Yhills Cyber Security Training

Day-1 : Introduction To Cyber Security

Table of Content:

Introduction Of mentor:

So, our talented mentor is vaishnavu C V, he introduces him self with us using Linkedin profile

First they introduce to main branch of Cyber Security VAPT using simple google definition which I like much Google can give many definition that are perfect to understand by reading once

VAPT - Vulnerability Assessment & Penetration Testing is a security testing methodology in which the IT systems such as computers, mobiles and networks, and software such as operating systems and application software are scanned in order to identify the presence of known and unknown vulnerabilities.

Simple definition: A person with ability, skill and knowledge to identify security flaw or vulnerability And he can assess that flaw, so he knows how to hack but for ethical purpose and helps to improve security posture of organization

What is Cyber Security? :

In Cyber security our job is to ensure that any software, program, physical device, the network, the system has proper cyber security protection to prevent from attacks.

What is Secure Coding:

Secure coding is the practice of developing software that is resistant to security vulnerabilities by applying security best practices, techniques, and tools early in development.

Ethical Hacking:

Practice of performing hacking techniques to hack the target but with permission of that target in order to provide more security to target.

Debate on How much amount of programming knowledge we require to become ethical hacker:

For me conclusion on this debate is, Programming knowledge always helps to boost cyber security career to advance level but at least we need survival knowledge of programming to make entry level or simple cyber security career.

Mainly it depends upon which field you want to choose according to that field's framework you can learn programming language

Furthermore, you can explorer what language to learn based on your career

Important for all Beginners:

Quote By sir: “Understand properly is Cybersecurity suitable for you”

And added just figerout by this course.

This is most important thing for me in this lecture.

Types of cyber security threats:

1. Phishing
2. Ransomware
3. Malware
4. Social Engineering
5. Men-in-the-middle attack
6. Zero-Day attack

1. Phishing:

It is practice of sending fraudulent emails that resemble emails from reputed sources.the aim is to steal sensitive data like credit card numbers and log in information.

Most used threat now a days because non-tech people still easily can be compromised by this attack

2. Ransomware:

It is type of malicious software. It is designed to extort money by blocking access to file or the computer system until ransom is paid.

3. Malware:

Malware is type of software designed to gain unauthorized access or to cause damage to a computer.

4. Social Engineering:

It is a manipulation technique that exploits human error to gain private information , access or valuables.

5. Men-in-the-middle attack

When criminals interrupt the traffic between a two-party transaction

6. Zero-day Attack

A zero-Day is a computer-software vulnerability either unknown to those who should be intrested in its mitigation or known and without a patch to correct it.

Types of hackers:

1. **White Hat Hackers**: These are ethical hackers who use their skills to find and fix security vulnerabilities. They often work for organizations to improve cybersecurity and are authorized to test systems.

2. **Black Hat Hackers**: These are malicious hackers who exploit vulnerabilities for personal gain, such as stealing data or causing damage. Their activities are illegal and unethical.

3. **Grey Hat Hackers**: These hackers fall between white and black hats. They might exploit vulnerabilities without permission but do so without malicious intent, often reporting the issues to the organization afterward.

4. **Red Hat Hackers**: Red hats are aggressive hackers who target black hat hackers. They might use illegal methods to stop or retaliate against black hats, sometimes operating in a vigilante style.

5. **Script Kiddies**: These are individuals with limited technical skills who use pre-written scripts or tools created by others to launch attacks. They lack deep understanding but can still cause significant harm.

6. **Hacktivists**: Hacktivists use hacking to promote political or social causes. Their activities are aimed at raising awareness or causing disruption to advance their agendas, often targeting organizations they oppose.

Teams in cyber Security: