

University of Colorado
 Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

PCI Security Standard

CS 4950/5950
Homeland Security &
Cybersecurity


Lesson 27
Exercise 3

Rick White, Ph.D.
University of Colorado, Colorado
Springs



1
Esc

1

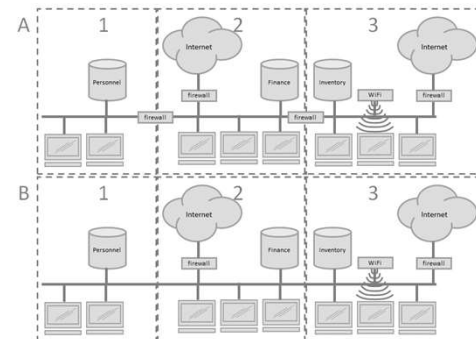


University of Colorado
 Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Problem 5


- Your company has allocated 24 hours for you to complete an audit of Network A.
- Given the current configuration, and knowing how long it will take to audit different components, what type of PCI audit are you going to conduct on Network A?



Component	Audit Type	Network A-1		Network A-2		Network A-3		Network B-1		Network B-2		Network B-3	
		Hours	#	Hours	#	Hours	#	Hours	#	Hours	#	Hours	#
Firewall	3	1	2	1	2	1	2	1	2	1	2	1	2
PC	2	2	3	2	3	2	3	2	3	2	3	2	3
Server	4	1	3	1	3	1	3	1	3	1	3	1	3
WiFi	1	0	0	0	0	1	0	0	0	1	0	0	1
Total													

2
Esc

2



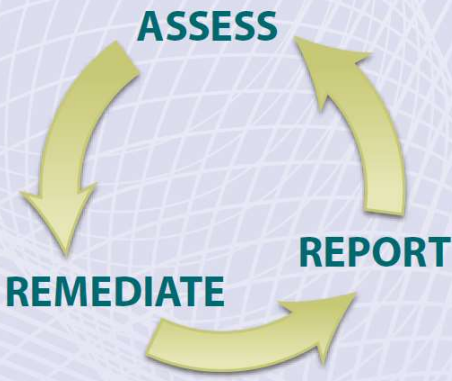
University of Colorado
 Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Remember


Step 1: Assessment

- a) Scope Applicability
 - Anything that transacts or stores credit card data is included in PCI DSS
- b) **Scope Assessment**
 - For smaller installations, assess entire suite
 - For larger installations, assess a sample suite
- c) Conduct assessment using PCI test procedures for each of the 12 DSS requirements



3 Esc

3



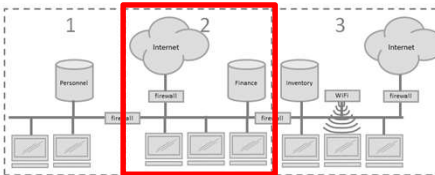
University of Colorado
 Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Remember

- # hours = hours (segment 1) +
 hours (segment 2) +
 hours (segment 3)
- hours (segment x) =
 hours (firewall) * # firewalls +
 hours (PC) * # PCs +
 hours (server) * # servers +
 hours (WiFi) * # WiFis
- **# hours = 16**

A



Component	Audit	Network A-1		Network A-2		Network A-3	
Type	Hours	#	Hours	#	Hours	#	Hours
Firewall	3	1	3	2	6	2	6
PC	2	2	4	3	6	3	6
Server	4	1	4	1	4	1	4
WiFi	1	0	0	0	0	1	1
		Total	11	Total	16	Total	17

4 Esc

4



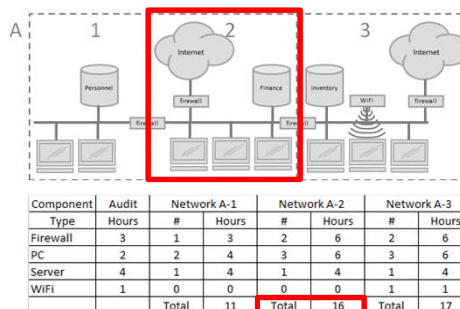
University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Answer

Because you have 24 hours to complete the audit, and it will take only 16 hours to do it, you have sufficient time to conduct a **Complete** audit.



5

Esc

5



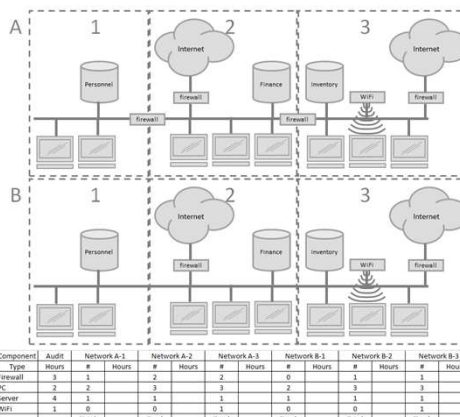
University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Problem 6

- Your company has allocated 24 hours for you to complete an audit of Network B.
- Given the current configuration, and knowing how long it will take to audit different components, what type of PCI audit are you going to conduct on Network B?



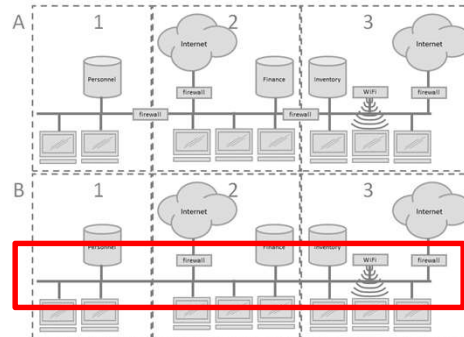
6

Esc

6

Remember

All segments of Network B must be included in the audit **because they share a common network bus that transacts Finance credit card data.**



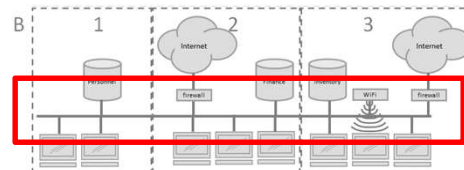
7

Esc

7

Remember

- # hours = hours (segment 1) +
hours (segment 2) +
hours (segment 3)
- hours (segment x) =
hours (firewall) * # firewalls +
hours (PC) * # PCs +
hours (server) * # servers +
hours (WiFi) * # WiFi
- **# hours = 8 + 13 + 14 = 35**




Component	Audit	Network B-1		Network B-2		Network B-3	
Type	Hours	#	Hours	#	Hours	#	Hours
Firewall	3	0	0	1	3	1	3
PC	2	2	4	3	6	3	6
Server	4	1	4	1	4	1	4
WiFi	1	0	0	0	0	1	1
		Total	8	Total	13	Total	14

8

Esc

8

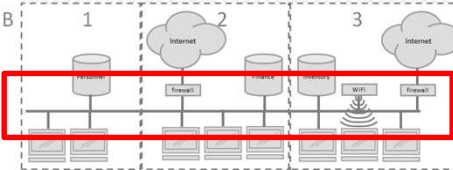


University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Answer


Because you have 24 hours to complete the audit, and it will take 35 hours to do it, you only have sufficient time to conduct a **Sample** audit.



Component	Audit	Network B-1		Network B-2		Network B-3	
Type	Hours	#	Hours	#	Hours	#	Hours
Firewall	3	0	0	1	3	1	3
PC	2	2	4	3	6	3	6
Server	4	1	4	1	4	1	4
WiFi	1	0	0	0	0	1	1
		Total	8	Total	13	Total	14

9
Esc

9




University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



10
Esc

10