Certificates & Certifications

מתן חיים סנדורי

כתב ויתור:

הפרויקטים המוצגים במסמך זה הינם קנייניים ועוצבו ופותחו על ידי מתן סנדורי. פרויקטים אלה אינם מיועדים לשכפול, רווח או שימוש אישי על ידי צד שלישי כלשהו. כל הפצה, הצגה או שכפול בלתי מורשית של פרויקטים אלה אסורים בהחלט. לבירורים או אם ברצונכם לראות את קוד המקור המלא, אנא פנו ישירות למתן סנדורי.

פרטי יצירת קשר:

שם מלא: מתן חיים סנדורי.

דוא"ל: Matans806@gmail.com

מספר טלפון: 052-658-2600

תעודת Tensorflow

השגתי ציון של 24/25 (96%) בבחינת ההסמכה של TensorFlow. מבחן אינטנסיבי זה בן 5 שעות, מאורגן על ידי גוגל, מעריך את היכולת של האדם לתכנן ולהטמיע רשתות עצביות ואלגוריתמי למידה עמוקה באמצעות חבילת TensorFlow. הציון משקף את מיומנותי במינוף היכולות של TensorFlow למיצוי הפוטנציאל שלה. גלה עוד על הסמכת TensorFlow כאן או בדוק את ספריית האישורים של Google.

פרויקטים שנבנו באמצעות Tensorflow:

- Google Drive
- GitHub

אמת תעודה זו.

תעודת PCAP


PYTHON INSTITUTE
OpenEDG | OPEN EDUCATION AND DEVELOPMENT GROUP

Verify this certificate's authenticity at
verify.openedg.org:
myQ2.dYNm.LpJn

CERTIFICATE

Exam Code: PCAP-31-03

Date Certified: September 7, 2023

Scope:

- Modules and Packages (12%)
- Exceptions (14%)
- Strings (18%)
- Object-Oriented Programming (34%)
- Miscellaneous (List Comprehensions, Lambdas, Closures, and I/O Operations) (22%)

of proficiency in the
Python programming language

Matan Haim Sandori

PCAP – Certified Associate in Python Programming
(Exam PCAP-31-0x)

Christopher Boguslawski
President, Python Institute

PCAP – Certified Associate in Python Programming
OpenEDG Python Institute

השגתי ציון 88/100 בבחינת PCAP-31-03 ממכון Python. הבדיקה כוללת חמישה חלקים המשתרעים על מודולים, טיפול בשגיאות, פעולות מחרוזות, תכנות מונחה עצמים וטכניקות מתקדמות כמו פונקציות lambda ופעולות I/O. הסמכה זו מדגישה את עומק הידע שלי ב-Python, ומשקפת מיומנות במושגי Python בסיסיים וגם מורכבים. בקר באתר האינטרנט של מכון Python.

פרויקטים שנבנו באמצעות Python:

- Google Drive
- GitHub

פרויקטים שנבנו באמצעות Tensorflow:

- Google Drive
- GitHub

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל

עברתי בהצלחה את תוכנית Google Cybersecurity Professional Certificate עם ציון ממוצע של 90.5%, בפרק זמן מרוכז של 5 ימים. תוכנית קפדנית זו, שנבנתה על ידי Google, תוכננה בקפידה כדי לספק לאנשים מיומנויות מוכנות לעבודה החיוניות לקריירה משגשגת בתחום אבטחת הסייבר.

תכנית הלימודים כוללת חקירה מקיפה של תחומים קריטיים כמו זיהוי סיכונים, איומים ופגיעות נפוצים, לצד טכניקות יעילות לצמצום. עם התמקדות ייעודית בהכנת שואפים לאתגרים בעולם האמיתי כאנליסטים של אבטחת סייבר, הקורס מאפשר הבנה חזקה של תחום הצמיחה הגבוה של אבטחת סייבר, ומאפשר ללמוד בקצב מואץ ולהיות מוכן לעבודה תוך פחות מחצי שנה. קרא עוד ב-Grow with Google.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

TryHackMe: Jr Penetration Tester

אני גאה שסיימתי בהצלחה את הסמכת TryHackMe: Jr Penetration Tester, המשקפת בסיס איתן במיומנויות הליבה הטכניות החיוניות לקריירה מתחילה בבדיקות חדירה. תוכנית מעמיקה זו ציידה אותי בידע המעשי הדרוש לביצוע הערכות אבטחה נגד יישומי ומערכות אינטרנט, שליטה בזיהוי והפחתה של פגיעויות בתשתית דיגיטלית.

מסלול הלמידה חזק, וכולל היבטים מרכזיים של בדיקות חדירה כגון ספירה, ניצול ודיווח. הוא גם מספק תרגילי פריצה מציאותיים שלא רק חידדו את החוש הטכני שלי אלא גם העשירו את ההבנה שלי בכלי האבטחה הרווחים בתעשייה. המעבדות האינטראקטיביות והמשחקיות בעולם האמיתי שהנחתה TryHackMe הגדילו משמעותית את היכולת שלי ליישם את הידע שנרכש באופן מעשי, והכינו אותי עוד יותר לקריירה פורייה כבוחן חדירה. קרא עוד ב-TryHackMe.

אמת תעודה זו.

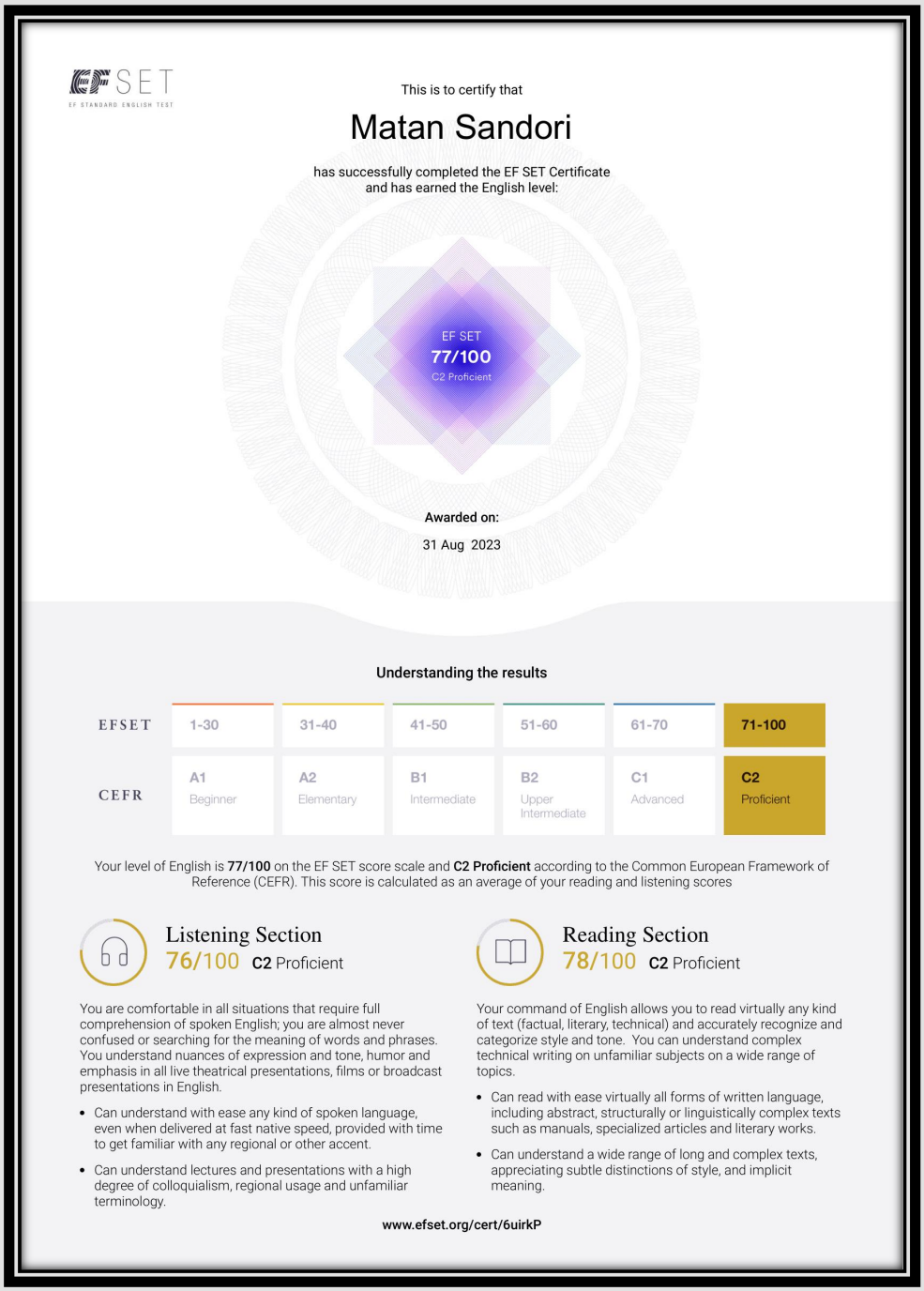
TryHackMe: Red Teaming certificate

השגתי בהצלחה את תעודת TryHackMe: Red Teaming, תוכנית שתוכננה בקפידה להקנות את הידע והמיומנויות הדרושים כדי לחקות התקפות יריב פוטנציאליות בסביבות מורכבות. שלא כמו בדיקות חדירה מסורתיות, מסלול זה מעמיק יותר בניהול התקשרויות מוצלחות של הצוות האדום כדי לאתגר ולשפר בקפדנות את יכולות ההגנה של לקוחות.

ההכשרה המקיפה הניתנת באמצעות תעודה זו מקיפה מספר רב של תחומים קריטיים לרבות ניצול של טכניקות מגוונות לגישה ראשונית, ספירה, התמדה על מטרות, התחמקות מפתרונות אבטחה וניצול של Active Directory. על ידי עיסוק בהדרכה מעשית בנושא אבטחת סייבר, חידדתי את היכולת שלי לחשוב ולפעול בדומה להאקרים מהעולם האמיתי, ובכך לזהות במיומנות את פערי האבטחה ולתכנן אסטרטגיות להפחתת סיכונים. גישה פרגמטית זו ללמידה חיזקה באופן משמעותי את היכולת שלי לאסוף, לנתח ולקבל החלטות מונעות נתונים כדי להגביר את אמצעי האבטחה הארגוניים. קרא עוד ב-TryHackMe.

אמת תעודה זו.

תעודת EF SET



EF SET
EF STANDARD ENGLISH TEST

This is to certify that

Matan Sandori

has successfully completed the EF SET Certificate
and has earned the English level:

EF SET
77/100
C2 Proficient

Awarded on:
31 Aug 2023

Understanding the results

EFSET	1-30	31-40	41-50	51-60	61-70	71-100
CEFR	A1 Beginner	A2 Elementary	B1 Intermediate	B2 Upper Intermediate	C1 Advanced	C2 Proficient

Your level of English is **77/100** on the EF SET score scale and **C2 Proficient** according to the Common European Framework of Reference (CEFR). This score is calculated as an average of your reading and listening scores

Listening Section
76/100 **C2** Proficient

You are comfortable in all situations that require full comprehension of spoken English; you are almost never confused or searching for the meaning of words and phrases. You understand nuances of expression and tone, humor and emphasis in all live theatrical presentations, films or broadcast presentations in English.

- Can understand with ease any kind of spoken language, even when delivered at fast native speed, provided with time to get familiar with any regional or other accent.
- Can understand lectures and presentations with a high degree of colloquialism, regional usage and unfamiliar terminology.

Reading Section
78/100 **C2** Proficient

Your command of English allows you to read virtually any kind of text (factual, literary, technical) and accurately recognize and categorize style and tone. You can understand complex technical writing on unfamiliar subjects on a wide range of topics.

- Can read with ease virtually all forms of written language, including abstract, structurally or linguistically complex texts such as manuals, specialized articles and literary works.
- Can understand a wide range of long and complex texts, appreciating subtle distinctions of style, and implicit meaning.

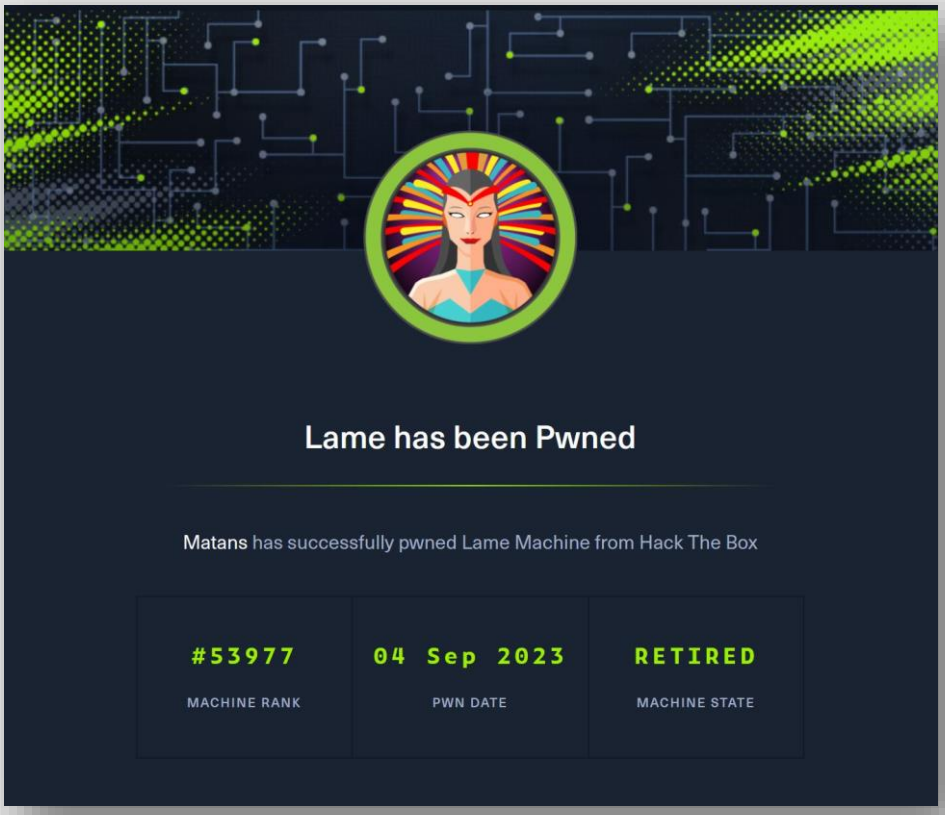
www.efset.org/cert/6uirkP

השגתי ציון של 77/100 בבחינה המאתגרת באנגלית EF SET, מה שמציב אותי בקטגוריית הבקיאות הגבוהה ביותר. השליטה שלי בשפה האנגלית לא באה לידי ביטוי רק בציוני המבחנים אלא גם בחיי היומיום שלי שבהם אני קורא, צופה, לומד וכותב בעיקר באנגלית. מיומנות זו מבטיחה תקשורת והבנה ברורה, במיוחד בעת טיפול בתיעוד Python, קורסים ואינטראקציות. למידע נוסף על בדיקת EF SET כאן.

אמת תעודה זו.

Hack The Box: Lame

הישג הסמכה



פרטי מכונה:

- קושי: קל
- קישור: https://www.hackthebox.com/achievement/machine/1636210/1

איך פרצתי:

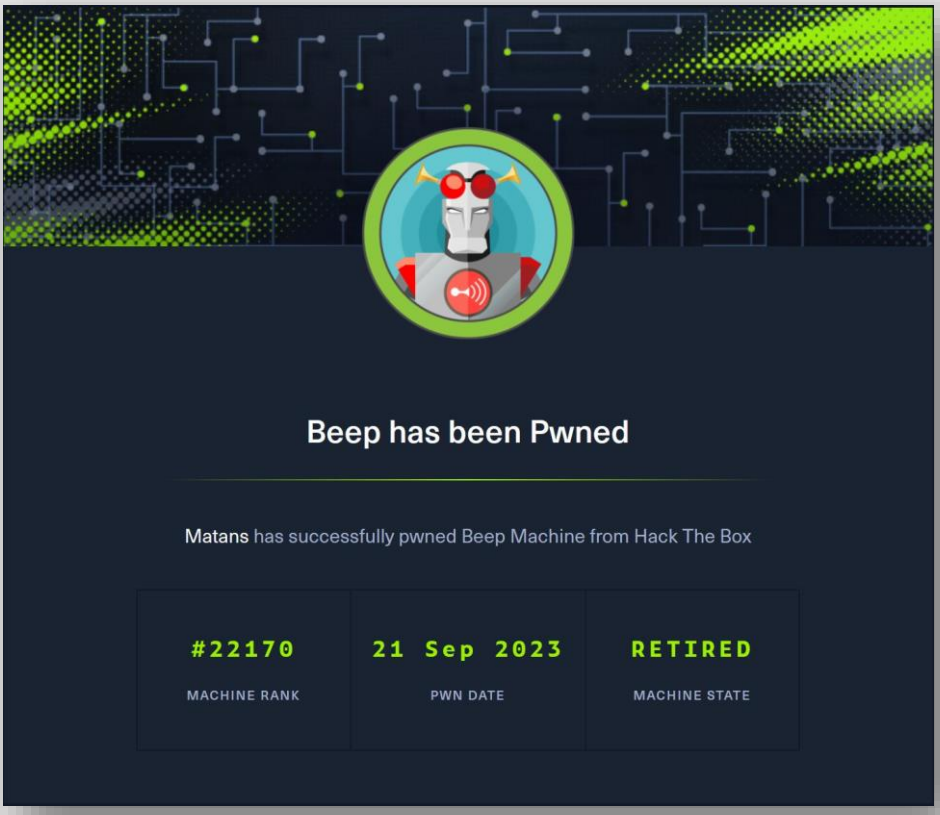
- גישה ראשונית: במהלך שלב הבדיקה הראשוני, חשפתי ניצול פוטנציאלי של הדלת האחורית. למרות שהניסיון שלי סוכל על ידי חומת האש, ההתמדה הובילה אותי לשדרה אחרת: ניצול בתוך בלוק ההודעות של השרת (SMB). ביצוע מוצלח של פגיעות זו העניק לי מעטפת. מחקר נוסף חשף ניצול של Distcc, המציג הזדמנות למעטפת נוספת.
- הסלמה של הרשאות: בניווט במערכת כמשתמש מוגבל, זיהיתי הרשאות שגויות בהגדרות שאפשרו ביצוע של פקודות sudo nmap ו-sudo find, מה שהוביל להסלמה של הרשאות. במאמץ נפרד, התגלה פגם במחולל המספרים הפסאודו-אקראי הניתנים לחיזוי (PRNG) עבור SSH. על ידי ניצול החולשה הזו, יכולתי לחזות את המפתח הפרטי מהמפתח הציבורי המתאים לו. המאמצים המתמשכים שלי גם הובילו אותי לנצל פגיעות של vsftpd 2.3.4 בדלת אחורית, וכתוצאה מכך הסלמה מוצלחת נוספת של הרשאות.

עמודים: 2 - 27

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Beep

הישג הסמכה



פרטי מכונה:

- קושי: קל
- קישור: https://www.hackthebox.com/achievement/machine/1636210/5

איך פרצתי:

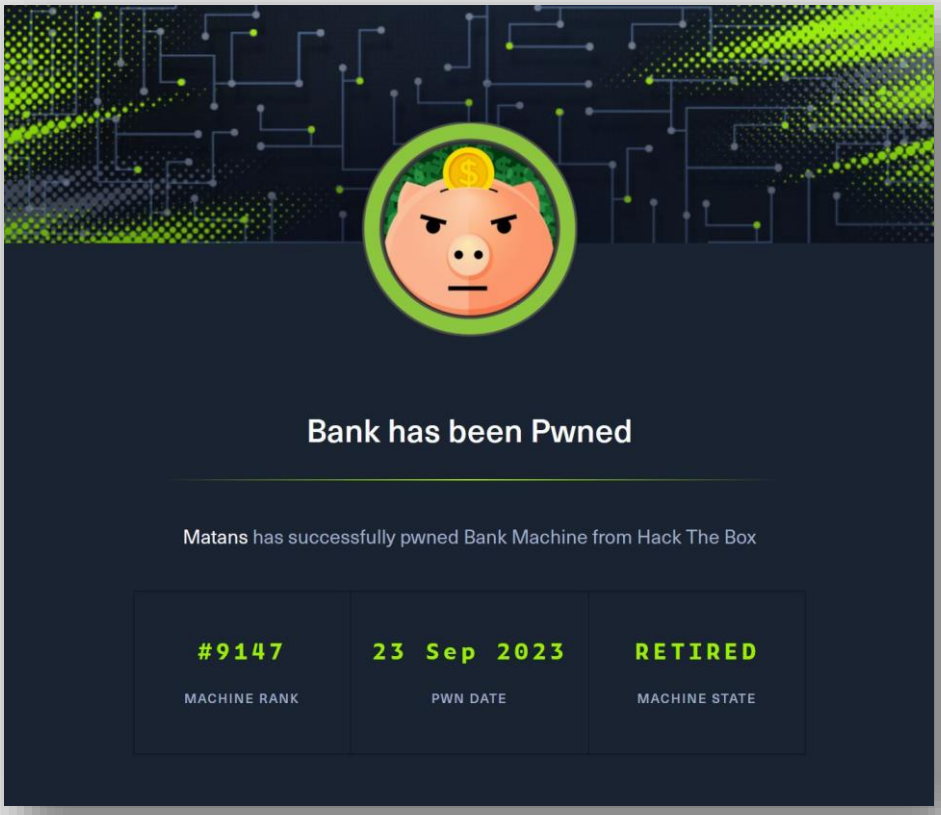
- גישה ראשונית: זיהיתי פגיעות LFI בתוך Elastix, מה שמאפשר לי לאחזר אישורים קריטיים. עם גישה מוצלחת לאתר ביציאה 10000, יצרתי ויזמתי מעטפת הפוכה. ניתוח נוסף חשף את רגישות האתר לפגיעות של ShellShock, ממנה השגתי מעטפת הפוכה נוספת. כדי להשלים את הגישה שלי, המצאתי קמפיין דיוג, תוך הטמעת קוד PHP בתוך המייל. לאחר מכן, תוך מינוף הניצול הראשוני של LFI, ביצעתי בהצלחה את ה-PHP המוטבע.
- הסלמה של הרשאות: לאחר גישה ראשונית, השתמשתי ב-linpeas כדי לסקור את הסביבה, וחשפתי הרשאות שגויות בתצורה. בעזרת הפקודה sudo nmap, השגתי הסלמה של הרשאות, והרחבת הגישה שלי בתוך המערכת.

עמודים: 28 - 49

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Bank

הישג הסמכה



פרטי מכונה:

- קושי: קל
- קישור: https://www.hackthebox.com/achievement/machine/1636210/26

איך פרצתי:

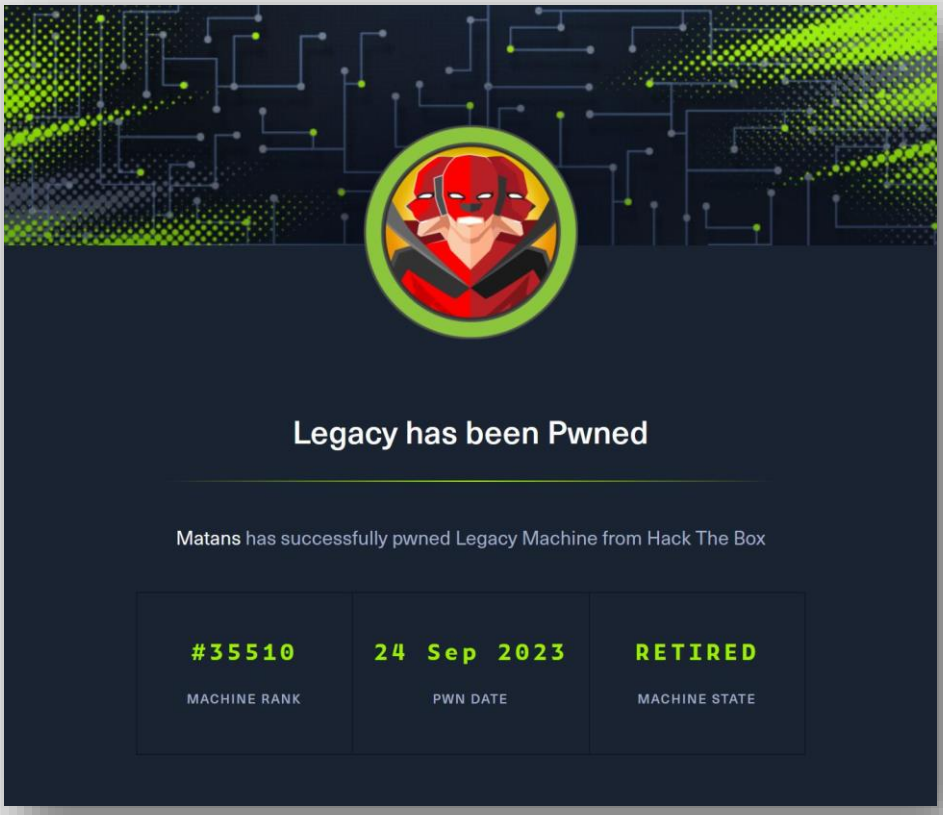
- גישה ראשונית: בעזרת כלים כמו 'dig' ו'gobuster', זיהיתי את הדף /-balance transfer. פרטי אימות שהתגלו בו אפשרו גישה לאינטרנט. יש לציין כי קוד המקור חשף שקבצים עם סיומת ".htb" נותחו כ-PHP, ויצרו חלון הזדמנויות. העליתי וביצתי סקריפט PHP, מה שהביא לרכישת מעטפת הפוכה מוצלחת.
- הסלמה של הרשאות: שני נתיבים הופיעו להסלמה: תצורה שגויה גרמה לכתיבה את הקובץ /etc/passwd, מה שאפשר למשתמש שלי בעל הרשאות נמוכות ליצור מופע של חשבון שורש. הנוכחות של סקריפט חירום העניקה הסלמה של הרשאות לכל משתמש.

