

# Cyber-Lab.Tech

David Kvatadze  
Tbilisi 2019



CYBER-LAB  
TECH

## Founders:



## Sponsors:



## Partners:



# History of Cyber Exercises and Idea of Lab Creation:

- CyberEXE for Public and Private Sector;

CYBER-EXE 2014  
GEORGIA14

CYBER-EXE 2015  
GEORGIA15

CYBER-EXE 2017  
GEORGIA17

CYBER-EXE 2016  
GEORGIA16

CYBER-EXE 2018  
GEORGIA18

- Cyber Cube for Students and Pupils;

CYBER CUBE 2017  
ქიბერკუბი

CYBER CUBE 2016  
ქიბერკუბი

CYBER CUBE 2018  
ქიბერკუბი

CYBER CUBE 2019  
ქიბერკუბი



CYBER-LAB  
TECH

# Aim of Cyber Lab:

- Increase awareness of cyber security;
- Testing and motivating young generation;
- Discovering new talents;
- First Cyber Lab in Caucasus region;
- Sharing knowledge during emergency situations;
- Implementation of unique platform;
- Support and Motivation of Georgian Universities;
- Support and Motivation of Public and Private Sector;
- Cyber security capacity building.





# Challenges of Cyber Lab:

- Not Enough Knowledge and Experience in Cyber Security;
- Lack of qualified staff in the country;
- Lack of product awareness and reaching the target segment;
- Lack of adequate resources.



# Preparation Process:

## I Phase

- Creation of a Structure of Cyber Lab;
- Selection of proper equipment;
- Development of proper software;
- Creation of cases and questions;
- Creation of teacher manuals.

## II Phase

- PR&HR activities;
- Meetings and presentations for universities and Organizations.

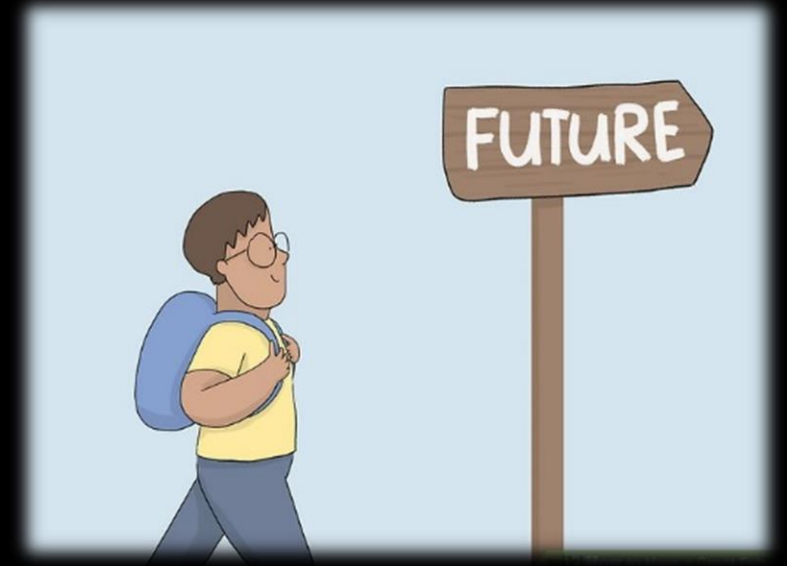
## III Phase

- Finding Sponsors.



# Future Plans:

- Translating the exercises into Russian and English;
- Adding more exercises;
- Improving the laboratory platform functions;
- Improvements in keeping the statistical data;
- Improving the integration of virtual machines with laboratory;
- Implementing PR activities in EaP countries.



# Target Audience:

- Universities,
- Public Sector,
- Private Sector.







