אוטומציה לתהליכי הקשחה לצמצום משטחי תקיפה

מאת שרון וילנסקי

הקדמה

במאמר זה אתאר את מתודולוגיית ההקשחה הניתנת ליישום בצורה אוטומטית במגוון מערכות התכנה בארגון, במטרה לצמצם משטחי תקיפה פוטנציאלים היכולים לנבוע מניהול אבטחת-מידע לוקה. בנוסף, אתאר את היכולות הקיימות בקהילה הקוד-פתוח המשמשות לאוטומציית תהליכי הקשחה למגוון רחב של מוצרים - מערכות הפעלה (Windows/Linux) ו\או מערכות שונות (Firewalls, Storage Servers וכו') - בהתאם לתקנים בין-לאומיים.

מהו תהליך הקשחה?

מערכת היא אוסף של יכולות שונות - חיבור רישתי, עבודה עם קבצים\מידע ואינטגרציה עם מערכות נוספות. כל אחד מהתהליכים יכול להוות משטח תקיפה, אשר עלול לאפשר ליישות זדונית לנצל ניהול לקוי בכדי לבצע את מטרותיו במערכות הארגוניות - הדלפת מידע, אחיזה רישתית, מניעת שירות וכד'.

תהליך ההקשחה מגדיר את אוסף הבקרות הנדרשות בכדי שארגון יוכל **לצמצם ולנהל** את משטחי התקיפה השונים הקיימים בארגון.

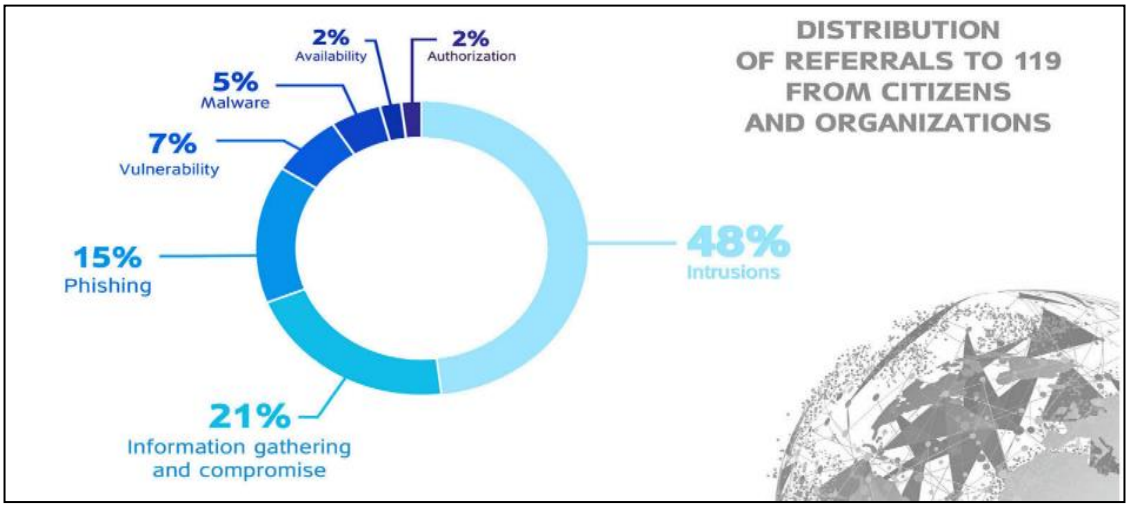
מוטיבציה

ארגונים שונים, גדולים עד קטנים, נוטים לממש מנגנוני אבטחה שכיחים באמצעות מוצרי אבטחה המייצרים שכבת הגנה סטנדרטית ברמת הרשת ומשאבי הארגון. למשל, שימוש ב-Firewall, מנגנוני הזדהות, הצפנת מידע וכד'.

ע"פ ממצאי מערך הסייבר הלאומי בישראל, גוף ממלכתי, ביטחוני וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל קידום וביסוס עוצמתה של ישראל בתחום, מתאר בסיכום שהפיץ בשנת 2019 כי ארגונים המדווחים לו על ארועי סייבר שונים (כ-4250 התראות לאותה שנה) מתחלקים ל-2 השלכות עיקריות:

1. חדירה למרחב הרישתי או למערכות של הארגון.
2. הדלפה ושליטה זדונית במידע הארגוני.

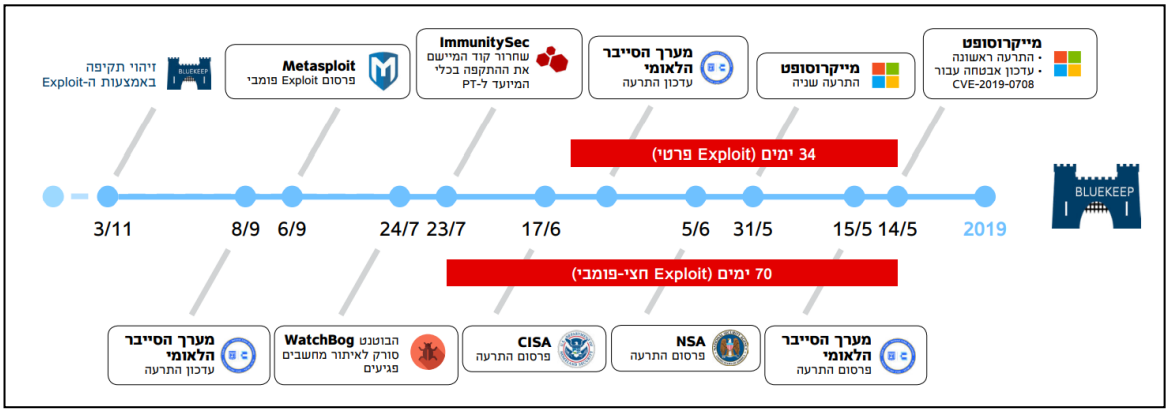
מתוך הדו"ח:



[איור 1 - התפלגות סוגי התקפות סייבר ע"פ מערך הסייבר הלאומי בישראל]

הממצאים הללו מעלים את השאלה "**האם אני מוגן ובטוח במקרה של אירוע סייבר?**" בהנחה והארגון מוגן ובטוח בזכות תרבות אבטחה מספקת, האם ניתן "לנשום לרווחה" ולהאמין שאנחנו מוגנים מארועי סייבר בעתיד?

לשם כך אתאר תקופת זמן ב-2019 בה מערך הסייבר הלאומי בישראל החל בהתרעה על חולשה קריטית (BlueKeep), העלולה להוביל לכך שתוקף פוטנציאלי יוכל לשלוט ואף להתפשט בתוך מערכות הארגון:



[איור 2 - ציר זמן מרגע גילוי חולשה ליכולת זיהוי השמשת החולשה]

1. התגלתה חולשה במוצרים של חברת Microsoft לקראת מאי 2019.
   א. החולשה התפרסמה לציבור הרחב לצורך ידיעה.
   ב. במעמד פרסום החולשה החברה האחראית למוצר מעדכנת את לקוחותיה בכדי שיערכו בהתאם.

2. לאורך 70 יום מרגע פרסום החולשה התקבלו התרעות מגופי אבטחת-מידע בינל"א.
   א. במהלך 70 יום קיימים גופים אנונימיים אשר מנצלים לרעה את המצאות החולשה שלא ניתנת לזיהוי באמצעים פשוטים (כפי שקורה ברוב הארגונים).
   ב. במסגרת תקופת הזמן הזו מפרסמים כלים אוטומטיים המאפשרים את **ניצול החולשה** לצורך השתלטות\התפשטות בארגון.

3. לאחר 70 יום, ספטמבר 2019, מתגלים עקבות של ניצול החולשה ע"י קבוצת תקיפה מוכרת בקרב גופי אבטחת-מידע בין-לאומיים.
   א. **נשים לב,** נדרש יום בודד מרגע שמפרסמים כלי לניצול חולשה באינטרנט ועד לרגע שתוקפים מנצלים אותו בצורה אינטנסיבית.

4. החל מנובמבר 2019 ניתן לזהות את החולשה באמצעות הפרסומים המאפשרים את ניצול החולשה - דרך פשוטה לזיהוי יישות זדונית המנסה לנצל את החולשה.

