Kickstart Your Career Into **Hacking World !**

By : Lakshit Verma
Courtesy : Youtube.com/AceTrivia

What **Modi ji** Says !

NCSS 2020

NCSS 2020
India's Strategy for a safe, secure,
trusted, resilient and vibrant Cyberspace

NATIONAL CYBER SECURITY STRATEGY 2020 (NCSS 2020)

Call for Comments

1. Need for NCSS 2020 India was one of the first few countries to propound a futuristic ***National Cyber Security Policy 2013(NCSP 2013)***. Since the adoption of NCSP 2013, the technologies, platforms, threats, services and aspirations have changed tremendously. The transformational Digital India push as well as Industry 4.0 is required to be supported by a robust cyberspace. However, Cyber intrusions and attacks have increased in scope and sophistication targeting sensitive personal and business data, and critical information infrastructure, with impact on national economy and security. The present cyber threat landscape poses significant challenges due to rapid technological developments such as Cloud Computing, Artificial Intelligence, Internet of Things, 5G, etc. New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime & cyber terrorism, and so on. Threats from organised cybercriminal groups, technological cold wars, and increasing state sponsored cyber-attacks have also emerged. Further, existing structures may need to be revamped or revitalised. Thus, a need exists for the formulation of a National Cyber Security Strategy 2020.

2. Formulation The Indian Government under the aegis of National Security Council Secretariat through a well-represented Task Force is in the process of formulating the National Cyber Security Strategy 2020 (NCSS 2020) to cater for a time horizon of five years (2020-25).

3. Vision Proposed vision is to ensure **a safe, secure, trusted, resilient and vibrant cyber space for our Nation's prosperity.**

4. Pillars of Strategy We are examining various facets of cyber security under the following pillars: -

a. **Secure** (The National Cyberspace)
b. **Strengthen** (Structures, People, Processes, Capabilities)
c. **Synergise** (Resources including Cooperation and Collaboration)

5. Submissions We wish to get your views on each of the above-mentioned aspects. You may comment, on any or all of the above-mentioned aspects or additional aspects,in a constructive and meaningful manner. Please contribute to make this strategic document a comprehensive `whole-of-nation' approach for securing our cyberspace.

“ 🎩Hacking Is Spirit Of 👼Innovation And 💜Romance With 📟Technology.💲 ”

What Is Security ?

Why We Need Security ?

Is Hacking Illegal ??

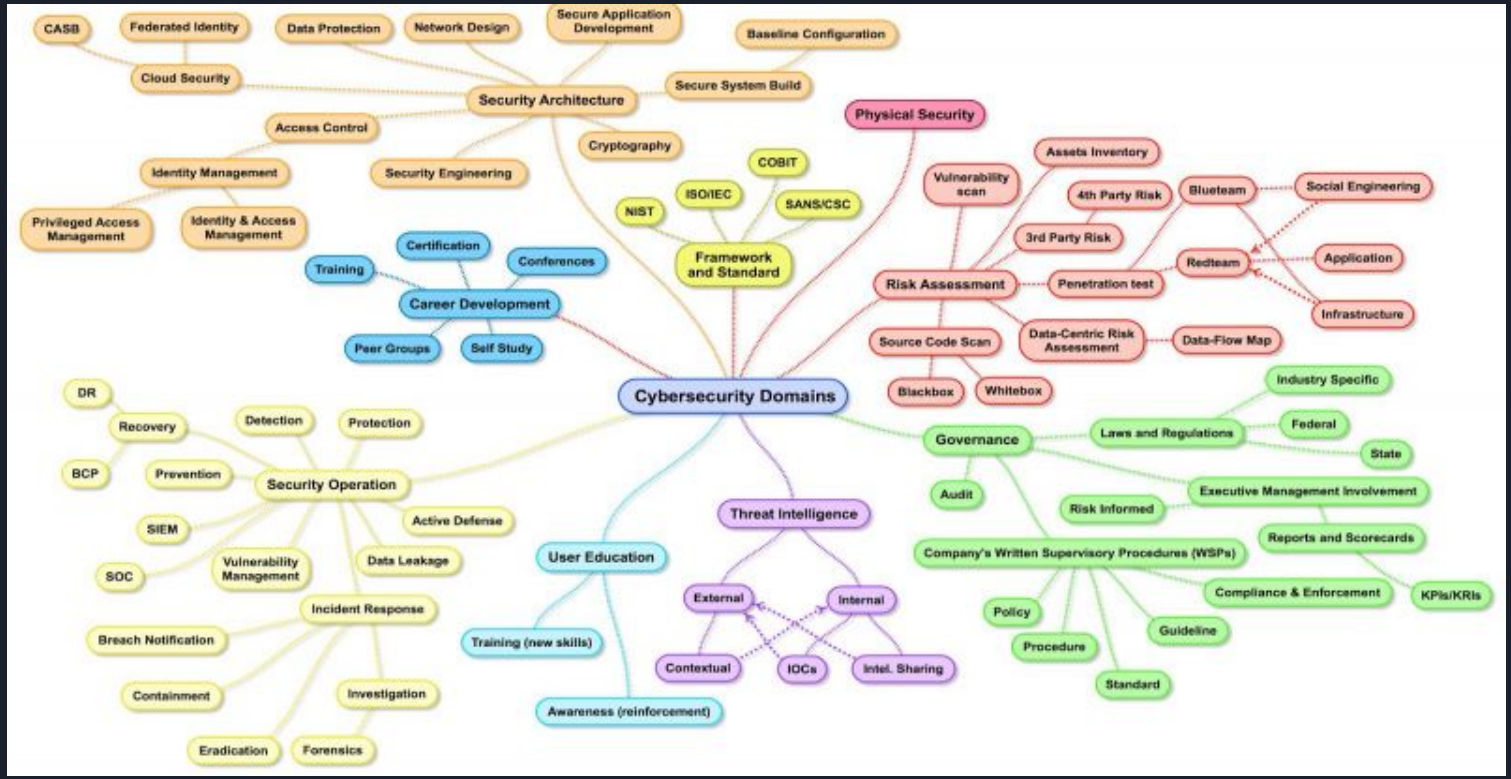
• Principles Of Data Security : CIA Triad