# CYBER-LAB TECH

კიბერ-ლაბორატორია

კიბერუსაფრთხოების საკითხებში რეალური ზოდნის დისტანციურად მიღების საშუალება

შესასვლელად მიჰყავით გვერდი



CERT.GOV.GE



EaPConnect  
Eastern Partnership Connect



GEORGIAN RESEARCH AND EDUCATIONAL  
NETWORKING ASSOCIATION



# CYBER-LAB TECH

კიბერ-ლაბორატორია

კიბერუსაფრთხოების საკითხებში რეალური ზოდნის დისტანციურად მიღების საშუალება

შესასვლელად მიჰყავით გვერდი



CERT.GOV.GE



EaPConnect  
Eastern Partnership Connect

GRENA  
GEORGIAN RESEARCH AND EDUCATIONAL  
NETWORKING ASSOCIATION

## Portal Information:

## კონტაქტი

	GRENA	DEA
ელ-ფოსტა:	<a href="mailto:CONTACT@CYBER-LAB.TECH">CONTACT@CYBER-LAB.TECH</a>	<a href="mailto:CONTACT@CYBER-LAB.TECH">CONTACT@CYBER-LAB.TECH</a>
ტელეფონი:	+995 32 225 05 90	+995 32 291 51 40
მისამართი:	თ.შოველიძის ქუჩა 10 0108 თბილისი, სავარძელო	ზენკვანთაძის ქუჩა 50 0186 თბილისი, სავარძელო

\* სახელი, გვარი:


ორგანიზაცია:

მისამართი:

ტელეფონი:

\* ბეჭდი:

\* შეფურცლვა:

☐ I'm not a robot
 
  
reCAPTCHA  
Privacy - Terms

გაგზავნა

[illegible]

# Student's Interface:

LOG ANALYSIS

AMADEUS (50)

BACKDOORE (50)

FORCED IT (50)

QUESTION 1 (10)

QUESTION 2 (10)

QUESTION 3 (10)

QUESTION 4 (10)

QUESTION 5 (10)

FISHEYE (30)

SUSPICIOUS CALL (40)

TWO-FACE (50)

USERPRO (80)

VICTIM-BLOGGER (50)

MALWARE ANALYSIS

REVERSE ENGINEERING

PCAP ANALYSIS

STEGANOGRAPHY

MIX

CRYPTOGRAPHY

ამოცანები

ამოცანა

FORCED IT

50

კომპანიის ვებსაიტზე განხორციელდა შეტევა, მგერამ მისი ყველა დეტალი უნეტოია. თქვენ გადმოგვს სერვერის ე.წ. ACCESS LOG-ი შეტევის მომენტები და უნდა გავიგოთ, თუ რა მოხდა შეტევის დროს?

CASE2.LOG

LOG ANALYSIS

AMADEUS (50)

BACKDOORE (50)

FORCED IT (50)

QUESTION 1 (10)

QUESTION 2 (10)

QUESTION 3 (10)

QUESTION 4 (10)

QUESTION 5 (10)

FISHEYE (30)

SUSPICIOUS CALL (40)

TWO-FACE (50)

USERPRO (80)

VICTIM-BLOGGER (50)

MALWARE ANALYSIS

REVERSE ENGINEERING

PCAP ANALYSIS

STEGANOGRAPHY

MIX

CRYPTOGRAPHY

ამოცანები

2 ამოცანა

FORCED IT: QUESTION 1

10

როგორი IP მისამართებიდან განხორციელდა შეტევა?

პასუხი

გამგზავნა

რამდენიმე პასუხს შემთხვევითი პასუხები გაოყავით სკეინით

ამოცანა

სერვერი

0 ამოცანა

სახელმძღვანელო

გარტვა

გამორტვა

სტატუსი

ნაშლა

გაფრტინლება: საიტზე უმოქმედოების შემთხვევაში ჰირტუალური სერვერი ავტომატურად გაითიშება 2 საათში, ხოლო 8 საათში ნაიგლება.

