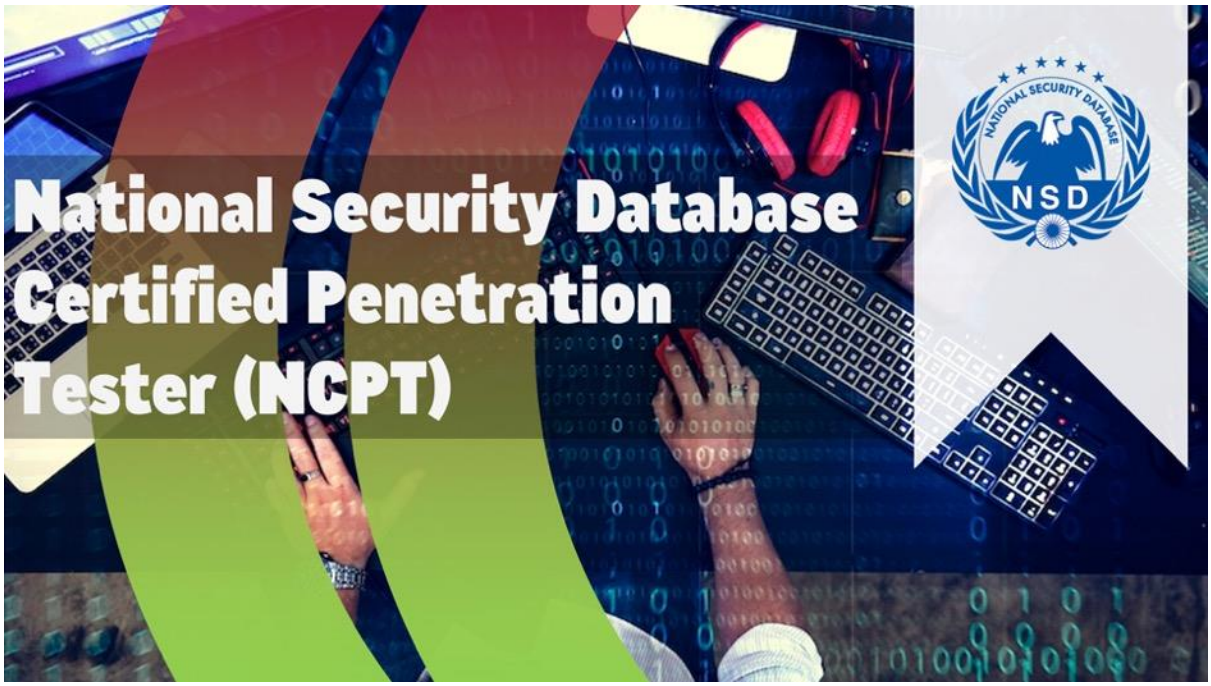


About SkillsDA

SkillsDA is a unique platform that brings **Academia, Industry and Skilled staff** together to delight the end **Customers**. We are a training & upskilling eco-system that caters to all 4 stakeholders across several sectors that are in dire need of high-quality experience.

SkillsDA offers training for the technical staff, in collaboration with the Industry / Brand owners in line with industry specifications. Individuals who wish to upskill & train themselves can access SkillsDA training & certification. Customers will have access to these trained staff either directly through the SkillsDA App/Website.

SkillsDA is an ISO 9001:2015 certified cyber security training institute.

We are part of the eco system with ISAC and Cyberange that has a PPP with NCIIPC and MOUs with AICTE and CERT for capacity building in cyber security as part of the Nation's Security.

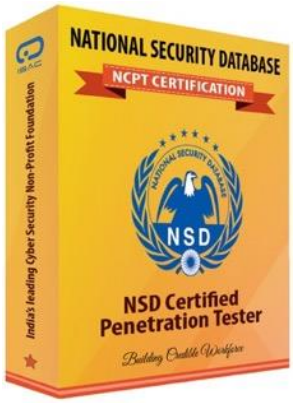
About National Security Database

National Security Database (NSD) is a prestigious certification program from Information Sharing and Analysis Center (ISAC), India's leading non-profit foundation committed to securing the cyber space of the nation by providing credible platforms for Information Sharing & capacity development.

ISAC is a Public Private Partner (PPP) with National Critical Information Infrastructure Protection Center (NCIIPC), under Prime Minister's Office, Partner with CERT-IN, under Ministry of Electronics and Information Technology and All India Council of Technical Education (ACITE), under Ministry of Human Resources and Development, Government of India.

