

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.11, NO. 11

OPEN

HOW TO BECOME A HACKER

**WHAT IS THE MOST IMPORTANT SKILL
TO HAVE AS A HACKER?**

**WHAT'S THE BEST OS
FOR HACKERS?**

**IS CEH AN IMPORTANT PART
IN HACKING CAREER?**

AND MORE...

HAKING

TEAM

Editor-in-Chief

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@haking.com

Marta Strzelec
marta.strzelec@eforensicsmag.com

Marta Ziemianowicz
marta.ziemianowicz@eforensicamag.com

Senior Consultant/Publisher:

Paweł Marciniak

CEO:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP

Marta Sienicka
sienicka.marta@haking.com

Cover Design

Hiep Nguyen Duc

Publisher

Haking Media Sp. z o.o.

02-676 Warszawa

ul. Postępu 17D

Phone: 1 917 338 3631

www.haking.org

All trademarks, trade names, or logos mentioned or used are the property of their respective owners.

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

WORD FROM THE TEAM

Dear readers,

Due to popular demand we decided to prepare a special issue dedicated to those of you that seek an answer to the ultimate question: *“How to become a hacker?”*.

When you refer that question to Google you get an astonishing number of 360,000 results, each promising to make you a cybersecurity expert. Among those are such beauties as “How To Become a Hacker - EPIC HOW TO“, “How to Become a Hacker: 12 Steps (with Pictures)”, and “How To Become A Hacker In 15 Minutes -- Or In 140 Characters Or Less“. The first is a video, the second’s a WikiHow article, and the third is a Dark Reading post about a cybersecurity awareness campaign from 2010. We thought about it long and hard, and decided to take another route to give you answers - plural, because there is no single correct one.

We invited 13 specialists from cyber security and hacking fields to join this project. They answered more than 20 questions about hacking, chosen by us from the dozens we get every day. They presented their opinions and experience. They made lists of their favorite online communities and resources.

While reading this issue you will learn what is the best tool for hackers. Is Kali Linux truly the best OS for your hacking career? What about programming? Is it truly that important to have this skill while becoming a hacker? All of that and more, from 13 different points of view, can be found in this issue.

Happy Holidays!

Haking Magazine’s

Editorial Team

TABLE OF CONTENTS

LUIS BORRALHO

Security Administrator at A2IT

7

ADITYA BALAPURE

Senior Application Security Engineer with Grubhub

20

ANDREA SANTESE

Penetration Tester

30

ANTHONY CALDWELL

Cyber Security Analyst

37

CORY MILLER

Principal Vulnerability Detection Analyst

43

KHALED SAKR

Information Security Engineer at Security Meter

55

RAJ CHANDEL

Director of Ignite Technologies and the founder of Hackingarticles.in

69

REX AANTONNY

Founder and Chief Executive Officer at Rex Cyber Solutions

82

TOM MADSEN

IT Specialist at United Nations

88

MIRIAM WIESNER

Premier Field Engineer for Security

98

SHANE RUDY

Senior Security Consultant

111

SULEMAN MALIK

Cyber Security Analyst

128

LOUAY SALEH

Information Security Manager

136

LUIS BORRALHO

SECURITY ADMINISTRATOR AT A2IT

I'm Luis Borralho, I am 39 years old, and I'm from Portugal. I've traveled to Finland, Estonia, Spain, and United States (California and Florida). I've been in the IT business for quite some time, about 16 years. For the past six years, I've been working on information security, having a role as a Security Administrator, Security Researcher, Security Enthusiast, mainly working with Unix/Linux systems and any open source stuff that is good for good for making my job easier, on our government and other state security departments. I've been managing, firewalls, intrusion prevention systems, intrusion detection systems, web application firewalls, implementing monitoring systems, like Nagios, Check_MK, and/or Cacti, trying to always find the best way to prevent attacks, implementing security operations and system centralized security management systems. I've done some penetration testing and ethical hacking in the past for the same government and state departments. I create scripts to automate daily tasks and graphic scripts to help make other team's jobs easier, devops kind of stuff, too. Academically, I'm no engineer nor do I have a PhD, I just graduated from high school and started my continued study on IT, doing hardware courses, networking architecture courses, security courses, norm courses (ISO 20000 and ISO270001), improving my knowledge on programming and scripting languages, like C, C++,

Python, Perl, Bash scripting, PowerShell, etc. I improved my knowledge on incident response teams, and the knowledge of security incident management. I won't write about all my knowledge or it would take me too much time and you'd fall asleep reading. :) My hobbies are divided between new hardware stuff, open source applications for security, monitoring and management, playing guitar, bass and drums, playing with the kids, cinema, reading good books. I maintain my domain opensecurity.eu and my redhat openshift machines, maintain my github for the community where I have my latest scripts (mainly in Python and Bash scripting).



WHY DID YOU DECIDE TO BECOME A HACKER?

always wanted to know how to hack, to know how to listen on communications between computers, know how to control my communications, to be able to know well my platform and create my own programs and scripts to do what I need. And use that knowledge become a security administrator and expert.

IF I WANTED TO BECOME A HACKER WHERE SHOULD I START?

First of all, from my point of view, you should start to know how a computer works and how communications between computers work. So the guidelines for understanding how a computer works, you'll need to be able to:

- ➔ Understand how a microprocessor works, learn its instructions and how to pass instructions to it so it can execute them for you: Need to study Binary, Hexadecimal, Assembly for microprocessors;
- ➔ Understand how RAM (Random Access Memory) works, what is the stack, what is the buffer, what is the heap, learn C so you can understand how you can put memory into RAM and take it out, and how to access that piece of data while in memory;
- ➔ Learn how to program computer languages, best language to start with is C, in spite of being a bit complex, if you learn its logic, it becomes real easy;
- ➔ Learn what the kernel is, how it communicates with your computer hardware, how it controls your communications, how drivers work with the kernel;
- ➔ Learn what an operating system is and how it works, I consider that Linux Distros are the best for you to start, because you have lots of documentation on it and learn to customize your kernel and compile it;
- ➔ Learn how TCP/IP works, how protocols work (HTTP, FTP, HTTPS, etc.), the ports used for communication;
- ➔ Learn the each layer of the OSI model so you can understand how network and applications work together.

Sources:

- <https://www.quora.com/How-does-a-computer-chip-work>
- <https://books.google.com/books?id=Q1zSIarI8xoC&pg=PA66>
- <http://www.vectorsite.net/tsfloat.html>
- [https://en.wikipedia.org/wiki/Kernel_\(operating_system\)](https://en.wikipedia.org/wiki/Kernel_(operating_system))
- <http://www.tuxradar.com/content/how-linux-kernel-works>
- <http://www.studytonight.com/computer-networks/tcp-ip-reference-model>
- <http://www.computernetworkingnotes.com/ccna-study-guide/osi-seven-layers-model-explained-with-examples.html>

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

Well you can do both, if you have the possibility for a formal education, like computer engineering, that would be great, if not, you can study on your own and do self-improvement.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

You have lots of information online, but you always need to find what suits your needs.

WEBSITES:

- <https://www.lynda.com/>
- <https://alison.com>
- www.cybrary.it
- <http://www.computerscienceonline.org/courses/>
- <https://www.coursera.org/>

BOOKS:

- Black Belt Hacking & Complete Hacking Book
- Hackers High School 13 Complete Hacking E-books
- Penetration Testing With Backtrack 5
- A Beginners Guide To Hacking Computer Systems
- Black Book of Viruses and Hacking
- Secrets of Super and Professional Hackers
- Dangerous Google Hacking Database and Attacks
- Internet Advanced Denial of Service (DDOS) Attack
- Computer Hacking & Malware Attacks for Dummies
- G-mail Advance Hacking Guides and Tutorials

- Vulnerability Exploit & website Hacking for Dummies
- Web App Hacking (Hackers Handbook)
- Security Crypting Networks and Hacking
- Botnets The Killer Web Applications Hacking
- Hacking attacks and Examples Test
- Network Hacking and Shadows Hacking Attacks
- Gray Hat Hacking and Complete Guide to Hacking
- Advance Hacking Exposed Tutorials
- 501 Website Hacking Secrets
- Internet Security Technology and Hacking
- CEH Certified Ethical Hacker Study Guide
- Advanced SQL Injection Hacking and Guide
- Web Hacking & Penetration testing
- OWASP Hacking Tutorials and Web App Protection
- CEH – Hacking Database Secrets and Exploit
- Ethical Hacking Value and Penetration testing
- Hack any Website, Complete Web App Hacking
- Beginners Hackers and tutorials
- Ethical Hacking Complete E-book for Beginners
- Backtrack: Advance Hacking tutorials
- SQL Injection attacks and tutorials by Exploit DB
- XSS + Vulnerability Exploitation & Website Hacking
- Ultimate Guide to Social Engineering attacks
- White Hat Hacking complete guide to XSS Attacks
- Cross Site Scripting and Hacking Websites
- The Hackers Underground Handbook (hack the system)
- Blind SQL Injection tutorials and Hacking
- Hacking Secrets Revealed
- Hacking Website Database and owning systems
- Reverse Engineering for Beginners
- Reverse Engineering (The Real Hacking)
- Computer Hacking
- Hack your Friend using Backtrack
- Reverse Engineering Hacking and Cracking
- Hack the System for beginners
- Hacking into Computer Systems
- Blind SQL Injection Discovery & Exploitation

**WHAT MISTAKES DO
BEGINNERS USUALLY
MAKE?**

Well, from my experience, what I've seen is most beginners start to use scripts for hacking systems, without knowing sometimes what these scripts do. Sometimes they use key-loggers without the knowledge of what they really do, or they use trojans but they don't understand what they do. Beginners forget that they need to know programming languages to become hackers, they download tools that sometimes put their systems at risk, just because those tools are "sold" like being able to hack this or that system.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

Well, the hacker community is big, and some are closed communities where you need to show your skills so you can enter, but most are open. Yes, I do know some forums and I'll pass some links below:

- **Cybrary – Free Cyber Security Training** - <http://www.cybrary.it>
- **Hak5 – New Hacks Every Week** - <https://hak5.org>
- **Tinkernut** - <http://www.tinkernut.com>
- **Cyberpunk** - <http://nowhere.net>
- **Exploit Database** - <http://www.exploit-db.com>

- **HackADay – Fresh hack everyday**
<http://hackaday.com>
- **Evil Zone – Hacking Community**
<https://evilzone.org>
- **Hack this Site**
<https://www.hackthissite.org>
- **Cellphone Hacks**
Forum <http://www.cellphonehacks.com>
- **HackSociety – Grey Hat Hacking Forum** <http://hacksociety.net>
- **Offensive Community – Code and Exploit Forum**
<http://offensivecommunity.net/>

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

I normally keep up to date with feeds, and information sent from CSIRT and CERT. The feeds I use are the following:

- **Forum Discussions**
<http://forums.alienvault.com/discussions>
- **Labs Researching**
<http://feeds.feedblitz.com/alienvaultotx>
- **How-To's**
<http://feeds.feedblitz.com/alienvault-security-essentials>

- **Blogs** <http://alienvault-blogs.com>
- **Security – Cisco Blog**
<http://blogs.cisco.com/>
- **Cisco Advisories**
<http://tools.cisco.com/security/center/psitrss20/CiscoSecurityAdvisory.xml>
- **Identity&Access**
<http://www.csoonline.com/category/identity-access>
- **Physical Security**
<http://www.csoonline.com/category>
- **Data Protection**
<http://www.csoonline.com/category/data-protection>
- **Darknet – The Darkside**
<http://feeds.feedburner.com/darknethackers>
- **Dark Reading Stories**
<http://www.darkreading.com/>
- **Breaches Today**
<http://databreachtoday.com>
- **Treehouse Blog**
<http://teamtreehouse.com>
- **Web Design Weekly**
<http://web-design-weekly.com>
- **DevOps.com** <http://devops.com>
- **DZone.com Feed** <http://dzone.com>
- **DevOps Reactions**
<http://devopsreactions.tumblr.com>
- **atomize.io - mot - testing**
<http://feeds.feedburner.com/>
- **Web Platform Blog**
<https://blog.webplatform.org>
- **SoftwareTestPro.com Conference Presentations Feed**
<http://www.softwaretestpro.com/RSS/tag/Conference+Presentations>
- **Blog**
<http://doc.emergingthreats.net/bin/view/Main/WebRss>
- **Security Advisories**
<http://www.fortiguard.com/>
- **Technical Docs**
<http://docs.forticare.com>
- **GNS3 - All Contents**
<https://thwack.solarwinds.com/>
- **Internet Security Systems**
<http://www.iss.net>
- **BIND DNS Security**
<https://www.isc.org>
- **Curated Security News**
<https://isc.sans.edu>
- **News** <http://www.kaspersky.com>
- **FreeBSD Advisories**
<http://www.linuxsecurity.com>
- **DNS-BH - Malware Domain Blocklist**
<http://malwaredomains.com>
- **MalwareDomainList updates**
<http://www.malwaredomainlist.com>
- **Malware DNSBL**
<http://www.malwaredomains.com/>

- **Malware-Traffic-Analysis.net - Blog Entries**

<http://www.malware-traffic-analysis.net>

- **McAfee Labs Security Advisories**

<https://community.mcafee.com/community/feeds/allcontent?community=2210>

- **Comprehensive Alerts**

<https://technet.microsoft.com>

- **Office 365 URLs and IP Addresses**

<https://support.office.com>

- **Updates**

<http://exchange.nagios.org>

NEWS

- <http://www.openstack.org/blog>
- <http://blog.osvdb.org>
- ha.ckers.org web application security lab
<http://ha.ckers.org/blog/>
- **Pentester.es**
<http://www.pentester.es>
- **PortSwigger Web Security Blog**
<http://blog.portswigger.net>
- **Open Web Application Security Project** <http://owasp.blogspot.com>
- **Web App Security**
<http://seclists.org>
- **Pentest Geek – Penetration Testing – Infosec Professionals**
<https://www.pentestgeek.com>

- **Zend Framework Security Advisories**

<http://framework.zend.com/security>

- **Tactical Web Application Security**

<http://tacticalwebappsec.blogspot.com>

- **All News**

<http://rss.packetstormsecurity.com>

- **SANS Internet Storm Center, InfoCON: green**

<http://iscxml.sans.org>

- **Handlers Diary** <https://isc.sans.edu>

- **CERT Advisories** <http://seclists.org>

- **HoneyPots** <http://seclists.org>

- **Penetration Testing**

<http://seclists.org>

- **The Exploit Database - CX Security.com**

<http://securityreason.com>

- **SecurityFocus Vulnerabilities**

<http://www.securityfocus.com>

- **National Vulnerability Databas**

<http://nvd.nist.gov>

- **Errata Security**

<http://erratasec.blogspot.com>

- **Fortinet Blog | Latest Posts**

<http://blog.fortinet.com>

- **Usability Sciences - Website Usability Testing&Online Usability Testing Company**

