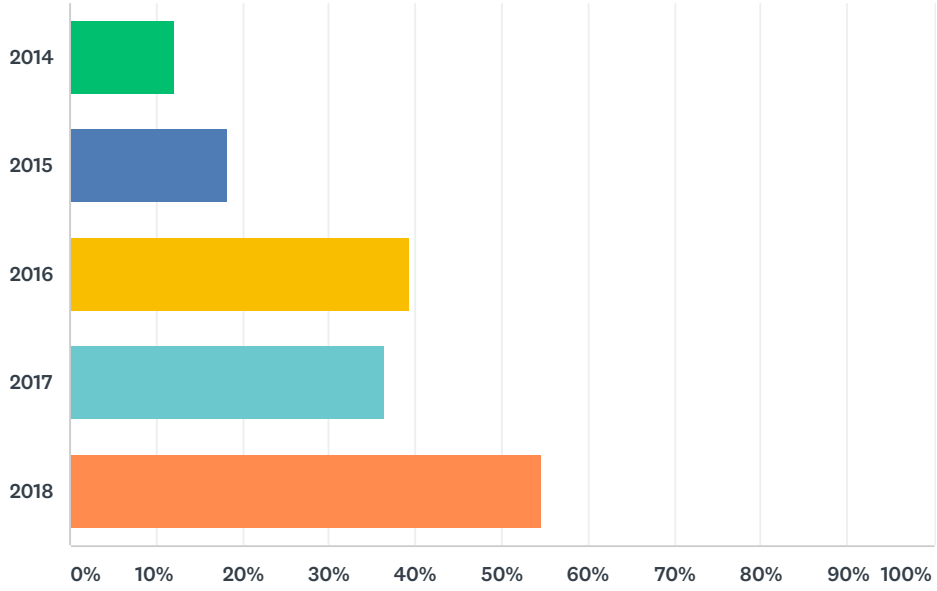
Q1 Year(s) of participation in NATO CCDCoE Crossed Swords exercise (formerly known as -- Red Teaming Workshop)

Answered: 33 Skipped: 0



ANSWER CHOICES	RESPONSES	
2014	12.12%	4
2015	18.18%	6
2016	39.39%	13
2017	36.36%	12
2018	54.55%	18
Total Respondents: 33		

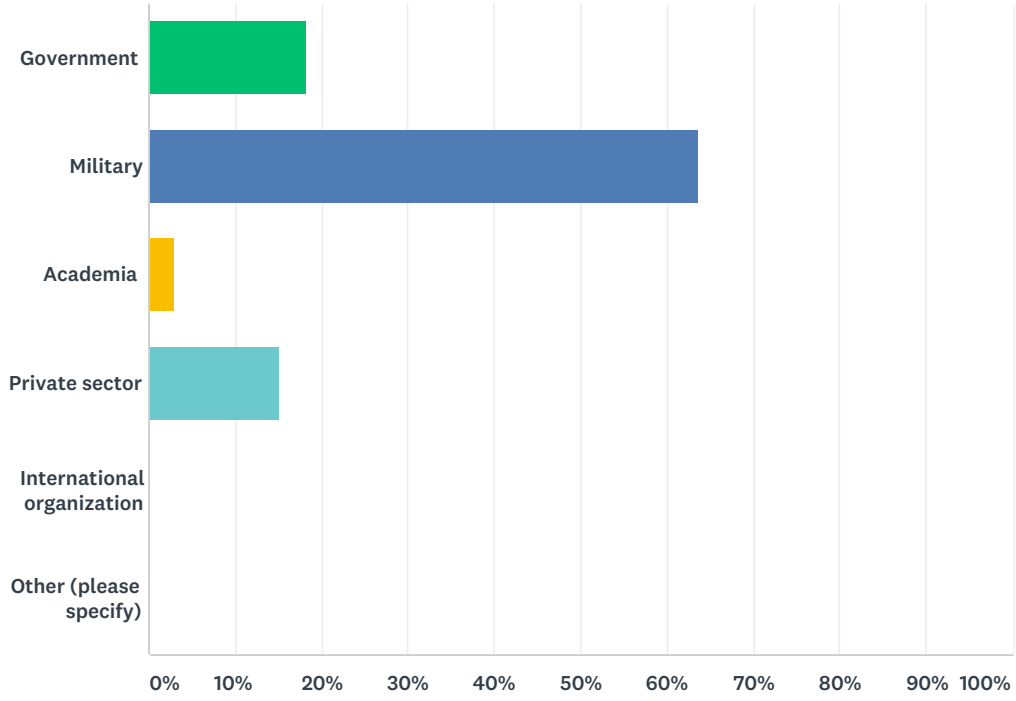
Q2 Country represented at the exercise (in case of an international organization -- the name of the organization)

Answered: 33 Skipped: 0

#	RESPONSES	DATE
1	Netherlands	10/25/2018 5:27 PM
2	Czech Republic	10/9/2018 10:47 AM
3	Germany	10/4/2018 11:06 AM
4	Spain - ESP CYBERCOM (MCCD)	9/25/2018 12:43 PM
5	Spain	9/24/2018 9:03 AM
6	CERT.LV	9/20/2018 4:51 PM
7	Austria	9/20/2018 10:09 AM
8	POLAND	9/20/2018 9:21 AM
9	Spain	9/19/2018 2:45 PM
10	MOD NLD	9/19/2018 1:13 PM
11	Netherlands	9/19/2018 12:55 PM
12	Czech republic	9/19/2018 10:42 AM
13	Netherlands	9/19/2018 10:33 AM
14	LV	9/18/2018 11:59 PM
15	Slovakia	9/18/2018 8:44 PM
16	Lithuania	9/18/2018 6:21 PM
17	Austria	9/18/2018 5:29 PM
18	Poland	9/18/2018 1:51 PM
19	Kudelski Security	9/18/2018 1:47 PM
20	CZ (GreyCortex)	9/18/2018 1:40 PM
21	LV	9/18/2018 12:44 PM
22	Canada	9/18/2018 12:39 PM
23	Slovakia	9/18/2018 11:12 AM
24	Latvia	9/18/2018 11:01 AM
25	Greece - HMOD	9/18/2018 11:00 AM
26	USA - UTICA College	9/18/2018 10:21 AM
27	Spain	9/18/2018 9:47 AM
28	netherlands	9/18/2018 9:34 AM
29	Germany	9/18/2018 9:31 AM
30	Spain	9/18/2018 9:23 AM
31	BHC Laboratory	9/18/2018 9:11 AM
32	USA - HTCI	9/18/2018 9:11 AM
33	BELGIUM	9/18/2018 8:43 AM

Q3 Type of the represented institution

Answered: 33 Skipped: 0

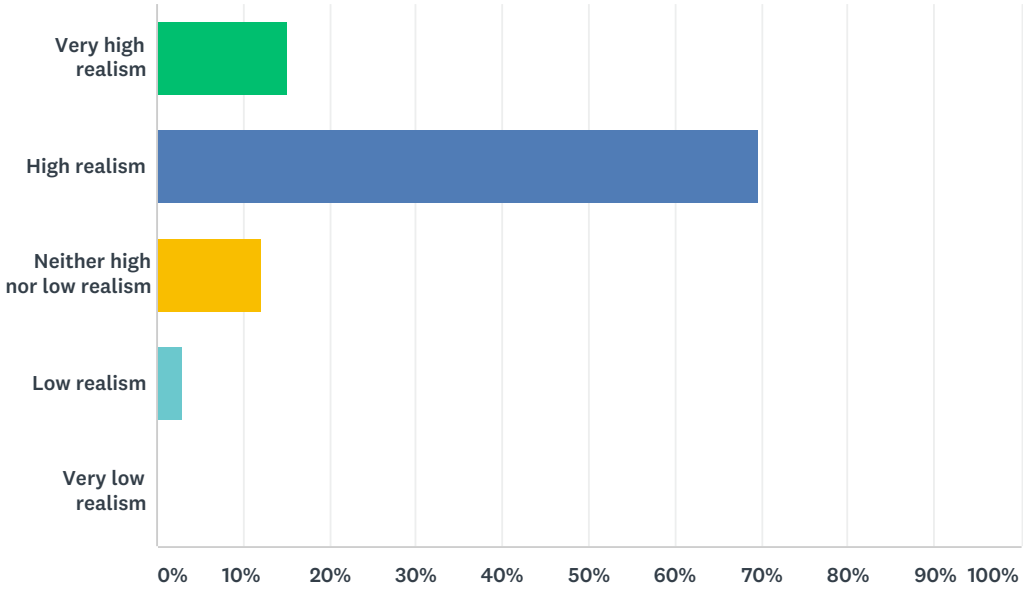


ANSWER CHOICES	RESPONSES	
Government	18.18%	6
Military	63.64%	21
Academia	3.03%	1
Private sector	15.15%	5
International organization	0.00%	0
Other (please specify)	0.00%	0
TOTAL		33

