Security protocols, listed below i.tgt-ticket granting

SecurityTerminologyDefine the following terms: 1. Authentication – ability to identify who it isa. ACL – (access control list) is associated w/ a given resource. Describes groups, users, machines and their permissions associated with that particular resource. i.

Token- one time only password keyb. CA- certificate of authority- creates certificates -system or entity trusted to generate and distribute digital certificates. Can be privately used or from a 3rd party e-commerce site. Verifies identity of user.

Authentication method. c. RA- Registration Authority-issues certificates-RA verifies credentials supplied by an agent and then sends the CA an okay to issue a certificate. d. PKI- Public Key Infrastructure- Policies and behaviors that surround the deployment and management of key pairs. How you issue two keys at one time.

e. Kerberos- Authentication method used by Microsoft. Uses 3 different protocols, listed belowi. TGT- Ticket granting ticket.

Allows you to request resources on the network from servers. ii. TGS- Ticket granting server. Accesses a particular network server for tickets. iii.

AS- Authentication Server. Equivalent to a morning check-in at security desk of a hotel. Checks the identity of a server. f. CHAP- Challenge handshake authentication protocol. Was designed to replace the PAP. Communication between server and client proving identity.

i. MS-CHAP- Microsoft CHAPg. PAP- Password authentication protocolh. X. 509- digital certificate that uniquely identifies a party. Standard structure of a certificate. i.

KDC- Key distribution centerj. Biometrics- Authentications based on human anatomy. k. Multifactor- Authentication based on 2 valid authentication methods.

l. Mutual Authentication- Client establishes identity to server. Server provides authentication information to client to ensure that illicit servers cannot masquerade as genuine servers. Both parties have to authenticate.

2. Encryption- hiding data using algorithms. protection, method of code, algorithms, formulas a. Asymmetric keys- pair of key values one public and one private. b.

Symmetric keys- single encryption key generated. c. DES- Data Encryption standard developed by government. d. Diffie-hellman- encryption algorithm named after its two creators. e. IPSec- used for encryption of TCP/IP traffic.

Method of encrypting any IP transmissions. f. PGP- Pretty good privacy- mainly used in email less secure than the PKI. g.

RSA- Rivest-Shamir-Adleman- encryption algorithm named after its 3 creators. Using two pair keys. h. SSL- Secure Socket Loader- used mainly on web servers to transmit securely via HTTPS://3.

Network protocols and organizationa. DMZ- Demilitarized zone- Zone used for public access. Used with FTP, web servers and DNS servers. b. IDS-

Intrusion Detection System- 2 types: Active and Passivec. NAT- Network Address Translation- Appends to your logical port. Protects internal hosts.

Used with proxy servers. Translates internal IP to Real IP. Uses unique port table. There is 65, 000 portsd. Tunneling- ability to go to 1 point to another as though you are a single proprietary line. 1 logical circuit. Used with Virtual Private Networks.

e. PPP- Point to point protocol. f. PPTP- Microsoft product.

Enhancement to point to point protocol. Called point to point tunneling protocol. Allows Point to point to be used in a tunnel. i. MPPE- MS point to point encryption. Encrypts within a tunnel.

g. L2TP- Layer 2 tunneling protocol Sisco’s version of MPPE. Works with IPSEC. Works to encrypt with Ipsec. h. RADIUS- Remote access dial in user service- usually used with Unix or LENIX systems.

An authentication system. i. RAS- Remote Access Server- provides users to dial in from anywhere. Allows you to connect with different location computers with dial up. j. RPC- Remote procedure calls. Links to another remote program.

Ability to access remoter computer and access a program and execute it on your own computer. Loads program onto your computer from another computer. 4.

Attacks and detectiona. Sniffing – Looking at network traffic and deciphering it for propaganda uses. b. Stateful Inspection- firewall protection.

Inspects entire packet. Looks at words in the packet. Used with proxy servers. c.

Spoofing- Impersonating a computer or network. d. Trojan horse- program that appears to be working fine and replicates good programs. Performs malicious acts to your PC.

e. Zombie (bot)- a logic bomb. A virus waiting for certain variables to be met before activating.

Program does same thing. f. DOS- Denial of Service- example- flood of pings. 1 person denied internet access.

g. DDOS- Distributed denial of service- Across the board denial of service. When an entire network goes down. h. Backdoor- allows you to enter a certain area with different credentials.

Easy way out. Creating another way to enter a system if your system gets hacked. i. Man in the middle- MITM- used to gather information between hosts.

j. Brute Force attack- Guessing passwords. Trial and error. k. Hijacking- take over someone’s computer. Aka-replayl.

Social engineering- Used by individual. Examples: looking over persons shoulder for password, dumpster diving, impersonating on phone, phishing through fake