# Information About Challenges:

LOG ANALYSIS	PCAP ANALYSIS	CRYPTOGRAPHY
AMADEUS (50)	COVERT CHANNEL (30)	BLINDWARE (30)
BACKDOORE (50)	HEIST-2 (80)	CAESAR MUSIC (10)
FORCED IT (50)	COVERT CHANNEL-2 (30)	CHAMBO (20)
FISHEYE (30)	DNS-FISH (80)	DES (40)
SUSPICIOUS CALL (40)	GUN-FIRE (100)	FONITEL (80)
TWO-FACE (50)	HIJACKING (140)	GEHEIMNIS (50)
USERPRO (80)	LOW-ORBIT (80)	GERMONA (20)
VICTIM-BLOGGER (50)	RAINBOW (80)	GOGEBÄ (30)
	HEIST-1 (120)	HUSKY (20)
MALWARE ANALYSIS	STEGANOGRAPHY	LAMBDA (70)
ADOBEREADER (35)	CORN (10)	LIKVIDA (20)
BOT (30)	DOGD0G (30)	LIKVIDB (20)
HILO (20)	KIM (30)	LORD (30)
RANS2 (50)	PYSTEGO (50)	MAFIA (40)
XRANSOM (95)	RAM (80)	MATRIX (15)
REVERSE ENGINEERING	YUCK (80)	MORPHEUS (25)
GEORGE PASSWORD (10)	MIX	QWERTY (50)
CRACKME (20)	BUFFER (20)	SCHEME-A (90)
ELF BINARY BOMB (90)	CASE13 (30)	SCHEME-B (110)
PE BINARY BOMB (90)	ETERNALROMANCE (200)	SCHEME-X (90)
SAMPLE 1 (20)	GUNMARKET (200)	SCHEME-Y (110)
SAMPLE 2 (30)	TROLLMACHINE (200)	SUBST (15)
SAMPLECUBE (30)	BUFFER-OVERFLOW (150)	WATCHMEN (10)
STAGE CRITICAL (100)	HACKLAB (15)	XOR BASE (35)
STAGE NEXT (100)		XOR CASE (35)
STAGE 1 (10)		XOR MASE (35)
STAGE1-BIN (30)		
STAGE1-JS (10)		
STAGE2 (10)		
STAGE2-BIN (50)		
STAGE2-JS (30)		
STAGE3-BIN (40)		
STAGE3-JS (10)		

## Number of Challenges 123:

- Log Analysis - 11
- Malware Analysis - 6
- Reverse Engineering - 27
- Pcap Analysis - 13
- Steganography - 11
- Cryptography - 28
- Cyber Hygiene - 1
- Forensics - 2
- Exploit Development - 6
- Penetration Test - 6
- Mix - 12

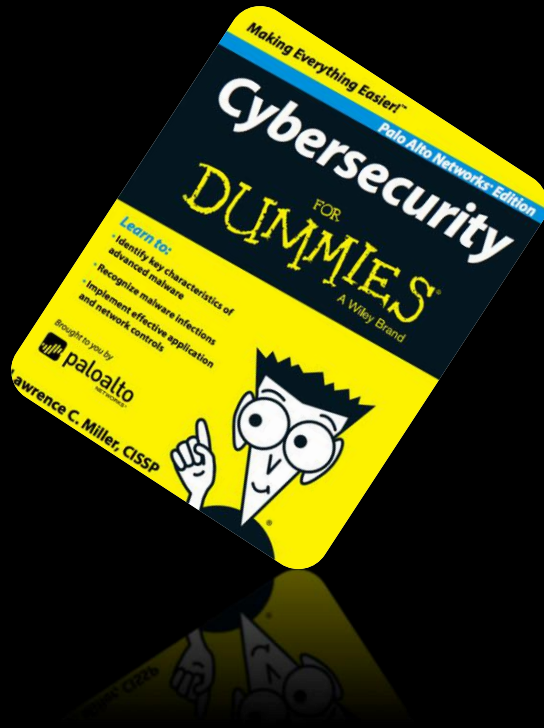
## Number of Questions 232:

- Log Analysis - 50
- Malware Analysis - 14
- Reverse Engineering - 35
- Pcap Analysis - 56
- Steganography - 11
- Cryptography - 28
- Cyber Hygiene - 1
- Forensics - 8
- Exploit Development - 6
- Penetration Test - 6
- Mix - 17