<http://www.usabilitysciences.com>

- **Security Intelligence**
<https://securityintelligence.com>
- **News** <http://www.securityfocus.com>
- **Latest News**
<http://www.securitymagazine.com>
- **Vulnerabilities - Exploits**
<https://securityvulns.com/exploits>
- **Securelist - Information about Viruses, Hackers and Spam**
<http://www.viruslist.com>
- **CarnalOwNage&Attack Research Blog**
<http://carnalownage.attackresearch.com/>
- **Naked Security**
<http://nakedsecurity.sophos.com>
- **Android Central - Android Forums, News, Reviews, Help and Android Wallpaper**
<http://www.androidcentral.com>
- **Schneier on Security**
<http://www.schneier.com/blog>
- **Threatpost | The first stop for security news**
<http://threatpost.com>
- **Security Advisories**
<http://www.tenable.com>
- **Malware - ThreatPost**
<https://kasperskycontenthub.com>
- **Web-Security - Threatpost**
<https://threatpost.com>
- **Security Tool Files ≈ Packet Storm**
<http://packetstormsecurity.org>
- **Exploit Files ≈ Packet Storm**
<http://packetstormsecurity.org/>
- **ToolsWatch.org – The Hackers Arsenal Tools Portal**
<http://www.toolswatch.org>
- **Threat Advisories**
<https://www.trustwave.com>
- **VMware vSphere Blog**
<http://blogs.vmware.com/vsphere/rss.xml>
- **Oracle's Virtualization Blog**
<http://blogs.oracle.com>
- **News** <http://www.citrix.com/news.rss>
- **E v e n t s**
<http://www.citrix.com/events.rss>
- **The OpenStack Blog**
<http://www.openstack.org>
- **VirtualBox Mania**
<http://vboxmania.net>
- **Exploits** <http://oday.today>
- **Exploits**
<http://www.exploit-db.com>
- **Vulnerabilities & Exploits**
<https://cxsecurity.com>
- **Vulnerability Lab (Index)**
<http://www.vulnerability-lab.com>

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

In my opinion, I never followed any formal training path, as I learned most of the stuff I know on my own and with other very experienced hackers, and with them I really learned a lot. It depends what path you want to take, but I recommend Kali Linux Courses:

1. Penetration Testing with Kali Linux
2. Offensive Security Wireless Professional
3. Offensive Security Web Expert
4. Offensive Security Expert
5. Offensive Security Exploitation Expert
6. Offensive Security Certified Professional

Of course, before you take these courses, I recommend you take Cisco Certified Network Administrator, so you can get the knowledge of networks, it's a somewhat basic course, but it's pretty good.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

Well, if you are beginning, yes it is important because you'll get knowledge on how some attacks are taken and how you can defend from some of them. But in my honest opinion, I think it is not that important.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

Among others, I think the most important skill for a hacker is programming, so you can create your own tools instead of using other people's tools.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

Well, I don't think there is a best programming language for hacking, but I can name a few that I consider excellent, like Python, Perl, Javascript, BASH scripting, and Windows Powershell. Of course, every hacker and security expert has their own preferences, those are mine.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

The language I prefer is Python, because it is a very powerful and dynamic language, you can use it for creating your own network, web, exploitation, reverse engineering tools, etc.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

Well, I use many tools like Maltego, nmap, dnsmap, sqlmap, OWASP Zap, Spiderfoot, Arachni, Burp, Nessus, Metasploit, aircrack. Well, that's a tough question, as there are some of them that are my favorites, but no doubt that Metasploit is my favorite tool, because it's the way you create your exploits, and use exploits and payloads for offensive security.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

I don't think that there's a best OS for hackers, as most have their own choices, some choose Pentoo (Gentoo based distribution for pentesting), some use Parrot OS (Debian based distribution for pentesting), BlackArch (Arch Linux based OS for pentesting), just to name a few. Well, I use Kali Linux as it is my favorite on the tools and it's light, and my favorite flavour of Linux, Debian based distro, but I tested all the others, and they all have their own singularity.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

I use a laptop core i5 with 16GB RAM and 2 SSD disks, one disk for the system and the other to run my virtual machines when needed. I sometimes use a Belkin wireless adapter as it has the promiscuous mode capability, I use a Raspberry pi with Kali Linux with various USB wireless adapters and sometimes DVB-T+DAB+FM.

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

Yes, I do follow a methodology, based on OSSTMM (Open Source Security Testing Methodology Manual). No, I don't have a specific workflow that I follow, but I always do the following in practice:

- Planning
- Reconnaissance
- Discovery
- Analysis
- Active intrusion
- Reporting

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Yes, certification is really important, and as we move on, we should make continuous certification programs, so we can improve our knowledge and skills. Well, for me, the most important is CompTIA Security+.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

First of all, people consider that hacking is some kind of magic, well let me tell you it is not, hacking relies on knowledge, science, the hacker's techniques and experience. Hacking is something more like a science and an art all together. The second misconception is the public in general tend to have the idea that hacking is like using daily known exploits and breaking into systems, well it is not, that's crime, being a hacker is someone who has the ability to break into a system they know well, and create workarounds to better those systems and those flaws, always with the consent of other party, or their knowledge. Third and last, the term hacker should not be used for bad abilities, bad behavior online like violating computer systems or networks.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

The advantages are you knowing a system so well that you can make it almost "bullet proof", to be able to create and implement security measures on your systems that prevent attacks and prevent malicious hackers to break in.

Some of the disadvantages are the use of knowledge, not only your own but those of ethical hacking communities to do harm and for cybercrime.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

For me, the most important is that you need to be good at problem solving, need to have good communication skills, be able to know that you'll always need to have explicit permission from the management to perform your work. You need to be passionate about it, you need to always be able to be open minded in learning anything that is useful to do your job well, like open to do certifications, and create certification paths, even if they are your own certification paths, to improve your skills. You need to have a critical spirit about your work, too.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

Yes, there was something I skipped because I thought it would not be that useful, it was Social Engineering, most like to describe it as hacking the humans. And yes I do regret it, I should have learned it earlier.. AHHAHAH 3:)

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

Yes, hardware security.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

Well, for me the greatest obstacle was to gain credibility.

WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

Remember that there are no bullet proof systems, every system has a flaw, so think outside the box.

DO YOU HAVE ANY OTHER STORY RELATED TO HACKING THAT YOU WOULD LIKE TO SHARE WITH US?

Well, I have plenty, but I can't share them with the public, sorry.

DO YOU HAVE ANY ADVICE FOR OUR READERS?

I do have some! If you're thinking about making a career in hacking, never give up, be humble, never think you know everything, you don't, well I don't :P, study to improve your knowledge and skills, and never forget that security is what people make of it.

ADITYA BALAPURE

SENIOR APPLICATION SECURITY ENGINEER WITH GRUBHUB

My name is Aditya Balapure, and I currently work as a Senior Application Security Engineer with Grubhub. Security and good food are the two obsessions of my life. When I am not doing Security, I also like gaming and travelling to places. Full disclosure, the thoughts shared below are mine personally and do not represent Grubhub in any form.



**WHY DID YOU DECIDE TO
BECOME A HACKER?**

I started off as a Computer Science Engineer solving programming problems and then came across the concepts of System Security. The idea of bad guys breaking into systems intrigued me and started my journey of being the good guy to save the world (pretty much like the Science Fiction movies). This was my start into the Cyber Security space. I have a knack for finding and solving problems, especially when they are related to computers. It motivated me to be a Cyber Security Professional, often termed a hacker. Computer Security is a complex problem, and there is not one silver bullet to solve all the challenges, making it even more interesting.

**IF I WANTED TO BECOME
A HACKER WHERE
SHOULD I START?**

To be on the path to become an expert Cyber Security Professional (a.k.a. a hacker), a good start would be the C programming language, networking concepts, assembly basics, understanding web browser concepts and the Open Systems Interconnection (OSI) model as a whole.

**AT THE BEGINNING,
WHICH IS MORE
IMPORTANT - INDIVIDUAL
WORK AND SELF-
IMPROVEMENT, OR
SOME KIND OF FORMAL
EDUCATION?**

It depends on the individual. Some people like to go through a formal education route that is well paced and more like a curriculum. Others like to learn as they go through individual work. There is no fixed route. You should try out both routes and see what works best for you. At the end of the day, you want to improve your knowledge and skills.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

I personally do not endorse any specific books or courses, but I'd like to share the resources that I have found to be helpful. They include: **Hacking: The Art of Exploitation**, **The Web Application Hacker's Handbook**, **The Browser Hacker's Handbook**, **Practical Malware Analysis**, **Reversing: Secrets of Reverse Engineering**, **The Art of Software Security Assessment**, **Cryptography Engineering**, **Bulletproof SSL and TLS**, etc. Again, the idea is to find resources that help you understand the basics well.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

I have found that beginners usually make the mistake of going through the "script kiddie" route where they just focus on running automated tools that magically make things happen for them. Rather, the idea should be to understand the actual vulnerability or the security bug that was flagged by the tool and go deeper to learn the facts.

Understanding the problem at the code level is really important in order to be able to patch it effectively and be a knowledgeable Cyber Security professional. In the end, it all boils down to the concepts that I covered when discussing where to start your journey to become a hacker.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

I strongly encourage beginners to be a part of the local chapters/meetups for Information Security. It is a great platform to grow one's knowledge and career prospects as an Information Security Professional. Going to Information Security conferences is again an easy way to meet like-minded people and acclimate to the hacker culture. Security mailing lists, IRC chat rooms and Twitter are great ways to be in touch with the hacker community and follow the leaders in this space.

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

Twitter and Reddit are my go-to sources to keep up with Cyber Security news. The sources mentioned here <http://www.gfi.com/blog/the-best-35-information-security-blogs-to-follow/> are a good start as well.

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

Getting the basics right and understanding the concepts first are important. Following online blogs,

watching video tutorials on websites like SecurityTube, reading Capture The Flag (CTF) write-ups, and taking security courses on Coursera form a great training path.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

I would not endorse any certifications personally, but yes, CEH is a good start in understanding some of the concepts I have discussed for beginners in Information Security.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

The most important skills to have as a hacker are patience and the motivation to keep trying harder.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

I prefer to use Python for security automation or similar tasks because of its ease of use and library coverage. It makes it simple to get difficult tasks done.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

As mentioned, it is really important to understand the core concepts of the C programming language and then move on to something like

Python or Ruby. Bash and Powershell are good to know as well since they help automate many system tasks.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

The suite of tools I use differs depending on the task at hand, but the latest version of Kali contains almost everything to get you started. The right tool really depends on the task you are trying to achieve. You might be fuzzing a web application using Burp Suite, information gathering using Nmap, understanding packet captures in Wireshark, or reversing a ransomware sample using IDA Pro or Ollydbg. The idea is to explore and be hands on with suites of tools to make them easier to use. Again, please remember that a hacker uses much more than just automated

tools. You should be comfortable writing and understanding code to find security flaws, leverage multiple environments (web, OS, IoT, Mobile), and understand technology at a deeper, technical level.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

It depends on what you want to achieve. These automated tools are compatible with most of the platforms, but the latest version of Kali OS has the whole suite of tools and reduces any installation overhead. I also run many virtual machines for emulating various test environments with a range of Windows and Linux installations.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

Any hardware with a good configuration in terms of memory, processor speed, and disk space will be able to support the work you are trying to achieve.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

Formal methodologies work best with compliance exercises. If you are doing a penetration test, then information gathering, understanding your target and exploiting the weaknesses is important, almost like a process flow. It is similar as well for malware reverse engineering. There is always a process to achieve an end goal. You get better with experience and will develop your own methodologies. Rather than a fixed methodology, I have an open mind when looking at problems, which helps me create better solutions.

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Certification and formal education may give you a head start or grow your Cyber Security knowledge, but it still boils down to how well you understand the core concepts, gain practical experience with the tools and understand the environment.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

Hacking can have a shady reputation since people sometimes do not understand what a hacker does professionally. There are good and bad aspects of hacking. It generally has a negative connotation since

people imagine that a hacker is someone trying to break into systems to compromise user data, gain access or steal money. This only reflects the bad aspects of hacking related to cybercrime.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

I am a strong believer in the Open Source way of thinking. Therefore, I see hacking for its positive qualities that do not involve any form of cybercrime. The advantages of hacking are white hat hackers who work with organizations and develop open source initiatives that make the internet more secure. Their contributions are finding vulnerabilities in software, reporting new forms of malware seen in the wild, reporting various phishing attempts, and building more secure software. The disadvantages of

hacking, as I said before, involve the hackers that commit cybercrimes, which is the wrong path.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

One of the things that I have always found to be useful is diving deep so that you understand the code. Having a good amount of coding skills certainly goes a long way in not only breaking systems but also solving security problems by creating tools and scripts.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

The only thing that became clear with time and experience was the shift from being a script kiddie to focusing on technologies and security concepts at a core level. I do not regret not learning something early on because I am a firm believer that it is never too late to learn new things.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

The most important aspects when planning any career are dedication and passion for the field. This is true for a career in Cyber Security as well. You must also have patience. You will be caught up in multiple situations in which there is no direct solution. A career in Cyber Security also involves coping with stress since you are at the forefront defending against cyberattacks and must be one step ahead of the bad guys.

**WHAT'S THE MOST
IMPORTANT THING TO
REMEMBER AS A
HACKER?**

The most important thing to remember as a hacker is that there is a fine line between being a good hacker and a bad one. The bad path is tempting because it can now be especially lucrative given the boom of information technology in our daily lives. It is about never crossing that line and focusing rather on making the internet more secure.

**WHAT IS THE GREATEST
OBSTACLE YOU HAD TO
OVERCOME TO GET
WHERE YOU ARE**

Life is a fun journey and obstacles help you become more mature. I definitely had obstacles early on since Cyber Security was not a very common career when I initially

started. It was still a Software Developer-focused market and Security was not seen as important. The trend has changed since then with the boom in Cyber Security careers. Sticking to your passion and getting a good education are really important to building a strong career.

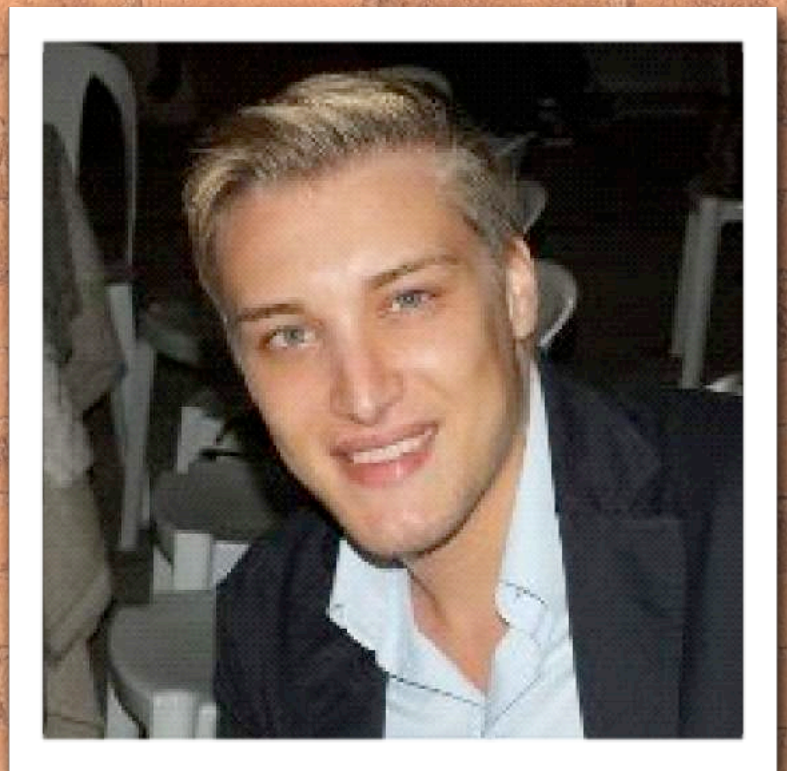
**DO YOU HAVE ANY
ADVICE FOR OUR
READERS?**

The only advice I have for the readers and budding Cyber Security professionals is to follow your passion, work hard and have a lot of fun along the way.

ANDREA SANTESE

PENETRATION TESTER

My name is Andrea Santese and I'm a Penetration Tester (Mobile/Web/Network). I've been a Bug Bounty Program Participant and my name has been listed in the Security Hall of Fame of Facebook, Google, Paypal, Yahoo, Ebay, Yandex, Barracuda Networks, Wordpress and many others.



WHY DID YOU DECIDE TO BECOME A HACKER?

I've always been fascinated by hackers since I was younger because I've always loved to see what a man can do with a computer. I started to deal with computers when I was fourteen after having seen the film that describes the history of Kevin Mitnick, Takedown. It has been a source of inspiration.

IF I WANTED TO BECOME A HACKER WHERE SHOULD I START?

I recommend to people that want to start dealing with hacking that a solid basis of how computers work is required. Passion and determination are necessary. The beginning can be very frustrating but the hard work pays off in the long run.

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL

I think that at the beginning individual work and self-improvement is the most profitable solution to people that want to dive into the hacking field.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

I think that online courses from SecurityTube are the best courses where you can learn how to pentest. The books I recommend are The Web Application Hacker's Handbook, the OWASP Guide, The Hacker Playbook and The Hacker Playbook 2.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

One of the most common mistakes that beginners make is to believe that they can become good hackers in a short period of time. They should invest instead all their life.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

I think that one of the best hacker communities where you can learn a lot of things is BugBountyHQ. In this website, people from all over the world publish their write-up on vulnerabilities found on websites like Facebook, Google, Paypal and so on. I have learned a lot of tricks there.

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

To keep updated, I usually check on SecurityWeek and Security Affairs. They are always the first to publish hacking news.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

Yes because nowadays it's one of the most requested certification. I think it's very useful because it covers multiple fields of information security.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

I think the most important skill a hacker should have is perseverance, because every time they come across a problem, they have to remember that a solution exists, they have only to try harder.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

In my opinion, the best programming language is C, because with it you can create whatever you want.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

I often use programming languages like Bash and Python because they facilitate and automate my penetration tests.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

The tools I use are usually web application related tools such as Burpsuite, which is an intercepting proxy, nmap, nikto, sqlmap, dotdotpwn, recon-ng, fierce, wpscan, CMS-Explorer, joomscan and many other. All the tools mentioned are useful but I think that the most powerful tool is the brain because every web application has their functionalities and only the brain can understand how a web application works. The use of the brain may allow finding of vulnerabilities that tools can't.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

I think that nowadays the best OS for hackers is Kali Linux, which is an

an operating system that is born with a lot of preinstalled tools that make the hacker's life easier.

After this, I try to understand how an application works to make the exploitation phase easier.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

For penetration testing, I recommend a laptop with an Intel Quad Core i7 processor with at least 8GB of RAM and a 500GB hard drive (solid state is recommended).

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

When I have to pentest a web application, the first thing I do is to take as much information as possible because every detail can be useful in hacking a web application. The most important phase of a penetration test is the information gathering phase.

FROM YOUR EXPERIENCE, IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

In a world where the number of hackers is increasing quickly, certifications are becoming increasingly important. Companies are always looking for people that have a certification because in addition to demonstrating a hacker's abilities, they also demonstrate how a hacker is prepared to try harder to solve problems. I think that the most important certifications are those that are released from Offensive Security. They are the most complete certifications that also teach you the methodology behind a penetration test.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

People generalize about hackers thinking that hackers are bad guys. There are both good and bad hackers. I simply try to make the world a safer place.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

One of the advantages of hacking is that good guys exist and they help companies improve their security, while one of the disadvantages is that blackhat hackers also exist that use hacking to violate computer security for personal gain.

**WHAT IS THE
GREATEST OBSTACLE
YOU HAD TO OVERCOME
TO GET WHERE YOU ARE
TODAY?**

I think that the greatest obstacle is the beginning, when a solid basis of how a computer works is necessary before starting to think about hacking. I remember that moment, it has been very frustrating.

**WHAT'S THE MOST
IMPORTANT THING TO
REMEMBER AS A
HACKER?**

Often when hackers take awareness of their abilities, they start to believe that they can do everything, thinking that they can hack the world, but they're wrong. So one of the things that a hacker should remember is to be an unpretentious person.

**DO YOU HAVE ANY
ADVICE FOR OUR
READERS?**

If you want to become a hacker, know that it's not as easy as you imagine. You have to be very keen and time is required before starting to hack things.

ANTHONY CALDWELL

CYBER SECURITY ANALYST

My name is Anthony Caldwell and I'm a cyber security analyst with a major insurance firm.

WHY DID YOU DECIDE TO BECOME A HACKER?

The opportunity to train as a hacker presented itself to me while working as a QA engineer along with a colleague who was already a hacker. He introduced me to the field and we took it from there.

IF I WANTED TO BECOME A HACKER WHERE SHOULD I START?

These days, it's much easier to find a legitimate course that offers ethical hacking. So try the academic route, the industrial route but definitely not the 'script kiddie' route.

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

For me, I dedicated myself to researching security on my own. These days there are formal educational institutes that offer industrial and academic courses.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

Haking, PenTestMag, and EForensics are great resources, of course. OWASP, the ISC2 and EC-Council also have excellent resources.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

It's easy to make mistakes in this game. Don't be fooled by YouTube videos showing you how 'easy' hacking is. Do the homework like the professionals do.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

The trade magazines like Hacking, PenTest, and EForensics are great places to start. Many also refer to ‘The Register’ also.

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

‘The Register’, ‘Phrack’, ‘HotForSecurity’ are quite good for headlines.

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

Yes. You could start by working in a call centre specializing in security issues and consider internal transfers to web application testing, threat analysis, etc., via mentoring programmes if available.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

Yes. CEH is important and I’d recommend having this cert in hand. There are others from SANS and OSCP, of course, but CEH is a good start.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

Patience!

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

Many recommend Python, but really programming experience in general is helpful.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

None to be honest. It's not my strength area. I tend to leave that to better people than me.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVOURITE HACKING TOOL AND WHY?

SQLMAP, BurpSuite and ZAP. They capture the essential traffic that you need.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

As I'm an employee in a large scale corporation, I'm bound to Windows OS. Using Kali is the hacker's preference for security tests, though.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

Not particularly. You can get remarkably sophisticated work done with low specs.

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

Yes, it's an internally developed system that is oriented around the OWASP framework.

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Yes. And for me it's the academic ones as a foundation. This could be general computer science or specifically digital forensics. Neither of which I have! I finished a PhD in information systems research and from this I learned on my own.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

All the typing and random DOS prompts!! TV shows and movies have a lot to answer for. Hacking is patience, lots of blind alleys and following a scientific mindset.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

Disadvantages are questions from the general public as regards 'can you hack into XXX?' The answer is always yes, but, as regards how long it'll take, that's a different story. Advantages are that it's a growing field and very interesting.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

To be prepared to work at the lowest levels first. All too often, recent college grads come out of college thinking that they're qualified. And while this is true on paper, they have no experience.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

Yes...focusing on programming. Never enjoyed it and don't think I ever will.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

Advanced academic research into security. This is a goldmine that has never failed me. Look at what's going on in universities because that's what we'll be asked to implement in industry five years or more from now.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

Managerial understanding about what security is as a process. It's not their fault, it's ours. We need to get managers and executives to see that security isn't just a big tick mark that's good for now and all time. Rather it's good 'for now'.

WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

No unauthorized testing. Locard's Principle: 'Every touch leaves a trace.'

DO YOU HAVE ANY ADVICE FOR OUR READERS?

Work hard and keep working hard. Never ever give up!

CORY MILLER

PRINCIPAL VULNERABILITY DETECTION ANALYST

Hello my name is Cory Miller; I currently work in Information Security focusing on vulnerability management and penetration testing I have been in Information Technology for over 10 years. During that time, I received my Bachelor's degree in Computer Science specializing in Information Assurance and Security. I currently hold certifications such as CISSP, GPEN, LPT, CEH, CHFI among other industry certifications. I enjoy participating in CTF challenges and utilizing what I have learned in my lab environment. In addition to reading about current InfoSec trends, I enjoy spending time with my family and being outdoors.

WHY DID YOU DECIDE TO BECOME A HACKER?

I have always had a passion and interest to how things work. Being able to take that curiosity and drive allowed me to pursue my hobby and interest as a career. There is nothing more fulfilling than getting paid for what you love to do.


to understand the basic concepts of how systems interact with software and vice versa. This will allow you to get a solid foundation of how things works overall. Remember, everyone has their strengths and weaknesses. During this time, try to focus on what interests you and take what you already know further; always remember to try to build on what you learn.

IF I WANTED TO BECOME A HACKER WHERE SHOULD I START?

There are many ways to get started in security. There are virtual images that are vulnerable and designed to teach you techniques such as Cross-site Scripting and SQL Injections to vulnerable web services. Security is a very fast evolving field so for starters, I would suggest that you take the time

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

Both, it is very important to concentrate on self-improvement in any environment but getting formal education and training will be key in allowing you to have the credentials to back up your skill-set and knowledge.



WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

There is no shortage of information and material that will teach you the various techniques to hacking. Below is a list of sites and books that will provide hours of training and reading.

SECURITY BOOKS:


- *The Web Applications Hacker's Handbook* - This is a great book that shows you various ways to exploit web applications.
- *A tangled Web* - This book walks through how browsers work and interact.
- *Hacking Exposed* - This book walks you through the methodologies that hackers use to collect information and exploit a system.
- *Burp Suite Essentials* - This book teaches you how to setup and use Burp Suite proxy, which can be followed step-by-step.
- *Haking9* – A great magazine for all types of tutorials; you can purchase a subscription, classes or just purchase separate magazine issues.
- *Pen Test Magazine*
- *eForensics Magazine*
- *Red Team Field Manual*

WEBSITES ONLINE HACKING AND VULNERABLE IMAGES:

- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- <http://www.amanhardikar.com/mindmaps/Practice.html>
- <https://www.offensive-security.com/metasploit-unleashed/requirements/>
- <https://www.vulnhub.com/>
- <https://www.root-me.org/?lang=en>
- <https://www.pentesterlab.com/>

**WHAT MISTAKES DO BEGINNERS
USUALLY MAKE?**

One thing that I had to focus on was to not get to overly ambitious learning everything at once. With all the Hollywood hacking movies, it's easy to get blind sided from all the glamour. Just as hacking a system is important, it is also equally important to learn how to communicate how you exploited the system and to write clear reports. Sometimes you will have to explain what you did to an audience that might not be as technical.



**WHAT ABOUT THE HACKER COMMUNITY?
DO YOU KNOW ANY FORUMS FOR NEW
HACKERS OR BEST WEBSITES TO MEET
PEOPLE WITH SIMILAR INTERESTS?**

There are many meetups and security conferences across the world. These are great ways to get involved in the security industry and network with other security professionals. Meetup usually has local meetings among people in the area, if there is not one in your area you might consider setting up one.

Security conferences are a lot of fun. There are usually Capture the Flag events where you can put your skills to the test against other hackers. They are for all types of skillsets so don't be afraid to just try it. Everyone is welcomed to participate and the people who run the CTF will help give hints from time to time. Some security conferences in the United States are Blackhat, Hack Miami, DerbyCon, TriangleInfoSecCon, Shmoocon and Defcon.

TUTORIAL AND HACKING FORUMS:

- <http://www.hacking-tutorial.com/#sthash.lfxyhfPr.dpbs>
- <http://offensivecommunity.net/>
- <https://hackforums.net/>

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

It is important to stay up-to-date with vendor security news as well as the latest vulnerabilities to help you stay current with what is going on. Below is a list of sites that can help provide valuable information regarding the security industry.

- <https://github.com/jhaddix/pentest-bookmarks/blob/wiki/BookmarksList.md> - [jhaddix complete list of sites](#)
- <https://threatpost.com> - [good up-to-date news.](#)
- <http://securityweekly.com> - [one of the best podcasts for security professionals.](#)
- <https://www.wired.com/category/security/threatlevel/>

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

I would highly recommend the OSCP from Offensive Security. The OSCP is a very challenging and rewarding certification to take. It is all hands on with a practical exam at the end. They give you 24 hours to exploit and gain root/administrator access to five systems. The passing score is a 70. You also have to write a penetration test report explaining how you gained access into the systems. There are hours' worth of training videos included, as well as lab access. Once you have completed the exam, you have have started a full penetration test and documented your steps. You will have a good understanding as to what is involved with hacking as a career.

**DO YOU THINK THAT
CEH IS AN
IMPORTANT PART IN
HACKING CAREER?**

The CEH is a good certification to take and will get you the knowledge of the penetration testing methodologies. However, I would concentrate on more hands on types of certifications. Certifications such as OSCP, SANS and eLearn Security are all very good hands on practical courses that will help strengthen your knowledge and skills in hacking.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

The ability to see things from a different perspective. You need to learn how to think like an adversary and try to identify ways that a system can be used in a way it wasn't meant to be used. Being able to have patience and perseverance to keep trying different techniques, sometimes things do work out of the box and it is important to understand what you are trying to achieve and how you can get the desired outcome.

and Ruby can be used for automating daily tasks and building your own toolset. The languages are very easy to learn, especially for beginners. Metasploit and its exploits are written in Ruby so being able to read and understand the exploit checks will put you at an advantage and allow you to utilize those tools more efficiently.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

I would recommend learning Python and or Ruby. Both Python

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

There is definitely no shortage of hacking tools today. I would focus on a small subset to start then expand from there. Keep in mind some of the tools have overlapping capabilities, it just takes time to learn and what you are most comfortable with. I would start with the below list.

- Metasploit
- Nmap
- Wireshark
- Nessus
- SQLMap
- BurpSuite
- Nikto
- John the Ripper
- Hydra
- Aircrack-ng

The tools listed above range from information gathering to exploitation of network and wireless systems. They are only a few of what Kali Linux provides and are all open source, excluding BurpSuite and Nessus, which offer a limited free version and a commercial full version.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

Understanding and being comfortable using both Windows and Linux will allow you to have the knowledge of how each of these operating systems work and will give you greater flexibility during a penetration test. I utilize both but enjoy Kali Linux because there are many tools that are integrated into the OS.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

I am big on performance. A lot of RAM and a good processor is key. Besides those two items, pick a system that you are comfortable with and an operating system that you know inside and out. This will

help you troubleshoot any issues you have with tools and testing along the way.

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

The Pen-Test Standard is a great methodology to follow. Their site is full of information that lists techniques and tools for penetration testing. You can find the methodology here:

http://www.pentest-standard.org/index.php/Main_Page. I would also recommend taking a look at the Open Web Application Security Project (OWASP). The OWASP site goes over the top 10 common vulnerabilities in web applications and basic testing techniques: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Certifications are important to show that you have the knowledge and help get you past the initial requirements at a company.

However, experience and skills are the most valuable asset. You need to know how to put your skills to the test.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

One of the biggest misconceptions is that a tool will do all the hacking for you. Although some tools are very beneficial and can help do a lot of the heavy lifting, it is crucial to understand how to gather

intelligence and how to exploit the system. In addition, sometimes tools do not work and being able to manually achieve what a tool can do will be your greatest asset.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

There are a couple of important things to consider when getting into this field. Technology changes rapidly, especially in the security field. Be prepared to stay on top of your knowledge. Many certifications require you to maintain CPE credits; this is designed to ensure that you are involved in the Security industry and continue to be relevant.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

I did not learn a programming language in the beginning. Applications are everywhere and as a pen tester, you will most likely be involved in testing such applications. Learning a language in the beginning will make testing and understanding how applications work easier.

DO YOU HAVE ANY ADVICE FOR OUR READERS?

Try. Try your hardest. Don't get discouraged, it takes time and patience. There is no amount of videos and books that can fully prepare you, they are only there to help guide you to get better at what you do. Keep learning and get involved in Security, both inside and outside of your organization.

