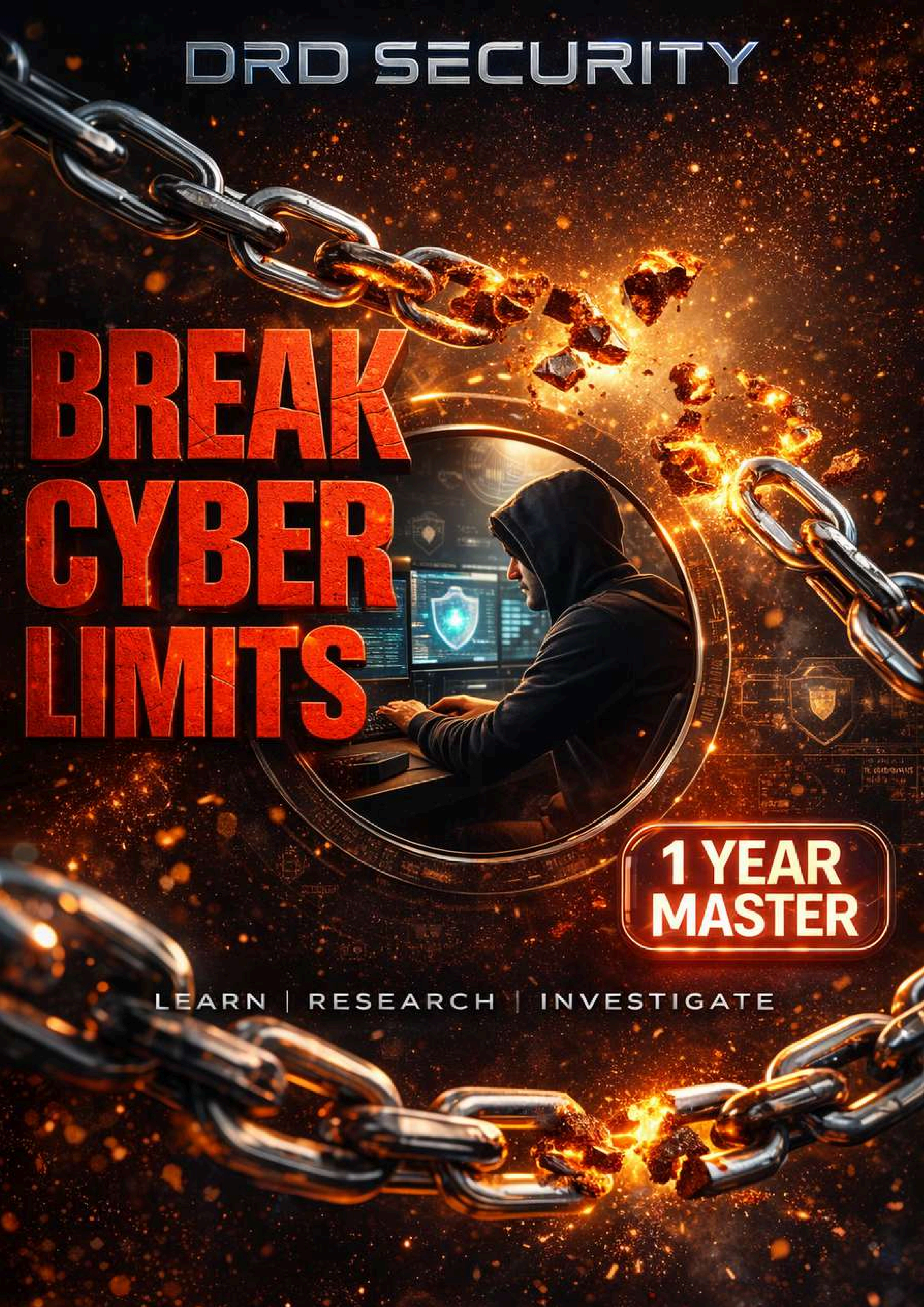

DRD SECURITY
BREAK
CYBER
LIMITS
1 YEAR
MASTER
LEARN | RESEARCH | INVESTIGATE

# D.R.D SECURITY PVT.LTD.

DRD Security Pvt. Ltd. is an Indian company that specializes in providing various security solutions, such as manned guarding services, electronic surveillance, and integrated security systems. They cater to a wide range of sectors, including industrial, commercial, residential, and government institutions, offering both physical and electronic security services.
the company actively engages with the cybersecurity community through global collaborations like Cyber Peace, D.R.D Global Clubs, where Cyber Abdul Masood serves as the Chapter Leader for Lucknow. This involvement in community-driven initiatives underlines D.R.D Security dedication to knowledge-sharing and collective efforts to strengthen cybersecurity measures.

