

SHAPEAI

BECOME AN ETHICAL HACKER.

Join us for a 2.5 month long intensive training and internship.
Get placed as a Full-Stack Web Developer or a Software Development
Engineer in your Dream Company.

LEARN FROM PEOPLE AT:



BATCHES STARTING FROM:
BATCH-A: 1ST JUNE 2021
BATCH-B: 1ST JULY 2021
ONLINE LIVE CLASSES

Learn, get certified from top institutions and companies, and then
intern with us Get .placed in your dream companies . **Limited seats (**
only 120 seats available) Join NOW!!!

BENEFITS:

- Data Structures and Algorithms
- Competitive coding Daily
- 2hr LIVE Doubt Session Every Day
- 2hr LIVE Classes Every Day
- Recordings for all the LIVE classes
- 10+ certificates from top MNC's
- Paid Internship Opportunities
- Fast Doubt Solving
- Interview Preparation
- Letter of Recommendation Certificates and many Projects.
- Complementary Data Analyst and Machine Learning Engineer Courses Free

ABOUT THE COURSE

This Training and Internship program is designed to help learners develop a deeper understanding of modern information and system protection technology and methods. It helps interns to instill in them the knowledge of the vast domain of Cyber Security which includes skills in defending computers, servers, mobile devices, networks, and data from malicious attacks. Students, developers, managers, engineers, and even private citizens will benefit from this learning experience. The learning process will be kept simple and accurate from pillar to post.



TECHNOLOGIES THAT WE WILL BE LEARNING:

- Understand networking, IP and Mac addresses
- Learn TCP, UDP & 3 way handshake
- Master OSI, DNS, Routing and Subnetting
- Grasp the concept of Reconnaissance
- Learn NMAP port scanning
- Learn to use Hacking tools and CSRF
- Master HTML and SQL injection
- Understand Authorisation and Authentication
- Learn JSON Web Tokens [JSON] with labs
- Explore OSINT with GitHub Recon
- Understand Business Logic Flaws and Password Reset attacks
- Learn Linux, Terminal Commands, Hashing and Bashing
- Enumerate SSH & SMB
- Understand OWASP and solve OWASP SKF labs/DevSlop Pixi
- Understand Cryptography and Encryption



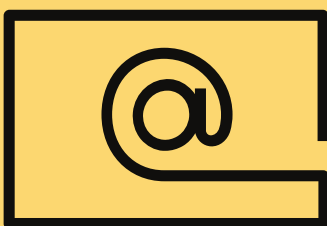
TOPICS WE WILL BE COVERING:

WEEK 1

- Introduction to Cyber Security
- Effective Note Keeping, Important tools and configuration
- Networking 101
- IP Addresses - IPv4, IPv6, Private & Public IP
- Mac Addresses

WEEK 2

- TCP, UDP & 3-way handshake
- Common Ports and Protocols
- OSI model
- DNS and Routing
- Subnetting



WEEK 3

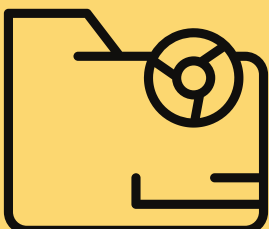
- Information Gathering - Reconnaissance
- Web Application Recon
- Subdomain enumeration
- NMAP Port scanning
- GitHub Recon and Gitrob configuration

WEEK 4

- Burp Suite Configuration(Cracked) & Fundamentals
- HTML & SQL injection
- Authorization & Authentication in Web applications
- Authorization & Authentication attacks Part - 1
- Authorization & Authentication attacks Part - 2

WEEK 5

- JWT Fundamentals
- JWT attacks with lab solving
- CSRF
- Insecure Direct Object Reference - H101
- Business Logic Flaws and Password Reset attacks



WEEK 6

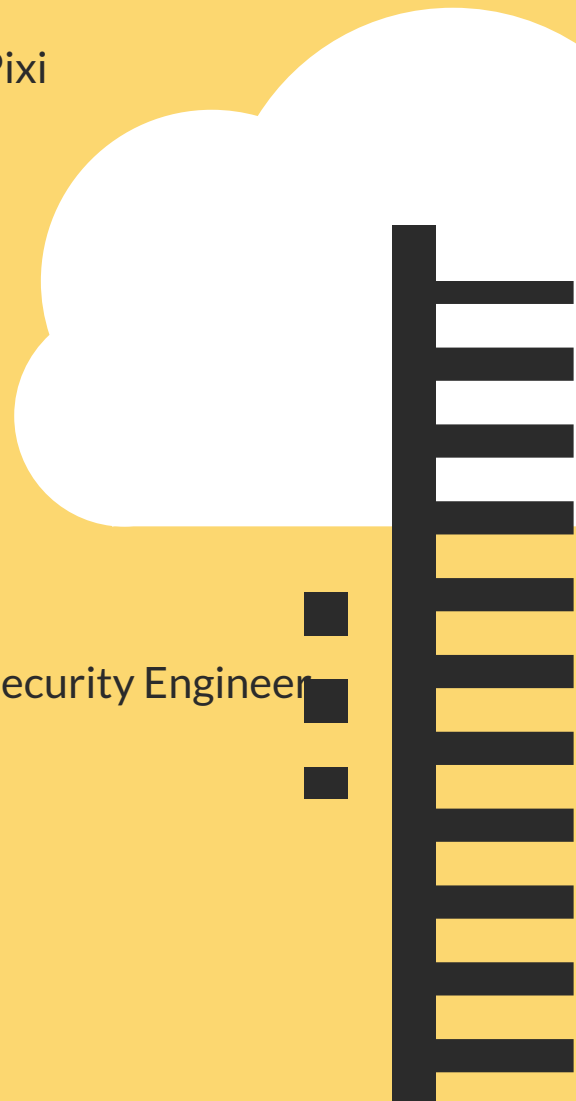
- Linux fundamentals
- Terminal and Linux commands
- BASH Programming Part -1
- BASH Programming Part -2
- Enumerating SSH & SMB

