



دانشگاه آزاد اسلامی  
واحد دولت آباد  
دانشکده فنی و مهندسی

موضوع:

## آشنایی با فایروال iptables

مربوط به درس:

امنیت شبکه های کامپیوتری

استاد مربوطه:

دکتر مهدی فقیه ایمانی

گردآورندگان:

مرضیه عطایی ، پریسا شاه علی ، شهرزاد شوقی

تأمین امنیت شبکه، بخش حساسی از وظایف هر مدیر شبکه محسوب می شود. محافظت های متفاوتی مورد نیاز باشد، لذا مکانیزم های گوناگونی هم برای تأمین امنیت در شبکه وجود دارد. یکی از مکانیزم ها استفاده از دیوار آتش یا فایروال می باشد. مدیر شبکه باید درک بالایی از انواع دیوار آتش، نقاط قوت و ضعف هر نوع، حملات تهدید کننده ی هر نوع، معماری های دیوار آتش، تأثیرات بر شبکه و کاربران، سیاست امنیتی سازمان و همچنین نیازهای فنی پیاده سازی داشته باشد تا بتواند راه حل مناسب را انتخاب و به درستی پیاده سازی نماید و سپس آن را مورد آزمایش قرار دهد. در همین راستا، سیستم عامل Linux برای پیاده سازی نرم افزاری دیوار آتش فیلترکننده ی بسته، ابزاری را به نام iptables در اختیار کاربر قرار می دهد تا با استفاده از دستورات این ابزار بتواند قوانین و فیلترهای مورد نیاز را برای کنترل مطلوب دسترسی، خواه از داخل شبکه به خارج و خواه بالعکس، پیکربندی نماید.

فایروال iptables توسط پروژه ی netfilter توسعه یافته و از زمان linux با هسته ی 4.2 در ژانویه 4002 به عنوان قسمتی از linux در اختیار عموم قرار گرفته، طی سالها ویژگی iptables بهبود یافته و آن را به یک فایروال قدرتمند یا بیشتر قابلیت هایی که عموماً در فایروال های تجاری پیدا می شود تبدیل کرد. برای مثال iptables قابلیت های جامع ردیابی وضعیت پروتکل، بررسی کاربرد بسته ها توسط لایه، کاهش نرخ، و یک مکانیسم قدرتمند جهت تأمین نمودن یک سیاست فیلتر کردن را ارائه می دهد. تمامی نسخه های اصلی linux شامل iptables هستند و خیلی از این نسخه ها نیز از همان ابتدای نصب، کاربر را وادار به استفاده از یک سیاست iptables می کنند.

## مراحل نصب Linux Ubuntu در نرم افزار VMware Workstation

VMware Workstation قدرتمند ترین و معروف ترین ابزار موجود در زمینه مجازی سازی ویندوز به شمار می رود. کاربران به راحتی می توانند بدون این که کوچکترین صدمه ای به سیستم عامل خود وارد نمایند، حجم ترین ابزار ها را بر روی یک سیستم مجازی نصب نمایند و به راحتی استفاده کنند.

یکی از گرافیکی ترین سیستم عامل های لینوکس نسخه Ubuntu است که بر پایه لینوکس Debian میباشد. در این نسخه بیشتر بر روی ظاهر و قابلیت های دسکتاپ آن تمرکز شده است.