At the heart of D.R.D Security's offerings are their cutting-edge cybersecurity courses, tailor- made for students aspiring to build a career in Information Technology or Cyber Security and Ethical Hacking. These courses cover a spectrum of vital areas including Penetration Testing, Digital Forensics, Advance Networking, Audit, Cloud Computing, Linux, Red Teaming, Blue Teaming, Purple Teaming Corporate Trainings, Compliance Trainings 70+ Scholarhip, Internship Programs, Life Time Membership many more services. Hackers Meetup conduct all over India, Cyber Security Awareness Programs, Internships Programs many more.

Dedicated Investigation Wing: D.R.D Security maintains a highly skilled team of investigators specializing in cybercrime. These experts meticulously analyze digital evidence, track down perpetrators, and build strong cases for prosecution. By bringing cybercriminals to justice, we not only deter future attacks but also offer a sense of security and restoration to victims.
Our Commitment: Building a Safer Digital World Social Media Fraud, and Investigation in Cyber Crimes, Cyber Law, Jurisprudence of Indian Cyber Law, Admissibility of electronic evidence, Cyber Crimes & Conventional crimes, Drafting of a Cyber complaint, .E-Commerce, Data Privacy Overview, IPR in Cyber space, Digital Intermediary many more.

The Revolution Wing understands that complex security solutions can be intimidating. Their mission is to create user-friendly tools that make staying safe online accessible to everyone, regardless of technical expertise.
Stay tuned! We look forward to sharing more about the revolutionary tools D.R.D Security is developing to keep you safe in the ever-evolving digital landscape.

# D.R.D SECURITY PVT.LTD.


*Mr. Abdul Masood is a prominent figure in the field of cybersecurity, known for his extensive contributions as the Founder, Director, and Lead Ethical Hacking Faculty at D.R.D Security Pvt. Ltd. He also serves as the Chapter Leaders to across the International or National and is an active member of OSINT India. His career is marked by a deep commitment to enhancing cybersecurity education and providing robust security solutions to various organizations.*

**Early Life and Education**

*Details about Abdul Masood's early life and education are not widely documented. However, his professional journey reflects a strong foundation in cybersecurity and ethical hacking, suggesting a background rich in technical education and hands-on experience.*

**Professional Career**

*Abdul Masood has played a pivotal role in supporting various law enforcement agencies, including the Police, Intelligence Bureau (IB), and the Central Bureau of Investigation (CBI). His expertise has been instrumental in assisting these agencies with cybersecurity matters, showcasing his commitment to national* ***security and cyber defense.***

*At D.R.D Security Pvt. Ltd. , Abdul Masood has been a driving force in providing both training and Vulnerability Assessment and Penetration Testing (VAPT) solutions under one roof. This integrated approach ensures that clients receive comprehensive cybersecurity services tailored to their specific needs. His leadership has positioned D.R.D Security Pvt. Ltd. as a trusted partner for organizations seeking to fortify their digital defenses.*

**Educational Initiatives**

*Recognizing the growing demand for skilled cybersecurity professionals, Abdul Masood has dedicated significant efforts to education and training. He has developed a one-year Diploma in Cyber Security course in Lucknow, meticulously designed with a focus on practical experience and real-world applications. This program not only equips students with the necessary skills but also guarantees 100% placement upon successful completion, reflecting his commitment to bridging the gap between education and employment in the cybersecurity sector.*

**Community Engagement**

*Abdul Masood fosters a collaborative environment for cybersecurity enthusiasts and professionals to share knowledge, discuss emerging threats, and develop innovative solutions. His involvement with OSINT India further underscores his dedication to the field, contributing to the collective efforts in open-source intelligence and cybersecurity awareness.*

**Conclusion**

*Abdul Masood's multifaceted career in cybersecurity encompasses leadership, education, and active collaboration with law enforcement agencies. His endeavors have significantly contributed to the advancement of cybersecurity practices and education in India, making him a respected figure in the community.*

# D.R.D SECURITY PVT.LTD.

# LEVEL - 1

## IN DEPTH NETWORKING

- Module 01 : Introduction to Networking
- Module 02 : OSI Model.
- Module 03 : TCP/IP Model.
- Module 04 : Subnetting / Summarisation.
- Module 05 : Packet Flow in Same & Different Network
- Module 06 : Information About Networking Device.
- Module 07 : IP / ICMP.
- Module 08 : APIPA.
- Module 09 : Address Resolution Protocol.
- Module 10 : Routing Protocols (Static & Dynamic).
- Module 11 : Static - Next Hop / Exit Interface
- Module 12 : Dynamic - RIP / EIGRP / OSPF & BGP
- Module 13 : Wan Technologies
- Module 14 : NAT
- Module 15 : ACL
- Module 16 : Dynamic Host Configuration Protocol
- Module 17 : Telnet & SSH
- Module 18 : Load Balancing Protocol
- Module 19 : Layers 2 Protocols
- Module 20 : VLAN
- Module 21 : Different Types of STP
- Module 22 : Ether Channel (L2)
- Module 23 : Port Security

127.0.0.1

**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

D.R.D SECURITY PVT.LTD.

