Curriculum Vitae

Purnendu Ghosh
Mobile no: +91-7318763477 /+91-7602024721
email-id: purnendu1996ghosh@gmail.com
B.tech (Electronics and Communication Engineering)

Career Objective:

Dedicated cybersecurity Soc Analyst with experience in SIEM ArcSight tool for 2+ years seeking to deliver airtight information security in an organization. Also, CEHv10 certified with experience in cyber forensics and exploitation tools able to work in various work environments as well as in a team that dynamically works towards the growth of the organization.

Educational Profile:

Degree/ Course	College/ Institute	Board/ Council	Year of Passing	Percentage
Secondary (X)	Jhakra high School	West Bengal Board of Secondary Education	2011	60%
Higher Secondary (XII)	Jhakra high School	West Bengal Council of higher Secondary Education	2013	55%
B.Tech (ECE)	Bankura Unnayani Institute of Engineering	Maulana Abul Kalam Ajad University of Technology	2017	71.6%

Technical Skills:

Networking (CCNA equivalent)
Linux
CEHv10

- **Information Gathering :-** Dmitry, Nmap, Automic Email Hunter
- **OSINT tools:** Shodan, Google Dorks, Recon-ng, FOCA, sn1per
- **Vulnerability Analysis :-** Nessus , Nikto, Nmap, Acunetix, Vega
- **Web Application Analysis :-** Burp Suite ,ZAP, Sqlmap, WPScan, No-redirect addon
- **Password Attack :-** Crunch, THC-Hydra, John the Ripper, Passware Password Recovery Kit, Kon-Boot
- **Exploitation Tools :-** BeFF, Metasploit Framework, Msfvenom , SEToolkit
- **Wireless Attack : -** Aircrack-ng,Cain & Able, WireShark ,MITMproxy, Ettercap
- **Honeypot : -** HoneyBOT ,KFSensor
- **Forensic tool:-** Autopsy, exiftool, jhead , rcstep153, usbview, lastActivityView, wifihistoryview, mini tool power data recovery, MOBILEedit Forensic Express, OSforensics, FTK

Certification : **Certified Ethical Hacker (**CEH v10 from EC-Council in October 2018).

Organization Profile:

Company Name : **Zulu Tele Service Pvt. Ltd.**
Designation : Field engineer
Duration : From 22-sep-2017 to 22-mar-2018
Experience : 6 months
Location : Kharagpur

Job Responsibilities:

1. To attend the customer with in SLA time check the issue in network of his location.
2. Send report for resolving the issue to appropriate team

Company Name : **SATTRIX Information Security Pvt. Ltd.((Project of NTT client UCO Bank)**
Designation : Cybersecurity Engineer (L1)
Experience : 2.6 years
Duration : February 2019 – Till Date
Location : Kolkata

Tool: ArcSight

Ticketing tool: HP Service Manager

Job Responsibilities:

- Responsible for 24x7 SOC Operations including Log monitoring through ArcSight ESM.
- Creating Incidents for different severity alerts and following up until the case is closed with proper RCA.
- Experience in log monitoring, filtering and report generation as per client's requirement.
- Managing customer SLAs for real time alerting, response and reporting.
- Analyze and investigate the alerts in SOC monitoring tools to report any abnormal behaviours, suspicious activities, traffic anomalies etc.
- Security event analysis on various types of security devices like firewall, Proxy.
- Operations and maintenance of HP's ArcSight ESM including ArcSight content developments i.e. rules, reports, dashboards.
- Carrying out log analysis, Event analysis, and Device analysis to detect abnormal activities.
- Generating Daily, Weekly and Monthly reports and making reports and charts.
- I have Basic knowledge on ArcSight Command Center , ArcSight Connector health check & ArcSight services health check.
- Threat Analysis/ Hunting
- Provide Level 1 support for vulnerability management campaigns; work in close collaboration with Level 2 & level 3 analysts to respond appropriately.
- Creating Queries, filters, Reports and Dashboards as per client's requirement.

Raising incidents with concern teams respond to the incidents and service requests
and bring together additional

- Follow up & closing of the tickets based on the client response.
- Maintain incident tracker and updating customer reply.
- Monitoring inbound and outbound traffic for the firewall and investigating events.

- Detecting suspicious logs, creating reports & charts for easy understandable to client, communicating with clients regarding issues.

Tool: Imperva (WAF)

- Responsible for 24x7 SOC Operations including Alert monitoring through WAF Management Console.
- Analyze and investigate the alerts in WAF management console to report any abnormal behaviour, suspicious activities, traffic anomalies etc.

Achievement: CVE-2019-12195 (https://www.exploit-db.com/exploits/46882) is discovered and identified the vulnerability, based on that, applied for a CVE and achieved it

Extracurricular activities:

1. Works as an individual security researcher
2. Individual penetration tester
3. Looks for vulnerabilities present in Web Applications and Network of various Companies and if any vulnerability is found I submit a report regarding my findings to the concerned Company.

Personal Information:

Date of birth :14th of March 1996
Sex :Male
Father's name :Tarun Ghosh
Mother's name :Chaina Ghosh
Nationality :Indian
Languages known :English, Bengali and Hindi

Permanent Address:

Vill :Chanda
P.O. :Jhakra
District :Paschim medinipur
Block :Chandrakona
PIN :721201
State :West Bengal

Declaration:

All the above information is True & Correct according to my belief & knowledge.

Date:
Place:

Purnendu Ghosh