Report z 39. konference europen.cz

www.europen.cz

EurOpen

Pavel Růžička
<ruza@ruza.eu>

Lightning talks, 10/2011

http://brmlab.cz | freenode #brmlab | brmlab@brmlab.cz

Co je konference EurOpen

www.europen.cz

EurOpen

Česká společnost uživatelů otevřených systémů EurOpen.CZ

* jarní a podzimní konference (nedělní tutoriál, Po-St přednášky)

* nezisková organizace

* cílem je seznamovat odbornou veřejnost s otevřenými systémy a podporovat jejich používání

* sborníky v brmlabí knihovničce, k dispozici i jako pdf

39. Europen, program

Formáty pro zaručený **elektronický podpis** (Libor Dostálek)

Sledování rozsáhlé počítačové **infrastruktury** (Pavel Tuček)

Uzamčená firemní **síť** (Ondřej Ševeček)

IPsec na Linuxu (Pavel Šimerda)

Šifrování disků nejen v Linuxu (Milan Brož)

PKI, sen nebo noční můra? (Luděk Smolík)

Elektronické pasy v praxi (Zdeněk Říha)

Správa revokovaných certifikátů v elektronickém platebním systému (Vít Bukač)

Moderné spôsoby návrhu distribuovaných a ťažko odhaliteľných **červ**ov (Norbert Szetei)

Sledování uživatelů prostřednictvím webových technologií (Jaromír Dobiáš)

SSC5 **EGI Security challenge**: Lehce na cvičišti. . . (Radoslav Bodó)

Bezpečnosť a vývoj **Rich Internet Application** (Juraj Michálek)

EGI security challenge 5

(Radoslav Bodó)

European Grid Infrastructure

Towards a sustainable grid infrastructure

Zapojená i ČR (ZČU, CESNET Metacentrum)

Resource Centres	~350
Participating countries	~50
CPU Cores	~250.000-330.000
Disk (PB)	106.7
Tape (PB)	112.8
Jobs 2010-2011 (usage)	949,000

Zdroj: http://www.egi.eu/infrastructure/Figures_and_utilisation/

Definice CSIRT

Computer Security Incident Response Team

Týmy typu CERT a CSIRT jsou týmy řešící a koordinují řešení bezpečnostních incidentů v definovaném poli působnosti (síť definovaná rozsahem adres, autonomní systém apod.).

Národní CSIRT České republiky

http://www.csirt.cz/page/885/faq/

EGI software

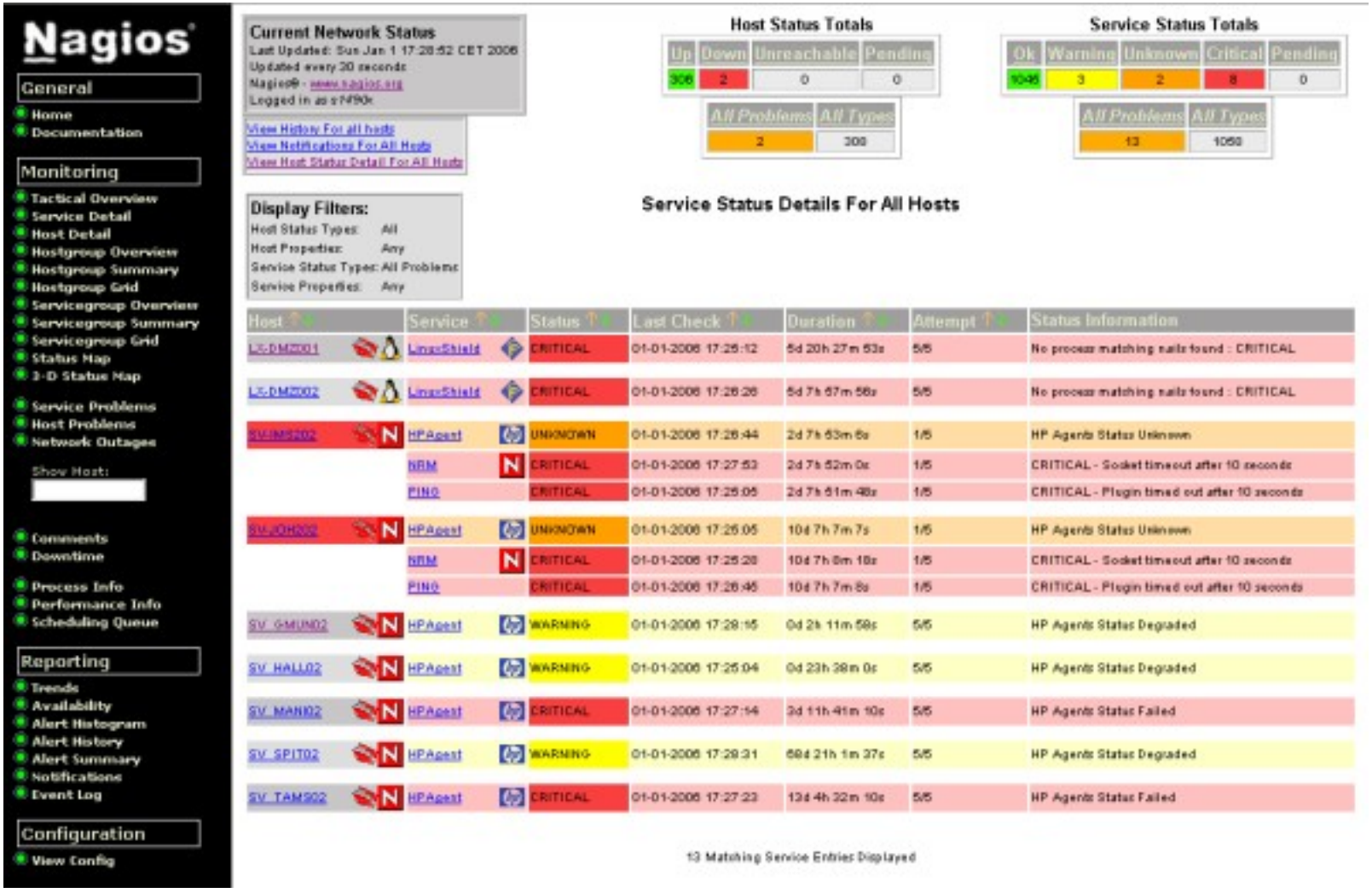
Nagios (www.nagios.org)

Pakiti (http://pakiti.sf.net)

ATLAS PanDA
(Production ANd Distributed Analysis system)

Další info: https://wiki.egi.eu/wiki/EGI_CSIRT:Monitoring

Nagios
(Network Monitoring Tool)



Pakiti

(a Patching Status Monitoring Tool)

www.europen.cz

EurOpen

Host/Package name	Installed version	Required version (Security repository, Main repository)	CVEs (Critical, Important, Moderate, Low) Show/Hide CVEs
	Domain:	Os:	Kernel:
autofs	1:5.0.1/0.rc2.55.el5.3	1:5.0.1/0.rc2.143.el5_5.4	
avahi	0:0.6.16/1.el5	0:0.6.16/9.el5_5	CVE-2008-5081 CVE-2009-0758 CVE-2010-2244
avahi-glib	0:0.6.16/1.el5	0:0.6.16/9.el5_5	CVE-2008-5081 CVE-2009-0758 CVE-2010-2244
crash	0:4.0/4.6.1	0:4.1.2/4.el5.centos.1	
cups	1:1.2.4/11.14.el5_1.6	1:1.3.7/18.el5_5.7	CVE-2009-0949 CVE-2008-3639 CVE-2008-3640 CVE-2008-3641 CVE-2009-0146 CVE-2009-0147 CVE-2009-0163 CVE-2009-0166 CVE-2009-0195 CVE-2009-0799 CVE-2009-0800 CVE-2009-1179 CVE-2009-1180 CVE-2009-1181 CVE-2009-1182 CVE-2009-1183 CVE-2010-0540 CVE-2010-0542 CVE-2010-1748 CVE-2009-3608 CVE-2009-3609 CVE-2009-2820 CVE-2009-3553 CVE-2010-0302 CVE-2008-5183
cups-libs	1:1.2.4/11.14.el5_1.6	1:1.3.7/18.el5_5.7	CVE-2009-0949 CVE-2008-3639 CVE-2008-3640 CVE-2008-3641 CVE-2009-0146 CVE-2009-0147 CVE-2009-0163 CVE-2009-0166 CVE-2009-0195 CVE-2009-0799 CVE-2009-0800 CVE-2009-1179 CVE-2009-1180 CVE-2009-1181 CVE-2009-1182 CVE-2009-1183 CVE-2010-0540 CVE-2010-0542 CVE-2010-1748 CVE-2009-3608 CVE-2009-3609 CVE-2009-2820 CVE-2009-3553 CVE-2010-0302 CVE-2008-5183
db4	0:4.3.29/9.fc6	0:4.3.29/10.el5_5.2	
dbus-glib	0:0.70/5	0:0.73/10.el5_5	CVE-2010-1172
device-mapper	0:1.02.20/1.el5	0:1.02.39/1.el5_5.2	
device-mapper-multipath	0:0.4.7/12.el5_1.4	0:0.4.7/34.el5_5.4	CVE-2009-0115
dhclient	12:3.0.5/7.el5	12:3.0.5/23.el5_5.1	
dhcp	12:3.0.5/7.el5	12:3.0.5/23.el5_5.1	
esc	0:1.0.0/32.el5	0:1.1.0/12.el5	CVE-2008-5913 CVE-2010-0182 CVE-2010-1121 CVE-2010-1125 CVE-2010-1196 CVE-2010-1197 CVE-2010-1198 CVE-2010-1199 CVE-2010-1200 CVE-2010-1202 CVE-2010-1203