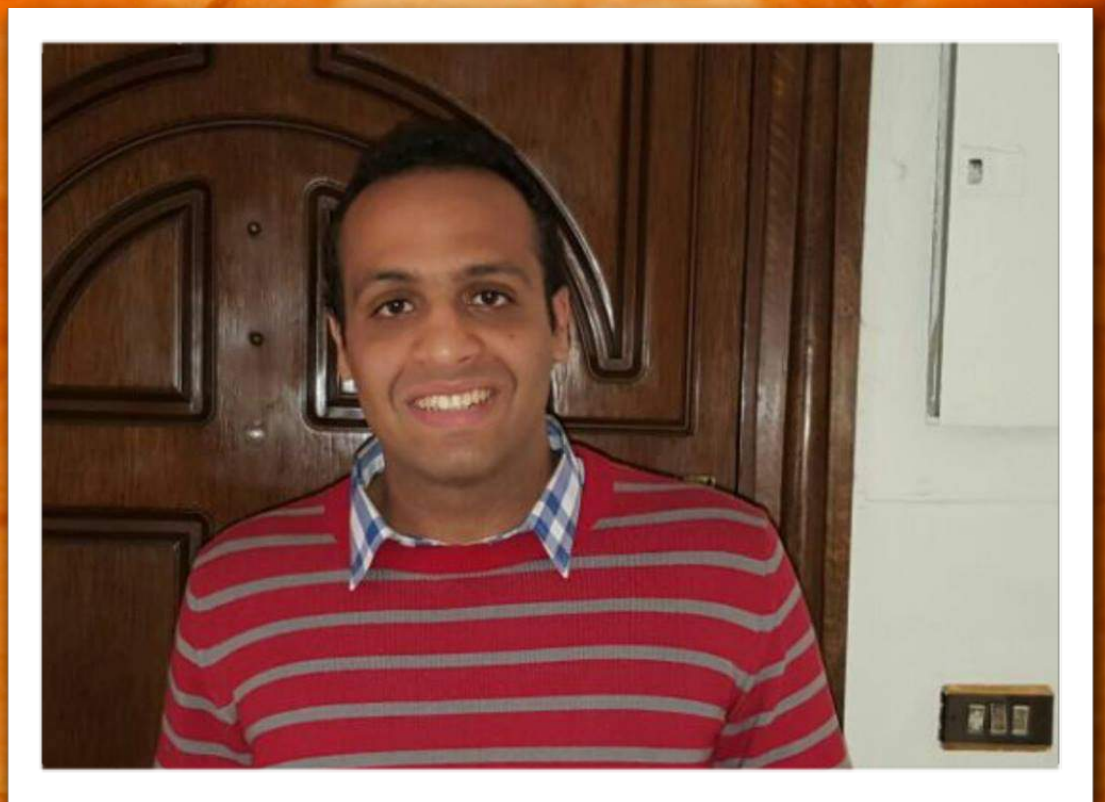
WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

Be moral and ethical in everything you do. Think about how you can impact a system or someone. Knowledge is power.

KHALED SAKR

INFORMATION SECURITY ENGINEER AT SECURITY METER

My name is Khaled Sakr, an information security engineer at Security Meter company in Egypt. I graduated in 2013 from the communication department at Cairo University.



I'm interested in the security field, especially in reversing and exploit writing. I performed multiple penetration test activities for major banks and companies inside Egypt and Qatar.

WHY DID YOU DECIDE TO BECOME A HACKER?

My love of computers and programming and the curiosity to understand how things works internally was my motivation to learn about hacking.

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

I believe that hacking is not purely an academic topic, so it's more practical and requires individual work and self-improvement.



IF I WANTED TO BECOME A HACKER WHERE SHOULD I START?

As a start, I will mention some of the fundamentals that you should start learning if you decide to become a hacker:

- Learn some **Linux**: one can't be a hacker if he can't understand or use Linux
- Learn Some Programming and scripting Languages: the thing that separates a hacker from script kiddies is programming skills. The most popular programming skills used in hacking and exploit writing are:
 - Python
 - Ruby
 - C,C++
 - Bash
- Learn **HTML** Language: Web application hacking is the most popular way that is used for gaining unauthorized access, due to the increase of its attack surface, as the number of websites on the internet are over billion. Of course, by knowing HTML only you will not be able to hack websites but still it's essential to start learning web application security.
- Learn **Networks**: Network is important to know the basics, starting from OSI layers to routing and switching protocols.
- Get **Hacker** Attitude: You got to have a hacker's attitude if you want to be one; as a start these attitudes combined with good skills will definitely make you a good hacker:
 - Innovation
 - Persistence
 - Problem Solver

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

First, I will mention some websites for video resources as they may be beginner friendly:

- Pentester Academy: This website contains courses for all types of hacking starting from network, web, Android, etc. And it describes the knowledge needed before every course and what knowledge will be acquired from the course. Most of the courses are authored by Vivek Ramachandran, who is considered one of the best hackers of all time. <http://www.pentesteracademy.com/>
- Cybrary: This website contains a good and free course for penetration testing that teaches you the basics of Linux, Programming, Metasploit, Webapps security, Exploit Writing, etc. <https://www.cybrary.it/course/advanced-penetration-testing>

Second, the most important book that I recommend studying is:

- **Hacking art of exploitation**

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

Diving in to hacking without probably learning basics.

Thinking that Metasploit can hack anything, it doesn't ... persistent does.

Thinking that hacking skills are related to how fast you can type :D

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

There are many forums, my favorites are:

- <https://hackyard.net/>
- <https://evilzone.org/>

WORKING IN CYBER SECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

News about hacking and hackers can be very informative and inspiring. The most popular pages with the latest news are:

- Twitter Account @TheHackersNews:
<https://twitter.com/thehackersnews?lang=en>
- Hackersone: <https://hackerone.com/>

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

Offensive Security Certification Path

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

Definitely No

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

Persistent

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

Python

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

Python, it's easy and beginner friendly.



WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

- Nmap
- Nikto
- Proxychains
- Burpsuite
- Dirbuster
- Sqlmap
- Volatility
- BeEf
- Nessus
- Enum4Linux
- John the ripper
- Veil
- Mimikatz
- Responder

My favorite tool is the ultimate proxy burp suite when it comes to web or mobile penetration testing and volatility when it comes to Forensics.

Also responder gets me a great output in pentests, you just run it on the network and it will get you lots of hashes.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

*nix based operating systems, I use Linux Mint.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

While learning, you will be required to run multiple virtual machines, so the minimum requirement for the machine is quad core processor and 8G RAM.



DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

My methodology in penetration testing:

Network: Attack people before servers. People are the weakest link in any network, huge things I found while doing penetration tests and surprisingly in banks, you will always find the following:

- Weak Passwords (123456,qwerty,P@ssword,<BankName@123>,....).
- Shared Backups for Emails, Hard Disks, etc.
- Stored passwords in clear text in Desktop.

So my first target is the employees by trying to crack their passwords, accessing shares or emails with these weak passwords, you can find backups of whole databases using share only.

Also run responder on the network, this tool listens performs llmnr or netbios poisoning. In parallel with checking user awareness, you can run Reconnaissance scan on the network using nmap followed by a vulnerability scan using Nessus and then you can view the results and analyze which vulnerabilities are exploitable and which framework can help in the exploitation. And also you can remove any false positives.

Web Application: My methodology in Web application is simple **Intercept and Manipulate** using our old friend **burp suite**. Never use web application scanners, they are useless, they produce tons of False positives and it might affect application performance.

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Unfortunately, certifications are important to most companies in order to at least consider you for interviews. So when taking a certificate, just make sure to take a prestigious one such as:

- Offensive security
- CISSP
- SANS Courses

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

- It takes an expert: Hacking is not rocket science, anyone familiar with computers, network and little programming knowledge can do it.
- You can hack anything over the internet (obviously you can't) but with the IOT evolving, some day you might be able to :D

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

Advantages:

- It's fun and sounds cool.
- If you know hacking, you are literally sitting on a gold mine.
- It can be taken as a profession (Penetration Testing, Security Consultants, etc.).

Disadvantages:

- It consumes time, so better balance your life.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

Assembly: Assembly most of the time is being neglected as it's more complex and harder to learn. Assembly was found to be very important when it comes to reverse engineering. Desktop Pentesting and Malware analysis; I admit it's a bit more complex to learn but it will prove to be very useful.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

- Improving your soft skills: Thanks to the movies, we always see hackers like geeks with glasses who lack all kinds of soft skills, if you are planning a career in hacking and you want to take it as a profession then you need to work on your soft skills. Many people can do an exploit or an attack but not all of them can present it in a good way.
- Taking OSCP.
- Never think you have reached your TOP because in this field, knowledge is infinite.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

Shell code: shellcode is just a hex payload instructions that gets executed by the processors once injected in the application stack, creating your own payloads can be extremely useful to bypass antiviruses. All of us just use payloads that exist on the internet, which will be caught very easily.

DO YOU HAVE ANY ADVICE FOR OUR READERS?

After getting some basic knowledge about information security, I advise our readers to practice their knowledge and start seeing hacking in action. I will mention two of the most important websites in my opinion:

Vulnhub: <https://www.vulnhub.com/>

This website contains vulnerable Virtual Machines, and its purpose is boot2root, meaning that you begin by powering on the machine, scan it, get its IP address and explore the machine till you get root access. You can start by the virtual machines that have in its description **Beginner**

Pentestit: <https://lab.pentestit.ru/>

This Russian web site creates a hacking lab free for anyone, it's just amazing what these guys are providing. It works by registering to the website, download a vpn configuration file and acquire your credentials, and download the network topology that you will start hacking and have fun!!

RAJ CHANDEL

DIRECTOR OF IGNITE TECHNOLOGIES AND THE FOUNDER OF
HACKINGARTICLES.IN



Mr. Raj Chandel, Director of Ignite Technologies and the founder of Hackingarticles.in, a website that captures the core essence of hacking and cyber security. I believe my articles guide and enhance the knowledge of my students and the e-hacking community as a whole.

**WHY DID
YOU DECIDE
TO BECOME
A HACKER?**

I have always been interested in anything related to penetration testing and cyber security, and e-hacking is like magic to me. As I started assimilating e-hacking, I started to imbibe everything about security too. So, there never was a particular enlightened moment for me that made me choose hacking, it has just always been my passion.

**IF I WANTED
TO BECOME
A HACKER
WHERE
SHOULD I
START?**

My advice to a beginner would be to have appropriate knowledge of the basic networking and programming of the computer system. Once this first step is accomplished, the person should joined the EC Council Certified Ethical Hacking course (CEH).

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

In my experience, individual work and self improvement is directly proportionate to a formal education. Conversion of theory in practice is the most important aspect of becoming a professional e-hacker. Lastly, my advice to all e-hackers is to keep updated on the surrounding and the profession.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

I believe attending class room courses from reputed institutes is a must. Online courses can give you an outline of these courses, however, they may lack in-depth knowledge.

**WHAT MISTAKES
DO BEGINNERS
USUALLY MAKE?**

Overconfidence and inadequate knowledge are major mistakes committed by beginners. Most beginners lack basic knowledge. A beginner is to be properly guided about the basics and taken step by step to higher levels of hacking course education. They forget that one should have ample knowledge of Networks, Linux, and Microsoft Windows.

**WHAT ABOUT THE
HACKER
COMMUNITY? DO
YOU KNOW ANY
FORUMS FOR NEW
HACKERS OR BEST
WEBSITES TO
MEET PEOPLE
WITH SIMILAR
INTERESTS?**

Hack Forums.net, vulnhub.com, EC Council, Security focus, EXPLOIT-DB, etc.

**WORKING IN
CYBERSECURITY
REQUIRES
KEEPING UP WITH
THE NEWS. DO YOU
RECOMMEND ANY
WEBSITES WHERE
BEGINNERS CAN
FIND RELIABLE
CONTENT?**

TheHackernews.com,
<http://securityaffairs.co/wordpress/>
are some of the sites recommended.

**IS THERE ANY
FORMAL TRAINING
PATH THAT YOU
WOULD
RECOMMEND,
ABOVE OTHERS?**

For any formal training, always go for EC-Council's courses. They provide a wide range of courses that are world class and if you have done these courses then you don't need to do anything else. I would always recommend that training should be taken from a reputed institute.

**DO YOU THINK
THAT CEH IS AN
IMPORTANT PART
IN HACKING
CAREER?**

CEH is very important part in hacking career as it lays a foundation stone for a hacker that further strengthens the roots of hacking/security career.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

Here I would like to refer to L. Frank Baum who once said “No thief, however skillful, can rob one of knowledge, and that is why knowledge is the best and safest treasure to acquire.” And by this I mean to say that knowledge is the best skill a hacker can acquire. For example, if a hacker has hacked into a server and finds out that it is a Linux server but the same person does not know Linux then there is no use of this hacking skills or what-so-ever. And this is not limited to Linux, if you are in hacking you should always know everything about anything as hacking is just another term for trespassing; you do not know what you will find so one should always be prepared beforehand.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

According to me, the best languages are Python, Ruby, Perl and even batch programming proves to be helpful.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

I usually prefer Python and Ruby because it even helps to conjure exploits in Metasploit.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

I use a combination of BurpSuite and Metasploit, Nmap, SET Toolkit and others commonly but you have to manage your tools on the basis of demand of the situation. Out of all the tools, Metasploit is my favorite because 1). I like to work through commands and 2). It has everything a hacker needs for various exploits.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

Kali Linux is undoubtedly the best OS for hackers. It comes with best of built-in hacking tools so you should never worry about using a third party tool.

**WHAT KIND OF
HARDWARE DO
YOU USE?
ANYTHING
SPECIFIC THAT
HELPS IN YOUR
DAILY WORK?**

I believe in using the latest technology. There is no specific preference in the hardware but it should have at least 8GB RAM with minimum of i5 processor.

**DO YOU FOLLOW
ANY
METHODOLOGY?
DO YOU HAVE A
WORKFLOW THAT
YOU STICK TO?**

I do follow a methodology from basic to advanced that is reflected in my work. It basically starts from Footprinting and Enumerating and more. After this, I focus on vulnerabilities that can be exploitable and then comes attacking.

**FROM YOUR
EXPERIENCE IS
CERTIFICATION
IMPORTANT IN
HACKING CAREER?
IF YES, THEN
WHICH
CERTIFICATE IS
THE MOST
IMPORTANT ONE?**

Certification endorses one part of your achievement. However, if you are one of the best in your field then certification complements your higher achievement. I recommend EC Council certification for hackers.

**WHAT ARE THE
BIGGEST
MISCONCEPTIONS
ABOUT HACKING?**

The misconceptions of hacking is that anything is easily hackable and that nothing can be hacked. It is hard work and requires a lot of patience.

**WHAT ABOUT
ADVANTAGES AND
DISADVANTAGES
OF HACKING?
HAVE YOU
NOTICED ANY?**

Keeping the current scenario, the advantages of hacking are that one can fight against the terrorism and national security breaches. It also helps us to be aware of Black hat hackers and their techniques. Converting into Black Hat hacking proves to be very tempting.

**WHAT DO YOU
THINK IS THE
MOST IMPORTANT
THING TO
CONSIDER WHEN
PLANNING A
CAREER IN
HACKING?**

Basic knowledge of computer systems, coding are some physical attributes. Concentration, hard work and endurance are other attributes.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

There are no shortcuts to gain knowledge. I recommend a foundation should be laid through basic knowledge of Microsoft Windows, Linux, networking and then move to hacking.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

In hacking, nothing is hidden, everyone knows about everything; it all comes down to how a hacker uses his skill to get what they desire.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

In hacking, nothing is hidden, everyone knows about everything; it all comes down to how a hacker uses his skill to get what they desire.

WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

As a hacker one should remember to never to give up his/her research, because in hacking, research is one thing that will take you places and we all know after that, the sky is the limit.

DO YOU HAVE ANY ADVICE FOR OUR READERS?

