תיאור האתגר:

אתה מעריץ של הסדרה בובספוג, כרגע אתה נמצא במפגש מעריצים בו נפרדים ממתרגם הסדרה הנוכחי פטריק (מחוברים לאותה רשת). במהלך המפגש ראש ארגון המעריצים מזכיר לכם לשאיר פידבק על האירוע בעמוד האתר. אתה יודע כי בשביל להשאיר פידבק, יש להתחבר עם חשבון המשתמש של פורום המעריצים ואתה יודע שגם פטריק הנוכח יעשה כך. המטרה שלך היא לפרוץ למחשב הפרטי של פטריק, וקבלת גישה לפרקים שעדיין לא פורסמו ואולי גם למצוא דרך לקבל את הפרקים החדשים גם אחרי שפטריק יעזוב.

שלבים:

1. השתלת קוד זדוני בפורום המעריצים:
2. אתה מודע לכך שפטריק הולך להיכנס לפורום ולהתחבר, אתה יודע מה שם המשתמש שלו בפורום. אליך לגלוש לפורום האתר ולשתול שם קוד Javascript זדוני בתוך טבלת ה-SQL של התגובות על המפגש.
3. תוך בדיקה מהירה קל לראות כי תיבת 'הערות נוספות' מוגנת מהכנסת תבניות HTML והכנסת תווים מסוימים, בין היתר תווים הנחוצים להשתלת קוד Javascript.
4. ניתן לראות כי האתר מציג את שמות המשתמשים של המשתמש המגיב, אתה צריך לזהות כי ניתן להשתיל שם קוד, שם המשתמש מוגבל ל-16 תווים ולכן מקשה על שתילת הקוד.
5. סידור התגובות בפורום מסודר על פי סדר האותיות, כלומר תצטרך לשתול את הקוד שלך בסדר מסוים כדי שיוצג במדויק אחד אחרי השני.
6. פריצת המשתמש של פטריק בפורום האתר:
7. כדי לקבל מידע נוסף כמו ה-IP של פטריק, הסיסמה שלו בפורום האתר, נבנה אתר פישינג של הפורום ונשתול קוד זדוני בפורום שיעביר את המשתמשים לאתר הפישינג שלנו במקום לאתר האמיתי ויעביר את המידע אלינו.
8. אנו יודעים את שם המשתמש של פטריק ולכן נוכל לזהות התחברות שלו, נוכל לראות את הסיסמה שלו וגם את כתובת ה-IP שלו.
9. התחברות למחשב של פטריק:
10. מניחוש מוצלח ניתן למצוא שפטריק לא מגן טוב מאוד על המחשב שלו ושם המשתמש שלו והסיסמה זהים למה שהיו בפורום, ניתן להתחבר אליו באמצעות SSH באמצעות כתובת ה-IP שמצאנו בסעיף קודם.
11. לאחר שאתה מתחבר אתה מגלה כי במחשב האישי של פטריק אין פרקים חדשים על המחשב האישי שלו.
12. מחיפוש במחשב של פטריק אתה מוצא את תוכנה Putty מותקנת על המחשב.
13. התחברות למחשב מרוחק של חברת ניקלודיאון:
14. מחקירת המחשב, תוכל למצוא במחשב מידע על המחשב המרוחק כמו כתובת IP, שם משתמש של המחשב המרוחק וקובץ Auth של SSH בו תוכל להשתמש כדי להתחבר ללא סיסמה.
15. בשלב זה, ניסיונות התחברות עם SSH ייכשלו, כדי לפתוח את פורט 22 הרצוי יש לבצע סוג של Port Knocking בו אתה שולח לפורט מסוים שבחרנו (במקרה שלנו 22) כמות חבילות מסוימות בזמן קצר, כאשר גודל כל חבילה קבוע ומסוים אותו בחרנו (במקרה שלנו 86). לאחר ביצוע ה-Port Knocking פורט 22 ייפתח לכמה שניות לבקשות SSH, אם תתחבר בזמן זה החיבור יישאר פתוח גם לאחר שפורט 22 ייסגר שוב.
16. כעת תוכל להתחבר לחשבון של פטריק במחשב המרוחק ברשת של חברת ניקלודיאון.
17. בשלב זה תוכל למצוא בחשבון שלו רק את הפרק האחרון אותו הוא תירגם.
18. התחברות לחשבון אחר בתוך המחשב המרוחק:
19. בשלב זה תוכל לכתוב סקריפט שיסרוק קבצים חדשים בחשבון של פטריק וישלח לך אותם, אך אתה יודע שפטריק עוזב את החברה ולכן יש סיכוי שחשבון זה לא יתעדכן. בנוסף יש לך גישה רק לפרק אחד ואתה רוצה למצוא פרקים נוספים.
20. לחשבון של פטריק גישה מוגבלת מאוד על המחשב, אך הוא מסוגל לקרוא בלבד קבצים כמו passwd כדי לראות איזה משתמשים נוספים יש במחשב (לא שלב הכרחי).
21. בעזרת חקירת המחשב תוכל לגלות שמחשב לינוקס זה לא משתמש בגרסה החדשה ביותר של לינוקס הקרנל, אלא משתמש באחת הגרסאות הקודמות (4.8.0-58).
22. חקירה של גרסה זו של הקרנל תוביל למציאת מספר חורי אבטחה שניתן להשתמש בהם.
23. אנחנו כיוונו לשימוש בפריצת אבטחה מסוג Privilege Escalation, זאת נותנת לך הרשאות רוט. אך ניתן לבצע שלב זה עם מספר פריצות נוספות.
24. לאחר שקיבלת הרשאות רוט תוכל להיכנס לתיקיית המשתמש של Eugene, המנהל של פטריק לו יש גישת רוט למחשב ושם תוכל לשתול את הסקריפט שימשוך אוטומטית פרקים חדשים וישלח לך אותם, אפשרי באמצעות netcat לדוגמה.

<https://github.com/ron1196/HackerGame>

ב-Repo ישנם רוב הקבצים שהשתמשנו בהם במהלך הפרויקט, מחולקים לפי המחשב בו השתמשנו בהם.

בתיקייה Fans Site Server מופיע כל תכולת האתר אותו העלינו לשרת.

בתיקייה Patrick Computer מצורף הסקריפט אשר פותח בלופים את השרת שלנו וממלא את פרטי ההתחברות של פטריק, זה מתבצע כל שתי דקות במחשב של פטריק. בנוסף מצורף קובץ ה-Auth עבור השרת המרוחק אותו ניתן למצוא במחשב וגם קובץ ה-rc.local בו הוספנו כי הסקריפט שלנו יופעל בהפעלת המחשב.

בתיקייה Nick Computer מצורף הסקריפט בו השתמשנו כדי לבצע את תהליך ה-Port Knocking.