Cyber Security Roadmap (Beginners)

Author : Abhinav Kumar

- Twitter : https://twitter.com/abhinavkakku
- Twitter Page : https://twitter.com/ethicalhackx
- LinkedIn : https://www.linkedin.com/in/abhinavkakku/
- Telegram Channel : https://t.me/ethicalhackx Discussion Group link on Channel

Starting The Journey

- Computer Fundamentals
  - CompTIA A+
    - Only if you have no idea of computer , this will teach very basics, Good to learn, but skip if you have been using computers
    - Official Link, not asking to do certification, but asking to learn from resources, aim is to gain knowledge, not the certification
    - Join Telegram Channel
    - Join Telegram Discussion Group
    - Link / references of anything mentioned on the roadmap will be embedded , join group to ask and download the resources
- Operating Systems
  - Windows OS
    - Learn about different OS from Microsoft, their versions, improvements over last versions (broadly)
    - Don't fear errors, every possible error is probably discussed online, search to solve
    - Just get around with day to day tasks in Windows OS, and very basic troubleshooting
  - Linux OS and Uses, different distributions
    - What is Linux
    - What is Linux Kernel, and its functions
    - What are Linux Distro/ or Distributions
    - Different Linux distributions idea, what's basic difference in Linux Distributions
  - The Best OS for Hackers
    - NEVER ! NEVER get into this debate, OS Does not makes better Hackers, Hacker is who can do his task on any OS. Windows or Linux all work equally well for most of the tasks. So one can choose any, be it any Linux distro (and installing all required applications) , or Windows (again installing required applications. Most so called Hacking OS are just dump of all the tools that probably very less people use daily.
- GOOGLE : Learning How to do Google Search like Hackers (this is THE MOST IMPROTANT SKILL to learn)
  - Searching / Research is what can really make someone Hacker, it is the most important skill
  - Search anything on Search engines, Facing any problem ? How to <problem> search this and you can get the solutions 99% of the times, at least something close related to the problem & solution
  - So Start by searching few of the things like How to become a hacker, Penetration Tester Roadmap, How to get Cyber Security Job, How to learn JavaScript, How does websites work
  - Never stop reading at one page (unless in hurry) Read few pages for every search you do Researching about things can only give more knowledge
    - It's said in today's time: Deep Web / Dark Web (which I feel funny about) Real Deep Web or Dark Web is Page 2 of Google Search Results Page. So always visit this Deep/Dark Web (Google Search results pages) , if you did not already find what you were looking for
- Learn What is Cyber Security / Hacking / Penetration Testing / Blue Teaming / Red Teaming / Different Cyber Security Domains(Jobs)
  - Now you already know searching SO search and learn about few things You may get definitions , none maybe 100% correct, but read more and more, get some clue, connect them all in mind
  - What is Cyber Security, What is Hacking
  - Why do we need Cyber Security
  - What Hackers do
  - What are jobs in Cyber Security
  - What all Skills are needed to get job in Cyber security
  - Searched Jobs already ! Now search the roles and responsibilities of few of the jobs on Linkedin or other job websites, this will let you know more about the things you would be interested in learning
  - Also see some recent news related to Cyber Security (from good and reputed websites)
  - Don't get inspired by movies, most often they way they how in movies are fake/false. These movies have put wrong image of Cyber Security & Hacking to allot of people
  - CURIOSITY | RESEARCH | PATIENCE Always try to Know more about things To break things efficiently, some knowledge of How to make things is better to have You cannot start now and suddenly start loosing patience, things can take some time, so be Patient Trust thing when you read from good reputed source, also question them in right way, beingg curious and being stupid are two different things, be curious

