THE NORTHCAP UNIVERSITY
POWERED BY
Arizona State University

25 YEARS OF EXCELLENCE

QS STARS RATING SYSTEM
TEACHING | EMPLOYABILITY | ONLINE LEARNING
2021

# Penetration Testing & Malware Analysis

## Academic and Industrial Training Program

13th June -23rd July 2022

**Organized by Department of CSE, The NorthCap university, Gurugram**

# About The NorthCap University

The NorthCap University (NCU), founded in 1996 as Institute of Technology and Management (ITM) is known for delivering high quality of education that transforms lives and forges alliances to handle the new world order locally and globally. Over the last 25 years, the institute has transformed into a multi-disciplinary university and a destination of choice, offering industry and socially relevant undergraduate, postgraduate, and doctoral degree programs in Engineering, Applied Sciences, Management, Liberal Arts and Law. NCU has earned itself a place among the top universities in the world for its academic offerings with a perfect score of 5 stars in Teaching, Employability, Academic Development, Online Learning, and Inclusiveness and an overall rating of 4 stars by the prestigious Quacquarelli Symonds (QS) Stars Ratings, the world's largest rating agency. Further, The School of Engineering and Technology at The NorthCap University has been ranked amongst the Top 100 Engineering Institutions across the country in All India NIRF Ranking 2021. NCU has been rated as BEST PERFORMER University in the category of 'Private-Self-Financed University' in the Atal Rankings of Institutions on Innovation & Achievements (ARIIA). The NorthCap University has been accredited by National Assessment and Accreditation Council (NAAC) and the Assessment Services to International Colleges (ASIC), UK in the category of 'Premier' Universities with 'Commendable' Grades. NCU has consistently achieved top rankings in different surveys for a good placement record of students and imparts value-based education.

# About CSE Department

TComputer Science (CSE) Department of The North Cap University encourages all modern endeavours in academia, learning innovations, socially relevant research and problem solving. The department aims at being recognized universally as a promoter of computing technologies and their applications. Seven specializations namely Full Stack Development, Cybersecurity and Forensics, Cloud Computing, Data Science, Gaming, AR&VR, Artificial Intelligence and Machine Learning and Blockchain based on latest industry needs are currently running in the department. The department has signed MoUs with different industries, organizations like NTRO to strengthen its curriculum, enhance placements, internships and opportunities for engagement of students in live projects. The Department has a hi-tech learning environment with well-equipped research laboratories. It has collaboration with leading foreign universities for research and for student and faculty exchange.

# Penetration Testing & Malware Analysis Academic and Industrial Training Program

## Prerequisites

General computer skills and access to the Internet for research and data gathering.

## Who should pursue this certificate?

- Academicians/Cyber security enthusiast
- Cyber Security Professional
- Network & System Engineer
- System Administrator
- Security Analyst
- Automation testers
- Blue team members
- IT & Network Administrator

## Resource Persons (Experts from Industry and Academia)

- CISSP certified
- CEH & CCNA Certified

## Duration & Time

- Six Weeks
- 60 Hrs

## Course Fee

- Training: INR 25000/-
- Training and Certification: INR 35000/-
  (Early bird registration by 30th April will get 30% discount)

## Registration Details

Registration Form: https://forms.gle/R5x47DZiG47yevkz9

Contact Details :

**Dr. Shilpa Mahajan , Associate Professor,**
Email: shilpa@ncuindia.edu, Phone: 9871310123

**Dr. Mehak Khurana, Assistant Professor,**
Email: mehakkhurana@ncuindia.edu, Phone: 9891599137

# Program Overview

PTMA course covers the concepts from a modern pen tester perspective ranging from Network Pen testing, Web Application Pen testing, Architecture fundamentals, Buffer overflow, Malware analysis and post-Exploitation. In this course, you will learn from basic to advanced levels of the practical side of ethical hacking. It offers In-depth technical excellence along with industry-leading methodologies to conduct high-value penetration tests. This course offers extremely hands-on Sessions with labs and exercises and you will be able to earn a bounty for finding out bugs. In this course, you will have a chance to keep yourself up-to-date and equip yourself with a range of Ethical Hacking skills.

## Outcomes

- Gain insight into how critical vulnerabilities in a corporate network can be exploited.
- Understanding of how to exploit servers, networks, and applications.
- Conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment
- Utilize the scanning tools to conduct comprehensive network sweeps, port scans, Operating System fingerprinting, scanning running services and versions to develop a map of target environments
- Choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems
- Analyze the output of scanning tools to manually verify findings and perform false positive reduction using Netcat and packet crafting tools
- Utilize the Windows and Linux command lines to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise, and help determine business risks
- Configure the Metasploit exploitation tool to scan, exploit, and then pivot through a target environment in-depth
- Utilizing Metasploit for maintaining access, escaping privileges, post exploitation and clearing the logs and history.
- Gathering password hashes, cracking passwords, taking screenshots, logging keystrokes etc.
- Provide good understanding of how to approach a machine and develop own methodology
- Enhance skills that make more marketable IT tech.

