**SAD Lab**

**EXPERIMENT NO. 1**

**Aim**: Study of different laws and standards of cyber security.

**Theory**:

1. Define cyber security

Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorised access to data centres and other computerised systems.

A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organisation's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

**Importance of Cyber security**

With an increasing number of users, devices and programs in the modern enterprise, combined with the increased deluge of data much of which is sensitive or confidential the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

**Types of Cyber security threats**

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyberthreats, which take many forms. Types of cyberthreats include:

* Malware is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans and spyware.
* Ransomware is another type of malware. It involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.
* Social engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
* Phishing is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of these messages is to steal sensitive data, such as credit card or login information.
* Spear phishing is a type of phishing attack that has an intended target user, organisation or business.
* Insider threats are security breaches or losses caused by humans -- for example, employees, contractors or customers. Insider threats can be malicious or negligent in nature.
* Distributed denial-of-service (DDoS) attacks are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website or other network resource. By flooding the target with messages, connection requests or packets, the attackers can slow the system or crash it, preventing legitimate traffic from using it.
* Advanced persistent threats (APTs) are prolonged targeted attacks in which an attacker infiltrates a network and remains undetected for long periods of time with the aim to steal data.
* Man-in-the-middle (MitM) attacks are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they are communicating with each other.

Other common attacks include botnets, drive-by-download attacks, exploit kits, malvertising, vishing, credential stuffing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC) and zero-day exploits.

1. Tools used for cyber security

**Kali Linux**

Kali Linux is among the most popular penetration testing tools with over 300 features for website and server security. Suited for users with varying levels of knowledge in cybersecurity, Kali Linux can be used to monitor network systems with one click. The tool is particularly useful for securing databases from various cyber-attacks and online threats. Currently maintained by Offensive Security, Kali Linux was initially developed as BackTrack – a Linux-based distribution tool used for penetration testing.

Key Features:

* Available with over 600 penetration testing tools, including Aircrack-ng for monitoring Wi-Fi network security and Jack the Ripper for decoding passwords.
* Available as a free and open-source tool
* Supports both ARMEL and ARMHF systems that are compatible with ARM-derived infrastructures like BeagleBone Black and Raspberry Pi.
* KDE Plasma look-and-feel, including light and dark themes.

[**Wireshark**](https://www.wireshark.org/)

Wireshark is a free and open-source cybersecurity tool that can analyse network protocols and can be used to enhance network security. Packet-sniffing in this console-based tool can monitor your network in real-time, along with network traffic at different levels. Cybersecurity professionals use this security tool to identify any network security weaknesses by capturing and analysing data packets.

Key features:

* Decryption protocol support for multiple network protocols
* Three-pane packet browser
* Live capture and offline analysis.
* Supports output formats including XML, CSV, and Plain Text
* Supports file decompressing captured in gzips
* Supported on MS Windows, macOS, Solaris, and FreeBSD

[**Snort**](https://www.snort.org/)

Snort is another open-source tool used for detecting and stopping attempted intrusions on computer networks. This tool supports Windows, Centos, FreeBSD, and Fedora platforms. The Snort, intrusion prevention tool, is capable of performing real-time analysis of network traffic and packet logging. Suited for small to medium-sized businesses, Snort is compatible with different types of operating systems and hardware configurations.

Key Features:

* Effective at detecting network attacks including CGI attacks, fingerprinting attacks, and buffer overflow attacks
* Performs protocol analysis along with matching data captured from traffic with a database of previous attacks
* Real-time data packet analysis and logging
* Firewall protection for blocking malicious network requests
* Timely alerts of potential intrusions to security professionals

1. Standards of cyber security

**ISO**

ISO stands for International Organisation for Standardisation. International Standards make things work. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard was officially established On 23 February 1947. It is an independent, non-governmental international organisation. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

**ISO/SAE 21434**

Standard covers the aspects of automotive cybersecurity. This standard includes a list of requirements related to cyber security risk management. It also covers a cybersecurity process framework that helps OEMs to come on a common platform and communicate risks related to security.

