RECON

CYBER SECURITY

WHO WE ARE?

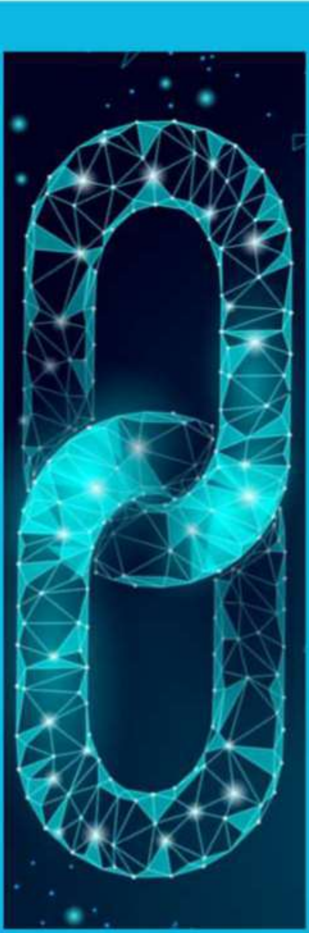
Recon Force Pvt. Ltd. is one of the jobs oriented Best **Cyber Security Training** institute in Delhi founded by academicians and managed by the highly experienced professional group. We are providing high-quality education to the students. The Institute offers **Cyber Security courses** for graduate and undergraduate students in the areas of Professional Courses. We are expertise in providing online best **Cyber Security Training** as well as Corporate Training to our students. Complete **Cyber Security** Training provided by Recon Cyber Security is designed as per the Industrial Requirement with Live Projects. At Recon Cyber Security, we offer our student's classroom training, corporate training, and online training for **Cyber Security** Training Programs. Ideally located, with the great ambiance and highly motivated staff makes Recon Cyber Security as a result-oriented best Cyber Security training institute.

CYBER SECURITY TRAINING & CONSULTING COMPANY.

About

We are a Cyber security Training and consulting company, which aims to provide best in class cyber security training with certificates in PAN India and across the globe, with highly skilled professional trainers. Apart from training we also aim to provide Cyber security solution, Testing services to different corporate clients in most affordable prices.

We want deliver a learning experience where theoretical knowledge is combined with dedicated practical to fill the gap between industry and education bodies.



Other objective of our company is to make students industry ready to work as a complete asset right from the day of joining, so that company and employ both feel more satisfied and valued in industry culture and work in the direction to making this technological world more secure and easy with their shear dedication.

RECON
CYBER SECURITY

OUR TRAINING CRITERIA

Corporate Area:

- IT Training Firms
- IT Organizations/ Society
- IT Consultants
- IT Experts
- IT Officers
- IT Institutions & Colleges

Individuals:

- IT Graduated or Computer Science Students
- School Students
- College Students
- IT Professionals
- IT and LAW Officers

Governance:

- Security Agencies
- Security Groups
- Govt. IT Institutions
- IT Govt. & Security Officers

OUR DELIVERED WORKSHOPS

MIET Jammu

NIIT Nemrana

IIT Delhi

IIT Roorkee

Lingava’s University

ARO-TEC Angola, South Africa

RECON
CYBER SECURITY

CYBER SECURITY TRAINING

Advanced Networking

Linux Essentials

Ethical Hacking

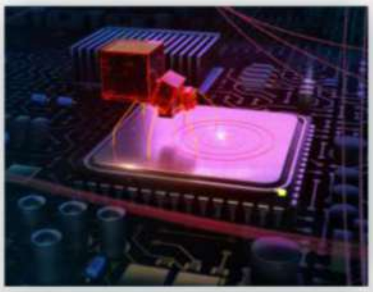
Python Programming

Penetration Testing

Web-App Penetration Testing

Mobile-App Penetration Testing

Apple IOS App-Pen-Testing



Bug Hunting

API Testing

Malware Analysis

CTF Challenge

RECON
CYBER SECURITY

CYBER SECURITY CERTIFICATION TRAINING

CEH-V11 Training

CEH Master

ECSA Practical

LPT [License Pen-Tester]

CompTIA Security+

CompTIA Network+

CompTIA PenTest+

OSCP Training

RECON
CYBER SECURITY

OTHER TRAININGS

```
 sure no other blo
def row_available(block, ro
# Determine which of the mai
boardRow = int(block / 3);
good = True
for b in range(boardRow * 3, (
if b != block:
if num in board[b][row]:
good = False
break
return good
```

Python

Data Science with Python

Machine Learning with Python

Artificial Intelligence with Python

OUR SERVICES

SOC Solution

A **security operations center** (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery.

