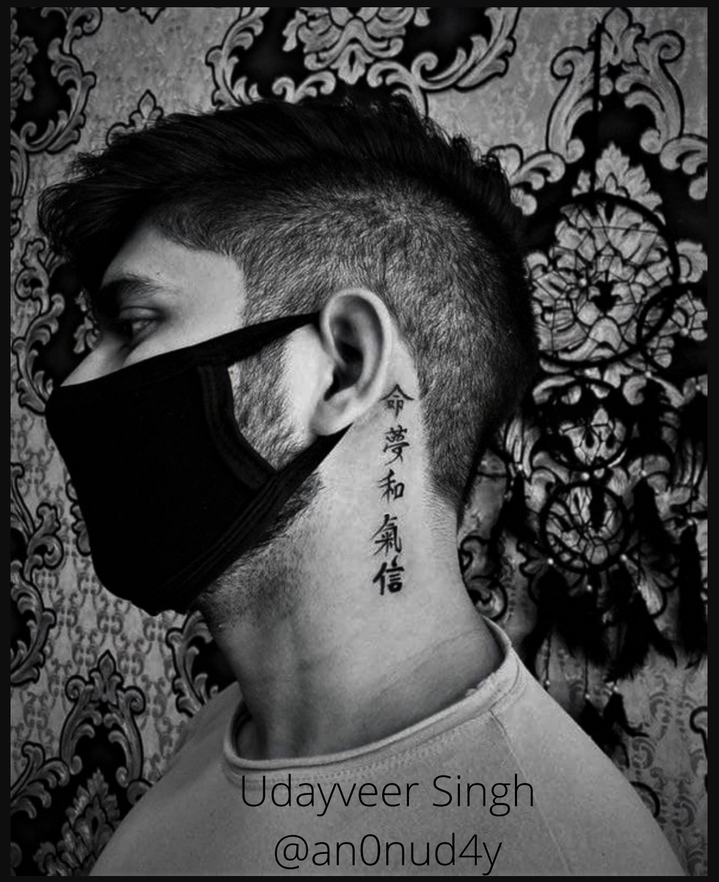
HACK CLUB
angelhack
Campus Hub NIT Sri.
ROADMAP TO
CYBERSECURITY

whoami

- Student @ NIT Srinagar
- CyberSec Enthusiast
- Stock Market
- Blogger
- Movies, Songs

- CTF Player
- Hacking Hardwares
- OSINT for Fun
- HiddenEye Developer
- Evilginx2 Contributor
- TryHackMe Top 1%
- HackTheBox : Hacker



Udayveer Singh
@an0nud4y

CERTIFICATIONS

THM - Offensive Pentesting
THM - Web Fundamentals
THM - CompTIA Pentest+
Pentester Lab - Intro Badge
Pentester Lab - PCAP Badge
Pentester Lab - Recon Badge
Pentester Lab - Unix Badge

Practical Buffer Overflow For OSCP
GPCSSI 2021

eJPT (Upcoming)
CEH Practical (Upcoming)

