DHCP Starvation

הקדמה: מה זה DHCP Starvation

המתקפה DHCP Starvation Attack, בתרגום לעברית - *מתקפת הרעבת DHCP*, עובדת כך:
לאחר שהתוקף קיבל כתובת IP מן הארגון אליו הוא התחבר, התוכנה הזדונית שלו שולחת בקשת DHCP (לקבלת IP) מכתובות MAC שונות ובכך גומרת את כל POOL הכתובות ולא נותר יותר כתובות כך שמשתמשים חדשים לא יכולים להתחבר לרשת זו.

כידוע, שרת DHCP מקצה למחשב כתובת IP לזמן מסוים ולא עד קץ הדורות, ולכן לכאורה, אחרי שיעבור זמן זה, השרת ימשיך לעבוד כרגיל. מצב זה נקרא persist.
גם על מצב זה מתקפה זו יכולה להתגבר, והיא עושה את זה באופן הבא:
כאשר מגיע הזמן לבקש הארכה לכתובת IP מן שרת DHCP, שזה אחרי שעבר 50%-87.5% מהזמן שהשרת נתן, התוכנה הזדונית שולחת בקשת הארכה ובכך גורמת לכתובת IP להישאר תפוסה.[1]

אופן הפעולה

פיצלנו את הקוד למחלקות הבאות:

- Starvation – המחלקה שמנהלת ומריצה את המתקפה.
- Lease – מחלקה המחזיקה פרטים על כתובת IP אשר שרת ה-DHCP "הקצאה" לתוקף ופרטים נוספים כגון זמן הקצאה וכו'. לכל כתובת שהתוקף מחזיק ישנו מופע של מחלקה זו.
- Sniffer – מנהלת ומבצעת את ההקלטה של פאקטות DHCP.

ראשית, השתמשנו בספרייה `argparse` על מנת לקלוט ולפרסר את פרמטרי השורה, ואת זה ניתן למצוא בפונק' `get_args()`.[2]
לאחר מכן, יצרנו מופע למחלקה `Starvation` והרצנו אותו.[3]
בפונק' `Starvation.run()` בדקנו האם המתקפה היא persistent או לא ופעלנו לפי זה.[4]
כאשר המתקפה היא לא persistent:
בלולאה שבפונק' `Starvation.run()` יוצרים מופע חדש של המחלקה `Lease`[5], ובו, ע"י קריאה לפונק' run[6] במחלקה sniffer, מתחילים את תהליך DORA לקבלת כתובת IP משרת DHCP, וע"י הפונק' Sniffer.handle_dhcp_packet(pkt)[7] ותופסים פעם אחת את כל הכתובות שהשרת יכול להקצאות. את כל הכתובות ש"תפסנו" אנו שומרים אותם במשתנה `Leases`[8] במחלקה `Starvation` ולבסוף מדפיסים את הכתובות התפוסות[9].

---

[1] דרך אפשרית להתגונן ממתקפת DHCP Starvation היא הגבלה על כמות כתובות ה-MAC על כל פורט וכל MAC מעבר (DROP)
[2] אשר מתחילה בשורה 293
[3] שורות 312, 314
[4] שורות 250-260
[5] שורה 259
[6] שורות 177-187
[7] שורות 189-214
[8] שורה 259
[9] שורות 240-249

כאשר המתקפה היא persistent:

מתחילים בדיוק כמו שעשינו עבור לא persistent, רק שהפעם, כאשר עברו 50% עד 87.5% מזמן ההשכרה של כתובת IP מסוימת, אנחנו שולחים `RENEW` לשרת על מנת להשאיר את כתובת ה-IP בשליטתנו. את כל זה ניתן למצוא בפונק' persistent שבמחלקה Starvation.[10]

צילומי מסך

תחילה, נציין שנתנו לשרת להקצאות רק 10 כתובות בתחום 192.168.56.100 – 192.168.56.110, וזאת כדי שהתהליך יהיה מהיר, ולכן גם בצילומי המסך הבאים, אנו רואים רק הקצאה של 10 כתובות IP.

ראשית, הוכחה שהקוד עובד ואכן השרת מקצה את כתובות ה-IP לקוד שלנו.

בתמונה שלמטה, רואים את רשימת הכתובות ששמורה בשרת שמראה איזה כתובות הוא הקצאה:

```
MAC                IP              hostname       valid until         manufa
cturer
=================================================================================
==================
08:00:27:4e:5c:37  192.168.112.109 kali           2020-11-02 16:59:51 -NA-

52:54:00:03:7f:a4  192.168.112.110 BOT2           2020-11-02 17:00:15 -NA-

52:54:00:26:41:a3  192.168.112.108 BOT0           2020-11-02 17:00:13 -NA-

52:54:00:29:ec:cb  192.168.112.104 BOT5           2020-11-02 17:00:18 -NA-

52:54:00:47:85:9b  192.168.112.100 BOT7           2020-11-02 17:00:21 -NA-

52:54:00:57:8e:7d  192.168.112.105 BOT3           2020-11-02 17:00:16 -NA-

52:54:00:7f:73:cd  192.168.112.107 BOT6           2020-11-02 17:00:19 -NA-

52:54:00:d9:21:27  192.168.112.101 BOT9           2020-11-02 17:00:23 -NA-

52:54:00:e4:d2:b3  192.168.112.102 BOT1           2020-11-02 17:00:14 -NA-

52:54:00:f0:47:1d  192.168.112.106 BOT8           2020-11-02 17:00:22 -NA-

52:54:00:f8:b5:54  192.168.112.103 BOT4           2020-11-02 17:00:17 -NA-
```

שנית, הרשימה שהקוד הזדוני שלנו מפיק, שמראה איזה כתובות תפסנו:

```
----------------leases----------------
BOT0: 52:54:00:26:41:a3, 192.168.112.108 , Release in 2020-11-02 12:00:13.497072
BOT1: 52:54:00:e4:d2:b3, 192.168.112.102 , Release in 2020-11-02 12:00:14.565634
BOT2: 52:54:00:03:7f:a4, 192.168.112.110 , Release in 2020-11-02 12:00:15.672815
BOT3: 52:54:00:57:8e:7d, 192.168.112.105 , Release in 2020-11-02 12:00:16.773624
BOT4: 52:54:00:f8:b5:54, 192.168.112.103 , Release in 2020-11-02 12:00:17.849193
BOT5: 52:54:00:29:ec:cb, 192.168.112.104 , Release in 2020-11-02 12:00:18.925051
BOT6: 52:54:00:7f:73:cd, 192.168.112.107 , Release in 2020-11-02 12:00:19.989812
BOT7: 52:54:00:47:85:9b, 192.168.112.100 , Release in 2020-11-02 12:00:21.067434
BOT8: 52:54:00:f0:47:1d, 192.168.112.106 , Release in 2020-11-02 12:00:22.166141
BOT9: 52:54:00:d9:21:27, 192.168.112.101 , Release in 2020-11-02 12:00:23.237184
------------End of leases----------------
```

ולבסוף, דוגמא אחת לכתובת IP שתפסנו ואנחנו שומרים עליה (במצב persistent):

```
-----------persistent-----------
BOT9: 52:54:00:d9:21:27, 192.168.112.101 , Release in 0:02:59.999942

---------END OF persistent---------
```

[10] שורות 262-291