ממאי ועד נובמבר, ניתן להבין כי מוצרי Microsoft (הנמצאים בשכיחות גבוהה בקרב ארגונים) היו חשופים לפירצה שקשה לזהות. לא כל ארגון יכול להצליח להתמודד עם חולשות שאין עבורן דרך זיהוי ברורה (שהתפרסמה בנובמבר), דבר שמשמעותו היא **שתוקף פוטנציאלי יכול לבצע פעולות מגוונות על המידע והמערכות הארגוניות.**

המאמר יתמקד בהנגשת דרך אוטומטית שתאפשר לייצר יכולת לצמצום משטחי התקיפה הזמינים דרך המערכות השונות בארגון תוך התמקדות ב-3 המטרות הבאות:

- **להגדיר פרופיל הקשחה** - אוסף הגדרות בהבטי אבטחת-מידע שיחולו על מערכת.
- **בקרה** - תמונת מצב המאפשרת לקבל חיווי לעמידה בפרופיל ההקשחה.
- **אכיפה** - החלת הקשחה על מערכת.

מבוא

בהינתן מערכת תוכנה, יש אוסף הגדרות שנדרש להגדיר מראש בכדי לאפשר צמצום של משטחי התקיפה הזמינים באמצעות המערכת. אוסף ההגדרות הנ"ל מהווה *פרופיל הקשחה* אשר ניתן להגדיר לכל מערכת בארגון.

לרוב, בכל חברה יהיה צוות אחראי על מערכת (או מקבץ מערכות) שידע לתחזק אותה.

- **איך נוכל לדעת כי הניהול נעשה תוך הקפדה על הגדרות אבטחה?**
- **איך נדע מה הם משטחי התקיפה שקיימים במערכת בצורה אוטומטית?**
- **איך נדע כיצד ניתן לצמצם משטחי תקיפה בצורה אוטומטית?**

לשם כך אתאר כלי קוד-פתוח הנתמך ע"י ארגון התקנים האמריקאי - **OpenSCAP**. בהמשך המאמר אציג את את אופן השימוש בכדי להגשים את 3 המטרות - הגדרת פרופיל הקשחה, בקרה ואכיפה.

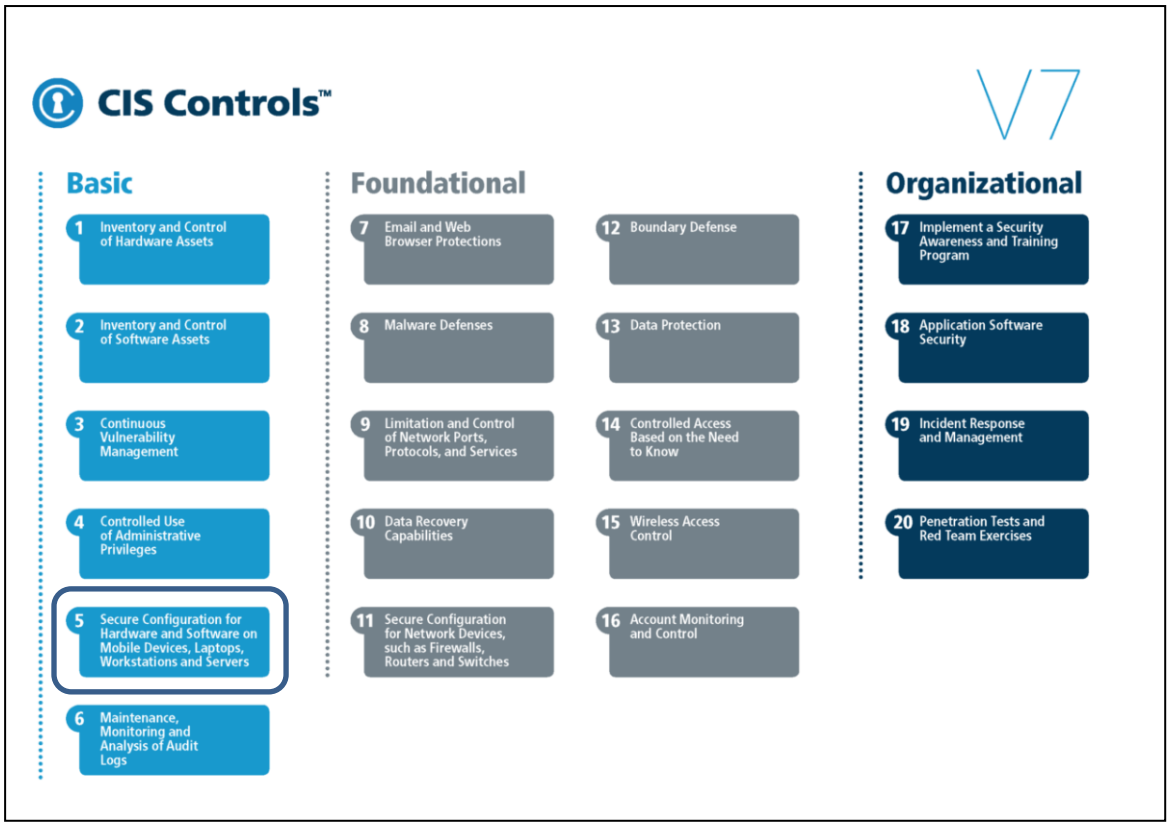
CIS - Center of Internet Security

CIS הוא ארגון בינל"א, ללא מטרות רווח, אשר שם כמטרה מרכזית להנגיש קוויים מנחים לאבטחת המידע בארגונים קטנים עד גדולים.

ארגונים שונים מגיעים לנקודת זמן בה הם מבינים (או מחוייבים) לעמוד בדרישות אבטחת מידע. אך מנגד, מתקשים לייצר תהליך מסודר בגלל מורכבות התכולות השונות: כח אדם, ידע טכנולוגי וכד'. לשם כך, הארגון, שמורכב מאנשי מקצוע מכלל התחומים הרלוונטים (אנשי IT\OT, סייבר, אבטחת מידע וכד'), יצר אוסף של תקני הקשחה עבור פלטפורמות תוכנה שונות - מערכות הפעלה, רכיבי רשת, תוכנות - בכדי להנגיש לציבור הרחב את מה שמוגדר כ-Best Practice עבור תהליכי אבטחת מידע.

ארגון CIS עוזר לאנשי הטכנולוגיה בארגון כלשהו לייצר סביבות טכנולוגיות, תוך צימצום משטחי תקיפה המהווים פתח למתקפות סייבר שונות אשר עלולות לפגוע בארגון.

בכדי להגשים את המטרה הזו הארגון הגדיר את אוסף הבקרות הנדרשות בכדי לספק מענה לכלל דרישות אבטחת המידע בארגון, מקטן ועד גדול - CIS Security Framework:



[איור 3 - אוסף בקרות אבטחת-מידע לכל סוג של ארגון]

לא נצלול במאמר זה לניתוח מעמיק של אוסף הבקרות שתקן ההקשחה מגדיר, אך ניקח כדוגמא את הבקרה המוגדרת ב-Basic CIS Control ונקראת - Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers *(ריבוע מס' 5 באיור 3)*.

ניתן להבחין כי ע"פ ארגון CIS השייכות של ארגון לקנה מידה מסויים לא משפיע על הדרישה לכך שיתבצע ניהול הגדרות אבטחת-מידע תקין.

אדגיש כי בעזרת המאמר הבא נוכל לקחת **כמעט כל תקן** הקשחה המתוחזק ע"י ארגון CIS ולהכיל אותו על תשתיות שונות בארגון. בהמשך המאמר נראה היכן נוכל למצוא את אוסף התכולות שנוכל להעזר בהן לצורכי הקשחה שונים.

משטחי התקיפה

כחלק משימוש בכלים שונים, קוד-פתוח ובתשלום, נקבל תהליך התקנה אשר יכיל הגדרות ברירת-מחדל עבור הפיצ'רים השונים המסופקים ע"י המוצרים - הגדרת תתי שירותים, משתמשים ברירת-מחדל בעלי הרשאות מנהל, סמאות, פרוטוקולים (לא מאובטחים) ושימוש בתוכנות צד שלישי, כאשר אלו מהווים משטחי תקיפה שונים על מערכות הארגון.

מוטיבציה

תהליך הגדרת אבטחת המידע עבור כלל מערכות הארגון דורש עבודה מורכבת של ישויות ארגוניות שונות וניתוח איומי סייבר מגוונים המשיקים לכל מערכות הארגון - דבר המהווה קושי עבור בניהול התהליך בארגונים.

