Present and Future of Infosec in Nepal

- Kailash Bohara

Introduction

- Kailash Bohara
- Penetration Tester at Eminence Ways
- Occasional Bug Hunter
- Multiple CVEs assigned
- And OWASP Chapter Leader

Looking Back

- OWASP Nepal Chapter started in 2012
- Pentester Nepal - 2013.
- Threatcon - 2018
- BountyBash - 2019
- CTF Events -NepHack/HackBack KU

NEPAL'S CYBERSECURITY INDEX

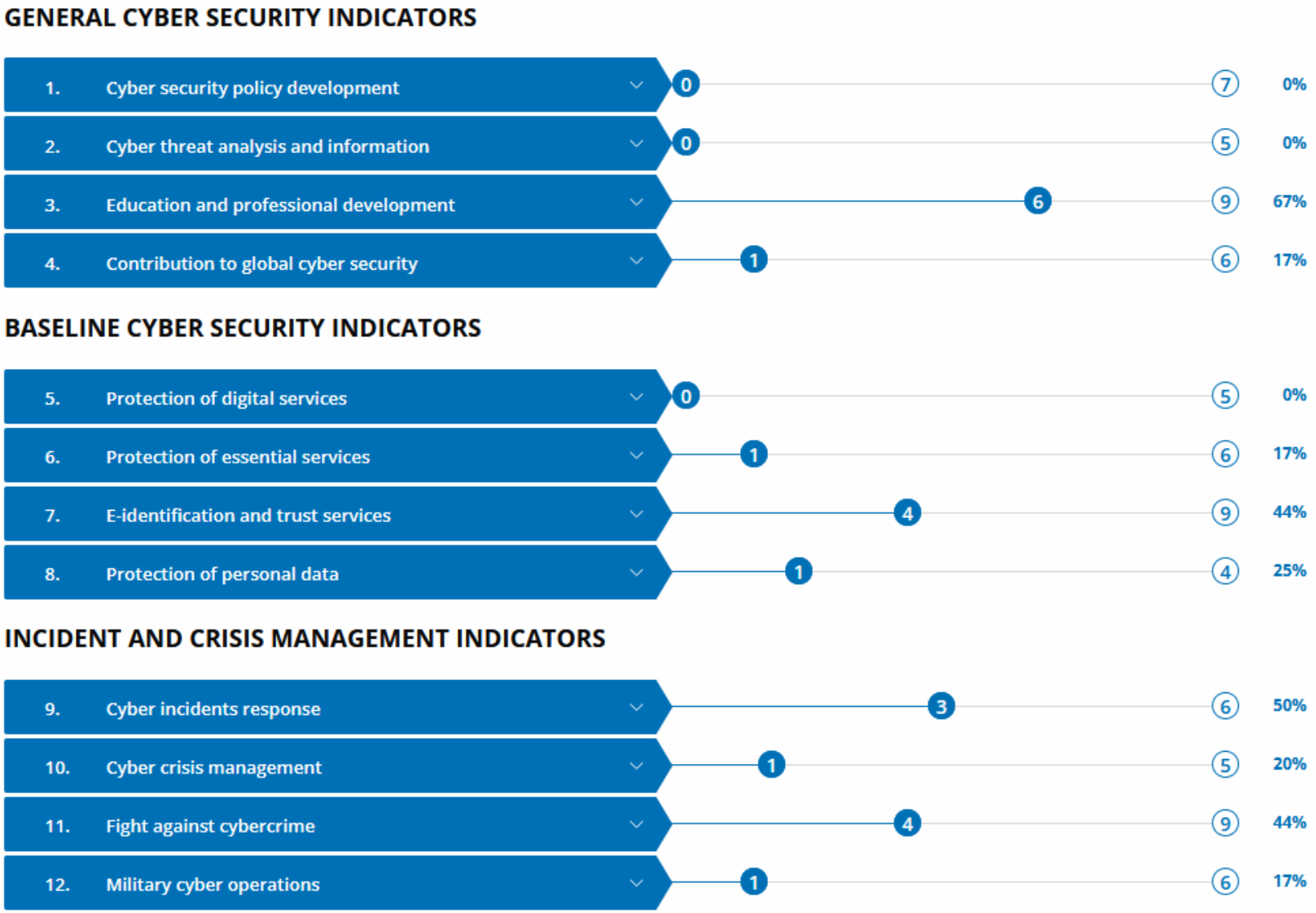
Nepal's Cybersecurity Index

Assessed Year	Global Score	Global Rank	Remarks
2014	0.118	25	Global Cybersecurity Index & Cyberwellness Profiles April 2015
2016	0.275	93	Global Cybersecurity Index (GCI) 2017
2017	0.260	109	Global Cybersecurity Index (GCI) 2018
2020	44.990	94	Global Cybersecurity Index 2020

