SHUBHAM CHOUBEY

+91-9589426407
bhamchoubey@protonmail.com
https://linkedin.com/shuhey
https://shumcheyy.github.io
https://github.com/shumcheyy

A budding security enthusiast, with experience in solving challenges in CTFs and platforms like hackthebox and hackerone, with interest and hands-on experience in the following domains**:**

- Linux Administration
- Network Security
- VAPT
- OSINT
- Malware Analysis
- Operating Systems

SECURITY CONCEPTS & TOOLS:

- Experience in working with Security Tools like Metasploit, BurpSuite, Gobuster, john, IDA pro, Impacket
- Experience in Privilege Escalation in Windows and Linux Environment
- Knowledge of various exploits like Eternal Blue, Heartbleed, Shellshock etc
- **Pwned 35+ machines on HackTheBox platform of varying difficulties.**
- Practical knowhow of OWASP Top 10 security risks like XSS, Injection techniques,Broken Authentication
- **Experience in Writing Penetration Testing Reports**

NETWORKING CONCEPTS & TOOLS

- Well versed with TCP/IP stack along with strong Networking Basics
- Experience in using Network protocol analyzers like Wireshark, tcpdump
- Experience in using Network mapping tools like nmap, Angry IP Scanner
- Good understanding of mechanisms behind protocols like TLS, DNS
- Knowledge of network and security systems like Routers, Switches, Firewalls, DMZs
- Elementary level experience in using SIEM tools like Splunk, Kibana, Grafana

PROGRAMMING, SCRIPTING LANGUAGES

Python , BASH , C (Moderate), x86 Assembly [Beginner]

WORK EXPERIENCE

JUNE 2019 - PRESENT
Freelance Security Analyst

I worked as a Freelance WebApp Pentester for a Fintech Company, where I:

- Performed GrayBox Testing on the application with the available credentials of 2 users and 1 admin
- Found some Low and Medium severity rating Findings which involved:
  -- Bruteforcing Login Fields was possible
  -- Login Field data sent in Plaintext to the server
  -- Back and Refresh attack possible
  -- Session Expiry(The expiry duration for the cookie was 1 year)
- Performed various manual and automated tests using tools like Burp Suite Pro, SqlMap, Nikto, ZAP
- Wrote the Pentest report which displayed the various findings in tabular and graphical format

MARCH 2019 – MAY 2019
TRAINEE, SHIVAM SERVICES, CHHATTISGARH

Shivam Services is the industry leading Wholesale Trading firm dealing with industrial electrical and electronic equipment where I:

- Learned to use few SIEM tools like Splunk, Grafana, Kibana for Log and Event Management
- Did security assessments on company's website using tools like Burp Suite, Beef
- Learned about various Security concepts like TLS, CIA triad, Risks, Threats and Vulnerabilities
- Got experience in using Cloud based services and gained knowledge of various service models like SAAS, PAAS, IAAS and gained foundational knowledge on Azure security with Security groups etc
- Wrote a report showcasing the strengths and weakness as well as the provided mitigation techniques

MAY 2018 – JUNE 2018

R&D INTERN, ERICSSON R&D, GURGAON

- As an Intern, I was involved in the Netsec automaton project for one of the modules which stores Business Application entities like currency, country codes etc.
- Automated detection of vulnerabilities like Input Validation, Sanitization, Exceptional Behavior and implemented a checker framework.
- Implemented OWASP's dependency checker using Maven which contains 30+ checks and followed SEI CERT Oracle Coding standard for Java
- Classified Severities using CVSS and created reports accordingly
- Got experience in using CI tool like Jenkins

PROJECTS

DYNAMIC MALWARE ANALYSIS LAB

- Through this lab I learned about various malware actions in a Windows Environment.Monitored their activities using sysinternal tools like procmon, procexp.Learned to use various Disassembler like Ida Pro, radare etc.Learned about Families of Malware.I used Remnux as the FakeNet and InetSim device with the victim machine in a host only env.

MALWARE ANALYSIS USING ML ALGORITHMS (RESEARCH PROJECT)

- This was a research based project involving Machine Learning using Classification algorithms like KNN,Naive Bayes, SVM, RF, Decision Trees using tools like KNIME WEKA, Orange and RapidMiner.

HOMELAB

- Built a Homelab using Virtual Machines which consisted of host machine using a bridged network along with a NAT for an internal network where Pfsense acted as a firewall for the vulnerable machine. The setup also consisted of another machine acting as an attacker.

EDUCATION

JULY 2019
B.TECH (IT), MUJ JAIPUR

JUNE 2015
HIGHER SECONDARY, OPJS, RAIGARH

CERTIFICATION(s)

- **CCNA R&S**