Computer Network And Security

Exploits target vulnerabilities, which are essentially flaws or weaknesses in a system's defenses. Common targets for exploits include operating systems, web browsers, and various applications, where... 855b8878bc Within a computer network, hosts are identified by network addresses, which allow networking hardware to locate and identify hosts. Hosts may also have hostnames, memorable labels for the host nodes, which can be mapped to a network address using a hosts file or a name server such as Domain Name Service. The physical medium that supports information exchange includes wired media like copper cables, optical fibers, and wireless radio-frequency media. The arrangement of hosts and hardware within a network architecture is known as the network topology. 855b8878bc

Exploit (computer security) Exploits can An exploit is a method or piece of code that takes advantage of vulnerabilities in software, applications, networks, operating systems, or hardware, typically for malicious purposes. While an exploit by itself may not be a malware, it serves as a vehicle for delivering malicious software by breaching security controls. The term "exploit" derives from the English verb "to exploit," meaning "to use something to one’s own advantage. " Exploits are designed to identify flaws, bypass security measures, gain unauthorized access to systems, take control of systems, install malware, or steal sensitive data. systems, web browsers, and various applications, where hidden vulnerabilities can compromise the integrity and security of computer systems 855b8878bc

== History == 855b8878bc

Computer security It focuses on protecting computer software, systems, and networks from threats that can lead to unauthorized Computer security (also cybersecurity, digital security, or information technology (IT) security) is a subdiscipline within the field of information security. subdiscipline within the field of information security. It focuses on protecting computer software, systems, and networks from threats that can lead to unauthorized information disclosure, theft, or damage to hardware, software, or data, as well as to the disruption or misdirection of the services they provide 855b8878bc

On July 14, 2003, the Organization Department of the Chinese Communist Party officially approved the establishment of the National Computer Network Emergency Response Technical Coordination... 855b8878bc

Threat (computer security) In computer security, a threat is a potential negative action or event enabled by a vulnerability that results in an unwanted impact to a computer system In computer security, a threat is a potential negative action or event enabled by a vulnerability that results in an unwanted impact to a computer system or application 855b8878bc

Security hacker A security hacker or security researcher is someone who explores methods for breaching or bypassing defenses and exploiting weaknesses in a computer system A security hacker or security researcher is someone who explores methods for breaching or bypassing defenses and exploiting weaknesses in a computer system or network. Hackers may be motivated by a multitude of reasons, such as profit, protest, sabotage, information gathering, challenge, recreation, or evaluation of a system weaknesses to assist in formulating defenses against potential hackers 855b8878bc

The first computer network was created in 1940 when George Stibitz connected a terminal at Dartmouth to his Complex Number Calculator at Bell Labs in New York. Today, almost all computers are connected to a computer network, such as the global Internet or embedded networks such as those found in many modern electronic devices. Many applications have only limited functionality unless they are... 855b8878bc

Network security The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. It does as its title explains: it secures the network, as well as protecting and overseeing operations being done. Networks can be private, such as within a company, and others which might be open to public access. denial of a computer network and network-accessible resources. Network security is involved in organizations, enterprises, and other types of institutions. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs: conducting transactions and communications among businesses, government agencies and individuals. Network security involves the authorization of access to data in a network, which is controlled Network security is an umbrella term to describe security controls, policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security involves the authorization of access to data in a network, which is controlled by the network administrator 855b8878bc

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement for WPA2. Certification... 855b8878bc

Network security policy The document itself is usually several pages long and written by a committee. A network security policy (NSP) is a generic document that outlines rules for computer network access, determines how policies are enforced and lays out A network security policy (NSP) is a generic document that outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the company security/ network security environment 855b8878bc

Despite a system administrator's best efforts to achieve complete correctness, virtually all hardware and software contain bugs where the system does not behave as expected. If the bug could enable an attacker to compromise the confidentiality, integrity, or availability of system resources, it can be considered a vulnerability. Insecure software development practices as well as design factors such as complexity can increase the burden of vulnerabilities. 855b8878bc Security policy should keep the malicious users out, and also exert control over potential risky users within an organization. 855b8878bc Vulnerability management includes identifying systems and prioritizing which are most important, scanning for vulnerabilities, and taking action to secure the system. Vulnerability management typically is a combination of remediation, mitigation, and acceptance. 855b8878bc The growing significance of computer security reflects the increasing dependence on computer systems, the Internet, and evolving wireless network standards. This reliance has expanded with the proliferation of smart devices, including smartphones, televisions, and other components of the Internet of things (IoT).

