Range Feedback

September 2021 1B4 Bootcamp

BLUF:

Technical challenges and growing pains caused a few headaches, but overall we were pleased with the responsiveness of Hadron and the performance of the Carthage range during this training iteration.

Training Profile:

We utilized the Carthage range for our annual/semi-annual 1B4 boot camp. A preparatory course for those awaiting Cyber Warfare Operations Initial Skills Training at Keesler AFB, MS. We utilized the range to teach Windows command-line, registry, and logs. Linux command line, and Cisco networking utilizing Packet Tracer (located on the Windows VMs). We also intended to use the range to teach basic pen-testing techniques, but were unable to for reasons noted below.

Initial setup & configuration:

The folks at Hadron worked very hard to get our range set up in time for our event. They set us up with admin access in Keycloak so that we could manage our own user accounts. This was a major positive over other solutions that we have used that relied on outside support for things like account creation, password resets, etc. One bit of criticism we had was that our initial meeting, running roughly 1.5 hours, was spent diving into the technical aspects of how the range operates (Ansible playbooks, back-end file structure, etc.) that we did not have the developer access to actually do anything with. It might be useful for the future, but didn't do much for our ability to utilize the range for our event. We felt the time would have been better served hammering out the specific requirements for our event rather than learning development procedures that we weren't able to use anyway.

During development we asked for a few changes. We asked to have Windows, CentOS, and Kali boxes available for our students to match the schoolhouse environment as closely as possible. The Hadron guys worked very hard to get it done, but the effort of adding the CentOS VMs may have led to other delays that put us very close on getting the range ready in time for the event. We also asked for some specific software to be installed (specifically PacketTracer and PyCharm EDU). They were able to make those additions in a timely manner.

In the end we had what we needed when we needed it, but we ended up without much lead-time to try everything out and work out bugs prior to Day 1.

Account setup:

Setting up user accounts in Keycloak was very simple for our admins to do. However, due to what we assume was a profile issue, email verification messages and password reset emails were not sent to students. We were able to work around this by manually verifying emails in Keycloak and directing students to the login page and having them click the "forgot password" link to reset their passwords. We had a couple of late adds, and the Hadron folks were quick to support in getting their VMs added to the range quickly.

During the event:

The account and VM issues were worked out within the first 1-2 hours of Day One. This set us back a tiny bit, but it was not unexpected. One major issue was the NextCloud collaboration platform. It was fantastic for getting project files on and off of the range, a functionality that we have not seen on other range platforms. However, we had some considerable issues with the video chat functionality. We initially intended to use NextCloud for our presentations, chat, and file sharing during the event. However, screen sharing in voice/video chats proved to be unusable. We had approximately 15 people in the call and whenever someone attempted to share their screen the presenter's computer would lock-up and cause them to have to exit the call to recover. We ended up moving to Discord for our presentation/chat.

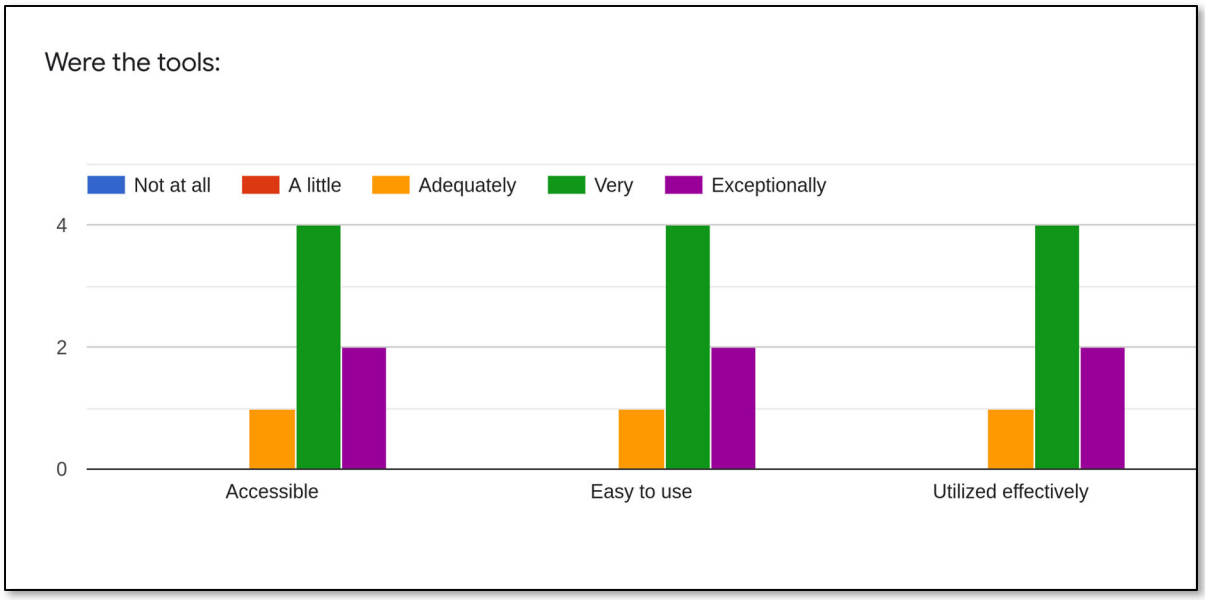
During the event, we primarily utilized the Windows and CentOS VMs. One thing that we didn't anticipate was the need to have Admin rights on the Windows machines to do some of the planned exercises (such as editing the registry). Since users did not have admin rights on the domain, we were able to work around this by using the RangeControl local admin account. We aren't sure what the most elegant solution for that would be, but it worked for our purposes.

