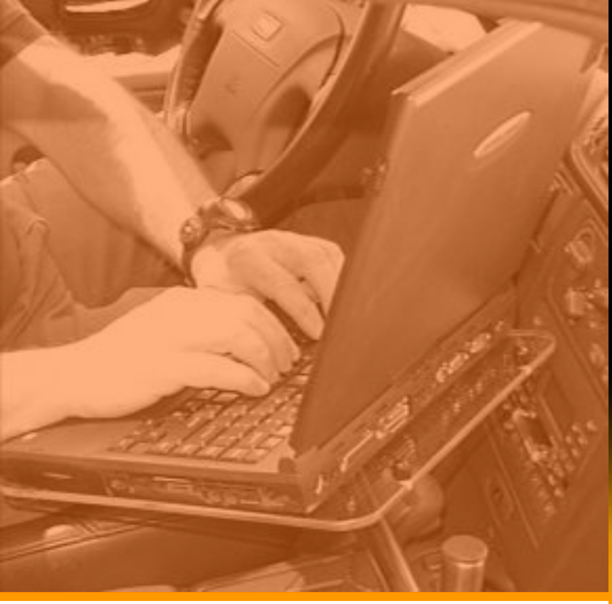
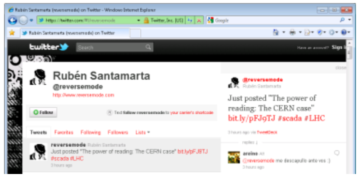


How things go wrong.

The lucky one and the unlucky one

Dr. Stefan Lüders (CERN Computer Security Officer)

3rd (CS)^2/HEP Workshop, Grenoble (France)
October 9th, 2011



Rubén Santamarta (reversemode) on Twitter - Windows Internet Explorer
https://twitter.com/#!/reversemode
Twitter, Inc. [US]
Google
Rubén Santamarta (reversemode) on Twitter
twitter
Search
Have an account? Sign in
close
Follow
Text follow reversemode to your carrier's shortcode
Tweets
Favorites
Following
Followers
Lists

Rubén Santamarta
@reversemode
http://www.reversemode.com

reversemode Rubén Santamarta
Just posted "The power of reading: The CERN case" bit.ly/pFJ9TJ #scada #LHC
3 hours ago

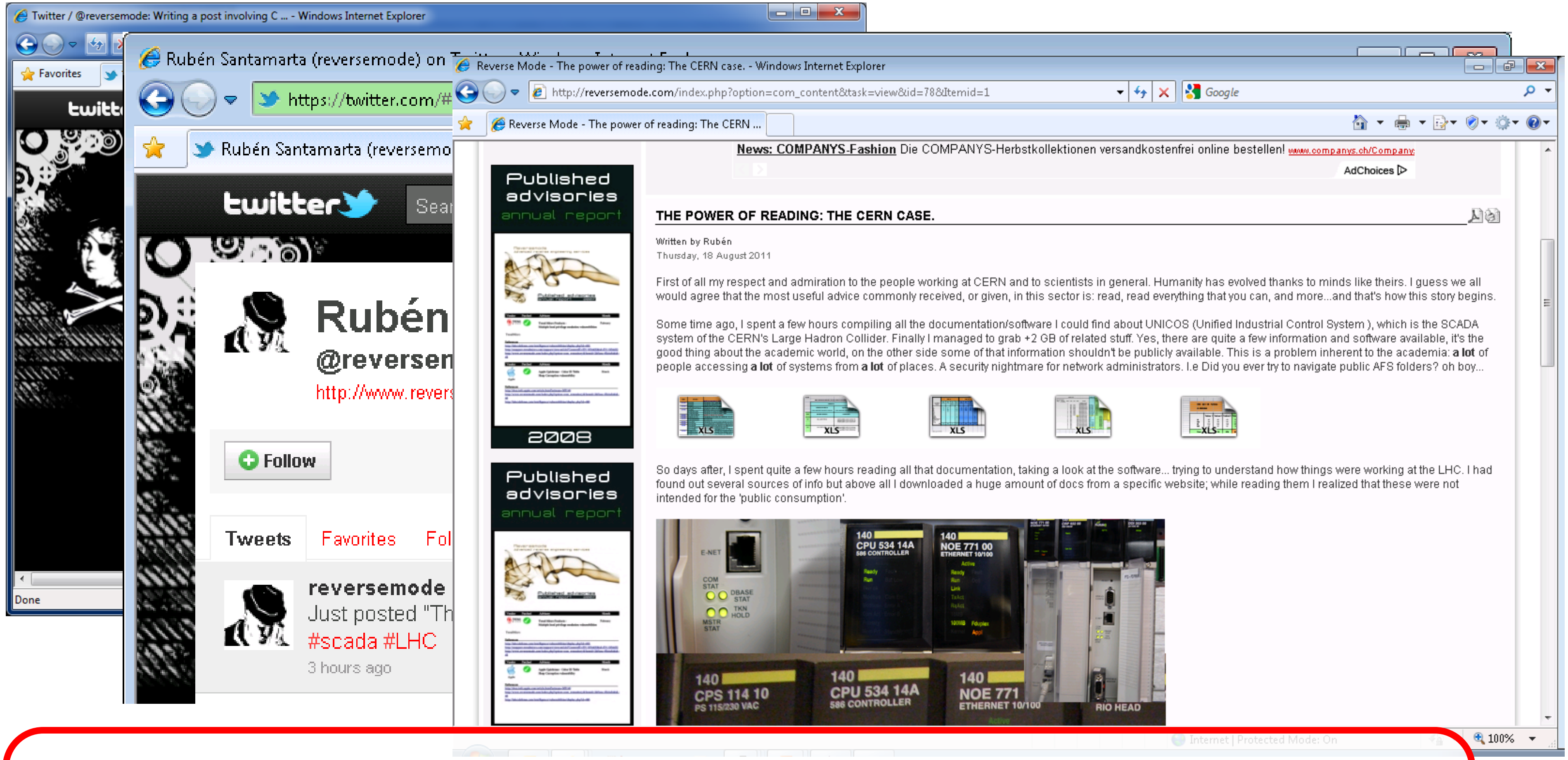
@reversemode
Rubén Santamarta
Just posted "The power of reading: The CERN case" bit.ly/pFJ9TJ #scada #LHC
3 hours ago via TweetDeck

replies ↓

areino Ari
@reversemode me descapullo ante vos :)
3 hours ago

The Lucky One

The SCADA Researcher


Twitter / @reversemode: Writing a post involving C ... - Windows Internet Explorer
Favorites
twitter
Done
Rubén Santamarta (reversemode) on Twitter - Windows Internet Explorer
https://twitter.com/#
Rubén Santamarta (reversemo
Sear
Follow
Tweets
Favorites
Fol
Reverse Mode - The power of reading: The CERN case. - Windows Internet Explorer
http://reversemode.com/index.php?option=com_content&task=view&id=78&Itemid=1
Google
Reverse Mode - The power of reading: The CERN ...
Published advisories annual report
2008
XLS
XLS
XLS
XLS
XLS
140 CPU 534 14A 586 CONTROLLER
140 NOE 771 00 ETHERNET 10/100
140 CPS 114 10 PS 115/230 VAC
RIO HEAD
Internet | Protected Mode: On
100%

Rubén
@reversemode
http://www.revers

reversemode
Just posted "Th
#scada #LHC
3 hours ago

THE POWER OF READING: THE CERN CASE.

Written by Rubén
Thursday, 18 August 2011

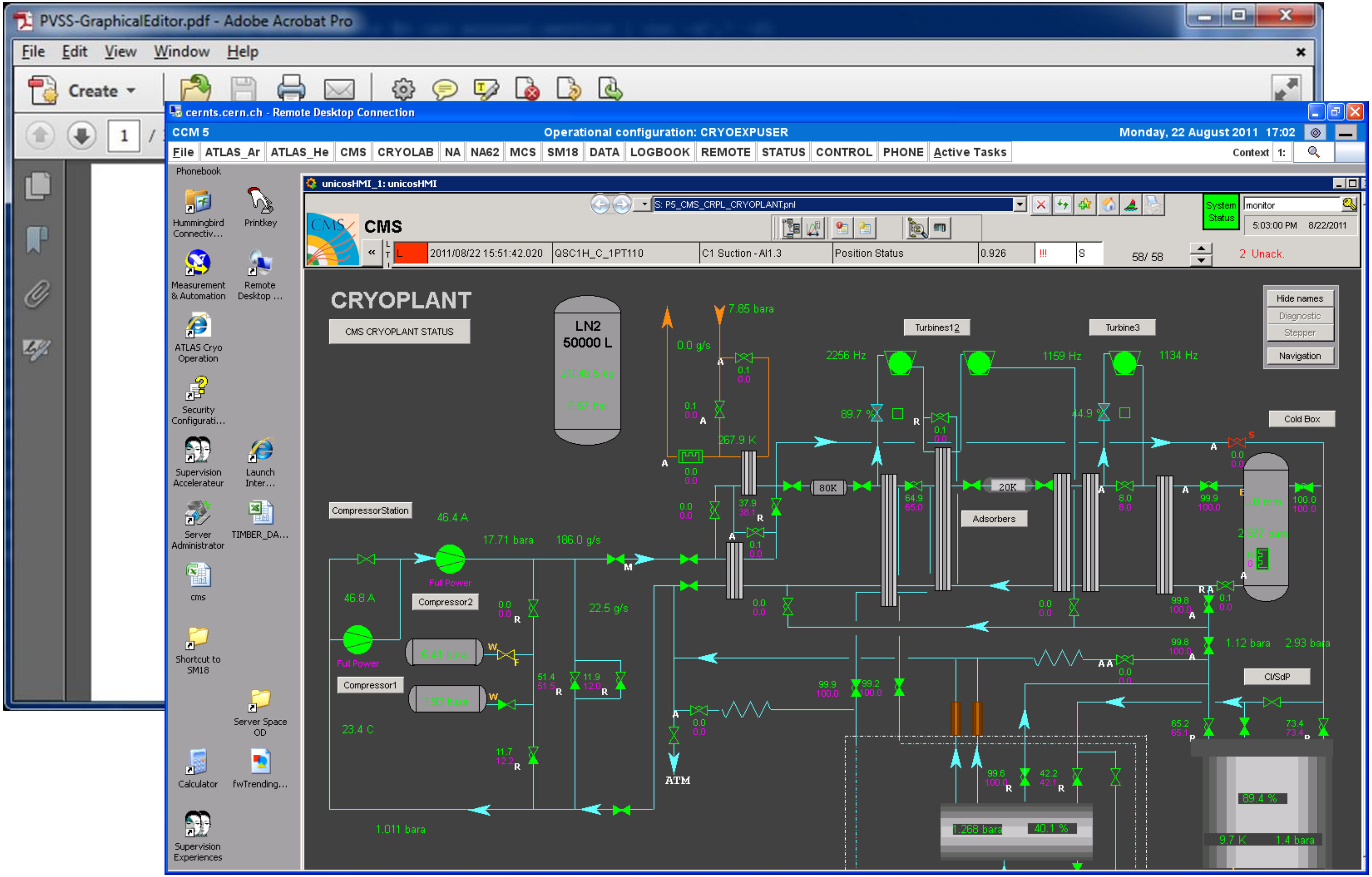
First of all my respect and admiration to the people working at CERN and to scientists in general. Humanity has evolved thanks to minds like theirs. I guess we all would agree that the most useful advice commonly received, or given, in this sector is: read, read everything that you can, and more...and that's how this story begins.

Some time ago, I spent a few hours compiling all the documentation/software I could find about UNICOS (Unified Industrial Control System), which is the SCADA system of the CERN's Large Hadron Collider. Finally I managed to grab +2 GB of related stuff. Yes, there are quite a few information and software available, it's the good thing about the academic world, on the other side some of that information shouldn't be publicly available. This is a problem inherent to the academia: **a lot** of people accessing **a lot** of systems from **a lot** of places. A security nightmare for network administrators. I.e Did you ever try to navigate public AFS folders? oh boy...

So days after, I spent quite a few hours reading all that documentation, taking a look at the software... trying to understand how things were working at the LHC. I had found out several sources of info but above all I downloaded a huge amount of docs from a specific website; while reading them I realized that these were not intended for the 'public consumption'.

A month earlier, the Researcher reported to the U.S. Department of Homeland Security who informed us via SWITCH and MELANI.

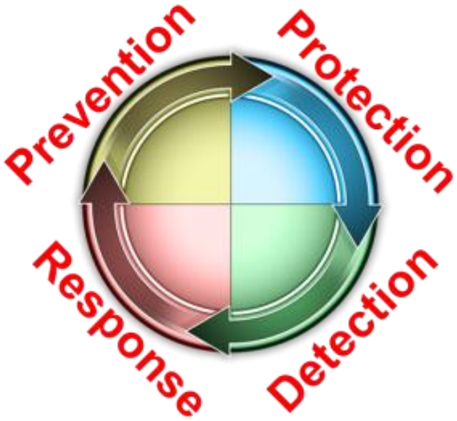
What happened?