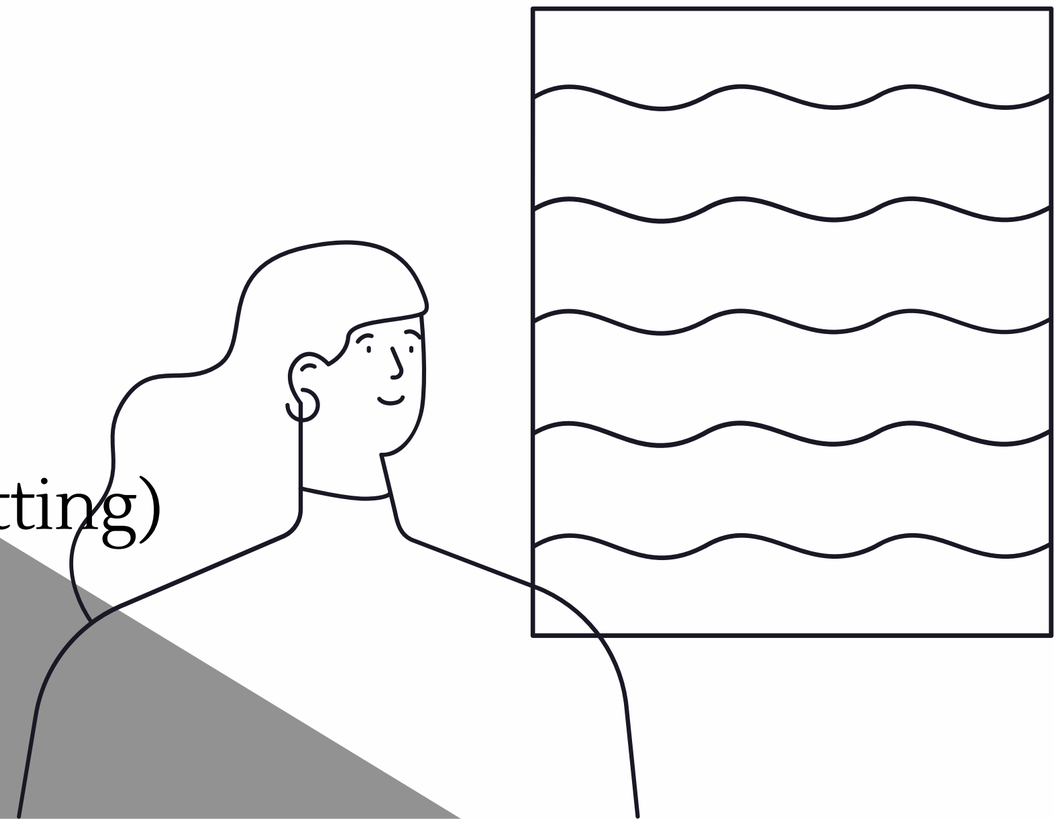
CONTACT

Twitter : @an0nud4y
Insta : @its_udy
Mail : anonud4y@gmail.com

To Know Multiple Platform Profiles
https://linktr.ee/its_udy

Table Of Contents

- Intro to Cybersecurity
- Types of Job Roles in Cybersec
- Roadmap & Resources
- Getting involved with infosec Community
- Hackers to Follow on Social Media
- Hacking Podcasts to listen
- Certifications You Should Have
- Building Your Resume
- Making Money in Cybersec
- My Goals (Understanding Plan/Goal Setting)



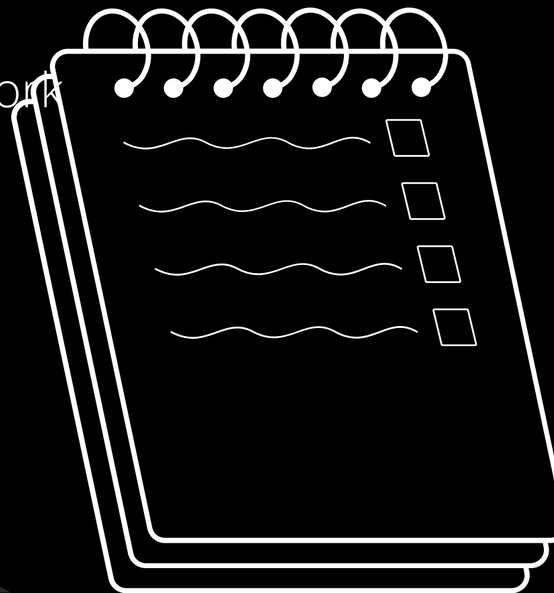
Intro to Cybersecurity

What is CyberSecurity ??

Cybersecurity is the art of protecting/recovering networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. (Acording to CISA)

Why we need Cybersecurity ??

- To Reduce the Risk of Data Breaches and attacks from Black Hat Hackers (APT and Individual Hacking Groups).
- To Prevent Unauthorized access to sensitive information
- To Prevent Services Disruption (Like denial-of-service attacks)
- There are lot more reasons like (Ensuring Business continuity, Protecting from network exploitations from outsiders)



Reference Blogs

https://medium.com/@IamLucif3r/what-is-cyber-security-268cccd0f4eb
https://medium.com/beyondx/what-is-cybersecurity-64a5f61cd0e3

