



Get in touch



Karaikudi, Tamil Nadu, Sivagangai



63855-40580



kishorekannank0001@gmail.com



@Driewtantrommi3



<https://triplek5.github.io/about-K-01>

Educational Growth Path

2014 – S.M.S V Hr Sec School – 96%

2016 – Alagappa Matric Hr Sec School - 87.75%

2021 – Shanmuganathan Engineering College – 7.72 CGPA

Skills

1 Script & Programming

Scripting Knowledge – Bash

Programming Knowledge – Python

2 Cyber Security

Web App Pentest

Application Pentest

Active Directory Pentest

Bug Hunt

Sailpoint IdentityIQ (IAM & PAM)

3 Ethical Hacking & Networking

Oracle VM & VMware

OWASP TOP 10

VAPT

4 Ethical Hacking Tools

Nmap, SQLmap, Nessus

Burpsuite

Metasploit Meterpreter, SEToolkit, RAT tools

5 OS & Server

Windows Server 2019 & 2022

Kali Linux & Parrot OS

KANNAN K

Organized Graduate engineer who enthusiastic to Cyber security research, planning, execution & maintenance with mitigations. Hands on practice with Application Security, Web Application Security, Network Security, IT Security, Penetration Testing, Bug Hunting & prevents infrastructure with networking, SOC, Network Security's preventive strategies & implement policies to defend.

Passionate Towards

- To work in CyberSecurity & Ethical Hacking domain as fresher/intern related jobs
- To accommodate myself as a Cyber Security Researcher, Cyber Security Analyst, Penetration Tester, Bug Hunter with Futuristic Innovative minds & implement my knowledge for futuristic developments
- To accommodate myself with latest technologies to learn & execute

Projects

Source: <https://github.com/Triplek5/PythonCyberProjects>

Source: https://github.com/Triplek5/sailpoint_assignment

- ARP Spoofing & Packet Sniffing to become MITM with Python
 - Skills Used - Python
- Create Backdoor & get reverse connection from the target using Python
 - Skills Used – Python
- Web Application Penetration Testing
 - Consider OWASP Top10 Vulnerabilities, found bugs, prioritize with its severities & report generated
 - Operating Systems – Kali Linux, Parrot Os
 - Skills Used – Nmap, Burpsuite, Netcat, SQLmap, Python Servers
- Active Directory Penetration Testing
 - Conduct Pentest on internal Active Directory Networks – found vulnerabilities on features with respective tools – present report with mitigation strategies
 - Operating Systems – Windows Servers 2019, 2022, Windows10
 - Skills Used – Responder, ntlmrelayx.py, Metasploit Meterpreter, MITM6, Powerview tools, Sharpbound.ps1, bloodhound, Python Impacket Modules, Mimikatz etc
- IAM Sailpoint IdentityIQ
 - On boarding Delimited Application with csv file.
 - On boarding JDBC Application.
 - On boarding LDAP Application.
 - On boarding employees via roles, contractors via lifecycle events on both JDBC & LDAP Applications.
 - Skills Used – Sailpoint IdentityIQ (IAM & PAM)

Co-Scholastic Activities

- Participated in **SUPPLY CHAIN MANAGEMENT** International conference on 4th September 2020 at Shanmuganathan Engineering College, Thirumayam,
- Participated in **FUTURE OF LEARNING & DEVELOPMENT** International conference on 10th October 2020 at Solamalai Engineering College, Madurai,
- Workshop
 - Participated in a Workshop on **FINITE ELEMENT ANALYSIS** held on 22nd February 2020 at Shanmuganathan Engineering College, Thirumayam
- Project
 - Mini project:
DESIGN & FABRICATION PROJECT OF ALLIUM CEPA REAPING MACHINE
 - Main project:
AGRO DYNAMIC REMOTELYOPERATED NAVIGATION EQUIPMENT