firefox	0:1.5.0.12/15.el5.centos	0:3.6.7/3.el5.centos	CVE-2009-2654 CVE-2009-3070 CVE-2009-3071 CVE-2009-3072 CVE-2009-3074 CVE-2009-3075 CVE-2009-3076 CVE-2009-3077 CVE-2009-3078 CVE-2009-3079 CVE-2009-2462 CVE-2009-2463 CVE-2009-2464 CVE-2009-2465 CVE-2009-2466 CVE-2009-2467 CVE-2009-2469 CVE-2009-2470 CVE-2009-2471 CVE-2009-2472 CVE-2009-2664 CVE-2009-1392 CVE-2009-1832 CVE-2009-1833 CVE-2009-1834 CVE-2009-1835 CVE-2009-1836 CVE-2009-1837 CVE-2009-1838 CVE-2009-1839 CVE-2009-1840 CVE-2009-1841 CVE-2009-1313 CVE-2009-0652 CVE-2009-1302 CVE-2009-1303 CVE-2009-1304 CVE-2009-1305 CVE-2009-1306 CVE-2009-1307 CVE-2009-1308 CVE-2009-1309 CVE-2009-1310 CVE-2009-1311 CVE-2009-1312 CVE-2009-1563 CVE-2009-3274 CVE-2009-3370 CVE-2009-3372 CVE-2009-3373 CVE-2009-3374 CVE-2009-3375 CVE-2009-3376 CVE-2009-3380 CVE-2009-3382 CVE-2009-3979 CVE-2009-3981 CVE-2009-3983 CVE-2009-3984 CVE-2009-3985 CVE-2009-3986 CVE-2010-2755 CVE-2010-0654 CVE-2010-1205 CVE-2010-1206 CVE-2010-1207 CVE-2010-1208 CVE-2010-1209 CVE-2010-1210 CVE-2010-1211 CVE-2010-1212 CVE-2010-1213 CVE-2010-1214 CVE-2010-1215 CVE-2010-2751 CVE-2010-2752 CVE-2010-2753 CVE-2010-2754 CVE-2008-5913 CVE-2010-0182 CVE-2010-1121 CVE-2010-1125 CVE-2010-1196 CVE-2010-1197 CVE-2010-1198 CVE-2010-1199 CVE-2010-1200 CVE-2010-1202 CVE-2010-1203 CVE-2010-0174 CVE-2010-0175 CVE-2010-0176 CVE-2010-0177 CVE-2010-0178 CVE-2010-0179 CVE-2009-1571 CVE-2009-3988 CVE-2010-0159 CVE-2010-0160 CVE-2010-0162 CVE-2010-0167 CVE-2010-0169 CVE-2010-0171 CVE-2009-0040 CVE-2009-0771 CVE-2009-0772 CVE-2009-0773 CVE-2009-0774 CVE-2009-0775 CVE-2009-0776 CVE-2009-0777 CVE-2009-0352 CVE-2009-0353 CVE-2009-0354 CVE-2009-0355 CVE-2009-0356 CVE-2009-0357 CVE-2009-0358 CVE-2008-5500 CVE-2008-5501 CVE-2008-5502 CVE-2008-5505 CVE-2008-5506 CVE-2008-5507 CVE-2008-5508 CVE-2008-5510 CVE-2008-5511 CVE-2008-5512 CVE-2008-5513 CVE-2008-0017 CVE-2008-5014 CVE-2008-5015 CVE-2008-5016 CVE-2008-5017 CVE-2008-5018 CVE-2008-5019 CVE-2008-5021 CVE-2008-5022 CVE-2008-5023 CVE-2008-5024 CVE-2008-3837 CVE-2008-4058 CVE-2008-4060 CVE-2008-4061 CVE-2008-4062 CVE-2008-4063 CVE-2008-4064 CVE-2008-4065 CVE-2008-4067 CVE-2008-4068 CVE-2008-2785 CVE-2008-2933 CVE-2008-2798 CVE-2008-2799 CVE-2008-2800 CVE-2008-2801 CVE-2008-2802 CVE-2008-2803 CVE-2008-2805 CVE-2008-2807 CVE-2008-2808 CVE-2008-2809 CVE-2008-2810 CVE-2008-2811 CVE-2008-1380