#	OTHER (PLEASE SPECIFY)	DATE
	There are no responses.	

Q4 Level of realism of the executed cyber operations at the exercise (Crossed Swords strives to provide the maximum training benefit and tries to replicate the real operational requirements as close as it is possible for a technical exercise)

Answered: 33 Skipped: 0



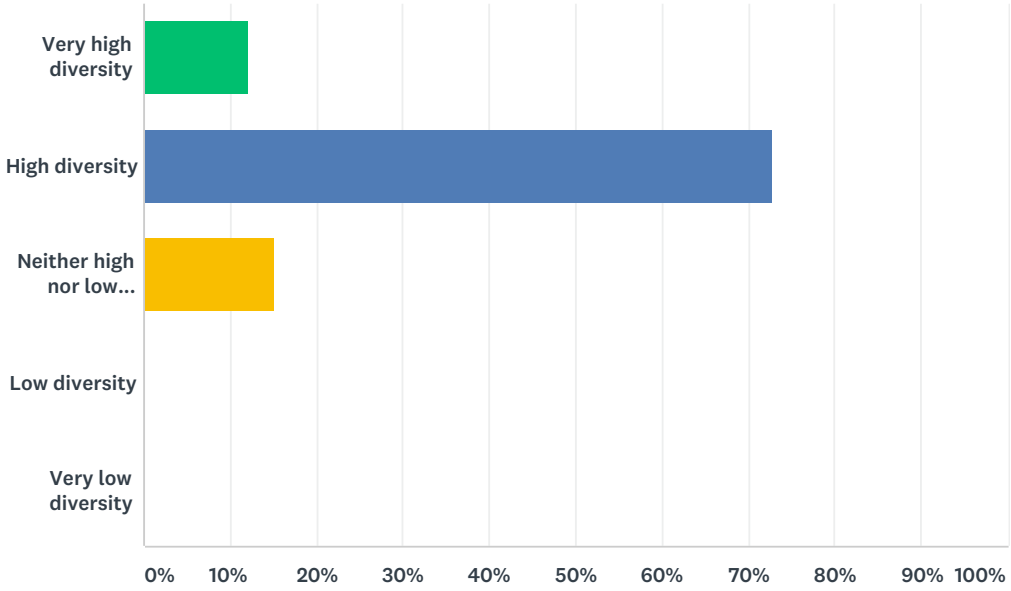
ANSWER CHOICES	RESPONSES	
Very high realism	15.15%	5
High realism	69.70%	23
Neither high nor low realism	12.12%	4
Low realism	3.03%	1
Very low realism	0.00%	0
TOTAL		33

#	COMMENTS (PLEASE SPECIFY)	DATE
1	high realism on the infrastructure part, low realism on the team communication part, because in my opinion it is rather hard/impossible to get a fully functional team	9/20/2018 4:51 PM
2	Technical yes, operational lack of processes not realistic in a military environment.	9/19/2018 1:13 PM
3	The client side could have increased their level of sophistication of the execution of their part by being more stealthy and coordinated. This would then increase the level of realism.	9/18/2018 8:44 PM
4	there where no actions from blue team side.	9/18/2018 5:29 PM
5	Can´t assess, as I haven´t been in situation dealing international/large scale cyber attack. Nevertheless, exercise shows quite well how things should (or shouldn´t :)) go in case of such incident (chain of command, cooperation between subteams/teamleaders/exercise leads etc.). It is really inspiring and useful in developing procedures for incident response.	9/18/2018 11:12 AM
6	You always have to trade some realism to achieve effective training in such an environment.	9/18/2018 10:21 AM
7	I took part in forensics spin off exercise	9/18/2018 9:47 AM
8	The compresion of time to fully cover all phases of the compromise takes away part of the realism.	9/18/2018 9:23 AM
9	It was high realism simulation.	9/18/2018 9:11 AM

