Introduction to cybersecurity

Careers, Paths and Domains.

BY: RAMI AHMED @OWASPsana'a

Agenda

- Why Cyber Security matters ?
- Advantages & Disadvantages of getting a job in Cyber Security.
- What it actually takes to be part of the Cyber Security Community ?
- Highly in-demand Cyber Security Jobs.
- Industry standard Certifications.
- Final Notes
- Useful Resources & References to get you up and running.

Why Cyber Security matters ?

CYBERATTACKS AFFECT ALL PEOPLE

THE FAST CHANGES IN TECHNOLOGY WILL CAUSE A BOOM IN CYBERATTACKS

DAMAGE TO BUSINESSES AND LOSS OF JOBS

CYBERSECURITY THREATS FACED BY INDIVIDUALS

CYBER CONCERNS MAY RESULT IN INCREASED REGULATIONS AND LEGISLATION

Pros & Cons of getting a job in Cyber Security.

Pros:

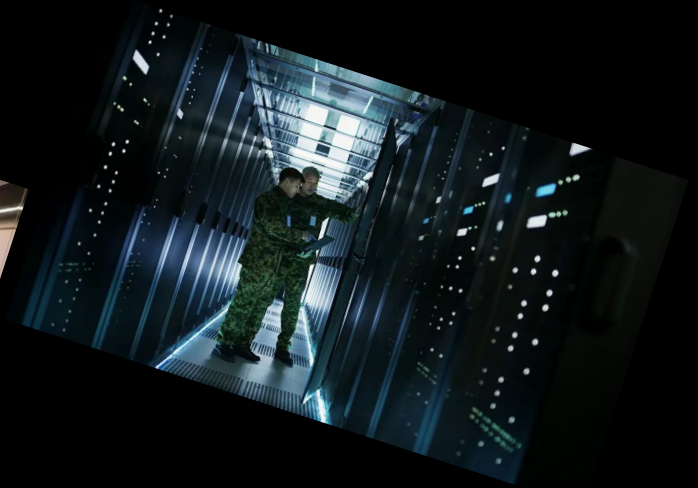
- Good Salaries !!! :)
- Cyber Jobs are everywhere.
- Ability to advance.
- Opportunity to be self-employed. (ex.Crowdsourced security)
- Opportunity to learn new things.

Cons

- On-call and Demanding hours.
- Some tasks are repetitive and boring.
- Job pressure (lotsssssssssss of it)
- The learning treadmill never stops.

What it actually takes to be part of the Cyber Security Community ?

Highly in-demand Cyber Security Jobs.



Offensive Approach

PENETRATION TESTER

What is it, and what would you do on a daily basis?

Background:

- *Programing / Scripting*
- *Networking*
- *System administration*
- *Extensive knowledge of OWASP top 10 for web and mobile*

Credits goes to @Ebrahim Hegazy

SECURITY CONSULTANT (RED TEAMING)

What is it, and what would you do on a daily basis?

Background:

- Good knowledge of system administration, specially in Windows environments.
- Networking
- Programing, or scripting (Python / Bash)
- Social engineering
- OWASP top 10
- Solid knowledge of Active directory, and its common attacks
- Solid knowledge of command-and-control (C2/C&C) concepts, and tools.

Credits goes to @Ebrahim Hegazy

SECURITY ANALYST
SECURITY OPERATIONS CENTER (SOC)

What is it, and what would you do on a daily basis?

Background:

- System administration
- Networking
- Scripting (Python / Bash)
- Basic knowledge of Incident handling process
- Basic malware analysis knowledge

Credits goes to @Ebrahim Hegazy

SECURITY ANALYST
TRIAGE TEAM MEMBER

What is it, and what would you do on a daily basis?

Background:

- Programing / Scripting
- OWASP top 10 for web & mobile
- Bug hunting
- Communication skills

Credits goes to @Ebrahim Hegazy

SECURITY CONSULTANT (THREATINTEL)

What is it, and what would you do on a daily basis?

Background:

- Extensive recon & information gathering knowledge
- Access to, and contentious monitoring of hacking forums
- Scripting knowledge (i.e. Python)

Credits goes to @Ebrahim Hegazy

SECURITY CONSULTANT (IDENTITY AND ACCESS MANAGEMENT))

What is it, and what would you do on a daily basis?

Background:

- System administration (Windows, and Linux)
- Good knowledge of Active directory, and Database management
- Networking Courses & Certifications:
- MCSE (Windows), RHCE (Linux)
- CISSP (IAM chapter)

Credits goes to @Ebrahim Hegazy

SECURITY ENGINEER (APPLICATIONS)

What is it, and what would you do on a daily basis?