# LEVEL - 2

## LINUX ESSENTIALS

- Module 01 : Getting Started with Red Hat Enterprise Linux.
- Module 02 : Accessing the Command Line.
- Module 03 : Managing Files from the command Line
- Module 04 : Getting Help in Red Hat Enterprise Linux
- Module 05 : Analyzing and Storing Logs
- Module 06 : Managing Local Users and Groups
- Module 07 : Controlling Access to Files
- Module 08 : Monitoring & Managing Linux Process
- Module 09 : Controlling Services and Daemons
- Module 10 : Configuring & Securing SSH
- Module 11 : Managing Networking
- Module 12 : Archiving and Transferring Files
- Module 13 : Installing Software Packages
- Module 14 : Accessing Linux File System
- Module 15 : Analyzing Servers

D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.

# D.R.D SECURITY PVT.LTD.

# LEVEL - 3

## MALWARE ANALYSIS

- Module 01 : Introduction Malware Analysis.
- Module 02 : Basic Analysis Technique And Tools
- Module 03 : Understanding File Format (L)
- Module 04 : Setting Up Your Isolated Environment /Malware (L)
- Module 05 : Static Analysis Basic/Advanced
- Module 06: Dynamic Analysis Basic/Advanced (Practical on Sample and Live Host)
- Module 07: Malware Functionality (Programming Language)
- Module 08: Reverse Engineering
- Module 09: Assembly Language (Intel X86/64)
- Module 10: Basic Programming Structures and Unions
- Module 11: Debugging Malware
- Module 12: Working with DLL/Rootkit/Network and Registry/API Call/Import and String Section
- Module 13: Code Injection/Extraction (Programming Language)
- Module 14: Advanced Computer and Network Test for Malware Analysis
- Module 15: Real-Time Attack Monitoring with IRC Logs (Internet Relay Chat) in Depth
- Module 16: Overview
- Module 17: Report

RANSOMWARE

D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.

# D.R.D SECURITY PVT.LTD.

# LEVEL - 4

## ETHICAL HACKING

- Module 1: Introduction to ethical hacking, including AI-driven techniques
- Module 2: Foot printing and reconnaissance
- Module 3: Scanning networks
- Module 4: Enumeration
- Module 5: Vulnerability analysis
- Module 6: System hacking
- Module 7: Malware threats
- Module 8: Sniffing
- Module 9: Social engineering
- Module 10: Denial-of-service
- Module 11: Session hijacking
- Module 12: Evading IDS, firewalls, and honeypots
- Module 13: Hacking web servers
- Module 14: Hacking web applications
- Module 15: SQL injection
- Module 16: Hacking wireless networks
- Module 17: Hacking mobile platforms
- Module 18: IoT and OT hacking
- Module 19: Cloud computing
- Module 20: Cryptography

127.0.0.1

# D.R.D SECURITY PVT.LTD.

# LEVEL - 5

## ADVANCE PENETRATION TESTING

- Module 01 : Introduction
- Module 02 : In-Depth Scanning
- Module 03 : Exploitation
- Module 04 : Command Line Fun
- Module 05 : Getting Comfortable with Kali Linux
- Module 06 : Bash Scripting
- Module 07 : Practical Tools
- Module 08 : Active Information Gathering
- Module 09 : Passive Information Gathering
- Module 10 : Introduction to Buffer Overflows
- Module 11 : Buffer Overflows
- Module 12 : Fixing Exploits
- Module 13 : Locating Public Exploits
- Module 14 : Antivirus Evasion
- Module 15 : File Transfers
- Module 16 : Windows Privilege Escalation
- Module 17 : Linux Privilege Escalation
- Module 18 : Password Attacks
- Module 19 : Port Redirection and Tunnelin
- Module 20 : Active Directory Attacks
- Module 21 : Power Shell Empire
- Module 22 : Trying Harder : The Labs
- Module 23 : Penetration Test Breakdown

**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

# D.R.D SECURITY PVT.LTD.

## LEVEL - 6

## CYBER FORENSICS INVESTIGATION

- Module 01 : Introduction Computer Forensics
- Module 02 : Methods by which Computer gets Hacked.
- Module 03 : Computer Forensics Investigation Process
- Module 04 : Digital Evidence Gathering.
- Module 05 : Computer Forensics Lab.
- Module 06 : Setting up Forensics Lab.
- Module 07 : Understanding Hard Disk.
- Module 08 : File Systems Analysis : Linux/Window/mac.