I would like to advise that if you plan your career in hacking, make sure that all the basics of networking, Windows and Linux are clear. Because as Albert Einstein said, "any fool can know but it is important to understand."

REX AANTONNY

FOUNDER AND CHIEF EXECUTIVE OFFICER AT REX CYBER SOLUTIONS

Rex Aantonny is the Founder and Chief Executive Officer at Rex Cyber Solutions. He also the Chief Trainer at Hexter Lab. He has given Information security based training to Private & Gov. officials at Coimbatore ,Chennai & Kerala. He is best known as the Tamil Nadu Executive of HANS (Anti Hacking Anticipation Society) which is an organization helps to create awareness in cyber threats. Initially he started his career as Research Associate at Inter-science Academic Research Centre during his college days after which he has been trained from National Informatics Centre as a Project Trainee. He later joined 'Cadgraf Digitals' as Software Executive where he played a pivotal role in the company's desition making. He is also one of the IT LAW Enforcement Adviser for Brisk InfoSec.



**IF I
WANTED TO
BECOME A
HACKER WHERE
SHOULD I
START?**

The basics of the computer and its technology, like how a file is stored, what kind of protocols are involved and how they work; those are the vital things you need to learn/know, that's the only thing that will help you to gear yourself up.

**AT THE
BEGINNING,
WHICH IS MORE
IMPORTANT -
INDIVIDUAL WORK AND
SELF-IMPROVEMENT,
OR SOME KIND OF
FORMAL
EDUCATION?**

Self-improvement is more important, but at the same time, follow the current issues and learn, hold a basic degree. If you can show your skill in the game, the degree won't matter.

**WHAT ONLINE
COURSES, BOOKS,
OR RESOURCES
WOULD YOU
RECOMMEND TO
PEOPLE WHO WOULD
LIKE TO BECOME
HACKERS?**

Follow the current trends, white papers and researches in the domain you focus on, but make sure you are strong in the basics. Continuously try the bugs and vulnerabilities in your Sandbox or in your lab. Try with your friends, don't touch the digital space without proper docs/permissions, "don't be a prey for your Curiosity."

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

“Be a hacker don’t be a cracker.”

Control your curiosity.

Get proper permissions from your friends also to try your attacks.

In the beginning, they have no clue what kind of damage they can cause by the free tools they use, it could cause them lifetime prison. “Be conscious and play wisely.”

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

There is no formal training method for hacking, the concern is not the certificate, it’s the trainer! Be clear to choose your trainer.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

In terms of corporate view, it’s just a way of shortlisting.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

To be a hacker you must be ready to learn every day never ever hesitate to help out or ask new things of others or observe.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

PHP, shell scripts are my favorite. More than 75% of the websites in the world are made by PHP so that gives a potential opportunity to gain more.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

Kali, I mostly use as a plugin tool that I love to use always, I prefer it because most of the toys we like are combined there so I love Kali.

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT

Not particularly, but certainly I use social engineering mostly that burns my pain.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

It's a double edged sword, as we know already. In my personal experience, during the time I was a software executive in a reputed company, I often practiced some attacks and other worms to make my self confident/satisfy the security level in the network, but sadly that caused my employer to throw me out of the company. At the same time, that's the push helped me to learn a lot about hacking and starting my company in forensics.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

The only thing I can suggest is hold a ton of passion in your heart and keep practicing; no one can stop you. Learn everyday.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

I should have started in my school days, that's the thing I regret because I started during my college days.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

My failures which helped me to move up, keep that in mind and use that as a fuel to fire you up, that will never let you down to get another bounty.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

Money, as everybody, your day to day expenses, it will take time to get a bounty or enter into the perfect job you dream of or creating one. Be passionate and never give up.

DO YOU HAVE ANY ADVICE FOR OUR READERS?

The only thing I could suggest is be passionate and keep learning.



TOM MADSEN

IT SPECIALIST AT UNITED NATIONS

My name is Tom Madsen. I am 47 years old and I am working within the UN system currently. I have been working for the UN for almost 13 years, and have in that time been occupied with everything from custom development, to forensic investigations.

**WHY DID YOU DECIDE TO
BECOME A HACKER?**

Well, it pretty much happened by accident. I have always been interested in security, and how to manage it. The deeper I dug into the intricacies in the various tools that companies buy in order to protect themselves, the more I understood that if I was to manage and configure these systems securely, I had to understand how an attacker would go about circumventing these systems. This, in conjunction with me being put in charge of a couple of forensic investigations, made me aware of all the entertaining things that a hacker can throw resources at to learn, or break!

**IF I WANTED TO
BECOME A HACKER
WHERE SHOULD I
START?**

That is THE question, is it not? If you take a look at the various educational opportunities at the various educational institutions, you can now find plenty of both Diploma, Bachelor and Masters programs focusing on IT security. These educations will teach all of the basics involved in security, but they will NOT turn you into a hacker. That being said, they will help you along the road to becoming one. Being a hacker is as much about a specific mindset, as it is about the skills you possess. But having a formal education is only the beginning, you will then have to teach yourself things like reverse engineering and the intricacies of the platform on which you have chosen to become a hacker. These are things that a formal education will not teach. Yet.

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

That is very much an individual choice. I am a firm believer in a formal educational base, but many, many hackers are self-taught and have used the skills they have acquired by themselves to develop a very successful career for themselves. If you do not have access to an educational institution that offers a security related degree program, then you have no choice but to self-teach. Many universities are offering some of their programs as online education, so you can still attend a formal education from afar. So, take a good look at yourself. Do you learn best on your own, or in some form of organized teaching? If you have doubts, then try one or the other to find out which works best for you.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

The Hacking Exposed series of books from McGraw Hill are still, in my opinion, the best books for a beginning hacker. This series of books cover both general hacking, as well as hacking and forensics on specific platforms and operating systems. Some of the books are beginning to age a little, but the information contained within is still relevant, especially on the subject of researching the target before launching an attack.

<http://www.Pluralsight.com> has some pretty good courses on penetration testing, as well as on the various policy frameworks that surround security policies around the world. There are also courses that cover the content in many of the most respected security certifications from both organizations and vendors.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

If one looks around on various fore or IRS channels, then the question often comes from a beginner: Teach me how to hack, I do not want to learn programming, just the hacking. Well, I am sorry, but you **HAVE TO LEARN** how to program. It is a requirement. Do you have to be a full-blown systems developer? No, but knowing and practicing programming is a core skill that every hacker has to have. I know of no hacker who does not know how to code in at least different languages. Some in many more languages. Why is programming a requirement? In order to break code, you have to understand how that code gets written, and how the specific language handles things like memory and the stack. And, as you move along in your career as a hacker, you will want to automate as many of the processes as you can, something that again needs programming skills.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

There are many of these, but not all of them are equally good! Some of them are even trying to scam the visitors to these forums, so if you go looking for some of these, please be careful. Many of the best forums are located in the deep web, or darknet. Accessing these requires a Tor browser, and again, care should be shown when going there!

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

I personally use two different websites for news on security. They are: <http://news.hitb.com> and <http://www.infosecurity-magazine.com>. Both of these websites organize conferences in addition to the various news. For hitb, the conferences happen in Asia and Europe. Infosecurity magazine organizes only in Europe. All of the other bit IT news sites are, of course, covering security related issues and incidents as well, so it can be worthwhile to subscribe to their RSS or Twitter feeds as well.

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

No. I personally believe in formal education, but you will know best what works for you. So try different approaches to find the way that works for you. Just remember, programming is a required skill for a hacker!

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

I know that the EC Council have changed the training requirements in recent years, but back when I took this certification, the training was basic, and the examination a breeze. That being said, it looks good on a CV!

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

Curiosity and thinking out of the box. Curiosity because you will have to continually acquire new skills in order to keep your skill set current. Thinking out of the box because a novel solution is often the only way to bypass some gizmo or system in place to protect against an attacker.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

The one that YOU like best. There is a plethora of languages out there, but I recommend that you learn at least one language that can be used across all platforms, like Linux, Mac and Windows.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

Python, because I can use it across platforms. This in addition to the

modules designed for numerical computation and mathematics makes this my current favorite as I am currently working on a Bach. Sc. in Mathematics. In other periods of my life, the favorite language was Perl or C++. Trust me when I say, that your favorite language will change over time as well.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

Kali Linux is my main go to platform for any hacking or research I do. Kali is a rolling Linux distribution, created and maintained by Offensive Security. Kali comes with every hacking tool imaginable, and you can install what you do not see in the menu yourself. That along with the fact that all of the books promising to teach you hacking, are utilizing Kali as the underlying tool of choice. No matter whether you need a tool for forensics or reverse engineering, a tool exists within Kali.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

My platforms of choice are Windows and Linux, so the hardware is x64 from Intel. If you are hacking Mac machines, the best way is to use a Mac for the purpose. I dislike the anal level of control Apple exhibits over what you can install and do with the systems, so I pretty much ignore Apple as a platform. As you progress in experience and skills, you will notice that you will need more and more RAM in the machine you use. This is because you will find it MUCH easier to install the systems you are researching in virtual machines rather than on physical hardware. The more virtual machines you have running, the more RAM you will need. The number of cores on the CPU are less important than the amount of RAM in the machine you use.

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

Yes! No matter if you are hacking by yourself, or as part of a team, some form of methodology is essential. All of the modern infrastructures are of such complexity that without some structure in how you proceed, it will soon result in you getting lost in all of the data you collect on the systems under attack. If you are part of a group conducting a penetration test for a customer, the customer will expect a report at the end of the project. Without a process in place, the final report for the customer will be a challenge to write!

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Well, the definite answer to this question is: it depends. Which area of IT security do you find interesting? Is it penetration testing? In which case, you should look at the certifications from EC Council, Offensive Security or GIAC. Are you mostly interested in security on a specific platform, like Cisco? Then you should look at the security related certifications from there. And so on. The one certification I do want to recommend you get is the CISSP from ISC2. Not because it's all that relevant to a hacker, but because when you apply for a job, the CISSP certification will get you through the HR firewall. Let's say there is a job opening. There are 100 applicants for the job, and the HR person has to do the long listing of candidates for the job. Who do you think the HR person will long list? Correct, the ones with the CISSP certification.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

It used to be an honorific, to be called a hacker. Now, if you present yourself as a hacker, the relation that immediately comes to mind in the listener is a criminal. Which can be true, no doubt about it, but not necessarily.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

Advantages? Your workday consists of playing ☺ Disadvantages, are the increasingly complex legal minefield that gets more and more complex as time goes by. Some things may be allowed in one area of the world, while being illegal in another. As you learn how to break or bypass stuff, make sure you learn using virtual machines on the Internet. Any traffic from you that might be viewed as malicious can land you in legal hot water nice and fast...

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

Choose your platform! By that I mean, which area do you want to specialize in? Is it Windows, or Web applications, or something else? You might as well resign yourself now to the fact that you will not be able to know everything about everything in the area of security. So if you want to be successful in hacking, the art of limiting yourself will help you along the way, much as I am sure this sounds boring 😊

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

As mentioned in the beginning, I kind of fell into the hacker role by accident. I was a software developer, and tester initially. So, my knowledge of networking and the protocols in the TCP/IP suite was pretty much non-existent. I seriously doubt anybody today even considering a career in hacking would do so without this particular knowledge already in place.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

Hmm... I do not know if anybody learns this particular bit, but I have found the integration area between different systems an area with rich pickings for a discerning hacker. For instance, if your database is running on a Unix system, while the web application runs on a Windows server, ignore the front end initially, and focus on the areas of the application that exist between the two platforms.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

Access to reliable knowledge. Information on hacking and learning resources are all over the Internet today, but way back when, this kind of knowledge was not publicly accessible. You had to know someone who knew someone, for access. Now there are books and websites dedicated to teaching how to break stuff, as well as to protect the same stuff from being broken. If I had not already told you how old I am, you would be able to guess based on these statements ☺

WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

Have fun!! As soon as you begin to get bored, you will find that the creative thoughts will slowly, but surely, disappear.

MIRIAM WIESNER

PREMIER FIELD ENGINEER FOR SECURITY



My name is Miriam Wiesner and I'm from Germany. I have worked as a systems administrator, as a programmer, as a system engineer and as a Consultant for Security. In February 2017, I will start at Microsoft as Premier Field Engineer for Security. I hold certificates such as CEH, MCSA, ITIL and TrendMicro Certified

Professional for Deep Security. In my spare time, I write articles for my blog miriamxyra.com and I'm also shooting video tutorials to explain IT Security issues in an easy way. Yes, I totally love IT security. ;-)

WHY DID YOU DECIDE TO BECOME A HACKER?

I never decided it. Computers always were a thing I was passionate for, so I started early when I was a child. I taught myself programming at the age of 8 – 10 years and wrote little QBasic games like “Kill the rabbit or the rabbit will kill you” and animated the graphics in ASCII art. Hacking was something cool to me, only the word sounded so illegal to me, I did not have the guts to learn stuff like that “officially” on the internet. But I read everything I could legally find about hackers and also bought books about it at local bookstores. During my apprenticeship, I realized that “hacking” was nothing bad, since it only meant being creative with given circumstances.

IF I WANTED TO BECOME A HACKER WHERE SHOULD I START?

Most people are starting with one of the following sections:

- System Integration
- Programming
- Network

Choose the most interesting topic for yourself to begin with. Never stop learning.

**AT THE BEGINNING, WHICH IS MORE IMPORTANT -
INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR
SOME KIND OF FORMAL EDUCATION?**

In my opinion, it's more important to learn by yourself. Formal education can be helpful, too, but if you want to know more than common standards, you should be motivated to find things out on your own. It's hard but it's worth it!

**WHAT ONLINE COURSES, BOOKS, OR RESOURCES
WOULD YOU RECOMMEND TO PEOPLE WHO
WOULD LIKE TO BECOME HACKERS?**

My favorite online resources are Cybrary (cybrary.it) and Haking9.

Cybrary contains a lot of free courses and tutorials. And if you created content by yourself, it's also possible to release it there on Cybrary oP3N.

In a regular manner, Haking9 releases new online magazines with interesting articles from specialists and they also have really cool online courses.

A great book I also read: "Hacking - the art of exploitation" written by Jon Erickson. It is not an easy lecture for beginners, but it really helped me to understand difficult topics.

Also learn about Google Hacking/Dorks. I once read "Google Hacking" by Johnny Long but there are also free resources on the internet.

What's also a great resource to be informed about hacking and security is Twitter - if you follow the right accounts. You read about important flaws or other topics first, even before popular magazines publish articles about it.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

The biggest mistake a beginner can make is to think that learning hacking is easy and not time consuming. Most people quit if they can't see results quickly.

If you really want to learn hacking, motivate yourself to keep on going. If you don't understand the desired topic, learn about it again and again until you know how it works.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

Again I recommend Cybrary and Twitter. On Cybrary there's a community of people obsessed to learn all about infosec.

On Twitter there are many active hackers from all over the world. After a while you will find your own community to connect to.

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

Best resource for me for keeping up to date: Twitter! Just as I said before, you will get your information faster than from news pages.

Other resources are thehackernews.com, the CVE security vulnerability database (www.cvedetails.com) or the exploit database (<https://www.exploit-db.com>).

In Germany, there are also newsletters from the "BSI Bürger-CERT" service, you can subscribe to. Those are provided by the official German office for internet security. If there is a new warning released concerning a special browser or programs, like Adobe PDF reader, you get the info quickly per email.

Maybe there is also a service in your home country similar to that.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

I got certified as CEH, so yes, for me it was an important part. I taught myself everything I know about hacking in my spare time. When I registered for the CEH exam, it was also a verification for myself if I understood everything I learned.

If you achieved CEH and entered it on social networks like LinkedIn, it is also easier for headhunters when they are looking for candidates for special hacker focused jobs.