בנוסף, ככל שמערכות מתקדמות ומתעדכנות (או נמצאים חולשות קריטיות במוצרים שונים), כך גם אותן הגדרות אבטחה. עם הזמן ועם ריבוי המערכות הארגוניות, עולה קושי בניהול שותף של אותם איומים הנובעים מכל תהליכי ההגדרה - חלק מתהליך הקשחת מערכת.

מסמך הקשחה

תחת ארגון CIS, מעבר לקווים מנחים לבקרות אבטחת-מידע, ניתן למצוא תקני הקשחה למערכות ספציפיות. אותם תקני הקשחה מכונים: "CIS Hardening Benchmarks"

תקני ההקשחה של ארגון CIS מחולקים בצורה נוחה לקטגוריות שונות, המאפשרות להבין את רמת החומרה של סעיפי הגדרה שונים. הקיטלוג נעשה בהתאם לרמת הרגישות של המערכת הנסקרת. בין תקני הקשחה שונים ניתן לראות קיטלוג מעט שונה בהתאם למטרת המערכת - לצורך ההדגמה במאמר נתמקד על תקן ההקשחה של Ubuntu 20.04.

כאשר אנחנו מתקינים מערכת מסוימת בתשתית שלנו ניתן להסיק כי רמת הרגישות של המערכת תלויה ביעוד שלה - האם היא שרת? האם היא עמדת פיתוח? האם היא עמדה 'חזקה' בעלת גישה למשאבים ארגוניים רגישים?

בכדי לענות על השאלות האלה נקבל פירוט על רמת ההחמרה המתאימה כבר במסמך ההקשחה.

אדגיש כי על מנת להקשיח ב-100% את כל סעיפי ההגדרה במערכת שלנו עלול לשבור יכולות קריטיות של מערכות שונות בארגון - ולכן חשוב לבצע את תהליך ההקשחה בצורה מחזורית ומתמשכת.

בחינת סעיפי הקשחה

בתהליך הבחינה, בוא נחליט על פרופיל הקשחה המורכב מאוסף הסעיפים שנחליט להכיל על מערכת, נוכל לראות כי כל סעיף הקשחה מכיל מידע רלוונטי ומשמעותי שיעזור לקורא להבין את המשמעויות השונות של הגדרת ההקשחה.

כל סעיף הקשחה בנוי מהחלקים הבאים:

- שם הסעיף ושיוכו המספרי:

1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)

- שיוך פרופיל לרמת החמרה:

Profile Applicability: • Level 1 - Server • Level 1 - Workstation

- פירוט על מטרת היכולת של המערכת בהקשר לסעיף:

Description: The `cramfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `cramfs` image can be used without having to first decompress the image.

- מוטיבציה בהבטי אבטחת-מידע - **הדגשה של משטח תקיפה:**

Rationale: Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

- הוראות הבדיקה לסטטוס סעיף ההקשחה במערכת הנבדקת:

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v cramfs | grep -E '(cramfs|install)'
install /bin/true
# lsmod | grep cramfs
<No output>
```

- הוראות למימוש עבור סעיף ההקשחה - הכלתו בפועל על המערכת הנבדקת:

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vim /etc/modprobe.d/cramfs.conf`
and add the following line:

```
install cramfs /bin/true
```

Run the following command to unload the `cramfs` module:

```
# rmmod cramfs
```

- שיוך מנגנון בקרה המוגדר ב-CIS Security Framework:

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

בצורה טבעית, נוכל להניח כי קיימים סעיפים אשר לא יתאימו להכלה בארגון שלנו. לכן, נרצה לבצע **ניטור** עבור משטחי התקיפה שהשארנו במערכות השונות.

בפרק הנ"ל הוצג אמצעי חינמי הזמין לכולם (CIS Benchmarks) אשר באמצעותו נוכל לקבל תקני הקשחה למס' מערכות, רכיבים ותוכנות. תקני ההקשחה השונים הוגדרו ע"י מומחים מתחומי עולמות הטכנולוגיה, במטרה לעזור לקהילה הבינל"א לפתח ולהקים מערכות ותשתיות בצורה מאובטחת.

תקני ההקשחה מאפשרים לנו להבין מה הם **משטחי התקיפה הפוטנציאלים** במערכות שלנו. בו בזמן, הם מאפשרים לנו לנתח את האיומים השונים בכדי להגיע להחלטה רלוונטית - זו תאפשר להעצים את רמת החוסן של מערכות הארגון.

NIST - National Institute of Standards and Technology

ארגון פדרלי-אמריקאי שמטרתו היא לפתח ולקדם דרכים שונות למדידה, יצירת סטנדרטים, שימוש בטכנולוגיות - במטרה לשפר את איכות החיים בעולם טכנולוגי.

NIST Cybersecurity Framework (NIST CSF)

כחלק מתהליכי יצירת סטנדרטים בעולם הטכנולוגי קם הצורך בקידום יכולות הגנה במרחב הקיברנטי (האינטרנט) כסטנדרט אמריקאי **שיחייב** את כלל המוסדות השונים הקיימים בארה"ב.

הסטנדרט שהוגדר תחת NIST CSF (אחד מתתי הגופים האמון על סטנדרטים בהקשרי סייבר) מגדיר כיצד יש לנהל ולהפחית את משטחי התקיפה במערכות תשתית טכנולוגית בארגון (בדומה ל-CIS) - וזאת בכדי ליצור קו אחיד לאופן **המניעה, הגילוי והתגובה** במקרה של ארועי סייבר. כמוכן, הארגון דואג לאכוף את תקן האבטחה תחת מוסדרות\ארגונים הכפופים ברחבי ארה"ב.

ארגון NIST CSF לקח על עצמו כמטרה ליצור כלי קוד-פתוח, אשר יהווה יכולת הנגשה של יכולות אבטחה וסדנטרטים שונים (למשל CIS עליו אנו מתמקדים במאמר זה) בצורה אוטומטית. כחלק מאותו כלי קוד-פתוח יצרו פרוטוקול חדש המיועד להנגשת סטנדרטים חדשים בשם SCAP - Security Content Automation Protocol. הפרוטוקול והכלי מתוחזק ע"י ארגון NIST ומשלב שימוש בפרויקטי קוד-פתוח המאפשרים יישום ואכיפה של סטנדרטים שונים.

NIST Repository

מסד-נתונים המוגדר כ-NCP - National Checlist Program. NCP מתוחזק ומוגדר ע"י ארגון NIST במטרה להוות מאגר של הכוונות בנושאי אבטחת-מידע. הכוונות ברמה מפורטת ומודרכת להגשת הגדרה מאובטחת של מערכות הפעלה ותוכנות בארגון.

ההכוונות המתוחזקות במאגר מסופקות בפורמטים אשר ניתנים לשימוש בהתאם לפרוטוקול SCAP.

קישור לאתר הרישמי של NCP

OpenSCAP

הכלי OpenSCAP הינו כלי קוד-פתוח המפותח ומתוחזק ע"י ארגון NIST העולמי. הכלי נועד בכדי לספק אוטומציה לכל הנוגע להבטי אבטחת-מידע במערכות שונות). המוצר מורכב ממס' כלי קוד-פתוח המיועדים בסופו של דבר להגשמת 2 מטרות: **בקרה ואכיפה של תקני הקשחה.** קיימות יכולות נוספות, כדוגמאת סריקת חולשות, אשר לא יתוארו ברמת המאמר הנ"ל.

באמצעות היכולות של המוצר ניתן לאפשר למנהלים\מבקרים לוודא את עמידת המערכות בארגון בתקני הקשחה שונים - ולא רק CIS Benchmark. לא אתאר תקני הקשחה נוספים - המגדירים אותן הגדרות אך מגדירים רמת חשיבות\החמרה בצורה שונה.

ניתן להבחין כי היתרון המובהק של המוצר מאפשר לנו לנהל את אבטחת המידע בקרב המערכות שלנו בעלות מינימאלית - אין צורך בתכולות מורכבות (כ"א יעודי והסמכות מיקצועיות) בארגון בכדי לאפשר בקרה\אכיפה.

SCAP Base

רכיב הבסיס של כלי ה-OpenSCAP אשר מאפשר, כספרייה או דרך Command-Line, לבצע סקירת תקן-הקשחה הנתמך ב-SCAP Standard.

SCAP Standard הוא אוסף הפורמטים השונים שניתן לספק לכלי כקלט בכדי לאפשר לו לבצע סריקה המתאימה לתוכן הקלט. למשל, אם נבחר להשתמש בקובץ XCCDF המספק את כלל סעיפי ההקשחה עבור מערכת מסויימת - נוכל לבצע סריקה באמצעות הכלי ולקבל פלט לעמידת המערכת בתקן ההקשחה.

חלק מהפורמטים הנתמכים:

- Extensible Configuration Checklist Description Format - XCCDF - קובץ המגדיר בצורה מפורשת את אוסף הסעיפים הנדרשים לבדיקה על מערכת מסוימת. לרוב, בהקשר של OpenSCAP יכיל הגדרות אבטחה בהתאם לתקן ההקשחה שנבחר.
- Open Vulnerability and Assessment Language - OVAL - קובץ המגדיר בצורה מפורשת את המצב הרצוי בהבטי אבטחת-מידע. מטרתו להכיל תיאור למציאת חולשות או מצב רצוי להגדרות במערכת. בניגוד ל-XCCDF מיועד למציאת חולשות ולא צמוד לתקן הקשחה.

SCAP Workbench

כלי המאפשר להשתמש ב-OpenSCAP בצורה גרפית הנוחה למשתמש הממוצע. הכלי מאפשר לעבוד בצורה גרפית בכדי לבצע את היכולות הנתנות באמצעות שימוש בספרייה SCAP Base. באמצעות הכלי נראה כיצד נוכל להגדיר פרופיל הקשחה מותאם לצרכי הארגון שלנו.

SCAP Security Guide

פוליסות אבטחה המהוות קבצי קלט בהתאם לפרוטוקול SCAP. הפוליסות מכסות מגוון רחב של הגדרות אבטחת-מידע המבטיחות שימוש Best Practice נכון במערכות השונות.

באמצעות הפוליסות ניתן לוודא עמידה של מערכות בתקנים שונים: PCI DSS, STIG ו-USGCB. במידה וקיימת דרישה לעמידת אחת המערכות הארגוניות בתקן הנתמך ב-SCAP נוכל בצורה קלה עמידה בדרישותיו.

החלק של SCAP Security Guide והנגשתו ככלי קוד-פתוח מאפשרת לארגונים שונים לתרום ממאמציהם בכדי לאפשר עמידה של מערכות שונות בתקן סטנדרטי, החל מתעשיות מודיעין וצבא, בריאות, תקשורת וכד'.

ניתן להוריד את הגרסא האחרונה עם כלל הפוליסות מאתר ה-GitHub של הכלי - כאן. אשתמש בהדגמה בפרופיל ההקשחה עבור Ubuntu 18.04 ואתאר את התקנים השונים הנתמכים בפרופיל.

Ansible

כלי OpenSource אשר ב-2015 אומץ ע"י RedHat (אשר ממשיכה לתרום לגרסאתו החינמית), משמש כמנהל הגדרות מרכזי העובד ללא התקנות של סוכנים במערכות שונות.

הכלי מאפשר, בהינתן Python במשאב המנוהל וגישת SSH, לייצר אוטומציות שונות ולהריצן על משאבי ארגון שונים. המטרה העיקרית היא לייצר רמה אחידה של אוטומציה בין סביבות שונות המנוהלות באמצעות הכלי. הכלי מאוד נח ללמידה ומבוסס על קבצי YAML, המכונים Playbooks, הקלים להבנה ושינוי בהתאם לדרישות. הרצתם מאפשר את שינוי הגדרות המכונה בהתאם להוראות ה-Playbook.

אוטומציית תהליך הקשחה

תהליך ההקשחה בנוי משלושה שלבים כפי שתואר בתחילת המאמר:

- הגדרת פרופיל הקשחה
- בקרה
- אכיפה

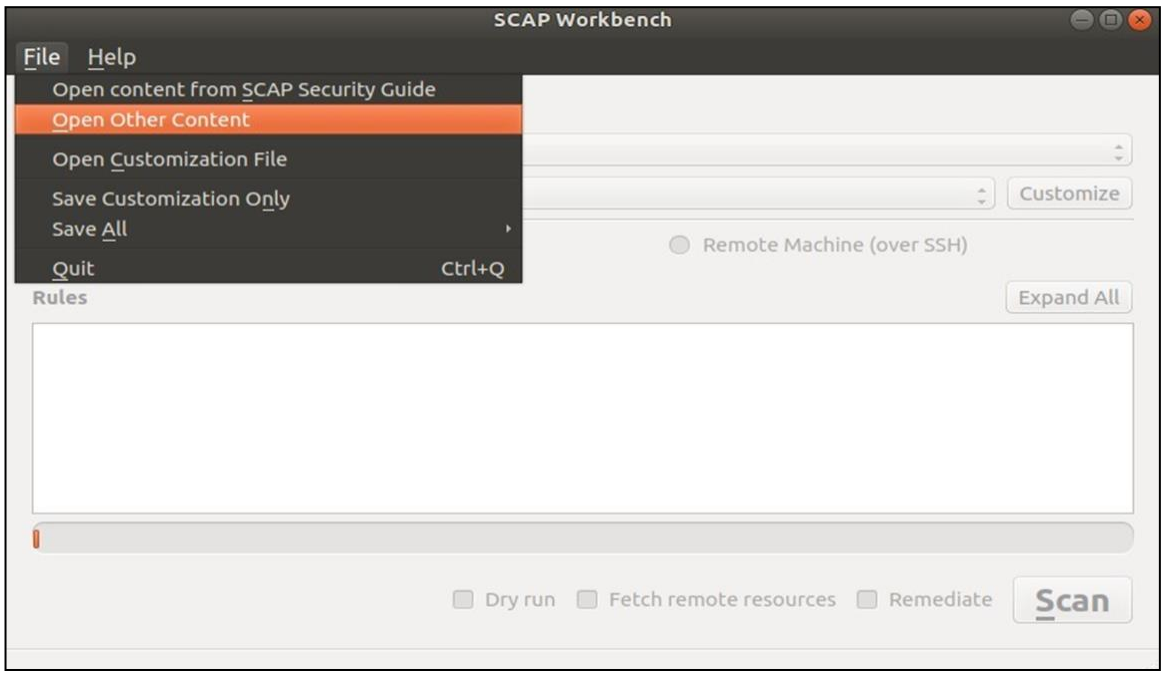
בחלקים הבאים נלמד כיצד לבצע את השלבים בצורה אוטומטית באמצעות OpenSCAP.

הגדרת פרופיל הקשחה

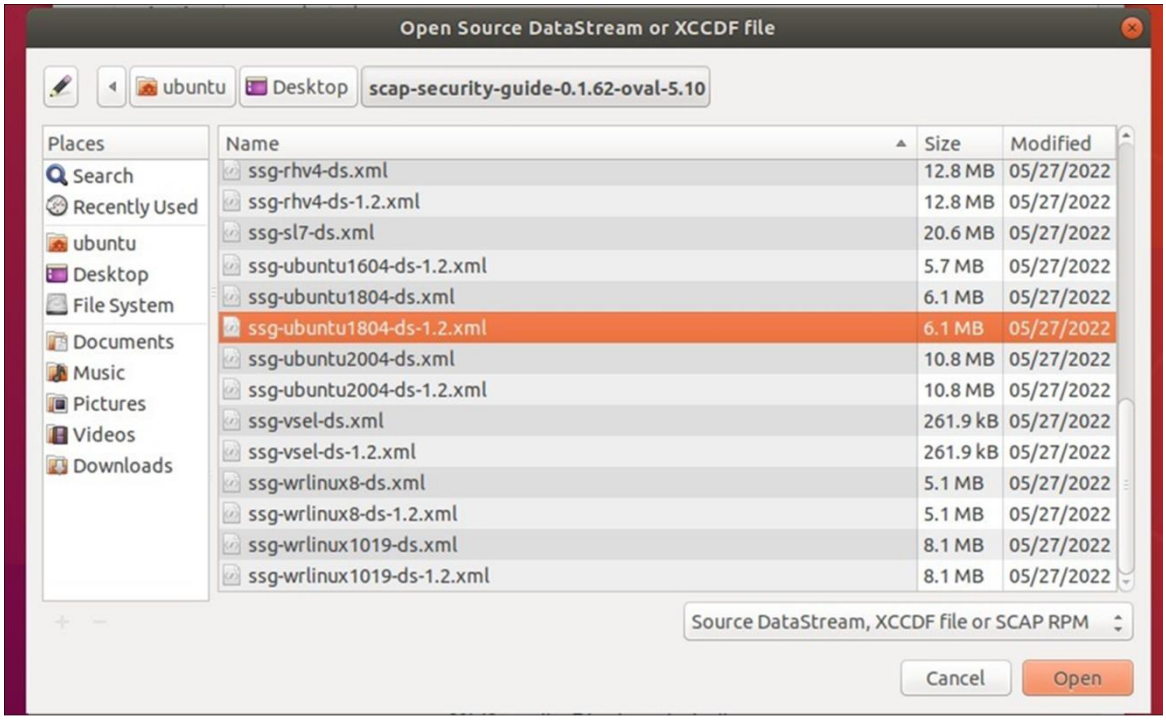
פרופיל הקשחה, כפי שהכרנו, מהווה אוסף הגדרות אותו נרצה להכיל בהתאם לתקן הקשחה שסקרנו. אחר שנוריד את SCAP Security Guide נוכל לראות את מגוון הפרופילים הזמינים לנו כקבצי XCCDF:

```
root@ubuntu1804:/home/ubuntu/Desktop/scap-security-guide-0.1.62-oval-5.10# ls
ansible                 ssg-centos8-ds-1.2.xml    ssg-debian11-ds.xml     ssg-fuse6-ds-1.2.xml
bash                    ssg-centos8-ds.xml        ssg-debian9-ds-1.2.xml  ssg-fuse6-ds.xml
Contributors.md         ssg-chromium-ds-1.2.xml   ssg-debian9-ds.xml      ssg-jre-ds-1.2.xml
guides                  ssg-chromium-ds.xml       ssg-eks-ds-1.2.xml      ssg-jre-ds.xml
kickstart               ssg-cs9-ds-1.2.xml        ssg-eks-ds.xml          ssg-macos1015-ds-1.2.xml
LICENSE                 ssg-cs9-ds.xml            ssg-fedora-ds-1.2.xml   ssg-macos1015-ds.xml
README.md               ssg-debian10-ds-1.2.xml   ssg-fedora-ds.xml       ssg-ocp4-ds-1.2.xml
ssg-centos7-ds-1.2.xml  ssg-debian10-ds.xml       ssg-firefox-ds-1.2.xml  ssg-ocp4-ds.xml
ssg-centos7-ds.xml      ssg-debian11-ds-1.2.xml   ssg-firefox-ds.xml      ssg-ol7-ds-1.2.xml
```

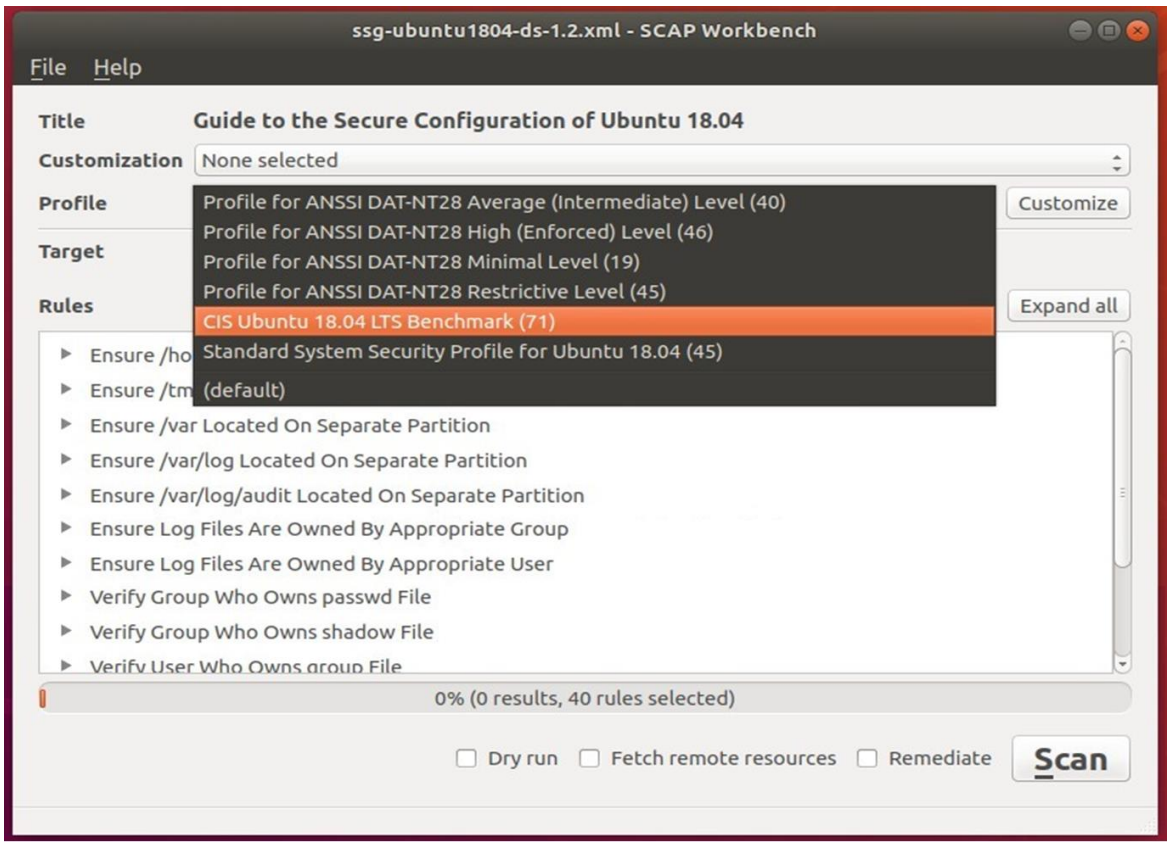
