

	CIS-162 Introduction to Network Security Comptia Security+ Exam Domain 2 Communication Security <small>Trang D. Nguyen</small>

	Remote Access
	Three steps in establishing proper privileges <ul style="list-style-type: none">• Authentication<ul style="list-style-type: none">• What you know (password)• What you have (token)• What you are (biometric)• What you do (new - dynamic biometric)• Authorization• Accounting <p>Where you are?</p> <small>Trang D. Nguyen</small>

	Remote Access - Telnet
	<ul style="list-style-type: none">• Port 23• Clear text• Vulnerable to sniffer <small>Trang D. Nguyen</small>

	Remote Access – SSH
	<ul style="list-style-type: none"> • Initiate port 22 • Use higher port for communication • Protocols <ul style="list-style-type: none"> • Transport layer protocol • User authentication protocol • Connection protocol • Utilities of SSH <ul style="list-style-type: none"> • SLogin (Secured Login) • SCP (Secured Copy) • SSH (Secured Shell)
	Trang D. Nguyen

	Remote Access – SSH (cont.)
	<ul style="list-style-type: none"> • Encryption <ul style="list-style-type: none"> • Symmetric <ul style="list-style-type: none"> • Default: International Data Encryption Algorithm • DES • Blowfish • Asymmetric <ul style="list-style-type: none"> • RSA for connection and authentication
	Trang D. Nguyen

	Remote Access – L2TP
	<ul style="list-style-type: none"> • Port 1701 - UDP • Layer 2 Forwarding Protocol (L2F) • Cisco implementation • Implement at hardware level • Use with IPSEC and DES • Work with AAA services <ul style="list-style-type: none"> • RADIUS (Remote Authorization Dial-In User Service) • TACACS+
	Trang D. Nguyen

	<h3>Wireless Access – IEEE 802.11</h3>
	<ul style="list-style-type: none"> • Base band using CSMA/CA Carrier Sense Media Access/Collision Avoidance <ul style="list-style-type: none"> • System asks for permission to transmit • Access point authorize when it is clear • System transmits and waits for ACK • Data is retransmitted if there is no ACK
	<small>Trang D. Nguyen</small>

	<h3>Virtual Private Network</h3>
	<ul style="list-style-type: none"> • Secure (encrypted) end-point communication • PPTP, IPSEC, SSH, L2TP • Share secret key
	<small>Trang D. Nguyen</small>

	<h3>IPSEC (IP Security)</h3>
	<ul style="list-style-type: none"> • End-point <ul style="list-style-type: none"> • Host-Server, Server-Server and Host-Host • OSI Layer 3 • Transport Mode <ul style="list-style-type: none"> • Encrypt only data (content) • Source and Destination exposed • Tunnel Mode <ul style="list-style-type: none"> • Encrypt entire package (context) • Router-Router
	<small>Trang D. Nguyen</small>

	<h3>IPSEC – Protocols</h3>
	<ul style="list-style-type: none"> • Traffic Security <ul style="list-style-type: none"> • Authentication Header (AH – Protocol 51) • Encapsulating Security Payload (ESP – Protocol 50) • Key Management and Key Exchange <ul style="list-style-type: none"> • Internet Security Association and Key Management Protocol (ISAKMP – Port 500) • Oakley • Secure Key Exchange Mechanism for Internet (SKEMI)
	<small>Trang D. Nguyen</small>

	<h3>IPSEC - Cryptography</h3>
	<ul style="list-style-type: none"> • Open framework using <ul style="list-style-type: none"> • Diffie-Hellman key exchange • Public key signing of Diffie-Hellman Key exchange • Encryption algorithms such as IDEA & 3DES • Hash (MD5 and SHA-1) • Hash Message Authentication Codes (HMAC) • Digital Certificates
	<small>Trang D. Nguyen</small>

	<h3>IEEE 802.1x</h3>
	<p>A standard for protocol to support user to an edge device communication before granting access to authentication servers such as RADIUS servers. User configuration is defined in the edge (NAS) device.</p>
	<small>Trang D. Nguyen</small>

	RADIUS – AAA - DIAMETER
	<p>Remote Access Dial-In User Service</p> <ul style="list-style-type: none"> • UDP • Client / Server protocol <ul style="list-style-type: none"> • Client is NAS • Server is daemon service • Authentication (protocol 1812) • Authorization (protocol 1812) • Accounting (protocol 1813) • DIAMETER (replacement for RADIUS) TCP and separate AAA <p style="font-size: small;">Trang D. Nguyen</p>

	TACACS+ Terminal Access Controller Access Control System+
	<ul style="list-style-type: none"> • TACACS - BBN Planet Corporation for MILNET • Cisco <ul style="list-style-type: none"> • XTACACS • TACACS+ • TCP and UDP port 49 • Multi-factor authentication • Client / Server protocol <ul style="list-style-type: none"> • Client is NAS • Server is daemon service <p style="font-size: small;">Trang D. Nguyen</p>

	Protocols and Ports																																																
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">TCP Port</th> <th style="text-align: center;">UDP Port</th> <th style="text-align: center;">Keyword</th> <th style="text-align: center;">Protocol</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">20</td> <td></td> <td>FTP-Data</td> <td>File Transfer Data</td> </tr> <tr> <td style="text-align: center;">21</td> <td></td> <td>FTP</td> <td>File Transfer Control</td> </tr> <tr> <td style="text-align: center;">22</td> <td></td> <td>SSH</td> <td>Secure Shell Login</td> </tr> <tr> <td style="text-align: center;">23</td> <td></td> <td>TELNET</td> <td>Telnet</td> </tr> <tr> <td style="text-align: center;">25</td> <td></td> <td>SMTP</td> <td>Simple Mail Transfer</td> </tr> <tr> <td style="text-align: center;">37</td> <td style="text-align: center;">37</td> <td>Time</td> <td></td> </tr> <tr> <td style="text-align: center;">49</td> <td style="text-align: center;">49</td> <td>TACACS+</td> <td>TACACS+ Login</td> </tr> <tr> <td style="text-align: center;">53</td> <td style="text-align: center;">53</td> <td>DNS</td> <td>Domain Name Server</td> </tr> <tr> <td style="text-align: center;">65</td> <td style="text-align: center;">65</td> <td>TACACS+</td> <td>TACACS+ Database Service</td> </tr> <tr> <td style="text-align: center;">80</td> <td></td> <td>HTTP</td> <td>Hypertext Transfer Protocol</td> </tr> <tr> <td style="text-align: center;">88</td> <td style="text-align: center;">88</td> <td>Kerberos</td> <td>Kerberos</td> </tr> </tbody> </table> <p style="font-size: small;">Trang D. Nguyen</p>	TCP Port	UDP Port	Keyword	Protocol	20		FTP-Data	File Transfer Data	21		FTP	File Transfer Control	22		SSH	Secure Shell Login	23		TELNET	Telnet	25		SMTP	Simple Mail Transfer	37	37	Time		49	49	TACACS+	TACACS+ Login	53	53	DNS	Domain Name Server	65	65	TACACS+	TACACS+ Database Service	80		HTTP	Hypertext Transfer Protocol	88	88	Kerberos	Kerberos
TCP Port	UDP Port	Keyword	Protocol																																														
20		FTP-Data	File Transfer Data																																														
21		FTP	File Transfer Control																																														
22		SSH	Secure Shell Login																																														
23		TELNET	Telnet																																														
25		SMTP	Simple Mail Transfer																																														
37	37	Time																																															
49	49	TACACS+	TACACS+ Login																																														
53	53	DNS	Domain Name Server																																														
65	65	TACACS+	TACACS+ Database Service																																														
80		HTTP	Hypertext Transfer Protocol																																														
88	88	Kerberos	Kerberos																																														

Protocols and Ports

TCP Port	UDP Port	Keyword	Protocol
443		HTTPS	Secured HTTP
500	500	ISAKMP	ISAKMP protocol
512		rexec	
513		rlogin	UNIX rlogin
	513	rwho	UNIX Broadcast Naming svc
514		rsh	UNIX rsh and rep
	514	SYSLOG	UNIX system logs
614	614	SSHLL	SSL Shell
	1701	L2TP	L2TP
1723	1723	PPTP	PPTP
1812	1812	RADIUS	Radius Authorization & Authentication
1813	1813	RADIUS-actg	Radius Accounting

Trang D. Nguyen