Towards Basic Knowledge of Security & Hacking

- Computer Programming (Start basics) Start with any 1 or two languages and give at least 20 hours to learn. It maybe Python | JavaScript or any other
  - is programming really necessary for hacking ? NO But do you want to be a good hacker without Knowing or understanding basic programming ? : Very rare chances
  - So What Programming Language do I Learn ? it Depends on what you have decided next you want to do But I suggest basic of some languages is always good to know. One never knows the next website you need to hack is built on PHP or Node.Js or asp.. it uses JavaScript or is based on some other framework.. You may need to read and understand through some VBScript Code or C++ code to understand the logic and complete the task Its always good knowing one or two languages, good enough to understand the program if you face it.
    - Python helps allot in automating day to day tasks, making things easier
    - JavaScript Hard to find websites today that dont use JavaScript these days, better learn the basics of javaScript
    - Any other Language like C++ or Java Recently Go (Golang) has also been catching attention
- Cyber Security & Hacking terms Search & Learn
  - Some terms in Cyber Security & Hacking keep coming , repeating every time, a common Jargon , so it's better to search and learn few of these terms, so when you see, don't get confused.
  - Vulnerability | Exploit | Threat | Malware | Virus | Botnet | Cloud | Firewall | Virus | Ransomware | Trojan | Worm | Spyware | Adware | Rootkit | Phishing | Spear Phishing | DoS | DDoS | Encryption | Encoding | Penetration Testing | Vulnerability Scanning | ....
  - Social-Engineering | Clickjacking | White-Hat | Black-Hat | SAST | DAST | APT (Advanced Persistent Threat) | Authentication | Authorization | Bug
  - ciphertext | CVE (Common Vulnerabilities and Exposures)| cryptography | decrypt | DMZ (Demilitarized Zone) | drive-by download | encode | encryption key | honeypot | IaaS | IDS | IPS | | insider threat | ISP | keylogger | LAN | OWASP | PaaS
  - packet sniffing | patch | PKI (Public Key Infrastructure) | SaaS | sandboxing | SIEM | sniffing | SPAM | spoofing| supply chain | two-factor authentication |
- Windows OS
  - Windows Installation yes you should know how to repair if you damaged while Learning, you can try on VM
  - What are the security features in Windows OS Learn how or what has Windows put in place to protect / defend against hackers
  - If you already know or are comfortable with the OS, don't spend time around whole courses, search things as they come and learn, If started learning, 15 hours on OS should be good enough
  - Read some blogs about Windows Internals, Basic understanding on Windows will help when protecting or attacking a Windows Machine
  - Know few things like auto-start locations, registry editors, services managers, task manager.....just normal admin tasks. Again we don't need to become Windows Administrator (yes this is also a thing), but we need to know enough to protect it or attack it, as both are job of a Security Engineer
- Linux OS
  - Just like Windows, Basic Linux Administrative Knowledge is required
  - We can again start installing Linux in VM and learn basic tasks
  - We need to know basic CLI commands as we don't every time get GUI interface , most of the times we are operating remotely and with CLI interface, so make CLI a friend
  - If you already know or are comfortable with the OS, don't spend time around whole courses, search things as they come and learn, If started learning, 15 hours on OS should be good enough
  - Linux is Everywhere, from Web- Servers to Mobile, TV, and almost in everything So understanding of Linux is required to some extent
  - Linux+ course is good enough to start with (you know where you can get it, just ask)
  - Make use of Linux in everyday use to get more comfortable almost any error can be solved searching on Google
- Computer Network
  - why is Network required & it's use Different Network devices like Router, Switch, Modem IP Address (Public & Private IP Address), Network Subnets and Calculations (Classful & Classless) , knowing different IP Ranges OSI Layers & TCP/IP Model
  - Server Client model DNS request, How Website request is made and resolved
  - What are Ports and Common Ports on computer What is DHCP , SSL their functions
  - Learn Networking only as much required, I am listing few topics which you can search and Learn & also some resources attached at end We want to become Security Engineers & Hackers, not Network Engineers only So spend time maybe 1-2 week on this
  - Proxy and It's uses (forward & reverse proxy), VPN, VLAN , MAC Address Firewall, Load-Balancers
- Virtual Machines(VM) / Virtualization (VirtualBox, VMWare, WSL)
  - Search and choose available virtualization software for your platform (OS)
  - Network Modes in Virtualization Software play very important role, search and read about : VirtualBox Network Modes VMWare Network Modes
  - Try Installing Windows OS on any VirtualMachine
  - also try setup of Dual Boot setups, Install Both Windows & Linux on Same VM take help of Google search as required
  - learn about Snapshots, backups in VMs and to restore them
  - Research the difference in available Virtualization Software, common ones are VirtualBox, VMWare Player/Workstation, VMWare Fusion, HyperV, Parallels
  - Bridged NAT Host-Only Network These are common network types, search and read when and why are these used(very important for LAB Setup)
  - Try Installing Linux OS on any VM
  - Windows Started featuring WSL Windows Subsystem for Linux Do read and try that too This is not actually a VM, but a good thing to try
- Courses / Certifications / Resources
  - When I say courses, I mean the learning materials , PDFs, Videos , Blogs, references for topics covered in a course. NOT doing the course actually if not required. We are referencing free resources and you know where to get them (if you read carefully above) Join t.me/ethicalhackx and ask for any of the resources mentioned on the page
  - Click to Join and ask/get these
    - Telegram Channel
    - Telegram Discussion Group
    - Twitter
  - Linux
    - CompTIA Linux+ (Udemy / ITProTV)
    - Linux 101 - TCM
    - Linux Essentials for Ethical Hackers - Full InfoSec Course - freeCodeCamp.org
    - Linux Essentials For Hackers - HackerSploit
  - Windows
    - Use Windows like a pro, break and make tihngs
    - Windows Internals (1,2,3) - Pluralsight
    - Microsoft documentations
  - Computer Networks
    - CCNA (Essential Topics Only)
    - Network+ (Udemy / ITProTV)
    - Search terms on Google
    - Search topics on Youtube