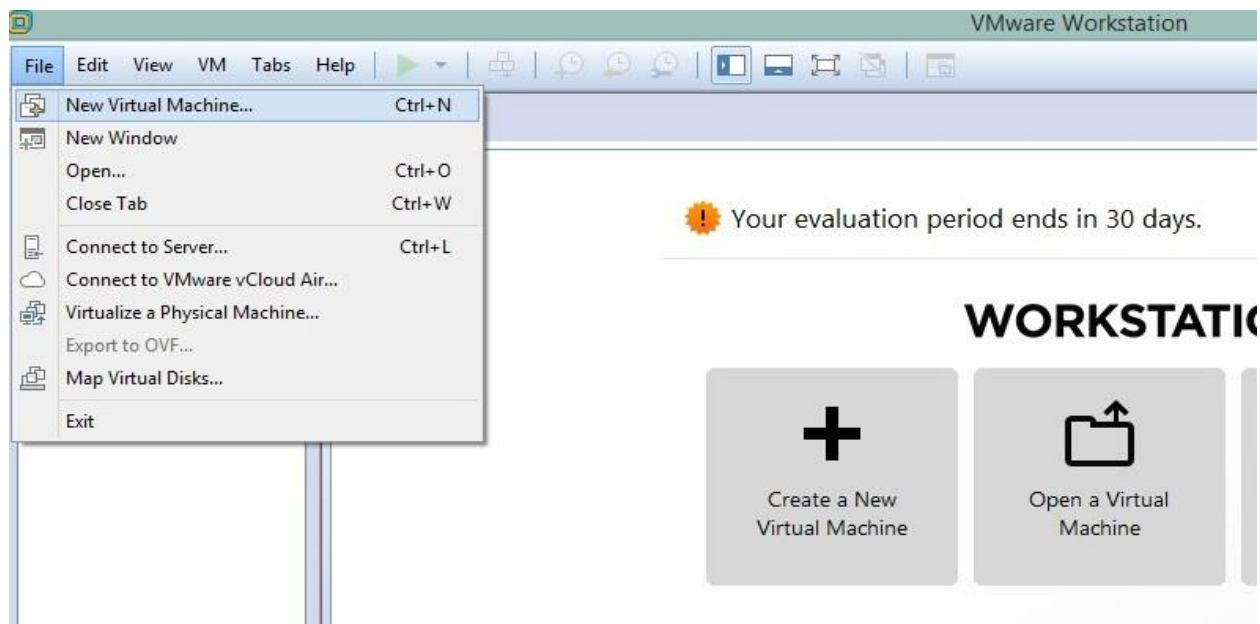
حداقل سیستم مورد نیاز برای نصب این سیستم عامل :

پردازنده : 1 گیگاهرتز

RAM : 1.5 گیگابایت

فضای هارد دیسک : 7 گیگابایت

این سیستم عامل را می توانید در کنار ویندوز نصب کنید. ولی توصیه می شود از برنامه VirtualBox یا VMware برای نصب این سیستم عامل و یادگیری و کار با آن استفاده کنید.



نرم افزار VMWare WorkStation را نصب کنید و آن را باز کنید و از منوی فایل گزینه new virtual machine را انتخاب کنید.



در پنجره جدید گزینه custom (advanced) را انتخاب کنید.

**New Virtual Machine Wizard**

**Choose the Virtual Machine Hardware Compatibility**  
Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware compatibility: Workstation 12.0

Compatible with: ☒ ESX Server

Compatible products:

- Fusion 8.x
- Workstation 12.0

Limitations:

- 64 GB memory
- 16 processors
- 10 network adapters
- 8 TB disk size

Help < Back Next > Cancel

**New Virtual Machine Wizard**

**Guest Operating System Installation**  
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:

DVD RW Drive (F:)

☐ Installer disc image file (iso):

