WHOAMI !!

× Apurv Singh Gautam | Sc0rpi0n | ASG_Sc0rpi0n

× Speaker at Null the Open Security Community, Pune Chapter

× Areas – Threat Intelligence, Network Pentesting/Security

× Given many workshops and talks on Cybersecurity and Privacy

× Play CTFs

× 5 Years

CompTIA Security+ CERTIFIED · CE

1.

ALL ABOUT CYBERSECURITY

Demand, Research Areas , Future Prospects and more

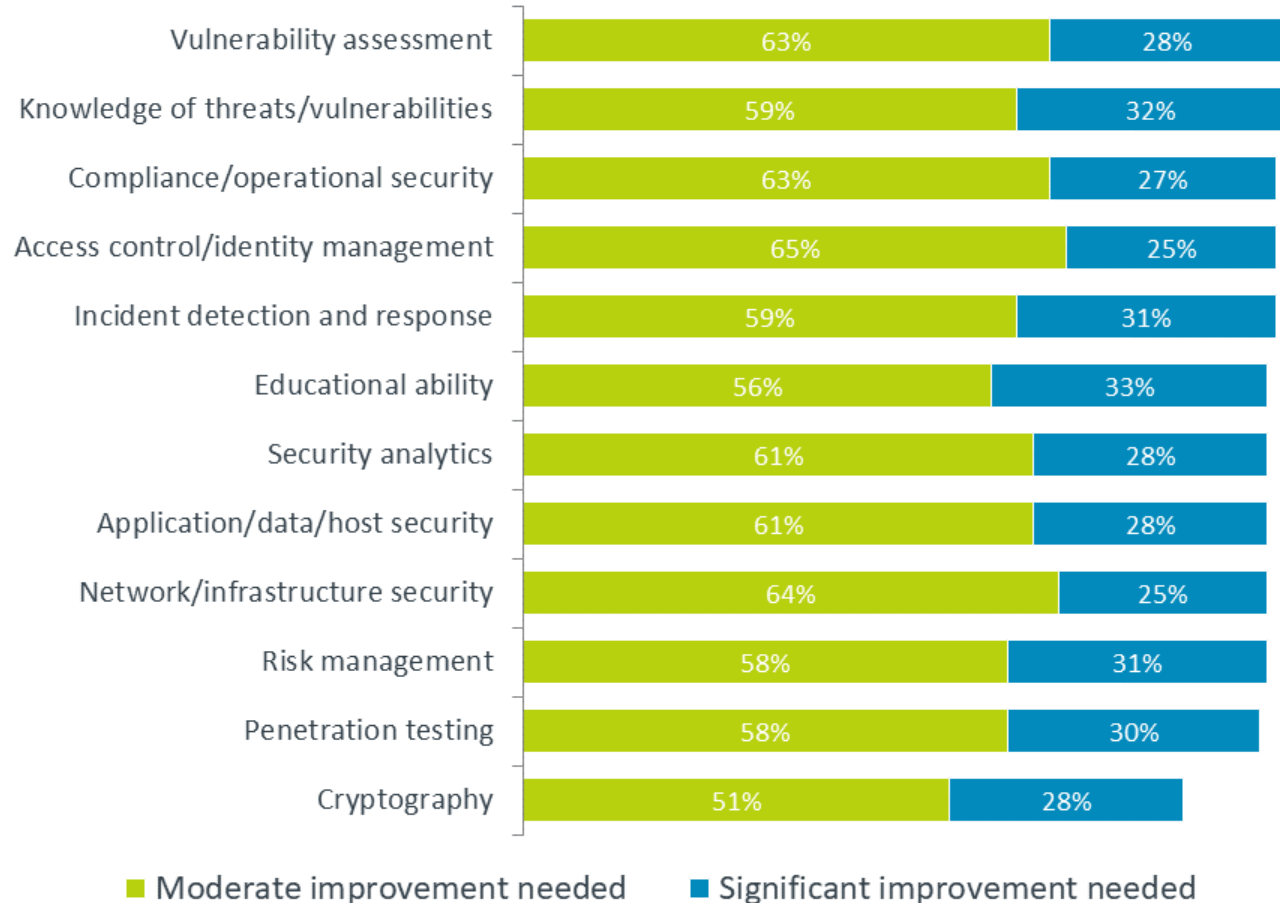# STATISTICS

× Cybersecurity Professionals get **Rs. 22–32 lakh** with **50–100% hikes** (before 25%)

