

עבודה SSH-מגיש סרגיו

מטרת העבודה

מניהול לא מאובטח לניהול מאובטח ומוצפן. (TechNet) העברת רשת הארגון הגדרת אימות משתמשים, והגבלת, SSH-ל Telnet התהליך כלל מעבר מפרוטוקול הגישה למנהלי רשת מורשים בלבד.

(R1 בוצע על) SSH-חלק א': הגדרות בסיס והכנה ל

לפני הפעלת ההצפנה, הוגדרה זהות לראוטר כדי שיוכל לייצר מפתחות הצפנה ייחודיים.

1. הגדרת שם ודומיין:

- פקודות: `hostname R1, ip domain-name raja.local`

2. יצירת מפתחות הצפנה (Crypto Keys):

- עם מפתח באורך 1024 סיביות RSA בוצע שימוש באלגוריתם.
- פקודה: `crypto key generate rsa general-keys modulus 1024`

3. הגדרת גרסת פרוטוקול:

- (נבחרה גרסה 2 (המאובטחת יותר).
- פקודה: `ip ssh version 2`

חלק ב': ניהול משתמשים והרשאות

במקום סיסמה כללית לכולם, עברנו לשיטת אימות אישית ומדורגת.

1. יצירת משתמש מנהל:

- עם הרשאות מלאות `raja` נוצר משתמש מקומי בשם (Privilege 15). וסיסמה מוצפנת.
- פקודה: `username raja privilege 15 secret 456`

2. אכיפת האימות בחיבורים:

- לדרוש שם משתמש וסיסמה VTY-וה Console-הוגדר לחיבורי ה.
- פקודה: `login local` (ה-Line-תחת ממשקי).

VTY Lines) חלק ג': אבטחת ערוצי הגישה

הקשחת "הדלתות" דרכן מתבצע הניהול מרחוק.

1. Telnet חסימת:

- SSH. הוגדר שהראוטר יקבל אך ורק תעבורת
- transport input ssh (line vty 0 4 תחת): פקודה

2. ACL) סינון כתובות:

- המאשרת רק את כתובת המנהל PC2RAJA נוצרה רשימת גישה בשם (10.2.2.1) וחוסמת את כל השאר
- access-class באמצעות הפקודה VTY-החלת הרשימה על ה PC2RAJA in.

Security Hardening) חלק ד': הקשחת אבטחה נוספת

וגניבת סיסמאות Brute Force הוספת שכבות הגנה למניעת התקפות.

- security passwords (אורך סיסמה מינימלי: הוגבל ל-8 תווים min-length 8).
- הוגדרה חסימה ל-2 דקות אם זוהו 3 ניסיונות: Login Block) מנגנון נעילה כושלים בתוך דקה.
- service (הצפנת סיסמאות: כל הסיסמאות בקובץ ההגדרות הוצפנו password-encryption).
- ניתוק אוטומטי: הוגדר ניתוק לאחר 5 דקות של חוסר פעילות (exec-timeout 5 0).