NorthSec 2015: behind the scenes

Posted on 2015/12/08 by Stéphane Graber

TLDR: NorthSec is an incredible security event, our CTF simulates a whole internet for every participating team. This allows us to create just about anything, from a locked down country to millions of vulnerable IoT devices spread across the globe. However that flexibility comes at a high cost hardware-wise, as we're getting bigger and bigger, we need more and more powerful servers and networking gear. We're very actively looking for sponsors so get in touch with me!

What's NorthSec?

NorthSec is one of the biggest on-site Capture The Flag (CTF), security contest in North America. It's organized yearly over a weekend in Montreal (usually in May) and since the last edition, has been accompanied by a two days security conference before the CTF itself. The rest of this post will only focus on the CTF part though.

A view of the main room at NorthSec 2015

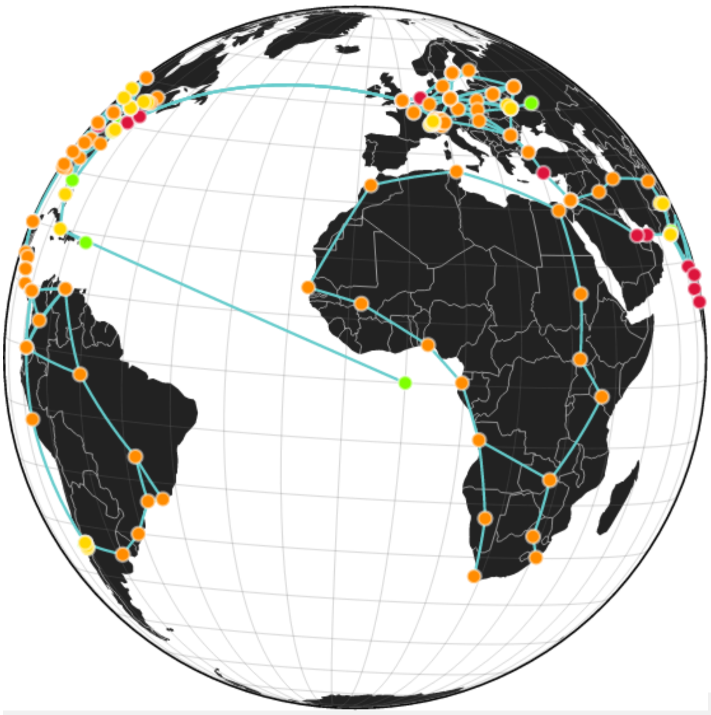
Teams arrive at the venue on Friday evening, get setup at their table and then get introduced to this year's scenario and given access to our infrastructure. There they will have to fight their way through challenges, each earning them points and letting them go further and further. On Sunday afternoon, the top 3 teams are awarded their prize and we wrap up for the year.

Size wise, for the past two years we've had a physical limit of up to 32 teams of 8 participants and then a bunch of extra unaffiliated visitors. For the 2016 edition, we're raising this to 50 teams for a grand total of 400 participants, thanks to some shuffling at the venue making some more room for us.

Why is it special?

The above may sound pretty simple and straightforward, however there are a few important details that sets NorthSec apart from other CTFs.

- It is entirely on-site. There are some very big online CTFs out there but very few on-site ones. Having everyone participating in the same room is valuable from a networking point of view but also ensures fairness by enforcing fixed size teams and equal network bandwidth and latency.
- Every team gets its very own copy of the whole infrastructure. There are no shared services in the simulated world we provide them. That means one team’s actions cannot impact another.
- Each simulation is its own virtual world with its own instance of the internet, we use hundreds of LXC containers and thousands of VLANs and networks FOR EVERY TEAM to provide the most realistic and complete environment you can think of.



World map of our fake internet

What’s our infrastructure like?

Due to the very high bandwidth and low latency requirements, most of the infrastructure is hosted on premises and on our hardware. We do plan on offloading Windows virtual machines to a public cloud for the next edition though.

We also provide a mostly legacy free environment to our contestants, all of our challenges are connected to IPv6-only networks and run on 64bit Ubuntu LTS in LXC with state of the art security configurations.

Our rack, on location at NorthSec 2015

All in all, for 32 teams (last year's edition), we had:

- 48000 virtual network interfaces
- 2000 virtual carriers
- 16000 BGP routers
- 17000 Ubuntu containers
- 100 Windows virtual machines
- 20000 routing table entries

And all of that was running on:

- Two firewalls (DELL SC1425)
- Two infrastructure servers (DELL SC1425)
- One management server (HP DL380 G5)
- Four main contest hosts (HP DL380 G5)
- Three backup contest hosts (DELL C6100)

On average we had 7 full simulations and 21 virtual machines running on every host (the backup hosts only had one each). That means each of the main contest hosts had:

- 10500 virtual network interfaces
- 435 virtual carriers
- 3500 BGP routers
- 3700 Ubuntu containers

- 21 Windows virtual machines
- 4375 routing table entries

Not too bad for servers that are (SC1425) or are getting close (DL380 G5) to being 10 years old now.

Past infrastructure challenges

In the past editions we've found numerous bugs in the various technologies we use when put under such a crazy load:

- A variety of switch firmware bugs when dealing with several thousand IPv6-only networks.
- Multiple Linux IPv6 kernel bugs (and one security issue) also related to an excess of IPv6 multicast traffic.
- Several memory leaks and other bugs in LXC and related components that become very visible when you're running upwards of 10000 containers.
- Several more Linux kernel bugs related to performance scaling as we create more and more namespaces and nested namespaces.

As our infrastructure staff is very invested in these technologies by being upstream developers or contributors to the main projects we use, those bugs were all rapidly reported, discussed and fixed. We always look forward to the next NorthSec as an opportunity to test the latest technology at scale in a completely controlled environment.

How can you help?

As I mentioned, we've been capped at 32 teams and around 300 attendees for the past two years. Our existing hardware was barely sufficient to handle the load during those two editions, we urgently need to refresh our hardware to offer the best possible experience to our participants.

We're planning on replacing most if not all of our hardware with slightly more recent equivalents, also upgrading from rotating drives to SSDs and improving our network. On the software side, we'll be upgrading to a newer Linux kernel, possibly to Ubuntu 16.04, switch from btrfs to zfs and from LXC to LXD.

We are a Canadian non-profit organization with all our staff being volunteers so we very heavily rely on sponsors to be able to make the event a success.

If you or your company would like to help by sponsoring our infrastructure, get in touch with me. We have several sponsoring levels and can get you the visibility you'd like, ranging from a mention on our website and at the event to on-site presence with a recruitment booth and even, if our interests align, inclusion of your product in some of our challenges.

Also, as I briefly mentioned at the beginning, we have a two days, single-track conference ahead of the CTF. We're actively looking for speakers, if you have something interesting to present, the CFP is here.

Extra resources

- Our website
- The conference call for papers
- Our Github account with the code for our internet simulation and our scoring system.

G+1 18

This entry was posted in Planet Ubuntu, LXC, Canonical voices, LXD and tagged containers. Bookmark the permalink.