EGI security challenge 5

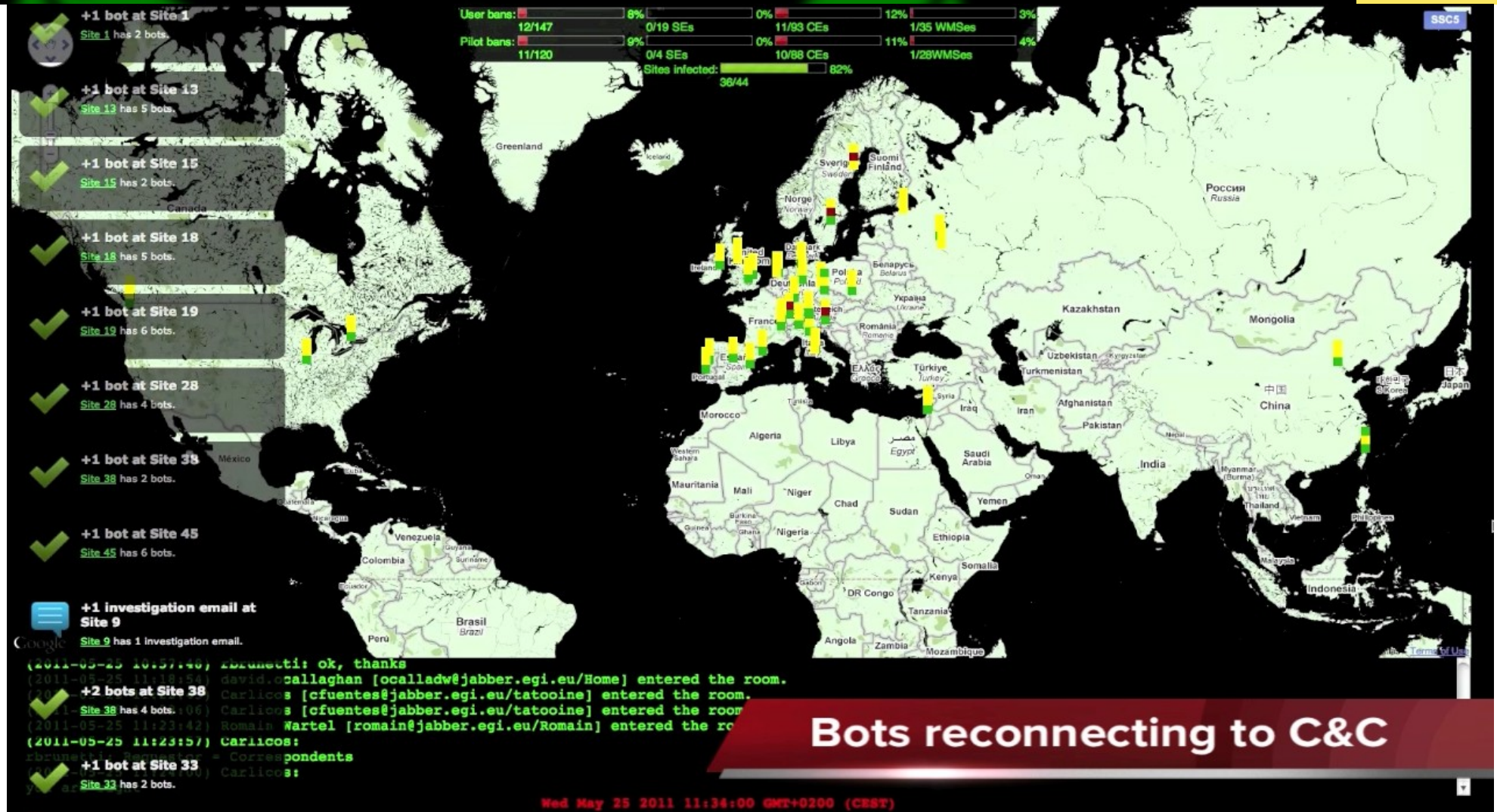
https://wiki.egi.eu/wiki/EGI_CSIRT:Security_challenges

http://www.nikhef.nl/grid/ndpf/files/Global-Security-Exercises/FIRST2011

SSC5 as it was seen
from a site administrator's lair

Eygene Ryabinkin, rea@grid.kiae.ru
National Research Centre "Kurchatov Institute"
http://goo.gl/Xeb0L