עמודים: 50 - 66

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Legacy

הישג הסמכה



פרטי מכונה:

- קושי: קל
- קישור: https://www.hackthebox.com/achievement/machine/1636210/2

איך פרצתי:

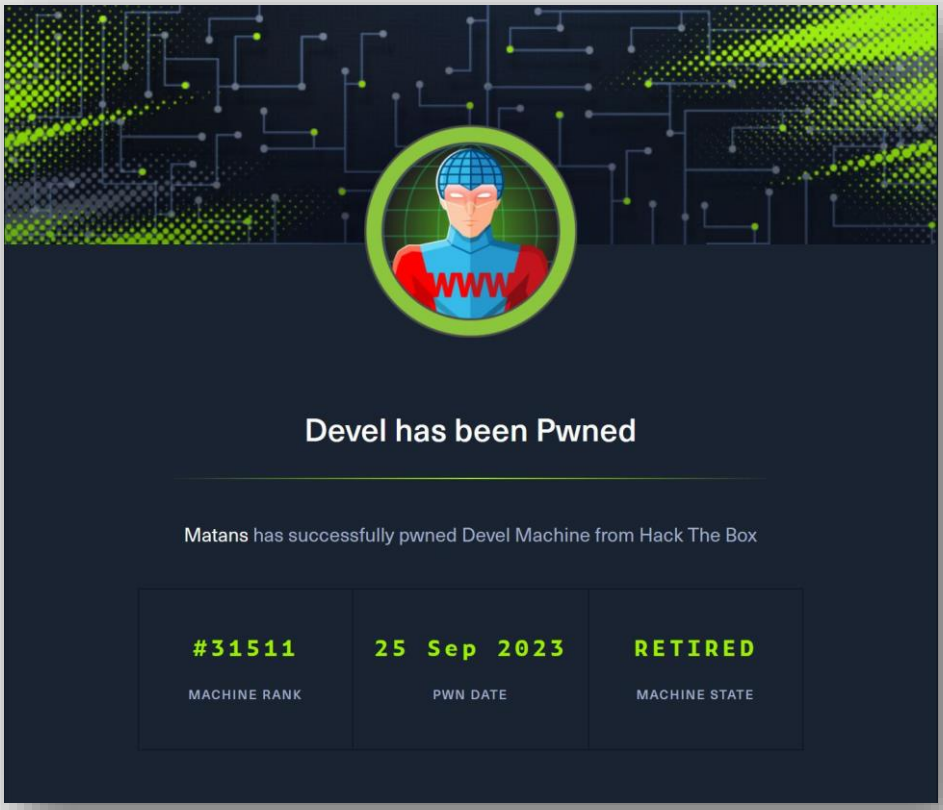
- גישה ראשונית: המכונה נקודות תורפה הן ל-EternalBlue והן ל-ms08-067, כמו גם ל-MS17-010. כשפריסה את המנצלים הללו בהצלחה, אישרתי את יעילותם, והשגתי גישה למעטפת.
- הסלמה של הרשאות: לאחר הניצול, מצאתי את עצמי כבר פועל עם הרשאות שורש.

עמודים: 67 - 86

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Devel

הישג הסמכה



פרטי מכונה:

- קושי: קל
- קישור: https://www.hackthebox.com/achievement/machine/1636210/3

איך פרצתי:

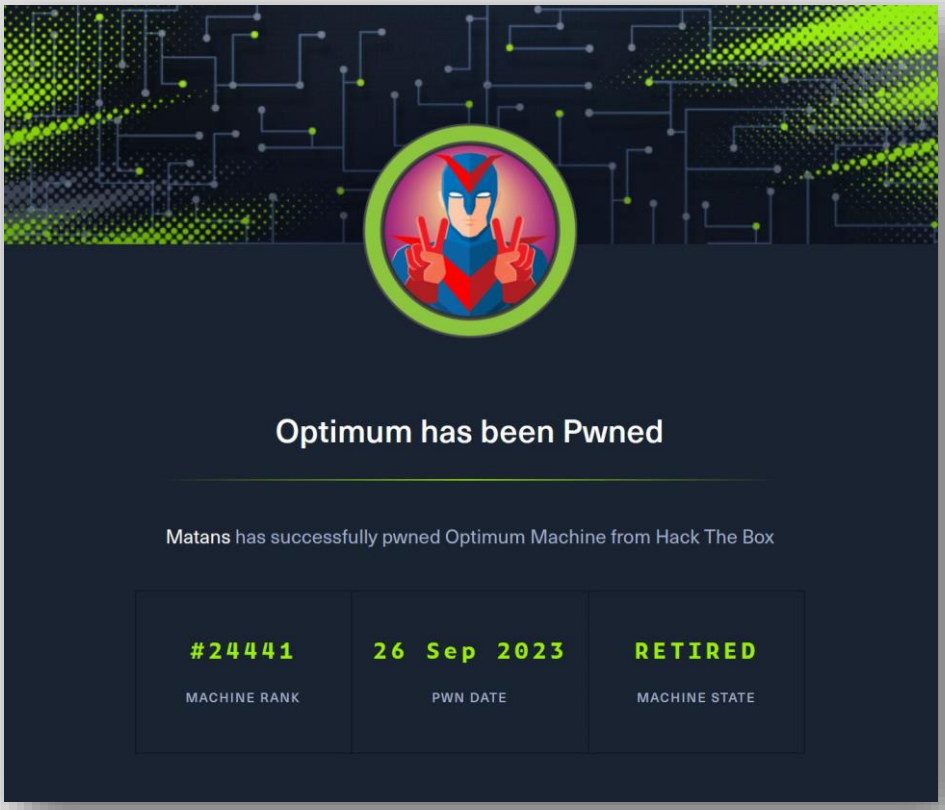
- גישה ראשונית: כשגיליתי את החיבור של האתר ל-SMB, העליתי בהצלחה קובץ 'aspx'. באמצעות msfvenom, יצרתי סקריפט של מעטפת הפוכה, משלים מעטפת הפוכה של PowerShell בהתאמה אישית לתוספת צדדיות.
- הסלמה של הרשאות: ניתוח מערכת חשף פגיעות ב-ms11-046. ניצלתי את החולשה הזו, השגתי הסלמה של זכויות יתר בצורה חלקה.

עמודים: 87 - 108

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Optimum

הישג הסמכה



פרטי מכונה:

- קושי: קל
- קישור: https://www.hackthebox.com/achievement/machine/1636210/6

איך פרצתי:

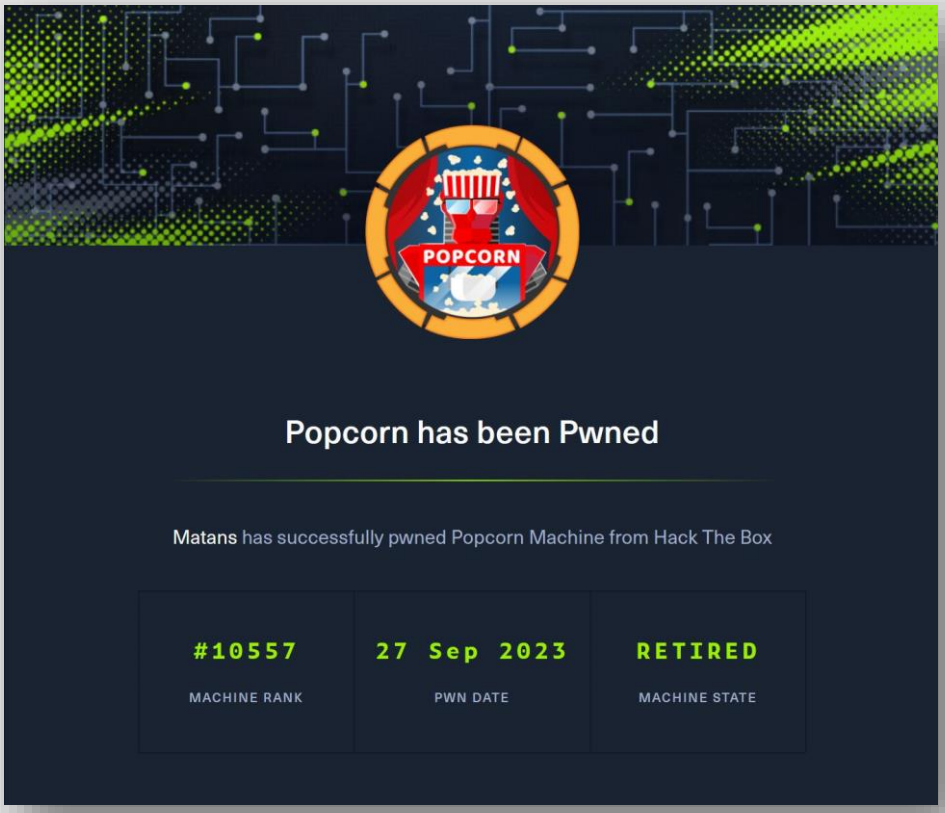
- גישה ראשונית: תוך מינוף CVE-2014-6287, ביצעתי פקודות במכונת היעד, מה שהקל על יצירת מעטפת הפוכה.
- הסלמה של הרשאות: בתחילה בסביבת PowerShell של 32 סיביות, השתמשתי בסקריפט שעבר למעטפת הפוכה של 64 סיביות. ניתוח מערכת ופריסה של MS16-032 לאחר מכן הסלמה מוצלחת של הרשאות.

