เอกสารข้อสอบฉบับนี้
จัดทำเพื่อใช้ในการทดสอบในโครงการ
Network Security Contest 2008
ชุดที่ 2 ข้อสอบข้อที่ 101-200

1. เวลาในการสอบ 3 ชั่วโมง
2. การสอบเป็นแบบ ปิดตำรา
3. ห้ามนำเอกสารใดๆ เข้าห้องสอบ
4. ห้ามใช้เครื่องมือสื่อสารใดๆ ทุกชนิด
5. ห้ามนำเอกสารฉบับนี้ออกนอกห้องสอบโดยเด็ดขาด
6. ให้ส่งเอกสารฉบับนี้คืนพร้อมกับกระดาษคำตอบ
7. การคิดคะแนนทีมที่แข่งขัน จะนำคะแนนของทั้ง 3 คนในทีมมารวมกันเป็นคะแนนของทีม
8. การคัดเลือกจะคัดเลือกทีมเข้ารอบสุดท้าย 10 ทีม
9. สำหรับทีมที่มาจากมหาวิทยาลัยเดียวกัน จะคัดเลือกทีมที่มีคะแนนสูงสุด 3 ทีมเท่านั้นในการเข้ารอบสุดท้าย

(คณะกรรมการจัดการแข่งขัน
จัดให้มีคณะกรรมการผู้ทรงคุณวุฒิเป็นคณะกรรมการตัดสินการแข่งขัน
และผลการตัดสินของคณะกรรมการถือเป็นที่สุด
และคณะผู้จัดทำขอสงวนสิทธิรางวัลชนะเลิศสำหรับทีมที่เหมาะสมที่สุดเท่านั้น)

ห้ามทุจริตในการสอบ
มิฉะนั้นจะถูกตัดสิทธิในการแข่งขันทันที

ชื่อ-นามสกุล ..... ชื่อทีม.....
....
ชื่อสถาบัน ..... เบอร์ติดต่อ....
.....

ข้อสอบตั้งแต่ข้อ 101-130 บางข้อมีตัวเลือกที่ถูกต้องมากกว่าหนึ่ง (Choose X) ต้องเลือกให้ถูกทุกข้อถึงได้คะแนน

101. In the scenario in the diagram, what is the risk?

a. The intruder gains access to all VLANs
b. The intruder can disrupt VLAN services through VTP
c. The intruder can access and disrupt all VLANsd
d. The intruder can not gain access to any VLAN

102. Smart cards or smart tokens provide which of the following features?
a. Isolation of security-related functions b. Tamper-resistant storage
c. Portability of information between devices d. All of the above
e. None of the above

103. A customer would like to deploy a scalable VPN with the security and flexibility of a PKI, but does not want the headaches of a large general purpose PKI. What would you recommend?
a. Implement a symmetric-algorithm-based full-mesh peer-to-peer system
b. Implement a separate, VPN-only PKI
c. It is not possible
d. Implement VPNs using MPLS
e. None of the above

104. Which management protocols provide the strongest security?
a. Telnet b.SNMPc.HTTP d.HTTPS e.RSH/RCMD f.SSH

105.What does the diagram represent?
a. Triple DES 168
b. DES CBC (Cipher Block Chaining)
c. DES CFB (Cipher Feed Back)
d. DES

106. When would you use outside NAT in a multihoming scenario?

a. When symmetric routing to the Internet needs to be guaranteed by the border routers
b. When using more than two ISPs
c. When BGP cannot be deployed for routing
d. When using RFC 1918 addresses

107. In the diagram, what is this firewall architecture called?

a. Screening router architecture
b. Screened Subnet architecture
c. Screened Host architecture
d. Screening device architecture

108. Which of the following are the common firewall architectures?
a. Screened subnet
b. Dual-homed subnet
c. Dual-homed host (gateway)
d. Screened router
e. Screening router
f. Application-layer gateway
g. Defense-in-depth

109. Where should anti-spoofing rules be deployed on a firewall system?
a. Only on the first packet of every session
b. On all packets coming from the Internet
c. On all packets coming from DMZ networks
d. On every perimeter interface

110. Based on the diagram, which of the following layered firewall strategies will NOT increase the level of security?

a. Having different stages run different code (e.g. different

vendors or operating systems)

b. Having different stages configured by different administrators
c. Having different stages use different cabling type like Ethernet and Token Ring
d. Having different stages designed by different designers

111. In the firewall scenario in the diagram, which of the following will not be a threat to the network's security?

a. Server software
b. Browser Functions
c. Trojan Horses simulating HTTP requests
d. Rejected outbound HTTP request because of address translation

