List out the advantages of vulnerability assessment

10 benefits of vulnerability scanning

Vulnerability scans are to enterprises what health checkups are to people; they're proactive check-ins on a system's health to ensure it stays in tip-top running condition. For companies, a vulnerability scan ensures every entry point to your network is protected by ensuring it's updated, closed off, or regularly monitored to ensure cyber criminals don't get it.

1) Identifies vulnerabilities before cyber criminals find them.
2)Optimises the fixes you need to do
3)Assesses your security risk level.
4)Protects the integrity of your business assets.
5)Manages resources more efficiently.
6)Increases operational efficiencies.
Save money.

Insider attack is dangerous than external attack:
What Is an Insider Threat
An insider threat is a security risk that originates from within the targeted organization. It typically involves a current or former employee or business associate who has access to sensitive information or privileged accounts within the network of an organization, and who misuses this access.

Traditional security measures tend to focus on external threats and are not always capable of identifying an internal threat emanating from inside the organization.

Types of insider threats include:

Malicious insider
Careless insider
A mole—an imposter

Illustrate the term cyber forensic:
Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

It can recover deleted files, chat logs, emails, etc
It can also get deleted SMS, Phone calls.
It can get recorded audio of phone conversations.

It can determine which user used which system and for how much time.
It can identify which user ran which program.

Role of computer forensic investigator

Computer forensic investigators help retrieve information from computers and other digital storage devices. The retrieved data can then be used in criminal investigations or as evidence in cases of cyber crimes. Learn whether this career at the intersection of cybersecurity and law enforcement might be a good fit for you and how to get started.

What do computer forensic investigators do?

Much like a forensic investigator captures evidence from the scene of a crime, a computer forensic investigator gathers evidence found on computers, mobile phones, and other digital devices.

Tasks and responsibilities

The specific tasks of a digital forensic investigator will vary depending on the company or agency and industry. These are some of the tasks you might expect to perform (based on actual job listings):

Retrieve data from virtual and physical devices

Collect and analyze network intrusion artifacts and evidence of malicious network activity

Reconstruct the series of events leading to a compromise or breach

Computer forensic report:

The main goal of Computer forensics is to perform a structured investigation on a computing device to find out what happened or who was responsible for what happened, while maintaining a proper documented chain of evidence in a formal report. Syntax or template of a Computer Forensic Report is as follows

Executive Summary
Objectives
Computer Evidence Analyzed
Relevant Findings
Supporting Details
Investigative Leads
Additional Subsections

Computer forensic audit:

A forensic audit examines and evaluates a firm's or individual's financial records to derive evidence used in a court of law or legal proceeding.

Forensic auditing is a specialization within accounting, and most large accounting firms have a forensic auditing department. Forensic audits require accounting and auditing procedures and expert knowledge about the legal framework of such an audit.
Forensic audits cover a wide range of investigative activities. Forensic audit investigations can uncover or confirm various types of illegal activities. Usually, a forensic audit is chosen instead of a regular audit if there's a chance that the evidence collected would be used in court.

Role of cyber law:
Cyber laws serve a variety of purposes crucial to the usage of the internet. Some of these laws protect internet users from becoming victims of any cybercrime. Whereas, some other laws lay down rules for individuals to use the internet and the computer system. Primary areas included under cyber laws are:

Fraud
Cyber laws are there to protect consumers from online frauds. They exist to prevent online crimes including credit card theft and identity theft. A person who commits such thefts stands to face federal and state criminal charges.

Copyright
Copyright is a legal area that defends the rights of an entity be it an individual and/or a company to profit from their creative work. Individuals and companies both need copyright laws to prevent copyright infringement and enforce copyright protection.

Defamation
Defamation laws are the civil laws that give immunity to individuals from publically made false statements or allegations that can prove to be damaging for the reputation of a person or a business. When such a mala fide deed is done online, it falls under the bracket of cyber laws.

Role of e commerce:
E-commerce (electronic commerce) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as business-to-business (B2B), business-to-consumer (B2C), consumer-to-consumer or consumer-to-business.

Role of e governance:
E-governance is one of the very important topics in understanding government machinery and its important functions. Candidates preparing for the Civil services examination must have a thorough understanding of the subject. Students who are preparing for other Government Exams can refer to this article as well.

Certifying authority:
The IT Act provides for the Controller of Certifying Authorities(CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users.

The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act for purposes of the IT Act. The Office of the CCA came into existence on November 1, 2000. It aims at promoting the growth of E-Commerce and E-Governance through the wide use of digital signatures.

Cyber information security:

The terms Cyber Security and Information Security are often used interchangeably. As they both are responsible for the security and protecting the computer system from threats and information breaches and often Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously. If we talk about data security it’s all about securing the data from malicious users and threats. Now another question is what is the difference between Data and Information? So one important point is that “not every data can be information” data can be informed if it is interpreted in a context and given meaning. for example “100798” is data and if we know that it’s the date of birth of a person then it is information because it has some meaning. so information means data that has some meaning.