Security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

SOURCE CODE REVIEW

ReconForce Pvt. Ltd. provides customized secure code review services to help you identify and fix security vulnerabilities in your application at the development stage. A number of security loopholes in both web and mobile apps originate right when the code is being written and developers either ignore or are unaware of secure coding practices. A secure code review is perhaps a better investment of your time and resources than penetration testing is and can help you fix basic flaws when it is still quick and easy to do so, and before any major damage has been done. While a number of app development companies use automated solutions to scan their code, these tools are often not adequate to detect and address all security issues in application code

Our code review team has years of experience both creating applications and conducting secure code reviews. We use a combination of automated and manual reviews to find and suggest fixes for coding errors that may eventually lead to serious security issues.

```
    border: 1px solid rgba(255,255,255,.1);
    color: #fff;
    }

/*
.btHardRoundedButtons any(select, textarea,
.btSoftRoundedButtons any(select, textarea,
/* Form elements */
select,
input {
    font-family: 'GreycliffCF-Regular', Arial
    font-weight: normal;
    font-style: normal;
    }
input:not([type='checkbox']):not([type='radio
button {
    -webkit-appearance: none;
    }
input:not([type='checkbox']):not([type='radio
textarea,
    font: inherit;
    width: 100%;
    background: transparent;
    line-height: 1;
    font-family: 'GreycliffCF-Heavy', Arial,
    font-weight: normal;
    font-style: normal;
    font-size: .8em;
    width: 100%;
    display: block;
    padding: .8em;
    background: transparent;
    }
.btTextRight input:not([type='checkbox']):not(
.btTextRight textarea,
.btTextRight select {
    text-align: right;
    }
input:not([type='checkbox']):not([type='radio
select {
.btHardRoundedButtons a.select2-choice {
.btHardRoundedButtons
    border-radius: 50px;
    }
.btSoftRoundedButtons input:not([type='checkbox
.btSoftRoundedButtons a.select2-choice {
.btSoftRoundedButtons
    border-radius: 3px;
    }
.btHardRoundedButtons textarea,
.btHardRoundedButtons select {
    border-radius: 20px;
    }
.btSoftRoundedButtons textarea,
.btSoftRoundedButtons select {
    border-radius: 3px;
    }
input:not([type='checkbox']):not([type='radio
textarea:focus {
    -webkit-box-shadow: 0 0 4px 0
    box-shadow: 0 0 4px 0
    border: 1px solid #333;
```

VA/PT Services

Vulnerability Assessment and Penetration Testing (VAPT) are both security services that focus on identifying vulnerabilities in the network, server and system infrastructure. Both the services serves a different purpose and are carried out to achieve different but complimentary goals.

A Penetration Test is an in-depth expert-driven activity focussed on identifying various possible routes an attacker could use to break into the network. In-addition with the vulnerabilities it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter.

- Any and all devices with an IP address can be considered for VAPT activity.
- Penetration Testing should focus on your organizations external parameters (IP Addresses, Offices, People, etc)
- Vulnerability Assessment should focus on your internal infrastructure (servers, databases, switches, routers, desktops, firewalls, laptops, etc)

RED TEAMING

Red Team testing is also known as an Adversary Simulation or simply Red Teaming. During Red Team testing, highly experienced security professionals take on the guise of a real attacker and attempt to breach the organization's cyber defences. The attack scenarios they enact are designed to exercise various attack surfaces presented by the organization and identify gaps in preventative, detective, and response related security controls. These attacks leverage a full range of tools available to the most persistent attackers—including social engineering and physical attack vectors, from careful crafted phishing emails to genuine attempts to breach onsite security and gain access to server rooms.

Prior to the assessment, rules of engagement are established between the Red Team members and the smallest possible set of participants within the organization to be tested. This number will vary but is typically no more than 5 people in key positions to view the organizations detection and response activities. Based on the rules of engagement, a Red Team may target any or all of the following areas during the exercise:

RECON
CYBER SECURITY

CONTACT US:

☎ +91-8595756252 | +91-8800874869

✉ Info@reconcybersecurity.com

www.reconcybersecurity.com

A-115, Gali No - 1, Main Shakharpur Road, Laxmi
Nagar, Delhi-110092, Near Metro Pillar No - 34

Gali no 8, Plot No 308, Main Market Sant
Nagar Burari Near aggarwal sweets, Delhi 110084