Practical Hacking & Security

- We have now decent knowledge about Windows, Linux, Networks, some Programming, Virtual Machines and Basic Hacking/Security terms. Now Let's START HACKING
- LAB setup for Practice
  - Setup Virtual Machine or Labs as Lab to attack or learn It's 100% Legal to Learn in Labs and what's better than to have your own Lab
  - Setup Labs with help of Virtualization Knowledge learnt earlier
- Network Hacking
  - Information Gathering & Reconnaissance
    - Host Discovery Network Scanning
    - port scan and discovery
    - nmap scripts
    - WhoIs and other similar search
    - Different nmap scan types
    - Scanning by Nessus or Qualys or other similar software
    - Active and Passing Search
    - email harvesting
  - Weaponization, Delivery, Exploitation
    - based on Reconnaissance choosing the exploits
    - exploit-db
    - find any 0day if you can get to exploit
    - Metasploit exploits and meterpreter
    - searchsploit
    - mapping knowledge of open ports or services to exploits/attacks
  - Exploitation & Command-Control
    - Windows Privilege Escalation
    - Reverse shells
    - one-liners that trigger and give back shells
    - Data Exfiltration techniques
    - Linux Privilege Escalation
    - by now at least learn netcat
    - Resources :
      - pentestmonkey
      - gtfobins
  - network sniffing
    - Wireshark & packet capture
    - TCPDump
    - Man in the Middle Attacks
- Web Application Security
  - Unpopular Opinion : But learn basic of Web languages (will help in long term) can give like 7 hours on each language to know some of it)
    - very basic HTML CSS, just intro only
    - PHP another most commonly found language Node.Js or other backend frameworks Basic idea help understand the communication to find high severity bugs sometimes
    - JavaScript you can find this in places where you don't find sunlight, if you know JavaScript, hacking becomes slightly easier as you can understand the application more
    - Database Technologies: MySQL, NoSQL, MongoDB....list never ends, some idea of few of these
  - MiTM proxy (BurpSuite Owasp ZAP)
    - speaking of Web App PT , and you don't hear BurpSuite 100 times is not an option, so learn it and different tools under BurpSuite For learning even the community version is good
    - OWASP ZAP is free, and good equally
  - OWASP Top 10 Web Application Vulnerabilities { 2013, 2017 , 2021....}
  - API Security (this also has a top 10 list from OWASP)
  - Vulnerabilities : Just Examples, list is never ending
    - Cross Site Scripting
    - Cross Site Request Forgery
    - SQL Injection
    - Directory Traversal
    - Business Logic
    - HTML Injection
    - XXE
    - File upload Vulnerabilities
    - Authentication & Authorization
    - Rate Limiting
  - Resources/references
    - hackerone reports
    - Read the Writeups on personal blogs as well as twitter #hashtags like #infosec #bugbounty #bugbountytips
- Cloud & Cloud Security
  - Basic Idea of AWS|Azure|GCP , specially security concerned functions
  - Docker Basics & Container Security
- Network Defense
  - Defending Network is a very challenging task, with ever evolving technology, increasing attack surface area, Defenders need to secure Network/Infra against all kinds of attack
  - Endpoint Security
    - -Antivirus / EDR Solutions -Malwares needs to kept out of the machines -Learn about common malware injection ways, -How Antivirus works -Asset/Inventory management to ensure Security software and security policies are applied to add machines -How malware can spread, this knowledge helps to make policies that can stop the spread or infection -DLP (Data Leak/Loss Prevention) systems to prevent the leak of sensitive data either by email, copying, file sharing , online uploads, printing
  - Email Security
    - Email is widely used by organisations for communications - prevent spam & Phishing email - understand how can we determine spam emails - How to detect phishing emails -email gateway security softwares
  - Firewall | Proxy | VPN
    - Configure Firewall policies for Security -Maintain ACLs -DNS Resolvers & Monitoring - Block Lists & and More Important Allow Lists -Enterprise VPN & Proxy Configuration
    - Web Application Firewall Ng Firewalls Configurations
  - Threat Hunting
    - Malware Analysis Reverse Engineering Insider Threat Analysis Attack Surface Determination
  - SIEM | SOC | IHR
    - SIEM or similar things act as central Security Log system - All Security Incidents at any function like firewall , AV , email....can be looked up and related at single point - Helps determine the spread of infection , source/origin and help mitigate by fact finding with concerned teams -Incident Handling & Response Teams (IHR) are the key between different teams and guide the mitigation or lead the investigation
  - Patch Management
- Courses / Certification / Resources
  - When I say courses, I mean the learning materials , PDFs, Videos , Blogs, references for topics covered in a course. NOT doing the course actually if not required. We are referencing free resources and you know where to get them (if you read carefully above) Also many many courses present, search and learn from any
  - Linux Learn Linux by using daily
    - Stackoverflow
    - Official Documentations of Linux Distributions
    - Google Search things where stuck
  - Starting into Security
    - CEH - Excellent source to know basics
    - CompTIA Security+
    - Practical Ethical Hacking - TCM
    - eJPT
    - SANS : SEC460
    - SANS SEC301
  - Defence
    - eNDP (Network Defense Professional)
    - Firewall - PaloAlto Firewall
    - eCTHPv2 - Threat Hunting Professional
    - SANS : SEC699
    - SANS : FOR500
    - SANS FOR508
    - SANS FOR572
    - SANS SEC555
  - Penetration Testing
    - eCPPTv2 - Penetration Testing Professional
    - LiveOverFlow Youtube Channel
    - SANS : SEC504
    - SANS SEC560
  - Programming/Scripting
    - Utilize Youtube Freecodecamp.org
    - SANS : SEC573
    - SNS SEC505
  - Web Application Security
    - PorSwigger Web Academy
    - eWPT - Web Application Penetration Testing Professional
    - SANS : SEC542
    - Ethical Hacking Penetration Testing & Bug Bounty Hunting
  - Cloud Pentest
    - SANS : SEC588
    - SANS : SEC488
    - SANS SEC534

