positive education

NAAD
Convenient, but Impenetrable

August 11—25, 2024
Russia, Moscow

Hello, student!

Do you want to get acquainted with the profession of a white hacker and try your hands at cybersecurity? We invite you to join the **unique program from Positive Technologies** – the leader in information security in Russia!

The program will take place in **Moscow from August 11 to August 25** and will offer you a full immersion into the hacking world. You will learn how to conduct attacks and understand how hackers think.

You can expect hands-on training under the guidance of experienced specialists. You will understand what it is like to be a white hacker as you will work with real cases. This is a unique opportunity to test your abilities, gain valuable skills and determine if you want to further develop in this field.

What is waiting for you?

- You will learn how to imitate attacks on IT-infrastructure and investigate security systems using vulnerability exploitation tools.
- You will learn tools for analyzing network and protocol traffic and adjusting client-service communication.
- You will learn ways to elevate privileges in information systems, websites, operating systems and network infrastructures.

Upon completion, you will receive a certificate and irreplaceable experience that will come in handy in your professional career.

Conditions of participation:

Complimentary:

- Accommodation
- Cultural programme
- Meals

From you:

- Flight to Moscow and back

Feel free to submit an application if:

- Your English is at least at B1 level;
- You know how internet and local networks work;
- You know how to work with Linux or Windows at an advanced user level (installing packages/programmes and configuring basic functions);
- You know what virtualization (VMware) is and how it works.

Please note that you will definitely need to bring a laptop with you that has at least:

- 8GB of DDR3 RAM;
- Processor with at least eight cores with a frequency of at least 2.3 GHz;
- HDD/SSD hard drive with at least 256 GB of free space;
- Support for hardware virtualisation (Intel VT-x, AMD-V);
- Modern operating system (Minimum: Windows 10 x64, Linux, MacOS).

How to apply?

Send your application by **15 July**. The number of places is limited, so hurry up!

Don’t miss the chance to be part of the future of cybersecurity!

REGISTER

You can submit your CV and ask any questions: ptcybercamp@naadsecure.ir

See you there,
Positive Technologies team

positive education

NAAD
Convenient, but Impenetrable

Course program

1. **Introduction to the course:** Preparing the working environment for the practical assignments, Preparing the cloud environment for practical tasks.
2. **White hacking:** Introduction, White hacker's roadmap.
3. **Level 1.** Reconnaissance in the customer's external infrastructure: Organization domain name search, Network scanning, Network nodes scanning, Port scanning.
4. **Level 2.** Primary Access Attacks.
5. **Level 2.1.** Web-application hacking: Authentication bypass vulnerabilities, OS command injection vulnerabilities, Access control vulnerabilities, Directory access control vulnerabilities, SQL injection vulnerabilities, XML external entity injection vulnerabilities, Cross-site scripting (XSS) attacks.
6. **Level 2.2.** Known vulnerabilities in network services exploitation: Exploiting one-day vulnerabilities in network services.
7. **Level 2.3.** Social engineering: Research for email addresses of employees in an organization.
8. **Level 3.** Securing access: Obtaining legitimate access to the system, Practice "Securing access".
9. **Level 4.** Privilege escalation on server systems: Exploitation of Linux administration errors, Practice "Privilege escalation on server systems in Linux".
10. **Level 5.** Going beyond the DMZ: Network Scanning, Analyze DMZ network traffic, MitM attacks on nodes in a DMZ network.
11. **Level 6.** Network traffic forwarding: Using standard protocols for traffic forwarding, Practice "Traffic Forwarding".
12. **Level 7.** Network reconnaissance and compromise of Windows machines: Detecting Windows machines on the network, Compromising Windows machines on a network.
13. **Level 8.** Privilege escalation on local network nodes: Extracting secrets and credentials, Exploiting Windows OS configuration vulnerabilities, Exploiting known Windows OS vulnerabilities.
14. **Level 9.** Capturing network infrastructure management: Exploitation of domain controller node vulnerabilities, Collecting information about objects in the domain, Exploitation of service misconfigurations in AD.
15. **Level 10.** Detection and response counteraction: Reducing activity on the network, Use of encrypted communication channels, Using IP switching tools.
16. **Hacker development:** Ethics, Independent study materials.