L 2011/08/22 15:51:42.020 QSC1H_C_1PT110 C1 Suction - AI1.3 Position Status 0.926 !!! S

Counter-Measures

Standard event response:

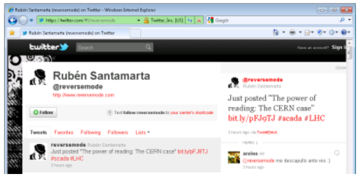


- ► Inform stakeholders
- ► Prepare press statement
- ► Take documents offline incl. Google cache
- ► Change passwords on all instances *(can be costly!)*
- ► Check access logs for unauthorized activity:
  We’ve been able to identify the corresponding actions,
  e.g. the original scan for the document and WTS accesses

Lessons Learned:

- ► Starting to block access from the Internet for selected service accounts (i.e. non-personal accounts)
- ► Working on a general policy prohibiting service accounts on LXPLUS and CERNTS

The Unlucky One


Rubén Santamarta (reversemode) on Twitter - Windows Internet Explorer
https://twitter.com/#!/reversemode
Twitter, Inc. [US]
Google
Rubén Santamarta (reversemode) on Twitter
twitter
Search
Have an account? Sign in
close
Follow
Tweets
Favorites
Following
Followers
Lists

Rubén Santamarta
@reversemode
http://www.reversemode.com

Text **follow reversemode** to your carrier's shortcode

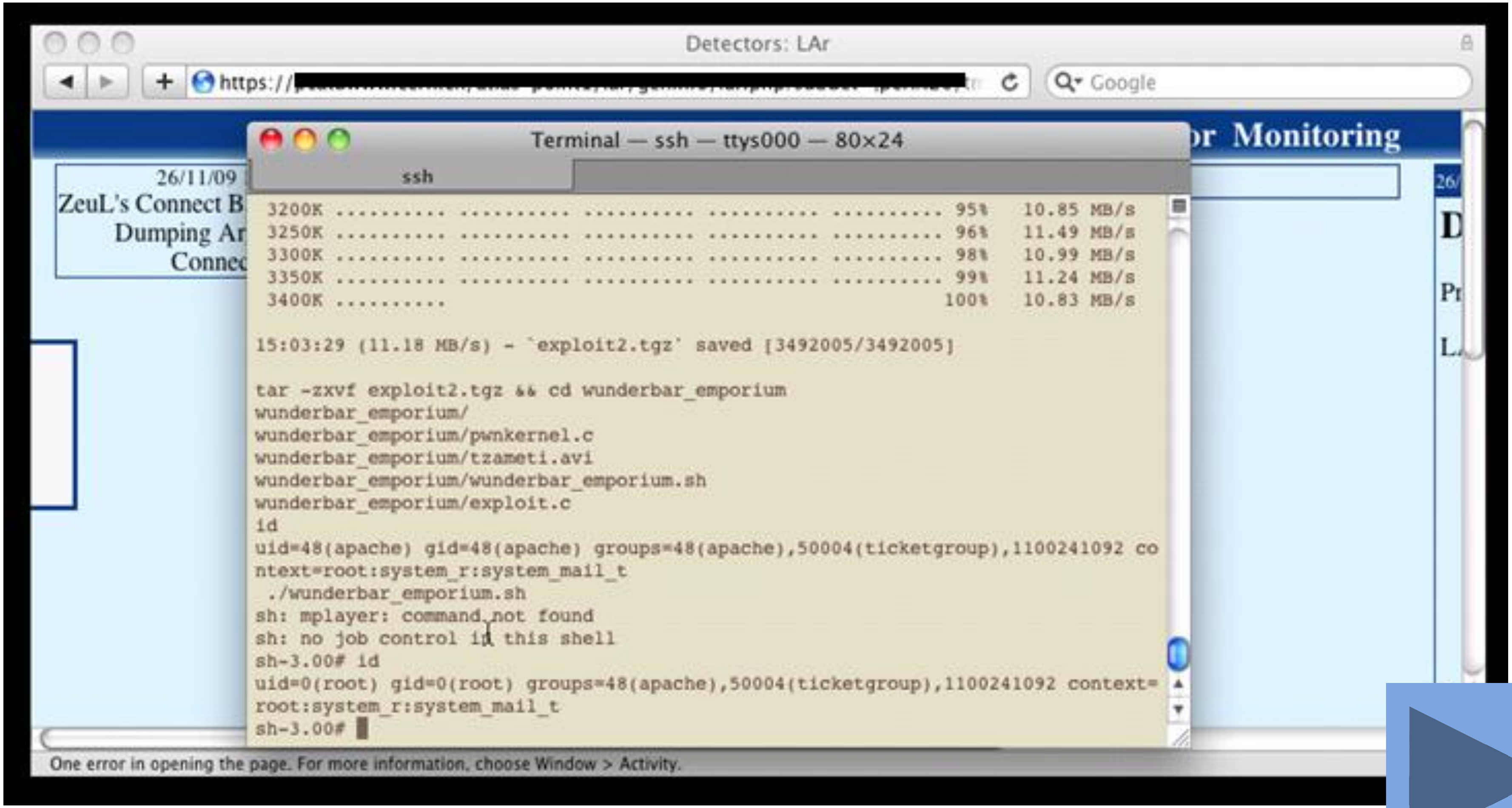
reversemode Rubén Santamarta
Just posted "The power of reading: The CERN case" bit.ly/pFJ9TJ #scada #LHC
3 hours ago