Hacking

- LETS HACK / DEFEND Like a PRO
  - Hope you have learnt allot by now So we can now test our Skills on Some platforms
  - There maybe many things that went missing in above levels But if you are here, I am sure you are good at searching and finding out things on your own, also decide what is best for you
  - Security is a big field, Some enjoy attacking Some enjoy defending (which is really hard) and many more fields coming up with evolving technology like IoT Security, Block Chain Security...
  - SECURITY / HACKING is all about Research Each of topic / keywords on this page can be expanded into a mind-map of it's own Since you are good at searching, you can search further to learn
- We have learnt Enough all the way till here Now we should Practice in Labs or real world (legally)
  - TryHackMe
  - HackTheBox
  - PortSwigger Labs
  - Try2Hack
  - echoCTF
  - CertifiedSecure
  - Root Me
  - VulnHub
  - OverTheWire
  - PentesterLab
  - LetsDefend
  - SecurityBlueTeam
- Courses / Certifications / Resources
  - Network Hacking
    - SANS SEC660
    - SANS SEC760
    - eCPTX - Advanced Penetration Testing
    - OSCP
    - IppSec Youtube Channel
  - Web Application
    - SANS SEC642
    - eWPTXv2 - Advanced Web Application Penetration testing
    - OSWE
  - Mobile
    - SNS SEC575
  - Threat
    - SANS FOR578
    - SANS FOR610
    - OSEE