Keysight's Guide To Network Security Terms And Acronyms

Network Security Terms & Acronyms

Network security is an intimidating and often misunderstood concept. Part of this is due to the constant change in security threats and threat responses. Nothing stays the same for too long, which creates consistent churn and confusion. This guide is intended to give you a quick and easy reference to common security terms and their meanings. Additional material is available at www.Keysight.com.com/solutions/network-security to help you further with your network security and visibility solution investigations.

Access Control:
U.S. government- approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Advanced Persistent Threats (APT):
This is a type of security threat that repeatedly tries to attack a target over a period of time. It usually has the ability to adapt to countermeasures that are deployed to stop it.

Anomaly Detection:
In security monitoring or data mining, the process of identifying items, events, or behaviors which do not conform to expected patterns and are then referred to as outliers.

Application and Threat Intelligence (ATI)
Real-time threat intelligence feeds with up-to-the moment content changes for security and application related data.

Block chain:
A shared listing that allows for recording the history of transactions to improve security.

Botnet:
A network of private computers or smart devices infected with malicious software and controlled as a group without the owners' knowledge

Bypass Switch:
Specialized network data tap that has fail-over capability integrated within it. Typically used for inline security tools to make them more reliable.

Chief Security Officer/Chief Information Security Officer (CSO/CISO)
CPerson responsible for the security direction of a given organization.

Cipher (or cypher):
An algorithm for performing the encryption or decryption of data.

Common Vulnerabilities and Exposures (CVE):
Research with a dictionary of known information about system vulnerabilities that is available to the public

Computer Incident Response Team (CIRT):
A team that is created to specifically respond to suspicious security-related incidences. This often includes threat identification and remediation or mitigation, if complete remediation (eradication) is not possible.

Crypto-mining:
The process of safeguarding important corporate information and data from loss.

Data Protection:
Monitoring that examines the payload or data portion of a packet, as opposed to just the packet headers.

Demilitarized Zone (DMZ):
A "neutral zone" that is deployed between an organization's private network and the Internet to provide a safety buffer.

Denial of Service (DOS):
A security attack that is intended to prevent or delay authorized users from accessing network resources.

Distributed Denial of Service (DDoS):
A denial of service technique that uses multiple hosts to perform the attack, not just one

Ephemeral Key:
A type of cryptographic key that is generated for each execution of a key establishment process. A cryptographic key is ephemeral if it is generated anew for each execution of the key. Ephemeral keys are becoming the gold standard for encryption, replacing static keys which were easier for hackers to break into over repeated attempts.

False Positive:
An alert that incorrectly indicates that malicious activity has or is happening.

Firewall:
Hardware or software functionality that is designed to control access between different networks and systems.

Forensics (Cyber Forensics):
The application of investigation and analysis techniques to find out exactly what happened on a computing device and who was responsible. Used in more complex, multi-stage cyberattacks.

Honeypot:
A purpose-built capability that is designed to be attractive to potential hackers (but does not compromise legitimate network data) so that the security team can study the hackers movements and objectives.

Identity Management:
A strategy designed to ensure the authentication of users and entities on the network. This is a first level of security defense.

Inline:
Deployment of a device directly in the path of network data to perform some action on the data, such as data inspection, SSL decryption/ re-encryption, quarantining of suspicious data, etc

Inline Network Packet Broker:
A network packet broker (which performs, load balancing, aggregation, and regeneration) that is deployed directly in the path of network data to manipulate the data.

Internet Key Exchange (IKE):
Protocol used within the Internet Security Protocol (IPSec) protocol suite to exchange decryption/ encryption keys between the host and endpoint.

Intrusion Detection System (IDS):
A hardware or software solution placed out-of-band that is designed to analyze information across the network to investigate possible security breaches. This includes internal and external threats.

Intrusion Detection and Prevention System (IDPS):
A combined intrusion detection and prevention solution that looks for signs of possible incidents and attempts to stop them.

Intrusion Prevention System (IPS):
Solution placed inline that can detect suspicious activity, investigate it, and attempt to stop the activity before it reaches the target address.

IP Security (IPSec):
Suite of protocols for securing Internet Protocol (IP) communications at the network layer (Layer 3 of the Open Systems Interconnection (OSI) model). IPSec also includes protocols for cryptographic key establishment.

Load Modules:
Hardware or software-based solutions for simulating complex traffic, including SSL-encrypted traffic and high-volume bursts of activity to observe how congestion affects latency, throughput, and concurrent processing.

Logic Bomb:
Security threat that is intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Man-in-the-Middle Attack (MITM):
Security threat that is run on the authentication protocol in which the attacker positions himself in between the claimant and verifier so that he can intercept and alter data traveling between them.

Malware/Malicious Code:
Software or firmware that is designed with the intent of having some adverse impact on the confidentiality, integrity, or availability of an information system (IS). Computer viruses, worms, Trojan horses, trapdoors, and logic bombs all fall under the definition of malicious code.

Multi-Stage Attacks:
An evolved form of an intrusion attack where a hacker penetrates a network to conduct one type of breach and is then able to move inside the organization to perpetrate other types of attacks. The initial breach may even be used to distract security analysts while the hacker moves on his/her primary target.

Personally Identifiable Information (PII):

Information that can be used to identify an individual's identity. This includes an individual's phone number, social security number, biometric records, email, place of birth, etc.

Phishing:
Tricking of individuals so that they disclose personal information through computer-based means.

Ransomware:
A security attack that encrypts the victim's hard drive and prevents the authorized user from accessing the hard drive without a special decryption key. This key is ransomed to the victim for a specified amount of money.

Sandboxing:
Often considered the same as a Honey Pot. This is a method of isolating network and application functions into distinct domains by software.

Secure Real-Time Transport Protocol (SRTP):
Variant of the IETF RTP protocol that is intended to provide encryption, message authentication and integrity, and replay protection for RTP data..

SecureStack:
Security-oriented features for Keysight Vision series network packet brokers (NPBs) that provide optimized handling for secure traffic. Capabilities include secure sockets layer (SSL) decryption.

Security Resilience:
The ability of your architecture to completely recover and return to a normal state of operation after an attack and/or breach.

Security Testing:
Use of traffic simulation across multiple protocols and applications. Testing lets the organization observe the behavior of security solutions, processes, and personnel, to identify gaps and measure how long it takes to isolate and recover from a security attack or breach

Threat Intelligence:
See definition for Application and Threat Intelligence

Threat Intelligence Gateway:
An appliance used to augment a firewall that uses ATI information to constantly scan for ingress and egress communications to known bad IP addresses and prevent that communication.

Transport Layer Security (TLS):
New updated version of the SSL protocol that is used for the encryption of data communications

Virus:
Malicious computer program that causes the target computer's program or memory to become corrupted. It usually has a copy function to replicate itself and transfer to other computers

Vulnerability:
Weakness in any system that could be exploited by a security threat.

Web Application Firewall (WAF):
This solution is a firewall for HTTP-based applications to block unwanted applications. This is commonly used to try to prevent cross-site scripting (XSS) and SQL injection.

Worm:
A worm is a program that allows the user to tap unused network resources to run computer programs. Worms can tie up all the computing resources on a network and essentially shut it down.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES