Operation CyberShakti

Beginner Ethical Hacking and Advanced Web Pentsting

2-Months Live Training | Course Module

Operation CyberShakti

🔥 **Independence Day Special Training**

💻 **Beginner-Only Batch | ₹3999**

📅 **2 Months | Live Classes | Limited to 10 Students**

🌐 brutsec.com/CyberShakti.pdf

🛡️ **What You Will Learn**

A complete journey from zero to skilled in Ethical Hacking & Web Pentesting.

🧠 **Module 1: Foundation of Ethical Hacking**

- What is hacking? Why hacking matters for India.
- Different types of hackers: Black Hat, White Hat, Grey Hat.
- Hacking vs Pentesting – Real-world use cases.
- Cybersecurity mindset and legal boundaries.

🌍 **Module 2: Footprinting & Reconnaissance (OSINT)**

- Active & passive reconnaissance explained.
- WHOIS, DNS, Netcraft, Shodan, ZoomEye, Censys usage.
- Email harvesting, metadata extraction, subdomain discovery.
- Google Dorking and real OSINT tricks.

🌐 **Module 3: Scanning & Enumeration**

- Port scanning with Nmap – theory & labs.
- Banner grabbing, service enumeration.
- Identifying vulnerable services, SMB/FTP scans.
- Nmap scripting engine (NSE) in depth.

💣 Module 4: Vulnerability Analysis

- CVEs, CVSS scoring, threat modeling basics.
- How to perform vulnerability assessments (Nessus/OpenVAS).
- Manual vs automated testing – when to use which.

🔐 Module 5: System Hacking (Windows & Linux)

- Brute-force attacks with Hydra, Medusa.
- Password cracking with John the Ripper and Hashcat.
- Privilege escalation (Windows & Linux paths).
- Creating backdoors, persistence methods.
- Post-exploitation tricks.

🌐 Module 6: Web Application Pentesting

- Understanding how web apps work – client/server model.
- OWASP Top 10 explained with practical labs:
- XSS (Reflected, Stored, DOM)
- SQL Injection (Auth bypass, Data dump)
- File Upload Exploits
- Command Injection
- Path Traversal
- XXE, SSRF, Host Header Attacks
- Burp Suite Mastery: Repeater, Intruder, Decoder, Comparer.

🔍 Module 7: Information Disclosure & Misconfigurations

- Finding sensitive info in robots.txt, .git folders, error pages.
- Exploiting misconfigured cloud buckets (S3, GCP).
- Directory brute-forcing with ffuf/dirsearch.

👁️ Module 8: Sniffing, Spoofing & MITM Attacks

- ARP poisoning with Bettercap, DNS spoofing.

- Packet sniffing with Wireshark – capturing passwords in real time.
- Evil twin attacks on WiFi networks.

⚙️ Module 9: Session Hijacking & Insecure Auth

- Understanding how sessions work.
- Session token stealing, fixation, and prediction.
- JWT and cookie abuse techniques.

🦠 Module 10: Malware, Trojans & Backdoors

- Real malware case studies.
- Building undetectable payloads using msfvenom.
- RATs & keyloggers – how attackers think.

🚨 Module 11: Denial of Service & Web Attacks

- Layer 4/7 DoS/DDoS attacks explained.
- Slowloris, LOIC/HOIC, HTTP request flooding.
- Web logic abuse for taking sites down silently.

🧩 Module 12: Bypassing Security Controls

- Bypassing 403/401 restrictions, WAFs.
- IP restrictions, user-agent, HTTP method tricks.
- Evasion techniques used in the wild.

🧪 Module 13: Bug Bounty Methodology

- Complete bug bounty mindset.
- How to choose a program.
- Real recon workflow: subdomain hunting, asset discovery, chaining vulnerabilities.
- Reporting and disclosure etiquette.

🧰 Module 14: Tools You'll Master

- Burp Suite, Nmap, Nikto, Hydra, ffuf, Subfinder, Amass, SQLMap, Dirsearch, Metasploit, Wireshark, Gobuster, John/Hashcat, httpx, gf, and more.

🧠 **Bonus Topics (Time-Permitting):**

- Basics of Mobile App Pentesting (Android).
- Cyber law & responsible disclosure in India.
- How to build your GitHub and write reports like a pro.

💼 **You'll Be Able To:**

1. Perform real-world penetration tests.
2. Find & report bugs on platforms like HackerOne & Bugcrowd.
3. Secure your own systems.
4. Understand and talk like a professional ethical hacker.

📩 **To Enroll / Ask Queries**

- Telegram: @wtf_brut
- WhatsApp: wa.link/brutsecurity
- 📞 +918945971332
- 🌐 brutsec.com

💥 **From complete beginner to battlefield-ready.**

This is not just a course. It's a mission.🛡️ Operation CyberShakti