The NSD Certification is awarded to credible & trustworthy Information security experts with proven skills to protect the National Critical Infrastructure & economy of the country.

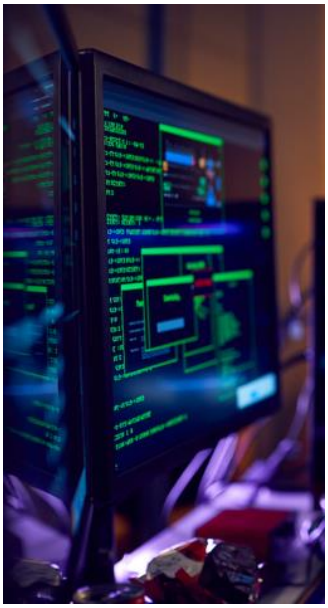
About Penetration Testing Certification



Penetration testing domain from NSD is a recognized empanelment program for information security professionals with hands-on proven experience in vulnerability analysis and penetration testing. The domains test a candidate's skill, approach and knowledge that can provide an organization with a reliable workforce for detection and mitigation of cyber security threats in a timely manner.

The program is a **foundation** for many other job roles including Security Information and Event Management (SIEM), Computer Forensics, Web Application Security, ISO 27001 Compliance, PCI-DSS, Internal IT Security Audit etc.

Course Objectives



1. Learn how to gather information
2. Understanding social engineering
3. Understanding system security
4. Learn about password security
5. Gain understanding of malwares
6. Gain skills in Vulnerability analysis
7. Conduct web security audits
8. Conduct network audits
9. Learn about exploitation
10. Creating professional reports

Course Conduct

Pre-qualification

- Understanding of OS Concepts.
- Exposure to Python will be an added advantage
- Knowledge of networking concepts such as DNS, TCP/IP
- Be comfortable with command line tools
- Basics of using Linux
- Keen interest in new technologies with research approach

Course Modules Covered under the Penetration Testing Certification

1. Ethics and Culture
2. Enterprise Security Challenges
3. Information Gathering
4. Introduction to Social Engineering
5. Systems Security
6. Password Hacking
7. Viruses and Trojans
8. Network and Web Application Security
9. Exploiting Approaches
10. Reporting

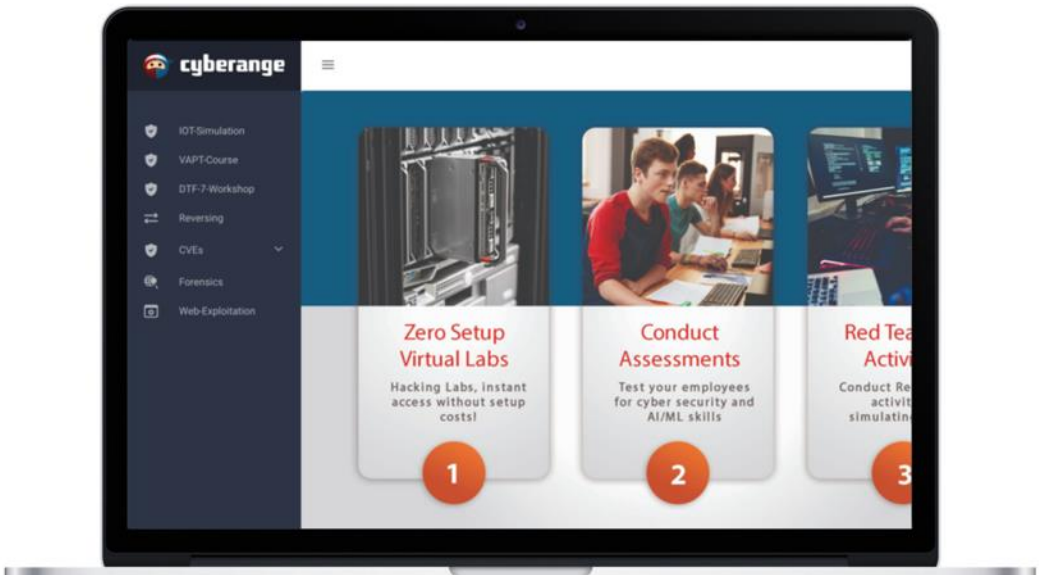
The NCPT certification is constantly updated with new techniques and approaches.

Assisted Fully Online Course

You can complete the NCPT certificate completely online, you will also receive live tutorials from our experts on the topic, you can confidently master the subject at your pace.

