Rise of the Cyber Security Squad!

“At first, I would like to thank all of my friends who fully made the web & network paths, um a reverse guy, my knowledge in pentesting/red-teaming is very limited. So, you can consider this roadmap is for folks who are interested in learning reverse engineering and malware analysis. Please note that this is my own vision which comes from an ACM ICPC problem solving background. As a consequence, I believe the most in learning the slow hard-way. Also, I’ve added a list of talented people in the community to learn from. Those are very nice people to have as friends.
If you have any thoughts or comments or want to edit or even to add something = feel free to contact me.“

Nidal Fikri in June 24th, 2018
Founder of the Cyber Security Circle at CAT Reloaded Student Branch - 2018
Former President at ICPC Mansoura Student Branch - 2020
Cyber Security Intern (CPITS) at Trend Micro - 2021
Malware Analyst at Hatching Triage - 2021
Malware Analyst at Recorded Future - 2022

(:) Acknowledgments:

First, I want to thank all the people who helped to build, to correct, and to maintain this roadmap. It’s not a single man’s effort at all. All this couldn’t have been real without them.

- Abdallah El Shinbari
- Mohamed K. Fathy
- Omar Shehata
- Mohamed Aboshady

(:) Non-Technical FAQ:

How can I use this document ?

First, read the FAQ (Frequently asked questions) sections. There are certain levels developed to take you gradually from quite 0 knowledge into a reasonable level in cyber security. If you are a total beginner, you can just read the entry level contents, and don't bother yourself with the intermediate and what it comes after, for now.

If you are more than a beginner, feel free to navigate through the document.

Also in the "Mentors" section, you can find a list of talented Cyber Security people to get in touch with.

What does the " (:) " and " (*) " symbols mean ?

This document is under regular development and updates, But you can consider any headline with the prefix (*) is somehow nearly completed, or is not under any considerations to be updated in the near future. While any headline beginning with the (:) prefix is the absolute opposite = it's under monthly updating and enhancing to make the best use of it.

How to directly contact the author or for more deep chatting?

Gladly um ready to help or contribute or even to take part in a project!

https://twitter.com/cyber_anubis

(:) Technical FAQ:

So what is "Cyber Security"?
It is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

Can Cyber Security attacks do harm to my company, my country, or even me?
HELL YES!, watch this video introducing "Israel" as one of the top 5 powerful cyber armies!
Click for Video
Scary AF ha?!

How did our world end so vulnerable to these cyber crimes?
Here is the answer in this video: https://www.youtube.com/watch?v=sdpxddDzXfE

Now, I do NOT want to be a bad guy , why do I need to be a cyber security criminal?
Well, I can change your mind ,hackers are NOT always bad! watch this :
https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

Do I need to have a lot of knowledge to start my journey into becoming a hacker?
This is a tricky question, of course, the more you know about computers the more comfortable you will become while learning anything especially cyber security. But for our newbies, I've added an entry level to computer science in general, to make you ready enough.

I need the best resources to go from 0 to hero in the minimum time possible, can you give me your secret books and courses?
Yeah of course, here you go: https://youtu.be/2TofunAI6fU

How to study Cyber Security?
This very important video tells you the most common three ways: https://youtu.be/vI79qT4IcfA

Cyber security is a very dynamic and sophisticated field , and requires an obsessed geek to handle all that moving flow and that much knowledge .
A cyber student's very normal life is to study or I should say " **master** " more than one technology and have to study them from many aspects , mainly the developer aspect vs the cracker aspect.
Cyber field and jobs are countless but we can - in the beginner level - sum up the filed into two main paths :

1- Web App Pentesting. 2- Reverse Engineering . 3- Network Pentesting.

It's assumed that the circle member doesn't have any computer science background. A circle member will study the basic info and technical skills in the entry level. A member can take the famous CS50 course [Link] before the entry level if he/she wants some warming up. Entry level contents can be skipped if the member is aware of them.
In intermediate level , a circle member will dig deep in his path to learn its hard bases in order to build upon it an amazing outstanding career , he or she will complete more than 3 medium sized books as well as video courses and articles in that level only .
Then it's time for the advanced guys ,I really don't consider myself - Nidal - one of them yet :"D , but um far steps (months) ahead of my circle members and I think when the time is right , I will be able - with my outer connections - to set up a well weaved plan, even when a cyber geek reaching this level can almost guide himself with a little supervision .

My vision in learning Cyber Security is about 4 main steps :
1st- Learn the technology you want to secure.
2nd- Do a lot of analysis during learning from 2 aspects (Cracker vs developer).
3rd- Learn the most common exploits/attacks , understand them and apply them.
4th- Make your own exploits and tools!
Some people just ignore the 1st and the 2nd steps mentioned previously, I can't say they are wrong, yeah their way can make you a good hacker, but in my opinion , my way is more efficient way to learn anything in general, the slow gradual progress , step by step , way. It may take a longer time, but I am sure it is really worth it.

This document is meant for all Cyber Security enthusiasts including the most addresed segment intended for : the new beginners. But more specially this document is for my local community in Mansoura city - Egypt. **Feel free to use it anytime, anywhere, in any context.**

My vision here in CAT Reloaded Mansoura is to make the first cyber security squad outside the capital. I've managed more than a student community before in well known communities.
Um a former ACM ICPC Mansoura president + former CyberTalents academic ambassador in Mansoura University .
I've gained trust and experience and I think I can dream one more time to be the reloaded founder of the CAT CyberSecurity circle .

(*) ENTRY LEVEL:

1- Description : "Introduction & elementary **4 or 5 weeks** level which every member must acquire its knowledge,it consists of **basic programming ,problem solving techniques as well as networking basics + intro to OS (linux + Win) + general knowledge about the cybersecurity field**".

2- Entry level contents are common for both paths of the circle .

3- The main objectives :

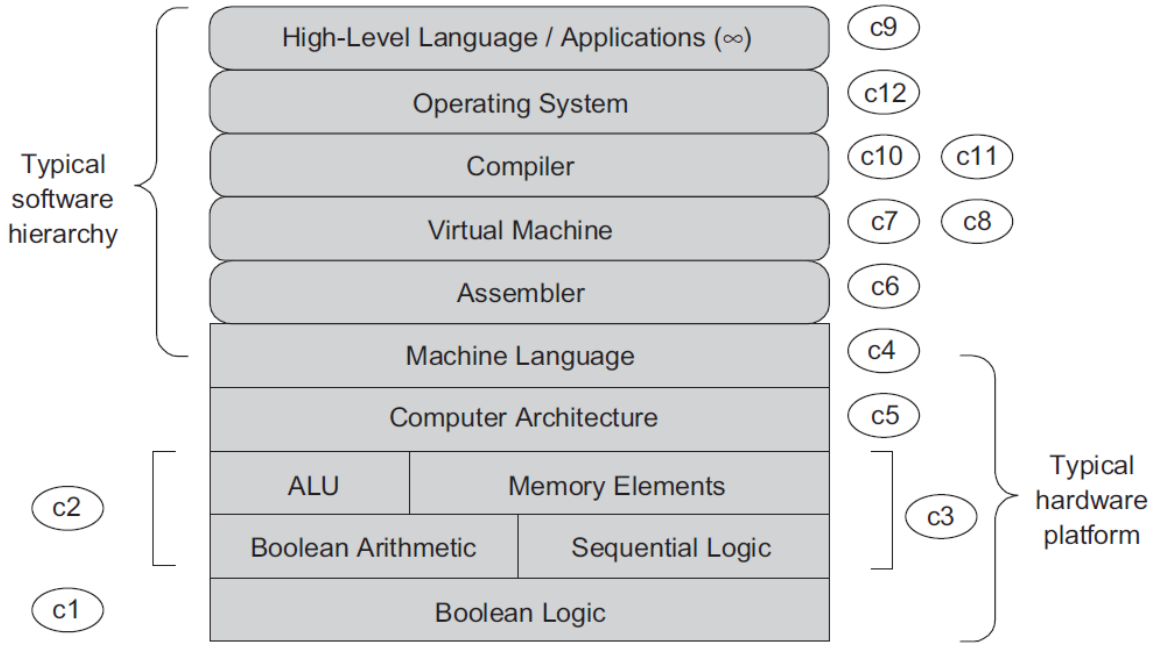
- Create an open , obsessed and curious mind about cyber security as well as to gain basic and enough information about the main two paths of the circle , **this will be achieved through many articles and talks that discuss the very shell of the cyber security field , famous attacks & defenses and real-life scenarios .**
- Developing the English and searching skills which are a must for every hacker ,almost every study material is in English ,**this will be achieved by the tasks meant for the articles and talks .**
  A member's main task after watching a talk or reading an article is to make his own summary written in his words .
- Gaining the basic technical skills which are common to both main paths of the circle ; programming + OS + networks .
  Making the entry level like a **crossroads or a fork to decide afterwards which path will be selected .**
  The contents are very easy and basic **but with many quizzes and tasks** which describe this entry level as **the warming up,endurance ,level which will measure the ability for every member to self-learn and his will to be a tech geek .**
- At the end of this level , a member can decide if he joined the right circle for him or not .
- Please note that the links and courses below are my recommended but may not be the best for everyone , so if you struggle during one of these , you should seek something else.

4- Technical roadmap:

- (1st week) I've decided that **Python** will be the intro to programming for the newcomers **+ Basic OOP concepts about using and making classes.**
  The members will do a lot of **mini projects** in the 2 selected courses below :
  https://goo.gl/4muhEP
  https://realpython.com/python3-object-oriented-programming/
  The members will solve the 1st most solved 30 ACM style algorithmic problems - codeforces - platform which will strengthen their implementation and coding power as well as thinking techniques.
- (2nd week) I've also decided that **networking** is a basic science for every hacker and understanding its concepts is a must to make a reliable mind and to understand the most common exploits nowadays .
  The members will study the famous N+ course. I believe that this content is enough for gaining the concepts of computer networking: shorturl.at/aBTV4
- (3rd week) A member will begin his first interaction with OS linux for the first time , learning basic command line and an intro to shell scripting .
  There are some excellent books for beginning with linux :
  CompTIA linux + : goo.gl/R7jQAq for more in depth learning
  * Recommended * **Linux basics for hackers** : goo.gl/1NWT5N
  Read as much as you can, use the terminal, know the internals, have fun!
  But any YouTube course will be fine btw.
- (4th week) *optional week* Very important for a cyber security geek, especially for every reverse engineer in the future, is to master the concepts of Operating systems and to know how it interacts with software.
  Operating system concepts by Abraham Silberschatz : goo.gl/yuJhoi
  It is my recommended book to begin your journey.
  But at entry level we are only meant to study the 1st chapter (the introduction) and you are free to dig as deep as you want!
- If the OS content got you excited, you should consider starting to learn reverse engineering!
- **To wrap up the entry level month** ; 1 week for Python + 1 week for Networking + 1 week for Linux + 1 optional week for OS book - 1st chapter + 1 extra week time = 4/5 weeks entry level .
- **Every 10-15 days**, once ,will be an offline **gathering session** for all circle members to discuss and receive feedback about the moving flow , as well as having some fun :D

Bonus topic:

You can do the "**Nand to Tetris**" side-project where you will build an actual 16-bit general purpose computer from scratch using only NAND logic gates. You will get much more understanding of low level stuff & how everything works together for a greater purpose!



Topics covered in the project:

1. Building ALU & RAM units = merge into CPU.
2. Design Assembly language from the bare hardware.
3. Build an Assembler.
4. Build a two-tier compiler with a stack-based virtual machine.
5. Develop simple OS functionalities.

For more info: https://github.com/NidalFikri/The-HACK-General-Purpose-Computer
Project course:

1. Part 1: https://www.coursera.org/learn/build-a-computer
2. Part 2: https://www.coursera.org/learn/nand2tetris2

(:) INTERMEDIATE LEVEL:

1- Description : " leveling up with the **remaining** strong passionate members, in 2 stages ,starting the very looong journey , **by selecting their 1st specialization** ; web or reversing , laying the strong underground and infrastructure to build upon the outstanding career ."

2- Intermediate level contents are **not** common for both paths but there are some courses and books which are needed for a novice hacker , these will be studied in both paths .

3- Intermediate level is consisting of two levels or stages to break the enormous amount of knowledge to be acquired by the members

4- The main goal to the intermediate level is to build the basic & essential knowledge in any specification a member chooses. **He or she first learns the technology from the developer's perspective then proceeds to take the other viewpoint from the cracker's perspective.** .