# Teacher's Manual Example:



ამოცანა სახელმძღვანელო

×

საპარამეტრო მომხმარებელი „LOG“ ფაილის გახსნის შემდეგ ვხედავთ ბევრ ჩანაწერს, თუმცა დასაწყისშივე ადვილად შევნიშნავთ შემდეგ ჩანაწერებს:

```
"GET /LgQ2vQ0j.1 HTTP/1.1" 404 285 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.2 HTTP/1.1" 404 285 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.access HTTP/1.1" 404 290 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:Non  
"GET /LgQ2vQ0j.adjunct HTTP/1.1" 404 291 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:Nor  
"GET /LgQ2vQ0j.AP HTTP/1.1" 404 286 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.asa HTTP/1.1" 404 287 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.asmx HTTP/1.1" 404 288 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.asp+ HTTP/1.1" 404 288 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.aspx HTTP/1.1" 404 288 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.axd HTTP/1.1" 404 287 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.back HTTP/1.1" 404 288 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.backup HTTP/1.1" 404 290 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:Non  
"GET /LgQ2vQ0j.bak HTTP/1.1" 404 287 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.bas HTTP/1.1" 404 287 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
"GET /LgQ2vQ0j.bas:ShowVolume HTTP/1.1" 404 298 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasi  
"GET /LgQ2vQ0j.bat[dlr HTTP/1.1" 404 291 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:Nor  
"GET /LgQ2vQ0j.BBoardServlet HTTP/1.1" 404 297 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasi  
"GET /LgQ2vQ0j.BIG5 HTTP/1.1" 404 288 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
```

აღნიშნულ „GET“ მოთხოვნებს აზვავს ვებ-სერვერი, ამ შემთხვევაში კი „NIKTO“. სპანიერება განხორციელდა „26.90.23.56“ IP მისამართიდან, შესაბამისად ვფიქრობთ ჩვენს „LOG“-ს, რათა გვაჩვენოს მოთხოვნები მხოლოდ ამ მისამართიდან. გადავად ფიქსირდება სხვა ვებ-სერვერები: WPSCAN და W3AF.

პასუხი მეორე კითხვაზე: NIKTO WPSCAN W3AF

```
"GET /index.php/comments/feed/?mode=phpInfo HTTP/1.1" 200 1639 "-" w3af.org  
"GET /index.php/comments/feed/phpInfo.php HTTP/1.1" 404 10190 "-" w3af.org  
"GET /index.php/comments/feed/phpInfo.php HTTP/1.1" 404 10190 "-" w3af.org  
"GET /index.php/comments/feed/phpInfo.php HTTP/1.1" 404 10190 "-" w3af.org  
"GET /index.php/comments/feed/PHPInfo.php HTTP/1.1" 404 10190 "-" w3af.org  
"GET /index.php/comments/feed/PHPInfo.php HTTP/1.1" 404 10190 "-" w3af.org  
"GET /index.php/comments/feed/PHPInfo.php HTTP/1.1" 404 10190 "-" w3af.org
```

იმის დასადასტურად, თუ როგორ მოიპოვა შემტევმა წვდომა სერვერზე, საჭიროა მოვიძებნოთ წარმატებული შეტევის ვექტორი. „Log“ ფაილის ბოლოს ფიქსირდება მასიური „POST“ მიმართულებები „wp-login.php“-ზე, რომლის შედეგადაც სერვერიდან მან მიიღო 302 პასუხი, ე.ი. Bruteforce შეტევა წარმატებით განხორციელდა და შემტევმა მოიპოვა ვებ-გვერდზე სრული წვდომა:

```
"POST /wp-login.php HTTP/1.1" 200 3128 "http://10.10.10.89/" "WPScan v2.9.1 (http://wpscan.org)"  
"POST /wp-login.php HTTP/1.1" 302 - "http://10.10.10.89/" "WPScan v2.9.1 (http://wpscan.org)"  
"GET /wp-admin/plugins.php?plugin_status=all&paged=1&s= HTTP/1.1" 200 39853 "http://10.10.10.89/wp-  
"POST /wp-login.php HTTP/1.1" 302 - "http://10.10.10.89/wp-login.php?redirect_to=http%3A%2F%2F10.10.10.89%2F" "WPScan v2.9.1 (http://wpscan.org)"
```










ვებ-გვერდზე ადმინისტრატორის პრვილეგიების დაუფლების შემდგომ, სერვერზე წვდომის მოსაპოვებლად შემტევმა გადაწყვიტა აეტივირთა მავნე „php“ ფაილი „vivaldi.php“, რომლის მეშვეობით მას შესაძლებლობა მიეცა სერვერზე დისტანციურად გაეშვა ბრძანებები.

```
/wp-admin/plugins.php?action=activate&plugin=vivaldi%2Fvivaldi.php&wpnonce=  
/wp-admin/plugins.php?activate=true&plugin_status=all&paged=1&s= HTTP/1.1 :  
/wp-content/plugins/vivaldi/vivaldi.php?cmd=ls HTTP/1.1" 200 23 "-" Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (T  
/wp-content/plugins/vivaldi/vivaldi.php?cmd=cat%20/etc/passwd HTTP/1.1" 200 :
```