× More than **30,000 jobs** are available in India

× Increased to **150%** from Jan 2017 to March 2018

× Cybersecurity companies reported growth of **50–60%** (start-ups & in-house cybersec ops)

× **3.5 million** job openings over the globe by 2021

CYBER SECURITY SKILL GAP

BY COMPTIA

Improvement needed across a broad set of skills

Skill	Moderate improvement needed	Significant improvement needed
Vulnerability assessment	63%	28%
Knowledge of threats/vulnerabilities	59%	32%
Compliance/operational security	63%	27%
Access control/identity management	65%	25%
Incident detection and response	59%	31%
Educational ability	56%	33%
Security analytics	61%	28%
Application/data/host security	61%	28%
Network/infrastructure security	64%	25%
Risk management	58%	31%
Penetration testing	58%	30%
Cryptography	51%	28%

■ Moderate improvement needed   ■ Significant improvement needed

Cybersecurity Domains

Security Architecture
- CASB
- Federated Identity
- Data Protection
- Network Design
- Secure Application Development
- Baseline Configuration
- Cloud Security
- Secure System Build
- Access Control
- Identity Management
- Privileged Access Management
- Identity & Access Management
- Security Engineering
- Cryptography

Framework and Standard
- COBIT
- ISO/IEC
- SANS/CSC
- NIST

Physical Security

Risk Assessment
- Vulnerability scan
- Assets Inventory
- 4th Party Risk
- 3rd Party Risk
- Penetration test
- Blueteam
- Redteam
- Social Engineering
- Application
- Infrastructure
- Source Code Scan
- Data-Centric Risk Assessment
- Data-Flow Map
- Blackbox
- Whitebox

Career Development
- Certification
- Conferences
- Training
- Peer Groups
- Self Study

Governance
- Industry Specific
- Laws and Regulations
- Federal
- State
- Audit
- Risk Informed
- Executive Management Involvement
- Company's Written Supervisory Procedures (WSPs)
- Reports and Scorecards
- Compliance & Enforcement
- KPIs/KRIs
- Policy
- Procedure
- Guideline
- Standard

Security Operation
- DR
- Recovery
- BCP
- Detection
- Protection
- Prevention
- Active Defense
- SIEM
- Vulnerability Management
- Data Leakage
- SOC
- Incident Response
- Breach Notification
- Containment
- Investigation
- Eradication
- Forensics

User Education
- Training (new skills)
- Awareness (reinforcement)

Threat Intelligence
- External
- Internal
- Contextual
- IOCs
- Intel. Sharing

KEY RESEARCH AREAS

- × Data Security & Privacy
- × Mobile Platform & Application Security
- × IoT Security & Privacy
- × Computer & Software Security
- × Cloud Computing Security
- × Human Behaviour–Based Security
- × Security Policy & Management

1,000,000,000

Total number of IoT devices worldwide

FUTURE TRENDS/RESEARCH AREAS

× IoT Security

× Threat Intelligence

× ML/AI in Security

× Automotive Security

× ICS Security

× Satellite Security

× Social Engineering

COMMON CYBERSECURITY JOB ROLES

× Cyber Security Analyst

× Secure Software Developer

× Cyber Security Engineer/Architect

× Vulnerability Analyst/Penetration Tester (Web/Mobile/Network)

× Threat Hunter

× Malware Analyst

× CISO

20 % OF TOTAL

% of Women in Cybersecurity

2.

ALL ABOUT MS IN US

Preparing for exams, Internships, Work Ex, Research Papers and more

ADMITS FOR MS IN CYBERSECURITY

GRE – 304 (Q:161, V:143)

TOEFL – 102

GPA – 8.86

Internship – 10 months

Research Paper – 1

EXAMS (GRE/TOELF)