@reversemode
Rubén Santamarta
Just posted "The power of reading: The CERN case" bit.ly/pFJ9TJ #scada #LHC
3 hours ago via TweetDeck

replies ↓

areino Ari
@reversemode me descapullo ante vos :)
3 hours ago

The Attack



```
 3200K .......... .......... .......... .......... .......... 95%   10.85 MB/s
 3250K .......... .......... .......... .......... .......... 96%   11.49 MB/s
 3300K .......... .......... .......... .......... .......... 98%   10.99 MB/s
 3350K .......... .......... .......... .......... .......... 99%   11.24 MB/s
 3400K ..........                                            100%   10.83 MB/s

15:03:29 (11.18 MB/s) - `exploit2.tgz' saved [3492005/3492005]

tar -zxvf exploit2.tgz && cd wunderbar_emporium
wunderbar_emporium/
wunderbar_emporium/pwnkernel.c
wunderbar_emporium/tzameti.avi
wunderbar_emporium/wunderbar_emporium.sh
wunderbar_emporium/exploit.c
id
uid=48(apache) gid=48(apache) groups=48(apache),50004(ticketgroup),1100241092 co
ntext=root:system_r:system_mail_t
 ./wunderbar_emporium.sh
sh: mplayer: command not found
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache),50004(ticketgroup),1100241092 context=
root:system_r:system_mail_t
sh-3.00# 
```

One error in opening the page. For more information, choose Window > Activity.

Counter-Measures

Prevention
Protection
Detection
Response

Standard event response:

- ► Inform stakeholders
- ► Prepare press statement
- ► Check network logs and attacker Ips
- ► Forensics of compromised server
  Difficult if local admins already have tampered with the data
- ► Determination of compromise extent
- ► Reinstallation after all *(painful)*

Lessons Learned:

- ► Patching is a must
- ► Central syslogging is a must, too
- ► Adequate security training is beneficial for *all*
  (“Once bitten, twice shy”☺)
- ► Deployment of so-called “Security Baselines”

Security Baselines

- …define basic security objectives
- …are simple, pragmatic & complete, and do not imply technical solutions

All systems/services must be implemented and deployed in compliance with their corresponding "Security Implementation Document"

- Non-compliance will ultimately lead to reduced network connectivity (i.e. closure of CERN firewall openings, ceased access to other network domains, full disconnection from the network).

Today, we have Security Baselines…

- …for servers (EDMS 1062500)
- …for file hosting services (EDMS 1062503)
- …for web hosting services (EDMS 1062502)
- …for Industrial Embedded Devices (EDMS 1139163)

Prevention is the key

Training & Awareness

- Dedicated training courses on “Secure programming in Java/PHP/Perl/Python” and “…for Web applications”
- Mandatory on-line security course every two years for all CERN account owners
- Awareness poster campaign through-out CERN
- Check out at http://cern.ch/security/training/en/index.shtml