Types of Job Roles

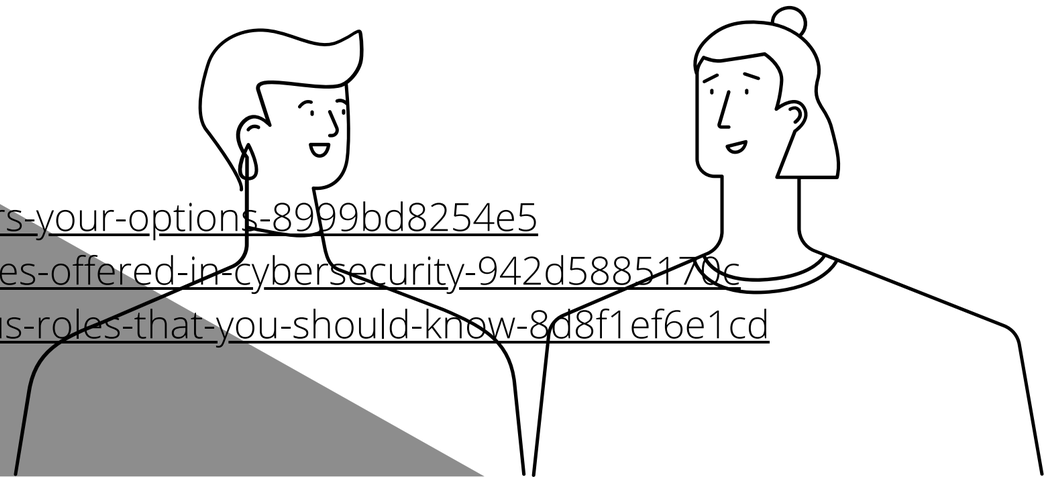
- Ethical Hacker/Penetration Tester
- Chief Information Security officer (CISO)
- Malware Analyst
- Exploit Developer
- Incident responder / Forensic Analyst
- Cryptographer
- Security Architect
- Security Engineer
- Security Analyst
- Security Consultant
- Security Researchers

References

https://vickieli.medium.com/cybersecurity-careers-your-options-8999bd8254e5

https://somyt536.medium.com/what-are-the-various-job-roles-offered-in-cybersecurity-942d58851706

https://medium.com/@shankarbala95/cybersecurity-its-various-roles-that-you-should-know-8d8f1ef6e1cd



Let's Understand these Job Roles ...

Ethical Hacker / Penetration Tester

- Hacking for good with written permission.
- Simulation Attacks on Network.
- Tries Not to Harm the infrastucture during Live attacks.
- Takes care of informative to High impact bugs.
- Provides a full test report and finding (Report writting).
- Need Good Communication skills.
- Part of Red team

Chief information Security Officer (CISO)

- Head of Security Team
- Directs the Strategy, operations & Budget for security.
- Responsible for major Security Decisions

Malware Analyst

- Identifies malware in a Computer or Network.
- Reverse Engineer malware to understand its functionality.
- Identifies ways to detect and prevent the malware from spreading.

Let's Understand these Job Roles ...

Exploit Developer

- Uses research and findings to creates exploit codes to exploit the vulnerabilities.

Incident Responder / Forensic Analyst

- Helps to analyze/recover erased/encrypted data.
- Analyzes and Monitors all network activities and logs.
- Helps to identify intrusions or suspicious activities inside network.
- Part of Blue Team.
- Works with Red team to fix the Bugs and Vulnerabilities

Cryptographer

- Develops algorithms and security systems to encrypt Confidential information.
- Encryption helps to share Confidential data from one to another end without fear of compromising.

Let's Understand these Job Roles ...

Security Architect

- Develops and organizes secured computer systems and networks to protect confidential information from hackers.

Security Engineer

- Liable for testing and screening various security software employed, for improving organizational security.

Security Analyst

- Performs several security related operations such as password complexity, data loss mitigation, and other security practices.

Security Consultant

- Position Mostly found in small organisations.
- Helps to strengthen security , by providing consultation and technical help.

Let's Understand these Job Roles ...

Security Researchers

- They helps to predict the future vulnerabilities by tracking current vulnerabilities.
- Research on products to find unknown or zero day vulnerabilities, which may be actively being exploited.

To Know about Life of a Security Researcher , Check out this blog

https://cybersecurity.att.com/blogs/security-essentials/the-life-of-a-security-researcher

Mindmap By: Harsh Bothra

- Reference: https://hbothra22.medium.com/how-do-i-get-started-in-cyber-security-my-perspective-learning-path-b53065189ba5
- Learn365 : https://github.com/harsh-bothra/learn365

