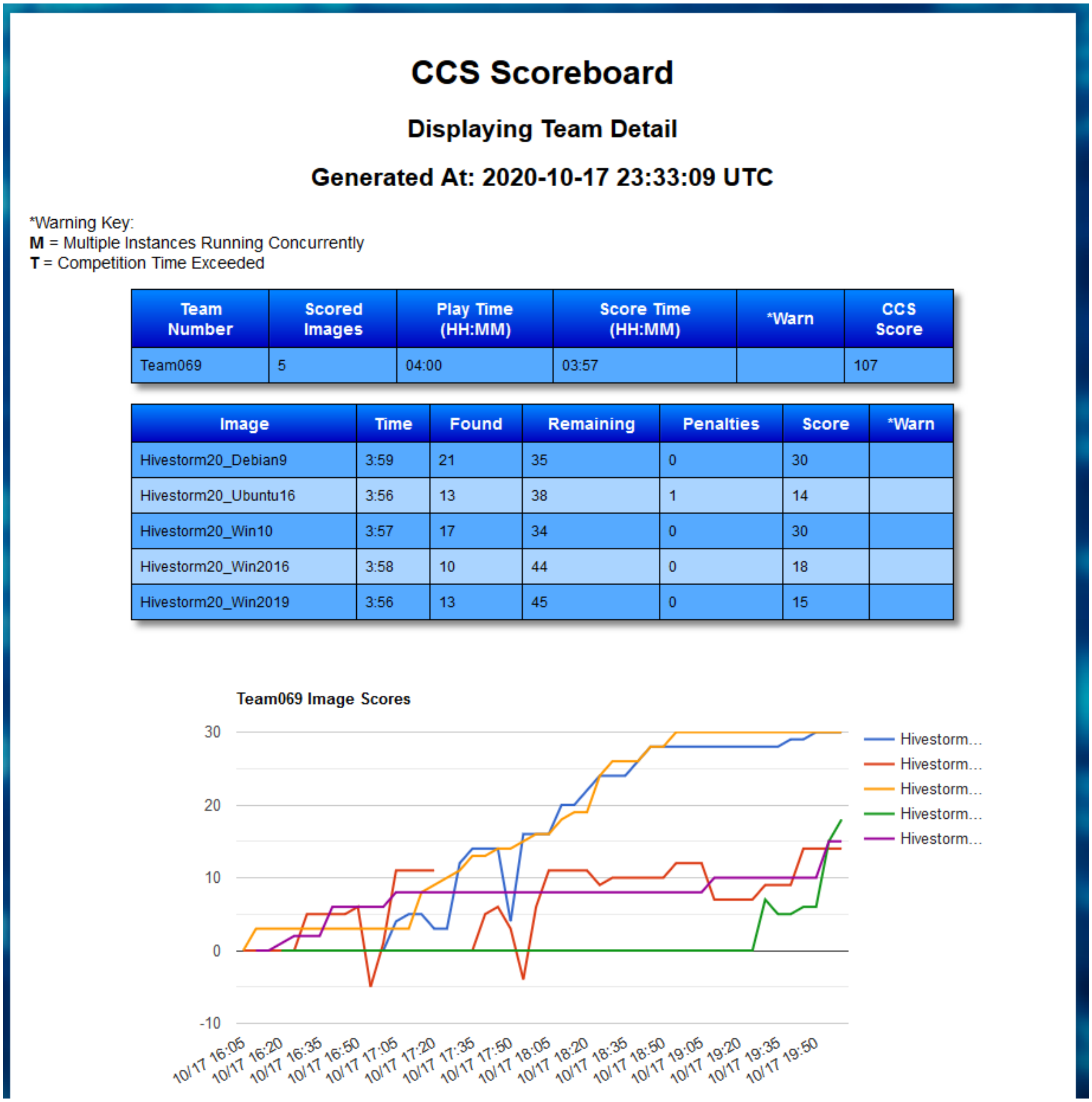
Debrief Hivestrom Team E

Score board



CCS Scoreboard

Displaying Team Detail

Generated At: 2020-10-17 23:33:09 UTC

*Warning Key:
M = Multiple Instances Running Concurrently
T = Competition Time Exceeded

Team Number	Scored Images	Play Time (HH:MM)	Score Time (HH:MM)	*Warn	CCS Score
Team069	5	04:00	03:57		107

Image	Time	Found	Remaining	Penalties	Score	*Warn
Hivestorm20_Debian9	3:59	21	35	0	30	
Hivestorm20_Ubuntu16	3:56	13	38	1	14	
Hivestorm20_Win10	3:57	17	34	0	30	
Hivestorm20_Win2016	3:58	10	44	0	18	
Hivestorm20_Win2019	3:56	13	45	0	15	

Team069 Image Scores

Team position

Name	Image	Score
Michael	Ubuntu 14	14
George	Debian	30
Yusuf	Windows 10	30
Yusuf	Windows 2016	18
Dorian	Windows 2019	15

Improvements

Windows server 2019:

1. Better checklist (especially when it comes to enabling services)
2. Better checklist GPO
3. Findings more way to enable a service, firewall rules, etc
4. Being more efficient running netstat/ see services running on the box
5. Forensic questions (dll, port#)

Overall Impression

Dorian: Fun for sure. Good first exposure to “hardening” boxes in a competition environment. The boxes were lagging for most of the time, until VMware workstation was used. The hivestorm practice was nothing compared to the actual competition in my opinion. Forensic questions were almost impossible to solve in my case. For the future, have better checklist, learn to enable services (http, rdp, ldap) faster and being able to see what services are already running faster.

Mike:
Images are a lot harder than the practice images. Keep in mind that there are 5 images in total that 4 people need to manage and work together on. I think that one the windows workstation user and server user end up getting stuck, they can check each other's things and start working on the last box (assuming the linux users don’t know windows server, which was Team 69’s situation). In terms of findings, updating software on a large scale using the gui can cause problems when restarting the box. I’ve found that on both, the practice image and the actual vm, that restarting can brick your computer. If you get the points from mass updating, good ig. In general, it is probably a better practice individually updating the software it wants you to keep updated in the readme. This is also probably a faster method of updating the programs since

you are not updating every single bit of the operating system. Also you can get easy points from deleting unauthorized users. I feel like for next year, having a greater understanding of the fundamental operating system will help a lot.

Yusuf:
Forensics questions were much harder than expected, the ones that we had for practice were extremely easy while some of the ones we had in the actual competition were things that I had never seen before. Spent too much time trying to figure out the forensics questions, definitely should have saved them for later. I think I had a decent checklist, it could have been better but I think I scored a decent amount. I’m probably going to use the thing that was sent in the Hivestorm chat for the next time. I definitely should have switched to the 2016 server VM way earlier, once I ran into a wall with the Windows 10 VM I wasted too much time when I could have done basically the same exact thing on the 2016 server VM and gotten many more points. I think the overall experience was pretty fun though and it was a worthwhile experience.