פרויקט סיום

עליך לממש תוכנית מחשב בשם myFileSystemMonitor שמדווחת למספר לקוחות על חדירה למחשב. לקוח בהקשר זה הוא כל מי מי שצופה בעמוד האינטרנט. התוכנית תנטר כל גישה לספרייה במערכת הקבצים בעזרת inotify . inotify מוצגת במודל, והיא מדגימה כיצד מנטרים מערכות קבצים. inotify תדווח על כך לשרת HTTP ו NETCAT . די לבדוק ספריה אחת.

1. דיווח ל WEBSERVER

על התכנית לעדכן בזמן אמת את קובץ index.html של ה WEBSERVER. השרת צריך להציג את המידע הבא:

A list of files that were accessed.

a. At which time
b. To what purpose: READ/WRITE

עדכון בזמן אמת הוא כזה שקורה בעת אירוע חדירה. עליכם לעדכן את index.html שוב ושוב. מאחר וקרוב לוודאי שעמוד ה- HTML לא מציג את העדכון בזמן אמת, מותר לסגור את ה FIREFOX ולפתוח אותו שוב. אין צורך לכתוב JAVA SCRIPT בשביל זה.

אנא צפו בסרטון המציג כיצד להתקין שרת APACHE ב- UBUNTU.

2. דיווח על גבי הרשת – netcat

בנוסף, יש להוסיף udp-client השולח מידע טקסטואלי ל - target ip בשורת ההפעלה של התוכנית. את המידע יש להציג בעזרת netcat (ראו סרטון). המידע חייב להיות בתצורה הבאה:

FILE ACCESSED: <File name>

ACCESS: <READ/WRITE>

TIME OF ACCESS: <DATE>:<HOUR>

For example:

FILE ACCESSED: /etc/shadow

ACCESS: NO_WRITE

TIME OF ACCESS: 28 August 2020: 21:55

בנוסף, עליכם לשבץ בתוכנית שרת Telnetd בתוך התוכנית, זאת בעזרת libcli .כאשר עושים אליו telnet אז הוא מאפשר פקודה בשם backtrace . כאשר פקודה זו ניתנת על ידי המשתמש, יצא backtrace של thread כלשהו אל תכנית ה- TELNET , אך לא ה THREAD של libcli עצמה, אלא THREADS אחר. את ה- backtrace יש לבצע בעזרת אינסטרומנטציה בלבד (ראה סרטון ודוגמא), על ידי התערבות בפונקציות האינסטרומנטציה.

קלטי התכנית

התכנית תקבל שני קלטים :

1. כתובת IP לשלוח מידע טקסטואלי על חדירה.
2. ספרייה לניטור

יש להשתמש ב- getopt של c כדי לקבל את הפלטים ולעבד אותם.

הפעלת התכנית:

```
$ myFileSystemMonitor -d /etc  -i 192.168.0.137
```

3. כאמור: ניתן להתחבר את התכנית הרצה בעזרת telnet <IP><PORT>

יש להראות את התקדמות הפיתוח תוך שימוש ב git . התכנית חייבת לעבוד ב- UBUNTU.

אופן הגשה

ניתן לפתח בגיטהאב.

ניתן להגיש בזוגות.