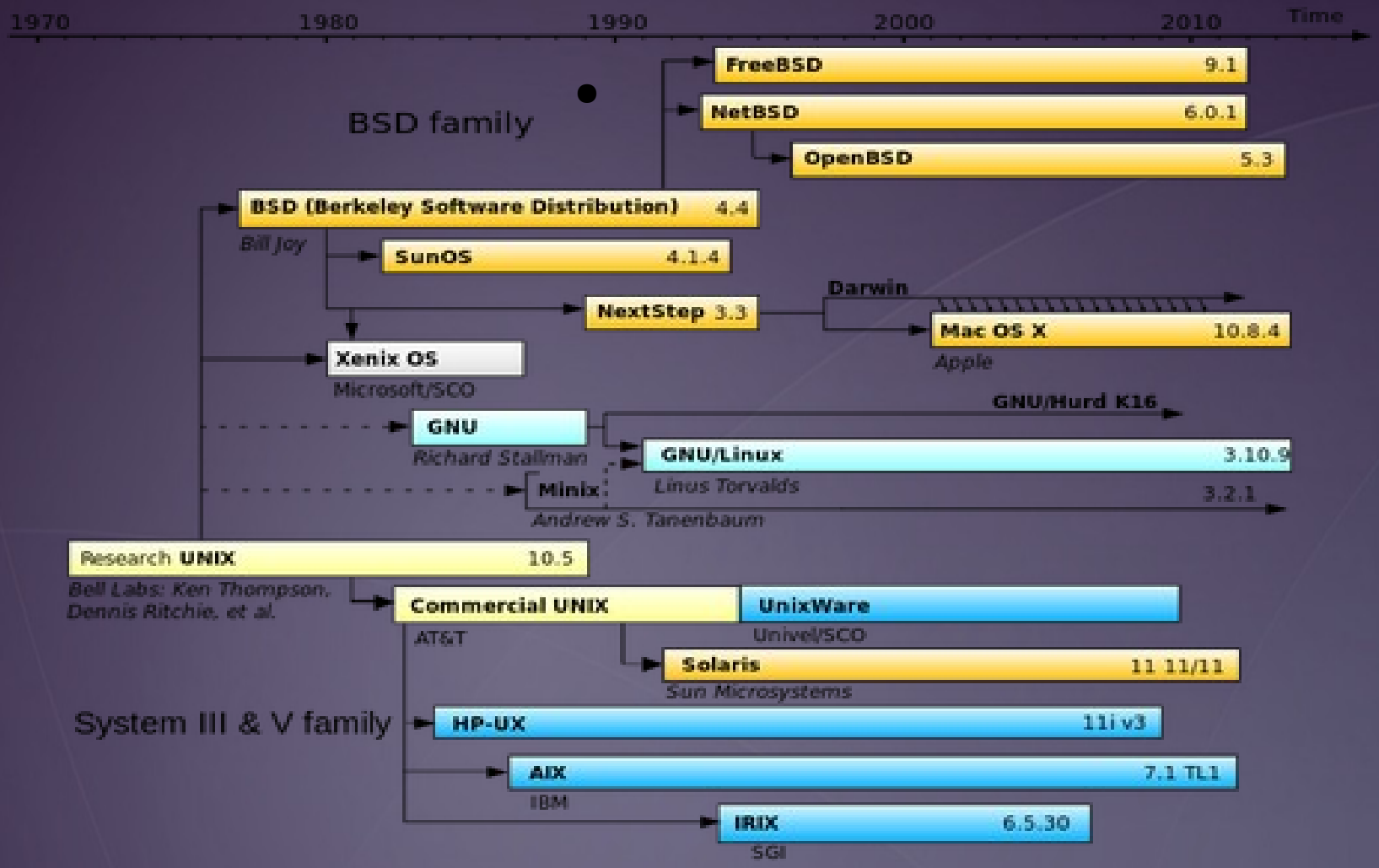
Terminal

Terminal

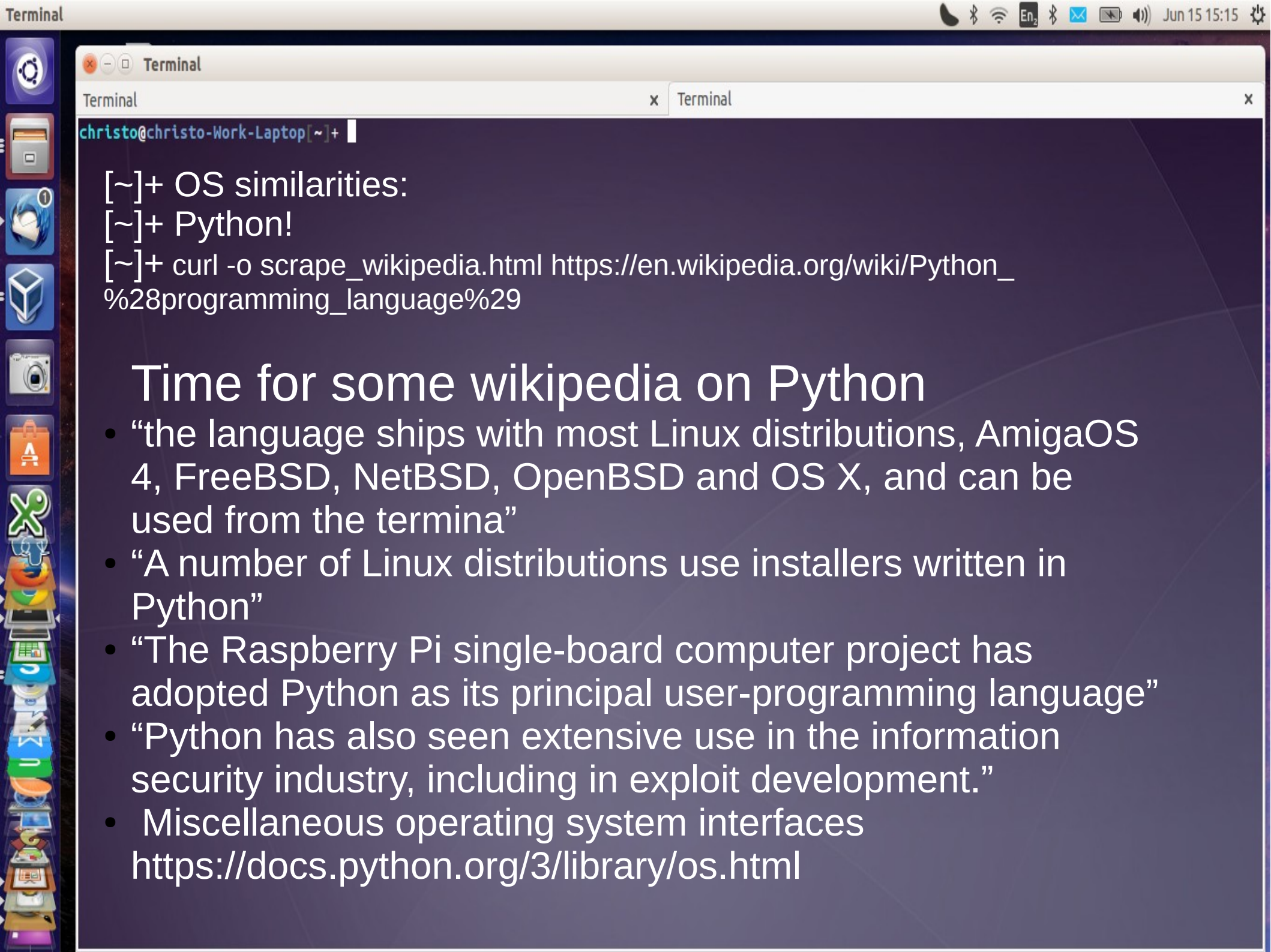
Terminal

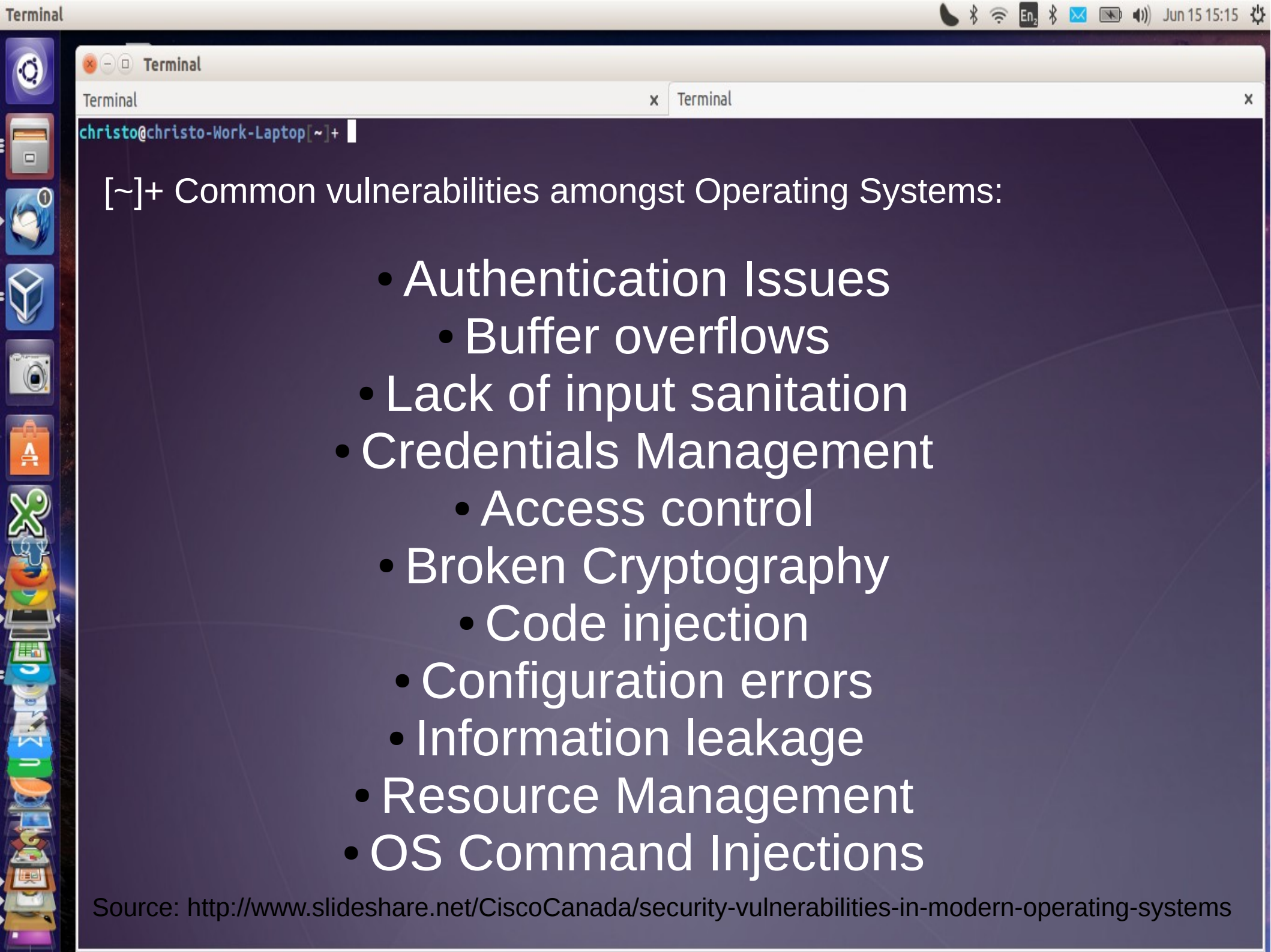
christo@christo-Work-Laptop[~]+

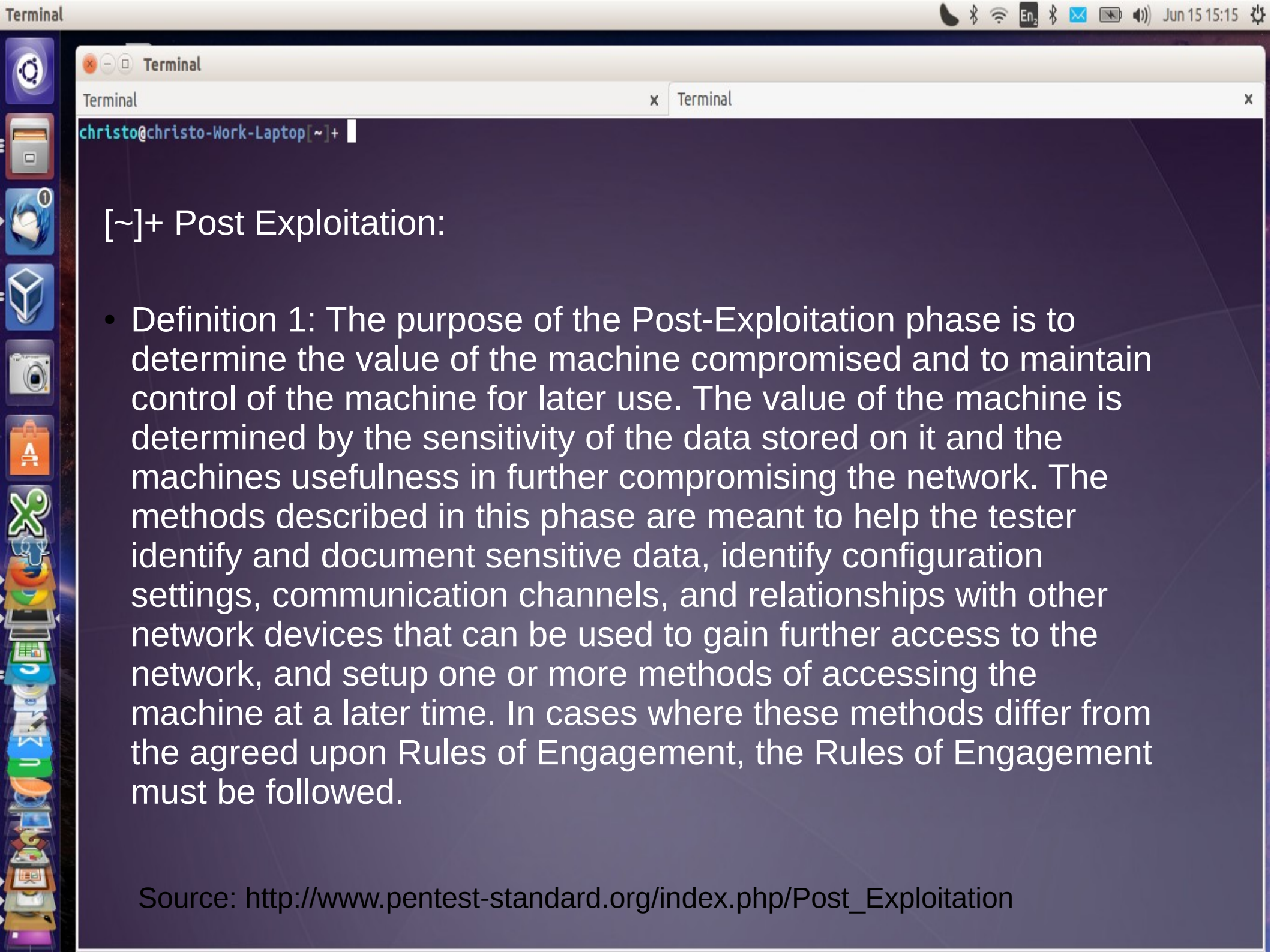
[~]+ OS similarities:
[~]+ Origins

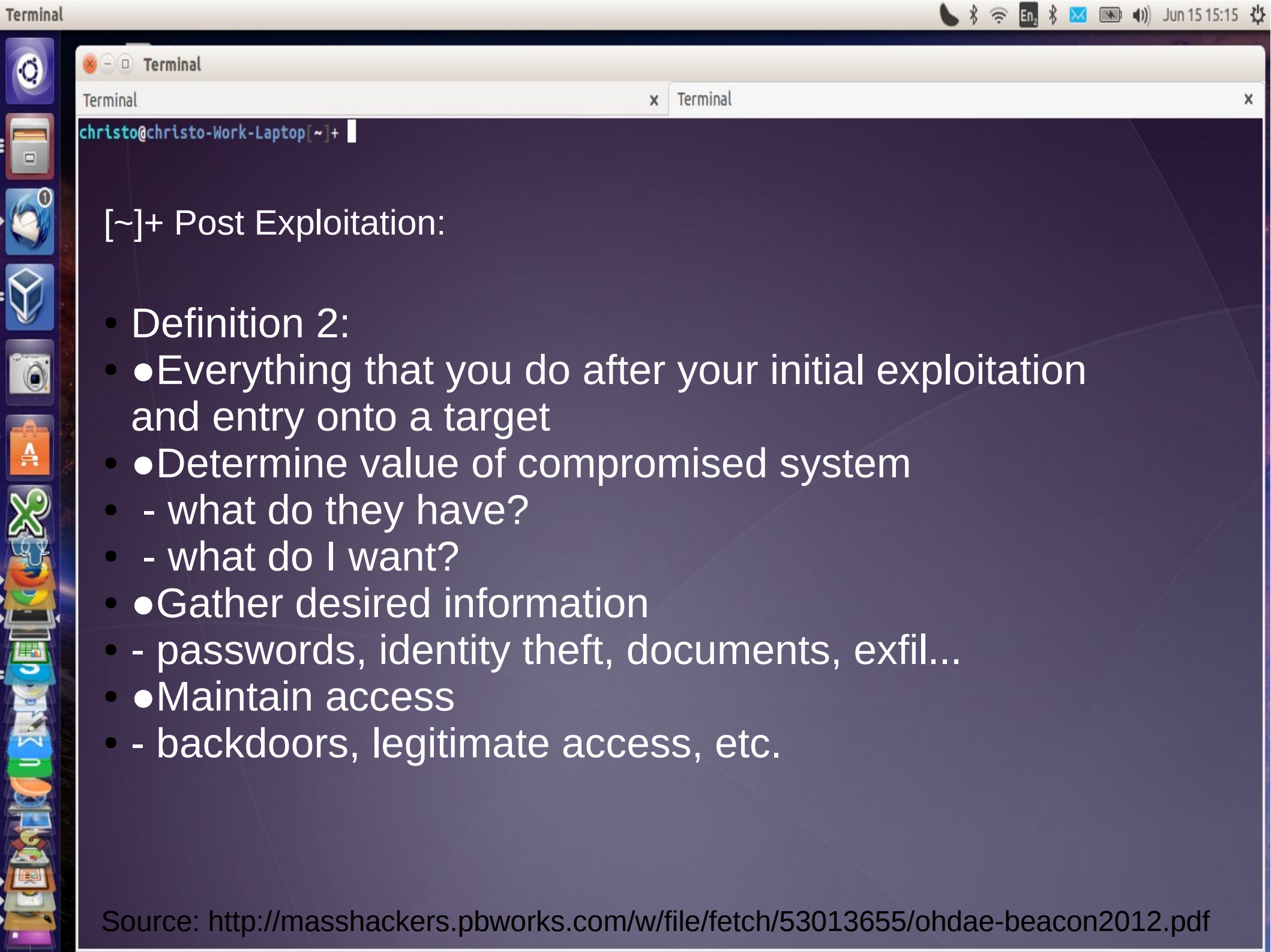


Source: http://qph.is.quoracdn.net/main-qimg-986eb78ba1ad31f7900023e55de349a4?convert_to_webp=true


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ OS similarities:
[~]+ Python!
[~]+ curl -o scrape_wikipedia.html https://en.wikipedia.org/wiki/Python_%28programming_language%29
Time for some wikipedia on Python
• “the language ships with most Linux distributions, AmigaOS 4, FreeBSD, NetBSD, OpenBSD and OS X, and can be used from the termina”
• “A number of Linux distributions use installers written in Python”
• “The Raspberry Pi single-board computer project has adopted Python as its principal user-programming language”
