

Table of Contents

Computer Security information for GT staff.....	1
CERN Computing rules.....	1
Security exposure.....	1
Security awareness.....	1

Computer Security information for GT staff

This page is for guidance only and describes several aspects of computer security. The objective is to highlight essential points of computer security when working in the IT-GT group.

CERN Computing rules

As a GT member, you are bound by the CERN Computing Rules, available at:

<http://cern.ch/ComputingRules/>

You should know about these rules...you have signed them when you have applied for a CERN account and/or a grid certificate from the CERN CA.

Security exposure

As in any large organisation, there are security risks inherent to running and maintaining computing services. As members of the Grid Deployment group, you are likely to have a certain degree of Unix or administrative privileges against a CERN host or some grid service. These privileges come with a responsibility, part of which includes being aware and keeping up-to-date with the most common security attacks CERN or the grid is facing.

A good starting point is the Security Questionnaire provided by the ISSeG project:

<http://cern.ch/ISSeG-training/Download/Questionnaire-V3.4.xls>

The questionnaire should give you a basic understanding of the security risks you and the organisation are facing, as well as common mitigating techniques.

Security awareness

The table below attempts to describe different areas of computer security and is regularly updated.

You should be have sufficient understanding of each of these areas, and in particular:

- Understand the main risk(s)
- Identify the recommended solution(s)
- Review your working practice and take corrective action if needed

Area	Topic	Where to find information
Desktop Security	Web browsing	Chat with Romain http://www.cert.org/tech_tips/securing_browser/ , http://noscript.net/
Desktop Security	Emails	Chat with Romain http://cern.ch/security/recommendations/
Desktop Security	Instant messaging and VoIP	Chat with Romain
Desktop Security	Windows security	https://winservices.web.cern.ch/winservices/Help/?kbid=050001
Desktop Security	Linux security	Armoring (Grid) Linux systems
Desktop Security	PDA's and phone security	Chat with Romain

Area	Topic	Where to find information
Network Security	Connecting to CERN from home	SSH gateways SSH Socks proxy ↗ SSH agent ↗ SSH port forwarding ↗ Man-In-the-Middle information ↗ http://www.cert.org/tech_tips/home_networks.html
Network Security	Wire(less) network security	Chat with Romain
Host Security	Authenticating using SSH at CERN	http://indico.cern.ch/getFile.py/access?contribId=0&resId=0&materialId=slides&confId= http://cern.ch/linux/docs/kerberos-access.shtml ↗ http://cern.ch/linux/scientific4/docs/rhel-rg-en-4/s1-kerberos-works.html ↗ http://cern.ch/linux/scientific4/docs/rhel-rg-en-4/s1-kerberos-additional-resources.html ↗
Host Security	AFS access control	Worldwide readable ↗ FS command ↗ PTS command ↗ kerberos AFS tokens ↗
Host Security	Managing root access	root access management in GD
Host Security	Linux Rootkits	http://indico.cern.ch/materialDisplay.py?contribId=4&materialId=slides&confId=43866 http://toorcon.org/2007/talks/11/Gabe_Lawrence.ppt ↗
Host Security	Linux host integrity	Chat with Romain
Software development	Web applications	http://indico.cern.ch/materialDisplay.py?contribId=38&sessionId=13&materialId=slides
Software development	Secure coding	http://cern.ch/security/SecureSoftware/checklist.htm ↗ http://cern.ch/info-secure-software/ ↗ http://cern.ch/security/SecureSoftware/Seminar-080515.ppt ↗
Know your enemy	Underground economy	http://indico.cern.ch/getFile.py/access?contribId=1&resId=1&materialId=slides&confId=
Know your enemy	Common security vulnerabilities and exploitation techniques	Chat with Romain
Know your enemy	Network traffic capture and live tampering	Chat with Romain
Know your enemy	Automating exploit preparation and attacks	Chat with Romain
Security incidents	Incident response, roles and procedures	Chat with Romain
Security incidents	How to contain and resolve incidents	Chat with Romain
Security incidents	Linux investigation tips and	Chat with Romain

Area	Topic	Where to find information
	standard forensic techniques	

This topic: ITGT > SecurityForStaff

Topic revision: r7 - 2011-03-08 - MariaALANDESPRADILLO



Copyright &© 2008-2024 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
or Ideas, requests, problems regarding TWiki? use Discourse or Send feedback