Glossary

A

- **Access Control List (ACL):** Access control list is a set of rules that filter incoming and outgoing traffic to mitigate network attacks and control network traffic.
- **Active Directory (AD):** Microsoft's active directory is a technology that can create and manage domains, users, and objects in a network.
- **American Standard Code for Information Interchange (ASCII):** American Standard Code for Information Interchange is a format that represents every alphabet, number, or special character in a 7-bit binary format for text files in systems and on the Internet.
- **Application Fingerprinting**: Application fingerprinting is a method of using gathered information about the targeted host system in order to determine the application server, web server, and OS running on the host machine.
- **Attack Patterns**: Attack patterns are a collection of methods used to find bugs/errors in the computer security code.
- **Attack Vector**: An attack vector is a pathway or method used by an attacker to gain access to the targeted system.
- **Authentication**: Authentication is a process of verifying the identity of a user/process.
- **Authorization**: Authorization is a security mechanism that determines the access levels or user/client privileges to system resources such as files, services, computer programs, and data.

B

- **Basic Input Output System (BIOS)**: Basic input output system is a hardware initializing mechanism that is activated during the OS boot.

C

- **Cellular Digital Packet Data (CDPD)**: Cellular digital packet data is a wide-area mobile data service that offers up to 19.2 Kbps Internet speed for user devices.
- **Certificate Authority (CA)**: Certificate authority is a trusted entity that issues digital certificates and public keys used for secure communication over public networks.
- **Content Filtering**: Content filtering prevents access to certain parts of content to prevent unauthorized access by implementing it through software or a hardware-based solution.
- **Cryptographic Algorithm/Cipher:** Cryptographic algorithm/cipher is a collection of well-defined, but complex, mathematical instructions used to encrypt and decrypt data.

- **Cyber Law**: Cyber law or Internet law or IT Law encompasses laws relating to cybercrimes, the Internet's relationship with technological and electronic elements of an organization, intellectual property, and data security and privacy.
- **Cyber Threat**: A cyber threat is a malicious act such as on that intends to damage data, steal data, and disrupt digital life.

D

- **Data Center**: Data center is a facility comprising a large group of networked computer servers used by an organization for remote storage, processing, or distribution of data.
- **Data Exfiltration**: Data exfiltration is a form of a security breach wherein an individual's or company's data are copied, transferred, or retrieved from a computer/server without authorization.
- **Data Loss Prevention (DLP)**: Data loss prevention is a practice of detecting and preventing data breaches, data exfiltration, or data destruction unwantedly.
- **Data Packet**: A data packet is a unit of data transmitted through the Internet.
- **Data Processing**: Data processing is the collection and manipulation of items of data to obtain sensible information.
- **Data Protection Officer (DPO)**: A data protection officer is an organization's security leadership role responsible for overseeing the strategy for data security and its implementation to ensure compliance with General Data Protection Regulation requirements.
- **Database**: A database is an organized collection of data that can be easily accessed, managed, and updated electronically through a computer.
- **Decryption**: Decryption is a process of decoding the data that have been encrypted into a secret format such that only authorized users can have access to the data.
- **Defense-in-Depth (DiD)**: Defense-in-depth is a cybersecurity approach to safeguard sensitive information through a series of layered defensive mechanisms such that, even if one mechanism fails, the other mechanisms prevent the attack.
- **Domain Name System (DNS)**: Domain name system is the Internet's system that converts alphabetical names into an IP address. For example, if a user types a URL name, then the DNS server returns the IP address associated with the URL name.
- **Domain Controller (DC)**: Domain controller is a server on the Windows network that allows host access to domain resources by storing account information, authenticating users, and enforcing security policies for Windows domains.
- **Domain Name System Query (DNS Query)**: Domain name system query or request is a request for information sent from a DNS client system to a DNS server.
- **Dynamic**: Dynamic is a process or system that is characterized by constant change, progress, or activity.
- **Dynamic Host Configuration Protocol (DHCP)**: Dynamic host configuration protocol is a network management protocol that assigns dynamic IP addresses for devices in a network.

- **Dynamic Static Tables**: Dynamic static tables are the tables that store cumulative data through which checkpoint firewall checks upcoming transmissions.
- **Dynamic-Link Libraries (DLLs)**: Dynamic-link libraries are a type of library of executable functions or data that provide one/more functions; applications access such functions by creating either a static/dynamic link to the DLL.

E

- **Electronic Storage Media**: Electronic storage media is any type of electronic device used to store data such as internal and external hard drives, USB drives, and CDs.
- **Encryption**: Encryption is a process of converting data into code to prevent unauthorized access.
- **End-point**: An end-point is a remote computing device that communicates within a network such devices include laptops, desktops, smartphones, and servers.
- **End-User**: An end-user is a person for whom the software or hardware device is designed.
- **Evolution-Data Optimized (EVDO)**: Evolution-data optimized is a 3G network standard that provides wireless data communication to connect to the Internet.

