21st TF-CSIRT meeting
May 3-4, 2007
Prague, Czech Republic

Author: Cătălin Meiroşu – Issue 2

1. Welcome and apologies

Gorazd Božič welcomed the participants to the 21st TF-CSIRT meeting. The list of attendees that registered through the TF-CSIRT website is attached at the end of this document.

2. Andrea Kropáčová – CESNET-CERTS presentation

Andrea Kropáčová introduced CESNET, an association of legal entities, established in 1996. CESNET had 26 members and about 320 participants in the network, including secondary schools, hospitals and libraries. CERT=devil in Czech. The CSIRT team was established in 2004 and now had 4 members. The main services offered by the team are targeting incident handling for the CESNET2 network. CESNET also had a monitoring centre, with 8 employees, to handle basic incident handling. The NOC of the CESNET2 backbone was operated with a team of 6 members. All these groups collaborate for handling the security incidents. The goals of the collaboration were to provide non-stop incident handling for the network and establish basic rules for such cases. In this respect, two basic incident handling policy documents were created last year last year. CESNET would like to help establish CSIRT teams in every big university.

3. Past Meeting Minutes and Action Items

The minutes of the 20th TF-CSIRT meeting were approved.

Action items:

18-1. Wilfried Wöber reported he needed to contact Ulrich Kiermayr and ask him to run the script again. Wilfried Wöber would then distribute the results via the tfcsirt mailing list. Wilfried Wöber asked Cătălin Meiroşu to remind him of this action item between the TF-CSIRT meetings. The action item is still open.

18-2. Wilfried Wöber reported progress. The whois v3 client was available from sourceforge. He thought that convincing the Linux distributions to include it would not be easy, but he will discuss this issue during RIPE NCC meeting in Tallinn. The action item is still open.

18-3. Wilfried Wöber reported that there was quite a lot of progress in this area, but further details were included in the IRT presentation. He proposed to keep the item open.

20-2. Item closed. Nobody volunteered to pick up the work on VDEF.

4. Václav Sedláček – CERT for Government and Administration of the Czech Republic

Václav Sedláček stated that a few weeks before the TF-CSIRT meeting, a memorandum from the Czech government announced the formation of CERTCZ. During his talk, he approached two questions – why CERTCZ and why RELSIE to do it.

The information system of Czech public administration was established in 2000; later it was transformed into the ministry of informatics of the Czech Republic. Information systems were established in all the components of the public administration. Several bodies were authorised by the ministry to provide tests of interfaces between different deployments. RELSIE had the greatest number of attests granted.

RELSIE was founded in 1992 for assessment of information systems in public administration. The company developed a methodology for the tests, and this was approved by the ministry. The company was certified ISO. In 2006 it joined the OQS group.

A project was setup to establish a service space for central and public administration offices. CERTCZ was made responsible for the interface between this space and the rest of the world. A supervisory body will be established and be responsible to handle incidents between points inside this central service space. The current solution called for only one IP address to be visible from outside this space.

Václav Sedláček said that the English translation of the original document in Czech contained some mistakes. The activity of CERTCZ will be centred on government and public administration. The errors in translation were being fixed. Václav Sedláček announced that the ministry of informatics was to be shut down by the Czech parliament, its competencies distributed between three ministries.

Gorazd Božič asked whether RELSIE will provide a government CERT or only limited services. Václav Sedláček answered that RELSIE will follow the Finland model.

Wilfried Wöber asked whether that one IP address to be visible was really one address or a block of addresses. Václav Sedláček answered that the solution required only one address to be made visible. However, he said that the project was still in a design phase.

Karel Vietsch asked what the advantages of such solution were. Václav Sedláček said that RELSIE had to follow some guidelines from the Czech government in this matter.

They were chosen to implement the solution based on their history of collaboration with the government.

Jan Meijer asked whether he understood correctly that RELSIE will follow the Finnish model for a government CERT, or perhaps the Dutch model. Václav Sedláček answered that this was an open problem. It could change in the future, as RELSIE and the government were still in the preparation phase of the project. Václav Sedláček asked the audience that would be interested in collaborating or communicating on these ideas to contact him.

Gorazd Božič welcomed RELSIE in the community, and reminded everybody that the major goal of TF-CSIRT was to share knowledge.