- Module 09 : Windows File Systems forensics.
- Module 10 : Data Acquisition Tools and techniques.
- Module 11 : Data Imaging Techniques and Tools.
- Module 12 : Recovery Deleted Files and Folders.
- Module 13 : Deleted Partitions Recovery Technique.
- Module 14 : Forensics Investigations Using Encase Tool
- Module 15 : Stenography and Image File Forensics
- Module 16: Application Password Crackers

- Module 17 : Log Computing and Event Correlation
- Module 18 : Network Forensics Tools : Cellebrite Tool
- Module 19 : Log Computing and Event Correlation
- Module 20 : Network Forensics Tools : Cellebrite Tool
- Module 21 : Investigating Tools
- Module 22 : Investigating Network Traffic : Wireshark
- Module 23 : Investigating Wireless Attacks
- Module 24 : Investigating Web Application Attacks via Logs
- Module 25 : Tracking and Investigating Various Email Crimes

**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

# D.R.D SECURITY PVT.LTD.

## LEVEL - 7

## WEB APPLICATION SECURITY

- Module 01 : Introduction
- Module 02 : Owasp Top 10
- Module 03 : HTTP and HTTPS
- Module 04 : Types of Url, VPN And PROXY
- Module 05 : OSI Model
- Module 06 : Cryptography and Encryption
- Module 07 : Types of Method and Description
- Module 08 : TCP three way handshak working
- Module 09 : DNS and Root name server
- Module 10 : BOXES testing (Black box , white box , grey box)
- Module 11 : Directory path traversal attack
- Module 12 : os command injection
- Module 13 : XXE - XML External Entities
- Module 14 : File upload vulnerability
- **Module 15 : Sql injection**
- **Module 16 : information disclosure**
- **Module 17 : SSRF - Server Site Request Forgery**
- **Module 18 : Google Dorking/ Zone transfer attack**
- **Module 19 : : XSS - Cross Site Scritpting**
- **Module 20 : Session Management and Broken Authentication Vulnerability**
- **Module 21 : cross site request foregery (CSRF)**
- **Module 22 : DOM Based vulnerability**
- **Module 23 : Cross-origin resource sharing (CORS)**
- **Module 24 : server side template injection**
- **Module 25 : Access control vulnerability**




**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

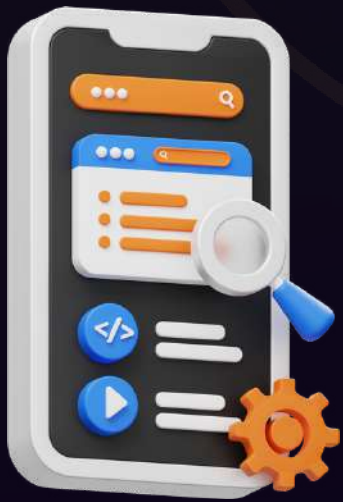
# D.R.D SECURITY PVT.LTD.