CYBER-LAB  
TECH

# Teacher's Management:

ჯგუფები +		
ჯგუფი	დამატებული	პარამეტრები
თეოლოგიური უნივერსიტეტი		  
სახელმწიფო უნივერსიტეტი		  
მღიას უნივერსიტეტი		  

CYBER-LAB  
T E C H

სტატისტიკა სტუდენტები ანგარიშის დავა ჯგუფები მათემატიკის კანონები პროფილი გავლა

სახელმწიფო უნივერსიტეტი

სტუდენტები +







სახელი

მოძებნეთ შესაბამისი სახელები

ჯგუფის მიხედვით გაფილტვრა

ჯგუფი დამატება

ჯგუფიდან წაშლა

იდენტიფიკატორი	სახელი	გვარი	სტატუსი	დამატებული	პარამეტრები
00000019	MONDOMEBUL1	MONDOMEBUL1@GRENA.GE	სტუდენტი		 
00000021	MONDOMEBUL2	MONDOMEBUL2@GRENA.GE	სტუდენტი		 
00000022	MONDOMEBUL3	MONDOMEBUL3@GRENA.GE	სტუდენტი		 

CERT.GOV.GE

EaPConnect  
Eastern Partnership Connect

GRENA  
Georgian Research and Emergency Network

# Statistics:

განმეშული პასუხები						
<div>განმეშული პასუხები</div> <div></div>						
იდენტიფიკატორი	სტადენტი	ამონაწი	განმეშული პასუხი	სტატუსი	თარიღი	ნაშლა
1	LASHA	ELF BINARY BOMB: QUESTION 5	^	სტატუსი	2018-11-07 09:50:03	×
2	LASHA	QWERTY	HAX	სტატუსი	2018-10-22 10:42:44	×
3	ADMIN	DES	FSFSFS	არასტატუსი	2018-10-19 12:05:45	×
4	LASHA	XOR MASE	0100	სტატუსი	2018-10-18 16:55:23	×
5	LASHA	XOR CASE	0XFO	სტატუსი	2018-10-18 16:55:09	×

სტატისტიკა				
ამონაწი	ამონსწავლის რაოდენობა	განმეშების რაოდენობა	ამონსწა	განმეშები
AMADEUS				
QUESTION 1	1	22	4%	96%
QUESTION 2	2	9	18%	82%
QUESTION 3	1	7	13%	87%
QUESTION 4	1	1	50%	50%
QUESTION 5	1	1	50%	50%
BACKDOORE				
QUESTION 1	1	5	17%	83%
QUESTION 2	1	3	25%	75%
QUESTION 3	1	1	50%	50%
QUESTION 4	1	1	50%	50%
QUESTION 5	1	1	50%	50%