נטען את הפרופיל דרך SCAP Workbench:

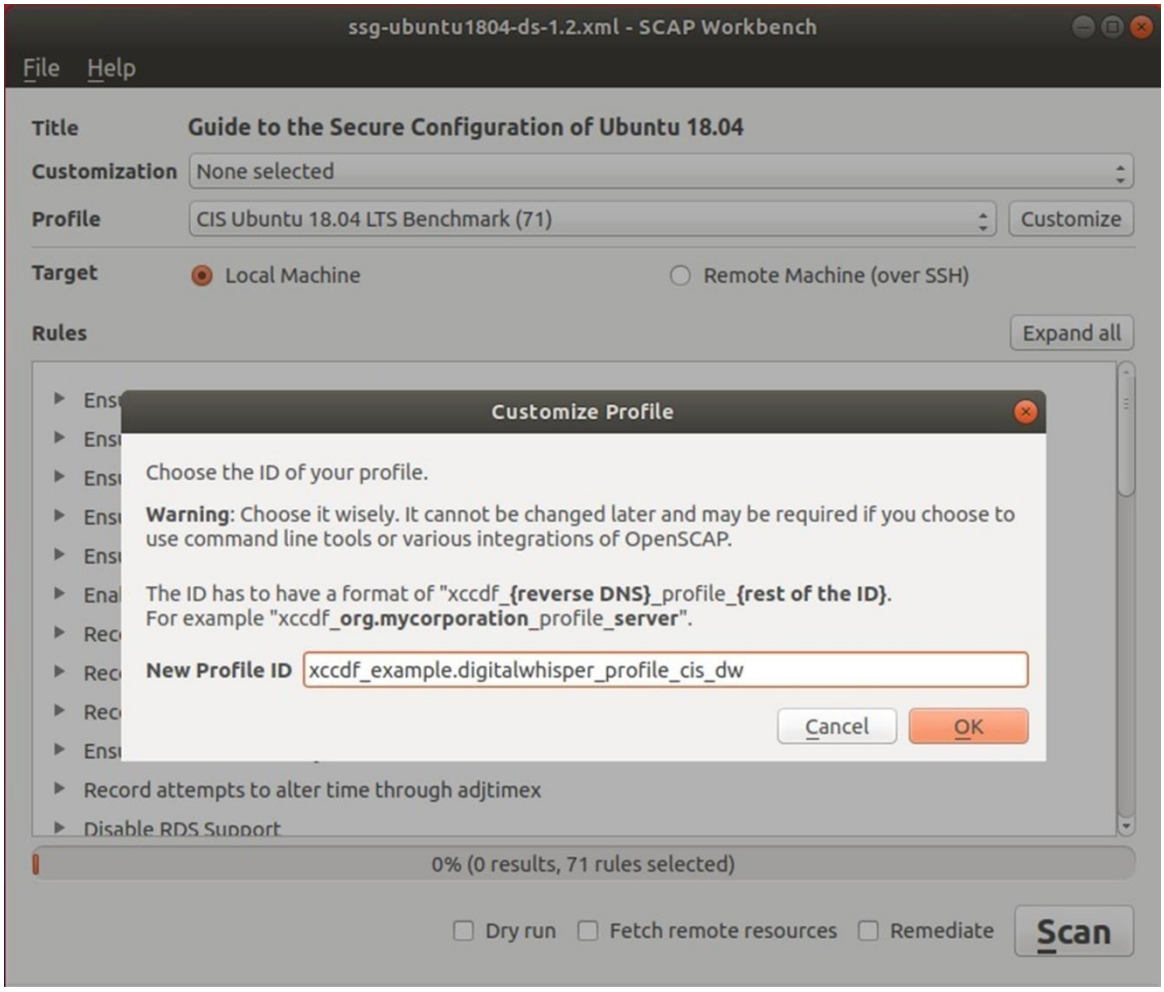


נבחר בגרסא אותה נרצה להגדיר (במאמר זה אני אתמקד ב-ubuntu18.04):

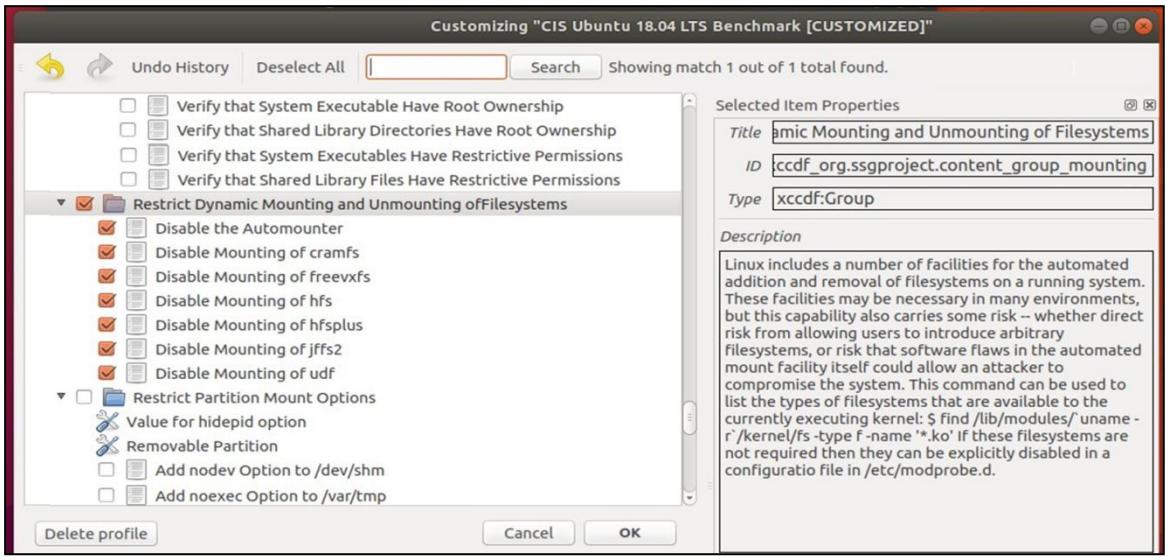


נגדיר פרופיל המתאים לתקן ההקשחה שאיפיינו עבור מערכות הארגון שלנו (בהתאם לתקן CIS):



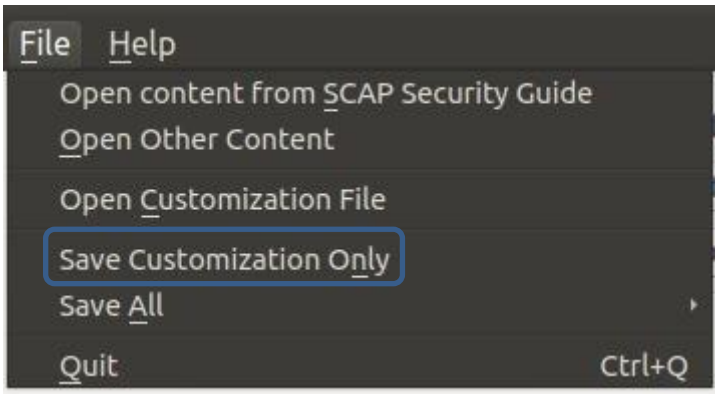


לצורך ההדגמה אפעיל הקשחה של תמיכה במערכות קבצים נוספות:

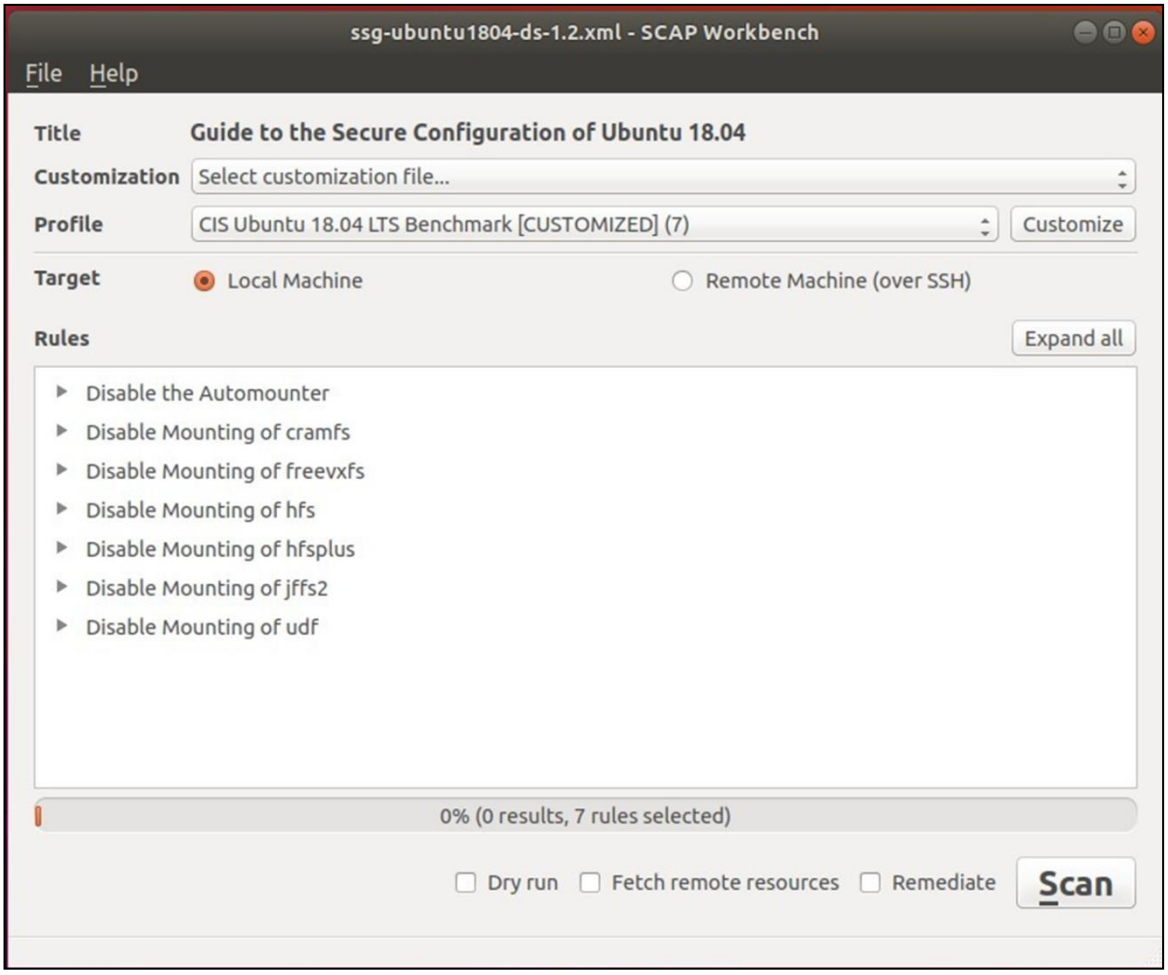


נוכל ללחוץ על כפתור Customize בכדי ליצור פרופיל מותאם עבור הפרופיל של CIS Ubuntu 18.04 LTS.

נשמור את הפרופיל המותאם שיצרנו:

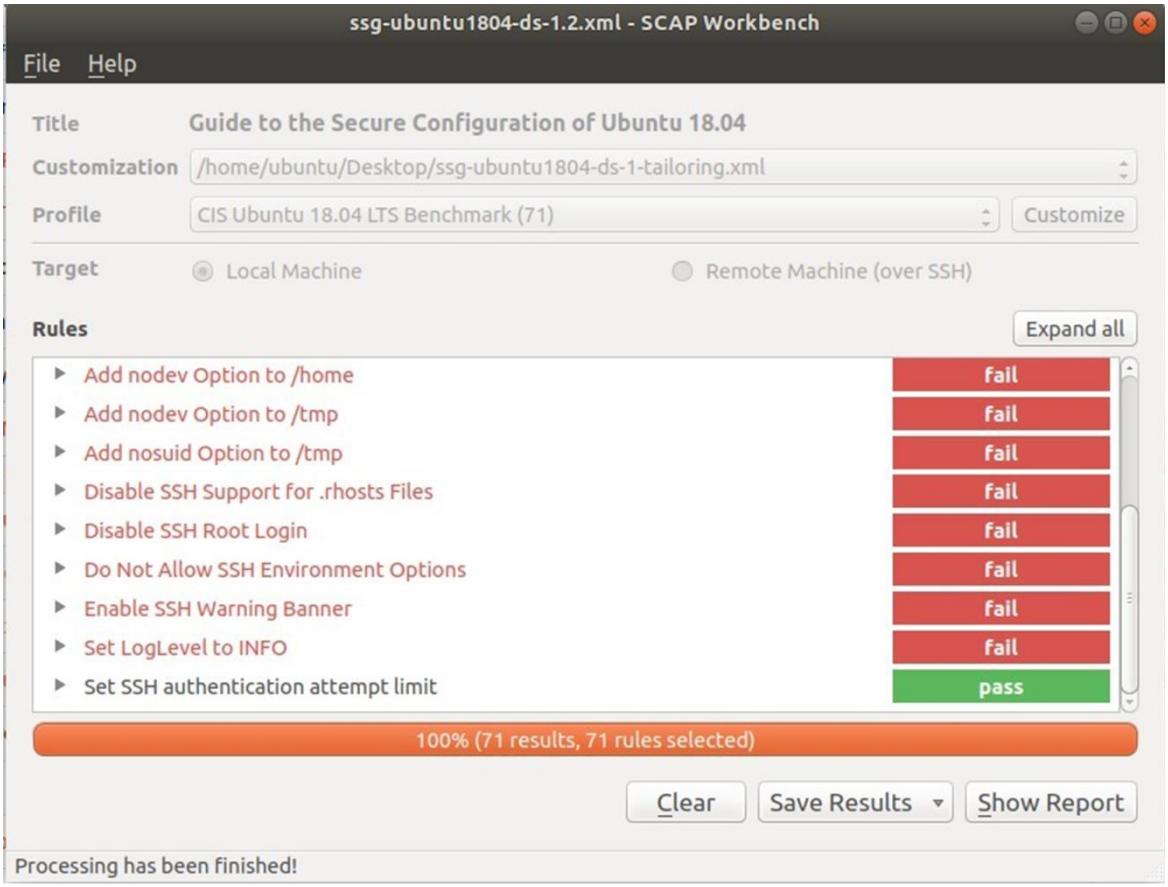


נטען אותה מהקובץ ששמרנו (יש לשים לב שהפרופיל המקורי צריך להיות טעון לפני שטוענים את הפרופיל המותאם שלנו). ונגיע למסך הבא:



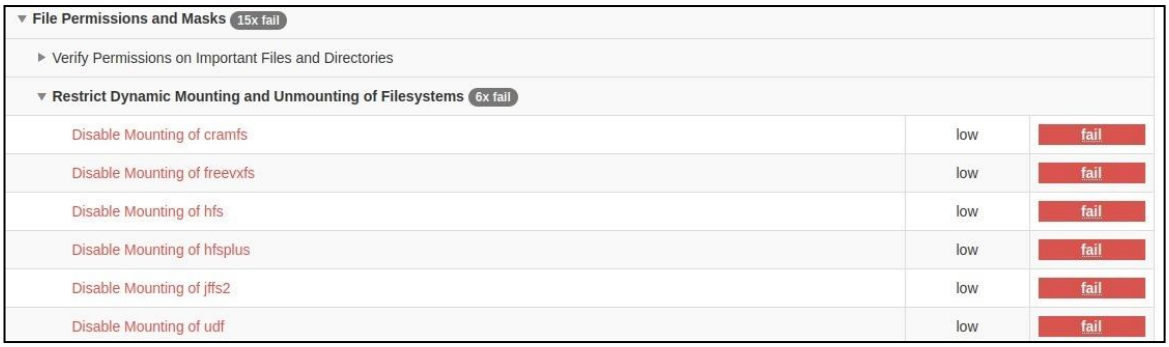
בקרה

לאחר לחיצה על כפתור SCAN במצב בו סורקים "Local Machine" נוכל לקבל בקרה על איכות ההקשחה הנוכחית של המערכת. בהתאם לפוליסת CIS שהגיע ברירת-מחדל עם SCAP Security Guide נוכל לראות את המידע הבא:



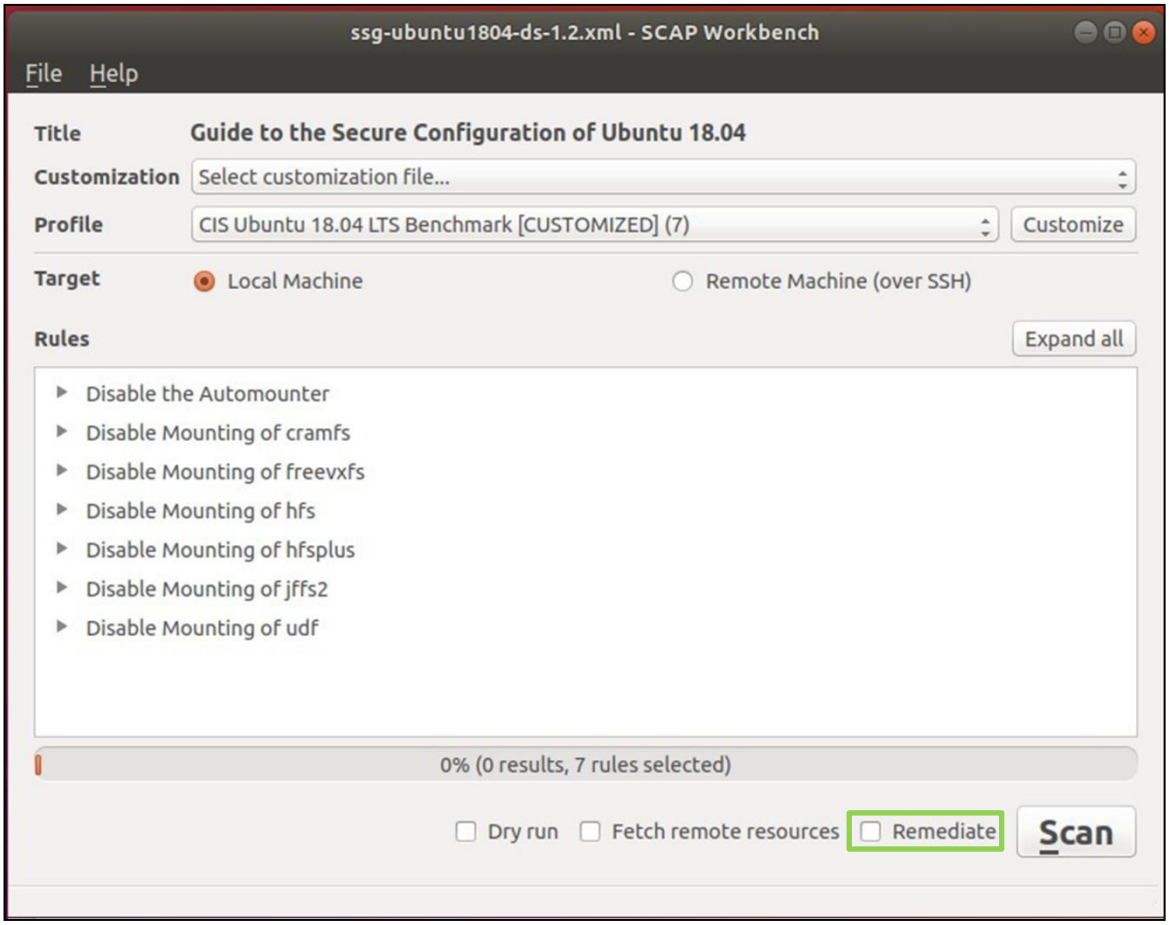
במידה ונסתכל על סיכום הסריקה ("Show Report") נראה שברירת המחדל שלנו עומדת על ~10% הקשחה:

במידה ונבחן את התוצאות נוכל לראות כי ברירת-מחדל של ubuntu18.04 לא מקשיחה את השימוש במסוגי מחיצות:



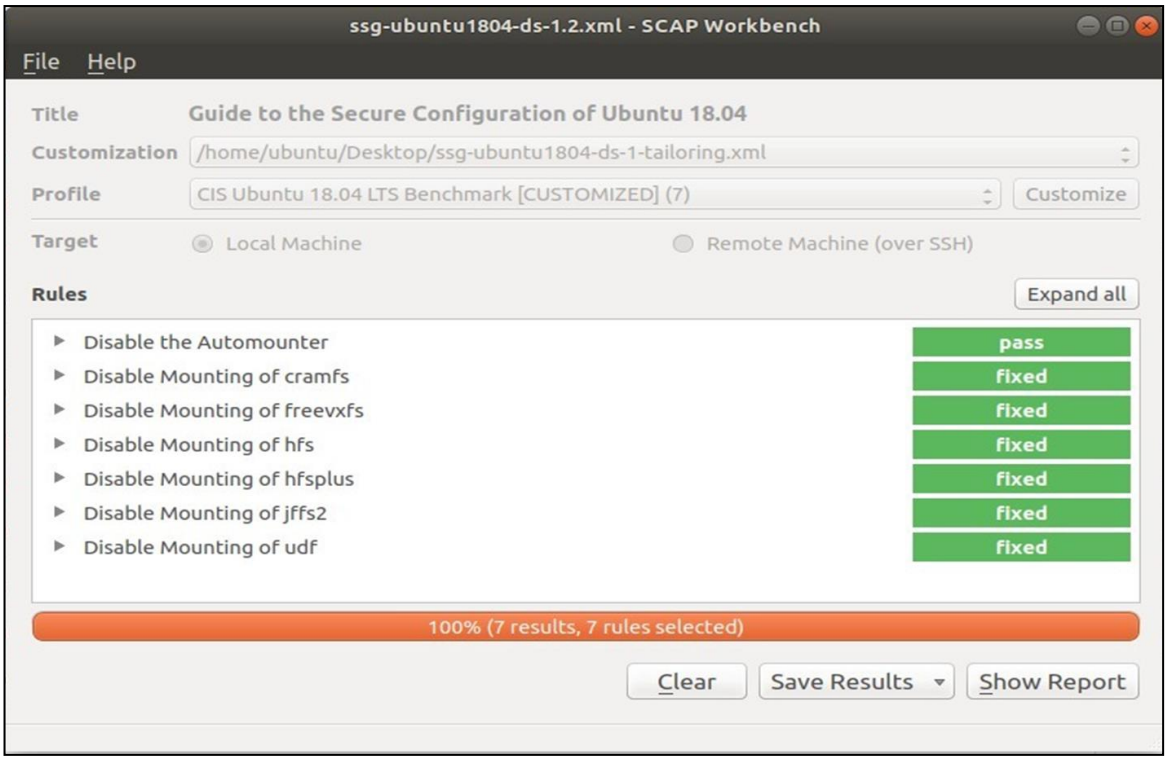
אכיפה

בכדי לבצע אכיפה לעמידה בפרופיל המותאם שיצרנו נבצע שימוש ביכולות "Remediate" של SCAP Workbench - ונריץ (לחיצה על "Scan"):

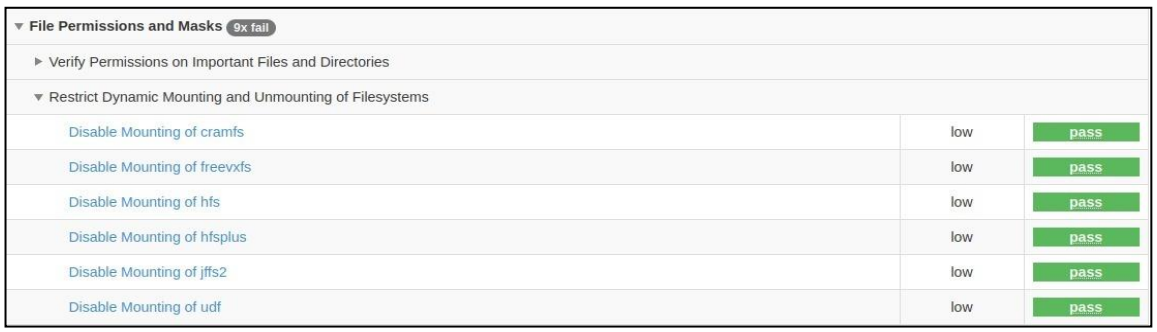


כשנשתמש ביכולת Remediate נוכל לבצע הקשחה של העמדה עלייה אנו עובדים (ה-"Local Machine").

נוכל לראות בסיכום שיוצג לנו כי השינויים התבצעו:



כעת, נבחן שוב את סיכום הסריקה אל מול פוליסת ברירת-מחדל שיש לנו מ-SCAP Security Guide. ניתן לראות כי פרופיל ההקשחה עלה ל-~14%:



תהליך ההקשחה האוטומטי

בחלק האחרון למדנו כיצד ניתן להשתמש ב-SCAP Workbench בכדי לבצע הקשחה אוטומטית לעמדה ישירות ממשק המשתמש. במקרים אחרים, נרצה לייצר Ansible playbook אשר אותו נוכל להריץ בסביבה לא נגישה ל-Workbench SCAN. לשם כך, נוכל להשתמש בפקודה הבאה:

```
oscap xccdf generate fix --profile xccdf_dw_example.org_profile_cis_ubuntu1804_template --fix-type ansible --tailoring-file ./ssg-ubuntu1804-ds-1-tailoring.xml ./ssg-ubuntu1804-ds-1.2.xml > output.yml
```

- --profile: מגדיר את שם הפרופיל שהוגדר ב-Customization.
- --fix-type: מאפשר להגדיר את סוג הקובץ שנקבל (תומך גם ב-Bash).
- --tailoring-file: שם הקובץ שהגדרנו כ-Customization.
- ssg-ubuntu1804-ds-1.2.xml: שם הקובץ פרופיל המקורי שטענו (וממנו יצרנו את ה-Customization File).
- output.yml: שם הקובץ אשר יכיל את תוכן ה-playbook שנריץ עם Ansible על התשתיות שלנו.

באמצעות הפלט - Playbook - נוכל להריץ דרך שרת Ansible את פרופיל ההקשחה שנרצה להכיל על מערכות הארגון השונות (Generate Ansible Playbooks).

סיכום

תהליך הקשחה למערכת דורש מאנשי טכנולוגיה להכיר את אוסף ההגדרות אשר מהוות תקן אבטחת-מידע עבור המערכת. באמצעות עמידה בתקן ההקשחה נוכל להבטיח כי תוקף, אשר עלול להשיג שליטה על משאבי הארגון, יחווה קושי בהתקדמות מטרותיות הזדוניות בזכות תהליך צמצום משטחי התקיפה אותו הוא יוכל לנצל.

במאמר הכרנו דרך בה נוכל לצמצם את משטחי התקיפה במערכות הארגון בצורה אוטומטית אשר תאפשר לנו להגדיר פרופיל הקשחה, יכולת בקרה ויכולת אכיפה עבור הופליסה שיצרנו. בנוסף, למדנו כיצד נוכל לייצר Ansible Playbook אשר יאפשר לנו לבצע את אוטומציית ההקשחה על משאבי הארגון הנגישים לאוטומציה דרכו.

על המחבר

בעל תואר ראשון בהנדסת תכנה, עוסק כמהנדס פתרונות אבטחה. בנוסף, עוסק בהוראה ופיתוח תוכן בעולמות הסייבר והטכנולוגיה.