10	as far as digital forensics / SOF is concerned at least	9/18/2018 8:43 AM

Q5 Diversity of target systems implemented in the exercise network

Answered: 33 Skipped: 0

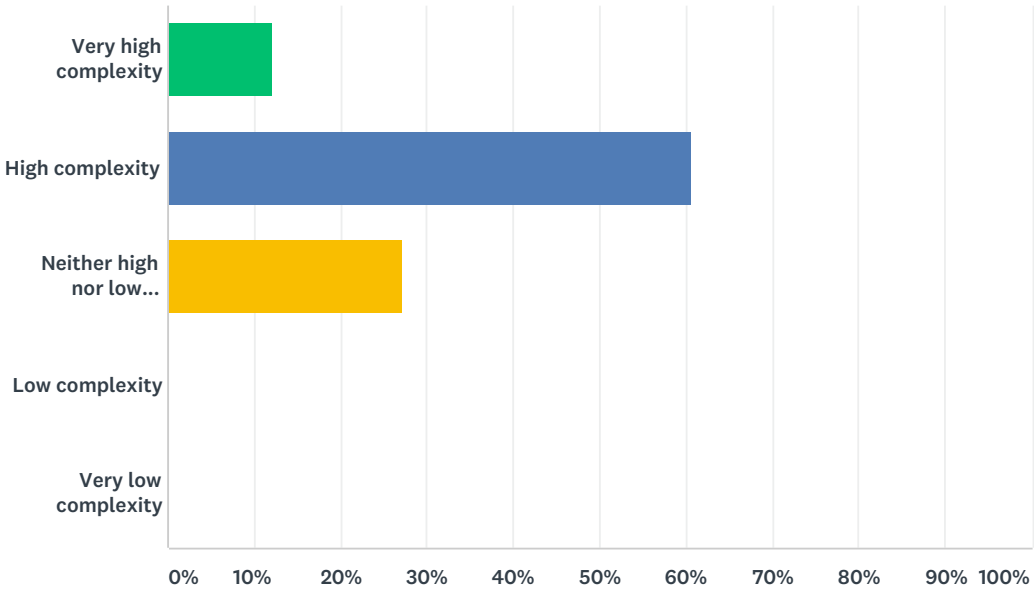


ANSWER CHOICES	RESPONSES	
Very high diversity	12.12%	4
High diversity	72.73%	24
Neither high nor low diversity	15.15%	5
Low diversity	0.00%	0
Very low diversity	0.00%	0
TOTAL		33

#	COMMENTS (PLEASE SPECIFY)	DATE
1	being on the yt part, it's somewhat hard to judge, but having taken part in this for one year as a red, i'd say it was reasonably well balanced with targets.	9/20/2018 4:51 PM
2	Compared to real life, or to other cyber exercises? :) Anyway, I think trere were quite lot of different things to play with, considering this is an exercise. I appreciate that exercise is evolving in this area, too - in 2018 there were definitelly more types of targets than in 2016.	9/18/2018 11:12 AM
3	As forensics investigator, changing target for sources of evidence	9/18/2018 9:47 AM
4	From my point of view, red team targets vere diverse enough to make necessary some kind of specialization on members of subteams	9/18/2018 9:23 AM
5	Sometimes it seemed that diversity was neither high or low it can be improved.	9/18/2018 9:11 AM

Q6 Technical challenge complexity level (taking into account the chain of attack, target system implementation and effort required for accomplishing the goal)