We originally intended to include a pen-testing block at the end of the course, but were unable to. This was largely due to the range not being completed in time for our pen-testing instructor to have time to develop any demonstration scenarios against the "defended" network. This was a "nice to have" and thus not detrimental to our training. However, now that the range is built I am confident that we could incorporate that in future iterations.

Student Feedback:

At the end of each block students were asked for feedback. We primarily used the range for Windows, Linux, and Cisco (PacketTracer). Below is individual feedback for each block.

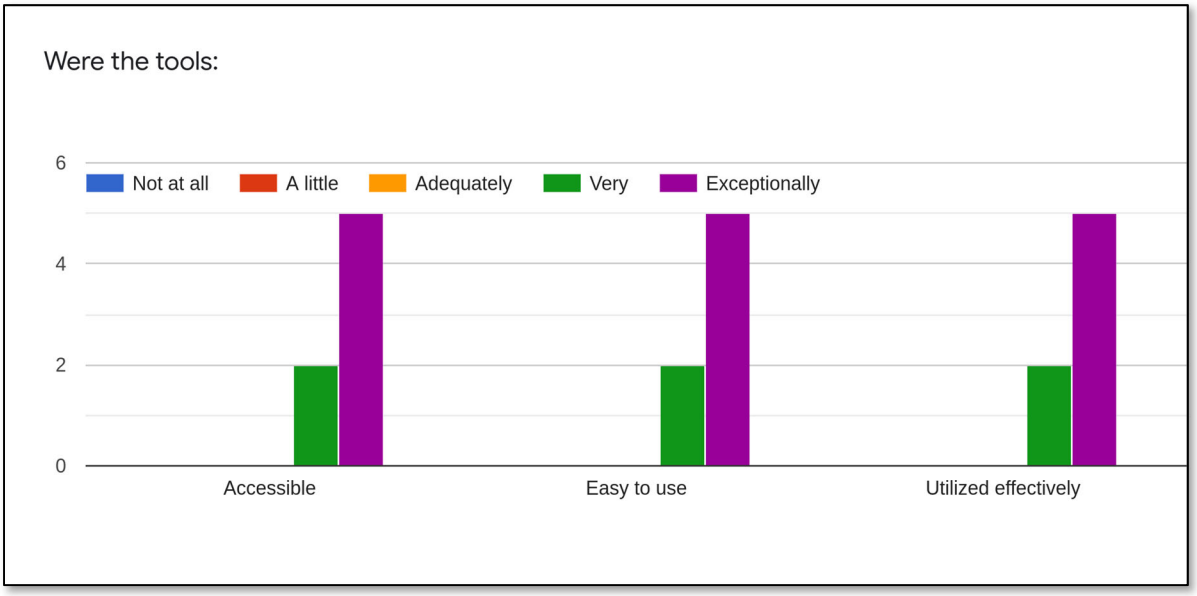
Block 1 (Windows):



Most students rated the range as “Very” or “Exceptionally” across every aspect we surveyed. Individual comments also often mentioned the hands-on portion as their favorite part of the block of instruction. One piece of negative feedback was the fact that the Windows VMs have an English (UK) keyboard set as

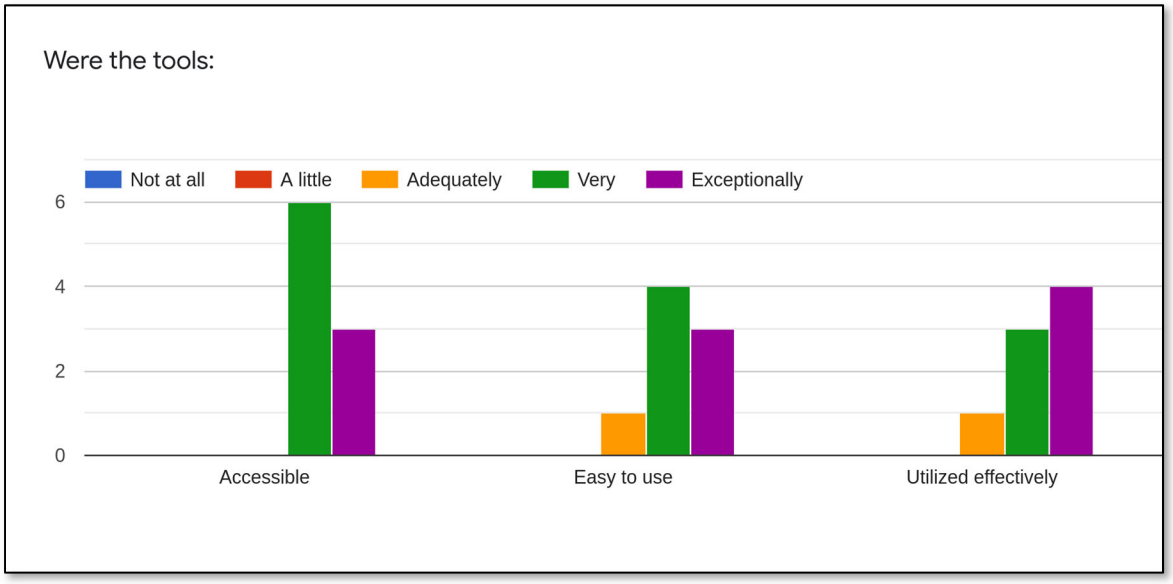
default, causing some keys to be mapped incorrectly on a US keyboard. We spoke to the Hadron guys about this and their answer was that it is a known issue that no one has had the time to fix.

Block 2 (Linux):



Again, for this block, all student feedback was either “Very” or “Exceptionally” for all aspects surveyed. Some noted in individual comments that their VMs timed out and locked pretty quickly. I doubt this is something that can be automated during the install process and is likely just an issue with GNOME 3 in general.

Block 5 (Cisco w/PacketTracer):



Continuing the trend, the majority of students rated the range “Very” or “Exceptionally” on all surveyed aspects. We did have some issues with the installed version of PacketTracer, but were easily able to correct it by using Nextcloud to transfer an installer for a compatible version to the VMs and get back on track in a timely manner. This did not appear to affect students' appraisal of the available tools.

Block 6 (Offensive Cyber Operations):

Unfortunately, we were not able to complete this block due to a lack of preparation time related to our requested changes and some technical challenges on the part of the Hadron guys in getting the range built. Given additional development time, we are confident we can conduct this block of training using the Carthage range in the future.

Conclusion:

Overall, we were happy with our experience using the Carthage range. We are especially thankful to the people of the New Hampshire National Guard for the generous loan of their equipment for our event. Also, thanks to Klee, Hunter, and the guys at Hadron for supporting us even though we are not their primary customer.

Positive aspects we experienced included:

- Ability to manage our own user accounts
- NextCloud collaboration platform
- Ability to do dev work on our own range (future)
- Responsiveness of the Hadron crew
- Ability to easily view student VMs (essential for remote training)

Negative aspects we experienced included:

- NextCloud functionality using screen sharing in video chat
- No access to dev consoles
- Dev seems to require a fair bit of technical knowledge/time
- Technical difficulties caused the range not to be fully ready in time for the event

If you have any additional questions about this report or our experiences using the Carthage range, please feel free to contact the 426 NWS CyT team at 426NWS.DOT.Training@us.af.mil.

REEVES.WILLIAM.DEAN.1298726390

Digitally signed by REEVES.WILLIAM.DEAN.1298726390
Date: 2021.12.03 15:54:58 -05'00'

WILLIAM REEVES, MSgt, USAF
Unit Training Manager
426th Network Warfare Squadron / CyT