5- The main objectives :

- Bringing more practical security topics into the mind and it's time for **approaching black hat methodologies** .
- Studying the main poles which underline their path , mostly ; **low level programming , OS Internals, Web dev. , OWASP famous web holes , reverse engineering techniques and intro to exploitations , intro to Cracking softwares , Cryptography as well as malware analysis introduction** .
- Introduction to the world of **CTF** games (Capture the flag) which are like ACM style problems but it discusses security bugs and faults , a little bit far from algorithmic programming problems .
- Creating the **1st library** for a circle member who will study more than 3 medium sized books and gain the habit of self learning .
- Please note that the links and courses below are my recommended but may be not the best for everyone , so if you struggle during one of these , you should seek something else.

6- **This is the longest and most important level in the circle's technical road map** , **it may take the whole year but it is really worth it** , a circle member with this knowledge will be fully ready to have internships and begin the professional advanced study phase.

7- **It's recommended to study the materials in the order mentioned below .**

8- The technical roadmap :

Below is the technical roadmap. Containing courses, books and labs.

● Reverse Engineering Path:

I. **“ Practical Malware Analysis “ book**: goo.gl/dQ9T5h

This is the best book to start your journey with Malware Analysis . one of the best books I’ve read ! It has many useful topics to any Reverse Engineer like : Static and Dynamic analysis , Anti reversing techniques .

It shows the importance of Windows API & its heavy interaction with software .

It has the most complete labs and exercises I’ve ever seen ! with excellent solutions and hints for more than half the book itself!

If you want to know more about binary headers = go and read the 1st three chapters from the next book (Practical Binary Analysis).

If you need to know more about Win Internals, then study the Pluralsight course.

If you finish the whole book, while being extremely interested, I am sure that you will have an awesome career in malware analysis!

II. **“OALABS” YouTube Channel: youtube.com/c/OALabs**

The purpose of this step is get your hands on **real-world** malwares & how malware analysts defeat them. Here you will learn & RE more advanced malwares which are currently in the wild. Watch & RE the following:

- IcedID malware: shorturl.at/bfLT0 then shorturl.at/GJSYZ
- IRC botnet: shorturl.at/jEIN0 then shorturl.at/ci025
- Warzone RAT: shorturl.at/hjwA1 then shorturl.at/ryL79
- PE entry points: shorturl.at/dqY01
- Defeating API Hashing using HashDB: shorturl.at/akqrF
- Guide for unpacking & unmapping: shorturl.at/ilmS2
- Malware Triage tips: shorturl.at/adhw2
- Unknown Malware Identification: shorturl.at/hSVY3
- Plugins for IDA Pro: shorturl.at/xCXY6
- IDA Pro Scripting: shorturl.at/bFshorturl.at/bFKNSKNS

Watch as many videos as you can from this amazing channel.If you spend X time learning, at least spend 2X time practicing!

III. **Create Your Own Technical Blog**

Start analyzing real-world malwares and post your analysis in your own blog. This is a very important step & will give you work opportunities as well as internships. You can create your blog using free GitHub Pages. How to create your blog?

- Read the first 4 articles here: shorturl.at/hkPWZ
- Read this: shorturl.at/dhmpS

At the end, you should end up with a personal blog like these:

- https://cyber-anubis.github.io/aboutme/
- https://n1ght-w0lf.github.io/

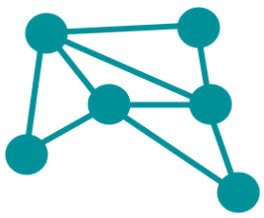
IV. **“ Practical Binary Analysis “ Book:** http://bit.ly/2FVrGlq
It covers the fundamentals of reversing concepts especially in the Linux environment and the famous ELF binaries in outstanding detail and simplicity + the virtual machine with the book which provides hands-on exercises.The reader will begin to create his own tools!. If you are not interested in reversing ELF for now , just read the first 3 chapters. They will feed you with the fundamentals of binary files structures which you may feel lost in especially in the next book.(skipping after the 1st three chapters is recommended for noobs)

V. **“ Reversing : Secrets of Reverse Engineering “ book**: goo.gl/xuYtx7
This book is introducing the first impact with windows file formats and windows internals which will be one of the cores of RE as well as introduction to software Cracking and bypassing protections . This book is one of the hardest books to understand so feel free to skip a lot.
It’s recommended to finish most of the book ; it covers great jumping offs and widely represents the reverse engineering fields. If you face hard times with assembly, I highly recommend that u read the topics u lack knowledge in with **The Art of Assembly Language** book or **RE4B** book: http://bit.ly/2JjchNV (It’s recommended to ignore ARM & MIPS in your first read)
If you already know the contents of certain chapters (especially the 1st four chapters) from previous books = skip them.

VI. **“ Practical Reverse Engineering“ book:** https://bit.ly/3jJ4kS3
The book represents something that we wish we had when we started learning about reverse engineering more years ago. The book covers x86, x64, and ARM (the first book to cover all three); Windows kernel-mode code rootkits and drivers; virtual machine protection techniques; and much more. Best of all, it offers a systematic approach to the material, with plenty of hands-on exercises and real-world examples.
It’s recommended -yet maybe hard- to finish the whole book

VII. **Through roaming between these books** , a member may inspect certain chapters from other **books** in order to cover the lacking prerequisites
RE4B - Operating Systems concepts: http://bit.ly/2xD1nM8 **- The IDA Pro book:** https://bit.ly/3lq8deX - **The Art of Assembly:** https://bit.ly/2SQsRJb - **The C programming Language:** https://bit.ly/30OOk9l - **Windows Internals pluralsight video course:** https://bit.ly/WindowsInternals - MCSA (Identity, Active Directory, ...stc): TODO
These books are the fundamentals of RE. You will spend a lot of time here.

I've meant to use the verb " roam " intentionally



cuz the intermediate level member is not required to finish the books one by one in the same order.
He or she will finish some chapters from the 1st book then other chapters in another book and may return to the starting point ...etc.

Like the previous cyclic graph- I believe that learning is cyclic but not linear- you read 10 chapters from book A then you move to book B then book C for 2 chapters , you may go back to book A or another book, I think you got the idea :)

If you get stuck while studying the previous resources = **skip , skip a lot ,** some of these books are old though , get the most important things = techniques + big pictures + concepts. Then apply them yourself!
Don't get stuck on a single page for a long time,skip, skip a lot, life is too short :)
And always remember to consult your mentor when you need help. This will save you months!

- **Web App Pentesting Path:**

  As I've mentioned, I don't have any significant knowledge about web pentesting . So, pls refer to the document below:
  Link: https://bit.ly/3iliQbt

- **Network Pentesting Path:**

  As I've mentioned, I don't have any significant knowledge about Network pentesting . So, pls refer to the document below:
  Link: https://bit.ly/2FdnnF5

(:) ADVANCED LEVEL:

Under construction ...

(:) Mentors:

Below are listed - in my own opinion - some of the most talented people in the CySec community in EG -whom only I've personally dealt with-, feel free to contact them. Nice, kind, very friendly & helpful friends to have/question about technical stuff.

PS no.1 : I might have forgotten a lot of other talents to mention below , sorry for that! I will update the list regularly.

PS no.2 : The ranking below has no value at all :)

Last updated: Jan, 2022

1. Mohamed Aboshady
2. Mohamed Fadel
3. Mohamed K. Fathy
4. Kareem Selim
5. Mohamed Soltan
6. Hady Azzam
7. Karim Shoair
8. Youssef A. Mohamed
9. Mohamed Eldeep
10. Mohammed Essam Mousa
11. Mahmoud Adel
12. Ahmed Sultan
13. Mohamed Osama
14. Abd El Aziz Saad
15. Amr Thabet
16. Muhammad Gamal
17. Youssef Mohammed Hassan
18. Ahmed Radwan
19. Amr Fathi
20. Magdy Moustafa
21. Abdallah Elshinbary
22. Mohamed A-Abd El Monim
23. Hassan Mostafa
24. Menna Essa
25. Ahmad Elmayyah
26. Mustafa Mahmoud
27. Ahmad Bahaa
28. Yasser Ali
29. Yasser Elsnbary
30. Alya gomaa
31. Asem eleraky
32. Amr Mosa
33. Abdelrahman Khater
34. Mohammad Hassan
35. Mohammad Labeeb
36. Gameel Ali
37. Youssef Zidan
38. Mahmoud Gamal
39. 3la2kb
40. Ahmed Hesham
41. Sam Muhamad
42. Eslam Akl
43. CSGAEE
44. Mohamed Mido
45. Mo Salah
46. Heidi Mohamed
47. Islam Mostafa Hosni
48. Mohamed Elawadly

49. Heba Farhat
50. Khaled Ibn Al-Walid
51.
52.
53.
54.
55.
56.
57.
58.
59.
60.
61.
62.
63.
64.
65.
66.
67.
68.
69.