



Cyber Security

Cybersecurity & Ethical Hacking
Internship Program



Our Website
www.apexplanet.in



Our Website
www.apexplanet.in

About Us

ApexPlanet Software Pvt. Ltd. – Innovating with Security at the Core

We deliver secure, high-performance web and mobile apps, blending cutting-edge technology with cybersecurity best practices. Our team builds cyber-resilient solutions using secure coding, encryption, and penetration testing to protect your business from evolving threats.

Beyond development, we train the next generation of developers in security-first engineering through hands-on internships.

Partner with us for future-proof digital solutions—where innovation meets ironclad security.

How to Submit Your Internship Task

1. Prepare Your Task

- Complete your task before the submission date.

2. Create a Screen Recording

- Record your project using screen recording software and the video file.

3. Upload Video to LinkedIn

- Log in to LinkedIn.
- Go to your profile, add the video under "Featured."
- Copy the video link.

4. Upload Project to GitHub

- Create a GitHub account (if you don't have one).
- Create a new repository and upload your project files.
- Make the repository public and copy the link.

5. Register and Log In to ApexPlanet

- Go to [ApexPlanet Internship](#).
- Register and log in.

4. Submit Your Task

- Go to "Manage Task."
- Verify using your offer letter ID and email.
- Click on the relevant task button.
- Fill in the details, paste the LinkedIn video link, and the GitHub repository link.
- Submit.

5. Open the Next Task

- After submitting, click to open the next task and repeat the process.

This streamlined process ensures your tasks are submitted professionally and on time.



Our Website

www.apexplanet.in

TABLE CONTENT



Task-1 Foundations of Cybersecurity

Task-2 Network Security & Scanning

Task-3 Web Application Security

Task-4 Exploitation & System Security

Task-5 Capstone Project & Incident Response



Foundation & Environment Setup

Objective:

- Build strong fundamentals in cybersecurity, networking, cryptography, and set up a professional hacking lab.

Steps:

1. Cybersecurity Basics

- Understand the CIA Triad: Confidentiality, Integrity, Availability.
- Explore Threat Types: Phishing, Malware, DDoS, SQL Injection, Brute Force, Ransomware.
- Study Attack Vectors: Social Engineering, Wireless Attacks, Insider Threats.

2. Lab Environment Setup

- Install VirtualBox or VMware.
- Install Kali Linux as the attacker machine.
- Install Metasploitable2 or DVWA (Damn Vulnerable Web App) as target machines.
- Configure a private lab network (Host-Only Adapter).

3. Linux Fundamentals

- File System Navigation (cd, ls, pwd).
- File & Directory Permissions (chmod, chown).
- Package Management (apt, dpkg).
- Networking Commands (ifconfig, ping, netstat, traceroute).



Our Website

www.apexplanet.in

Foundation & Environment Setup

4. Networking Basics

- OSI Model Layers & Functions.
- TCP/IP Protocol Suite.
- DNS & HTTP/HTTPS Deep Dive.
- IP Addressing, Subnetting, and NAT.

5. Cryptography Basics

- Symmetric vs Asymmetric Encryption.
- Hashing (MD5, SHA256).
- Digital Certificates & SSL/TLS.
- Hands-on: Encrypt and Decrypt messages using OpenSSL.

6. Tool Familiarization

- Wireshark (packet capture).
- Nmap (network scanning).
- Burp Suite (web proxy).
- Netcat (network debugging).

Deliverables:

- Lab Setup Report (screenshots of Kali, Metasploitable, Wireshark test capture).
- GitHub Repo with notes & Linux cheat-sheet.
- 5-min Video walkthrough of lab setup.



Objective:

- Learn reconnaissance, scanning, and network traffic analysis.

Steps:

1. Reconnaissance

- Passive Recon: Whois, Nslookup, Google Dorking, Shodan.
- Active Recon: Ping Sweep, Banner Grabbing.

2. Port & Service Scanning

- Nmap TCP & UDP Scans (-sS, -sU).
- Service Version Detection (-sV).
- OS Detection (-O).
- Create a scan report for target systems.

3. Vulnerability Scanning

- Setup OpenVAS or Nessus Essentials.
- Scan test VM (Metasploitable2).
- Analyze Vulnerability Reports (Critical/High/Medium/Low).

4. Packet Analysis with Wireshark

- Capture HTTP, FTP, DNS traffic.
- Filter credentials from unencrypted FTP traffic.
- Analyze SYN flood attack (simulate with hping3).