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

Well, that depends on what you want to become. For my part, I got certified as a Certified Ethical Hacker (CEH) and one of my next big goals is the CISSP certificate.

There are also some product certifications you may want to achieve that can be also helpful for you.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

Patience! You will fail several times, patience is the one skill that keeps you from quitting.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

Python, C, C++, C#, Assembler. But you should also learn scripting languages, like JavaScript, PHP, Perl and Bash, and also markup languages, like HTML/XML.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

I have no preference for one specific language. To understand how memory declaration works, C languages are great (the programs in my video tutorials about buffer overflow were written in C++). C# is better than C or C++ to produce safer code and Python is easy to learn and good to read.

WHAT TOOLS DO YOU USE?**WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?**

Oh there are many tools, it depends on what your goals are. For website analysing hacking Burp Suite is a great tool. For capturing and analysing network packets I prefer wireshark. And of course many standard tools like nmap, metasploit, medusa...

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

There is no "best" OS in my opinion. It's the OS that fits best for you. For my part, I like all OS'. I used Windows, Linux and I also installed Metasploit and other tools on a Mac.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

Nothing specific. But if you want to host several virtual machines, it is not bad to have at least 16 GB RAM and an appropriate processor.

**DO YOU FOLLOW ANY
METHODOLOGY? DO YOU HAVE
A WORKFLOW THAT YOU STICK
TO?**

Reconnaissance / Information Gathering -> Port & Vulnerability Scanning -> Exploiting / Gaining Access -> Maintaining Access -> Report (Or clearing tracks for the bad guys).

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Many employers are looking for certified employees, so yes, depending on where you want to work. I think the most important certificate is the CISSP because it covers all sections of security.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

No, I will NOT hack your friend's facebook account!!! :D

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

Advantages:

- People are very impressed when they find out.
- You understand technical contexts easier.
- You are looking for the easiest solution in every aspect.

Disadvantages:

- People fear you might hack them.
- “Can you please hack the facebook account of my friend?!?”

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

In the beginning, figure out what you want to become and what your goals are. Don't lose track. Keep your motivation to never stop learning and to explore complex issues.

Think outside of the box to solve difficult puzzles. There is not always a predefined way you have to go.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

I wish I'd had more interest in network and protocols earlier.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

Phew, hard question! But I think IPv6 is a protocol only few people know by heart. I think it will be soon important to master it.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

People that tell you that you can't do it.

WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

Nothing is unbreakable, be patient.

**DO YOU HAVE ANY OTHER STORY
RELATED TO HACKING THAT YOU
WOULD LIKE TO SHARE WITH US?**

When I dated my boyfriend, we wanted to book a table in a restaurant. Unfortunately, this restaurant was very popular, so it was very hard to get a table for the same evening. They also had a online form to book a table. But you had to book at least two days in advance. Since I wanted the table for this evening so badly, I investigated and found out that the code was not secured on the server side. Bingo! I changed the JavaScript blocker so that I could book the table anyway. Two hours later an employee of the bar called me. He was so sorry that they did not call me back by now and - of course! - they still did have a table for us. I guess he thought that we really booked that table two days ago. Pretty easy thing, but we got a table for the same evening and my boyfriend was so impressed, he is still bragging about the day I hacked us a table.

**DO YOU HAVE ANY ADVICE FOR
OUR READERS?**

If you doubt and fall, stand up and move on. Never quit, believe in yourself.

SHANE RUDY

SENIOR SECURITY CONSULTANT

My name is Shane Rudy and I've been professionally hacking since 2008. (employer undisclosed)

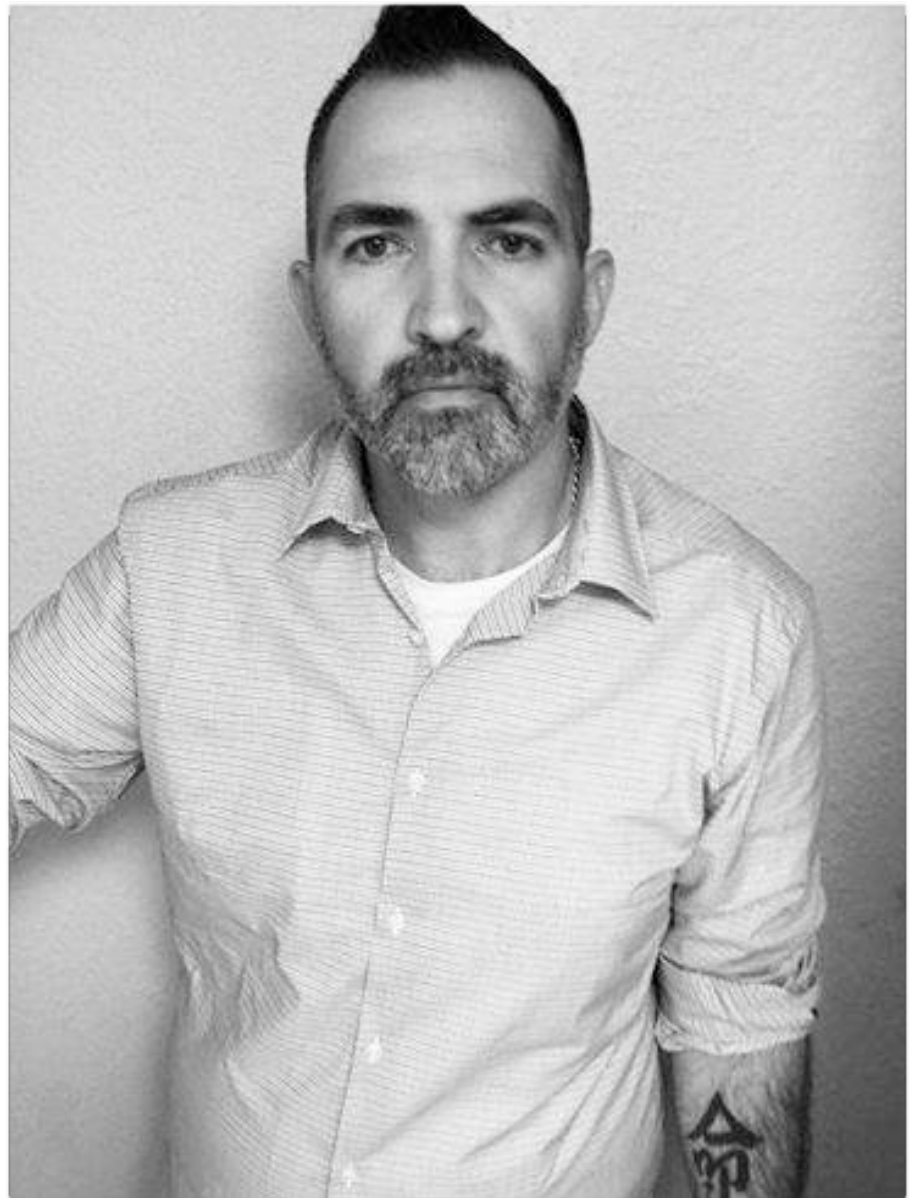
Certifications: CEPT, CPT, CEH, ECSA, RCSE, MCITP:EA, MCSA, MCTS

Email: ara1212@gmail.com

Twitter: @H011YxWood

LinkedIn:

<https://www.linkedin.com/in/about-shane-rudy>



**WHY DID YOU DECIDE TO
BECOME A HACKER?**

For me hacking and cyber security was the one thing within this huge world of information technology that always kept me interested and I never got bored with. I was a very rebellious youngster growing up and always looked for ways to bend or break the rules. When I began my career in IT, I was very intrigued with the bad guys who would break into computers by bending or breaking the rules of protocols, systems and software. Being who I was, this became a natural progression for me and I started tenaciously pursuing it.

**IF I WANTED TO BECOME
A HACKER WHERE
SHOULD I START?**

Well, that depends really on your current experience. I personally believe the best hackers have very strong and diverse technical backgrounds, as well as the ability to work hard and figure things out on their own. I would learn as much as you can about Hardware, Operating Systems such as Linux, Windows, Networking (OSI Model), Programming and Web Applications just for starters. I think it is better for people if you have a strong foundation. I always tell people, you don't have to know it all and you won't, but you must have the ability to be able to research, understand, and apply what you have learned. Next, you must be able to explain it to others. If you can't, you haven't learned it.

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

I think the biggest thing that employers are looking for these days is grit. Grit is one of those qualities that you must possess in order to work and succeed in the Cyber Security field. Second, I do believe a formal education, like a graduate degree, is very important. Truth be told, I do not have a degree, but I have had amazing experience, worked very hard while supporting a wife and three young children at the time just to get into the Information technology field. That was me and I am now 42 years old. For young people it's not that way anymore. I would tell people to get a degree, I would also tell them to do it on their own and not ask their parents for the money. Instead, earn scholarships and work to pay for it on your own. I say this because the top employers in the cyber security world are looking for talent that has proven that they have worked hard and for the younger generation it is tough for them to get a job because they lack experience. This is one way that you can show your prospective employer that you're different than the rest. For hacking in general, you learn by doing, so learn and do as much as you can while you're putting yourself through school, or if you're already in Information technology, start down a certification course like the CEH just to see where you are at and then move onto more challenging programs, like the OSCP, IACRB:CPT. Eventually, you can accomplish more advanced certifications, such as the OSCE or IACRB:CEPT, which are considered expert level certifications. In this field, the learning never stops.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

The list is long and exhaustive, however, I will try to narrow it down some based upon my experience and what I am doing currently. There are many facets of hacking and newer ones, such as IoT and mobile, are something I'm looking forward to learning!

COURSES:

If you're new, start with your CEH from EC-Council, just to get familiar. Once you have done that and think you understand go for the OSCP, IACRB:CPT.

ONLINE RESOURCES:

There's a plethora of great online resources to learn so much that it is often overwhelming so don't be surprised if this list overwhelms you ;) I will try to break it down a little.

ONLINE LEARNING AND COURSES:

- Pentester Academy: At \$40 bucks a month, this site is great for beginners and pros alike. New content is always added and it's just a great place to start messing around, as well as learning new concepts, tools and skills. www.pentesteracademy.com
- Udemy: For learning programming, which is an essential skill needed to move from script kiddie to hacker. <https://www.udemy.com>
- Code Academy: This is another great site where you can learn for free and it's great for beginners.
- VulnHub: Looking to test your skills? Download one of the hundreds of vulnerable virtual machines on this site and go at it. All VMs come with walkthroughs if you get stuck and they range from beginner to just plain crazy difficult.

BOOKS:

I'm not going to spend a lot of time here because the list is just too exhaustive and tech changes fast, however, there are some staples that every hacker should have, in my professional opinion.

- **Learning Penetration Testing with Python by Christopher Duffy.** This is hands down one of the best books on penetration testing and Python. This book is different and isn't like the others that I have read. It's 5 stars and it's a must have.
- **Hacking The Art of Exploitation 2nd Edt. by Jon Erickson.** This book is dated, however, I personally believe it was one of the best books ever written on understanding system exploitation and is a must read for any aspiring hacker.
- **The Web Application Hacker's Handbook 2nd Edt.** This book is also dated, however, it is still the defacto guide to learning about web application vulnerabilities and I highly recommend it. I would complement this with another book titled: The Browser Hacker's Handbook.
- **The Hacker Playbook editions 1 and 2.** This is one of the best books on pentesting that I have seen in a while. Wonderfully written, short and to the point. Pick up both editions.
- **Windows Internals 7th edition.** These books discuss Windows system architecture, processes, threads and memory management for Windows systems.
- **Windows Server 2008/2012/2016 Server Inside and Out books.** These books are great for learning about Windows Servers quickly as well as Active Directory and Windows Domains.
- **The Red Team Field Manual:** Want to get better in the shell? Pick up this book.
- **TCP/IP Illustrated:** Everything you ever wanted to know about TCP/IP.
- **The Shellcoder's Handbook:** Now dated but another useful resource for learning Exploit/Dev. Required mandatory reading for the IACRB:CEPT certification.
- **Assembly Language Step by Step 3rd Edt.** Not light reading by any means but a great resource for learning x86 assembly.

ONLINE RESOURCES: (A FEW OF MY FAVORITES):

- Read the RFC's for any protocol you're interested in. You will learn how it works and in hacking, you have to know how stuff works.
- Twitter: Twitter is one of the best resources for information within the InfoSec Community.
- Books in PDF. Do a little Google hacking and chances are you'll find the book in PDF you're looking for.
- SS64 Command Line Reference: <http://ss64.com>
- SANS Windows CMD Line Cheat Sheet:
https://www.sans.org/security-resources/sec560/windows_command_line_sheet_v1.pdf
- *Nix Cheat Sheets:
<https://www.cyberciti.biz/tips/linux-unix-commands-cheat-sheets.html>
- OWASP: https://www.owasp.org/index.php/Main_Page
- https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet
- PortSwigger Blog: <http://blog.portswigger.net/>
- XSS Cheat Sheet: <https://gist.github.com/sseffa/11031135>
- Tons of stuff here: <http://pentestmonkey.net/category/cheat-sheet>
- SQLmap Wiki <https://github.com/sqlmapproject/sqlmap/wiki/Usage>
- SQLmap User Manual (A great read):
<https://raw.githubusercontent.com/sqlmapproject/sqlmap/master/doc/README.pdf>
- HarmJoy cheat sheets on popular tools: <https://github.com/HarmJoy/CheatSheets>
- Windows Exploit/Dev:
https://github.com/endo/awesome-windows-exploitation#windows_heap_overflows
- Post Exploitation: <https://github.com/mubix/post-exploitation>

- Attack Research: <http://carnal0wnage.attackresearch.com/>
- Corelan Team: <https://www.corelan.be/>
- Password Cracking Cheatsheet:
https://www.unix-ninja.com/p/A_cheat-sheet_for_password_crackers
- Hashcat Wiki: <https://hashcat.net/wiki/>
- Crypto Cheatsheets:
https://www.ethical-hacking.de/pdf/Crypto_Cheat_Sheet-Best_Practices-en.pdf
- Networking Cheatsheets: <http://packetlife.net/library/cheat-sheets/>
- Nmap Reference Guide: <https://nmap.org/book/man.html>
- SANS Reading Room Library: <https://www.sans.org/reading-room>

As far as learning Linux, sure you could read a book or you could install it and dive right in like I did. I'm mainly a Debian guy but Arch is a fantastic distro as well. I prefer Ubuntu or Kubuntu because of the support and their strong knowledgebase. As you get into hacking, you will learn Linux. It's just the natural evolution of becoming a hacker. Kali Linux is a fantastic Linux distribution for penetration testing, however, I do not run it as my main operating system but instead run it in a virtual machine if I need it. I would advise this type of setup.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE ?

I think one of the biggest things is a lack of patience. Learning takes time and sometimes if you're struggling, get up and take a break for a while and come back to it. I can't tell you how many times early on in my career that I refused to do this and it ended up costing me even more time because I began to have tunnel vision after a while. This stuff takes time to learn and some topics may come easier to you than others but just be patient with yourself.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

On the Internet I typically follow people and cyber security companies on Twitter. Twitter is a great resource for new information within the community. I would also try to find local meet up groups in your area where you can network with others and learn from them. I would also advise going to some conferences if you can. (DefCon, Bsides, Backhat etc.)

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

I personally like SANS Newsbites, Dark Reading, Carnalownage Attack Research, Motherboard, Krebs on Security and the Cryptogram and there are tons of others. The list is too long!