5. Karel Vietsch – TRANSITS update

TRANSITS training courses consist of 5 modules, presented during two days of very intensive work. They were intended for people that are going to work for, or in the setting up a new CSIRT. The curricula were setup in 2001 by volunteers. Three phases in the project history: 2002-2005 – EU-funded project TRANSITS that paid for several workshops throughout Europe. The materials were also used for training at the national level, as well as utilised by FIRST for trainings worldwide. In 2006, there were three courses sponsored by ISPA and ENISA. In October 2007, a contract was signed with Don Stikvoort to act as editor in chief of the material. Now TERENA is continuing the series, next workshop scheduled in Sofia. Sponsorship from ENISA allowed maintaining the fees low. Deadline for applications: 11th of May. Places were still available.

Maurizio Molina asked whether there exist precedents when the materials were given for workshops organised by other entities. Karel Vietsch mentioned national trainings. TERENA put some conditions, such as the teachers should have attended previous trainings. In The Netherlands, trainings were done for hospitals in the country. In Norway, people from different universities and schools were trained in a series of workshops. Internationally, quite a few were organised by FIRST, up to 3-4 a year in APAN and Latin America. For example, a couple of months ago such a workshop was held in Lima. FIRST organised a “train the trainers” session at their annual conference.

6. Andrew Cormack – ENISA update

Andrew Cormack updated the community on the meeting of the ENISA Permanent Stakeholder Group (PSG) that took place in Crete at the end of April 2007. ENISA is a body setup by the European Commission to advise member states on issues related to security of communication networks and information systems. Andrew Cormack was asked by TF-CSIRT to apply for a place in the PSG. The PSG advises the Executive director on the Agency’s work programme.

The discussions at the meeting in Crete were focused on activities for 2008 and following years. In the past, the agency was very much concentrating at yearly activity timespans. This time, they look at results they want to achieve and have people involved from all parts of the agency. Help SMEs in the member states, identify emerging risks and making sure that decision makers were better informed and understand the problems were some of the subjects discussed. Information security statistics were debated. Some of them might have been published in order to support a certain point of view. It is important to talk to CSIRTs on how statistics that are meaningful and understandable could be generated.

At the next meeting in June, The PSG will review a list of workpackages. Andrew Cormack asked the community to contact him with ideas on what the agency could do. He announced that as he was asked to apply for the PSG in 2005, his term will expire in the summer of 2007. A call for new members was already published. That call was open until May 15. Andrew Cormack invited the audience to apply for this call. The number of places with "academic background" in the PSG was increased, so there may be opportunities for more people to join. He announced that he applied to continue his role in the Group.

Karel Vietsch noted that the workplan will now be for a longer period, even though a few years ago, ENISA was established for a limited time interval. Andrew Cormack answered that the current mandate of the agency is supposed to end in 2009. There were ongoing discussion on whether and how the agency will continue after this date.

Karel Vietsch asked whether a formal evaluation of the agency's work was carried out. Andrew Cormack answered that such evaluation took places and was positive. Gorazd Božič noted that the European parliament is discussing the agencies. He thought the Parliament asked the Commission for an evaluation of the work of all agencies. But the feeling was that ENISA will continue for another term. However, this will have to pass through the vote in the Parliament. Andrew Cormack believed the latest evaluation of the activities took place last year. Gorazd Božič thanked Andrew for applying again for the PSG. He also agreed that Karel Vietsch's suggestion was also very wise – to watch if there will be an evaluation, and in that case if TF-CSIRT could form an opinion on ENISA and send it to the relevant body.

7. Wilfried Wöber – RIPE IRT Object update

What is going to be discussed next week at the RIPE-NCC.

Wilfried Wöber announced that the crypt-pw will be phased out. RIPE-NCC were in the final phase of making sure nobody will be using it for the RIPE database. The suggested way would be to use certificates and GNU PGP instead of crypt-pw.

After the meeting in Budapest, he received many questions from the participants. It turned out that most of the database documentation was not updated since late 2002. For

example, X509 certificates were not included. Also, parts of the documentation on the IRT were simply wrong because the implementation changed. Two of the documents were updated; the last one was still in draft status. A completely new users guide on updating objects on the database was made available to the community. There was also an e-learning module on using PGP and X509. Wilfried Wöber noted that people will have to create their own identity and use it to access the module, in addition to the standard RIPE database identity.