# Course Outline

## Course Contents

### Module 1 : Penetration Testing Essentials

- Linux - Basic commands, wordlist generator - crunch, ceWL
- Networking Fundamentals-TCP, UDP, ARP, DHCP, FTP, SSL ,DNS, Malwares, phishing, and Attacks
- Exercise - Attendees will create their own virus

### Module 2 : Information Gathering

- Google Dorks - Netcraft - Whois Reconnaissance - DNS Reconnaissance - Forward/reverse lookup bruteforce -Email Harvesting
- Maltego,NSlookup, Snowden, FOCA, Archive
- Netbios Information Gathering
- Exercise: Attendees will gather information and build an organizational profile using discussed resources in this module

### Module 3 : Port Scanning and Sniffing

- Port Scanning Basics
- Scanning Techniques
- Nmap - Port Scanning, Network sweeping, OS fingerprinting, Service enumeration, Version scans
- Hping3
- Nmap Scripting Engine
- Wireshark Basics- Creating filters in Wireshark, Password cracking using Wireshark
- Exercise: Packet crafting with Hping3
- Exercise: Attendees will identify live hosts, OS versions, open ports and services along with their version numbers of a machine

### Module 4: Spoofing and Session Hijacking

- ARP Spoofing
- DNS Spoofing
- Connecting and listening on TCP/UDP port with Netcat
- TCP Session Hijacking
- UDP Session Hijacking
- SSL Man in the Middle
- Exercise: Attendees will perform attacks as discussed in this module

### Module 5: Vulnerability Assessment

- Vulnerable management Lifecycle
- Databases -NVD, CVE, MITRE
- Configuring and Scanning with Open Vulnerability Assessment
- System (OpenVAS)
  Assessing vulnerabilities using Nessus
  Nexpose vulnerability scanner
- Exercise: Attendees will identify vulnerabilities for a domain

### Module 6: Buffer Overflow

- Fuzzing
- Controlling EIP
- Shell coding - Shellcode encoding, Windows Command Execution
- Shellcode, Connect back Shellcode
- Exercise: Exploiting Buffer Overflows

## Module 7: Client Side Exploitation

- Password Attacks- Offline/Online
- Password Cracking Tools in Action: Hydra, Cain and Abel, John the Ripper...
- Trojan Creation using RAT
- Exercise : Attendees with exploit client machine using RAT tool

## Module 8: Metasploit

- Metasploit Framework Fundamentals
- Using Metasploit Exploits
- Types of Payloads
- Metasploit Auxiliary Modules
- Armitage
- Compiling and Executing Linux and Windows exploits
- Exercise: Attendees will attempt to exploit a target machine by fixing, compiling and executing given exploit code
- Exercise: Attendees will use Metasploit to get remote shell of target servers

## Module 9: Post Exploitation & Clearing Tracks

- Privilege Escalation
- Persistent Backdoor - Enabling Remote Desktop
- Exercise: Attendees will attempt to gain SYSTEM level privileges on remote system. - Cleaning event logs
- Exercise: Create backdoor by a script to enable remote desktop and create user account - Packet sniffing on compromised machines

## Module 10 : Web Application Hacking

- Introduction to Web Scripting
- Web Application Threats
- Cross-Site Scripting
- SQL Injections
- Blind SQL Injections
- Enumerating DBs - SQLPwnag
- Arbitrary Code Injection
- Website Defacement through shell programming
- Exercise: Attempt attacks discussed in this module on different web applications
- Exercise: Get a shell by exploiting Microsoft SQL based web application - Command Injection Flaws

## Module 11: Wireless Hacking

- WEP Cracking
- WPA Cracking
- Exercise: Attendees will crack WEP and WPA Wireless Networks

## Module 12: Bug Bounty

- Authentication Bypass
- OTP Bypass
- Captcha Bypass
- Login Bypass

## Module 13: Memory forensics and Reverse Engineering

- Malware Analysis using Memory forensics
- Crash Course in Assembly
- Reverse Engineering using IDA Pro
- Exercise- CrackMe Challenges

## Module 14: Malware Analysis

- Packed and obfuscated malware
- Basic static analysis of Windows based malware
- Basic dynamic analysis of Windows based malware
- YARA rules

## Module 15: CTF & Valedictory Session

- Attendees will be given two vulnerable machines for exploitation.
- Valedictory Session

## Why NCU?

Ranked amongst
Top100 Institutions in
Engineering Category,NIRF 2021.

Rated Overall
4 Stars - QS World University
Ratings, 2021.

Legacy of 25 years,
11000+ Strong
Alumni.

Academic collaboration with
Top Ranked International
Universities.

Well-qualified faculty
and learner-centered
collaborative pedagogy.

Analytics India Magazine
Top UG & PG Data Science
Program in India

## Why Cyber Security?

As per NASSCOM, by 2025, the
Indian cyber security industry will
touch $13.6 Billion

Cybersecurity jobs will
grow 31% through 2029, over seven
times faster than the national
average job growth of 4%.

Demand for Cybersecurity Experts
3.5 million cybersecurity
jobs in India by 2025.

Demand Across Industries
IT, Telecommunications,Financial Services,
Government, Health Care, Manufacturing,
Retail, Small business, Travel and
transportation, Energy and utilities,
Ecommerce, etc

## Program Highlights

24X7 Content Repository &
Best-In-Class Support

Eminent and Certified Experts

Face-to-face &
Project Based Learning

Hands-on exposure &
Industry Connect

Placement ready outcomes
& Career advancement

Curriculum in sync with
the latest industry needs

## Patrons

**Prof. Prem Vrat,**
Pro-Chancellor ,
The NorthCap University, India

**Prof. Nupur Prakash,**
Vice-Chancellor ,
The NorthCap University, India

## Program Chair

**Prof. Rita Chhikara ,**
**HOD CSE**
The NorthCap University, India

## Program Conveners

**Dr. Shilpa Mahajan**
Associate Pofessor,
The NorthCap University, India

**Dr. Mehak Khurana**
Assistant Professor,
The NorthCap University, India

THE NORTHCAP UNIVERSITY
POWERED BY
Arizona State University

**HUDA Sector 23-A,Gurugram, Haryana, India - 122017**
**www.ncuindia.edu**