112. What is a limitation of firewall deployment?

a. The firewall always presents a performance bottleneck
b. The firewalls permit too many applications
c. The applications, which are permitted through the firewall, are rarely secure themselves
d. The complexity of tracking and maintaining logs

113. Which routing protocol is best suited to run across a firewall?

a. BGP b. OSPF c. RIP d. RIPv2

114. Which type of IPsec VPN Application is shown in the figure?

a. Remote access b.Hub and spoke c.SOHO d.Site-to-site e.Wireless access VP

115. Which of the following statements regarding IPsec transport mode are correct?
(Choose 2)

a. Processing of QoS flags is supported b. Requires a new IP header to reach peer

c. Data endpoints must terminate IPsec d.Routers can terminate IPsec on behalf of end systems
e. The inner IP header is encrypte

116. When considering a VPN WLAN design, which protocols are particularly Vulnerable to DoS attack? (Choose 2)
a. DHCP b.IPSec c.IKE d.DNS e.802.1x f.EAP-TLS

117. Which method is used to prevent inter-client communication in wireless Networks?
a. The Public Secure Packet Forwarding (PSPF) protocol
b. The Service Set Identifier (SSID)
c. Inter-client communication is not possible if there is an AP present
d. Open System Authentication

118. Which of the following solutions would you use to mitigate VPN path failures?
a. Using a backup ISP on both sides of VPN connections
b. Using a redundant VPN device on both sides of VPN connections
c. Using a backup interface on both sides of VPN connections
d. Using HSRP on both sides of VPN connections

119. In the scenario in the diagram, which type of function is typically used for challenge response authentication?

a. A hash function b. Encryption c. XOR (Exclusive OR) d. DES

120. In terms of identity, what is the purpose of authentication protocols?
a. To allow certain users to perform defined actions
b. To prove the identity of a subject
c. To log user actions in a file or database
d. To backup password lists from one authentication server to another

121. What is the main strength of an anomaly-based IDS/IPS?
a. It can detect unknown attacks.
b. New signatures can be added quickly.
c. It has low number of false positives on noisy networks.
d. It defines the nature of the attack exactly.
e. False negatives are easy to detect.

122. Which kind of attacks cannot be detected/prevented by signature-based NIDS/NIPS?

a. any malformed network packet b. HTTP exploits c. network sweeps and scans
d. TCP exploits e. ARP exploits

123. Which network IDS/IPS technology would be best to deploy if you needed to protect the web server from unknown HTTP-based application attacks?

a. signature NIPS b. policy NIPS c. signature NIDS d. anomaly NIPS e. policy NIDS

124. What must be considered when filtering Layer 3 addresses as an IDS response?

a. Always block the complete subnet. b. Never block internal addresses.
c. Only block outside addresses. d. Never block vital hosts.
e. Always block the NIPS device itself, as it may be compromised.

125. Which mode of placement is the most reliable to detect an attack when using NIDS?

a. in-line placement b. passive placement
c. network tap placement d. switch SPAN ports
e. placement in front of a firewall

126. What is a typical limitation of NIDS/NIPS?

a. It cannot see the low-level network events.
b. It can be overloaded by high volume traffic.
c. Sensors may not be available for all operating systems.
d. Correlation of composite events is impossible.

127. Which function does IDS typically perform when deployed in an organization with a reactive security attitude?

a. It provides the organization with the ability to define custom signatures to detect new attacks.
b. It allows for post-mortem incident analysis.
c. It provides the organization with insight about possible future attacks.
d. It allows the organization to identify attackers well ahead of their actions.

e. It permits the organization to respond to attacks not detected by firewalls in real-time.

128. What is a technique to prevent an attacker from spreading to other resources?
a. installing more NIDS devices in neighboring network segments
b. creating a honey pot system
c. making the NIDS more sensitive
d. confusing the attacker by reconfiguring the compromised system

129. What should you do to eradicate the cause of an attack?
a. Deny traffic from the attacker's IP address. b. Identify and remove all back doors.
c. Keep the system's current state. d. Leave all root kits on the system.

130. How do stateless packet filtering firewalls recognize the first packet of the UDP session?
a. Through the SYN bit in the header b. Through the ACK bit in the header
c. Through application-layer data d. Through an idle timer
e. They cannot recognize it from the packet headers

<u>ข้อสอบตั้งแต่ข้อ 131-166 ให้ใช้ตัวเลือกดังต่อไปนี้</u>

เลือก a. ถ้าถูกเฉพาะข้อ ก,ข, ค
เลือก b. ถ้าถูกเฉพาะข้อ ก, ค
เลือก c. ถ้าถูกเฉพาะข้อ ข, ง
เลือก d. ถ้าถูกเฉพาะข้อ ง
เลือก e. ถ้าถูกข้อ ก,ข,ค,ง

Computer Security Ethics (Case Study)

131. นโยบายความปลอดภัยระบบคอมพิวเตอร์ ที่มีปัญหาในทางปฏิบัติมากที่สุด คือ.
ก.ผู้ดูแลแม่ข่ายฐานข้อมูล ไม่มีสิทธินำข้อมูลออกจากแม่ข่ายได้เอง
ข.ผู้บริหารเครือข่าย ไม่มีสิทธินำข้อมูลออกจากแม่ข่ายได้เอง
ค.ผู้ดูแลระบบความปลอดภัยเครือข่าย ไม่มีสิทธินำข้อมูลออกจากแม่ข่ายได้เอง
ง. ผู้บริหารระดับสูง ไม่มีสิทธินำข้อมูลออกจากแม่ข่ายได้เอง

132. งานของการรักษาความปลอดภัยระบบคอมพิวเตอร์ ครอบคลุมถึง
ก. การป้องกันการขโมยเครื่องคอมพิวเตอร์ ข. การสูญหายของเอกสารต้นฉบับ
ค. การส่งข้อมูลด้วย e-mail สาธารณะ ง. การใช้งานอินเตอร์เน็ท

133. สิ่งที่ผู้ดูแลระบบคอมพิวเตอร์ มักละเลยคือ
ก. update virus signature ข. freqently change admin

password

ค. install lastest software or patch ง. study new security threat

134. ภัยคุกคามที่เกี่ยวกับ hacker คือ ส่วนใหญ่

ก. ป็นคนภายนอก ที่เจตนาร้าย

ข. เป็นคนภายใน ที่ไม่ใส่ใจนโบาย security

ค. เจาะระบบ เพื่อต้องการผลประโยชน์ มากกว่า ความสนุกในการเจาะ

ง. เป็นผู้มีความรู้และการศึกษาสูง

135.นโยบายความปลอดภัยจะได้ผลดี เมื่อ

ก. ครอบคลุมทุกด้าน ข. ปรับปรุงให้ทันสมัยเสมอ

ค. บุคลากรฝ่ายคอมพิวเตอร์ทุกคนรับทราบ ง. นำมาใช้ได้จริง

136. สิ่งใดที่ผู้บริหารระบบเครือข่ายไม่ควรทำ

ก. ทำ backup ฐานข้อมูล และเก็บไว้ไม่ให้คนอื่นรู้

ข. ทำ backup ข้อมูลผังเครือข่าย และเก็บไว้ไม่ให้คนอื่นรู้

ค. พิมพ์รหัสผ่านของผู้ใช้ทั้งหมด ออกมาเก็บไว้ในที่ปลอดภัย

ง. จดรหัสผ่านเข้าใช้ระบบ ลงบนกระดาษ post-it ก่อนปิดไว้ที่ข้างจอ

137. การกระทำใด น่าจะมีความผิดตาม พรบ. คอมพิวเตอร์ 2550

ก. พัฒนาโปรแกรมไวรัสขึ้นใหม่

ข. ปรับปรุงโปรแกรมไวรัสเดิมที่แพร่กระจายอยู่ ให้ตรวจสอบได้ยากขึ้น

ค. ปรับปรุงโปรแกรมไวรัสเดิมที่แพร่กระจายอยู่ ให้กระจายตัวได้เร็วขึ้น

ง. ส่งโปรแกรมไวรัสที่พัฒนาเสร็จ ให้เพื่อนรุ่นน้องทดสอบใช้

138. ลักษณะของ Computer Freud ภายในองค์กร ที่ทำให้องค์กรเสียหาย

ก. ส่วนใหญ่เป็นจากบุคลากรที่จ้างใหม่ ข. ถ้าเป็นจากบุคลากรที่ทำงานมานาน ส่วนใหญ่ทำมาเกิน 5 ปี

ค. ส่วนใหญ่ ทำโดยไม่รู้ ง. ส่วนของผู้ที่รู้และจงใจทำ ก่อให้เกิดความเสียหายอย่างมาก

139. บุคลิคของผู้ที่เป็น computer freud ในองค์กร คือ

ก. มีความรู้และการศึกษาดี ข. ทำงานหนัก พักร้อนน้อย

ค. เบื่องานที่ทำ ง. อัตตาสูง

140. ปัจจัยพื้นฐานที่ทำให้เกิด freud คือ

ก. โอกาส (opportunity) ข. แรงกดดันเรื่องการงาน

ค. แรงกดดันเรื่องการเงิน ง. วิถีชีวิตที่เปลี่ยนแปลง

141. ตัวชี้วัด ว่า น่าจะเริ่มมีภัยคุกคาม (computer threat) จากคนภายในองค์กร

ก. มีการเข้าถึงข้อมูลอื่น เกินกว่า ความจำเป็นในการทำงาน

ข. มีการเข้า internet เพิ่มขึ้นอย่างมาก

ค. เกิด exception report ที่ไม่พบสาเหตุ

ง. ไม่มีการตรวจสอบ access logs

142. ปัจจัยที่ทำให้ hacker ภายนอก ผ่านระบบรักษาความปลอดภัยเครือข่ายได้ง่ายขึ้น
ก. ข้อมูลความปลอดภัยรั่วไหล จาก consultant
ข. ข้อมูลความปลอดภัยรั่วไหล จากผู้บริหารระดับสูง โดยไม่เจตนา
ค. ข้อมูลความปลอดภัยรั่วไหล ฝ่ายซ่อมบำรุงโทรศัพท์
ง. เทคโนโลยี redbox

143. แรงจูงใจของ Freudster จากภายนอก
ก. บริษัทคู่แข่ง ต้องการข้อมูล
ข. เพื่อทดสอบระบบ security
ค. บริษัทที่ไปทำงานใหม่ ต้องการหลักฐานความสามารถ
ง. ต้องการล้างแค้น

144. Profiles ของ hacker ในปัจจุบันคือ
ก. เพศชาย
ข. เป็นนักเรียนระดับมัธยม
ค. ทำเพื่ออวดความสามารถ
ง. เป็นอาชญากรรมข้ามชาติ

Concept & Protection in Computer Fraud

สมมุติท่านทำงานที่ บริษัท ebay.com สาขาประเทศไทยในฝ่าย computer security ให้ท่านประเมินสิ่งต่อไปนี้ ในคำถามข้อ 145-154

145. ภัยคุกคามใด ที่น่าเป็นปัญหาต่อ บริษัท amazon
ก. คอมพิวเตอร์โน้ตบุค ของฝ่ายประชาสัมพันธ์ ถูกขโมย
ข. RAM ในคอมพิวเตอร์โน้ตบุค ของฝ่ายประชาสัมพันธ์ ถูกขโมย
ค. คอมพิวเตอร์ของฝ่ายประชาสัมพันธ์ ถูกขโมย
ง. RAM ในคอมพิวเตอร์ของฝ่ายประชาสัมพันธ์ ถูกขโมย

146. ภัยใด ที่เป็นปัญหาต่อ บริษัทอย่างรุนแรง.
ก. โน้ตบุคของหัวหน้าฝ่ายบัญชี หายที่บริษัทไป 3 วันก่อนจะหาเจอ
ข. ข้อมูลภายในคอมพิวเตอร์ของฝ่ายบัญชี ถูกไวรัสทำลายหมดสิ้น
ค. ตรวจพบโมเด็ม ต่อกับคอมพิวเตอร์ของหัวหน้าฝ่ายการเงิน
ง.ข้อมูลภายในคอมพิวเตอร์ของหัวหน้าฝ่ายการเงิน ถูกลูกจ้างที่ลาออก ลบทิ้งหมดสิ้น

147. มีการประชุมที่สำนักงานใหญ่ หัวหน้าฝ่ายต่างๆ นำโน้ตบุคของ บ. ติดตัวไปด้วย ข้อใดที่ไม่น่าเป็นปัญหาร้ายแรงต่อ บริษัท
ก. คณะกรรมการบริหาร ทำสไลด์ power point สรุปผลงานในรอบปี ใส่โน้ตบุค
ข. หัวหน้าฝ่ายประชาสัมพันธ์ ใส่เพลงและหนังที่ซื้อมาจากแม่สาย
ค. หัวหน้าฝ่ายการเงิน ใส่สรุปข้อมูลบัญชี ของ บ.อื่นๆ ลงไปในโน้ตบุค
ง. หัวหน้าฝ่ายคอมพิวเตอร์ ติดตั้งชุดโปรแกรม SATAN ลงในโน้ตบุค

148. ท่านวางแผนทดสอบระบบโดยวิธี blackbox penetration
ก. อาจก่อเกิดปัญหาต่อ บ.สาขาในไทย
ข. อาจก่อเปิดปัญหาต่อ บ.สาขาในญี่ปุ่น
ค. อาจก่อเกิดปัญหา ต่อ บ.แม่
ง. อาจก่อเกิดปัญหาต่อทุก บ.สาขาทั่วโลก

149. ท่านวางแผนทดสอบระบบโดยวิธี whitebox penetration

ก. อาจก่อเกิดปัญหาต่อ บ.สาขาในไทย ข. อาจก่อเปิดปัญหาต่อ บ.สาขาในญี่ปุ่น

ค. อาจก่อเกิดปัญหา ต่อ บ.แม่ ง. อาจก่อเกิดปัญหาต่อทุก บ. สาขาทั่วโลก

150. หากมีการบุกรุกเข้าระบบได้สำเร็จ ความเสียหายใดจะทำความเสียหายให้ บ.เป็นมูลค่าสูงมาก

ก. ข้อมูลในแม่ข่ายฝ่ายบัญชี ในไทย ถูกทำลายเสียหายหมด

ข. ข้อมูลในแม่ข่ายฐานข้อมูลลูกค้า ถูกทำลายเสียหายไปเกินกว่าครึ่ง

ค. ข้อมูลภายใน router หลัก เสียหายหมด

ง. มีรายชื่อลูกค้า เผยแพร่ออกสู่เน็ต

151. ท่านคิดว่า แผนการป้องกันการบุกรุกเครือข่ายใด ที่ท่านเสนอแล้ว หัวหน้าของท่านจะไม่รับพิจารณา

ก. ปิด SSID broadcasting ข. เปิด Mac Address Filtering ใน Access Point ทุกตัว

ค. ใช้ WPA-PSK แบบ 64 hex digits ง. ติดตั้งระบบป้องกันไวรัสใน router ทุกตัว

152. ท่านคิดว่า แผนป้องกันแม่ข่าย และห้องแม่ข่าย แผนใดที่ไม่มีประโยชน์

ก. ติดตั้งระบบแจ้งเตือนน้ำท่วม

ข. ติดตั้งระบบตัดไฟอัตโนมัติ เมื่อมีไฟชอร์ตในห้องเครือข่าย

ค. ติดตั้งระบบ fingerprint scanning ในการเข้าห้องเครือข่าย

ง. ติดตั้งระบบป้องกันไฟไหม้ห้องแม่ข่าย ด้วยระบบฉีดน้ำอัตโนมัติ

153. รุ่นพี่ของท่านคนหนึ่ง เคยเป็น database admin และสอนท่านเรื่องการดูแลระบบ แต่ลาออกไปแล้ว มาหาเพื่อขอเอาข้อมูลที่เคยฝากไว้ server ออกมา

ก. ท่านปฏิเสธเด็ดขาด ไม่ให้เข้าถึง server

ข. ท่านไม่กล้าปฏิเสธ แต่ให้รุ่นพี่เขียนชื่อไฟล์ที่ต้องการให้ และท่านจะสำเนาข้อมูลใส่ DVD ให้เอง

ค. ท่านไม่กล้าปฏิเสธ แต่รายงานเรื่องให้หัวหน้าของท่านทราบ ก่อนให้รุ่นพี่ทำอะไร

ง. ท่านอนุญาตให้เข้าใช้ server ได้ โดยท่านเฝ้าระวังอย่างใกล้ชิด

154. รุ่นพี่ของท่านอีกคนซึ่งเคยเป็น security admin และสอนท่านเรื่อง security แต่ลาออกไปแล้ว มาหาเพื่อขอเอาข้อมูลที่เคยฝากไว้ server ออกมา

ก. ท่านปฏิเสธเด็ดขาด ไม่ให้เข้าถึง server

ข. ท่านไม่กล้า แต่ให้รุ่นพี่คอยบอกชื่อไฟล์ ระหว่างสำเนาข้อมูลใส่ DVD ให้เอง

ค. ท่านไม่กล้าปฏิเสธ แต่รายงานเรื่องให้หัวหน้าของท่านทราบ ก่อนให้รุ่นพี่ทำอะไร

ง. ท่านอนุญาตให้เข้าใช้ server ได้ โดยท่านเฝ้าระวังอย่างใกล้ชิด

155. การป้องกัน freud ชั้นใด ที่ต้องเฝ้าระวังอย่างใกล้ชิดเป็นพิเศษ

ก. ระดับ administion ข. ระดับ technical ค. ระดับ physical ง. ระดับ data

156. สิ่งที่ควรกระทำ ก่อน implement ระบบ security
ก. เปรียบเทียบผลิตภัณฑ์รักษาความปลอดภัย ข. กำหนดนโยบาย
ค. ตรวจสอบ user's requirements เพิ่มเติม ง. ประเมินความเสี่ยง

157. สิ่งที่ควรกระทำหลัง implement ระบบ security เสร็จสิ้น
ก. เปรียบเทียบผลิตภัณฑ์รักษาความปลอดภัย ข. กำหนดนโยบาย
ค. ตรวจสอบ user's requirements ง. ประเมินความเสี่ยง

158. ในการวางระบบ security การ outsource มีผลดีกว่าการพัฒนาเองคือ
ก. รวดเร็วกว่า และครอบคลุมกว่า ข. TCO ต่ำกว่า
ค. บริหาร จัดการ เฝ้าระวังในระดับมืออาชีพ ง. มีผู้รับผิดชอบชัดเจน

159. ระบบ security ที่ดีควรมีลักษณะ
ก. การป้องกัน ครอบคลุมทุกด้าน ข. มีความอ่อนตัวสูง
ค.ไม่มีจุดอ่อนช่องว่าง ง. บำรุงดูแลรักษาง่าย

160. ระบบ security ที่มีความอ่อนตัวสูง ควรแก้ไขปรับปรุงเงื่อนไขการป้องกันได้
ก. โดยไม่ต้องเปลี่ยนแปลงการทำงานขององค์กร ข. โดยไม่ต้องเปลี่ยนนโยบายองค์กร
ค. โดยไม่ต้องเปลี่ยนแปลงโครงสร้างระบบ ง. โดยผู้ที่ไม่มีความรู้เรื่อง security

161. มีการตรวจพบจุดอ่อนมากๆ ของระบบ security ที่องค์กรมีใช้มานาน ควรป้องกันหรือแก้ไขโดย
ก. วางระบบป้องกันเสริม ที่มีจุดแข็งมาก ในการป้องกัน ที่ตรงกับจุดอ่อนมากของระบบแรก
ข. ยกเลิกระบบ security เดิม และวางระบบใหม่ที่ไม่มีจุดอ่อนแบบระบบแรก
ค. เสริมการเฝ้าตรวจระวัง การบุกรุกผ่านจุดอ่อน ในกรณีที่แก้ไขไม่ได้
ง. ไม่ต้องทำอะไร ในกรณีที่จุดอ่อนของระบบ security เกิดที่จุดที่ไม่มีความสำคัญเลย

162. การตรวจสอบการจราจรบนระบบเครือข่ายอย่างสม่ำเสมอ จะช่วยในเรื่อง
ก. ตรวจพบผู้บุกรุกผ่าน firewall ตั้งแต่เริ่มแรก
ข. ตรวจพบ e-mail ความลับบริษัท ที่คนภายในส่งออกให้คนนอก ตั้งแต่แรกเริ่ม
ค. ตรวจพบไวรัส ในระบบเครือข่าย ตั้งแต่แรกเริ่ม
ง. ตรวจพบความต้องการในการขยายระบบเครือข่าย ตั้งแต่แรกเริ่ม

163.การตรวจสอบการจราจรบนเครือข่ายความเร็วสูงอย่างสม่ำเสมอ จะสร้างปัญหาใด
ก. Bandwidth overhead ข. Database slowdown
ค. Information overloaded ง. System crash frequency

164. สิ่งที่ควรถูก monitor บนเครือข่ายอย่างสม่ำเสมอ
ก. Network traffic ข. Availability
ค. Events ง. Alerts

165. การตรวจสอบ Network traffic แบบต่างๆ ทำเพื่อ
ก. measurement ในกรณีที่รู้แล้วว่าจะตรวจสอบอะไร ข. monitor ในกรณีที่ไม่รู้ว่าจะตรวจสอบอะไร
ค. charaterization เพื่อสร้างโมเดลการใช้งาน ง. probe

เพื่อเจาะหาจุดที่สงสัยต่างๆ

166. ปัญหาของ Network sniffing คือ
ก. ให้รายละเอียดที่ไม่มากพอวิเคราะห์
ข. ไม่สามารถใช้แก้ปัญหาระดับ Layer 1 ได้
ค. ข้อมูลที่ได้มา น้อยเกินกว่านำไปสร้าง model การใช้งานเครือข่าย
ง. อาจมีการละเมิดสิทธิส่วนบุคคล

167. โปรโตคอลใดไม่เหมาะสมที่จะนำมาใช้สร้าง VPN connection
a. PPP
b. PPTP
c. IPSEC
d. L2TP
e. SSL

168. ข้อใดไม่ถือว่าเป็น Social Engineering
a. Dumpster Diving
b. Shoulder Surfing
c. Data Diddling
d. Phishing
e. ไม่มีข้อถูก

169. ข้อใดไม่เกี่ยวข้องกับ Cryptography
a. MD5
b. RC4
c. Trust Relationship
d. Traffic Padding
e. ไม่มีข้อถูก

170. วิธีการใดใช้ลักษณะทางกายภาพในการยืนยันตันตน
a. Smart Card
b. I&A
c. Encryption
d. Biometrics
e. CHAP

171. ข้อใดคือความหมายของ Confidentiality
a. การทำให้มั่นใจได้ว่าข้อความจะไม่ถูกแก้ไขโดยที่ไม่สามารถตรวจจับได้
b. การทำให้มั่นใจได้ว่าจะสามารถเข้าถึงข้อมูลได้ตามที่ได้ระบุเอาไว้
c. การทำให้มั่นใจได้ว่าข้อมูลจะไม่ถูกเปิดเผยโดยผู้ที่ไม่ได้รับอนุญาต
d. การมั่นใจว่าได้ว่าใครเป็นผู้สร้างข้อความและส่งข้อความนั้นให้ผู้รับ
e. ไม่มีข้อถูก

172. ข้อใดคือความหมายของ Integrity
a. การทำให้มั่นใจได้ว่าข้อความจะไม่ถูกแก้ไขโดยที่ไม่สามารถตรวจจับได้
b. การทำให้มั่นใจได้ว่าจะสามารถเข้าถึงข้อมูลได้ตามที่ได้ระบุเอาไว้
c. การทำให้มั่นใจได้ว่าข้อมูลจะไม่ถูกเปิดเผยโดยผู้ที่ไม่ได้รับอนุญาต
d. การมั่นใจว่าได้ว่าใครเป็นผู้สร้างข้อความและส่งข้อความนั้นให้ผู้รับ

e. ไม่มีข้อถูก

173. ข้อใดคือความหมายของ Availability
   a. การทำให้มั่นใจได้ว่าข้อความจะไม่ถูกแก้ไขโดยที่ไม่สามารถตรวจจับได้
   b. การทำให้มั่นใจได้ว่าจะสามารถเข้าถึงข้อมูลได้ตามที่ได้ระบุเอาไว้
   c. การทำให้มั่นใจได้ว่าข้อมูลจะไม่ถูกเปิดเผยโดยผู้ที่ไม่ได้รับอนุญาต
   d. การมั่นใจว่าได้ว่าใครเป็นผู้สร้างข้อความและส่งข้อความนั้นให้ผู้รับ
   e. ไม่มีข้อถูก

174. วิธีการเข้ารหัสแบบใดไม่ใช่ Symmetric Encryption
   a. AES
   b. 3DES
   c. RC4
   d. WEP
   e. ไม่มีข้อถูก

175. ข้อใดกล่าวไม่ถูกต้อง
   a. การเข้ารหัสแบบ DES ใช้คีย์ (key) ที่มีความยาว 56 บิท
   b. การเข้ารหัสแบบ 3DES มีความปลอดภัยเป็น 3 เท่าของ DES
   c. การเข้ารหัสแบบ AES นั้นไม่จำเป็นต้องมีการกระจายคีย์ (key) กันก่อนใช้งาน เพราะผู้รับและผู้ส่งสามารถสร้างคีย์ในการเข้ารหัสขึ้นได้เอง
   d. ข้อ ข และ ค
   e. ไม่มีข้อถูก

176. ในระบบ Symmetric-key Cryptosystem ที่มีการใช้งาน KDC (Key Distribution Center) นั้นหากมีจำนวนผู้ใช้ทั้งหมด 100 คน ผู้ใช้แต่ละคนจะต้องเก็บคีย์ไว้กับตัวจำนวนเท่าไหร่
   a. 4,950 คีย์
   b. 100 คีย์
   c. 50 คีย์
   d. 2 คีย์
   e. 1 คีย์

177. ในระบบ Symmetric-key Cryptosystem ที่ไม่มีการใช้งาน KDC (Key Distribution Center) นั้นหากมีจำนวนผู้ใช้ทั้งหมด 100 คน ผู้ใช้แต่ละคนจะต้องเก็บคีย์ไว้กับตัวจำนวนเท่าไหร่
   a. 4,950 คีย์
   b. 100 คีย์
   c. 50 คีย์
   d. 2 คีย์
   e. 1 คีย์

178. ข้อใดเป็นข้อดีของการนำแฮชฟังก์ชัน (Hash function) มาใช้ในการสร้างลายเซ็นต์ดิจิตอล (Digital Signature)
   a. เป็นการซ่อนเอกสารไม่ให้ผู้ที่ไม่ได้รับอนุญาตเปิดอ่านได้
   b. เป็นการลดขนาดของเอกสารก่อนนำไปเข้ารหัส
   c. เป็นการลดขนาดของเฮดเดอร์ (Header) ของเอกสารก่อนนำไปเข้ารหัส
   d. ใช้ในการลดขนาดของไพรเวทคีย์ (Private key) ก่อนการเข้ารหัส
   e. เป็นการตรวจสอบความถูกต้องของอัลกอริที่มในการสร้างลายเซ็นต์ดิจิตอล

179. ข้อใดไม่ใช่คุณสมบัติของแฮชฟังก์ชัน
   a. เป็นฟังก์ชันทางเดียว
   b. การสร้างค่าแฮชใช้เวลาไม่นาน
   c. ทนทานต่อการที่อินพุทสองค่ามีค่าแฮชที่ตรงกัน
   d. เป็นฟังก์ชันที่รับอินพุทที่มีความยาวคงที่และสร้างเอาท์พุทที่มีความยาวไม่จำกัด
   e. ไม่มีข้อถูก
180. ข้อใดกล่าวได้ถูกต้องเกี่ยวกับแฮชฟังก์ชัน (Hash function) และ Message Authentication Code
   a. ในการสร้าง Message Authentication Code จะต้องใช้แฮชฟังก์ชันเท่านั้น
   b. Message Authentication Code จะปลอดภัยเพียงไรนั้นขึ้นอยู่กับแฮชฟังก์ชันที่เลือกใช้
   c. HMAC เป็น MAC ที่สามารถใช้งานได้ร่วมกับ MD5 หรือ SHA-1 เท่านั้น
   d. แฮชฟังก์ชันมีความปลอดภัยมากกว่า Message Authentication Code
   e. ไม่มีข้อถูก
181. ข้อใดกล่าวได้ถูกต้องเกี่ยวกับ IPSec
   a. การเชื่อมต่อ IPSec ในโหมด Transport เหมาะกับการสร้าง Network-to-network VPN
   b. หากดักจับแพ็กเก็ตหลังจากที่ได้สร้าง IPSec connection แล้ว จะเห็นเฉพาะแพ็กเก็ตชนิด Authentication Header เท่านั้นที่มีการรับ-ส่ง เนื่องจากแพ็กเก็ตชนิด Authentication Header ไม่ได้ถูกเข้ารหัส
   c. โฮสต์แต่ละเครื่องสามารถรองรับ IPSec connection ได้แค่ครั้งละ 1 connection เท่านั้น
   d. หากใช้คำสั่ง Traceroute กับโฮสต์ที่เชื่อมต่อ IPSec แบบ End-to-end แล้วจะพบจำนวน Hop เพียงแค่ 2 hop เท่านั้น
   e. ไม่มีข้อถูก

182. ข้อใดกล่าวได้ถูกต้องเกี่ยวกับ SSL (Secure Socket Layer)
   a. SSL ใช้งานได้ร่วมกับ HTTP เท่านั้น
   b. SSL เรียกอีกอย่างว่า TLS (Transaction Layer Security) เนื่องจากเป็นสิ่งที่ทำให้การทำธุรกรรมต่างๆ ได้ปลอดภัยยิ่งขึ้น
   c. SSL Record Protocol นั้นมีการเข้ารหัสแบบ Public-key encryption
   d. SSL เป็นเทคโนโลยีการรักษาความปลอดภัยในระดับ Application layer
   e. ไม่มีข้อถูก
183. ข้อใดเป็นข้อดีของการเข้ารหัสที่ Application layer
   a. ทำงานได้เร็ว เหมาะกับ streaming data
   b. ไม่ขึ้นอยู่กับแอพพลิเคชั่นที่เข้ารหัส
   c. สามารถทำ content filtering ได้
   d. สามารถเลือกเข้ารหัสที่ port บาง port ได้เป็นพิเศษ
   e. ไม่มีข้อถูก
184. NAT (Network Address Translation) ประเภทใดที่เหมาะกับการกำหนดหมายเลขไอพีแอดเดรส (IP address) ให้กับเซิร์ฟเวอร์ที่อยู่ใน Demilitarized Zone
   a. Private NAT
   b. Static NAT
   c. Dynamic NAT
   d. Port Address Translation (PAT)

e. ไม่มีข้อถูก.

185. ข้อใดคือความหมายของ Zero-day Attack
   a. การโจมตีในขณะที่ระบบปิดปรับปรุง
   b. การโจมตีที่เกิดกับส่วนหนึ่งของระบบที่ยังไม่ได้มีการป้องกัน
   c. การโจมตีที่ใช้เวลาเพียงแค่ไม่ถึง 1 วันในการแก้ไข
   d. การโจมตีที่จู่โจมระบบที่ไม่มีการป้องกันได้อย่างรวดเร็ว สามารถแพร่กระจายได้ทั่วถายในเวลาไม่ถึง 1 วัน
   e. ไม่มีข้อถูก
186. ข้อใดเป็นข้อจำกัดของ Network-based Intrusion Detection System (NIDS)
   a. ทำงานได้ช้า
   b. กินทรัพยากรในระบบมาก
   c. ถูกจัดเป็น Signature-based Intrusion Detection System
   d. ป้องกัน Zero-day Attack ได้ไม่ดีนัก
   e. ถูกทุกข้อ