Wilfried Wöber presented a novel idea to take the concept of an organisation object and find out whether this could improve the use of an abuse object. He also announced that a new task force on data protection (privacy) was scheduled to be started at the RIPE meeting on Monday morning. He did not know what delayed the activity of the task force.

Wilfried Wöber mentioned results coming from another RIPE task force. Instead of a plain email from a registry stating that a certain set of IP addresses has been assigned, the owner of the addresses would receive a digitally signed email. This has potentially interesting influences on the database machinery and is related to the development project of Secure BGP.

Wilfried Wöber asked the community whether the current situation with the database was considered insecure. The answer would be that it was not considered insecure itself, but there was no a link between management of IP addresses and routing announcements (which are made by contractual agreements currently). We need to address IP blackholing; some of the scripting and manual work for ACL could be replaced by automated processes based on signed information. The routing layer could be made more secure and resilient against errors, typos, and other things that should not happen. The link between the management of IP addresses and the routing layer could be formalised.

8. Christoph Graf – JRA2 update

Christoph Graf announced the community that the GN2 project has been extended by half a year, running till 2009. In charge of running the geant2 network, the GN2 project was divided in several categories of activities. JRA2 was aimed at improving the overall security in the Geant2 community. About 1/3 of the partners are participating in this activity.

What they aim at doing in the remaining time of the project was to work to improve the security capabilities of the participants. Of particular interest was the security compliance level – bring the lagging teams above the line, and improve the other teams as well.

The toolset developed by JRA2 consisted of flowmon and nfsen. They had pilots running. Results will be available shortly, when the deliverables will be out.

Action point 21-1: Christoph to check the public flag on the deliverable

A formal framework was created for providing security advice to other activities in the GN2 project. However, there were no novelties to report in this area in addition to the first such case that happened mid-2006.

Meetings of the JRA2 and the JRA2 Advisory Panel were scheduled after the end of the TF-CSIRT meeting. There were two vacancies in the Advisory Panel. Christoph Graf asked for applications for filling these positions. They were looking mostly for people from commercially oriented CSIRTs, in particular Because Jimmy Arvidsson had to leave the group.

Wim Biemolt asked why the project was extended. Christoph Graf answered that the decision was taken at higher management level. Karel Vietsch commented that some money that was originally allocated was still available and Geant3 is only going to start at the earliest of summer 2009. Therefore, a time interval needed to be bridged so if everything works fine the leftover money would be just enough to cover for this interval.

9. Peter Haag - nfsen/nfdump update

Peter Haag presented nfsen, a part of the JRA2 toolset that is continuously developed. People could still find the familiar interface in the new version. Now it was based on a channel architecture, more configurable. A small simulation mode was integrated in the software. This could be used for training.

On shadow profiles, ntfolow data was not stored away in order to save disk space. Channels can be configured very flexibly – colour, order, filters; the sources can also be specified. All these things could be changed when the channels were created. AS information could also be displayed. Adding, deleting and modifying channels could be done at any time.

Also, data could be displayed differently by specifying different filters. Shadow profiles only stored graphical information about traffic. Processing flows was based on the live profile data.

One could also convert profiles onto eachother. You can have a history profile, that keeps data but is no longer updated. You could stop temporarily the data collection.

IP lookup was a nice feature for flow processing. This was done by simply clicking on the IP address and a small popup widow appeared. The lookup could be customised via a Perl script.

There was no alerting in nfsen. You could also see what happened when you sat by the laptop, so additional plugins needed to be written for alerting. The solution, now integrated in the nfsen itself, consists in filters, conditions, triggers and actions associated with a live profile. The values could be either absolute or just percentages with respect to

a baseline. The actions were flexible, for example do nothing, send email, run a plugin or a system command.

Nfsen daemon allowed for external applications to talk to nfsen. An example would be alarms collected by software running on other operating systems. You can do anything what nfsen can do over this communication socket.

The simulator allowed for collecting the data in advance, define the start of the dataset and how much time should be in the simulation mode. You could also create profiles and alerts. This allowed for applying the same data with different parameters and fine-tune the alerts.

The to-do list was still growing. But this is a sign that people were using the software, so that's good. Features include adding an SQL-lite backend, user authentication and authorisation for different roles, importing and exporting profile/alert definitions.

Teun Nijsen asked when to expect the release 1.3, and whether a debian package would be supplied with the distribution. Peter Haag answered that the expected release date was July. He thought somebody already created a debian package. He would like to give this back to the community – if someone is using this system, and would like to do a package please send it to Peter Haag.

Maurizio Molina asked for further details on upgrading from the stable release. Peter Haag noted that upgrading is guaranteed from the stable version. But the upgrade was only supported from the last stable release. Also fine for any snapshots in between

Wim Biemolt observed that sampling was missing from the wishlist, so he was curious what the status was. Peter Haag answered that Maurizio Molina sent him an interesting paper about sampling, so there are still hopes to implement it for the 1.4 version.

Any other Business

Gorazd Božič announced he had not yet received a confirmation for the meeting in September in Porto. However, a backup option was available. He was also investigating options for the January meeting. Gorazd Božič discussed with Mike Caudill; it might be interesting to have a joint meeting with FIRST again, so if someone in the community would like to host the meeting please contact Gorazd Božič. It was more difficult to host this particular meeting in view of the large number of attendeed. Dates for the January meeting were not setup yet and would have to be coordinated with FIRST. Possibilities were: (mon, tue, wed) 21st or 28th of Jan.

Annex – List of attendees

First name	Last name	Organisation
Alberto	Lopez Ruiz	INTECO(National Institute for Communications Technologies)
Ales	Padrta	CESNET
Alexander	Talos	Univie / ACOnet
Andrea	Kropacova	CESNET
Andreas	Bunten	DFN-CERT
Andrew	Cormack	UKERNA
Baiba	Kaskina	LATNET
Balazs	Szekeres	CERT-Hungary
Branko	Mažar	CARNet CERT
Chelo	Malagon	IRIS-CERT/RedIRIS
Christoph	Graf	SWITCH
Claudio	Allocchio	GARR
Cyril	GAYET	CERTA
Cătălin	Meiroşu	TERENA
Daniel	Schirmer	ACOnet CERT
David	Pybus	Diageo plc
David	Freeman	ITsafe
Derek	Simpson	BTCERTCC
Detlef	Lange	Volkswagen Group
Dimitrios	Kalogeras	GRNET
Dmitry	Avramenko	RU-CERT
Don	Stikvoort	Trusted Introducer
Elisabeth	Stroem	UiO-CERT
Erika	Stockinger	SITIC
Ferenc	Suba	CERT-Hungary
Geoff	Jones	GovCertUK
Gilles	André	CERTA
Godert Jan	van Manen	DTO/CSIRT Team
Gorazd	Božič	SI-CERT (ARNES)
Gustavo	Neves	CERT.PT
Henrik	Skantz	SITIC
Hillar	Aarelaid	CERT-EE
Ian	Bryant	ITsafe Service
Jan	Heisler	CERTCZ
Jan	Meijer	UNINETT
Jimmy	Arvidsson	TS-CERT CC
Jochen	Schoenfelder	DFN-CERT
Karel	Vietsch	TERENA
Koen	Van Impe	BELNET-CERT
Ladislav	Lhotka	CESNET
Leila	Pohjolainen	Funet CERT
Luka	Pauk	CARNet CERT
Manuel	Ransan Blanco	INTECO(National Institute for Communications Technologies)
Margrete	Raaum	UiO-CERT

Maria	Jansson Rådström	TeliaSonera Abuse
Marius	Urkis	LITNET CERT
Maurizio	Molina	DANTE
Michelle	Danho	CERT RENATER
Mika	Müller	Ericsson PSIRT
Mikhail	Ganev	RU-CERT
Milda	Mimiene	LITNET CERT
Oliver	Pietsch	Volkswagen Group
Orod	Badjelan	DK-CERT
Pavel	Kácha	CESNET
Pavel	Vachek	CESNET
Peter	Haag	SWITCH-CERT
Phons	Bloemen	KPN-CERT
Przemek	Jaroszewski	NASK/CERT Polska
Rudolf	Schraml	Bundeskanzleramt
Sergey	Linde	RU-CERT
Solvita	Rovite	LATNET CERT
Teun	Nijssen	SURFnet-CERT
Thomas	Stridh	SUNet CERT
Till	Dörges	PRE-CERT - PRESECURE Consulting GmbH
Vladimir	Bobor	TS-CERT CC
Vladimir	Trestik	CESNET
Václav	Sedláček	CERTCZ
Werner	Schram	SURFnet
Wilfried	Woeber	ACOnet-CERT
Wim	Biemolt	SURFnet-CERT