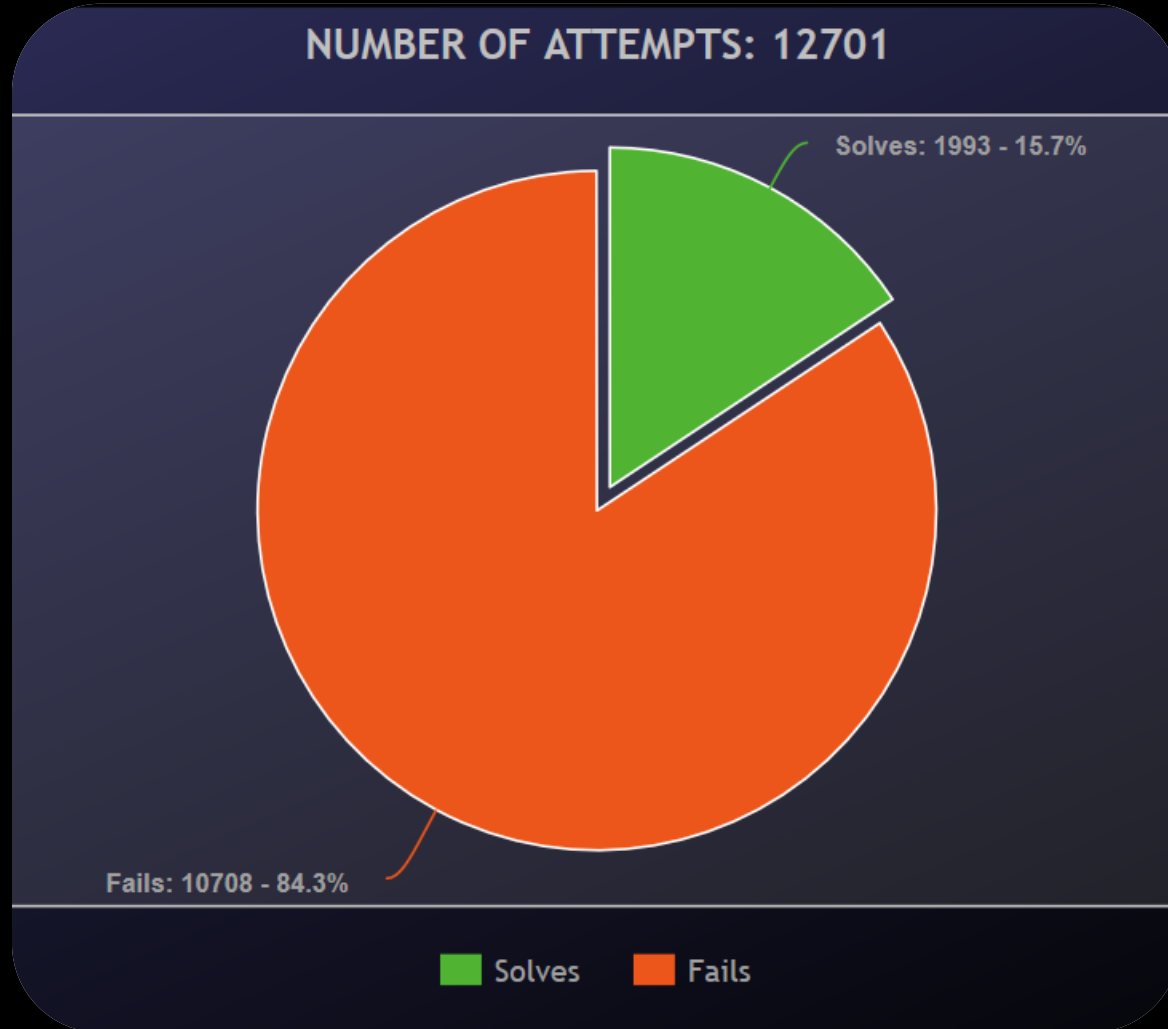
კატეგორია	ამონსწავლის რაოდენობა	განმეშების რაოდენობა	ამონსწა	განმეშები
LOG ANALYSIS	41	71	37%	63%
MALWARE ANALYSIS	14	0	100%	0%
REVERSE ENGINEERING	29	8	78%	22%
PCAP ANALYSIS	43	16	73%	27%
STEGANOGRAPHY	6	0	100%	0%
MIX	8	2	80%	20%
CRYPTOGRAPHY	29	3	91%	9%

ანგარიშის დაფა		
ადგილი	სტადენტი	ანგარიში
1	MONDOMBULI1	4000
2	MONDOMBULI2	70
3	MONDOMBULI3	30



# Statistics:

From the Date of Establishment 26 November 2018.



Number of Registered Students: 194.

Number of Registered Organizations: 14.

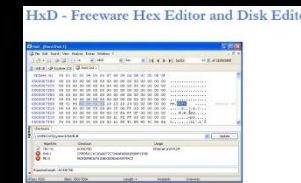
Number of Attempts: 12,701;

Amount of Solves: 1,993;

Amount of Fails: 10,708.



# Recommended Tools and Applications:





# Cyber-Lab.Tech Team Contact Information:

E-mail: [contact@cyber-lab.tech](mailto:contact@cyber-lab.tech)

Tel: +995 32 291 51 40

Address: 50 University Street  
0186 Tbilisi, Georgia



E-mail: [contact@cyber-lab.tech](mailto:contact@cyber-lab.tech)

Tel: +995 32 225 05 90

Address: 10 Chovelidze Street  
0108 Tbilisi, Georgia



[www.facebook.com/Cyber-Lab.Tech](https://www.facebook.com/Cyber-Lab.Tech)



Thank You For Your Attention!