עמודים: 109 - 128

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Popcorn

הישג הסמכה



פרטי מכונה:

- קושי: בינוני
- קישור: https://www.hackthebox.com/achievement/machine/1636210/4

איך פרצתי:

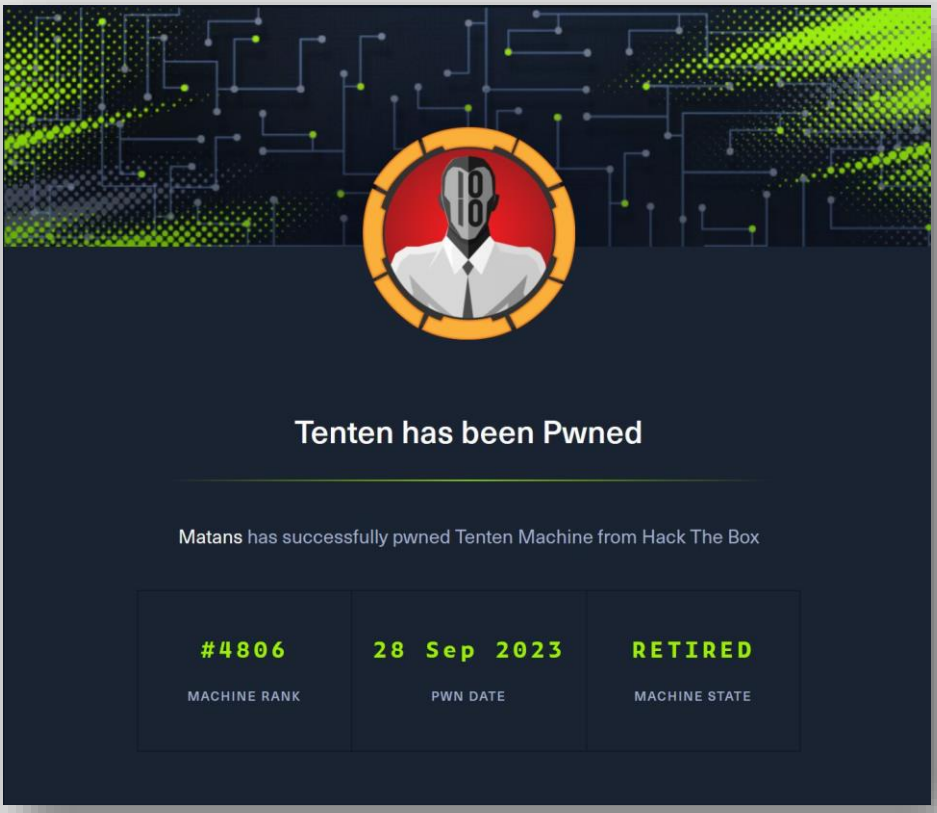
- גישה ראשונית: שימוש ב-sqlmap בדף הכניסה הניב אישורים, והזרקת SQL בסיסית הקלה על הגישה. בניווט בבלוג, ציינתי את שם המשתמש 'admin' וקיבלתי כניסה באמצעות המחרוזת "'admin'#". למרות שיכולתי ליצור משתמש חדש, בחרתי לנצל תכונת העלאת קבצים, תוך עקיפת הגבלות בחוכמה על ידי הוספת קוד PHP לבייטים הקסומים של התמונה, וכתוצאה מכך סיומת הקובץ הבלתי שגרתית ".png.php". גישה יצירתית זו אפשרה ביצוע פקודות על היעד וגישה למעטפת לאחר מכן.
- הסלמה של הרשאות: שלושה ניצולים בולטים - Full Nelson, DirtyC4w ו- PAM 1.1.0- CVE-2010-0832 - הציעו הסלמה פוטנציאלית של הרשאות. כל אחד הועסק בהצלחה, והעניק לי הרשאות מוגברות.

עמודים: 129 - 144

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: TenTen

הישג הסמכה



פרטי מכונה:

- קושי: בינוני
- קישור: https://www.hackthebox.com/achievement/machine/1636210/8

איך פרצתי:

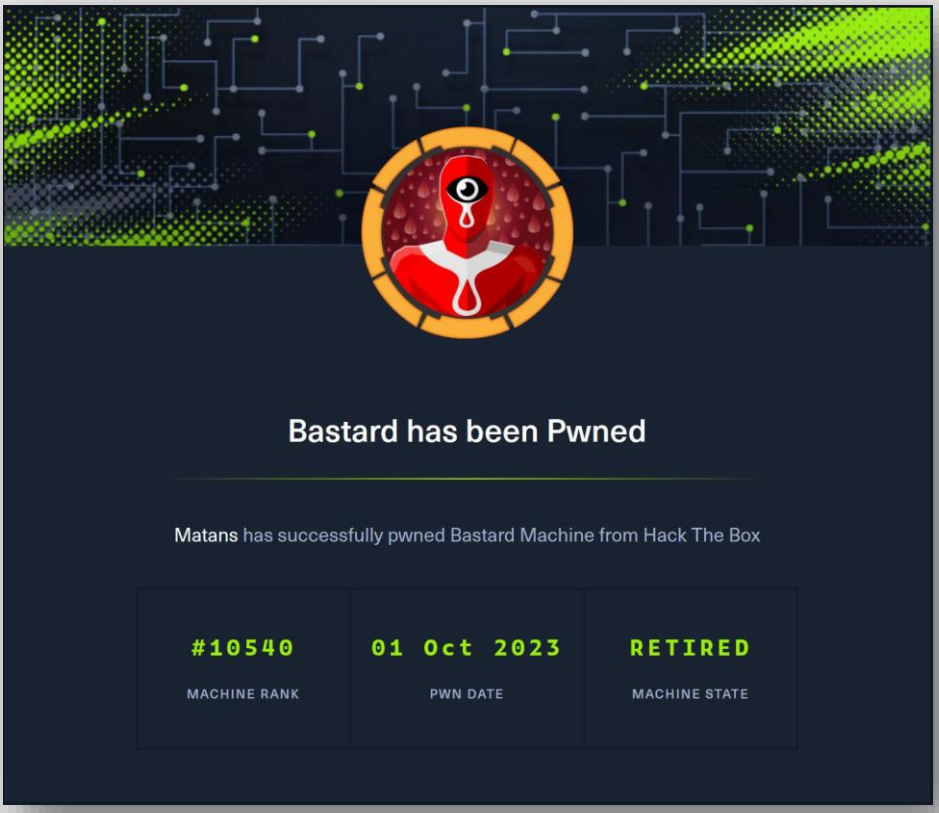
- גישה ראשונית: במיקוד לאתר וורדפרס, השתמשתי ב-wpscan, וחשפתי את הפגיעות CVE-2015-6668. תוך מניפולציה של כתובת האתר על ידי החלפת '/8' במספרים שרירותיים, נתקלתי בכותרת "HackerAccessGranted". תוך שימוש ב-CVE-2015-6668 עם תסריט מותאם של Python brute-force, חשפתי את הקובץ "HackerAccessGranted.jpg", שהכיל ביטוי סיסמה עבור מפתח SSH מוצפן. John the ripper, בשימוש בשילוב עם rockyou.txt, פיענח את ביטוי הסיסמה, ואיפשר גישה ל-SSH באמצעות המפתח המפוענח.
- הסלמה של הרשאות: כשנתקלתי בקובץ המעניק ביצוע פקודה כשורש, יזמתי מעטפת נוספת עם הרשאות גבוהות. בנוסף, תצורת ה-LXD של המערכת הציגה חולשה ידועה ניתנת לניצול, אותה מינפתי להסלמה נוספת של הרשאות.