Background:

- Experience in applications development
- Deep technical understanding of applications vulnerabilities (i.e. OWASP Top 10)
- Experience in code reviews, vulnerability detection, and root cause analysis
- Pentesting / Bug hunting

Credits goes to @Ebrahim Hegazy

SECURITY ENGINEER (SYSTEMS)

What is it, and what would you do on a daily basis?

Background:

- System administration
- Extensive Networking, and network security knowledge
- Scripting
- Good knowledge of corporate security concepts, and tools (i.e. Firewall, IDS/IPS, DLP, VPN)
- Knowledge of incident response, and malware behavior analysis

Credits goes to @Ebrahim Hegazy

SECURITY ENGINEER (ICS)

What is it, and what would you do on a daily basis?

Background:

- System administration (Windows)
- Extensive IT & OT Network protocols experience
- Good knowledge of corporate security concepts, and tools (i.e. Firewall, IDS/IPS, DLP, VPN, Data Dayood)
- Good understanding of OT environment factors (safety, hazards, policies, how machines works)
- Knowledge of PLC's, DCS, and SCADA systems

Credits goes to @Ebrahim Hegazy

Defensive Approach

INCIDENT HANDLER

What is it, and what would you do on a daily basis?

Background:

- System administration (Windows), and Linux
- Networking
- Knowledge of various logs (i.e. network logs, webservers logs, and system logs)
- Knowledge of Digital forensics, and malware behavior analysis
- Knowledge of red teams techniques, tactics, and procedures (TTP)

Credits goes to @Ebrahim Hegazy

MALWARE ANALYST

What is it, and what would you do on a daily basis?

Background:

- Good knowledge of low level programing languages (i.e. C, C++, and Assembly)
- Hands on knowledge of debuggers (i.e. IDA, OllyDbg)
- Good knowledge of binary reverse engineering
- Good understanding of windows internals

Credits goes to @Ebrahim Hegazy

CHIEF INFORMATION SECURITY OFFICER (CISO)

What is it, and what would you do on a daily basis?

Background:

- System administration
- Networking experience
- Basic knowledge of all infosec jobs

Credits goes to @Ebrahim Hegazy

Industry standard Certifications.

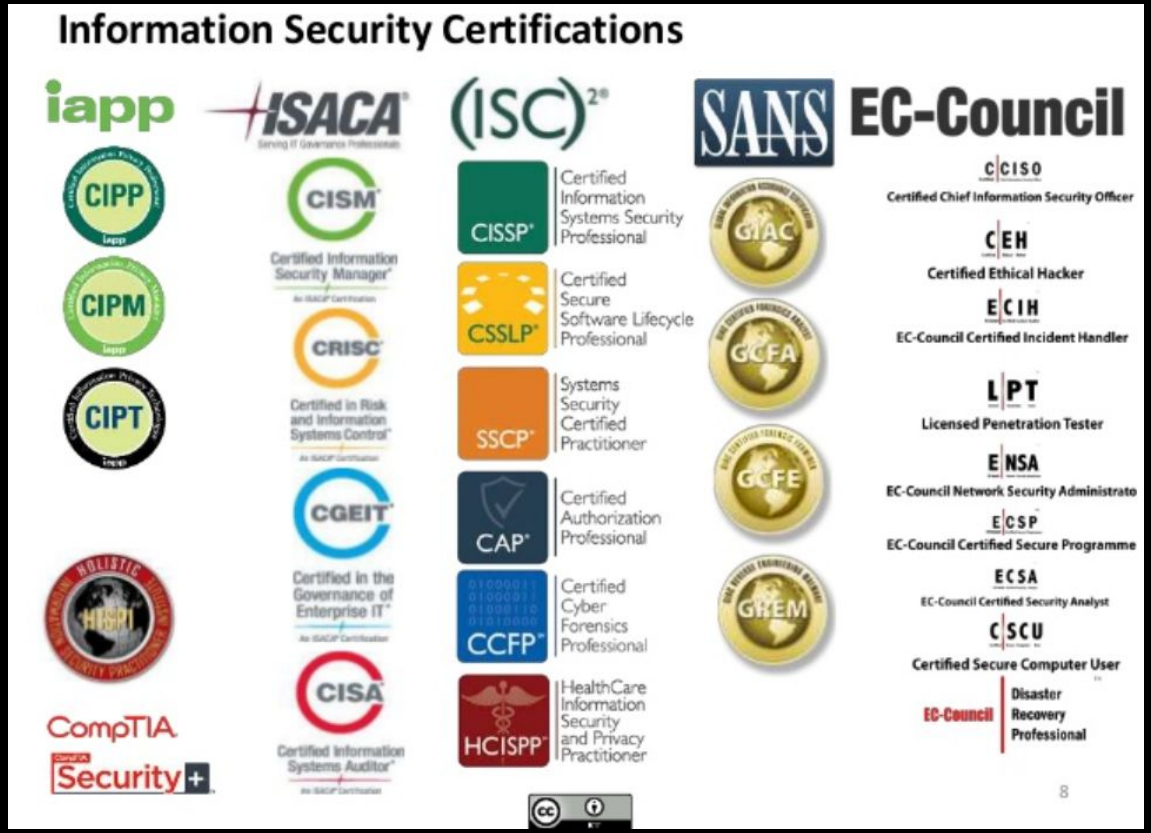
OFFENSIVE security
OSCP

GIAC SECURITY LEADERSHIP CERTIFICATION
GSLC

LEVEL 400 ADVANCED
C)IHE
INCIDENT HANDLING
mile2

CompTIA
PenTest+

Well-known Certifications in Cyber Security Nowadays



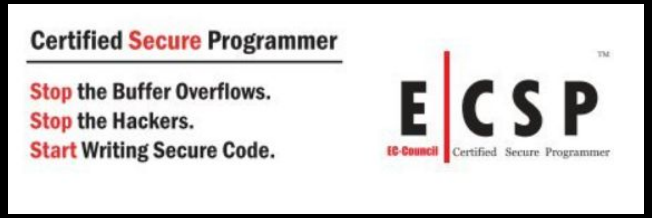
- https://www.comptia.org/content/it-careers-path-roadmap/cybersecurity-specialist


E-COMMERCE CONSULTANTS INTERNATIONAL COUNCIL
EC-Council

EC-Council


EC-Council
ECSA
TRAINED


EC-Council
CSCU
CERTIFIED


Certified Secure Programmer
Stop the Buffer Overflows.
Stop the Hackers.
Start Writing Secure Code.
ECSP
EC-Council Certified Secure Programmer


ECSA
EC-Council Certified Security Analyst


ENSA
EC-Council Network Security Administrator

Offensive Approach

- Offensive Security Certified Professional
- Comptia pentest+

- GIAC Certified Penetration Tester (GPEN)
- GIAC Web Application Penetration Tester (GWAPT)

- IACRB Certified Penetration Tester(CPT)
- IACRB Certified Expert Penetration Tester (CEPT)
- IACRB Certified Red Team Operations Professional (CRTOP
- Licensed Penetration Tester (LPT)

Defensive Approach

Operating System & Device In-Depth Certifications:

- GIAC Battlefield Forensics and Acquisition (GBFA)
- IAC Certified Forensic Examiner (GCFE)
- GIAC Advanced Smartphone Forensics (GASF)

Incident Response & Threat Hunting Certifications:

- GIAC Network Forensic Analyst (GNFA)
- GIAC Cyber Threat Intelligence (GCTI)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Forensic Analyst (GCFA)

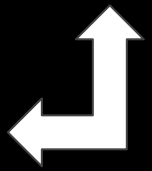
Final Notes

- You always have to give back to the community.
- Don't try to be a jack of all trades, cuz you won't !!!
- Focus only on one area and be the best in what you do.
- If you don't have a twitter account, go now and create one !!!
- Always keep yourself up-to -date.
- You Won't stop learning in this field.
- Read, Read, and Read.

Useful Resources & References to get you up and running.

@Zigoo0
@PyroTek3
@f_aswad
@NahamSec
@TomNomNom
@stokfredrik
@sawaba
@ashk4n
@BillBrenner70
@BrianHonan
@briankrebs
@schneierblog
@WeldPond
@craiu

Information Security Influencers You Should Be Following



Very Useful Online Courses and Youtube content

- https://www.cybrary.it/
- https://pentesterlab.com/
- https://www.pentesteracademy.com/
- https://www.youtube.com/results?search_query=ebrahim+hegazy+
- https://www.youtube.com/results?search_query=nahamsec
- https://www.youtube.com/channel/UCQN2DsjnYH60SFBIA6IkNwg
- https://www.youtube.com/channel/UCvgMmTPBM7xRyxU07-cBpbg
- https://www.youtube.com/user/faswadi

Thanks to

Every single Individual that contribute to the Cyber security Community in order to really make an impact and influence people to get involved in this field.