Zero Trust Networks Glossary

Created by: Natisha Stiles, Teaching Assistant

1. **Access Controls** - A process or software used to control access to systems, company locations, or resources.
2. **Active Directory** - A centralized directory for user account information and access.
3. **Anti-virus** - is a software solution that helps protect a PC or system from viruses.
4. **Authentication** - Proving that one is who they claim to be.
5. **Authorization** - Permissions to view or otherwise manipulate the data or locations on the network that are being accessed.
6. **Biometrics** - Unique physical attributes that are used for authentication, such as a fingerprint or facial recognition.
7. **Blacklist** - Specifically deny a site or application while allowing everything else.
8. **Breach** - An attack on your network that is performed by circumventing the access and security controls in place which can result in unauthorized access or theft of data.
9. **BYOD** - Bring Your Own Device: This is when a company allows employees to bring their own cell phone, laptop, or other device to connect and use at work.
10. **CA** - Certificate Authority: the CA signs and publishes the keys that are used to validate applications.
11. **Certificates** - A record signed by a trusted CA to help enable trust in devices.
12. **Cloud** - or the Cloud, is a term used to describe a set of systems accessed through a network. Cloud networks can be either internal or external to the organization, and are often accessed remotely.
13. **Denial of Service Attack** - **DoS** - This type of attack happens when the resources of a system are used up preventing further access to that system.
14. **Distributed Denial of Service Attack** - **DDoS** - Distributed Denial of Service: In a DDoS attack, multiple distributed systems are used to deny service on a larger scale. See also, DoS.
15. **DMZ** - In networking, this refers to the network zone that sits between firewalls, and is typically the first point of entry from the internet or other un-trusted network locations.
16. **Enumeration** - Enumeration in cybersecurity is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the

system, and the same can be used for further exploitation of the system (What is Enumeration?, 2018).

17. **Firewall** - Either a software or hardware solution that restricts network traffic using rules to deny or allow specific communications.
18. **Flat Network** - A network that has no rules to allow or deny traffic through a firewall to any other zone on the network.
19. **Fwknop** - Firewall Knock Operator: An open source, single packet authorization scheme (Rash).
20. **Golden Image** - Last known good image of a fully patched and updated device.
21. **Hostile Takeover** - An attack on a network where the attacker has control of the system.
22. **IPCONFIG** - a command line tool that provides network configuration information like the IP address and subnet mask as well as other relevant network details.
23. **Keylogger** - A virus that is meant to send credentials and other text back to the attacker by recording keystrokes.
24. **LAPS** - Local Administrator Password Solution (M): A Microsoft product that allows administrators create local passwords for each workstation on the network as well as setting timelines for expiry and change.
25. **Least Privilege** - Granting the user permissions that are required to perform their tasks and no more than necessary.
26. **Malware** - Malicious software that includes viruses and other harmful programs that are designed to cause damage to or gain access to a system or network.
27. **Phishing Attack** - The attempt to obtain information from an individual through deceptive e-mails that are disguised as coming from a legitimate company or being from a person you may know.
28. **Pivoting** - The ability a hacker has to move from one node or computer to the next on the network.
29. **PKI** - Public Key Infrastructure: is the infrastructure that securely distributes and validates public keys in an un-trusted network. Used for authentication against a certificate authority.
30. **Plane** - **Control** - Sets policies for connection access, used by the data plane.
31. **Plane** - **Data** - Sends the request if the right attributes are present.
32. **Port Scan** - Checking for open ports on a system.
33. **Key** - **Private** - Used to decrypt received messages signed with the public key. This key should be kept private by the owner.
34. **Key** - **Public** - Used to encrypt a message and provide a means of verification that can only be decrypted with the private key. This is the key that can be shared with others.

35. **Privilege Creep** - [referenced as Scope Creep] is having more permissions than are required, usually obtained overtime as roles or privileges change.
36. **Reconnaissance** - Information gathering or the preliminary stage before attack.
37. **Reverse Shell** - The connection from the target computer back to the attacker computer.
38. **RFC 3552** - This document is a threat model for the Security Considerations Section that is written into other RFC documents. The purpose of this is both to encourage document authors to consider security in their designs and to inform the reader of relevant security issues. (RFC3552, 2003).
39. **SAAS** - Software as a Service: Software that is offered on a pay per use or pay monthly service.
40. **Scope Creep** - See Privilege Creep.
41. **Script Kiddies** - Persons that uses other peoples programs or scripts to perform their attacks.
42. **Shell** - A command line interface that is used to run scripts commands to perform tasks.
43. **SSL Inspection** - is when secure traffic is inspected for malware.
44. **Subnet** - A logical subdivision of a network.
45. **Threat** - An event that can cause harm to a system or company, like data loss, unauthorized access, malware, etc. Threats can happen by unintentional or intentional means.
46. **Threat Model** - A representation of a system and the threats to each part of that system. Some widely used models are STRIDE, Pasta and Trike.
47. **UEFI** - Unified Extensible Firmware Interface: This is an interface that connects firmware to the operating system meant to be a BIOS replacement. It is the first program run when a computer starts.
48. **Virus Total** - This is a website that checks files and urls against antivirus products as an additional means to help verify trust.
49. **VPN** - Virtual Private Network: is a tunnel that allows internet traffic to be kept private while in the public zone.
50. **Whitelist** - Specifically allow a site or application while denying everything else.
51. **Zero Trust Model** - Is a concept that is designed to automatically treat all hosts as if they are hostile.
52. **Zone** - A place on the network that has different levels of trust including; DMZ, Internet, Trusted, Privileged.
53. **Zone** - **Privileged** - The innermost layer of the network where sensitive data resides.
54. **Zone** - **Trusted** - The network layer between the privileged zone and a DMZ.

55. **Zscaler Private Access** - A product that provides services as a VPN replacement solution.

Anthony, S. (2011, September 22). Demystifying UEFI, the long-overdue BIOS replacement. Retrieved July 08, 2019, from https://www.extremetech.com/g00/computing/96985-demystifying-uefi-the-long-overdue-bios-replacement?i10c.ua=1&i10c.encReferrer=&i10c.dv=20

M. (n.d.). LAPS. Retrieved July 08, 2019, from https://www.microsoft.com/en-us/download/details.aspx?id=46899

Rash, M. (n.d.). Cipherdyne.org. Retrieved July 8, 2019, from https://www.cipherdyne.org/fwknop/

[RFC3552] Rescorla, E., "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3522, July 2003.

What is Enumeration? (2018, February 28). Retrieved July 5, 2019, from https://resources.infosecinstitute.com/what-is-enumeration/