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

If you have previous information technology and Linux experience, I would go with Offensive Security's OSCP or IACRB:CPT, both are entry level hands on certifications.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

I think it is a good overall certification to get if you are completely new to hacking from a high level viewpoint and have zero knowledge of hacking methodology. The CEH is a multiple choice exam and it is not hands on like the OSCP, IACRB:CPT and others. If you decide to do your CEH, I personally would recommend a class over self-study to get initial hands on experience if you can. Classroom environments can also be beneficial for asking questions and interacting with other students who may or may not have experience just like you.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

I wouldn't really call it a skill but moreover a character trait, and that trait would be tenacity. This job requires at times, long hours banging away at a network, host or an application etc. and not giving up. Even if the customer that I am testing doesn't have much exposed I always try to find something. Always try to find something!

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

In my opinion Python.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

Personally, I like Python for tool and exploit development. For starters, it's an easy language to learn and second a lot of talented hackers write code in Python because you can do just about anything with it and there is a ton of support for it available, so if you're struggling with something, more than likely you can find someone who can help you quick and easy.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

There are so many and the list is always growing but I will list a few that I use on a regular basis. I will break this down by the areas I have the most experience with:

Phishing: I write my own code for this typically.

Phone Social Engineering: Spoofcard

Reconnaissance: Recon-NG, Discover Scripts from Lee Baird and Spiderfoot

Scanning: Nmap, Nessus and Metasploit Auxiliary Modules

Web: Burp Suite Professional, Beef, Nikto, Nmap, DIRB, SQLmap, WPScan, CMSmap, EyeWitness as well as custom scripts I have written.

Hash Grabbing: Responder or Invoke-Inveigh

Internal Testing Tools: Honestly, this really depends on what I run into and the type of environment I am in but here are a few that I use to get a lay of the land: Nessus, Responder, Invoke-Inveigh, Nmap, Metasploit, CrackMapExec, Powersploit, EyeWitness as well as my own scripts and tools. My favorite tools are the ones that make your life easier. I'm currently writing one in Python that will help me automate my methodology when performing penetration testing and it's been very rewarding and fun.

Password Cracking: Hashcat with Nvidia Graphics Cards.

Wireless: Kismet, Aircrack Suite, Reaver, Pixie and a WiFi Pineapple.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

Linux and I use Kubuntu for my base operating system. Kali is great as a tool running in a VM on VirtualBox.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

I have a laptop for daily work that runs Kubuntu, a password cracking box that I built with Nvidia GPU's, specifically the GeForce 750Ti Series. Affordable cards and great performance.

For wireless hacking, I use the ALFA Model: AWUS036NHA card with the Atheros chipset. Stick to Atheros based cards. For phishing, I typically run three Ubuntu servers; one runs Apache2 with PHP for Virtual Hosting and malicious payload hosting out on the internet, the second sits on the internet as a smarthost and acts as a relay that sends the mail, and the third runs Zimbra on the internal network, which I use to create mailboxes and perform Man In The Middle of the Email attacks. Zimbra is free and it has a great graphical user interface. I also like to have a public Metasploit box running on Ubuntu server. Hostvirtual hosting is great for this (no firewall rules to mess with) and it really comes in handy at times. They also allow you to create reverse PTR records for your mail server in your panel!

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

I prefer the Penetration Testing Execution Standard (PTES) as an overall methodology for performing engagements. I try to stick to the following:

- Information Gathering: Reconnaissance and Open Source Intelligence Tools to gather information about the target (Phishing or Social Engineering may or may not be involved depending on scope)
- Enumeration: Discover hosts, services, versions and web applications
- Identify Vulnerabilities using automated and manual testing and attack methods
- Determine attack vectors and planning
- Perform exploitation
- Perform privilege escalation, data exfiltration
- Pivot to other systems looking for sensitive data or establishing control over the network and users
- Establish persistence on the network to test customer's awareness and defenses
- Report all findings

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

I believe certification is very important for development as well as career and personal growth and I recommend certifications that require actual hacking, like the OSCP, OSCE, IACRB:CPT and IACRB:CEPT, because they demonstrate that you are a highly capable individual. Multiple choice exams are not enough and people cheat on them. The four that I have listed here are solid certifications from beginner (OSCP, CPT) to expert levels (OSCE, CEPT) where help on the internet is NOT available. You must know what you are doing.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

I think the biggest misconception has to do with the negative image that the word hacker creates. Hacking is necessary because the evil guys are doing it, and nation states and governments are doing it. We no longer live in an age where we can pretend that our data is completely safe from anyone or that our systems are impenetrable. Hacking is a necessity and it is required to keep our systems secure and our data safe from evil people. I always ask customers: Would you rather me find your vulnerabilities and exploit them first and show you how to fix them? Or would you rather your competitor or some other evil entity find them first exploit them? It is our job to educate and to hold vendors, as well as entities, accountable for keeping systems secure and our data safe. Hackers do amazing work every day and the majority of us are curious, dedicated and caring individuals.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

I always like to quote Stan Lee creator of Spiderman because when it comes to hacking it is quite the paradox: *“With great power comes great responsibility...”* Meaning that we know more than you could imagine about computers. We are doctors of the computing world and we work on computing immune systems, however this is a craft that can have grave consequences for you personally and professionally if you’re careless with it.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

The many hours it takes to learn and do this job as well as being successful. Will your family and friends support you? This job takes a lot of time. My laptop and phone have become extensions of my physical body.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

I wish I would have learned deeper programming concepts sooner. Programming is one of the quintessential things you need to know to be a hacker. Learn a language like Python, you won’t regret it.

IS THERE ANYTHING THAT YOU KNOW OF THAT ALMOST NOBODY LEARNS, BUT IS INCREDIBLY USEFUL?

I have had the privilege of being a system's engineer who has implemented, managed, performed troubleshooting and fixed many different types of technology during my journey to becoming a hacker. It has allowed me to learn so much and gain real hands on experience with the technologies I attack and perform assessments against on a regular basis. It also has allowed me to have a strong background for teaching clients how to design and architect secure networks.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

Myself. I didn't go to school for computers. I wasn't even interested in them in college. I hated school and was a troubled kid. Instead, I went to chef school and was a chef and worked in the food service industry for around six years. It wasn't until I was in my late twenties and had a wife and three kids on a single family income when I decided to change my stars and landed my first helpdesk job years ago. There was a lot to overcome for me. I never thought I was smart or good enough and I would let fear and doubt sink in but I kept at it, kept trying, kept failing but kept learning and realized that I had what it takes and, eventually, I got to where I am today. Never give up on your dreams. I am living proof to my family and friends who deeply know me that they come true. John Wayne once said, Courage is being scared to death and saddling up anyway. There will be times when you're scared or think that you won't get it or can't do it, but if you love it, keep at it. If you fail, keep trying.

WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

Be humble.

DO YOU HAVE ANY OTHER STORY RELATED TO HACKING THAT YOU WOULD LIKE TO SHARE WITH US?

Remember, in hacking as well as life, all failure means is that you just learned how something didn't work. That's all it means.

DO YOU HAVE ANY ADVICE FOR OUR READERS?

My advice would be to work hard, and remember to be patient. Learn as much as you can and do it by hands on learning. If at first you don't succeed, try try again. Start networking with other hackers. Don't be afraid to fail! In hacking we get used to failure because we're constantly learning and trying to prove out how things work or don't work and how they can be exploited so naturally, failure is something you get used to and you eventually overcome it and succeed and it's the greatest feeling in the world. Remember that while this is a very demanding and stressful job, it is also very rewarding and fun as well as downright hilarious at times. People will amaze you when you social engineer them. You will own 80% of a large company just by sending them an email or discover a oday and it is legendary. You will eventually pop your first shell or own a couple of driver's license servers like I did for an entire state for two days.

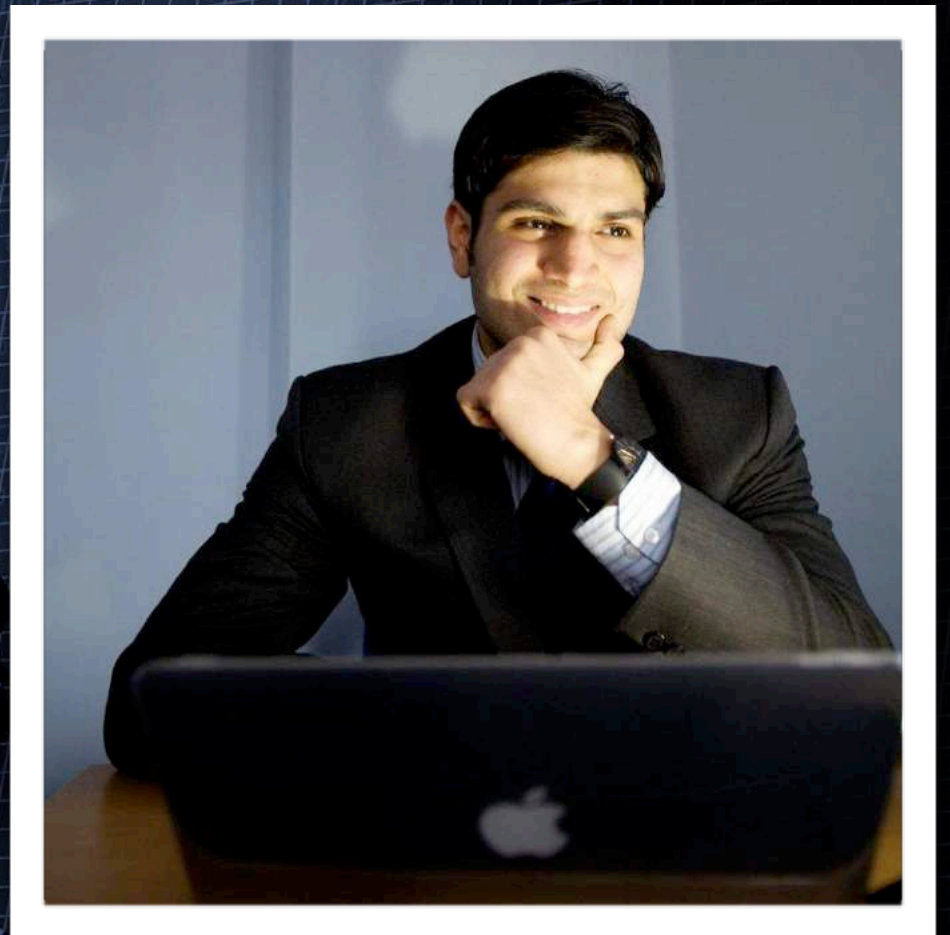
So when the day comes that you become a pro, be humble and be a thoughtful mentor and a responsible security professional to those who want to learn from you because the information security talent pool is sparse and we need to do a better job of educating our young people. Most of all don't be afraid to be passionate and to express that passion for what you do to your employer and your clients. That is the one thing that I have heard time and time again from my clients and fellow coworkers is that they know how passionate I am about what I do and they trust me because they know I love this stuff and that makes me good at it because I love working hard to be good at it. It will benefit you in many ways and separate you from your competition. In closing if this is something you really want to do and you dream about it like I did many moons ago, but you doubt yourself or how you're going to get there, just remember I used to be a chef...

SULEMAN MALIK

CYBER SECURITY ANALYST

M.Suleman Malik is a dedicated and resourceful computer professional with 9+ years extensive learning experience in Cyber Security, Penetration testing, Security researching, recovering and maintaining a diverse range of hardware and software. He is based in Leeds, UK and is currently a full time student studying Computer Forensic & Security. He is an I.T. security professional and has a keen interest in Ethical hacking/Pen-Testing, social engineering, security researching and developing exploits.

<https://www.ted.com/profiles/5201069>



WHY DID YOU DECIDE TO BECOME A HACKER?

I have been doing this all since I was a kid and started learning from internet sources. At a very initial stage, I made low level software that was protected with a password and then I broke into it and that encouraged me to build my figure in that particular field. I couldn't even afford to pay thousands of dollars to the website that provides the ethical hacking course. But I had an idea and I went through that idea. The idea that I discovered was finding the syllabus of CEH certification and OSCP certification. Once I got the syllabus, I started reading the table of contents from the syllabus and searching each line from table of contents in Google search. Many experts have uploaded videos and blogs about that content and all I needed to do was read the blogs and watch the videos to understand how it works. Through that way, I learned all on

IF I WANTED TO BECOME A HACKER WHERE SHOULD I START?

To become a hacker, you should start from independent learning. I would recommend you start your learning from web application penetration testing. It will make you stronger to understand about client side and server side attacks. You will also learn the common web apps vulnerabilities and how to exploit them. There are some pentest virtual machines that are freely available online and will help you to understand the vulnerabilities. The few popular VM machines are Metasploitable, Dojo web, Pentest Lab and Hack Labs. You can download them and start learning from these machines, as they are made for beginners.

AT THE BEGINNING, WHICH IS MORE IMPORTANT - INDIVIDUAL WORK AND SELF-IMPROVEMENT, OR SOME KIND OF FORMAL EDUCATION?

University/college education is important but 70% relies on individual work and self-improvement. The era we are living in today is a dream coming true. Everything is available on internet. So you should start learning from internet sources and it will help you at your initial stage. So keep in your mind that individual work is more important than anything else.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

If you want to know about me, I never read any books. I would recommend that you download the VM machines that I mentioned earlier. Use those VM to figure out how it works. These VM machines are vulnerable and especially

made for those who want to learn and test their skills. Download them and start learning from these machines. All instructions will be given there, like what type of vulnerability is this and how would you exploit this type of vulnerability. When you understand the vulnerability then you can test your skill there and feedback will be given on the spot. If you are keen to learn more, I would recommend that you apply for CEH certification first and then go for OSCP course.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

Beginners are always confused because they don't know where they should start. This is a vast field and if you want my opinion, I would say start it from web penetration as it will help you to kick start your learning.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR INTERESTS?

I can't say anything about the hacker community, but I'm connected with top hackers on LinkedIn and Facebook. Try adding experts from LinkedIn. It's much easier to connect via LinkedIn to get yourself up to date.

WORKING IN CYBERSECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

I am following the official verified twitter account @TheHackersNews. They will keep you up to date with the latest news.

<http://thehackernews.com/>

IS THERE ANY FORMAL TRAINING PATH THAT YOU WOULD RECOMMEND, ABOVE OTHERS?

No/No idea apart from the above. All those that I mentioned above are the best of my knowledge.

DO YOU THINK THAT CEH IS AN IMPORTANT PART IN HACKING CAREER?

Yes, CEH is for beginners. This course will help you to understand the basic fundamentals of ethical hacking. This course includes the basic of web application hacking, computer hacking, connecting proxy, information gathering, scanning and exploitation.

WHAT IS THE MOST IMPORTANT SKILL TO HAVE AS A HACKER?

The two most important skills to have as a hacker are understanding and research skills. If you understand the communication protocols and how they work, you can do a lot. If you have command over various computer languages, that will also help you to understand and manipulate the code in order to get the desired result. No one can become a hacker within a week or month. Obviously, you need to spend your time on learning and researching these things.

WHAT IS THE BEST PROGRAMMING LANGUAGE FOR HACKING?

There are a few programming languages for hacking, like Python, Ruby, Bash, C and Java, etc. If you have command over one language, as I mentioned above, you can write your own hacking tools and exploits.

WHICH PROGRAMMING LANGUAGE DO YOU PREFER AND WHY?

I prefer Python because it takes much less time to develop. Python programs are typically three to four times shorter than the other Java or C programs. There are many good reasons if you go through Python. As you can see, nowadays, many exploits and tools are written in Python. I would recommend Python instead of any other programming language.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVOURITE HACKING TOOL AND WHY?

I use many tools when carrying out the test. There are a few stages of hacking where we use different tools. For example, nikto, nmap, zap, retina scanner, maltego, etc. Tools help in the stage of information gathering, whereas Metasploit console, which is a built-in platform helps the hacker to

exploit the vulnerability and cover a few more stages including post exploitation and maintenance access. My favourite tool is netcat. Netcat is a small tool but worth more than any other tool. This tool is also known as the TCP/IP Swiss army knife.