עמודים: 145 - 162

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Bastard

הישג הסמכה



פרטי מכונה:

- קושי: בינוני
- קישור: https://www.hackthebox.com/achievement/machine/1636210/7

איך פרצתי:

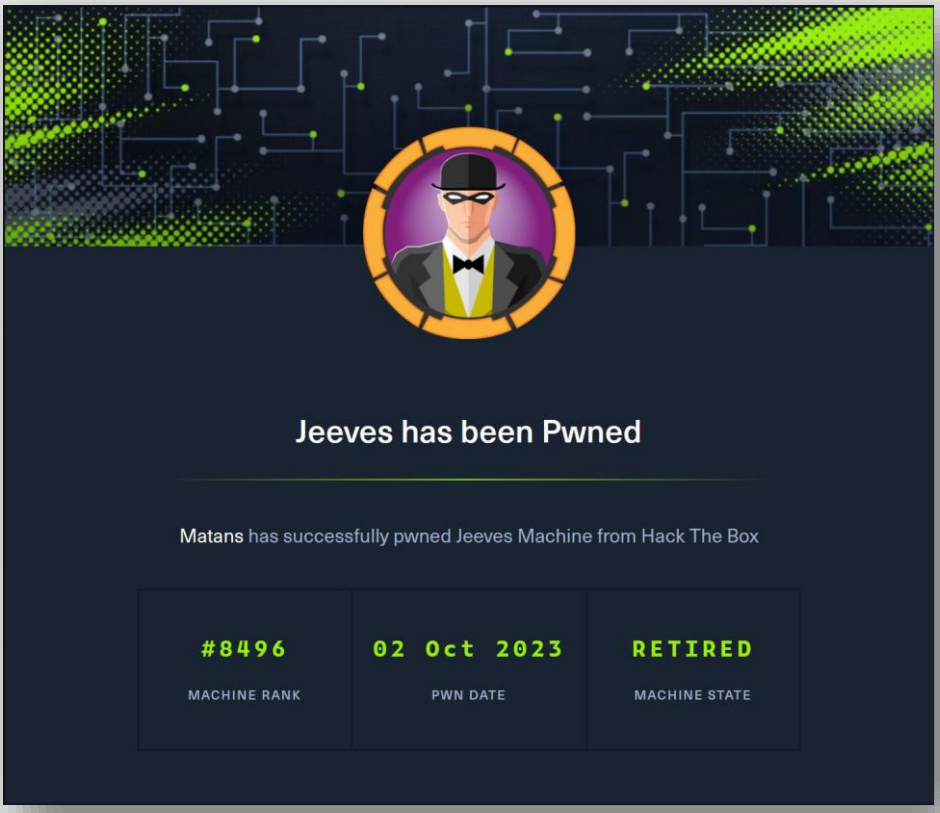
- גישה ראשונית: ניצלתי פגיעות ב-Drupal 7.x שחושפת נתונים רגישים, כולל אישורי משתמש וגם מאפשרת ביצוע פקודות. עם השגת ופענוח ה-hash של המנהל, הפעלתי תוסף קוד PHP, העליתי סקריפט PHP הפוך של מעטפת ויצרתי חיבור.
- הסלמה של הרשאות: ניתוח מערכת חשף פגיעות ב-MS15-051. בהתבסס על זה, ביצעתי פקודות כשורש ויזמתי מעטפת הפוכה נוספת, והסללתי בהצלחה את ההרשאות שלי.

עמודים: 163 - 191

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Jeeves

הישג הסמכה



פרטי מכונה:

- קושי: בינוני
- קישור: https://www.hackthebox.com/achievement/machine/1636210/114

איך פרצתי:

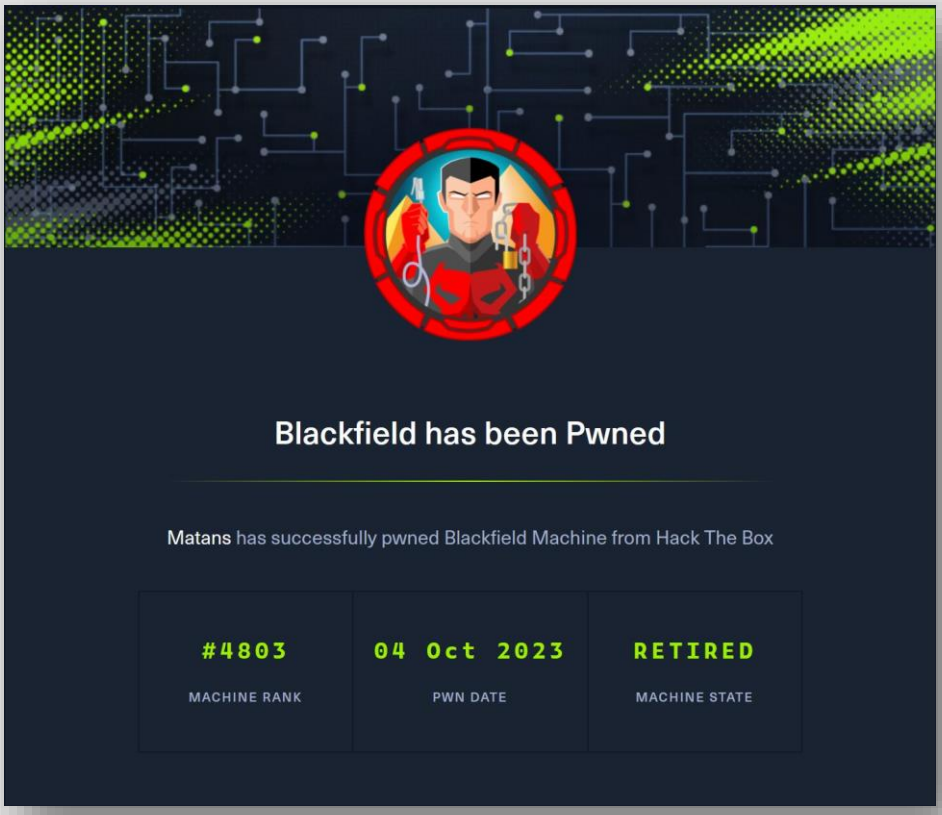
- גישה ראשונית: חדרתי למכונה המחקה את מנוע החיפוש "שאל את ג'יבס". סריקת רשת חשפה שרת HTTP ביציאה 50000. התקפת מילון בכוח גס חשפה את הדף "ask-jeeves/" שבו ניצלתי את היכולת של מסוף הסקריפטים להפעיל סקריפטים של Groovy, תוך פריסה מוצלחת של סקריפט מעטפת הפוך לגישה ראשונית.
- הסלמה של הרשאות: ניווטתי בספריות של המכשיר, אחזרתי קובץ KeePass מוגן בסיסמה. חילצתי את ה-hash של הסיסמה ופיענחתי אותו באמצעות John the Ripper, וחשפתי אישורים בתוך הקובץ. על ידי שימוש ב-'pth-winexe', טכניקת pass-the-hash, ניגשתי לחשבון משתמש ניהולי. בנוסף, היה ניתן לנצל את רגישות המערכת לפגיעות JuicyPotato, והשגתי הסלמה של הרשאות בכמה חזיתות.

עמודים: 192 - 223

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Blackfield

הישג הסמכה



פרטי מכונה:

- קושי: קשה
- קישור: https://www.hackthebox.com/achievement/machine/1636210/255

איך פרצתי:

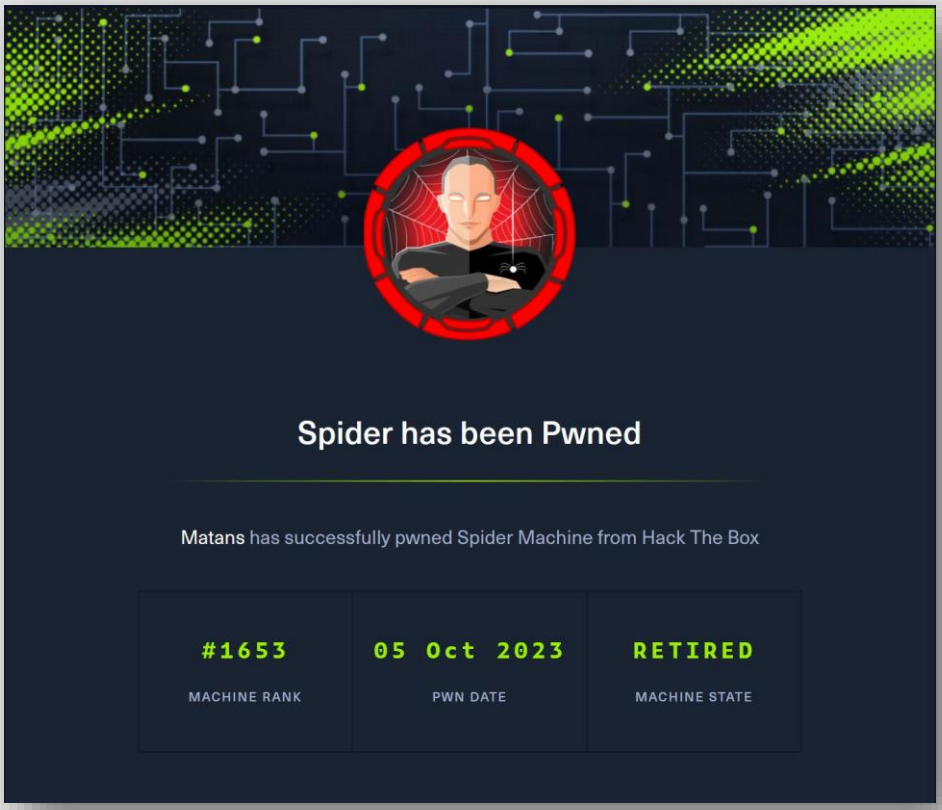
- גישה ראשונית: לאחר סיור רשת, ניגשתי לשיתוף SMB, וזיהיתי מספר תיקיות ריקות. על ידי המרת תיקיות אלו לרשימת משתמשים, GetNPUsers.py אישר את נוכחות המשתמש "Support". פיצוח ה-hash שלו סיפק גישה עמוקה יותר. יש לציין, Bloodhound ציינה את היכולת לשנות את הסיסמה עבור המשתמש "AUDIT2020", אותה ביצעתי. גישה זו הובילה לגילוי הקובץ "lsass.zip". באמצעות Pypykatz, חילצתי את ה-hash עבור "svc_backup" ויזמתי מתקפת Pass-The-Hash מוצלחת.
- הסלמה של הרשאות: בזמן שרכשתי גם את קבצי ה-SAM וגם את ה-SYSTEM, משתמש האדמין נשאר בלתי נגיש. הרשאות המשתמש שלי אפשרו אחזור של הקובץ "ntds.dit" מגיבויים. הטמעה נוספת של מתקפת Pass-The-Hash עם הנתונים האלה הובילה להסלמה של הרשאות.

עמודים: 224 - 267

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Spider

הישג הסמכה



פרטי מכונה:

- קושי: קשה
- קישור: https://www.hackthebox.com/achievement/machine/1636210/350

איך פרצתי:

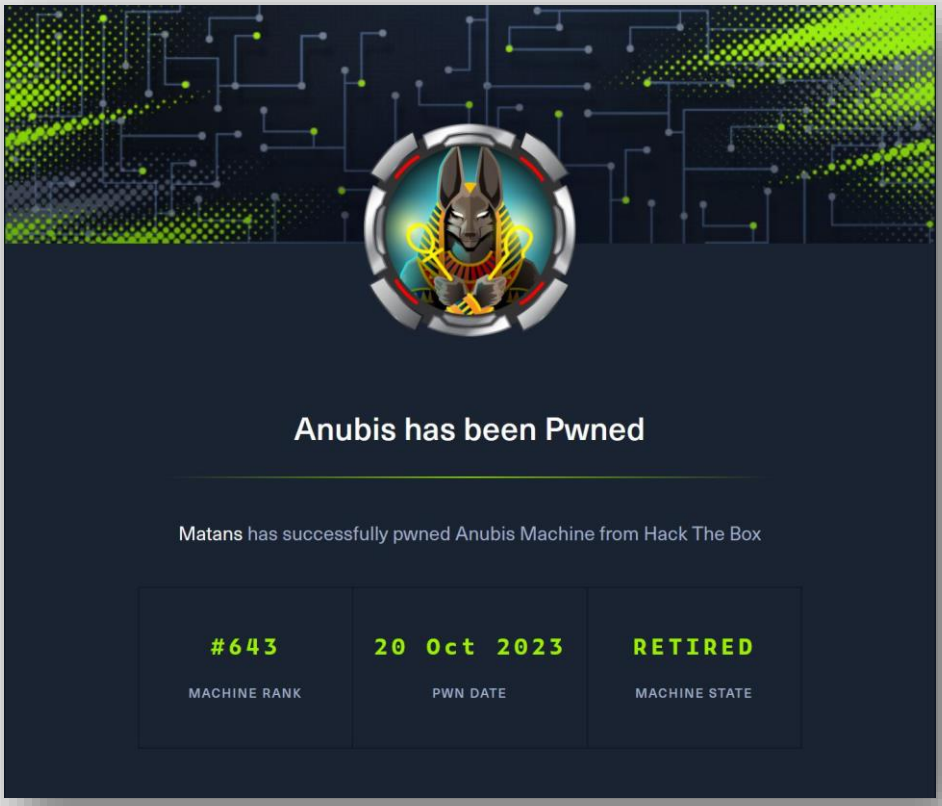
- גישה ראשונית: בזמן הניווט באתר, זיהיתי נקודות תורפה ל-XSS וגם ל-SSTI בדף הכניסה של המשתמש. בגלל המגבלה של 10 תווים על SSTI, לא הצלחתי להשיג מעטפת ישירות. עם גילוי ה-SECRET_KEY וההבנה שהפלטפורמה מבוססת על Flask, פינשתי את ה-cookie המשויך. למרות שהמניפולציה של המפתח סודי התבררה כלא יעילה, המשתנה UUID בתוך ה-cookie הציג פגיעות של הזרקת SQL. באמצעות SQLmap חילצתי את האישורים של האתר. על ידי ניתוח תקשורת פנימית, זיהיתי דף תמיכה לא שלם, שלמרות כמה מגבלות אופי, עדיין היה רגיש ל-SSTI. זה איפשר לי ליצור חיבור מעטפת הפוך.
- הסלמה של הרשאות: איתור המפתח הפרטי של ה-SSH עבור המשתמש הנוכחי שלי, ושמתי לב לפעילות של פורט 8080, השתמשתי במנהור SSH כדי לעבד את האתר במחשב ה kaliשלי. לאתר הייתה פגיעות של הזרקת XML. ניצלתי את החולשה הזו, השגתי את מפתח ה-SSH הפרטי של השורש ולאחר מכן הסלמתי את ההרשאות שלי.

עמודים: 268 - 293

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

Hack The Box: Anubis

הישג הסמכה



פרטי מכונה:

- קושי: מטורף
- קישור: https://www.hackthebox.com/achievement/machine/1636210/371

איך פרצתי:

- גישה ראשונית: החקירה שלי התחילה באתר 'windcorp', הפגיע ל-XSS ו-SSTI, שדרכו הקמתי מעטפת הפוכה. עם זאת, מצאתי את עצמי מוגבל בתוך מיכל. באופן מסקרן, יציאה 80 נחשפה ב-DefaultGateway IP, מה שגרם לי להשתמש ב'chisel' כדי לנתב מחדש את היציאות. אתר אינטרנט שלאחר מכן, באינטראקציה עם IP חיצוני, חשף ניסיון תקשורת ביציאה 5985 כאשר הפניתי את התעבורה. כשאני משתמש ב-'responder', תפסתי את ה-hash של המשתמש 'localadmin'. פריצת הדרך הזו הובילה אותי ל-SMB, שם חשפתי קובץ 'Whatif.omv' שהופעל לאחרונה, המשויך לתוכנת 'Jamovi' הרגישה ל-CVE-2021-28079. העברת קבצים נחוצים ל-Windows VM שלי, ניצלתי את הפגיעות הזו, יצרתי מטען באמצעות 'charlotte' ו-'msfvenom', ושילבתי XSS כדי להפעיל את הסקריפט שלי, ולבסוף פרצתי את גבולות הקונטיינר.
- הסלמה של הרשאות: בתוך סביבת ה-active directory של המחשב ולהפעלת "Active Directory Certificate Services", קלטתי את הגישה של המשתמש שלי לתעודת האינטרנט. בניסיון להביא את אישור המנהל דרך ADCS.ps1, נתקלתי בתקלה הקשורה ל-UPN, שתיקנתי על ידי עריכת סקריפט הקוד. עם התעודה שנרכשה, השתמשתי ב-Rubeus.exe כדי ללכוד את ה-TGT של Kerberos. אימות שימושיות ה-hash עבור גישת מנהל דרך crackmapexec, השתמשתי ב-psexec לצד טכניקת Pass-The-hash, והשגתי הסלמה של הרשאות. בנוסף,

מצאתי את המערכת פגיעה ל-CVE-2021-42278 ו-CVE-2021-42287. בפתרון אי התאמה באזור הזמן של Active Directory, רתמתי את noPAC כדי להיכנס ל localadmin, באמצעות סיסמה שזוהתה בעבר.