GRE — Graduate Record Examination

TOEFL — Test of English as a Foreign Language
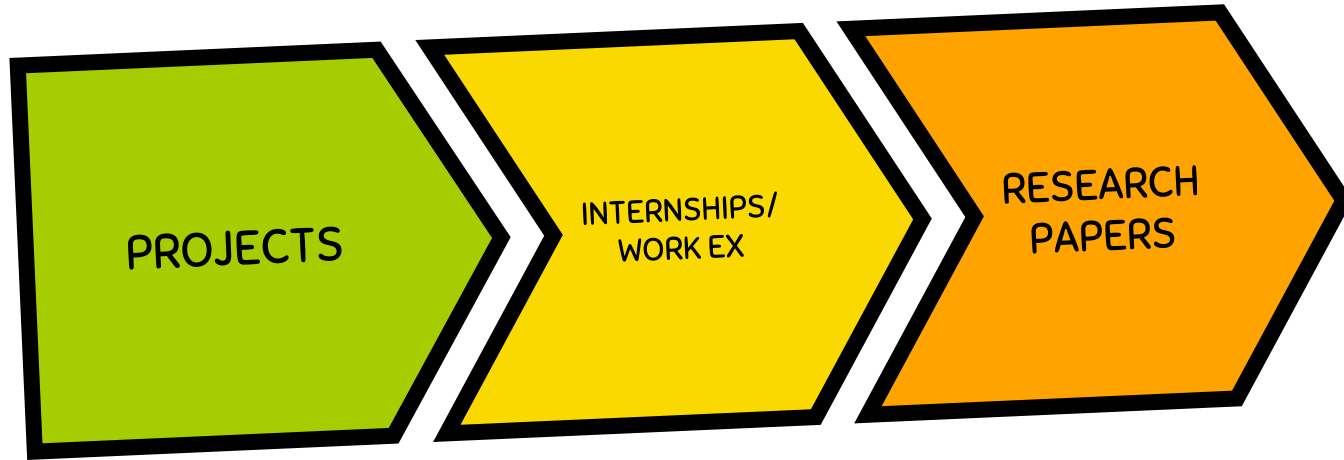
GOOD COLLEGES FOR MS IN CYBERSECURITY

3.

MY PROJECTS/PAPERS

Minor/Major Projects, Research Papers, Internship Projects, B.Tech Project

MY PROJECTS/PAPERS (RELATING TO CYBERSECURITY)

× Recent Trends in the Era of Cyber Crime (Research Chapter)

× Anonymous Traffic Network (Research Paper)

× Question Mark (Python Flask Project)

× Database Encryption (C++ Project)

× UserCred Hack

× Reverse HTTP Shell

INTERNSHIP PROJECTS (10 MONTHS)

× Pastebin Scraping

× General Forum Scraping

× Dark Web Forum Scraping

× Dark Web Dump Shops Scraping

HACKER FORUM EXPLOIT & CLASSIFICATION OF PROACTIVE CYBER THREAT INTELLIGENCE

B.TECH RESEARCH PROJECT

WHAT IS CYBER THREAT INTELLIGENCE ??

CTI includes both the information relevant to protecting an organization from external and inside threats as well as the processes, policies and tools designed to gather and analyse that information.

1,500,000,000,000

Cyber crimes created over $1.5 trillion in profits in 2018

New Thread

Server Stress Testing

SYT | Mark

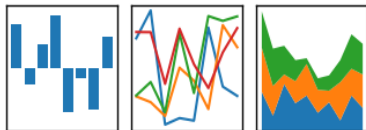| Thread / Author	Replies	Rating	Last Post [asc]
Important Threads			
▶ ROOTERBOOTIN | CUSTOM SOURCE | 5 DAY BOOT TIME | UNLIMITED ATTACKS | STOP BTN (Pages: 1 2 3 4 ... 8) ● LOW PRICE Lennie Small	77	■■■□□	Today 09:00 PM Last Post: C∩D♥C}eĐ
▶ SynStress | Best on HF | Huge XML-RPC DDoS | Unlimited Boots | 100% Uptime | Stop Btn (Pages: 1 2 3 4 ... 79) HOT OFFER Joey	780	■■□□□	Today 08:53 PM Last Post: Joey
▶ TacticalPrime| Layer4&7 | Down protected hosts | Unmatched | $5 | 350 Gbps TN (Pages: 1 2 3 4 ... 8) ƒσяѕαкєи™	71	■■□□□	Today 06:17 PM Last Post: Morrissey
▶ CriticalBOOT | Unlimited BOOTS | OVH | Stop/Resume/Renew | VIP | 300Gbps | API (Pages: 1 2 3 4 ... 130) stratos	1,298	■■■□□	Today 05:27 PM Last Post: stratos
▶ Fury Booter | 5-10Gbps Per Attack Guarantee | Layer 4 & Layer 7 | Instant Activation (Pages: 1 2 3 4 5) Confirm	49	■■■□□	Today 04:46 PM Last Post: Confirm
▶ reBOOT | Since 2013 | BEST LAYER 4/7 DDOS | 100% Uptime | PP/BTC | Unlimited Boots (Pages: 1 2 3 4 ... 11) ★ HOT DEAL Xepher The Cat	103	■■■□□	Yesterday 05:25 PM Last Post: Xepher The Cat
▶ ILLUMINATI / / EXTREME POWER / / OFFICIAL GROUP STRESSER / / PP AND BTC PAYMENTS / (Pages: 1 2 3 4 ... 14) ● GREATEST Bandors	136	■■■□□	09-20-2016 10:34 PM Last Post: Omniscient
Normal Threads			