TimeLine : Days 13-24

TASK - 2



Network Security & Scanning

TimeLine : Days 13-24

TASK - 2

5. Firewall Basics

- Create simple iptables rules (allow/deny specific ports).
- Demonstrate blocking a port scan attempt.

Deliverables:

- Nmap Scan Report + OpenVAS Vulnerability Report.
- GitHub Repo with detailed scan analysis.
- 5-min Demo Video showing a scan & findings.



Web Application Security

TimeLine : Days 25-36

TASK - 3

Objective:

- Identify and exploit OWASP Top 10 vulnerabilities in a controlled lab environment.

Steps:

1. SQL Injection

- Install DVWA in Kali Linux.
- Perform SQL Injection to extract usernames & passwords.
- Demonstrate prevention using Prepared Statements.

2. Cross-Site Scripting (XSS)

- Stored XSS attack on DVWA.
- Reflected XSS using query parameters.
- Mitigation: Input Validation & Content Security Policy (CSP).

3. Cross-Site Request Forgery (CSRF)

- Create a CSRF attack to change a user's password in DVWA.
- Demonstrate token-based protection.

4. File Inclusion Attacks

- Local File Inclusion (read sensitive files).
- Remote File Inclusion (execute malicious code).



Web Application Security

TimeLine : Days 25-36

TASK - 3

5. Burp Suite Advanced

- Intercept and modify login requests.
- Perform fuzzing with Intruder tool.

6. Web Security Headers

- Use securityheaders.com to analyze a test site.
- Add proper HTTP headers in Apache config.

Deliverables:

- Security Testing Report (SQLi, XSS, CSRF with screenshots).
- GitHub Repo with attack scenarios + mitigation notes.
- 8-min Video Demo of an exploitation & its fix.



Exploitation & System Security

Objective:

- Learn penetration testing workflow and exploit vulnerabilities responsibly.

Steps:

1. Penetration Testing Methodology

- Phases: Recon → Scanning → Exploitation → Post-Exploitation → Reporting.
- Document every step in detail.

2. Exploitation with Metasploit

- Exploit a known vulnerability in Metasploitable2.
- Create a reverse shell to gain system access.
- Run post-exploitation commands (sysinfo, hashdump).

3. Password Attacks

- Brute-force SSH login using Hydra.
- Crack hashed passwords with John the Ripper.

4. Social Engineering (Simulation Only)

- Create a phishing simulation page.
- Show awareness training for phishing detection.



Exploitation & System Security

TimeLine : Days 37-48

TASK - 4

5. Malware Basics

- Study how malware works (static vs dynamic analysis).
- Analyze a benign sample in a sandbox environment.

6. System Hardening

- Apply security patches.
- Configure firewall to block malicious traffic.
- Disable unused services.

Deliverables:

- Penetration Testing Report with screenshots.
- GitHub Repo documenting exploitation steps + mitigations.
- 10-min Demo Video of an exploit with explanation.



Capstone Project & Incident Response

TimeLine : Days 49-60
TASK - 5

Objective:

- Apply all skills in a self-chosen capstone project and simulate an incident response.

Steps:

1. Capstone Project Selection (Choose one):

- Web Application Pentest Report (on DVWA/bWAPP).
- Vulnerability Assessment of Test Network.
- Build a Mini SIEM (Security Information & Event Management) with ELK Stack.
- Create Security Awareness Phishing Simulation.

2. Project Planning

- Define Objectives, Scope, Tools, Timeline.
- Create ER Diagram or Network Diagram.

3. Implementation

- Conduct Recon, Scanning, Exploitation (controlled).
- Document Findings with Evidence.
- Suggest Mitigation Strategies.

4. Incident Response Simulation

- Detect attack in logs.
- Contain & eradicate the simulated threat.
- Write Post-Incident Report.



Capstone Project & Incident Response

TimeLine : Days 49-60
TASK - 5

5. Final Documentation

- Prepare Professional Report (with Executive Summary, Methodology, Findings, Mitigations).
- Include ER Diagrams, Screenshots, Tool Outputs.

6. Presentation

- Record a 12-min Final Video showcasing the project.
- Share Hosted Report / GitHub Link.

Deliverables:

- Capstone Project Report PDF (detailed findings + screenshots).
- GitHub Repo with scripts, notes, and methodology.
- 12-min Final Presentation Video.
- Final Submission: Report + GitHub Repo + Video Link.



Thank You For Your Attention

More Information



Our Phone
+91 9905879870



Email
info@apexplanet.in



Our Website
www.apexplanet.in