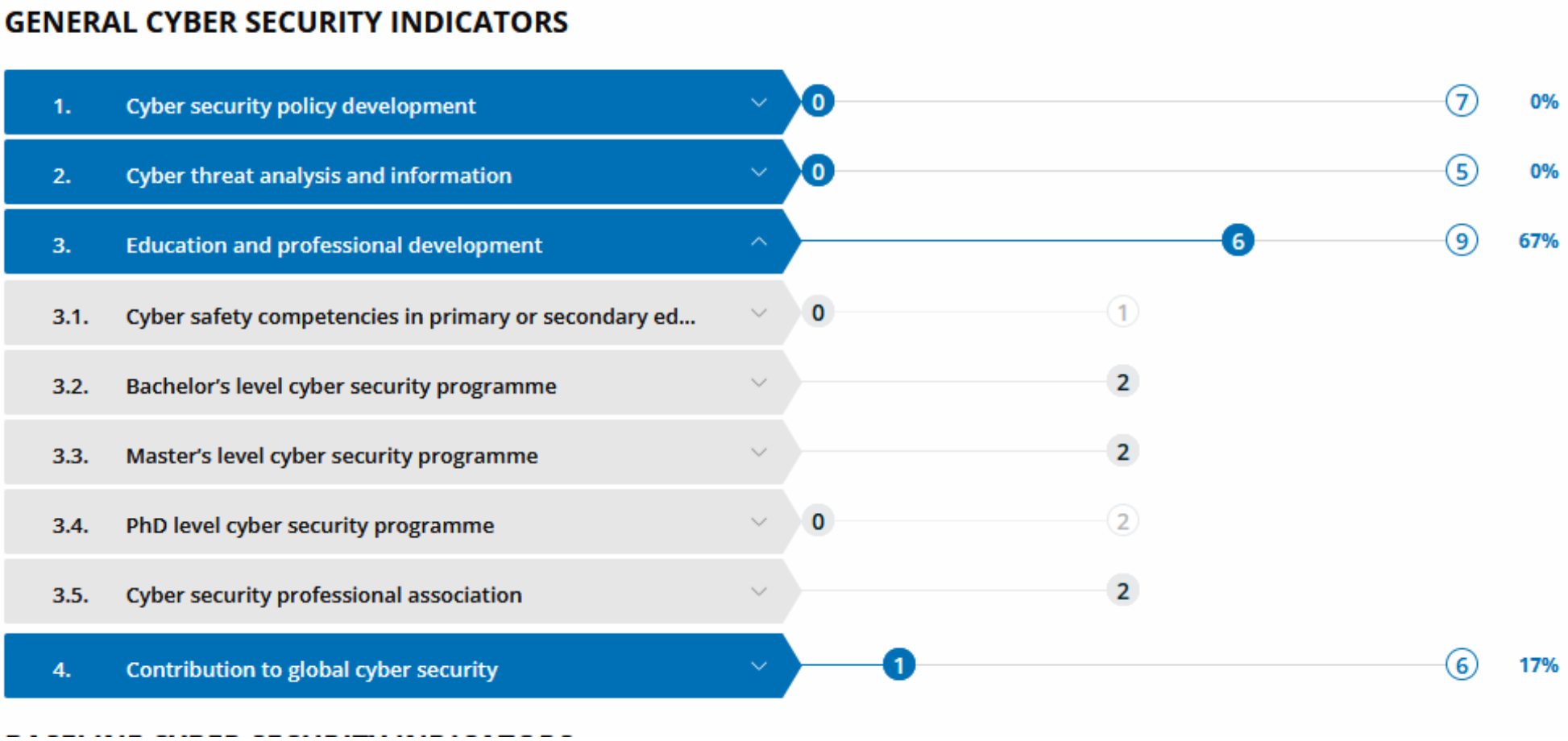
Nepal- Threat Index

- Nepal ranked **94th** out of various countries in Global Cyber Security Index
- Over **1,200 complaints** of cybercrime were registered during an **11-month** period

Indicators


GENERAL CYBER SECURITY INDICATORS
1. Cyber security policy development 0 7 0%
2. Cyber threat analysis and information 0 5 0%
3. Education and professional development 6 9 67%
4. Contribution to global cyber security 1 6 17%
BASELINE CYBER SECURITY INDICATORS
5. Protection of digital services 0 5 0%
6. Protection of essential services 1 6 17%
7. E-identification and trust services 4 9 44%
8. Protection of personal data 1 4 25%
INCIDENT AND CRISIS MANAGEMENT INDICATORS
9. Cyber incidents response 3 6 50%
10. Cyber crisis management 1 5 20%
11. Fight against cybercrime 4 9 44%
12. Military cyber operations 1 6 17%

Indicators


GENERAL CYBER SECURITY INDICATORS
1. Cyber security policy development
0
7
0%
2. Cyber threat analysis and information
0
5
0%
3. Education and professional development
6
9
67%
3.1. Cyber safety competencies in primary or secondary ed...
0
1
3.2. Bachelor's level cyber security programme
2
3.3. Master's level cyber security programme
2
3.4. PhD level cyber security programme
0
2
3.5. Cyber security professional association
2
4. Contribution to global cyber security
1
6
17%

Some Positive Aspects

- Formation of National Information Technology Emergency Response Team) by Government.
- Cyber Security Bill.
- International Security Conferences.
- Educational Institutions with specialized cyber security degree.
- And more...

Cyber Incidents in Nepal

Cyber incidents

- Cases of Ransomware/Malware
- Cases of Data Theft
- Compromised Email System
- Phishing Scams
- Social Engineering Attacks
- Website Defaced

Problems with Forensics

HOW TO START AS A BEGINNER ?

Approach to Information Security

OFFENSIVE

DEFENSIVE

APPLICATIONS

Web Applications

Mobile Application (Android/IOS)

API

Desktop Applications (Thick and Thin clients)

NETWORK SYSTEMS

- Servers
- Workstations
- Firewalls
- Virtualization System
- Cameras
- Domain Controller
- Printers
- Switches
- Wireless System
- Fingerprint Devices
- And more...

FOLLOW TESTING GUIDELINES

- OWASP Web Security Testing Guide
- OWASP API Security Project
- Mobile Security Testing Guide (MSTG)
- NIST Framewaork
- OSSTM (Open-Source Security Testing Methodology Manual)