You can also download the Teachable Mobile App on iPhone / iOS to access your course on the go.

Powered by Online Virtual Labs



Get trained online with Cyberange ® Virtual Labs - Launch servers / applications at a click of a button and start attacking using latest tools & techniques. Access over 300+ Virtual labs for learning VAPT, Forensics, SOC Analysis, Web Security, IOT Security, Reversing and Latest attack vectors.

You only need a web-browser and internet connection to access all the labs. No need to download any tools or install any applications as everything is provided online for your comfort.

Detailed Couse Outline

Ethics and Culture

Understanding the ethics and culture behind the motivation and behaviour of hackers and security researchers is essential to gain the right perspective in not only handling and anticipating security incidents but also respecting the effort of hackers in modernising and securing much of today's technology. The domain tests a candidate's knowledge on the current trend of hacker ethics and beliefs.

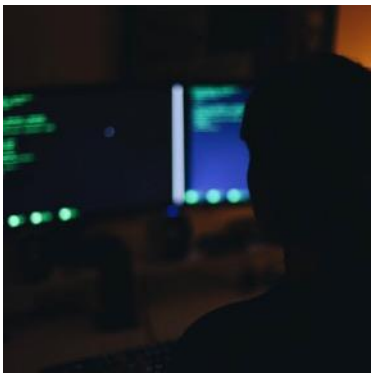
The candidate is expected to research on various hacker groups, their language, lingo used, broad activities etc. and understand their motivation. Depending on the exam paper, you may be asked to write a short essay of 300 words during the exam on this subject.

Enterprise Security Challenges

Running a business is not easy. With high capital costs, manpower costs and maintenance, most organizations focus on ensuring they are able to market and sell their services and products in a profitable manner. With thin profit margins, Information security and its associated costs is always the last aspect of investment.

Even as organizations do invest in Information security, there are multiple internal challenges of skilled manpower, limitations of resources, time consuming processes and funds. There is always an opportunity to make mistakes that can compromise the organization network and it's sensitive information by a persistent attacker. The objective of this domain to make the candidate realise that it is always possible to hack any organization, no matter how big or small.

Information Gathering



One of the most important skills for a penetration tester, detailed information gathering can often give insight and leads for hard-to-find deployed systems.

This domain, in the context of the examination focuses on candidate's skill to plan and collect information about a target organization or its assets for effective use in further vulnerability analysis and penetration testing.

The candidate is tested on their knowledge for effectively using search engines such as BING, Google, Shodan etc and documenting their findings for further use.

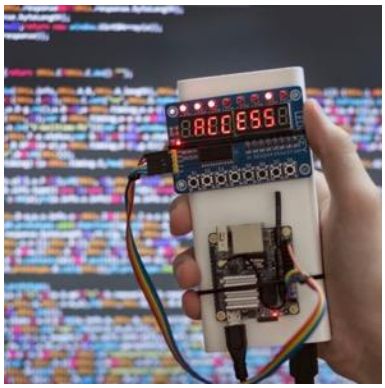
Social Engineering

From making a phone call to an unsuspecting employee for gathering sensitive information to sending a legitimate looking email to hack accounts, Social Engineering is one of the most successful techniques used by the attackers against their targets.

We look at how hackers exploit love, faith, belief, trust, anger, hatred, generosity etc. for their gains and advantage by social engineering.

Some of the questions expected in the lab exam include drafting an email to a target for gaining trust, crafting a phishing mail, approaches for using social media to gain credibility or proving their story to a possible victim etc.

Systems Security



Finding vulnerabilities in systems and compromising them is a key skill for a successful penetration tester. This can be done best by professionals who understand the systems and their workings in detail. The domain focusses on various offensive attacks to bypass systems security.

From the context examination, the candidate will be tested for technical competencies on using various offensive tools and their approach to compromise a system. Information Security professionals must constantly upgrade their knowledge in this domain.

Password Hacking

Passwords are the basic form of protection used by network devices and systems for allowing access to resources. Each system or technology may employ a different approach for using and managing passwords for access control and hence a strong knowledge of various password hacking techniques is crucial for security professional conducting an assessment.

Some of the areas covered in this domain include use of steganography, rainbow tables, decrypting password hashes, using brute force techniques etc. The candidate may be assessed for their skills in using the right approach to gain passwords for a system in a limited time.

Malwares

Malwares are the most prized weapons of attackers as they provide extraordinary capabilities in accessing infected systems and networks. With over a million new malware variants released every six months on the internet and a few dozen anti-virus companies to defend against them, the battle among the enterprise and the attackers is constantly increasing in complexity.

A good understanding of various malwares such as viruses, Trojans, worms, rootkits, botnets etc is essential to allow a professional in handling a compromised system. While use of malwares in a penetration testing assignment is unconventional, it should not be prohibited as it is the only way to test the effectiveness of deployed anti-measures.

The examination involves testing a candidate's skill and knowledge of handling a malware and using them for effectively compromising systems.

Network, Web Application and Social Media Security

Denial of service attack is the most common form of network attack used by attackers to voice their protest or take down an organization. As a penetration tester, it is important to test how vulnerable an asset or a network is from this attack. From the context of examination, a candidate may be tested for their knowledge of such attacks and countermeasures commonly used.

This domain also covers Web application security and the candidate is expected to be well versed with OWASP Top 10 attacks with hands-on experience. The examination includes detailed testing of skills in web application hacking and security.

Exploiting Approaches

This is the most advanced and important domain in examination. From using a remote exploit to a local exploit, the skill mostly allows the attacker to gain administrative access to the targeted system.

The examination includes testing of pivoting skills, using metasploit, compiling and running exploits, using zero days etc. The approach of the candidate in their choice of exploit and use is also ranked.

Reporting

In this module, we focus on various methods of reporting and how to present the findings professionally to the senior management.

Why join the National Security Database

With 300,000 plus jobs available in India alone, it is increasingly becoming difficult for companies to find good cyber security professionals. Organizations no longer want to trust professionals who become "ethical hackers" by simply passing an online objective based exam, as they seldom have the real world perspective and confidence to execute the job once given. Professionals with incomplete knowledge are not only putting their organization at risk, but also their Nation, as they handle sensitive projects impacting the economy of the country.

The National Security Database is the only not-for-profit program, well recognized and respected by various Corporate and Government organizations for its stringent process and hands-on lab exams for assessing the credibility of a professional.

When you pass the rigorous lab exams from National Security Database, you not only prove your credibility and skills, but also enter the elite database of chosen professionals in India who are the first preference by the law enforcement, corporate and multiple Government organizations for cyber security jobs and sensitive positions.

The domain requirements have been carefully chosen after extensive survey of the business need and reflect the latest skills needed by the Corporate Industry.

Benefits to Certified Professionals

1. Gain recognition for your skills from the National Security Database
2. Exclusive access to Priority Job reference Network
3. Up to 3 Job Interviews on passing NSD Lab exams
4. Get connected with local law enforcement and Intelligence agencies to support them in various Cybercrime and related cases
5. Qualify to participate in exclusive cyber security projects open only for National Security Database professionals by various Government of India organizations
6. Network with elite cyber security professionals and hackers in India
7. Special benefits for entrepreneurs for start-ups in Information Security domain

Benefits for Employers

1. Hands-on proven skills recognized by National Security Database mean less time in training and faster "business ready" professionals
2. Hire with Confidence - Minimize your risks as you always hire the right people with right skills
3. Clean Exit Program empowers your business and ensures peace of mind as candidates will not risk violating the code of ethics
4. Provides increased credibility for your organization when working with vendors, contractors and government organizations
5. Guaranteed discounts on Training and security events across India for your IT staff, supported by SkillsDA

Questions?

Please contact us on info@skillsda.com for any further queries.

NSD Certified Penetration Testing Course
(Under ISAC – AICTE MoU)
Delivered by
SkillsDA – ISO 9001: 2015 Training Center

Highlights of NCPT Programme

- ✓ **Course duration 45+ Hours**
- ✓ **More than 120+ Lecture & 25+ videos**
- ✓ **25+ Virtual Labs**
- ✓ **Self-paced online programme combined with instructor assisted classes**
- ✓ **Course includes 10 hours of practical hands on smart city simulator-based training at SkillsDA campus**
- ✓ **Internship Certificate**
- ✓ **Placement support**
- ✓ **NSD Professional Penetration Tester Certificate for qualified students**
- ✓ **Unlimited E-Learning Access & 30 Days of Virtual Lab access**
- ✓ **Course Fee Rs.25,000 + GST**

For Course demo & registration: **https://elearn.skillsda.com**

Contact Us

INGU's Knowledge Academy Pvt Ltd.

Plot No.193, Nehru Nagar 1st Main Road, OMR Kottivakkam, Chennai – 600096, INDIA

Mobile: **+91 9090599696** | +91 **9090589696**