XMind
Trial Mode

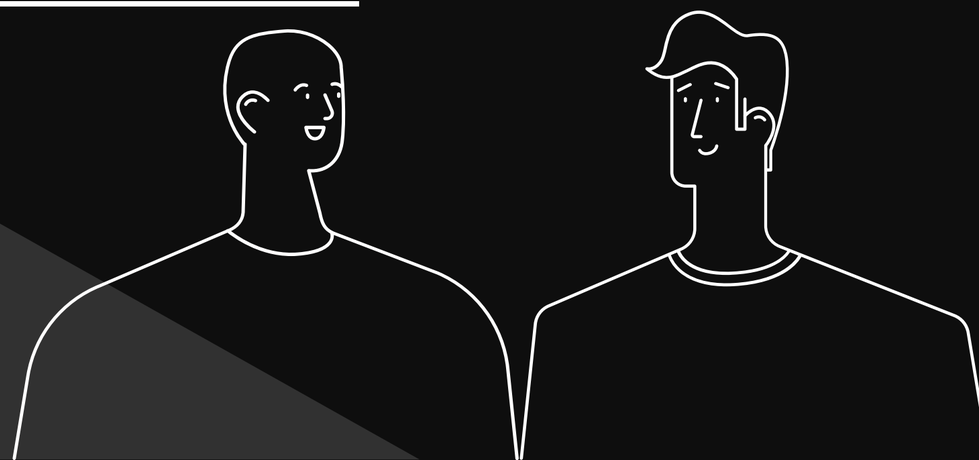
Cyber Security

- **Defensive Cyber Security**
  - Security Operations Center (SOC)
  - Blue Teamer
  - Cyber Forensics
  - Cyber Compliance & Risk Advisory
  - Secure Software Developer
  - Security Architect
  - Incident Response
- **Offensive Cyber Security**
  - Application Security Expert — This guy mainly focuses on Web, Mobile, APIs & Micro-Services, Thick Clients, etc.
  - Red Teamer
  - Penetration Tester — This guy is comfortable performing penetration testing on any given target including Wireless and Network
  - Bug Bounty Hunter
  - Cloud Auditor
  - Code Reviewer
- **Research Oriented**
  - Threat Analysis
  - Malware Analysis
  - Security Trend Analysis
  - Zero-Day & Exploit Developers (Can also be considered in Offensive Part)

Roadmap & Resources

List of Resources

1. TryHackMe Pathways + Labs
2. HackTheBox Machines
3. HackTheBox Academy Modules
4. TCM-Sec Courses
5. Tiberius Privesc Courses
6. Naga Sai Nikhil Courses
7. Portswigger Academy
8. PentesterLab Badges
9. Bug Bounty Courses By XSSRAT and Offensive Hunter
10. Pentester Academy
11. Hacker101 Resources
12. OWASP TOP10
13. Google



Roadmap & Resources

Extra Resources

- BugCrowd University
- Nahamsec BB(BugBounty) Roadmap
- Medium Blog Writeups
- HackerOne BB Disclosed Reports
- Zseano's BB Methodology
- Pentester Land
- BugBountyHunter
- Intigriti Hackademy

Reference

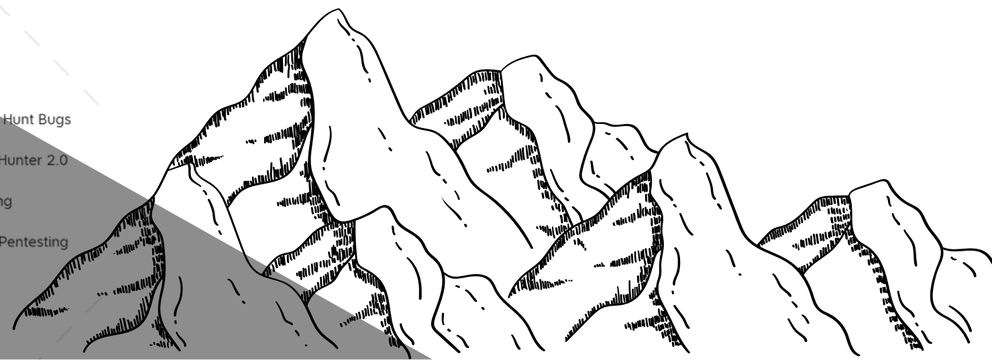
- https://securitytrails.com/blog/popular-bug-bounty-courses

ROADMAP FOR BEGINNERS

- Basics
  - OS Fundamentals
    - Linux Basics
    - Windows Basics
  - Programming Languages
    - Python
    - Bash Scripting
    - Javascript
  - Web Fundamentals
    - HTTP Requests
    - Response Codes
    - Basic web Application Flow
- TRY HACK ME
  - PATHWAYS
    - PreSecurity Pathway
    - Complete Beginner Pathway
    - Web Fundamentals Pathway
    - CompTIA Pentest+ Pathway
    - Jr Penetration Tester Pathway
    - Offensive Pentesting Pathway + (Naga Sai Nikhil Buffer Overflow course)
    - Cyber Defense Pathway
  - Network
    - Wreath Network (THM)
  - MACHINES
- Pentester Lab
  - ALL BADGES
- TCM-SEC Courses
  - Linux 101
  - Practical Ethical Hacking (PEH)
  - Python 101
  - Python 201 (Upcoming)
  - Open Source Intelligence (OSINT) Fundamentals
  - Linux Privilege Escalation + Tiberius (Linux Priv Esc) + HTB Module (Linux Priv Esc)
  - Windows Privilege Escalation + Tiberius (Windows Priv Esc) + HTB Module (Windows Priv Esc)
  - External Pentest Playbook
  - Movement Pivoting & Persistence
  - Practical Malware Analysis & Triage
  - Mobile Application Penetration Testing
  - Practical Phishing Assessments
- Portswigger Academy
  - Server Side Topics
  - Client Side Topics
  - Advanced Topics
- HACKTHEBOX
  - HTB ACADEMY
    - MODULES
    - PATHWAYS/TRACKS
  - MACHINES
    - Starting Point Machines
    - Machines
    - OSCP Like Machines
    - Tracks
      - SRT Track
      - Pro Labs
      - Other Tracks
- Bug Bounty Hunting
  - HackersEra
    - Offensive Approach to Hunt Bugs
    - Offensive Bug Bounty Hunter 2.0
    - Offensive API Pentesting
    - Offensive Thick Client Pentesting
  - XSSRAT courses
    - BB Guide
    - Broad Scope BB

Download Roadmap

Click Here



Getting involved with infosec Community

Where to Find Good(Ethical) hackers ??

- Twitter - Most hackers/Researchers are on twitter.
- Youtube - They also helps Community to learn through Youtube
- Discord - They Have Discord Servers to talk/share stuffs with each other.
- Medium - They helps Community by writing there work/findings.
- Reddit - Infosec thread.
- Linkedin - They Have professional profiles too.
- Forums - You can Find Black Hat Hackers too.
- Github - They helps community by building tools and sharing there tools.
- Telegram - Some awesome Groups are there.

So What to do ?? Where to start from ??

Join Twitter Today, and Follow the Hackers mentioned in next slide.

List of Hackers to Follow

Twitter

https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/media.md#twitter

Youtube

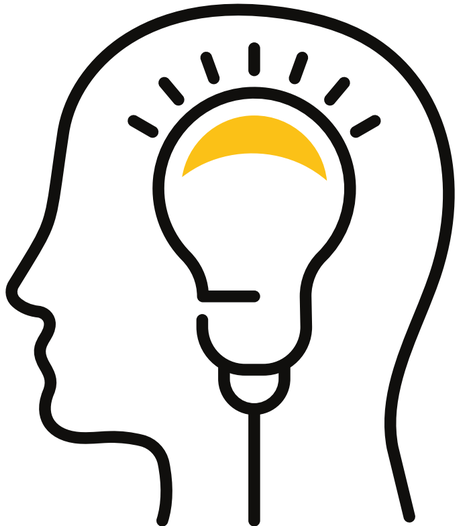
https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/media.md#youtube-channels

Streamers

https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/media.md#streamers

Discord Servers

https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/media.md#discord-servers