EXAMPLE OF A HACKER FORUM

WHAT WE USED?

python™

K Keras

Natural Language Analysis
with Python NLTK

pandas
$y_{it} = \beta' x_{it} + \mu_i + \epsilon_{it}$

scikit
learn

Relevant	http:/www.crackingarena.com/accessdriver-lates...	None	NaN	_2540echo_257Fuw8ecr	NaN	\r\n\t\t<div id="post_message_53">\r\n\t\t\t\r...	Download Link : You do not have sufficient rig...
Relevant	http:/www.crackingarena.com/c-force-v1-01b-29-...	None	NaN	_2540echo_257Fuw8ecr	NaN	\r\n\t\t<div id="post_message_54">\r\n\t\t\t\r...	C-Force is a bruteforcer for both Basic Author...
Relevant	http:/www.crackingarena.com/all-ocx-files-need...	None	NaN	_2540echo_257Fuw8ecr	NaN	\r\n\t\t<div id="post_message_55">\r\n\t\t\t\r...	move all .ocx u need to register in same progr...
Relevant	http:/www.crackingarena.com/apex[se]-v-1-0-0-a...	None	NaN	_2540echo_257Fuw8ecr	NaN	\r\n\t\t<div id="post_message_56">\r\n\t\t\t\r...	Download link : You do not have sufficient rig...
							* Improved

EXAMPLE OF HACKER FORUM DATA

RESULTS
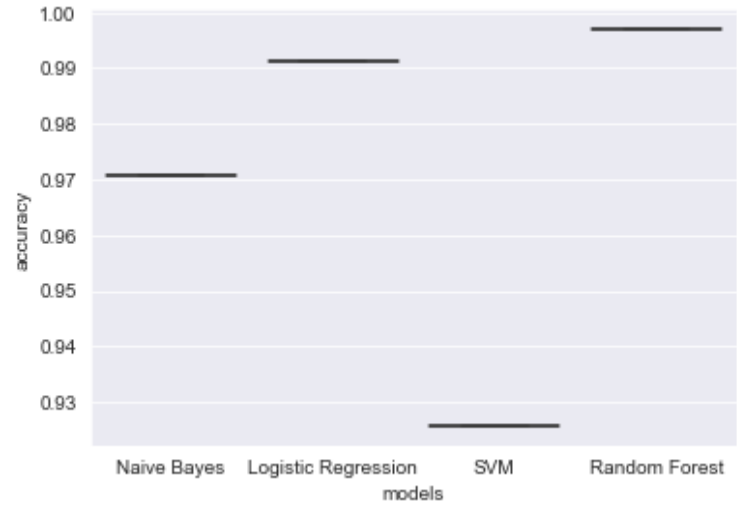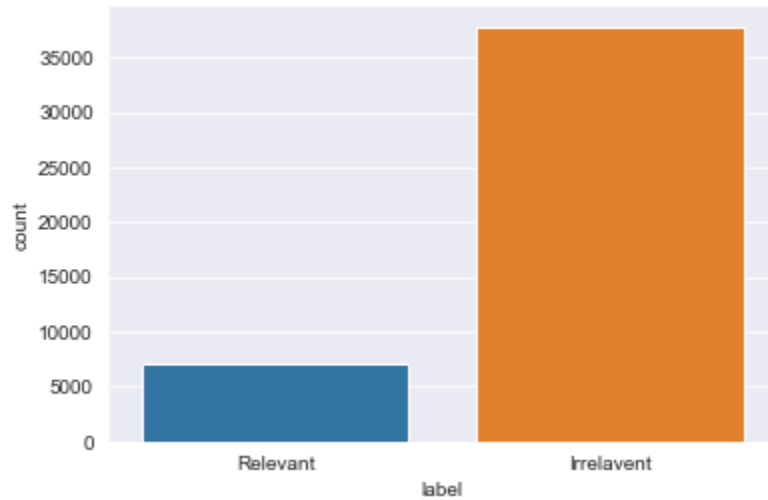
THANKS!

You can reach out for any further questions:

Website – apurvsinghgautam.me
Email – apurvsinghgautam@gmail.com
Social Handle – apurvsinghgautam
(LinkedIn, Quora)