Network security

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.[1] Network security involves the authorization of access to data in a network, which is controlled by the network administrator. 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 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. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: it secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Contents

Network security concept

Security management

Types of attack

See also

References

Further reading

Network security concept

Network security starts with authentication, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users.[2] Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS)[3] help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account.[4]

Communication between two hosts using a network may be encrypted to maintain security and privacy.

Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Honeypots are placed at a point in the network where they appear vulnerable and undefended, but they are actually

isolated and monitored.[5] Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.[6]

Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. In order to minimize susceptibility to malicious attacks from external threats to the network, corporations often employ tools which carry out network security verifications (https://ipfabric.io/product/network-security/).

Types of attack

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movements to find and gain access to assets available via the network.[7]

Types of attacks include:[8]

- Passive
  - Network
    - Wiretapping
    - Passive Port scanner
    - Idle scan
    - Encryption
    - Traffic analysis
- Active:
  - Virus
  - Eavesdropping
  - Data modification
  - Denial-of-service attack
  - Active Port scanner
  - DNS spoofing
  - Man in the middle
  - ARP poisoning
  - VLAN hopping
  - Smurf attack
  - Buffer overflow
  - Heap overflow

- Format string attack
- SQL injection
- Phishing
- Cross-site scripting
- CSRF
- Cyber-attack

See also

- Cloud computing security
- Computer security
- Crimeware
- Cyber security standards
- Data loss prevention software
- Greynet
- Identity-based security
- Metasploit Project
- Mobile security
- Netsentron
- Network enclave
- Network Security Toolkit
- TCP Gender Changer
- TCP sequence prediction attack
- Timeline of computer security hacker history
- Wireless security
- Dynamic secrets
- Low Orbit Ion Cannon
- High Orbit Ion Cannon

References

1. "What is Network Security? Poda myre" (https://www.forcepoint.com/cyber-edu/network-security). *Forcepoint*. 2018-08-09. Retrieved 2020-12-05.
2. A Role-Based Trusted Network Provides Pervasive Security and Compliance (http://newsroom.cisco.com/dlls/2008/ts_010208b.html?sid=BAC-NewsWire) - interview with Jayshree Ullal, senior VP of Cisco
3. Dave Dittrich, *Network monitoring/Intrusion Detection Systems (IDS)* (http://staff.washington.edu/dittrich/network.html) Archived (https://web.archive.org/web/20060827234520/http://staff.washington.edu/dittrich/network.html) 2006-08-27 at the Wayback Machine, University of Washington.
4. "Dark Reading: Automating Breach Detection For The Way Security Professionals Think" (http://www.darkreading.com/operations/automating-breach-detection-for-the-way-security-professionals-think/a/d-id/1322443). October 1, 2015.
5. "What is a honeypot? How it protects against cyber attacks" (https://searchsecurity.techtarget.com/definition/honey-pot). *SearchSecurity*. Retrieved 2021-03-04.
6. "*Honeypots, Honeynets*" (http://www.honeypots.net). Honeypots.net. 2007-05-26. Retrieved 2011-12-09.

7. Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
8. "BIG-IP logout page" (https://web.archive.org/web/20120227163121/http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) (PDF). Cnss.gov. 1970-01-01. Archived from the original (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) (PDF) on 2012-02-27. Retrieved 2018-09-24.

Further reading

- *Case Study: Network Clarity* (http://www.scmagazine.com/case-study-network-clarity/article/324988), SC Magazine 2014
- Cisco. (2011). What is network security?. Retrieved from cisco.com (http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html)
- Security of the Internet (http://www.cert.org/encyc_article/tocencyc.html) (*The Froehlich/Kent Encyclopedia of Telecommunications vol. 15*. Marcel Dekker, New York, 1997, pp. 231–255.)
- *Introduction to Network Security (http://www.interhack.net/pubs/network-security)*, Matt Curtin, 1997.
- *Security Monitoring with Cisco Security MARS*, Gary Halleen/Greg Kellogg, Cisco Press, Jul. 6, 2007. ISBN 1587052709
- *Self-Defending Networks: The Next Generation of Network Security*, Duane DeCapite, Cisco Press, Sep. 8, 2006. ISBN 1587052539
- *Security Threat Mitigation and Response: Understanding CS-MARS*, Dale Tesch/Greg Abelar, Cisco Press, Sep. 26, 2006. ISBN 1587052601
- *Securing Your Business with Cisco ASA and PIX Firewalls*, Greg Abelar, Cisco Press, May 27, 2005. ISBN 1587052148
- *Deploying Zone-Based Firewalls*, Ivan Pepelnjak, Cisco Press, Oct. 5, 2006. ISBN 1587053101
- *Network Security: PRIVATE Communication in a PUBLIC World*, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN 9780137155880
- *Network Infrastructure Security*, Angus Wong and Alan Yeung, Springer, 2009. ISBN 978-1-4419-0165-1