CSCI 420 SOFTWARE SECURITY

MIA WEBER

05/08/2023

NCAE Cyber Games Report

Prior to the Competition

Prior to the competition I watched all 38 tutorial videos. The first fifteen were primarily concerned with basic Linux commands, useful services, and important steps to take in configuring user accounts. The topics from this section of videos that proved most helpful during the competition were user permissions and access management. There were a few times during the competition that I had to create files or directories to house configuration files, and I needed to ensure that the permissions were set correctly in order for the configuration to work correctly.

The next eight were concerned with networking and services. The videos focused on networking configuration using tools like netcat, netplan, ping, and interfaces and ifcfg files. The topics from this section of videos that proved most helpful during the competition were the videos concerning network configuration. The internal Ubuntu machine that I was working with in order to configure DNS had a lot of networking problems and vulnerabilities that needed to be addressed and videos from this section proved helpful in troubleshooting the network issues on the system.

The last fifteen videos were concerned with routing and services. The videos covered SSH configuration, router configuration, DNS service configuration, as well as the importance of backups and some backup techniques including rsync and cronjobs. This section also covers firewall configuration. The topics from this section of videos that proved most helpful during the competition was DNS configuration. I focused a lot on the DNS configuration during the competition and found my notes from the DNS configuration videos particularly helpful. Below are pictures of my notes from the DNS videos that were most helpful during the competition.

**INSERT PIC

During the Competition

During the competition I primarily worked on the infrastructure portion of the challenge. There were numerous aspects to the infrastructure portion of the challenge, including configuring the router, configuring FTP, setting up the web servers, and configuring DNS (both internal to the network and

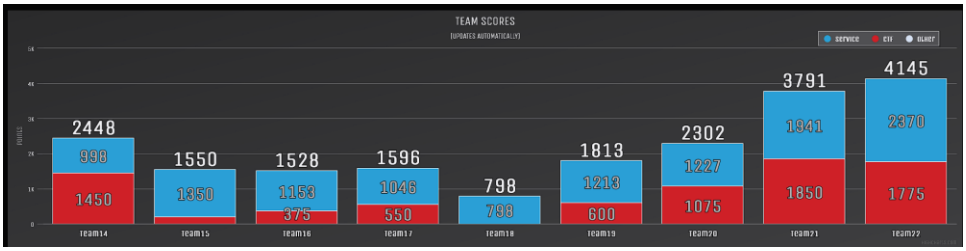
external through the router). I focused on configuring DNS, setting up the machines to match the required network topology (including IP addresses and user permissions and passwords), as well as working on the web server. The most difficult part of the infrastructure configuration was that all of the internal machines were already corrupted by the red team as soon as the competition began. This meant that configuring things like FTP and DNS didn't just involve configuring them from scratch but also fixing elements of the system that were corrupted just to be able to get to the point of configuring the services. This was very challenging because while I was configuring DNS, I would run into issues with resolving the host and although I could ping outside IP addresses, attempts at using commands like curl and wget in order to view the content of webpages was unsuccessful. This was frustrating at times because it made it hard to determine if there were connectivity problems because of the configuration files that I had created and written for DNS or if it was a larger system issue caused by an exploited vulnerability. I had to fix numerous configuration files for bind to get DNS working and there were symlinks to other files that were set incorrectly and needed to be changed. Because there was no firewall enabled on the system it made it difficult to determine why there were issues connecting with the local host at times because there shouldn't have been any restrictions. In the end I ended up spending most of my time attempting to get DNS up and running as well as helping to troubleshoot issues with FTP when those services were taken down by the red team (although we were ultimately unable to get those services back up after a key user was removed). I also worked on the web services and attempting to get those up and running but ran into issues with that since the DNS was not yet working. I ended up successfully being able to get the DNS service running but wasn't able to fix the networking issues that was preventing the responses to the DNS requests to go through so the internal DNS was never fully working (ended at level yellow instead of level green which meant that the service was running but the configuration wasn't working correctly). There were a lot of dependencies iin the challenge. Many things would run into a dead end until other things were configured- for example the web serves couldn't get up and running correctly until the external DNS over the router was correctly configured but that of course couldn't happen until the internal DNS was configured which was dependent on fixing the network vulnerabilities on the Ubuntu machine.

The consequence of all of these dependencies was that it made it hard when you hit a wall because you couldn't really switch gears and try to work on something else. You just had to keep pushing and hope you could figure it out. And since each section of the competition was three hours long by 2:30 or 3:00 nothing was working and even the things we had working (like FTP) had been taken down by the red team. It made it challenging to keep working on the same issue because you couldn't

really take a step back and approach a different aspect of the challenge super easily. By the end of the competition most of the team had switched our focus to CTF since those challenges were easier to work on incrementally and had less dependencies.

Conclusion and Takeaways

Overall, I enjoyed the competition. There were definitely some frustrating aspects, and I did feel generally unprepared going into the competition. I was still confused on exactly what the competition would look like until just a few days before and although the extensive notes that I had taken while watching the videos were super helpful during the competition, the sandbox VMs that could be used for practice were not as helpful and didn't have a clear connection to the things that ended up being involved in the actual competition. I definitely think that I would have enjoyed it more if we were not being actively attacked by the red team because configuring things like DNS from scratch are difficult enough, then add in the fact that I was configuring DNS on a really old Ubuntu system with only a command line and was working with an already corrupted machine while being actively attacked. It was challenging to say the least, but I definitely learned a lot and got a lot of practice with configuring things and setting up a system according to specifications and a network topology diagram which was good. There were times where I got really frustrated that I wasn't able to get DNS working but then I had to remind myself that only team 21 got both the internal and external DNS working and team 22 was the only other team to get anything green on DNS and the red team took that down numerous times. In the end I was proud to have gotten both internal DNS tasks to the yellow state and even after they got shut down, I fixed them and got it working again. I am super proud of what we were able to accomplish as a team, everyone worked super well together, and our diverse backgrounds and different knowledge areas were helpful and ultimately was a large reason for the success we saw. Below is a screenshot of our team's final placement (we were team #20). I also included a screenshot of the output that I saw at one point while trying to get DNS configured correctly (there were issues with IPv6 configuration on the Ubuntu machine that caused issues) that represents some of the common issues that I ran into while configuring DNS.



```
root@planetarium:/etc/bind# systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-03-11 21:13:15 UTC; 1h 4min ago
       Docs: man:named(8)
   Main PID: 651 (named)
      Tasks: 8 (limit: 2271)
     Memory: 29.7M
     CGroup: /system.slice/named.service
             └─651 /usr/sbin/named -f -u bind

Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 199.7.91.13#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 2001:500:a8::e#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 192.5.5.241#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 2001:dc3::35#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 2001:500:2::c#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 2001:503:c27::2:30#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 198.97.190.53#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 199.9.14.201#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 192.36.148.17#53
Mar 11 22:17:35 planetarium named[651]: network unreachable resolving 'ns1.team20.net/A/IN': 2001:7fd::1#53
root@planetarium:/etc/bind#
```