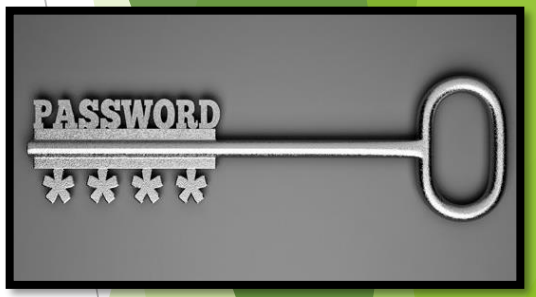
Port Security

Guard Your Switch

Port Security

- במהלך הקורס למדנו שקיימות מספר דרכים להגן ולשמור על המתג שלנו, מגורמים המעוניינים לגרום נזק לתשתית הרשת עליה אנחנו אחראים.
- נעילת ציוד הרשת-מקום ייעודי בו המתג ימוקם, לדוגמה חדר תקשורת או ארון, אשר מוגנים ונעולים, כך שגורם שאינו מורשה לא משיג גישה לציוד הרשת.
- הגנה בעזרת סיסמאות-הגדרת סיסמה לחיבור ה-Console במידה וגורם שאינו מורשה ינסה להשחית או לשנות את ההגדרות הקיימות. הגדרת סיסמה לערוצי ה-VTY במידה וינסו להגשת אל המתג דרך הרשת ולגרום נזק בצורה מרוחקת. כמובן שקיימת דרך לאבטח את כל דרכי הגישה האחרים אל הרכיב.
- Port Security-הוא פיצ'ר אבטחה שנועד לאבטח ולהגן על הפורטים (ממשקים) של המתג וכך לצמצם את רמת הפגיעות של הרשת. ולמנוע מכל גורם הרוצה להסב נזק, להתחבר למתג ולהפוך לחלק מהרשת.



Port Security

- עלינו להיות בבקרה אילו רכיבי רשת מחוברים למתג שלנו אשר שולחים/מקבלים מידע ברשת. מצב בו אדם מתחבר למתג ומשתיל תוכנת נוזקה במערכת הוא פשוט מאוד וקל לביצוע, במידה ואין הגנה על הממשקים של המתג שתמנע ממנו גישה לרשת מלכתחילה.

- בעזרת הגדרות Port Security על הממשקים במתג אנו יכולים להיות בבקרה תמיד, מי מתחבר לרשת ואם הוא רשאי לכך או לא. להפחית את חשיפת המתג למתקפות שבהן אדם מתחבר בצורה ישירה. לדוג' בעזרת מחשב נייד לפורט פנוי במתג.
- אם הגדרנו Port Security על המתג והתקן לא מורשה מתחבר למתג ומנסה לשלוח דרכו מידע, המתג יחסום אותו ולא יעביר את המידע לרשת.

Port Security

- הגדרת Port Security תגן על המתג תמיד, אבל כיצד המתג יודע מי מורשה להתחבר ומי לא, המתג מזהה את התקנים על בסיס **כתובת ה-MAC הייחודית** שלהם, כלומר כאשר מתג מקבל נתונים הוא בודק מאיזו כתובת MAC הם הגיעו ואם יש רשות לכתובת ה-MAC הזו לשלוח מידע דרך אותו פורט (ממשק), המתג יבצע את בדיקה זו לא רק אם המידע הגיע ממחשב, אלא מכל רכיב המחובר אליו.
- הגדרת Port Security מתבצעת על ממשק יחיד, או בעזרת פקודת Range על כמה ממשקים בבת אחת.
- ניתן להגדיר על פורט (ממשק) לא רק כתובת MAC אחת, אלא כמה במידה ואליו מתחברים משתמשים מתחלפים. לדוג' בארגונים מסויימים קיימת מדיניות BYOD (Bring Your Own Device) מה שאומר שהעובדים יכולים להגיע עם המחשב האישי שלהם לעבודה ולבצע עליו את המשימות שלהם.

- כברירת מחדל כל ממשק שומר כתובת MAC אחת חוקית.

Port Security

Port Security Violation

- מצב של הפרה (Violation) הוא מצב שבו רכיב רשת שולח מידע דרך פורט מסויים מכתובת MAC שאינה מורשת. במצב כזה המתג יכול לנקוט באחת משלוש אפשרויות:

1. Shutdown-אופציה זו גורמת למתג להתריע ולשלוח דו"ח לתוכנת ניהול רשת (מנהל הרשת). בנוסף הפורט מועבר למצב Shutdown זאת אומרת מכבה את עצמו. *מצב הפרה זה מוגדר כברירת מחדל.*
2. Restrict-אופציה זו גורמת למתג להתריע ולשלוח דו"ח לתוכנת ניהול רשת (מנהל הרשת). ובשונה מהמצב הקודם, מצב זה רק חוסם את הפורט הבעייתי.
3. Protect-אופציה זו גורמת לחסימה של הפורט הבעייתי בלבד.

- שימו לב! שמצב Shutdown הוא שונה מביצוע פקודת הכיבוי על הממשק. בפועל המתג מעביר את הפורט למצב Error-Disabled (Err-Disabled) מה שגרום למתג לא לשלוח/לקבל מידע דרך אותו פורט. אם ברצוננו להפעיל מחדש את הפורט עלינו להכניס את הפקודה Shutdown ראשית ולאחר מכן את הפקודה No Shutdown.

Port Security Configuration

- הגדרת כתובת ה-MAC המורשת על הממשק יכולה להתבצע בשתי דרכים:

1. Manual-להגדיר בצורה ידנית לאיזה כתובת MAC מותר להתחבר לממשק. החיסרון הגדול של שיטה זו היא אם אנו צריכים להגדיר מספר רב של ממשקים ורכיבי רשת, הרי שלאתר ולהגדיר את כתובות ה-MAC של כל אחד מרכיבי הרשת בפורט המתאים כנראה צפוי להיות תהליך ממושך ובעל סיכוי גבוה לשגיאות.

2. Sticky-אופציה זו גורמת למתג להגדיר בצורה אוטומטית את כתובת ה-MAC הראשונה שנשלחת דרך הפורט הפיזי. לכן חשוב לוודא שהרכיב המורשה אכן מחובר לפורט המתאים. דרך זו חוסכת זמן יקר בהגדרה ותחזוקה לעומת האופציה הקודמת. *סיטואציה בה מורשות עד שתי כתובות MAC לפורט, Sticky יגדיר אוטו' את כתובתם של שני הרכיבים הראשונים.

Configuration Steps

- השלבים הבסיסיים להפעלת והגדרת הפיצ'ר:

1. שינוי מצב הפורט למצב Access.
2. הפעלת הפיצ'ר.
3. הגדרת כתובת MAC מורשת באחת משתי הדרכים Manual או Sticky.

- שינוי הגדרות ברירת המחדל:

4. מצב ההפרה (Shutdown\Restrict\Protect)
5. כמות הכתובות המקסימאלית.

Command Page

- רשימת הפקודות המלאה והסבר, נמצאת בקובץ Command Page Port Security.