WEEK 7

- NMAP & Masscan scanning
- OWASP top 10
- Solving OWASP Juice shop
- OWASP API Top 10
- Solving OWASP SKF labs/DevSlop Pixi

WEEK 8

- Introduction to Cryptography
- Encryption
- Hashing
- Hashing vs Encryption
- Discussing Interview questions for Security Engineer role



FUNDAMENTALS OF CYBER SECURITY

In this part, we will be covering all the basic and advanced topics needed for understanding further security domains. We will start learning from networking and IPs and then proceed with the succeeding topics. The task will be assigned to you on the basis of the daily teaching program.

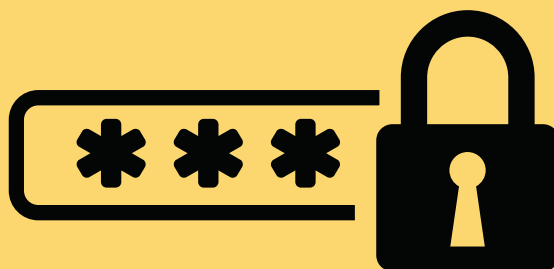
- Networking
- IPv4, IPv6
- Private IP
- Public IP
- Mac Address
- 3 way Handshake
- Ports and Protocol
- OSI model
- DNS and Routing
- Subnetting
- Reconnaissance
- Web Application Recon
- Subdomain enumeration
- NMAP Port scanning



WEB APPLICATION PENTESTING & SECURITY TOOLS

We will help you to configure the following tools needed for Web Application Pentesting.

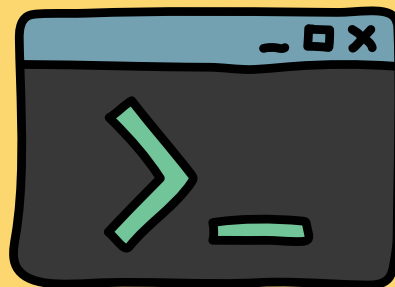
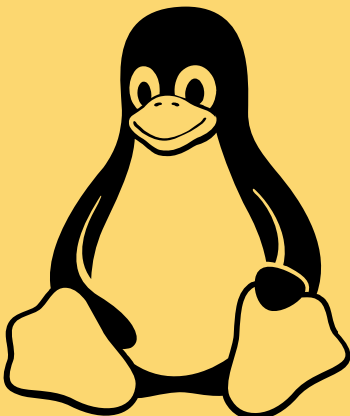
- BURP SUITE Professional
- Open Source Security Tools from GitHub
- HTML injection
- SQL injection
- Authorization and Authentication Attacks
- JWT Fundamentals
- JWT lab
- Cross-Site Request Forgery [CSRF]
- GitHub Recon
- Gitrob configuration
- Business Logic Flaws
- Password Reset attacks



LINUX AND OWASP

We will explore linux software and learn its commands. We will further be learning Bashing and OWASP as mentioned below:

- Linux Fundamentals
- Terminal Commands
- Bash Scripting
- Enumerating SSH
- Enumerating SMB
- NMAP Scanning
- Solving OWASP Juice Shop
- OWASP API
- OWASP SKF labs/DevSlop Pixi



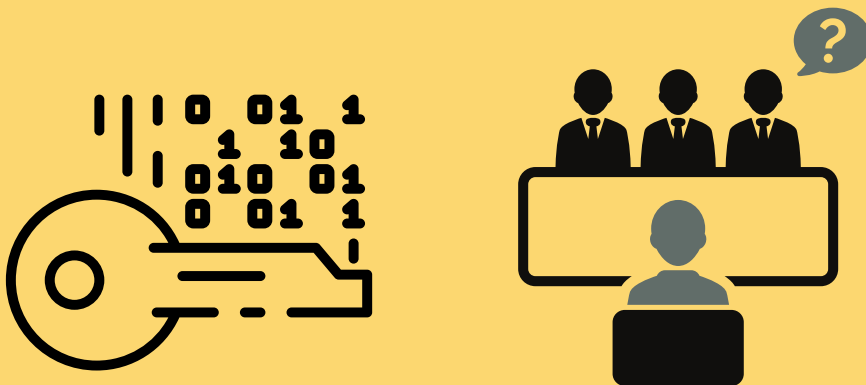
CRYPTOGRAPHY

We will be introduced to cryptography and learn about several related

- Introduction to Cryptography
- Encryption
- Encrypting Tools
- Decrypting Tools
- Hashing
- Hashing vs Encryption

INTERVIEW QUESTIONS

Here we will be discussing several questions that appear in security interviews of various MNCs [Amazon, Google, Facebook, Gojek, etc]



ONE TIME PAYMENT

**FOR ENTIRE 2 MONTH-LONG
TRAINING & INTERNSHIP**

RS.5500

The cost will include the certification of training. On the completion of the final project ,you will receive a completion of internship certificate and a letter of recommendation as well. As all the topics that you cover will also come with a small quiz, upon the completion of the quiz you will receive certificates from IBM, Google, Michigan, and many more companies and universities(for FREE). **Limited seats (120)** so apply now...

LEARN FROM PEOPLE AT:

