Ducara Info Solutions (P) Ltd.

C|NPT

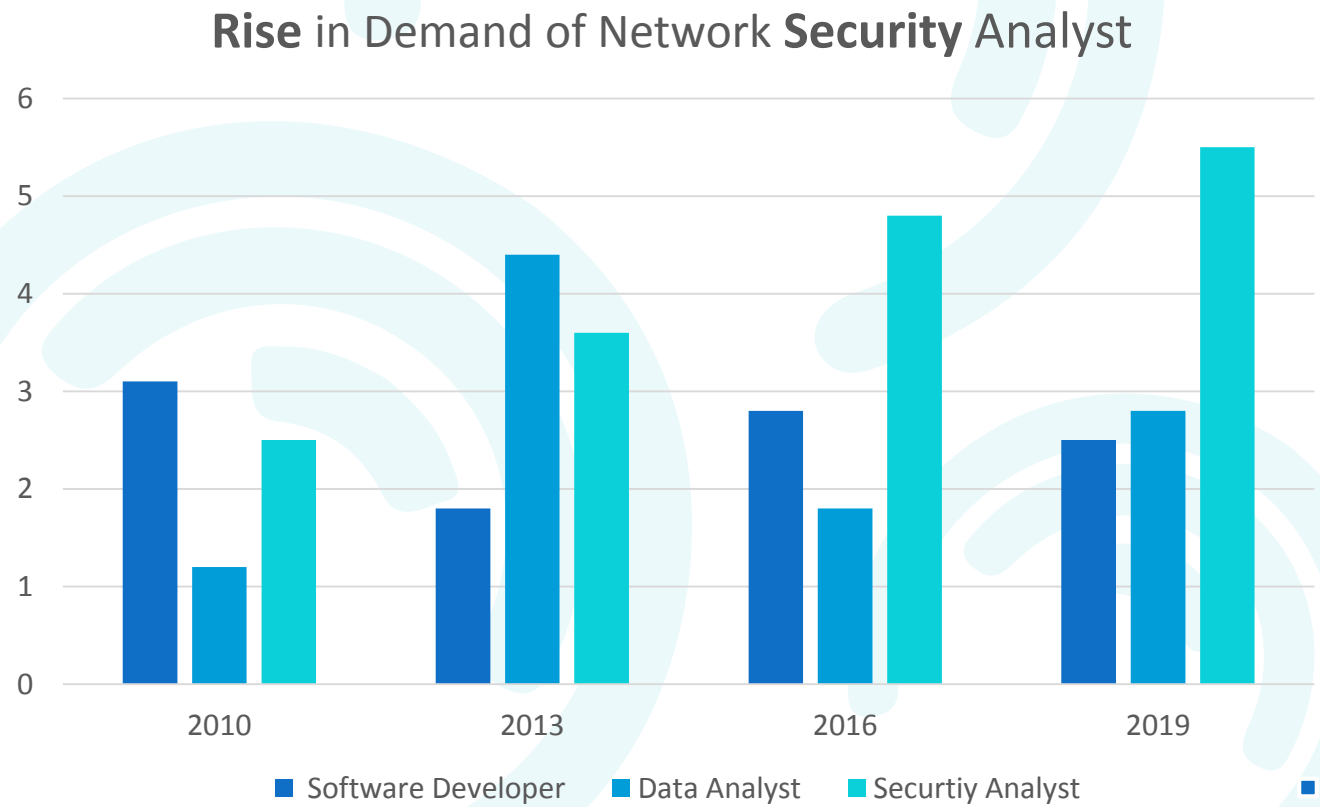
Certified Network Penetration Tester

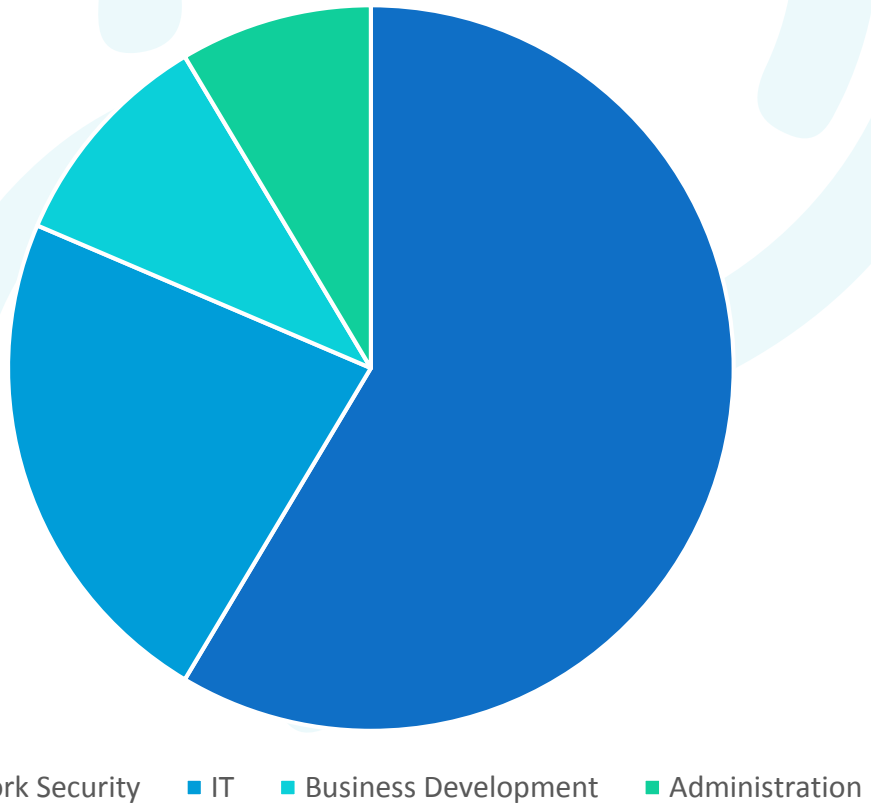
WHY C|NPT?

Network **Penetration** Testing is an authorized, proactive attempt to measure the security of an IT system by safely exploiting its vulnerabilities, mostly to evaluate application **Flaws**, improper configurations, **Risky** end-user behavior.

WHAT TREND SAYS?

The need for **Penetration** testers has grown well over what the IT industry ever anticipated. Running just a vulnerability scanner is no longer an effective method to determine whether a **Business** is truly secure. Pen-testers are among the **Highest** paid professionals in the IT industry.





TARGET AUDIENCE

DURATION: 40 HRS

PENETRATION TESTERS

ETHICAL HACKERS

SECURITY AUDITORS

FORENSICS SPECIALISTS

The Network Pen-tester program is designed to make you an **Expert** in vulnerability management and implement an end-to-end **Robust** vulnerability management and penetration testing program. Primary audience for this certification is cyber security personnel and **Defenders**.

WHAT IS THE OBJECTIVE?

Individuals **certified** at this level will have a demonstrated **understanding** of IT Security**.**

- Serve as the central point of contact for **Enterprise Security** for other Technology teams within the organization.
- **Scan** and test security architectures for various information systems.
- Design and implement architectures that will allow business requirements to be met with a minimal degree of **Risk** to the organization.
- Represent security **Platform** in development and implementation of the overall global enterprise architecture.
- **Conduct** a full-scale, high-value penetration test and develop the most effective penetration testing **skills** to protect your Network.
- Conduct an end-to-end pen test, applying **knowledge**, tools, and principles.
- Every organization needs skilled information security personnel who can find vulnerabilities and **mitigate** their effects.
- Exploit vulnerabilities in a **realistic** sample network, demonstrating the skills.

Become an **Expert** with Ducara, the stage is all set, get **Certified** with our best Network **Penetration** testing program.

C|NPT
CERTIFIED NETWORK PENETRATION TESTER

SCAN YOUR NETWORK FOR VULNERABILITIES

DUCARA

WHAT YOU WILL LEARN IN THE COURSE?

1. VULNERABILITY MANAGEMENT GOVERNANCE
2. PENETRATION TESTING BASICS
3. SECURITY ASSESSMENT PREREQUISITES
4. CUSTOMERS & LEGAL AGREEMENTS
5. NETWORK INFORMATION GATHERING
6. NETWORK SCANNING
7. NETWORK VULNERABILITY ASSESSMENT
8. NETWORK EXPLOITATION
9. SYSTEM & PASSWORD EXPLOITATION
10. PRIVILEGE ESCALATION & EXPLOITATION
11. WIRELESS EXPLOITATION
12. SNIFFING & SPOOFING
13. FIREWALL PENETRATION TESTING
14. IDS PENETRATION TESTING
15. WRITING THE PENETRATION TESTING REPORT

MODULE 1

VULNERABILITY MANAGEMENT GOVERNANCE

1. **Security** basics
2. **Need** for Security Assessments
3. **Business drivers**
4. **Calculating** ROIs
5. **Setting** up the Context
6. **Policy** & Procedure
7. **Penetration** Testing Standards
8. **Industry** Standards

DUCARA

MODULE 2

PENETRATION TESTING BASICS

1. **Vulnerability** Assessment
2. **Goals** and Objectives
3. **Types** of Penetration Testing
4. **Phases** of Penetration Testing
5. **Gathering** Requirements
6. **Preparing** Test Plan
7. **Providing** Test Objectiveness & Boundaries
8. **Project** Management
9. **Third-party** Approvals
10. **Categorization** of Vulnerabilities

MODULE 3

SECURITY ASSESSMENT PREREQUISITES

1. **Target** Scoping and Planning
2. **Gathering** Requirements
3. **Deciding** type of Vulnerability Assessment
4. **Estimating** the Resources and Deliverables
5. **Preparing** a Test Plan and Test Boundaries
6. **Getting** Approval and Signing NDAs

MODULE 4

CUSTOMERS & LEGAL AGREEMENTS

1. **Legal** Consequences
2. **Confidentiality** and NDA Agreements
3. **Penetration** Testing Contract
4. **Liability** Issues
5. **Negligence** Claim
6. **Drafting** Contracts
7. **Rules** of Engagement (ROE)
8. **ROE** includes Key Elements
9. **Description** of Key Elements
10. **Steps** for Framing ROE
11. **Clauses** in ROE

MODULE 5

NETWORK INFORMATION GATHERING

1. **Discovering** Live Servers over the Network
2. **Bypassing** IDS/IPS/Firewall
3. **Discovering** ports over the Network
4. **Using** unicornscan for faster Port Scanning
5. **Service** Fingerprinting
6. **Determining** the OS using nmap and xprobe2
7. **Service** Enumeration
8. **Open-source** Information Gathering

MODULE 6

NETWORK SCANNING

Check for Live Systems by using Ping

Check for Open and Closed Ports using Nmap

Various Scanning Techniques by using Nmap

MODULE 7

NETWORK VULNERABILITY ASSESSMENT

Manual Vulnerability Assessment

Integrating nmap with Metasploit

Metasploitable Assessment with Metasploit

OpenVAS Framework

MODULE 8

NETWORK EXPLOITATION

Operations

Intelligence & Counter Intelligence

Reconnaissance

Surveillance

MODULE 9

SYSTEM & PASSWORD EXPLOITATION

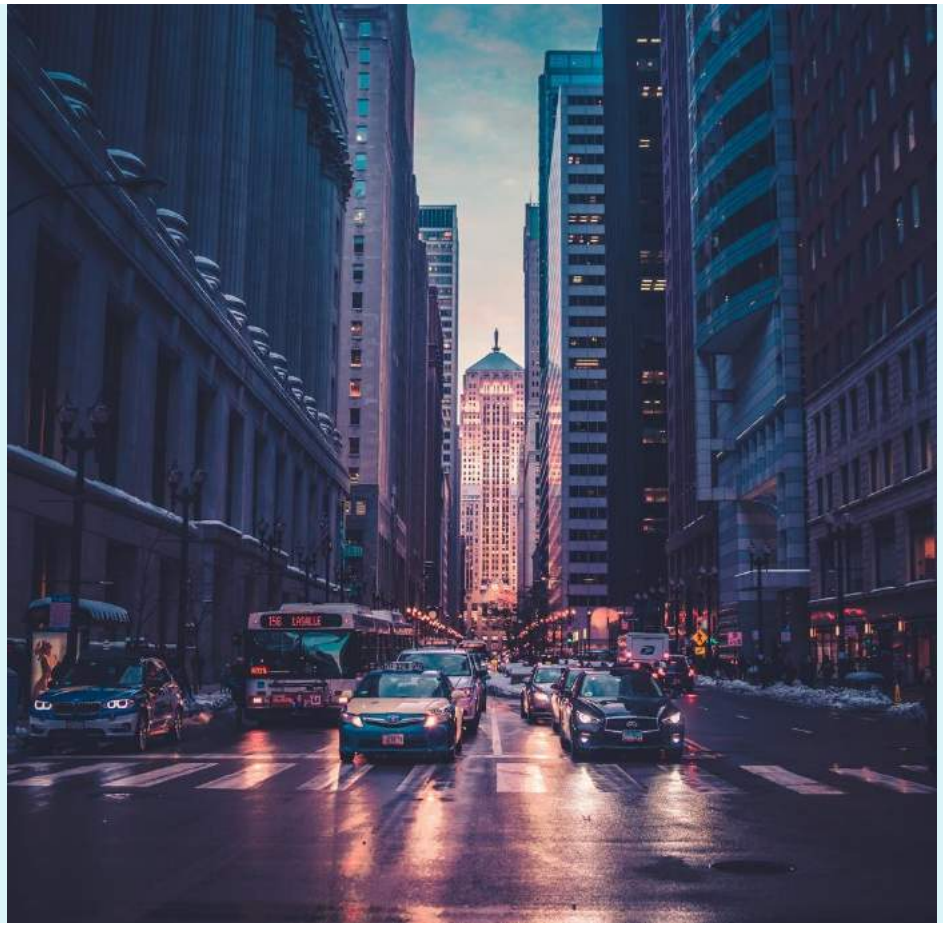
Using local Password-Attack tools

Cracking Password Hashes

Using Social-Engineer Toolkit

Using BeEF

Cracking NTLM Hashes



MODULE 10

PRIVILEGE ESCALATION & EXPLOITATION

Using WMIC

Sensitive-Information Gathering

Unquoted Service-Path Exploitation

Service Permissions Issues

Misconfigured Software Installations

Insecure File Permissions

Linux Privilege Escalation

MODULE 11

WIRELESS EXPLOITATION

- MAC Address Filtering
- Cracking WEP Encryption
- Cracking WPA/WPA2 Encryption
- Cracking WPS

MODULE 12

SNIFFING & SPOOFING

- Sniffing Network Traffic
- Spoofing Network Traffic
- Denial-of-Service Attacks

MODULE 13

FIREWALL PENETRATION TESTING

- Introduction
- Firewall **OPERATIONS**
- **FIREWALL** Logging Functionality
- Firewall **POLICY**
- Firewall **IMPLEMENTATION**
- **MAINTENANCE** & Management of Firewall
- **TYPES** of Firewall
- Steps for Firewall **PENETRATION** Testing