**ISO/IEC 20243-1**

This Information technology standard refers to the Open Trusted Technology ProviderTM Standard (O-TTPS). This particular standard helps in mitigating maliciously tainted and counterfeit products.

**ISO 27000 Series**

It is the family of information security standards which is developed by the International Organisation for Standardisation and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organisation to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organisation faces. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

The ISO 27000 series can be categorised into many types. They are-

* **ISO 27001**- This standard allows us to prove the clients and stakeholders of any organisation to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.
* **ISO 27000**- This standard provides an explanation of terminologies used in ISO 27001.
* **ISO 27002**- This standard provides guidelines for organisational information security standards and information security management practices. It includes the selection, implementation, operating and management of controls taking into consideration the organisation's information security risk environment(s).
* **ISO 27005**- This standard supports the general concepts specified in 27001. It is designed to provide the guidelines for implementation of information security based on a risk management approach. To completely understand the ISO/IEC 27005, the knowledge of the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is required. This standard is applicable for all kinds of organisations such as non-government organisations, government agencies, and commercial enterprises.
* **ISO 27032**- It is the international Standard which focuses explicitly on cybersecurity. This Standard includes guidelines for protecting the information beyond the borders of an organisation such as in collaborations, partnerships or other information sharing arrangements with clients and suppliers.

1. Laws of cyber security

**1. IT Act**

The Information Technology Act also known as ITA-2000, or the IT Act main aims is to provide the legal infrastructure in India which deal with cybercrime and e-commerce. The IT Act is based on the United Nations Model Law on E-Commerce 1996 recommended by the General Assembly of the United Nations. This act is also used to check misuse of cyber networks and computers in India. It was officially passed in 2000 and amended in 2008. It has been designed to give the boost to Electronic commerce, e-transactions and related activities associated with commerce and trade. It also facilitates electronic governance by means of reliable electronic records.

IT Act 2000 has 13 chapters, 94 sections and 4 schedules. The first 14 sections concerning digital signatures and other sections deal with the certifying authorities who are licenced to issue digital signature certificates, sections 43 to 47 provides penalties and compensation, section 48 to 64 deal with appeal to high court, sections 65 to 79 deal with offences, and the remaining section 80 to 94 deal with miscellaneous of the act.

**2. Copyright Act**

The Copyright Act 1957 amended by the Copyright Amendment Act 2012 governs the subject of copyright law in India. This Act is applicable from 21 January 1958. Copyright is a legal term which describes the ownership of control of the rights to the authors of "original works of authorship" that are fixed in a tangible form of expression. An original work of authorship is a distribution of certain works of creative expression including books, video, movies, music, and computer programs. The copyright law has been enacted to balance the use and reuse of creative works against the desire of the creators of art, literature, music and monetize their work by controlling who can make and sell copies of the work.

The copyright act covers the following-

* Rights of copyright owners
* Works eligible for protection
* Duration of copyright
* Who can claim copyright

The copyright act does not covers the following-

* Ideas, procedures, methods, processes, concepts, systems, principles, or discoveries
* Works that are not fixed in a tangible form (such as a choreographic work that has not been notated or recorded or an improvisational speech that has not been written down)
* Familiar symbols or designs
* Titles, names, short phrases, and slogans
* Mere variations of typographic ornamentation, lettering, or colouring

**3. Patent Law**

Patent law is a law that deals with new inventions. Traditional patent law protects tangible scientific inventions, such as circuit boards, heating coils, car engines, or zippers. As time increases patent laws have been used to protect a broader variety of inventions such as business practices, coding algorithms, or genetically modified organisms. It is the right to exclude others from making, using, selling, importing, inducing others to infringe, and offering a product specially adapted for practice of the patent.

In general, a patent is a right that can be granted if an invention is:

* Not a natural object or process
* New
* Useful
* Not obvious.

**4. IPR**

Intellectual property rights is a right that allows creators, or owners of patents, trademarks or copyrighted works to benefit from their own plans, ideas, or other intangible assets or investment in a creation. These IPR rights are outlined in the Article 27 of the Universal Declaration of Human Rights. It provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

**Conclusion**:

Thus we studied an overview of cybersecurity and cybercrimes, the tools that are used and the important standards and laws related to cybersecurity