Podcasts/Books for Cybersecurity

Podcasts

https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/media.md#podcasts

Books

https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/media.md#books

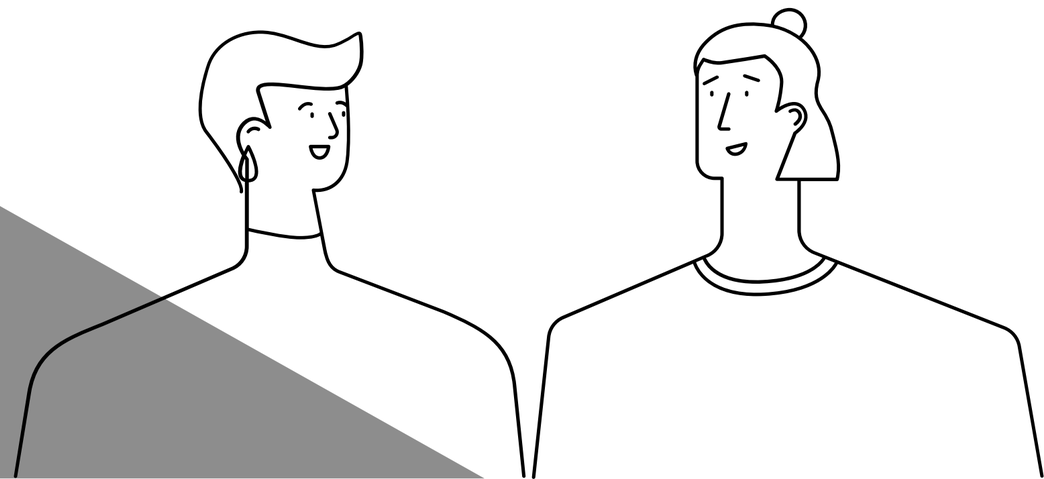
News/Updates of Cybersecurity

Telegram

https://www.sentinelone.com/blog/top-10-telegram-cybersecurity-groups-you-should-join/

Websites

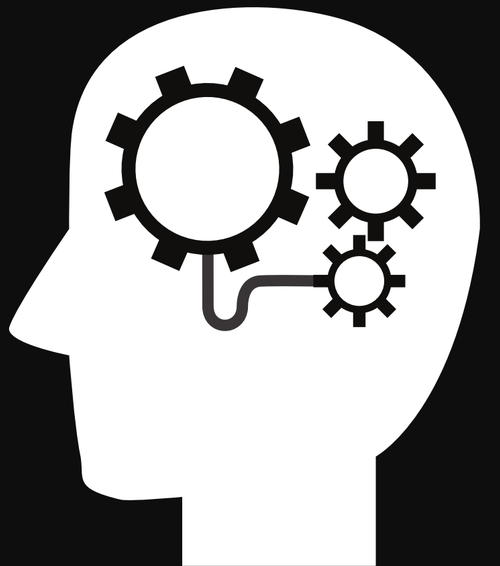
https://www.usefulblogging.com/cybersecurity-websites-to-follow/



Certifications

Few Certifications Recommended For Beginners

- eJPT
- CEH (Practical)
- PNPT
- eWPT (Get Portswigger Cert if Possible)
- eWPTX
- eCPPT
- eCPPTx
- OSCP
- OSWE
- CRTP/CRTE
- OSED



Resume Building

Understand From Experts in Infosec

John Hammond

https://youtu.be/ZAt8MM8WG0o

Jhaddix/Nahamsec

https://youtu.be/Zs28J_SDXYQ

Making Money in Cybersec

Bug Bounty Hunting

- Hackerone
- Bugcrowd
- Open Bug Bounty
- YesWeHack
- intigriti
- Synack Red Team (SRT)

Reference :
https://www.hackerone.com/ethical-hacker/how-become-successful-bug-bounty-hunter

Other Ways

- Penetration Testing (On demand)
- Security Consultancy to small orgs
- Cybersec Content Creation
- Courses Selling
- Creating and selling tools and methodologies

My Goals

Twitter thread

https://twitter.com/an0nud4y/status/1457545560076873736

Udayveer Singh @an0nud4y · Nov 9

Replying to @an0nud4y

Learning Resources I am following in order.
1) @TCMSecurity Courses
2) @0xTib3rius PrivEsc Courses
3) @WebSecAcademy Labs
4) @PentesterLab Badges
5) Bug Bounty Courses from @theXSSrat and @OffensiveHunter

1/3

2 4

Udayveer Singh @an0nud4y · Nov 9

Certifications To Get: eJPT, PNPT, eWPT , eCPPT, OSCP
Optional Certs : eWPTx , eCPPTx , Portswigger Cert, CRTP, CRTE.

Resources I will Use as Reference For Practice/Learning:
1) @hackthebox_eu Machines
2) @hackthebox_eu Academy Modules
2) @RealTryHackMe Labs + Modules

2/3

1 1

Udayveer Singh @an0nud4y · Nov 9

Along with Learning From Above Listed Resources, I will be Passively Preparing for OSCP, and will Follow these Resources -

1) THM Boxes List By @nagasainikhil to build Basics for OSCP. (Youtube)
2) HTB OSCP Like Machines by @TJ_Null
3) Proving Ground By @offsectraining

3/3

1 2

Udayveer Singh @an0nud4y · Nov 9

I will also try to document everything i am learning on My github Repo (Will Update once a week) & Blogs on @Medium.

For Note Taking i am Using @obsdmd + Github For backup + Gitbook For Notes Hosting.

Updates of My #Learn365 Journey Can be Found in Below Comments.

1 2

ANY
QUESTIONS???
quickmeme.com