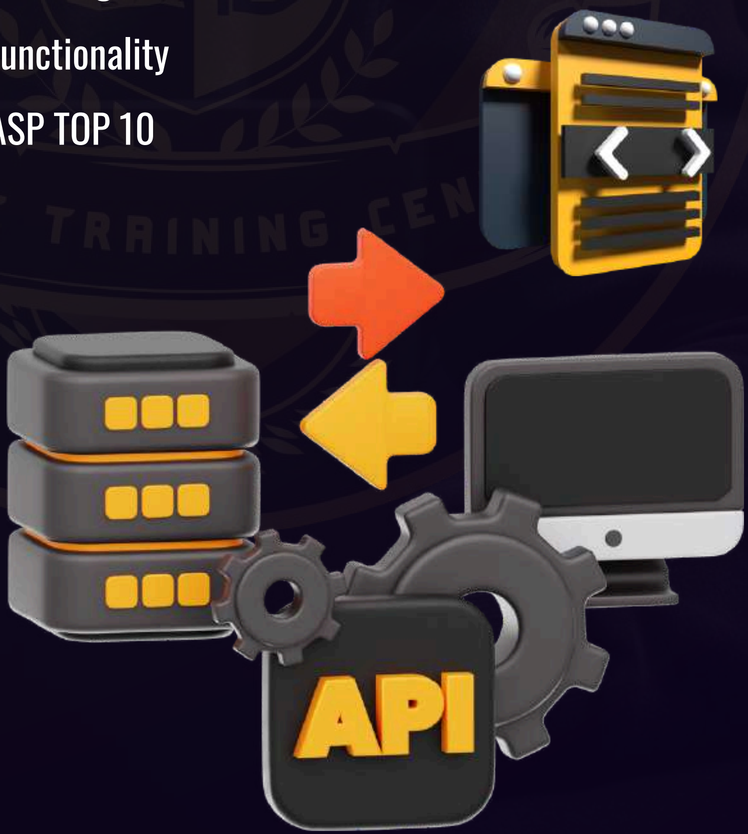
# LEVEL - 8

## MOBILE APPLICATION SECURITY

- Module 01 : Improper Platform Usage.
- Module 02 : Insecure Data Storage.
- Module 03 : Insecure Communication
- Module 04 : Insecure Authentication
- Module 05 : Insufficient Cryptography
- Module 06 : Insecure Authorization
- Module 07 : Client Code Quality
- Module 08 : Code Tampering
- Module 09 : Reverse Engineering
- Module 10 : Extraneous Functionality
- Module 11 : Mobile OWASP TOP 10

- INSECURE DATA
- CRYPTO
- CC QUALITY
- REVERSE ENGINEERING
- CODE TAMPERING






D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.

# D.R.D SECURITY PVT.LTD.

# LEVEL - 9

## INTERNET OF THINGS (IOT) PENTESTING

- Module 01 : Overview of Why IoT is so important.
- Module 02 : Introduction of IoT
- Module 03 : Introduction to Sensor Network & Wireless protocol
- Module 04 : Review of Electronics Platform, Production & Cost Projection
- Module 05 : Conceiving a new IoT product- Product Requirement document for IoT
- **Module 06 : Introduction to Mobile app platform & Middleware for IoT**
- **Module 07 : Machine learning for intelligent IoT**
- **Module 08 : Analytic Engine for IoT**
- **Module 09 : Iaas/Paas/Saas-IoT data, platform and software as a service revenue model**

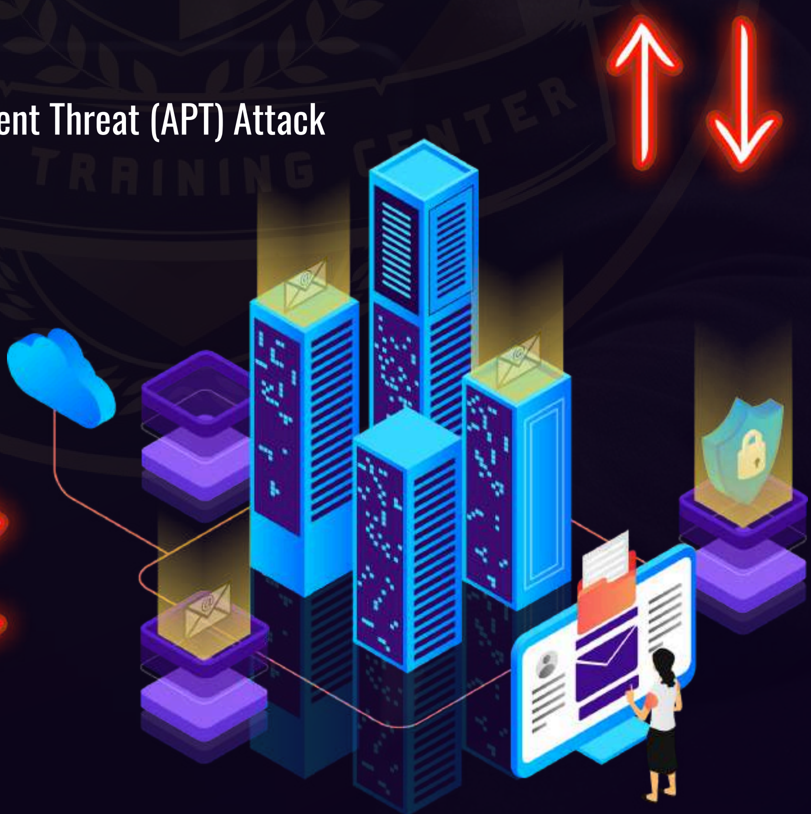
**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

# D.R.D SECURITY PVT.LTD.

# LEVEL - 10

## END POINT SECURITY

- Module 01 : Implementing Internet Security Anti Virus.
- Module 02 : MFA Multifactor Authentication
- Module 03 : Mobile Device Management For Industry.
- Module 04 :Security Information and Event Management
- Module 05 : Mitre Attack Framework
- Module 06 : EDR
- Module 07 : MDR
- Module 08 : Next Generation Firewall
- Module 09 : Unified Threat Management
- Module 10 : Physical Security
- Module 11 : ISO 27001
- Module 12 : Advance Persistent Threat (APT) Attack