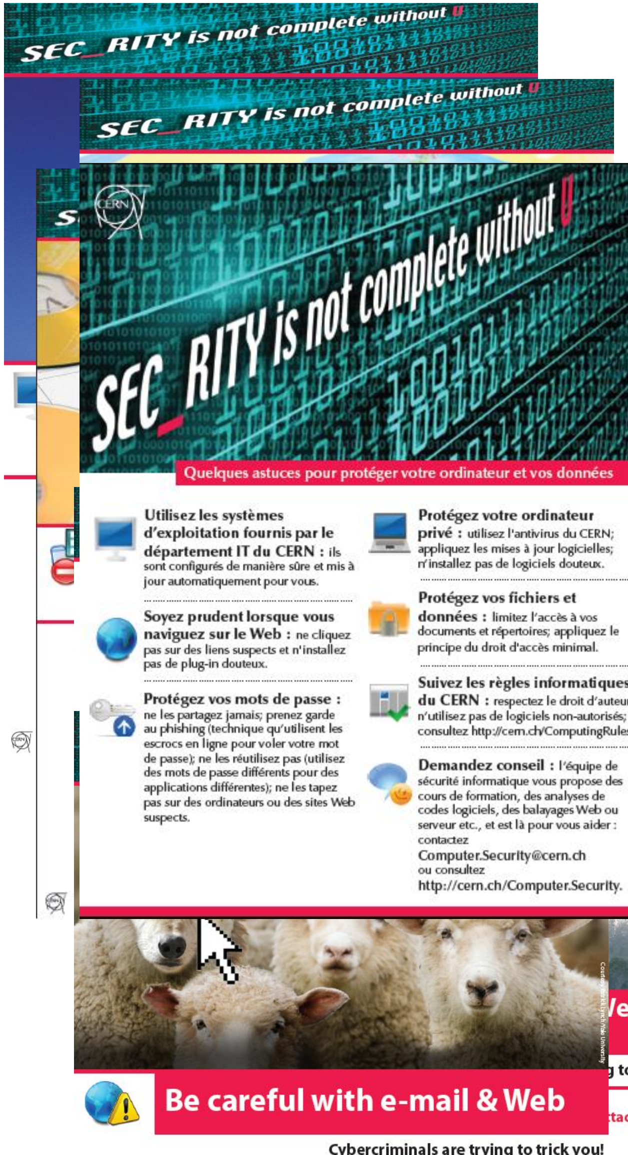
Consulting & Assistance

- Helping system owners with securing their services

Website scanning

- …plus Nessus…

skipfish



SEC_RITY is not complete without U

SEC_RITY is not complete without U

SEC_RITY is not complete without U

Quelques astuces pour protéger votre ordinateur et vos données

Utilisez les systèmes d'exploitation fournis par le département IT du CERN : ils sont configurés de manière sûre et mis à jour automatiquement pour vous.

Soyez prudent lorsque vous naviguez sur le Web : ne cliquez pas sur des liens suspects et n'installez pas de plug-in douteux.

Protégez vos mots de passe : ne les partagez jamais; prenez garde au phishing (technique qu'utilisent les escrocs en ligne pour voler votre mot de passe); ne les réutilisez pas (utilisez des mots de passe différents pour des applications différentes); ne les tapez pas sur des ordinateurs ou des sites Web suspects.

Protégez votre ordinateur privé : utilisez l'antivirus du CERN; appliquez les mises à jour logicielles; n'installez pas de logiciels douteux.

Protégez vos fichiers et données : limitez l'accès à vos documents et répertoires; appliquez le principe du droit d'accès minimal.

Suivez les règles informatiques du CERN : respectez le droit d'auteur n'utilisez pas de logiciels non-autorisés; consultez http://cern.ch/ComputingRules

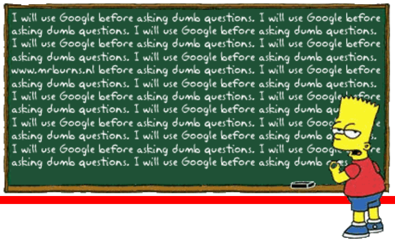
Demandez conseil : l'équipe de sécurité informatique vous propose des cours de formation, des analyses de codes logiciels, des balayages Web ou serveur etc., et est là pour vous aider : contactez Computer.Security@cern.ch ou consultez http://cern.ch/Computer.Security.

Courtesy Patrick Lynch/Yale University

Be careful with e-mail & Web

Cybercriminals are trying to trick you!

Thank you!


I will use Google before asking dumb questions. I will use Google before asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl

Questions?