

הנחיות פרויקט תקשורת נתונים ואבטחת מידע-

חלק ב

הגשה ספר הפרויקט והגנה על הפרויקט תהיה באחד המועדים
(א או ב) של הקורס לפי מערכת לוח הבחינות.

דרישות:

1. ספר פרויקט – כולל תיעוד ביצוע הפרויקט וכל פקודות ה - CLI לכל משימה – 20% - לא לשכוח להוסיף צילומי מסך של הפקודות בספר הפרויקט.
2. תקינות הטופולוגיה – 30%
3. הגנה על הפרויקט – 50%

חלק 2:

הוספת רכיבים לארגון

לאחר מילוי טבלת ה IP בכל פרטי החברה שלנו, הסניפים השונים, חלוקת המחלקות – הוילאנים, חלוקת הכתובות וכו'. כעת אנו יכולים לגשת לפאקט טרייסר ולהתחיל לבנות את טופולוגיית הרשת שלנו.
דגש: חשוב לעבוד כאן בצורה מסודרת ועל פי הכללים על מנת לחסוך באגים בהמשך.

הוספת נקודת גישה ושרתים לקומה

נוסיף נקודת גישה וגם נצרף שרתים לקומה שלנו
נקודת הגישה תספק חיבור אלחוטי לסניף, ואת נקודת הגישה יש להוסיף בהתאם לתכנון הרשת שלנו

הגדרות ה vlan - בסוויץ' ושיוך פורטים לוילאן המתאים

שלב הגדרת הסוויץ', והקמת ה VLAN - ים שנמצאים בקומה על גבי הסוויץ' ולאחר מכן נדרש לשייך את הפורטים הממשקים (ל VLAN) – המתאים.

הגדרת שרתים FTP, MAIL, DNS, HTTP, DHCP

- שרת אימייל- MAIL Server
- שרת חלוקת כתובות- DHCP Server
- שרת מיפוי שמות מתחום- DNS Server
- שרת אינטרנט- HTTP Server
- שרת העברת קבצים FTP Server

(נספח – הגדרת שרתים)

הגדרת הראוטר (Router) – ניתוב בין וילאנים

הגדרת ממשקים וירטואליים (תתי ממשקים - sub-interfaces) על מנת לקרוא VLANs על תתי ממשק
(נספח – הגדרת נתבים)

אבטחת סוויצ'ים – port security ו-802.1x

בשלב זה נבצע אבטחת הסוויצ'ים שלנו, ע"י Port-Security וע"י סיסמא.
(נספח – אבטחת סוויצ'ים)

סיום הקמת סניפים ב-LAN

ספר פרויקט (דיגיטלי):

1. הצעת הפרויקט
2. תוכן עניינים
3. נספחים
4. שרטוט Packet tracer
5. מקורות

משימות (אפשרות לבחור בין משימה 7 ו 8):

1. חיבור הסניף בעזרת פרוטוקול OSPF (לא משנה איזה סניף)

2. לחסום את מחשבי העובדים (לא מנהלים) של אחד

הסניפים לבחירתך את הגישה לתכני FTP.

3. לפתוח תיבת דוא"ל לכל העובדים (מנהלים + עובדים רגילים)

ולאפשר שליחת וקבלת מייל רק בין העובדים באותו סניף.

הסבר : עובד בתת סניף ' 1 ' יכול לשלוח לעובד בתת סניף ' 1

' 2 ' ולא יכול לשלוח למנהל בתת סניף ' 2 ' .

מנהל יכול לשלוח לכל העובדים (גם למנהלים וגם לעובדים

רגילים.)

4. לחסום את מחשב המנהל של אחד הסניפים את הגישה

לתכני HTTP .

5. הקמת שרת DHCP לסניף.

6. לנהל את תהליך האימות בשרת. AAA

7. הקמת שרת חומת אש Firewall לאחד הסניפים עם

הרשת הפרטית של הסניף

8. גישה באמצעות VPN לשרת HTTP מאחד הסניפים

לבחירתך

בהצלחה