**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

# D.R.D SECURITY PVT.LTD.

# LEVEL - 11

## AWS ASSOCIATE

**Module 01 : Designing Highly Available, cost effective, scalable systems**

(a) Planning and Design

(b) Monitoring and Logging

(c) Hybrid IT Architectures

(d) Elasticity and Scalability

**Module 02 : Implementation and Deployment**

(a) Amazon EC2

(b) Amazon S3 (c) Amazon Web Service Cloud Formation

(d) Amazon Web Service VPS

(e) Amazon Web Service IAM

**Module 03 : Data Security**

(a) AWS IAM (Identify and Access Management)

(b) Amazon Web Service VPC

(c) Encryption Solutions

(d) Cloud watch logs

(e) Disaster Recovery

(f) Amazon Route 53

(g) AWS Storage Gateway

(h) Amazon Web Service Import/Export

**Module 04 : Troubleshooting**

# D.R.D SECURITY PVT.LTD.

# LEVEL - 12

## AWS SECURITY

- Module 01 : Given an AWS Abuse Notice, Evaluate a Suspected Compromised Instance or Exposed Access Key
- Module 02 : Verify that the Incident Response plan includes relevant AWS services
- Module 03 : Evaluate the Configuration of Automated Alerting and Execute Possible Remediation of Security-Related Incidents and Emerging Issues
- Module 04 : Design and implement security monitoring and alerting
- Module 05 : Troubleshoot security monitoring and alerting
- Module 06 : Design and Implement a Logging Solution
- Module 07 : Design Edge Security on AWS
- Module 08 : Troubleshoot Logging Solutions
- Module 13 : Troubleshoot an Authorization and Authentication System to Access AWS Resources.
- Module 14 : Design and implement key management and use
- Module 15 : Troubleshoot key management
- Module 16 : Design and implement a data encryption solution for data at rest and data in transit

**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

# D.R.D SECURITY PVT.LTD.

# MASTER
## RED TEAMING

**Module 1: Introduction to Red Teaming**
- Understanding Red Teaming: Objectives, methodologies, and real-world applications
- Difference Between Red Teaming, Pentesting & Blue Teaming
- Adversarial Mindset & Thinking Like an Attacker
- Case Studies of Notable Red Team Operations

**Module 2: Reconnaissance & OSINT (Open-Source Intelligence)**
- Passive vs. Active Reconnaissance
- OSINT Techniques & Tools (Maltego, Recon-ng, SpiderFoot)
- Domain & Subdomain Enumeration (Amass, Sublist3r, crt.sh)
- Social Engineering Recon & Profiling Targets
- Threat Intelligence & Dark Web Research

**Module 3: Initial Access & Exploitation Techniques**
- Phishing Attacks & Social Engineering (SET, Evilginx)
- Web Application Attacks (SQLi, XSS, SSRF, IDOR, etc.)
- Exploiting Misconfigurations in Cloud & On-Premises Environments
- Zero-Day Exploitation & Custom Exploit Development
- Exploiting Active Directory Weaknesses

**Module 4: Privilege Escalation & Lateral Movement**
- Windows Privilege Escalation (PowerUp, WinPEAS, BloodHound)
- Linux Privilege Escalation (LinPEAS, GTFOBins, Kernel Exploits)
- Credential Dumping & Pass-the-Hash Attacks
- Lateral Movement Techniques (PsExec, RDP Hijacking, WinRM, Kerberoasting)
- Bypassing Endpoint Detection & Response (EDR) Solutions

**Module 5: Persistence & Defense Evasion**
- Creating & Maintaining Persistence on a Target System
- Process Injection & Rootkits
- Fileless Malware & Living-off-the-Land Binaries (LOLBins)
- Domain Persistence & Golden Ticket Attacks (Mimikatz, Rubeus)
- Defensive Evasion & Avoiding Detection (Obfuscation, Packing, Encryption)

**Module 6: Command & Control (C2) Frameworks**
- Understanding C2 Concepts & Communication Channels
- Popular C2 Frameworks (Cobalt Strike, Empire, Sliver, Mythic)
- Building a Custom C2 Infrastructure
- Detecting & Evading Network Defenses
- Payload Delivery & Execution Techniques

**Module 7: Red Teaming in Cloud Environments**
- Cloud Recon & Enumeration (AWS, Azure, GCP)
- Exploiting Cloud Misconfigurations (S3 Bucket Misconfig, IAM Privilege Escalation)
- Attacking Kubernetes & Container Security
- Cloud Persistence Techniques
- Detection & Evasion in Cloud Environments

**Module 8: Physical Red Teaming & Social Engineering**
- Physical Security Assessments (Badge Cloning, Lockpicking, RFID Attacks)
- Social Engineering & Pretexting Techniques
- Weaponized USB & Drop Devices (Rubber Ducky, Bash Bunny)
- Bypassing Security Guards & Physical Controls
- Red Teaming Physical Entry Methods