Application Information Gathering

Sublister, Subfinder, Amass

Dirbuster, Dirsearch, Dirb

Shodan, Censys, Google, Github

Wayback Machine

Source code Analyze

Must Have Tools

Burp Suite

Nessus

MobSF

Frida

Nuclei

reNgine

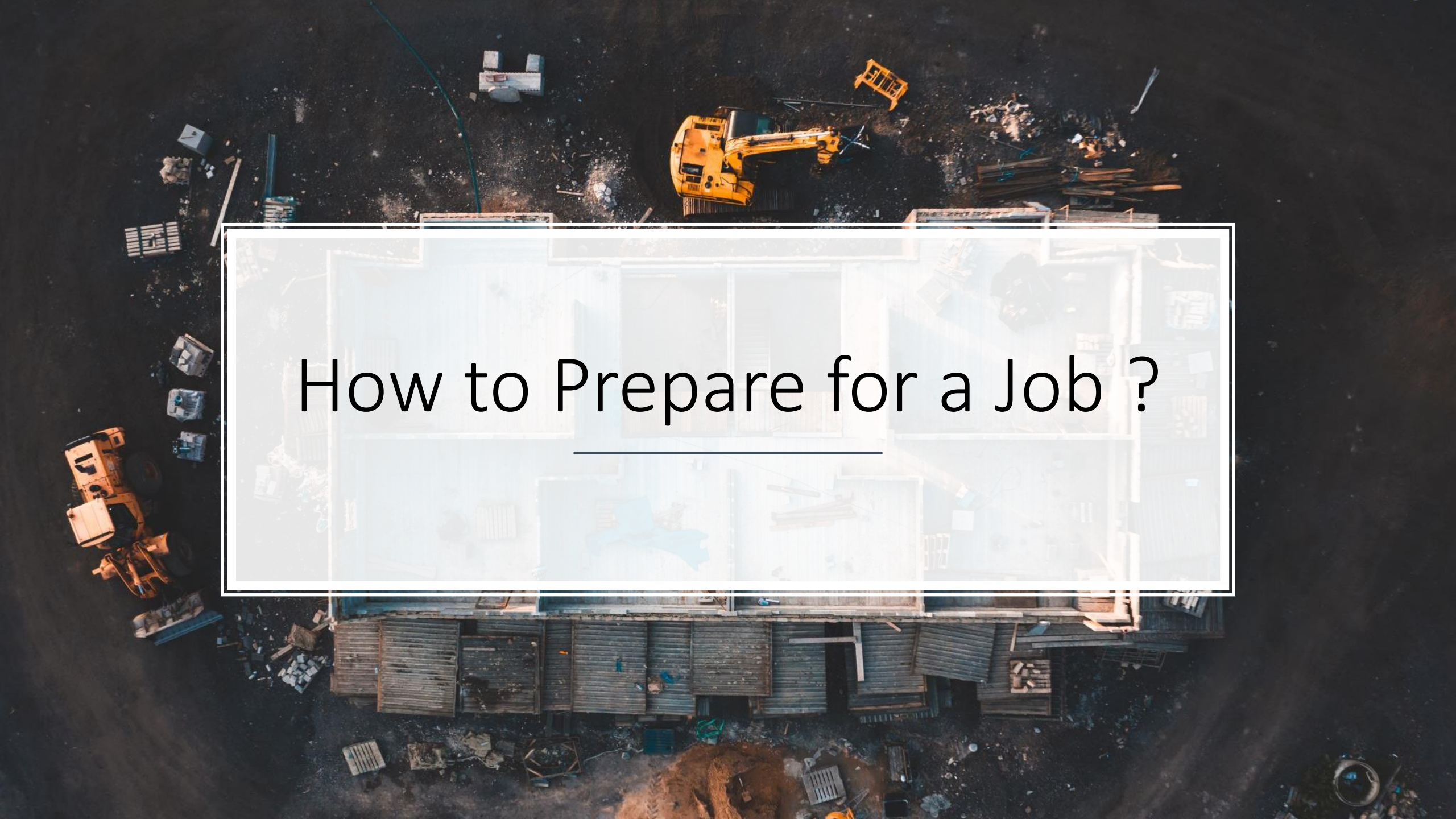
Nmap

Metasploit

OpenVAS

Start solving Labs

- TryHackMe
- HackTheBox
- PortSwiggerAcademy
- DVWA
- VulnHub
- CTF



How to Prepare for a Job ?

Do

Try	Try to gather Hall of Fames, Acknowledgement Letters, Bounty etc.
Solve	Solve as much as Labs and CTF.
Start	Start writing blogs.
Develop	Develop few handy tools or scripts.
Follow	Like minded persons on twitter, Linkedin, etc

Certifications

COMMON DOMAINS OF SECURITY IN NEPAL

Application Security

Network Security

Information Systems Audit

Digital Forensic

Security Operations

Incident Response

POSSIBLE AREAS FOR JOB

- Banking and Financial Institutions (Governed by NRB)
- Software Development Companies
- ISP (Governed By NTA)
- Insurances (Governed By Beema Samiti)
- Government Sector
- Telecoms
- Information Security Companies
- National Defence Bodies – (Nepal Army, Nepal Police, CIB)
- Payment Service Providers

THE FUTURE ?

DIVERSE DOMAINS

- Cloud Security (AWS, Azure, Google, …)
- Threat Hunting
- Hardware Security Assessment
- Blockchain Security
- DevSecOps
- IoT Security
- ICS Security
- Malware Analysis
- And more...

POSSIBILITIES WITH US

- Be Hub for security outsourcing
- Have more security jobs as digitization is rapid
- Can have more Bug bounty hunters
- Government led Responsible Disclosures Programs

THANK YOU FOR BEING HERE.