What Is **Cyber Security** ?

- Cyber : Anything Related To Internet
- Security : Securing personal things from being accessed by 3rd party
- Cyber + Security = Cybersecurity can be defined as securing your imp things available on internet from being accessed by 3rd party or unauthorized access.

Is Cyber Sec Is Limited To **Bug Bounty/PT/VA** ?

Answer Is **Big Noo** !!



There’s No Job To Be Termed As Ethical Hacker !!

What **Infosec** One Do As Job ??

- Security Professional.
- Tests The Security And Identifies Loopholes.
- Create Reports And Analysis
- Authorized With Proper Permissions.
- Earns money And Respect Too

Difference **B/W**

- **Bug**
- Is an error , flaw or fault in a computer program or system that causes it to produce an incorrect or unexpected result.

- **Vulnerability**
- It can be defined a logical flaw , error that can have an business impact over a company/organisation.

Lets Get Familiar With Some Infosec Terms

- Infosec : Information security / cyber security / data security.
- Pentesting (Penetration testing) : Testing & Reporting Security Loopholes.
- Vulnerability Assessment : testing and reporting the security loopholes , and thow to fix them.
- Vulnerability : A Weakness That Can Be Exploited.
- Threat : One who exploits a Vulnerability.

Domains In Infosec

- Web Application Security.
- Cyber Forensics
- Malware Analysis
- Vulnerability Assessment & Exploit Development
- IOT Pentesting
- Blockchain & Decentralised Systems
- API-Pentesting
- RFID - Pentesting
- Cryptography & Encryptions
- Hardware Security

What To Learn & From **Where** ?

What You Should **Learn** To Make Your First Step Into **Infosec Domain** ?

- Basic Knowledge Of Computer Peripherals
- How A Software Works , Interpreter/Compiler , Binary
- Software , Handling , Working , Types
- Network , Networking , Topologies , Networks
- Protocols & Ports : HTTP/S , SMTP , TC/IP ,UDP FTP
- OS : Dos , Windows , Kali , Parrot
- Understand How Browser Works , How Request Is Manipulated
- Programming/Secure Coding : **Not Must**

What You Should **Learn** To Make Your First Step Into **Infosec Domain** ?

Programming Languages :

- Malware & Reverse Engineering : C , C++ , Assembly , C# , Embedded C
- Scripting : Python , Ruby , Perl.
- Web App Testing : php , html SQL , Java , Python.
- Shell Scripting : Bash , Shell Scripting

Note : It's Not Necessary To Learn Programming !
It Helps You To Easily Understand Source Code & Manipulating It
You Can Create Your Own Customised Tools , Scripts , Exploits !