**Module 9: Adversary Simulation & Purple Teaming**
- MITRE ATT&CK Framework & Adversary Emulation Plans
- Collaboration Between Red & Blue Teams
- Threat Hunting & Defensive Countermeasures
- Automating Red Team Operations with MITRE Caldera, Atomic Red Team
- Using SIEM & EDR Logs to Simulate and Detect Attacks

**Module 10: Reporting & Post-Engagement Activities**
- Creating Effective Red Team Reports
- Communicating Findings to Executives & SOC Teams
- Remediation Recommendations & Incident Response
- Lessons Learned & Continuous Improvement
- Ethics & Legal Considerations in Red Teaming
- Final Assessment & Red Team Challenge
- Hands-on Red Teaming Engagement Simulation
- Red vs. Blue Team Capture the Flag (CTF)
- Live Assessment of a Simulated Enterprise Network
- Certification Exam & Final Evaluation

**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**

# D.R.D SECURITY PVT.LTD.

# MASTER

## BLUE TEAMING

**Module 1: Introduction to Blue Teaming & Defensive Security**

- Understanding Cybersecurity Defense: Red vs. Blue vs. Purple Teams
- Roles & Responsibilities of a Blue Team
- Cyber Kill Chain & MITRE ATT&CK Framework
- Defensive Mindset: Proactive vs. Reactive Defense

**Module 2: Security Operations Center (SOC) & SIEM Mastery**

- Overview of SOC Architecture & Components
- SIEM (Security Information and Event Management) Fundamentals
- Log Collection, Parsing & Correlation
- Hands-on with SIEM tools (Splunk, ELK, Microsoft Sentinel)
- Real-world Incident Detection with SIEM

**Module 3: Threat Intelligence & Adversary Profiling**

- What is Cyber Threat Intelligence (CTI)?
- OSINT (Open-Source Intelligence) for Threat Hunting
- Tactical, Operational, Strategic Intelligence
- Tracking & Analyzing APT Groups (Advanced Persistent Threats)
- Threat Intelligence Platforms (TIPs) & STIX/TAXII

**Module 4: Digital Forensics & Incident Response (DFIR)**

- Incident Response Lifecycle (Preparation, Detection, Containment, Eradication, Recovery)
- Memory & Disk Forensics (Autopsy, Volatility, FTK Imager)
- Network Forensics & Packet Analysis (Wireshark, Zeek)
- Malware Analysis & Reverse Engineering Basics
- Hands-on Incident Handling Scenarios

**Module 5: Endpoint Security & Hardening Strategies**

- Windows & Linux Security Monitoring
- EDR (Endpoint Detection & Response) Tools (CrowdStrike, SentinelOne, Microsoft Defender ATP)
- Sysmon for Advanced Endpoint Logging
- PowerShell & WMI Threat Hunting
- Securing Active Directory & Group Policy (GPO)

**Module 6: Network Security & Intrusion Detection**

- Firewalls, IDS/IPS (Suricata, Snort, Zeek)
- Network Traffic Analysis & Threat Detection
- Securing VPNs & Zero Trust Architectures
- DNS & Web Filtering for Network Defense
- Real-world Case Study: Detecting Lateral Movement

**Module 7: Cloud Security & Defense Strategies**

- Cloud Security Fundamentals (AWS, Azure, GCP)
- Identity & Access Management (IAM) Security
- Cloud Security Monitoring & Logging (AWS GuardDuty, Azure Sentinel)
- Securing Serverless & Kubernetes Workloads
- Cloud Incident Response & Threat Hunting

**Module 8: Threat Hunting & Advanced Detection Techniques**

- Understanding Threat Hunting Methodologies
- Hypothesis-driven vs. Intelligence-driven Threat Hunting
- Using YARA & Sigma Rules for Detection
- Behavioral Analytics & Anomaly Detection
- Hands-on Threat Hunting in ELK & Splunk

**Module 9: Security Automation & SOAR (Security Orchestration, Automation, and Response)**

- Automating Incident Response with SOAR (Cortex XSOAR, Splunk Phantom)
- Playbook Development for Automated Defense
- Scripting for Blue Team (Python, PowerShell, Bash)
- Automating Threat Intelligence Enrichment
- Case Study: Automating Phishing Response

**Module 10: Cyber Resilience & Compliance**

- Security Frameworks: NIST, CIS, ISO 27001, GDPR
- Risk Assessment & Vulnerability Management
- Security Awareness Training for Organizations
- Building a Cyber Resilient Organization
- Final Project: Developing a Full-Scale Blue Team Defense Strategy

D.R.D SECURITY PVT.LTD.