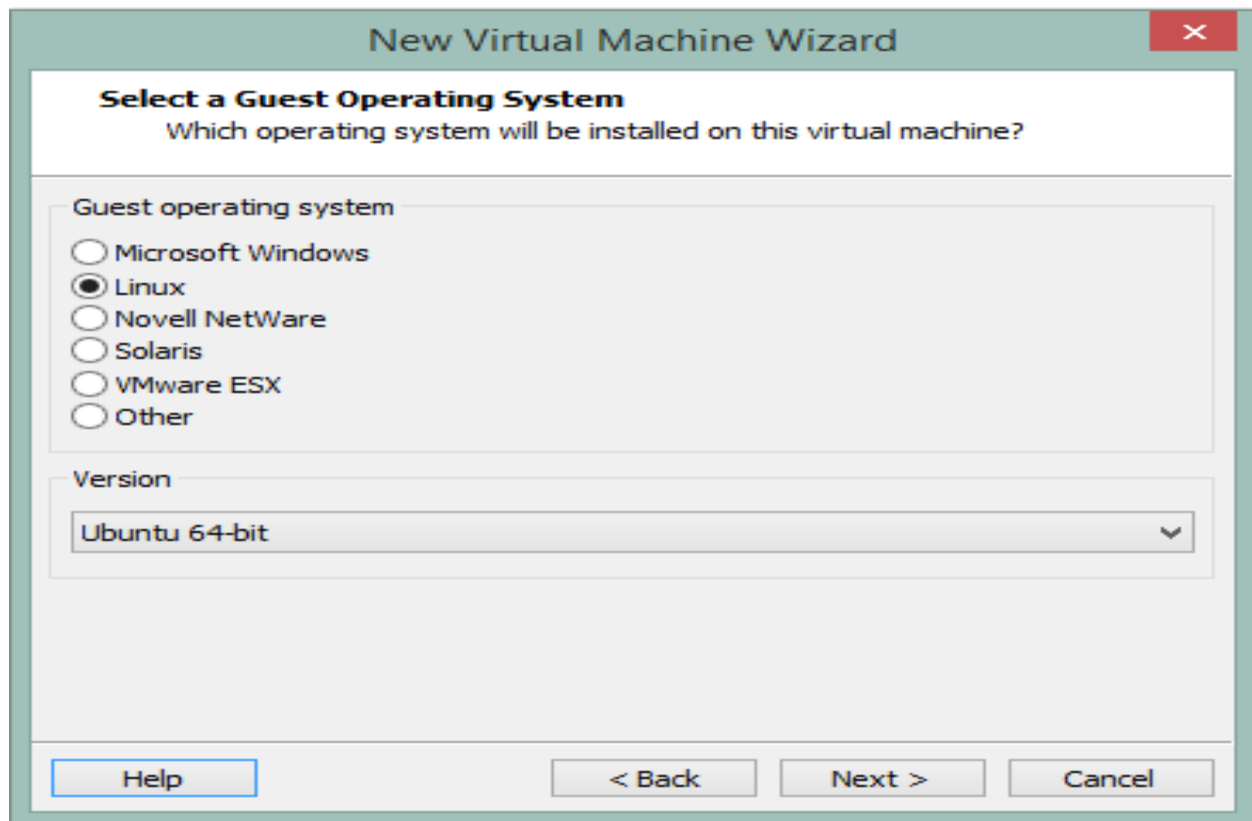
Browse...

☒ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

در صفحه ی Guest operating system installation روی گزینه ی آخر که I will install.... کلیک کنید و Next بزنید.



The image shows the 'New Virtual Machine Wizard' window, specifically the 'Select a Guest Operating System' step. The window has a title bar with a close button. The main heading is 'Select a Guest Operating System' with a subtitle 'Which operating system will be installed on this virtual machine?'. Below this, there is a section titled 'Guest operating system' containing a list of radio buttons: 'Microsoft Windows', 'Linux' (which is selected), 'Novell NetWare', 'Solaris', 'VMware ESX', and 'Other'. Below the radio buttons is a 'Version' section with a dropdown menu currently showing 'Ubuntu 64-bit'. At the bottom of the window are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