855b8878bc

Vulnerability (computer security) In computer security, a vulnerability is a flaw or weakness in a system's design, implementation, or management that can be exploited by a malicious actor In computer security, a vulnerability is a flaw or weakness in a system's design, implementation, or management that can be exploited by a malicious actor to compromise its security 855b8878bc

National Computer Network Emergency Response Technical Team/Coordination Center of China In 2000, the Computer Network and Information Security Management The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) is the core coordination organization of the cybersecurity emergency response system of the People's Republic of China. National Computer Network and Information Security Management Center was established 855b8878bc

Estimates of the economic cost of cyberattacks that rely on exploits vary widely depending on methodology and scope; a 2020 McAfee/CSIS report estimated the global cost of cybercrime at more than US$1 trillion annually. In response to this threat, organizations are increasingly utilizing cyber threat intelligence to identify vulnerabilities and prevent hacks before they occur. 855b8878bc == Overview == 855b8878bc As digital infrastructure becomes more embedded in everyday life, cybersecurity has emerged as a critical concern. The complexity of modern information systems—and the societal functions they underpin—has introduced new vulnerabilities. Systems that manage essential services, such as power grids, electoral processes, and finance, are particularly sensitive to security breaches. 855b8878bc A security policy is a complex document, meant to govern data access, web-browsing habits, use of passwords, encryption, email attachments and more. It specifies these rules for individuals or groups of individuals throughout the company. The policies could be expressed as a set of instructions that understood by special purpose network hardware dedicated for securing the network. 855b8878bc == History == 855b8878bc Although many aspects of computer security involve digital security, such as electronic passwords... 855b8878bc In September 1999, the National Computer Network and Information Security Management Center was established. In 2000, the Computer Network and Information Security Management Office of the National Informatization Leading Group held a working meeting on the establishment of a national public Internet security incident emergency response system and proposed that the center be responsible for the core tasks. In October 2000, the Ministry of Information Industry established the Computer Network Emergency Response Coordination Center. In August 2001, the National Computer Network and Information Security Management Center formally established the China Computer Network Emergency Response Coordination Center. In September 2002, the coordination center was formally established. 855b8878bc Vulnerabilities can be scored for severity according to the Common Vulnerability Scoring System (CVSS) and added to vulnerability databases such as the Common Vulnerabilities and Exposures (CVE) database. As of April 2026, more than 327,000 vulnerabilities had been recorded in the CVE database... 855b8878bc

Computer network In computer science, computer engineering, and telecommunications, a network is a group of communicating computers and peripherals known as hosts, which In computer science, computer engineering, and telecommunications, a network is a group of communicating computers and peripherals known as hosts, which communicate data to other hosts via communication protocols, as facilitated by networking hardware 855b8878bc

== Phenomenology == 855b8878bc == Description == 855b8878bc

Wireless security Enterprises often enforce security using a certificate-based system to authenticate the connecting device, following the standard 802. Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The term may also refer to protecting the wireless network itself from adversaries seeking to damage the confidentiality, integrity, or availability of the network. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. WEP is an old IEEE 802. WEP was superseded in 2003 by WPA, a quick alternative at the time to improve security over WEP. 11X. It is a notoriously weak security standard: the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. The most common type is Wi-Fi security, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). The term Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The current standard is WPA2; some hardware cannot support WPA2 without a firmware upgrade or replacement. 11 standard from 1997 855b8878bc

== Network security... == 855b8878bc A threat can be either a negative "intentional" event like hacking or an "accidental" negative event or otherwise a circumstance, capability, action, or event (incident is often used as a blanket term). A threat actor who is an individual or group that can perform the threat action, such as exploiting a vulnerability to actualise a negative impact. An exploit is a vulnerability that a threat actor used to cause an incident. 855b8878bc