MODULE 14

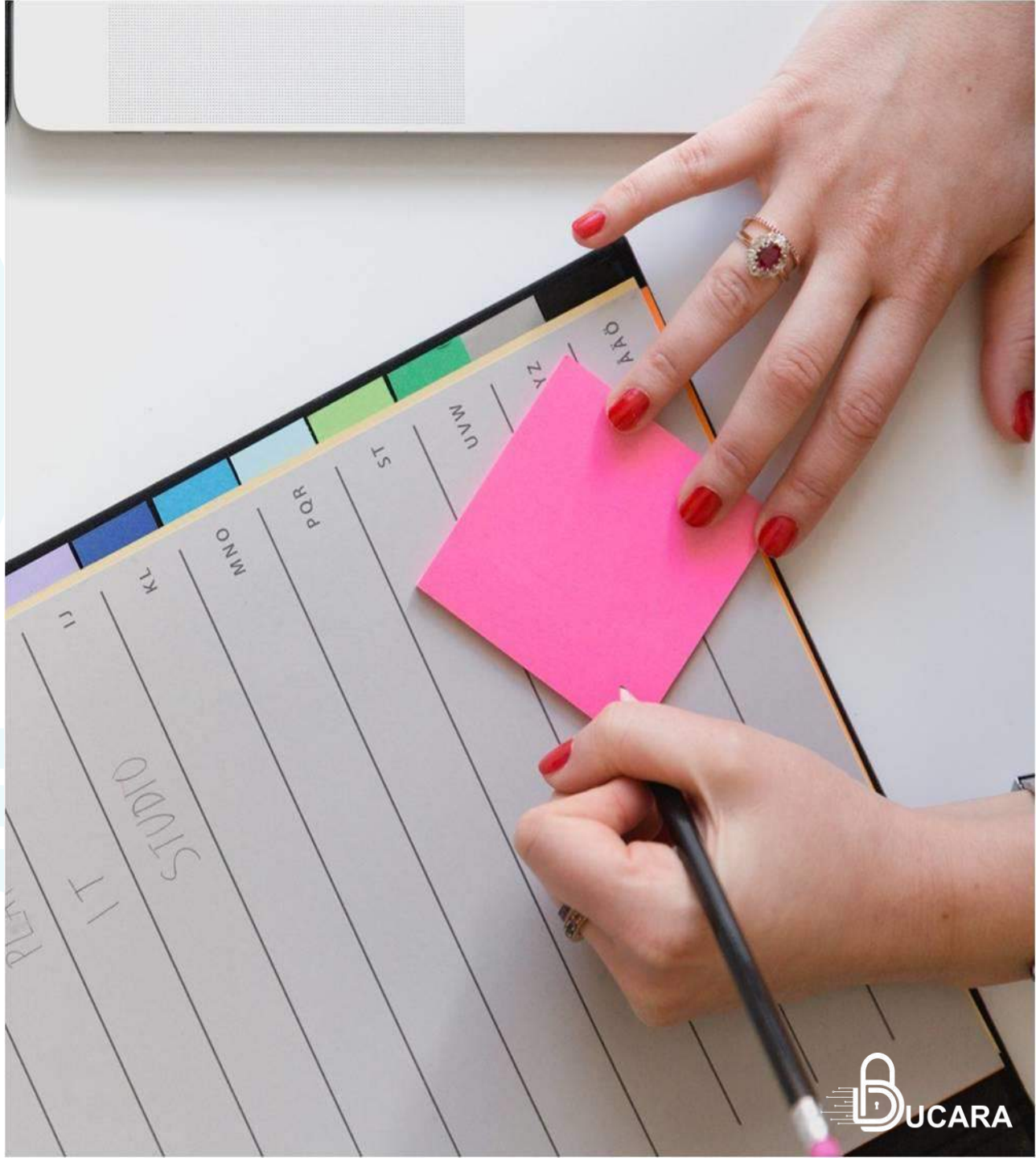
IDS PENETRATION TESTING

- Introduction
- Intrusion Detection **SYSTEM**
- **TYPES** of IDS
- **MULTI-LAYER** IDS
- Wireless **IDS**
- Common **TECHNIQUES** to Evade IDS
- Snort **ANALYSIS**
- IDS **PENETRATION** Testing Steps

MODULE 15

WRITING THE PENETRATION TESTING REPORT

1. **Gathering** all your data
2. **Importance** of defining Risk
3. **Structure** of a Penetration Test
4. **Report** Building the Report
5. **Delivering** the Report



DUCARA

THE TECHNOLOGY IS CHANGING EVERY DAY AND WE AT DUCARA ARE COMMITTED TO DEMONSTRATING VALUES. EMBRACING A DIGITAL TRANSFORMATION STRATEGY WHICH DRIVE RETURNS ON IT SECURITY INVESTMENT.

CONNECT US!

INFO@DUCARAINFO.COM

WWW.DUCARAINFO.COM