# MASTER
## PURPLE TEAMING

**Module 1: Introduction to Purple Teaming**
- Understanding Red Team vs. Blue Team vs. Purple Team
- Importance of Collaboration Between Offensive & Defensive Teams
- Overview of Cyber Kill Chain & MITRE ATT&CK Framework
- Case Studies of Successful Purple Teaming Engagements

**Module 2: Threat Intelligence & Adversary Simulation**
- Understanding Advanced Persistent Threats (APTs)
- Threat Hunting with Cyber Threat Intelligence (CTI)
- Intelligence-Driven Defense: Utilizing Open-Source Threat Feeds
- Hands-on Lab: Analyzing Real-World APT Reports

**Module 3: Red Team Tactics & Techniques**
- Reconnaissance: OSINT, Active & Passive Recon
- Exploitation: Vulnerability Research & Exploitation Techniques
- Privilege Escalation: Local & Network-Based Escalation
- Lateral Movement & Persistence: Pass-the-Hash, Kerberoasting
- Evasion Techniques: Antivirus & EDR Bypasses
- Hands-on Lab: Conducting a Full Red Team Attack Chain

**Module 4: Blue Team Defensive Strategies**
- Security Monitoring & Logging: SIEM Tools (Splunk, ELK)
- Network Traffic Analysis: Detecting Suspicious Activities
- Incident Detection & Response: SOC Operations & IR Playbooks
- Forensic Analysis: Memory & Disk Forensics with Volatility
- Hands-on Lab: Threat Hunting & Log Analysis

**Module 5: Purple Teaming & Attack Simulation**
- Aligning Offensive Tactics with Defensive Detection
- Simulating Advanced Attacks with MITRE ATT&CK
- Purple Team Engagement Planning & Execution
- Measuring Detection & Response Effectiveness
- Hands-on Lab: Conducting a Purple Team Assessment

**Module 6: Deception Technologies & Threat Hunting**
- Deploying HoneyTokens, HoneyPots & HoneyFiles
- Understanding & Implementing EDR & XDR Solutions
- AI & ML for Threat Detection & Anomaly Detection
- Hands-on Lab: Implementing Deception Technologies

**Module 7: Red Team & Blue Team Toolkits**

Red Team Tools:
- Cobalt Strike, Metasploit, Empire, Covenant
- BloodHound, Mimikatz, Responder, CrackMapExec

Blue Team Tools:
- Splunk, ELK, Velociraptor, Sysmon
- Wireshark, Suricata, OSQuery, Zeek
- YARA Rules & Sigma Rules for Detection

**Module 8: Real-World Simulations & Case Studies**
- Simulating APT Attacks in a Lab Environment
- Purple Teaming for Ransomware Defense
- Breaking & Defending Active Directory (AD)
- Log4Shell & Supply Chain Attacks
- Purple Teaming in Cloud Security (AWS/Azure)

**Module 9: Certifications & Career Growth**
- Certified Red Team Professional (CRTP)
- Certified Purple Team Professional (CPTP)
- MITRE ATT&CK Defender (MAD)
- OSCP vs. OSDA vs. CRTE – Which Path to Choose?
- Building a Career in Purple Teaming
- Final Project: Conduct a Full Purple Team Engagement
- Students will conduct a Red Team Attack Simulation
- Blue Team will detect, analyze & mitigate attacks
- Purple Team will enhance detection & security controls

D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.

# D.R.D SECURITY PVT.LTD.

## ALL INDIA SESSIONS


INTEGRAL UNIVERSITY


DELHI FCRF


SHRI RAMSWAROOP MEMORIAL UNIVERSITY


DEVX VADODARA


SR GROUP OF INSTITUTIONS


DEV X PUNE


ZONE STARTUPS MUMBAI


IITM Group of Institutions, Murthal (Haryana)


LUCKNOW


Indian Institute Of Management (IIM)


INTEGRAL


DEVX AHMEDABAD


HINDU GIRLS COLLEGE (SONIPAT)


Kamla Nehru Group of Institutions (KNGI)


DELOITTE BANGALORE

## MORE UPCOMING MEETUPS

D.R.D GLOBAL CLUB

D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.

# D.R.D SECURITY PVT.LTD.

## FACILITIES

- Global Meetups Access
- 1000+ chatgpt prompts
- Lifetime Access
- Premium Tools 110 GB
- 100% Job Placement
- Internship Opportunity
- 12gb + ebooks
- Connect With Cyber Community
- Lifetime Membership
- Give 1-on-1 guidance


Certificate Demo

TOTAL 17 Certificates you in this master course


Final Certificate Demo

## CONTACT

+91-9335041909

+91-8601030795

+91-7800122004

Daliganj , Lucknow - 226020

contact@drdsecurity.com

drdsecurity.com

**D.R.D (DIVINE REVOLUTION DEVELOPMENT) SECURITY PVT.LTD.**