Answered: 33 Skipped: 0

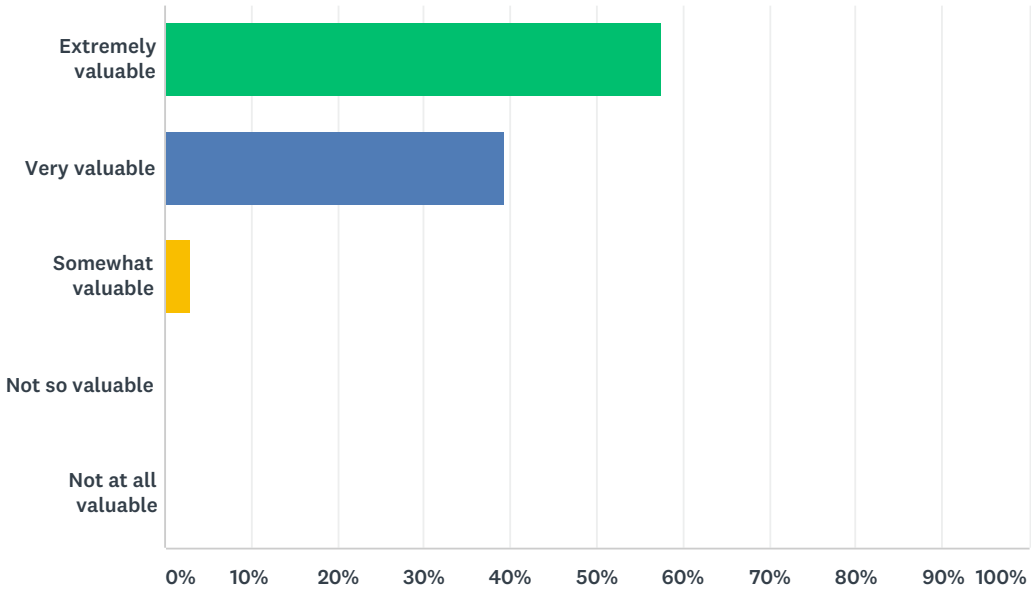


ANSWER CHOICES	RESPONSES	
Very high complexity	12.12%	4
High complexity	60.61%	20
Neither high nor low complexity	27.27%	9
Low complexity	0.00%	0
Very low complexity	0.00%	0
TOTAL		33

#	COMMENTS (PLEASE SPECIFY)	DATE
1	and again, this comes out based only on one year as a attacker, there were targets that were a low hanging fruit, and then there were plc controllers where there was some time for research needed to understand what's going on there, also buffer overflows/ropchains :>	9/20/2018 4:51 PM
2	for all specialisms high complecity, independences inbetween.	9/19/2018 1:13 PM
3	A good combination	9/19/2018 12:55 PM
4	The technical complexity was well balanced. I think the communication and coordination of operations had higher complexity.	9/18/2018 8:44 PM
5	technical challenge for host team was low.	9/18/2018 5:29 PM
6	Just right complexity. I remember that some targets were easy in the end, but to find them and find right way of exploiting took some time. Considering limited time of exercise execution, complexity level is IMHO satisfying.	9/18/2018 11:12 AM
7	Some of the exercises part of the forensic scenario were just difficult because a hyped storyline	9/18/2018 9:47 AM
8	One important thing to learn in this exercise is the necessity of internal collaboration so complexity is not high enough to make exercise impossible for a great majority of participants.	9/18/2018 9:23 AM
9	It was very challenging and the tasks very very nicely delivered via chain of attack.	9/18/2018 9:11 AM
10	clearly there has been an evolution (in the 2 years I participated / DF-SOF was implied). Some lessons identified have been learned, other / new ones are still on the todo list.	9/18/2018 8:43 AM

Q7 Exercise benefits and training outcome value (the benefit of the exercise for your and development and experience, as well as joint operation in an international context)

Answered: 33 Skipped: 0



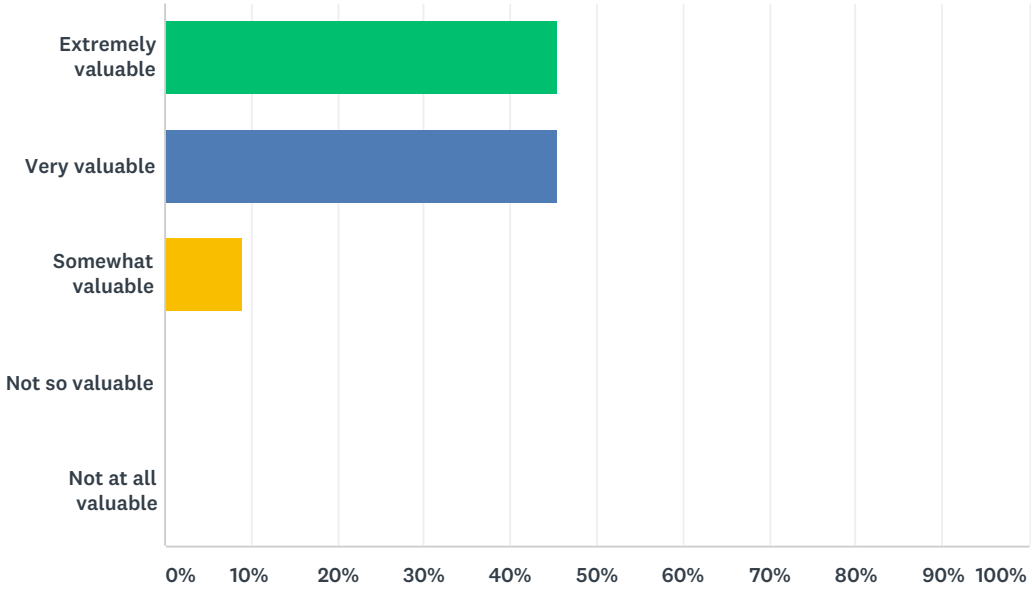
ANSWER CHOICES	RESPONSES	
Extremely valuable	57.58%	19
Very valuable	39.39%	13
Somewhat valuable	3.03%	1
Not so valuable	0.00%	0
Not at all valuable	0.00%	0
TOTAL		33