• “Python has also seen extensive use in the information security industry, including in exploit development.”
• Miscellaneous operating system interfaces https://docs.python.org/3/library/os.html


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Common vulnerabilities amongst Operating Systems:
• Authentication Issues
• Buffer overflows
• Lack of input sanitation
• Credentials Management
• Access control
• Broken Cryptography
• Code injection
• Configuration errors
• Information leakage
• Resource Management
• OS Command Injections
Source: http://www.slideshare.net/CiscoCanada/security-vulnerabilities-in-modern-operating-systems


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Post Exploitation:
• Definition 1: The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network. The methods described in this phase are meant to help the tester identify and document sensitive data, identify configuration settings, communication channels, and relationships with other network devices that can be used to gain further access to the network, and setup one or more methods of accessing the machine at a later time. In cases where these methods differ from the agreed upon Rules of Engagement, the Rules of Engagement must be followed.
Source: http://www.pentest-standard.org/index.php/Post_Exploitation


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Post Exploitation:
• Definition 2:
• ●Everything that you do after your initial exploitation and entry onto a target
• ●Determine value of compromised system
• - what do they have?
• - what do I want?
• ●Gather desired information
• - passwords, identity theft, documents, exfil...
• ●Maintain access
• - backdoors, legitimate access, etc.
Source: http://masshackers.pbworks.com/w/file/fetch/53013655/ohdae-beacon2012.pdf

Terminal

Jun 15 15:15

Terminal

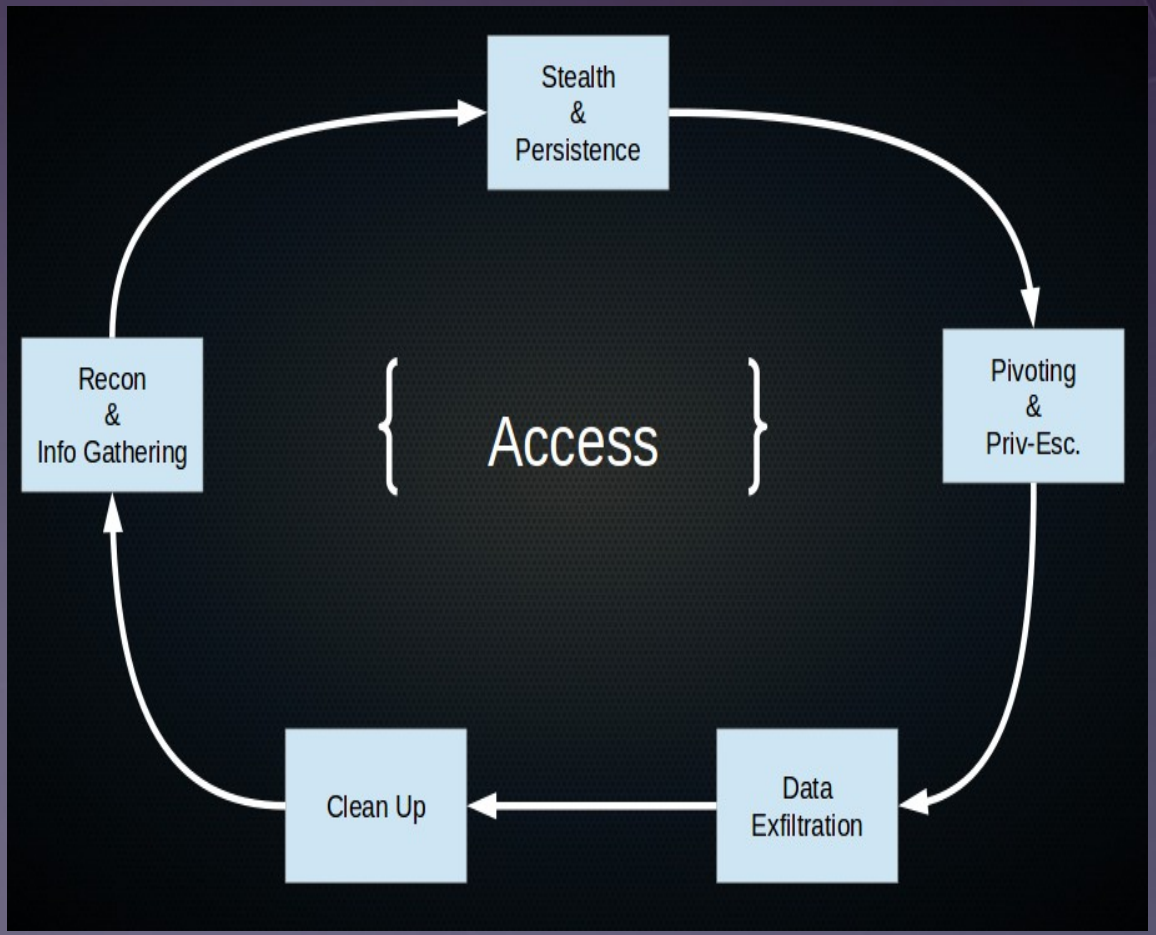
Terminal

Terminal

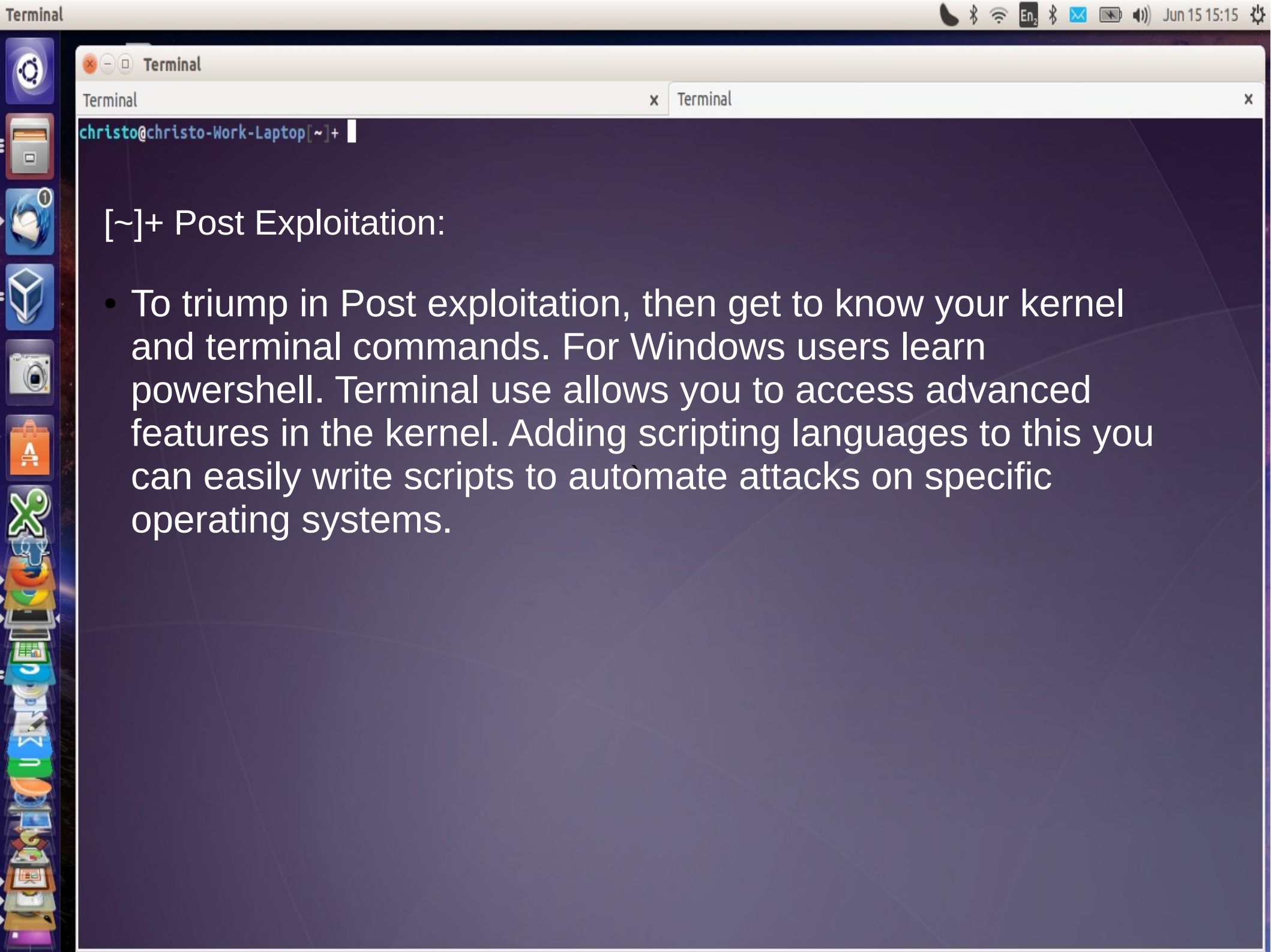
christo@christo-Work-Laptop[~]+

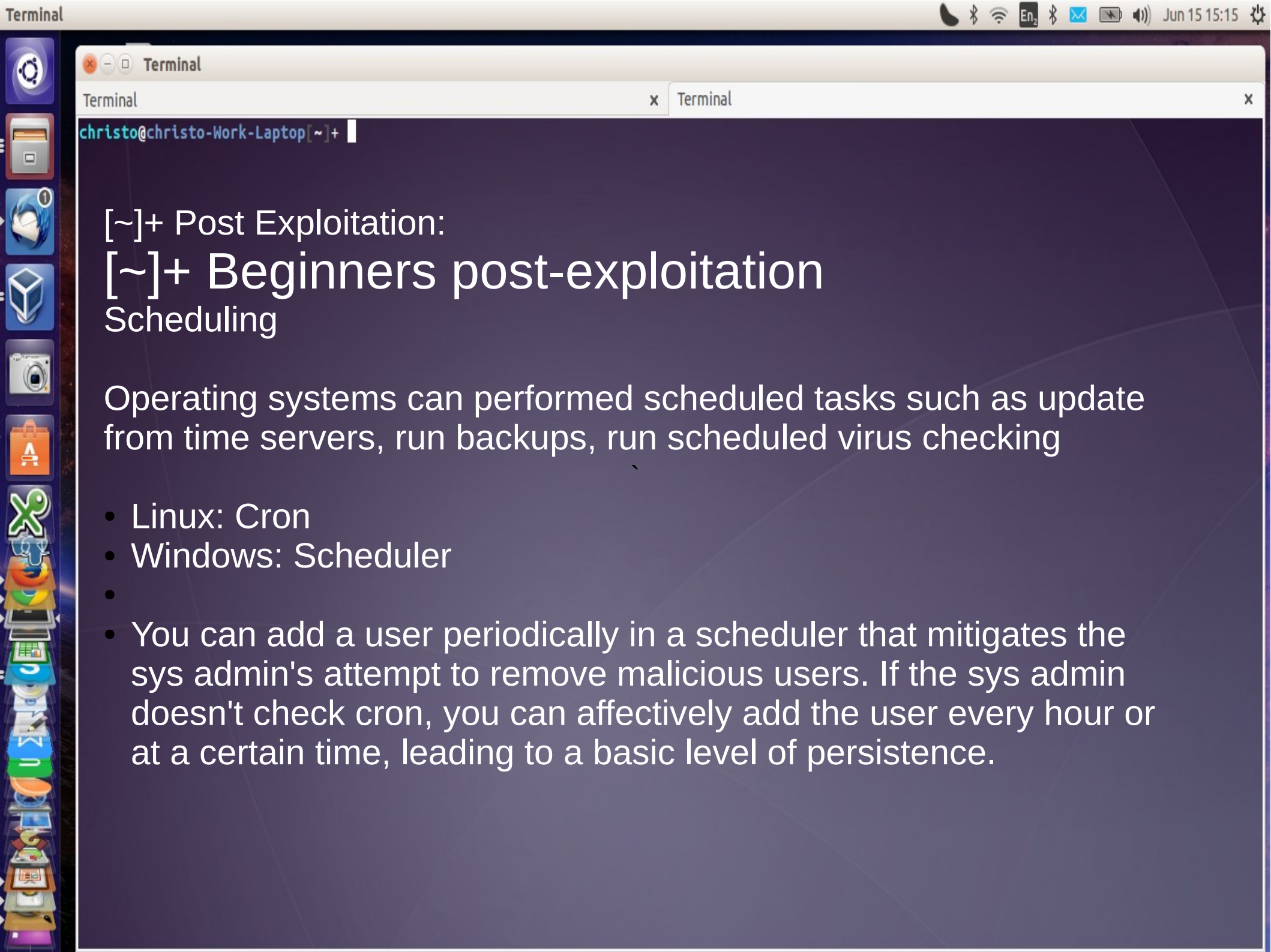
[~]+ Post Exploitation:

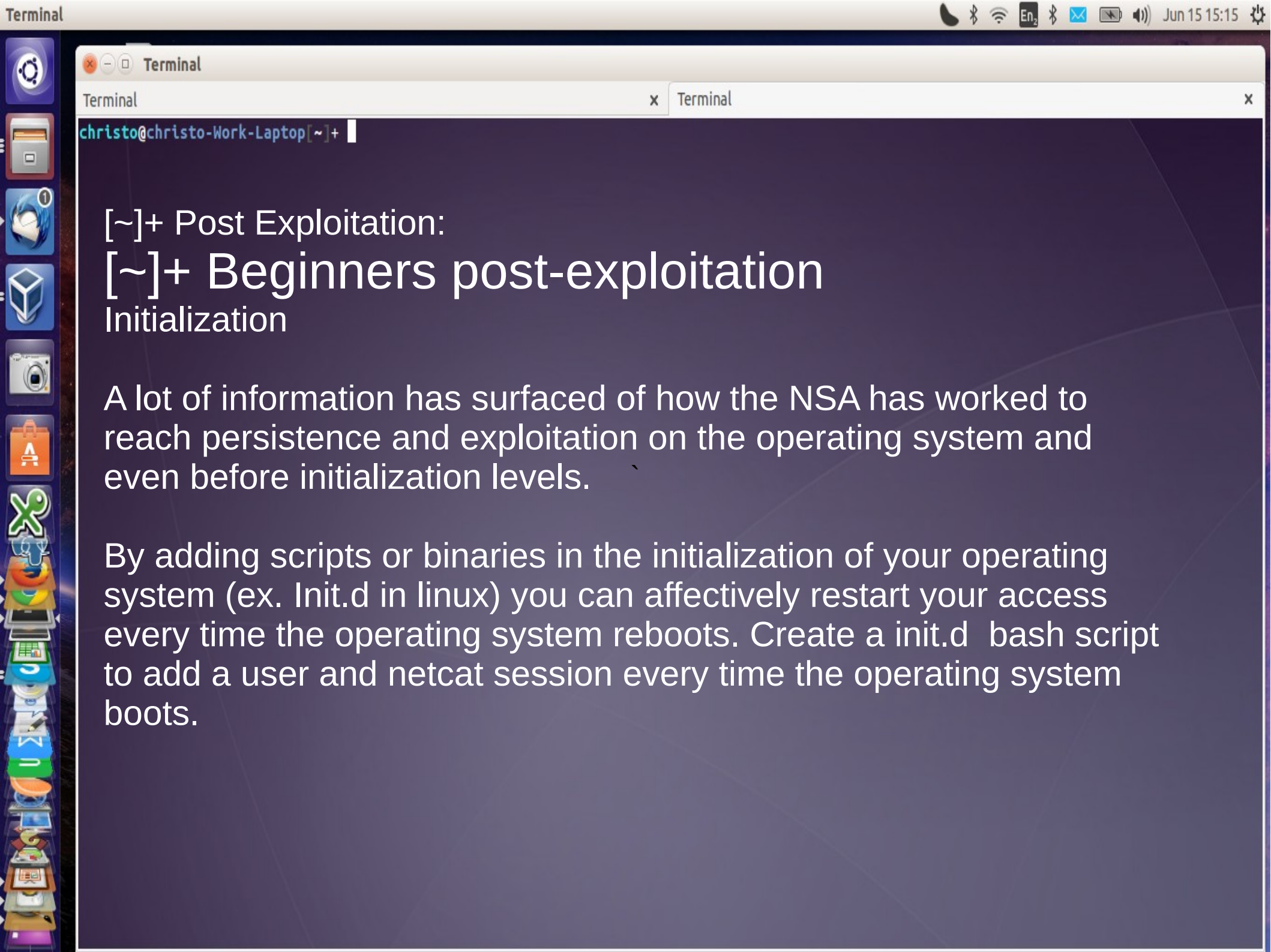
- Persistence
- Recon
- Pivoting
- Privilege escalation
- Extract
- Remove traces
- Surveillance