- **Common Certifications**

  - CEH : Certified Ethical Hacker
  - OSCP : Offensive Security Certified Professional

Note : It's Only Required If You’re Looking For Job! Or Only If a Company Asks For A Certifications As a Job Criteria

5,80,000

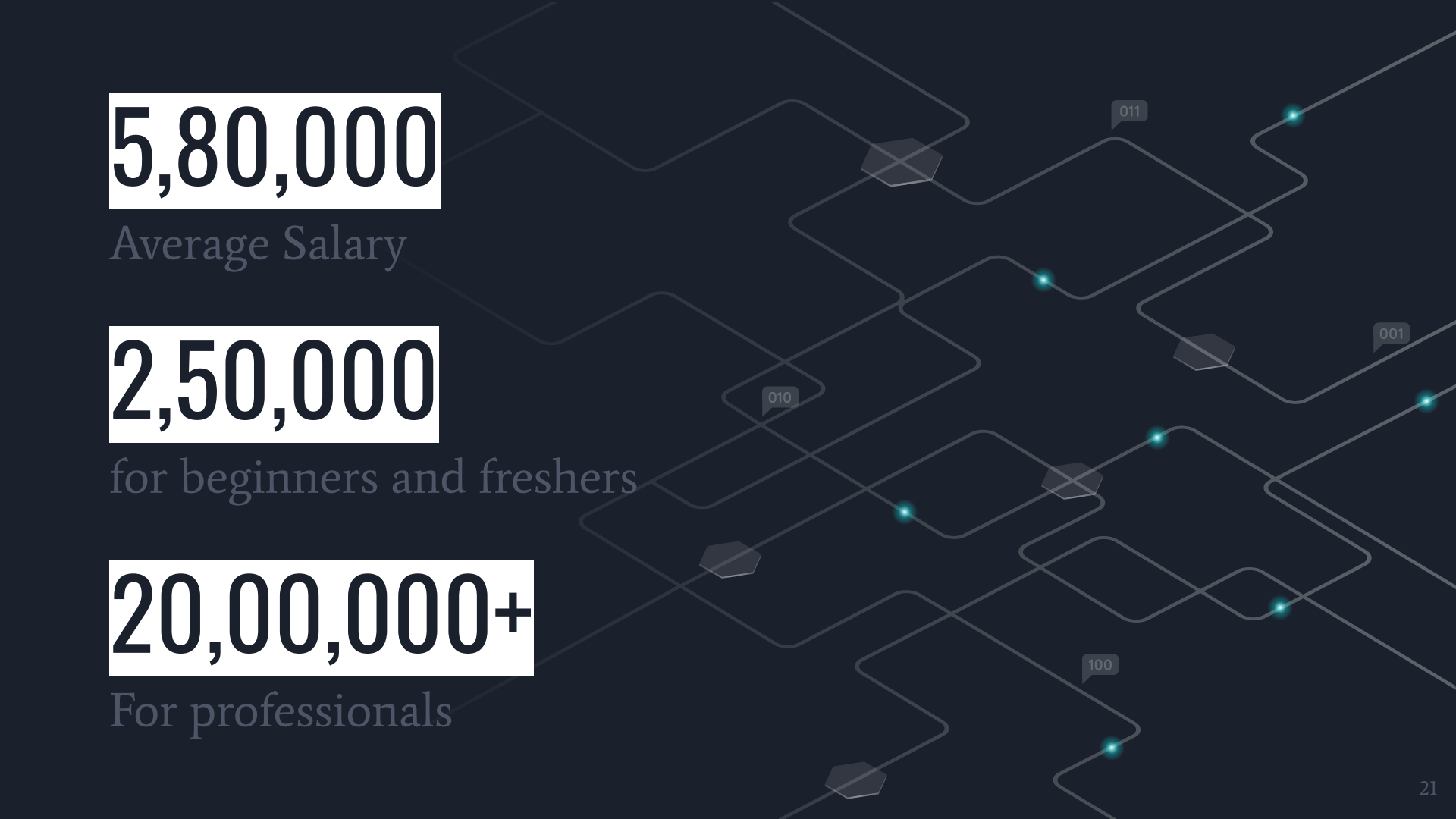
Average Salary

2,50,000

for beginners and freshers

20,00,000+

For professionals



1,50,000$

Average Salary

80,000$

for beginners and freshers

250,000$

For professionals

Future Domains In Infosec

- Vehicle Pentesting
- Drone Hacking
- Automations Using Quantum Computing
- CAR Hacking
- VoIP

Some Sort **Personal** Advice?

- Get Ready To Deal With Errors
- Learn To Use Google Like Pro
- Understand Deep Web
- Be Updated With Realtime Cases
- Security Forums , Community
- Connect With Infosec Professionals

Any questions?

You can find me at:

Twitter : @acelakshitverma

acelakshitverma@gmail.com