#	COMMENTS (PLEASE SPECIFY)	DATE
1	brush up things one has forgotten, learning new things, brainstorming with people who know more than oneself, also getting a grip on teamwork/peopleskillz.	9/20/2018 4:51 PM
2	Communication, coordination, leadership, feedback on stealthiness and detectability of operations.	9/18/2018 8:44 PM
3	I felt that this provided the most value: the chance to work with other teams, share ideas and techniques, and practice clear communication during an urgent, time-limited exercise.	9/18/2018 1:47 PM
4	I was there as an observer and believe the training was extremely valuable as many nations participated.	9/18/2018 12:39 PM
5	Great experience, both in technical point of view and in operational/management: It is valuable opportunity to test your managing and communicational skills, and to realize how tough it can be to keep a picture of everything going on, as the exercise goes on with new injects/findings every few minutes.	9/18/2018 11:12 AM
6	Training deficiencies were identified as well as ideas being generated for new TTPs.	9/18/2018 10:21 AM
7	I personally learnt a lot on working in groups with participants from other countries but the participation of civilians (from civilian companies) as trainees (attacking) made it weird since they will not be involved in a real operation. The use of the force is strictly reserved to government personnel in NATO countries...	9/18/2018 9:23 AM

8	Red team based teamwork was a big benefit and exercise challenges did provide a personal improvements as well.	9/18/2018 9:11 AM
9	cfr supra, lessons identified also for the internal (national) side	9/18/2018 8:43 AM

Q8 The value of provided detected attack feedback to the red team (exercise develops and implements novel technologies for attack detection and near real-time information provision to the red team)

Answered: 33 Skipped: 0



ANSWER CHOICES	RESPONSES	
Extremely valuable	45.45%	15
Very valuable	45.45%	15
Somewhat valuable	9.09%	3
Not so valuable	0.00%	0
Not at all valuable	0.00%	0
TOTAL		33

#	COMMENTS (PLEASE SPECIFY)	DATE
1	even if it is the low hanging fruit, people on the wire will notice it and one will get burnt, so it's not only on how good one is at the computer, it's also about how good one is to stay below the grid	9/20/2018 4:51 PM
2	every detection was very well described and we were informed what changes w can make to improve.	9/20/2018 9:21 AM
3	There were to many tools not known previously and was hard to figure out information	9/19/2018 2:45 PM
4	deliverd al lot of lessons identified, specially back to the own organisation	9/19/2018 1:13 PM
5	I was in yellow team. Feedback from red team was nice!	9/18/2018 5:29 PM
6	'||sleep(5)# BR :)	9/18/2018 1:51 PM
7	I can't comment this, since I was yellow team :)	9/18/2018 1:40 PM
8	No doubt it is really cool to see what´s going on, how your attacks are detected. By answering "Somewhat valuable" I mean that knowledge of us being detected did not influence our actions that much - as the time went, more and more focus was on completing the mission, even if our actions were detected. Generally, this feedback is very valuable as it makes you consider your actions more in real scenarios, outside cyber exercise.	9/18/2018 11:12 AM
9	Best part of the exercise to me was to be able to see how my actions were appearing in different log and representation systems and the oportunity to adapt my attacks and try again with a low visibility profile.	9/18/2018 9:23 AM

10	This was best aspect since it is essential to move as quite as possible in red teaming missions. Helps to improve stealthiness.	9/18/2018 9:11 AM
11	Not really applicable for digital forensics, since we were acting completely off-line	9/18/2018 8:43 AM