F

- **False Positive**: A false positive is a test result that wrongly indicates that the condition or attribute is present.
- **Framework**: Framework is a supporting structure to build software applications or programs.
- **File Transfer Protocol (FTP)**: File transfer protocol is a standard network protocol used to transfer files between the client and the server in a computer network.

G

- **Group Policies**: Group policies constitute a Windows Active Directory feature that provides controls to users and user accounts.
- **Group Policy (GP)**: Windows’ Group Policy is a tool that allows the control of a user’s status and activities on a specified system in a network.

H

- **Hacktivism**: Hacktivism is an act of misusing the computer or network for social or political benefits.

I

- **Incident**: An incident is any event that disrupts the standard business functions of an organization, and if not managed instantly, could lead to disaster.
- **Infrastructure**: Infrastructure is a basic physical system of a business/region such as electric systems and communication networks.

- **Integrated Services Digital Network (ISDN)**: Integrated services digital network is a set of communication standards that allow digital transmission of data, voice, and signaling.
- **Internet Control Message Protocol (ICMP)**: Internet control message protocol is an Internet protocol used by network devices such as routers to validate whether the data are reaching its target device promptly and, if not, it reports an error.
- **Internet Service Provider (ISP)**: Internet service provider is an organization that allows users to access and use the Internet through specific services.

L

- **Layer 2 Switch**: Layer 2 switch or data link layer switching is a network switch that uses a MAC address to decide the path on which frames should be sent.
- **Layer 7**: Layer 7 is the seventh and top layer of the Open Systems Interconnect Model, which supports end-user processes and applications (application layer).
- **Load Balancer**: Load balancer is a virtual hardware that acts as a reverse proxy in order to distribute traffic across multiple servers.
- **Local Security Authority (LSA)**: Microsoft Windows' Local Security Authority is a part of Client Authentication Architecture; it allows a service to authenticate and create a logon session for local systems.

M

- **Media Access Control Address (MAC address)**: A MAC address or physical address of a network device is a unique 48-bits hardware identification number embedded into network cards such as an Ethernet card or Wi-Fi card during its manufacturing in order to uniquely identify each network device.
- **Microsoft Management Console (MMC)**: Microsoft Windows' Microsoft Management Console is a framework that allows management, administration, and configuration of systems through a user interface.
- **Minimal Installation (Minimal)**: Minimal Installation is an OS installation that offers users a choice between the full-fat Ubuntu installation or a semi-skim version during the set-up of Bionic Beaver.
- **Mitigation**: Mitigation is an act of minimizing the severity or seriousness of an event.
- **Multimedia Content**: Multimedia content is an aggregation of multimedia objects such as text, images, audio, and video.

N

- **Network Interface Card (NIC)**: Network interface card is a hardware component of a computer that helps connect the system to a network.
- **Network Protocols**: Network protocols are formal standards and policies that define communication among devices over a network and prevent mobile devices from network-based threats.

- **Network Segmentation**: Network segmentation is the practice of splitting the computer network into multiple segments or subnetworks, wherein each segment acts as a small network.
- **Network Time Protocol (NTP)**: Network time protocol is an open-source protocol that is used for time synchronization in a network.
- **Network Traffic**: Network traffic is the movement of data in a computer network at a given point in time.
- **Next-Generation Firewall (NGFW)**: Next-generation firewall is a deep-packet inspection firewall that provides application-level inspection, intrusion prevention, and cloud-delivered threat intelligence.

O

- **Open Mobile Alliance (OMA)**: Open Mobile Alliance is a standards body that provides worldwide mobile service interoperability.
- **Open-Source OS**: Open-source OS is a software in which the source code of the software is available for public use in order for users to make changes to the OS as per their requirement and at no cost.

P

- **Package**: Package is a compressed file archive that comprises all files that come with an application in Linux.
- **Packet Forwarding**: Packet forwarding is the transmission of packets from one network segment to another by nodes in a computer network.
- **Patching**: Patching is a process of repairing a vulnerability or a flaw that is identified after the release of software in the market.
- **Phishing**: Phishing is a fraudulent attempt to obtain a user's sensitive information such as username, passwords, or credit card details by posing as a trustworthy entity in an electronic communication.
- **Policy**: Policy is a high-level document that states regulatory and best practice requirements to ensure proper administrative security of the organization's confidential data.
- **Post Office Protocol (POP3)**: Post office protocol is a protocol that is used to retrieve e-mail from a mail server.
- **Proxy Server**: A proxy server is a server application/appliance that acts as a mediator for requests from the client seeking resources from the servers that provide those resources.
- **Public Cloud**: Public cloud is a type of computing wherein the provider makes resources available to the public through the Internet.
- **Public-Key Cryptography (PKC)**: Public key-cryptography is an encryption system that uses a paired public (known to everyone) and private key (known to the recipient of the message) algorithm for secure data communication and helps a user.

R

- **Regulatory Framework**: A regulatory framework comprises laws, regulations, and policies approved by governments for implementing strong administrative network and data security.
- **Remote Desktop Protocol (RDP)**: Microsoft's remote desktop protocol is a protocol that offers application data transfer protection and encryption between client devices and a virtual network server.
- **Risk**: Risk is a potential for exposure to loss/damage.
- **Root User/Root Account/Super User**: The root user/root account/super user is a username or account that has access to all files and commands on a Linux OS.
- **Router**: Router is a computer networking device that connects all switches to form a larger network, which might be at single or multiple locations.

S

- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Protocols**: Secure sockets layer/transport layer security protocol encrypts internet traffic and ensures secure Internet communication by authenticating communication between servers, systems, applications, and users.
- **Security Breach**: A security breach refers to unauthorized access to an organization's protected systems and data.
- **Security Controls**: security controls are countermeasures to detect, minimize, and counteract security risks.
- **Security Identifier (SID)**: A security identifier is a unique ID number used to identify an object (user/users' group) in a network by a system/domain controller.
- **Service Provider**: A service provider is an organization/vendor that allows access to its subscribers to the Internet.
- **Service Set Identifier (SSID)**: A service set identifier is a unique ID that comprises 32 characters and used for naming wireless networks to ensure data are sent to the correct destination.
- **Signature-based Detection**: Signature-based detection is a process wherein a unique identifier of a known threat is established in order to recognize the threat in the future.
- **Simple Network Management Protocol (SNMP)**: Simple network management protocol is an Internet standard application-layer protocol that allows the management and monitoring of network devices and their functions on IP networks.
- **Simulation**: Simulation is an imitation of a process or event.
- **Single Sign-On (SSO)**: Single sign-on is an authentication mechanism that allows accessing multiple applications with one set of login credentials.
- **Social Engineering**: Social engineering, in the context of cybersecurity, is psychological manipulation of a user of a computing system such that the user reveals sensitive information that can be used to gain unauthorized access to the system.

- **Switch**: Switch is a computer networking device that facilitates the sharing of resources by connecting all devices, including computers, printers, and servers, in a small network.
- **System log daemon (syslogd)**: System log daemon is a common logger that can manage messages from servers and programs in Linux and Unix.

T

- **Tamper-Proofing**: Tamper-proofing is a methodology that hinders, deters, or detects unauthorized access to a device.
- **Telnet**: Telnet is a network protocol that allows a user on one computer to log in to another computer within the same network.
- **Threat Landscape**: A threat landscape is a collection of threats in a specific domain with information on threats, risks, vulnerable assets, threat actors, and observed trends.
- **Thwart**: Thwart is to prevent an entity from action.
- **Timestamp**: Timestamp is a part of a log event that informs when an event occurs.
- **Trusted Platform Module (TPM)**: Trust platform module is a computer chip (microcontroller) that securely stores passwords, certificates, encryption keys, among other sensitive information, which are later used to authenticate the system.
- **Trojan**: A trojan is a malware disguised as genuine software.
- **Tunneling**: Tunneling is a protocol that provides secure communication among networks by providing encryption, data integrity, and authentication.

U

- **Universal Plug and Play (UPnP)**: Universal plug and play is a collection of networking protocols that allows networking devices (e.g., computers, printers, and mobile devices) to discover each other's presence and establish functional network services for data sharing, communications, and entertainment.
- **User Datagram Protocol (UDP)**: User datagram protocol is a part of the TCP/IP suite of protocols or a stateless protocol that establishes low-latency and loss-tolerating communication among applications on the Internet.

V

- **Virtual Private Network (VPN)**: Virtual private network is a private network that uses a public network to connect users/sites remotely.
- **Vulnerability**: Vulnerability is a weakness in a system that could be exploited by an attacker in order to gain unauthorized access.

W

- **Wide Area Network (WAN)**: Wide area network is a computer network that spans over a large geographical area.

- **Windows PowerShell**: PowerShell is a command-line shell automation platform for Windows and Windows Server systems, with a scripting language integrated into the .NET framework.
- **Wireless Application Protocol (WAP)**: Wireless application protocol is a protocol that allows wireless data access through mobile wireless networks.
- **World Wide Web Consortium (W3C)**: The World Wide Web Consortium is an access log for web servers that can be enabled on a server session or URL group.

Z

- **Zero-day Threat**: Zero-day threat is a threat that has not been identified before and that does not match with any known malware signatures.
- **Zero-day Virus**: Zero-day virus is an unknown virus/malware without any identified antivirus software signatures.