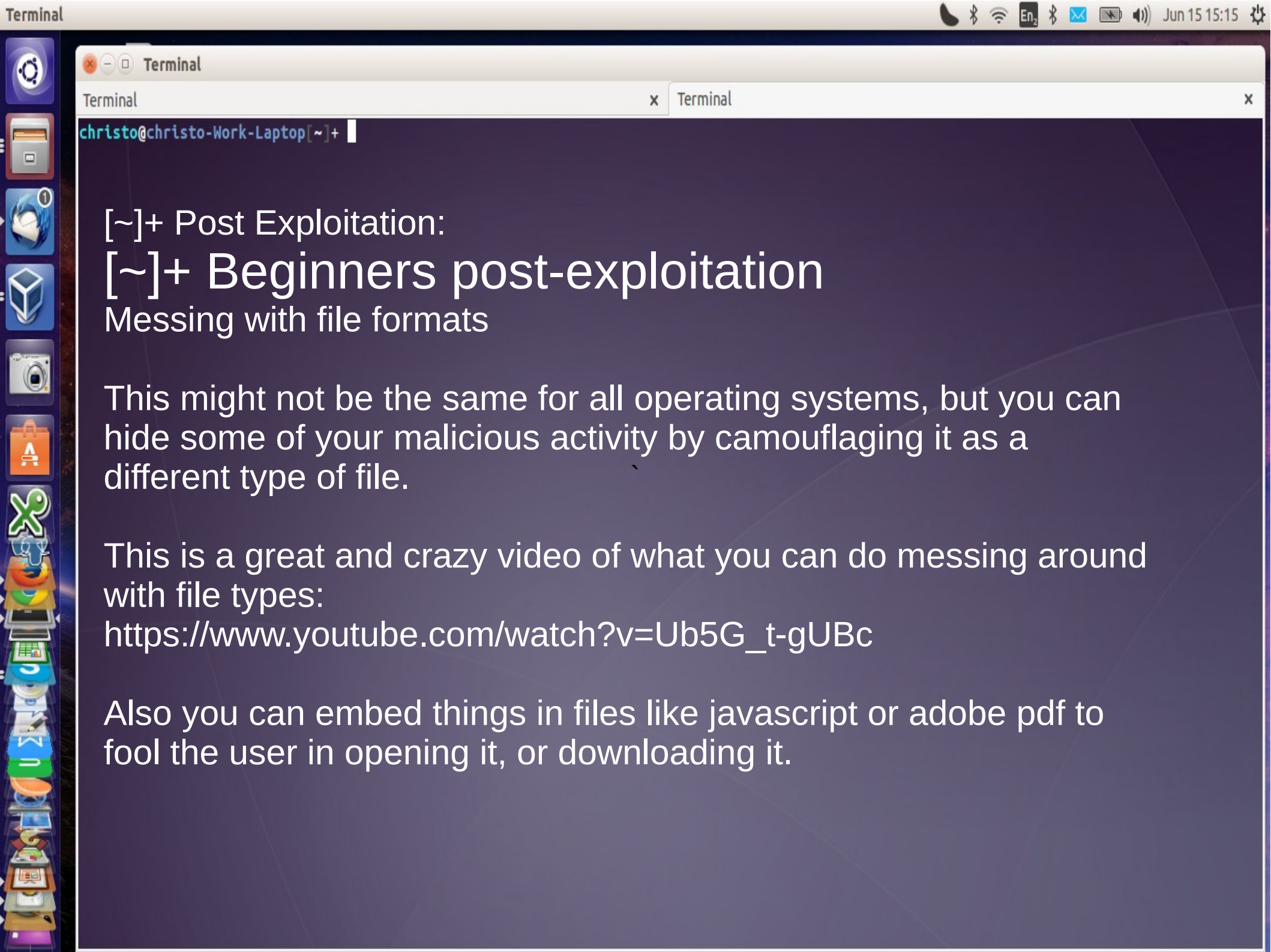


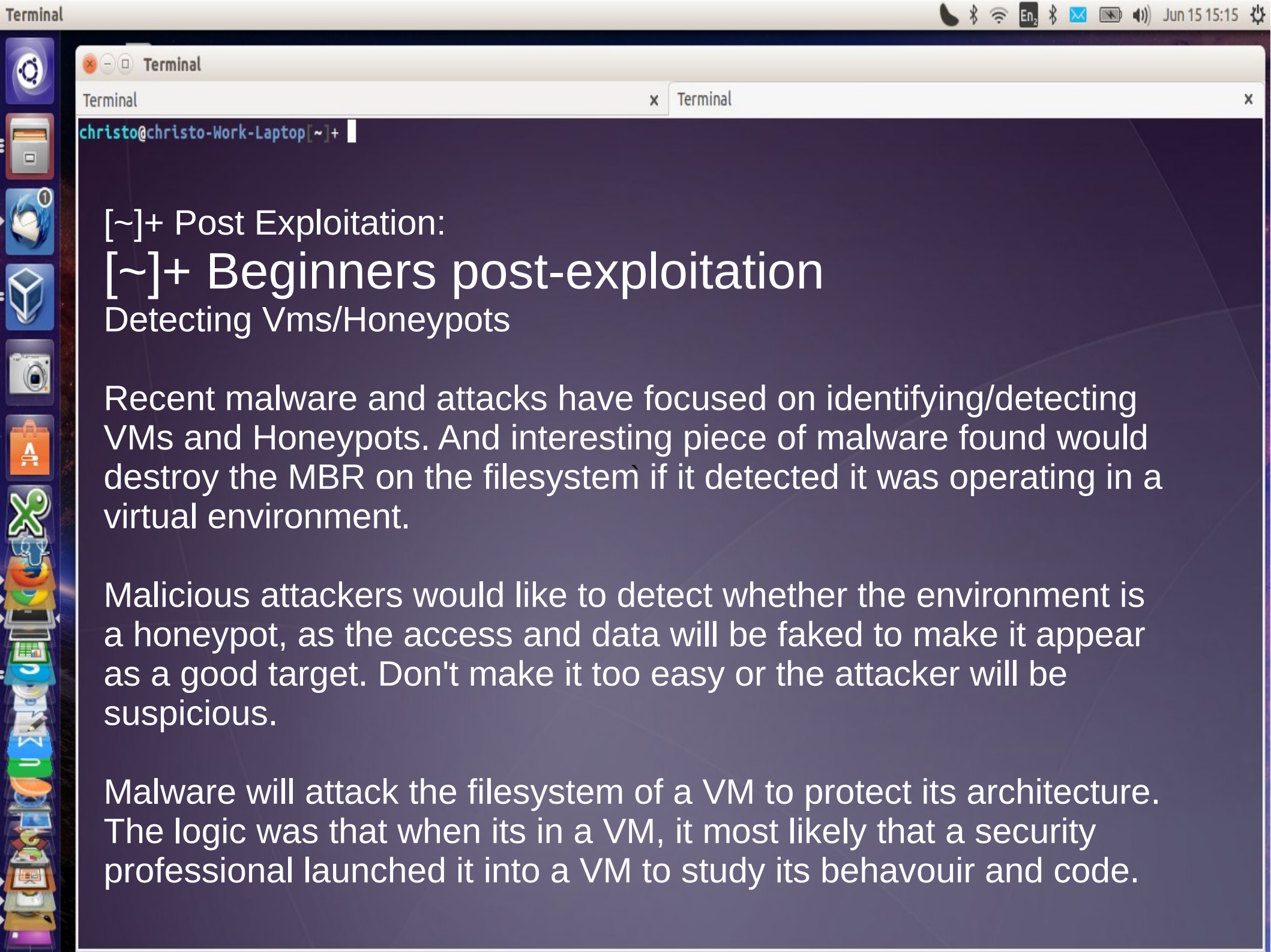
Source: http://masshackers.pbworks.com/w/file/fetch/53013655/ohdae-beacon2012.pdf

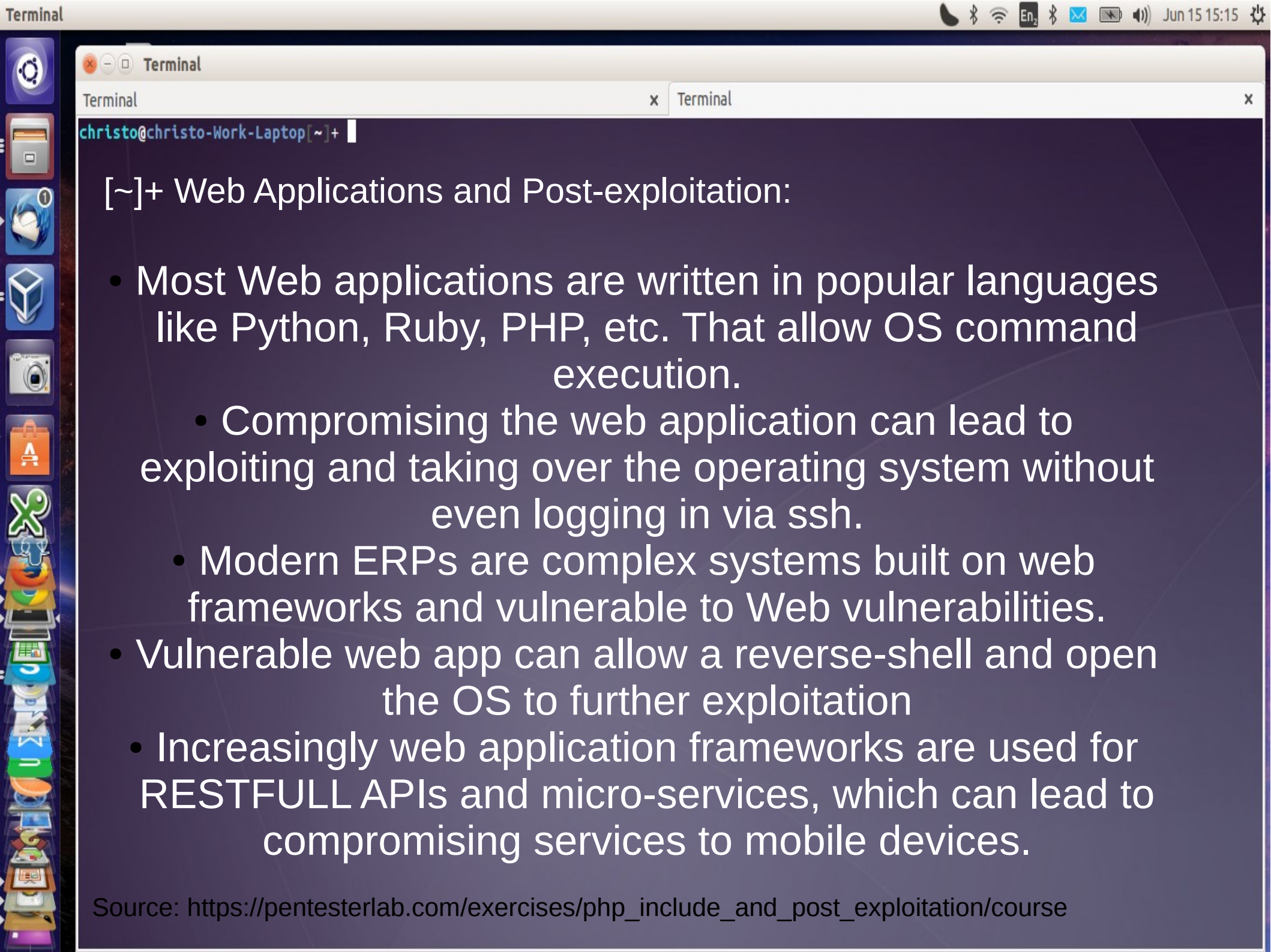

Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Post Exploitation:
• To triump in Post exploitation, then get to know your kernel and terminal commands. For Windows users learn powershell. Terminal use allows you to access advanced features in the kernel. Adding scripting languages to this you can easily write scripts to automate attacks on specific operating systems.


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Post Exploitation:
[~]+ Beginners post-exploitation
Scheduling
Operating systems can performed scheduled tasks such as update from time servers, run backups, run scheduled virus checking
• Linux: Cron
• Windows: Scheduler
•
• You can add a user periodically in a scheduler that mitigates the sys admin's attempt to remove malicious users. If the sys admin doesn't check cron, you can affectively add the user every hour or at a certain time, leading to a basic level of persistence.


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Post Exploitation:
[~]+ Beginners post-exploitation
Initialization
A lot of information has surfaced of how the NSA has worked to reach persistence and exploitation on the operating system and even before initialization levels.
By adding scripts or binaries in the initialization of your operating system (ex. Init.d in linux) you can affectively restart your access every time the operating system reboots. Create a init.d bash script to add a user and netcat session every time the operating system boots.


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Post Exploitation:
[~]+ Beginners post-exploitation
Messing with file formats
This might not be the same for all operating systems, but you can hide some of your malicious activity by camouflaging it as a different type of file.
This is a great and crazy video of what you can do messing around with file types:
https://www.youtube.com/watch?v=Ub5G_t-gUBc
Also you can embed things in files like javascript or adobe pdf to fool the user in opening it, or downloading it.


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Post Exploitation:
[~]+ Beginners post-exploitation
Detecting Vms/Honeypots
Recent malware and attacks have focused on identifying/detecting VMs and Honeypots. And interesting piece of malware found would destroy the MBR on the filesystem if it detected it was operating in a virtual environment.
Malicious attackers would like to detect whether the environment is a honeypot, as the access and data will be faked to make it appear as a good target. Don't make it too easy or the attacker will be suspicious.
Malware will attack the filesystem of a VM to protect its architecture. The logic was that when its in a VM, it most likely that a security professional launched it into a VM to study its behavouir and code.


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Web Applications and Post-exploitation:
• Most Web applications are written in popular languages like Python, Ruby, PHP, etc. That allow OS command execution.
• Compromising the web application can lead to exploiting and taking over the operating system without even logging in via ssh.
• Modern ERPs are complex systems built on web frameworks and vulnerable to Web vulnerabilities.
• Vulnerable web app can allow a reverse-shell and open the OS to further exploitation
• Increasingly web application frameworks are used for RESTFULL APIs and micro-services, which can lead to compromising services to mobile devices.
Source: https://pentesterlab.com/exercises/php_include_and_post_exploitation/course

Terminal

Jun 15 15:15

Terminal

Terminal

Terminal

christo@christo-Work-Laptop[~]+

[~]+ Post Exploitation:

- Why is this important?
- 1. In a pentest: Getting past the Web Application or firewalls isn't always mission accomplished

Source: http://masshackers.pbworks.com/w/file/fetch/53013655/ohdae-beacon2012.pdf

Terminal

Jun 15 15:15

Terminal

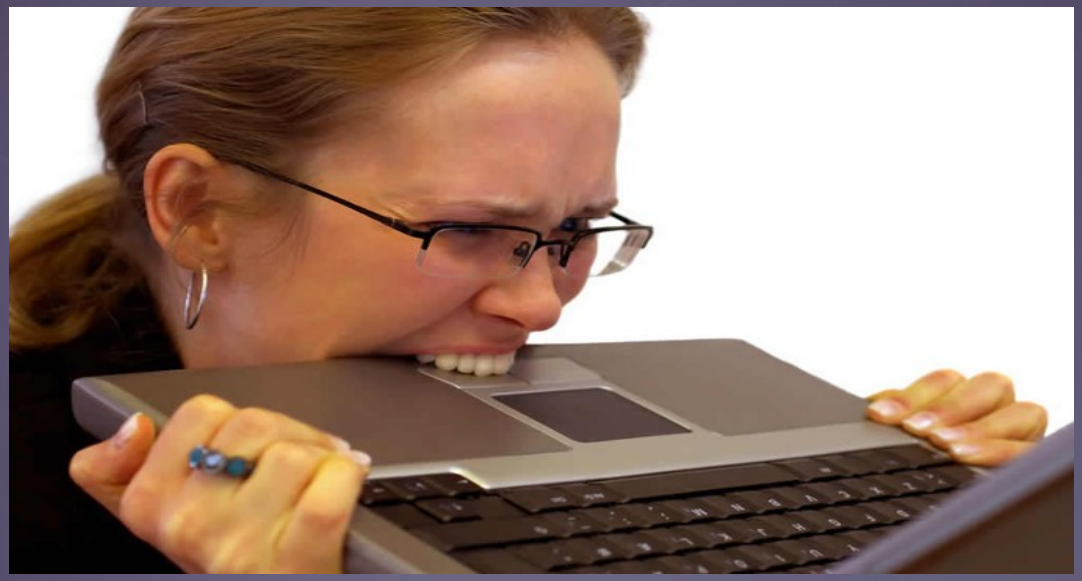
Terminal

Terminal

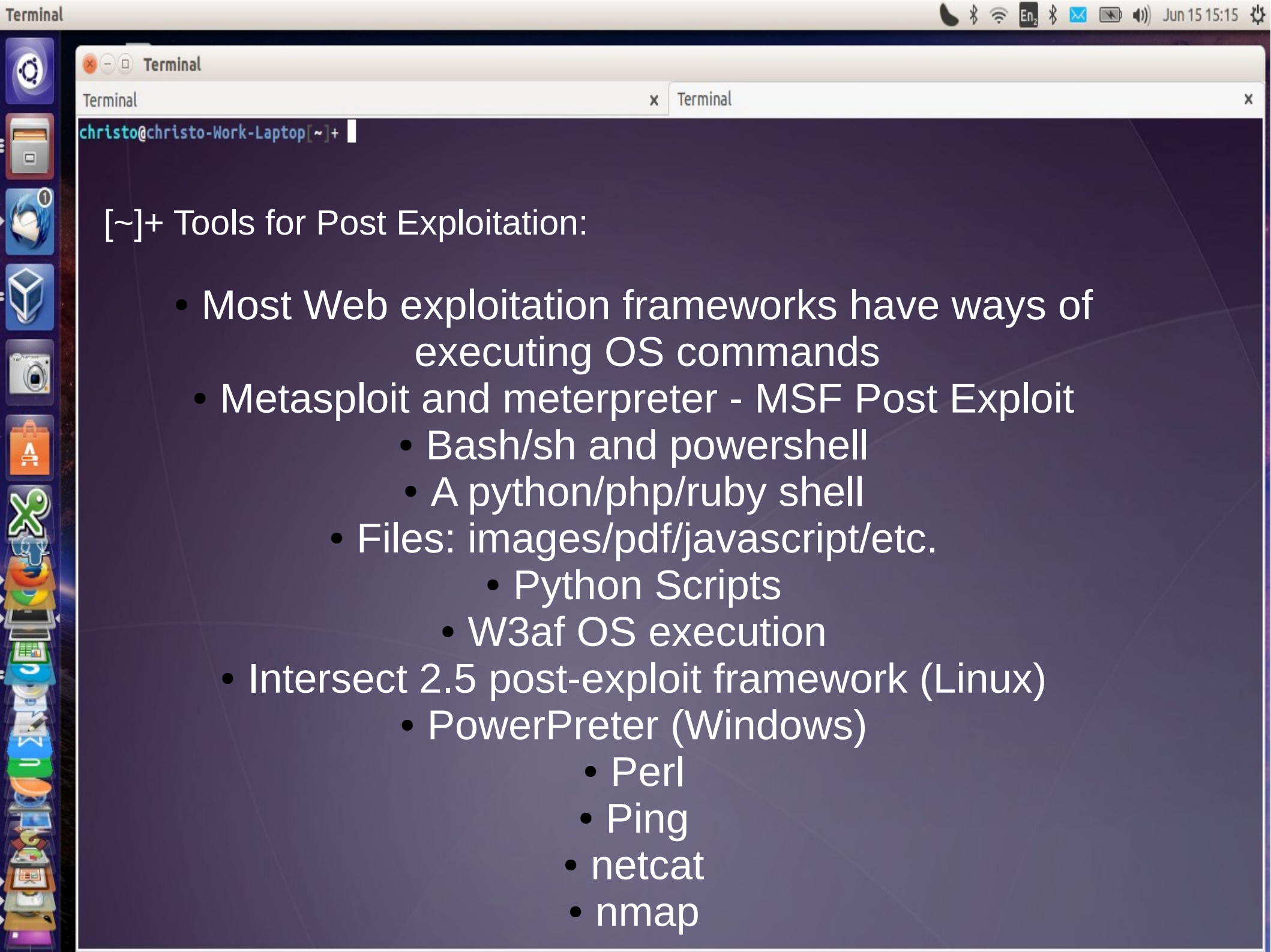
christo@christo-Work-Laptop[~]+

[~]+ Post Exploitation:

- Why is this important?
- 2. For a Sys Admin: You need to fix whats been done. Think like a hacker to stop one



Source: http://masshackers.pbworks.com/w/file/fetch/53013655/ohdae-beacon2012.pdf


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ Tools for Post Exploitation:
• Most Web exploitation frameworks have ways of executing OS commands
• Metasploit and meterpreter - MSF Post Exploit
• Bash/sh and powershell
• A python/php/ruby shell
• Files: images/pdf/javascript/etc.
• Python Scripts
• W3af OS execution
• Intersect 2.5 post-exploit framework (Linux)
• PowerPreter (Windows)
• Perl
• Ping
• netcat
• nmap

Terminal

Jun 15 15:15

Terminal

Terminal

Terminal

christo@christo-Work-Laptop[~]+ honeybadger

[~]+ Post Exploitation immune:

- Enter the HoneyBadger

Source: https://www.youtube.com/watch?v=Ys86goB5MQw

Terminal

Jun 15 15:15

Terminal

Terminal

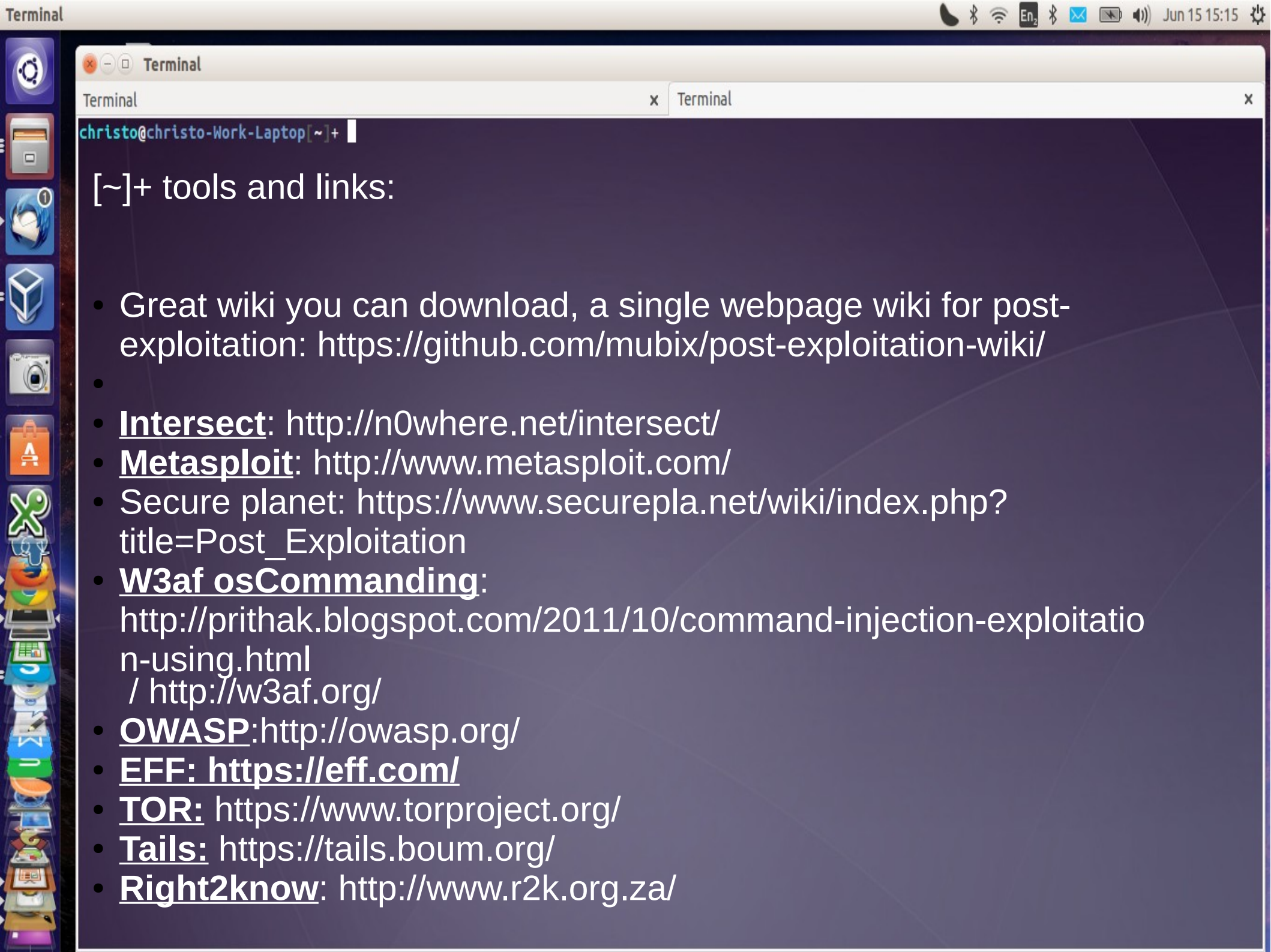
Terminal

christo@christo-Work-Laptop[~]+ honeybadger

[~]+ what is honeybadger?:

- Imagine you have to find and track someone such as a internet/smartphone active indiviual (terrorist).
- Identify target web patterns or lure target to compromised/your own server
- Exploit target/someone through Javascript/PDF/Java etc. This is used for further post-exploitation
- Post exploitation through metasploit and other tools
- Once badger has foothold on target, look for system info and geolocation data
- Use geolocation data with Google Geolocation API
- Match geolocation data with social media or access point info.
- Track or apprehend target.
- They have only covered identifying, could expand much further...

Source: https://www.youtube.com/watch?v=Ys86goB5MQw


Terminal
Jun 15 15:15
Terminal
Terminal
Terminal
christo@christo-Work-Laptop[~]+
[~]+ tools and links:
Great wiki you can download, a single webpage wiki for post-exploitation: https://github.com/mubix/post-exploitation-wiki/
Intersect: http://n0where.net/intersect/
Metasploit: http://www.metasploit.com/
Secure planet: https://www.securepla.net/wiki/index.php?title=Post_Exploitation
W3af osCommanding: http://prithak.blogspot.com/2011/10/command-injection-exploitation-using.html / http://w3af.org/
OWASP:http://owasp.org/
EFF: https://eff.com/
TOR: https://www.torproject.org/
Tails: https://tails.boum.org/
Right2know: http://www.r2k.org.za/

Terminal

Terminal | Terminal

christo@christo-Work-Laptop[~]+ whoami

[~]+ sources of talk
>>>for x in sources:
>>> print '*%s' %x
>>>* http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/
>>>* https://en.wikipedia.org/wiki/Kernel_%28operating_system%29#/media/File:Kernel_Layout.svg
>>>* http://qph.is.quoracdn.net/main-qimg-986eb78ba1ad31f7900023e55de349a4?convert_to_webp=true
>>>* wikipedia.html https://en.wikipedia.org/wiki/Python_%28programming_language%29
>>>* https://www.youtube.com/watch?v=Ys86goB5MQw
>>>* http://www.lextrait.com/vincent/implementations.html
>>>* http://www.slideshare.net/CiscoCanada/security-vulnerabilities-in-modern-operating-systems

Source: http://www.lextrait.com/vincent/implementations.html