EGI security challenge 5



EGI security challenge 5

tcpdump, netflow, natstate, ipcs
dd /dev/kmem

ps, ls -la /proc/$PID/exe
file (not-stripped), ldd, strings, readelf
objdump

VM, strace, tcpdump (*.switch.vexocide.org)

EGI security challenge 5

Let's look at the workDir of the job:

ROOT.py
jobO.eee190ce-0f5c-4441-9975-24cf82e6ca86.**tar.gz**
pakiti-ssc-client
ratatosk.sh
tmp.stderr.c1756e3f-7027-48c2-801d-326e4c5f557b
tmp.stdout.f692706c-0838-44a8-9627-284a86401cb9
wopr_build_centos64.ANALY_GLASGOW

And what's in the .tar file:

$ tar tf jobO.eee190ce-0f5c-4441-9975-24cf82e6ca86.tar.wopr_build_centos64.ANALY_GLASGOW
wopr_build_v6_debian32.ANALY_GLASGOW
ratatosk.sh
pakiti-ssc-client

EGI security challenge 5

We have a script named job_setup.sh in the PandaJob directory:

<init stuff>
./**runGen-00-00-02** -j "" --sourceURL https://voatlas177 -p "%22ratatosk.sh %22"
-a jobO.eee190ce-0f5c-4441-9975-24cf82e6ca86.tar.gz -r --lfcHost lfc-atlas.grid.sara.nl --inputGUIDs 1>**prun_stdout.txt** 2>**prun_stderr.txt**

EGI security challenge 5

tcpdump, netflow, natstate, ps
VM, strace, tcpdump (*.switch.vexocide.org), file (not-stripped)

EGI security challenge 5

strace + tcpdump

"7\336\215\201\206Z\366\373\305@u\177-\210\207\301\340u\vp\236\
\346I\372O\\237\33s\311\16\234\3309-09a0-4e82-a258-80a425cb1fed\", \
\"version\": 6, \"payload\": { \"hostname\": \
\"xxxxx.grid.kiae.ru\", \"network\": { \"lo\": [{ \"family\": \
\"AF_INET\", \"ip\": \"127.0.0.1\", …

* It terribly reminds JSON;
* But it has 32 bytes (or 256 bits) of junk at the beginning and UUID-like stuff just after it;

EGI security challenge 5

First of all, let's understand what type of binary we have.

$ file wopr_build_centos64.ANALY_GLASGOW

wopr_build_centos64.ANALY_GLASGOW:\
ELF 64-bit LSB executable,\
x86-64, version 1 (SYSV), statically linked,\
for GNU/Linux 2.6.9, **not stripped**

EGI security challenge 5

Let’s try the simple tools first:

$ nm wopr_build_centos64.ANALY_GLASGOW | grep crypt

0000000004047f0 T **aes**_decrypt
0000000000403720 T **aes**_encrypt
000000000040ba80 T evbuffer_decrypt
000000000040bb80 T evbuffer_encrypt

looks like AES encryption was used for the first 32 bytes of JSON.

EGI security challenge 5

Running **strings** over the binary shows that it uses **libevent**, perhaps some library called scar_log that analyzes environment variable SCAR_DEBUG_LEVEL, it uses json-c and it has the string

“**omgwtfbbqidkfaiddqd**”

Heh?

IDA Pro, OllyDbg

“**omg wtf bbq idkfa iddqd**” used for encryption

“%x” in switch.vexocide.org is just the current time().

return codes from the library functions are
not really checked

author is relying on the fact that the incoming
string will always be larger than 32 bytes.

EGI security challenge 5

Let’s try the simple tools first:

$ nm wopr_build_centos64.ANALY_GLASGOW | grep crypt

0000000004047f0 T **aes**_decrypt
0000000000403720 T **aes**_encrypt
000000000040ba80 T evbuffer_decrypt
000000000040bb80 T evbuffer_encrypt

looks like AES encryption was used for the first 32 bytes of JSON.

Adobe, elektronický podpis

Softwareově prosazováno firmou Adobe jako standart

Podepisovací tablet

40. konference EurOpen

www.europen.cz

EurOpen

Česká společnost uživatelů otevřených systémů
EurOpen.CZ

Vaše příspěvky na jarní konferenci vítany

Více info na http://www.europen.cz