Hardware doesn't matter. All you need to have is a working system.

DO YOU FOLLOW ANY METHODOLOGY? DO YOU HAVE A WORKFLOW THAT YOU STICK TO?

There are a few different methodologies that are use in vulnerability assessments, e.g. NIST, OSSTMM, OWASP, etc. But I stick with the workflow that I made for my convenience.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

The best operating system for hacking is Kali Linux. Kali Linux is especially designed for penetration testing and all the tools that I mentioned above are available in Kali Linux. There are bundles of other security tools that helps during the vulnerability assessment.

WHAT KIND OF HARDWARE DO YOU USE? ANYTHING SPECIFIC THAT HELPS IN YOUR DAILY WORK?

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Yes, certifications are important. I would recommend OSCP, CEH and OSWE.

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

There is a lot of difference between hacking and ethical hacking. If you discovered a vulnerability and exploit it for financial gain, that is illegal and you will end up in prison. If you report the vulnerability you discovered, that is legal even though the vendor will acknowledge you. This is the best advantage to get acknowledged from the top vendors.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

Learn as much as you can. It's a massive field. So, keep practicing on those VM that I mentioned earlier. You will face a lot of obstacles, but don't lose your strength and keep practicing. This is how we become hackers.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

I started learning from system and network hacking but later I realised that I should have started from web hacking because at that time, there were a lot of web vulnerabilities and vendors were acknowledging researchers for reporting security vulnerabilities.

WHAT IS THE GREATEST OBSTACLE YOU HAD TO OVERCOME TO GET WHERE YOU ARE TODAY?

As I said before that I couldn't even afford to pay thousands of dollars to learn ethical hacking and that was my biggest obstacle. I learned all on my own. And today I'm a professional in web hacking, network penetration, etc. I have been acknowledged by many top companies including Microsoft, Intel, eBay, Blackberry, IBM, Cisco, Google, BMW, etc.

WHAT'S THE MOST IMPORTANT THING TO REMEMBER AS A HACKER?

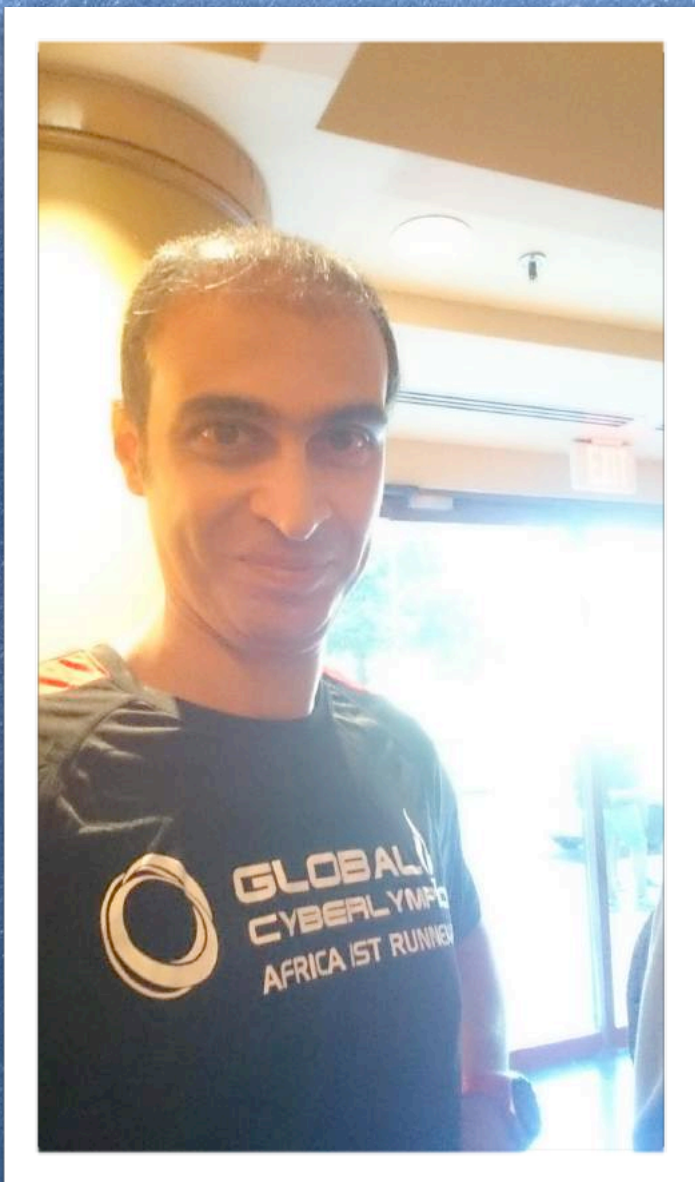
Be positive, ethical and don't break privacy and law. Always use your skills to defend and secure the digital world.

DO YOU HAVE ANY ADVICE FOR OUR READERS?

Hacking is a vast field and involves lot of learning, practice and keeping yourself up to date with the latest security. Learn and dig as much as you can and keep practicing. Practice is the only way to clear your hands. You can't even find a single vulnerability if you don't practice on those VMs that I mentioned. Install VMs and start your practice from today. Don't give up and start from basic level. No one is a born hacker. Years ago I was asking the same question, how to become a hacker. At the start, it might seem a little difficult but with the passage of time you will enjoy learning new stuff. You can email me if you have any questions or visit my website to contact www.sulemanmalik.com

LOUAY SALEH

INFORMATION SECURITY MANAGER



My name is Louay Saleh. I work as an Information Security Manager at one of the large governmental banks in Egypt. I am mainly responsible for the Vulnerability Management program (i.e. the technical assessments such as Penetration Testing & Vulnerability Assessment), in addition to the Security Incident Investigations.

**WHY DID
YOU DECIDE
TO BECOME A
HACKER?**

I am not sure if you can call me a hacker or not. I am a security professional who understands about hacking. I do not hack systems on daily basis, but I hope to do that. It happened when I was a junior during my university years that I realized I wanted to work in the Information/Cyber Security area; surprisingly enough, it was because of the idea of 'hacking' itself! In the English language, a hacker is traditionally “a person who has a high level of skill in computer technology or programming; a computer expert or enthusiast” (Dictionary.com), and the term also replaced the exact meaning of a cracker by people outside of the security domain to be “someone who is able to use or change the information in other people’s computer systems without their knowledge or

permission” (Longman Dictionary). So, it was the idea of understanding computer systems and breaking into them by breaching their security rules or controls that really fascinated me. I do not mean that I wanted to learn to break into the systems to steal information or do any malicious activity. I was fascinated with the idea of learning that to be able to protect the systems.

**IF I
WANTED TO
BECOME A
HACKER WHERE
SHOULD I
START?**

First of all, you have to have the passion. You should like the idea of learning how systems work and how to break them. This means you can start with understanding operating systems, networks, and applications (mainly web applications). In recent years, it also became necessary that one understands programming since the

area of Application Security started booming after businesses relied more and more on web applications.

**AT THE
BEGINNING,
WHICH IS MORE
IMPORTANT -
INDIVIDUAL WORK AND
SELF-IMPROVEMENT,
OR SOME KIND OF
FORMAL
EDUCATION?**

Well, there is no secret recipe here. You cannot say that one is more important than the other. In my own opinion, I see that both are important. It really depends on which option you had first. For example, if you are studying Computer Science or Computer Engineering, then this is your chance to orient your formal education towards specializing in Cyber Security, whether through the courses you have or through the projects or both. This does not mean that when you graduate you will not do any kind of self-improvement; on the contrary, you still need to learn on a daily

basis by reading, practicing, taking courses, working on projects, researching, etc.

If you did not originally study Computer Science or Engineering, but are interested in becoming a hacker, then you have to work on the 'self-improvement' part extensively and try to prove yourself. You may do a kind of formal education at a later stage by joining a post graduate program if it is possible, or you may not need to. It is really a subjective issue and could differ from one person to another. What is more important is the continuous learning cycle, whether it is through formal education or personal efforts.

WHAT ONLINE COURSES, BOOKS, OR RESOURCES WOULD YOU RECOMMEND TO PEOPLE WHO WOULD LIKE TO BECOME HACKERS?

There are countless resources. I will just give some examples:

For online courses: SANS provides a lot of their courses in an online version, but the problem is that they could be too expensive for a lot of people. There is also eLearn Security, whose course prices could be affordable to many persons compared to SANS.

Other examples include Cybrary and EHacking.Net.

For books: the Hacking Exposed series is excellent, since it covers a lot of areas like Networks, Web Applications, Windows Security, Linux Security, Mobile Security, Malware, Forensics, etc.

Other resources: Playing CTF competitions, whether online or in real events, can really help in learning a lot.

WHAT MISTAKES DO BEGINNERS USUALLY MAKE?

Being impatient or not persistent enough. Building the experience and gaining the required skills can be a long process that needs time.

WHAT ABOUT THE HACKER COMMUNITY? DO YOU KNOW ANY FORUMS FOR NEW HACKERS OR BEST WEBSITES TO MEET PEOPLE WITH SIMILAR

There are local communities in many countries such local chapters or conferences and there are international communities represented in the very famous Cyber Security conferences such as DEFCON, Black Hat, Infosecurity Europe, and SecTor. A very good online portal for building a strong community is LinkedIn, where anyone can get connected with a huge number of security professionals and exchange knowledge and news.

There are a lot of excellent Cyber Security news portals. Some of the examples include: The Hacker News, Security Affairs, Krebs on Security.

WORKING IN CYBER SECURITY REQUIRES KEEPING UP WITH THE NEWS. DO YOU RECOMMEND ANY WEBSITES WHERE BEGINNERS CAN FIND RELIABLE CONTENT?

**IS THERE
ANY FORMAL
TRAINING PATH
THAT YOU WOULD
RECOMMEND,
ABOVE
OTHERS?**

If we are talking about learning how to hack, then any track of 'Ethical Hacking' can be useful. For example, the SANS courses that I mentioned before. Also, the Offensive Security track has started to gain huge popularity in the security community lately. In addition, the EC-Council track could also be fine.

C|EH is very useful for those who want to take a first step in the 'Ethical Hacking' area. A lot of professionals criticize it because it may focus more on the tools rather than the methodology. A lot of security consultants who already have good practical experience do not really find that C|EH will add to them, but for sure those who are looking for a good start to learn hacking and did not have an earlier chance of working in the field can really benefit from studying it.

**DO YOU
THINK THAT
CEH IS AN
IMPORTANT
PART IN
HACKING
CAREER?**

**WHAT IS
THE MOST
IMPORTANT
SKILL TO HAVE
AS A
HACKER?**

Wanting to learn something new every day. This is the 'passion' that I talked about earlier.

**WHAT IS THE
BEST
PROGRAMMING
LANGUAGE FOR
HACKING?**

I cannot say that there is something considered as the best. It is really subjective, depending on what you want to do and how flexible this language is. For example, if you are doing Reverse Engineering of a legacy

or a client-server application, it is crucial to understand Assembly. If you are writing a repeater when you are testing a specific web application, you may use C#. It really depends. One of the very popular programming languages of the recent years that is used in writing scripts for both Network and Web Penetration Testing is Python.

**WHICH
PROGRAMMING
LANGUAGE DO
YOU PREFER
AND WHY?**

I used to like C during my university years because it was very flexible, but I have not used it in any project related to security. I have some initial knowledge in Python, and I intend to dedicate some time next year to fully

study it and start working with it since it became very popular in security testing, as I indicated.

WHAT TOOLS DO YOU USE? WHAT'S YOUR FAVORITE HACKING TOOL AND WHY?

My favorite framework is Kali, which contains a lot of tools for Ethical Hacking and other areas like Forensics. However, remember that hacking does not only depend on tools. There are a lot of techniques that are done manually.

WHAT'S THE BEST OS FOR HACKERS? WHICH ONE DO YOU USE?

Again, you cannot really look at it that way. A good hacker should mainly know how to use many operating systems, mainly Windows and Linux. I would say Linux is becoming more important because of its stability and flexibility, but the more you learn to use a lot of operating systems, the better expertise you will have.

I mainly use Windows and Linux, but I also plan to enhance my Linux skills and try to use it more on daily basis. I also wish I can gain more knowledge in mobile operating systems like Android and iOS.

**WHAT KIND
OF HARDWARE
DO YOU USE?
ANYTHING SPECIFIC
THAT HELPS IN
YOUR DAILY
WORK?**

The best and simplest hardware to use is to have a good machine with a minimum of 8GB of RAM and a strong processor (Core i5 or Core i7) that can support running as many virtual machines as you want.

The machine that I am using in my daily work is, unfortunately, below that specification, but I am currently working on acquiring a new personal one that can help me in building a very good security testing lab environment at my home.

FROM YOUR EXPERIENCE IS CERTIFICATION IMPORTANT IN HACKING CAREER? IF YES, THEN WHICH CERTIFICATE IS THE MOST IMPORTANT ONE?

Certification can definitely be a good source of knowledge, but it should not be the ultimate target. There should be a good balance between certification and hands-on experience. For the general security certificates, I would say CISSP is an excellent one. For the hands-on ones, especially those covering Penetration Testing, I think GIAC (certificates of the SANS courses) and Offensive Security are the best.

WHAT ARE THE BIGGEST MISCONCEPTIONS ABOUT HACKING?

That hacking is the same as cracking. As I indicated earlier, a lot of people think that the hacker is the bad guy who breaks into the systems to steal information or take them down and do malicious stuff, which is the exact definition of the cracker. Hacking is mainly understanding how things work. In Cyber Security, a hacker is the one who does that kind of understanding in order to protect the systems (the other definition is White Hat Hacker, but a lot of people in the community have concerns about that definition and indicate that hacking is hacking, and nothing is white or black. This is a different story).

WHAT ABOUT ADVANTAGES AND DISADVANTAGES OF HACKING? HAVE YOU NOTICED ANY?

I think the biggest advantage is that you learn a lot. The main disadvantage could be that someone loses his social and personal life. I heard about such cases.

WHAT DO YOU THINK IS THE MOST IMPORTANT THING TO CONSIDER WHEN PLANNING A CAREER IN HACKING?

That someone has to be persistent and patient and ready to exert a lot of effort to get the necessary experience.

IS THERE SOMETHING YOU SKIPPED AT THE BEGINNING THAT HAS LATER PROVEN VERY USEFUL? DO YOU HAVE ANY REGRETS FOR NOT LEARNING SOMETHING EARLY ON?

Maybe I waited for a longer time for someone to guide me and put me on the right track rather than starting with enhancing my skills when things were delayed. It was not my fault that I was confused and did not know how to start and that is why I wanted someone to guide me, but when I look at it now I feel that I had to do more effort in working on the 'self-improvement' part instead of waiting more. Anyway, I always believe that "It is never too late".

**WHAT IS THE
GREATEST
OBSTACLE YOU HAD
TO OVERCOME TO
GET WHERE YOU
ARE TODAY?**

By all means, I cannot say that I reached what I aimed at. I only achieved something that does not exceed 1% of what I really wanted to do, or dreamed of. Although I had the vision of working in the Cyber Security field since I was an undergraduate student, things went very slow and I finally entered the field later than I expected. I did not know where to start and no one from my employers really cared about the security field, and therefore no one was able to guide me. It was really difficult to find a job in the field at that time, especially that in our geographical region we were (and still) not as advanced in Cyber Security as the western world. I had to work on my

skills and initially show my 'passion' until I found a job that is more or less related to Cyber Security.

**DO YOU HAVE ANY
ADVICE FOR OUR
READERS?**

My main advice is: Learn, learn, learn. The more knowledge you gain, the better experience you have. The field is dynamically changing and you always have to be up to date. My second advice is: Always aim high and make the sky your limit.