עמודים: 294 - 372

- קרא את הערות הפריצה המלאות ב-Google Drive
- קרא את הערות הפריצה המלאות ב- Github

תעודת מקצוען אבטחת סייבר של גוגל: יסודות אבטחת הסייבר

"יסודות אבטחת הסייבר" הוא הקורס הפותח בתוכנית Google Cybersecurity Certificate, שמטרתו לצייד את הלומדים במיומנויות החיוניות לתפקיד התחלתי בתחום אבטחת סייבר. באמצעות תוכנית לימודים אינטראקטיבית שנוצרה על ידי Google, קורס זה מציג את תחום אבטחת הסייבר, ומכסה את ההיבטים הבסיסיים שלה, כולל איומים, פגיעויות, והכלים, הטכנולוגיות והאסטרטגיות המשמשות לניהולם. יתרה מזאת, היא מתעמקת בכלי אבטחת סייבר ושפות תכנות, ומציעה תובנות לגבי כלים נפוצים המשמשים אנליסטים של אבטחת סייבר לזיהוי והפחתת סיכונים, לצד הסבר על כלי אבטחה וניהול אירועים (SIEM), מנתחי פרוטוקול רשת ושפות תכנות כמו Python ו- SQL.

ציון: 88.78%

אורך: 14 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל: שחק בטוח נהל סיכוני אבטחה

הקורס "שחק בטוח: נהל סיכוני אבטחה" הוא הפרק השני בתוכנית Google Cybersecurity Certificate, המספק הבנה מעמיקה יותר של מושגי אבטחת סייבר מרכזיים. קורס זה מדגיש את ניצול המסגרות והבקרות על ידי אנשי אבטחת סייבר כדי להגן על הפעילות העסקית. הוא מנחה את הלומדים בשלבי ניהול סיכונים, ומאפשר להם להבחין באיומים, סיכונים ופגיעות נפוצים איתם מתמודדים עסקים מודרניים. תכנית הלימודים מעוצבת בקפידה כדי להציע סקירה מקיפה של ניהול סיכונים, ולספק ללומדים מיומנויות חיוניות לנווט בנוף המורכב של אבטחה ארגונית.

ציון: 92.88%

אורך: 11 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל: התחבר והגן רשתות ואבטחת רשת

קורס "התחבר והגן: רשתות ואבטחת רשת", בהיותו השלישי בסדרת תעודות אבטחת הסייבר של גוגל, מתעמק במורכבות של חיבורי רשת בין מכשירים מרובים, ומבטיח ערוצי תקשורת מאובטחים. הוא מתבסס על נושאי היסוד שהוצגו בקורס הקודם, ומאפשר הבנה מעמיקה יותר של פעולות ופרוטוקולים של רשתות מודרניות. בפרט, הלומדים נלמדים כיצד ללכוד ולנתח תעבורת רשת, לזהות ולצמצם התקפות הסתננות שונות על ידי שחקנים זדוניים, ולהשיג הבנה מוצקה של מודל פרוטוקול/פרוטוקול אינטרנט (TCP/IP) של בקרת שידור. יתר על כן, הקורס בוחן את התפקידים הבסיסיים של חומרת רשת כגון נתבים ומודמים באפשרות העברת נתונים מאובטחת בין רשתות.

ציון: 88.72%

אורך: 14 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל: כלי המסחר לינוקס ו-SQL

"כלי המסחר: לינוקס ו-SQL", כאבן הדרך הרביעית בתוכנית Google Cybersecurity Certificate, מאפשר חקירה מקיפה של מיומנויות מחשוב חיוניות המשמשות אנליסטים של אבטחת סייבר. תכנית הלימודים של הקורס תוכננה בקפידה כדי לספק תרגול מעשי באמצעות לינוקס, מערכת הפעלה שאומצה באופן נרחב בתחום אבטחת הסייבר. הלומדים ינווט וינהלו את מערכת הקבצים באמצעות פקודות לינוקס דרך מעטפת Bash, יאמתו ויאשרו משתמשים ויתעמקו במבנה של מסדי נתונים יחסיים. בנוסף, הקורס מקנה ידע כיצד להשתמש ב-SQL כדי לאחזר מידע מבסיסי נתונים, להחיל מסננים על שאילתות SQL ולהשתמש ב-Joins לשילוב טבלאות מרובות. ההכשרה גם מאירה את הקשר בין מערכות הפעלה, יישומים וחומרה, ומשווה בין ממשקי משתמש גרפיים לממשקי שורת פקודה, מציידת את הלומדים בהבנה חזקה המסייעת לתפקידי אבטחת סייבר ברמת הכניסה.

ציון: 94.59%

אורך: 27 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל: נכסים, איומים ופגיעויות

הקורס "נכסים, איומים ופגיעות" עומד כאבן המדרגה החמישית בתוכנית Google Cybersecurity Certificate, שנועדה להעמיק את ההבנה של הלומדים במושגי הליבה של אבטחת סייבר שנבנו בקורס הקודם. קורס זה מגולל את היסודות של נכסים, איומים ופגיעות בתחום הסייבר, ומספק תובנה יסודית כיצד נכסים מסווגים וכיצד לזהות ולצמצם איומים ופגיעות שונים שעלולים להשפיע עליהם. זה משמש כמאמץ חיוני עבור אלה השואפים להיכנס לתפקידי אבטחת סייבר ברמת הכניסה, ומעצים להם את הידע הדרוש כדי לשמור על נכסים ארגוניים ביעילות.

ציון: 88.12%

אורך: 25 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל: השמע את האזעקה זיהוי ותגובה

הקורס "השמע את האזעקה: זיהוי ותגובה" הוא הפרק השישי בתוכנית תעודת אבטחת הסייבר של Google, משכלל את הכישורים הנדרשים לזיהוי ותגובה של תקריות. בהתבסס על נושאי היסוד שכוסו בקורסים הקודמים, תכנית לימודים זו מתמקדת בהגדרת אירועי אבטחה, הבהרת מחזור החיים של התגובה לאירועים, והבהרת התפקידים והאחריות של צוותי תגובה לאירועים. הלומדים מנווטים בתהליך של זיהוי ותגובה לתקריות באמצעות מערכת זיהוי חדירה, ביצוע לכידת מנות וניתוח, ובכך מקבלים הבנה מעמיקה של האמצעים הקריטיים שיש לנקוט במהלך איומי אבטחה פוטנציאליים.

ציון: 93.47%

אורך: 24 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל: הפוך משימות אבטחת סייבר לאוטומטיות עם Python

הקורס "אוטומציה של משימות סייבר עם Python" משמש כמודול השביעי בתוכנית Google Cybersecurity Certificate, ומאפשרת תובנה מקיפה למינוף שפת התכנות Python בהקשר של אבטחת סייבר. בהתבסס על מושגי אבטחת הסייבר הבסיסיים שנחקרו בקורסים קודמים, קורס זה מציע מבוא לתכנות Python, תוך שימת דגש על היישום שלו באוטומציה של משימות אבטחת סייבר. הוא מנחה את הלומדים דרך מושגי פייתון בסיסיים, כולל סוגי נתונים, משתנים, הצהרות מותנות ואיטרטיביות, ומתרחב לתרגילים מעשיים המשפרים את יכולתם לכתוב קוד Python יעיל המותאם לתרחישי אבטחת סייבר. הניסיון וההסמכה הקודמת שלי ב-Python (PCAP) ללא ספק חיזקו, ואפשרו לי להצטיין ולהשיג ציון יוצא דופן בקורס זה.

ציון: 99.41%

אורך: 29 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.

תעודת מקצוען אבטחת סייבר של גוגל: הכניסו את זה לעבודה היכונו לעבודות אבטחת סייבר

הקורס "הכנס את זה לעבודה: היכונו לעבודות אבטחת סייבר" הוא המודול השמיני והאחרון בתוכנית תעודת אבטחת הסייבר של גוגל, שמטרתו לצייד את הלומדים במיומנויות הנדרשות לתפקידי אבטחת סייבר ברמת ההתחלה. קורס זה כולל גישה פרגמטית לקראת הכנה להגשת מועמדות לעבודה בתחום אבטחת הסייבר. הלומדים יעסקו ביצירת קורות חיים מקצועיים ומכתב מקדים, יחד עם פעילויות מעשיות ודוגמאות המדמות משימות אבטחת סייבר נפוצות. תכנית הלימודים מועשרת בסרטונים ובהדרכה של עובדי Google הנוכחיים הפועלים בתחום אבטחת הסייבר, ומציעה פרספקטיבה אמיתית על קבלת החלטות מושכלות והסלמה של תקריות לבעלי עניין, ובכך מבטיחה הכנה מגוונת לאנשי מקצוע שואפים בתחום אבטחת הסייבר.

ציון: 98.10%

אורך: 18 שעות.

קרא עוד ב-Coursera.

צפה בפרויקטים שלי מהקורס של Google Cybersecurity Professional כאן.

אמת תעודה זו.