New Virtual Machine Wizard

**Select a Guest Operating System**  
Which operating system will be installed on this virtual machine?

Guest operating system

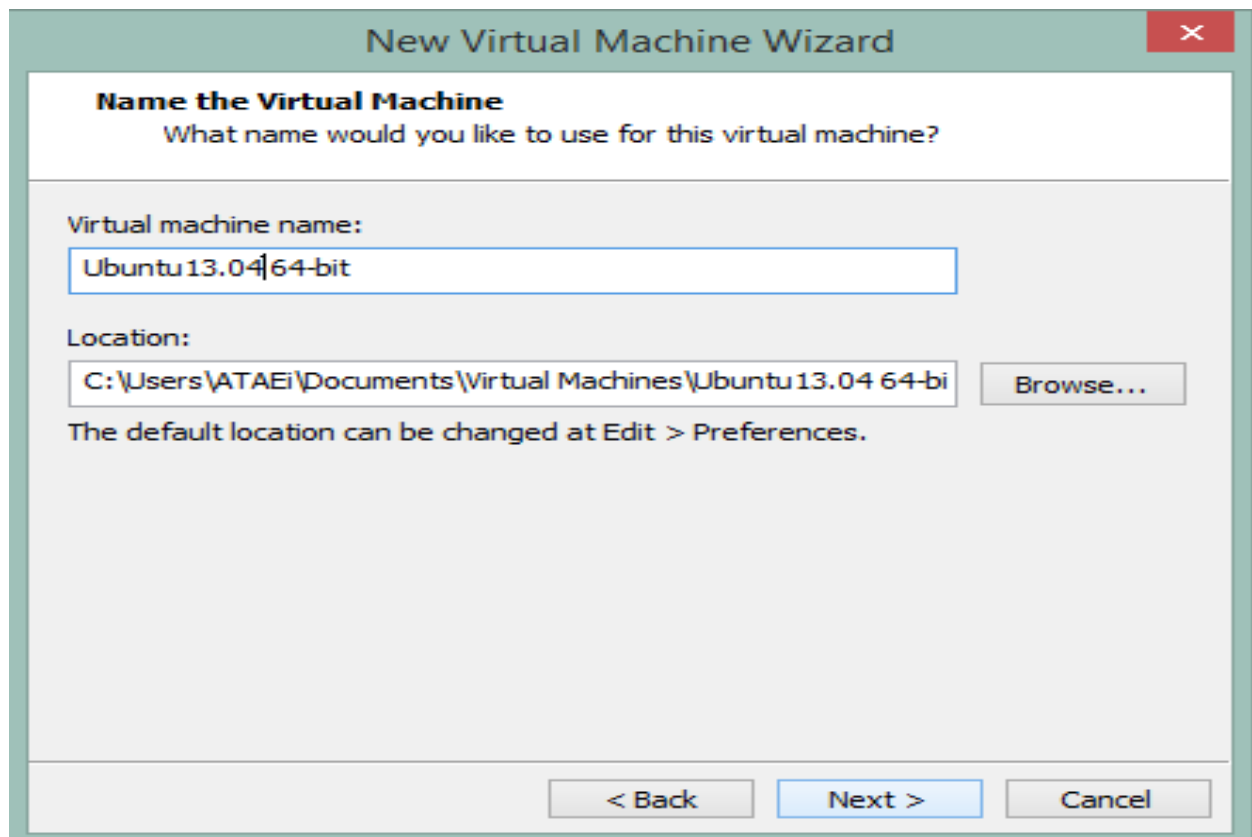
- ☐ Microsoft Windows
- ☒ Linux
- ☐ Novell NetWare
- ☐ Solaris
- ☐ VMware ESX
- ☐ Other

Version

Ubuntu 64-bit

Help < Back Next > Cancel

در صفحه Select a guest operating system در قسمت بالا روی گزینه linux کلیک کنید و در قسمت پایین که ورژن را مشخص میکند Ubuntu 64-bit را انتخاب کنید.



The image shows the 'New Virtual Machine Wizard' window, specifically the 'Name the Virtual Machine' step. The window has a title bar with a close button. The main heading is 'Name the Virtual Machine' with a subtitle 'What name would you like to use for this virtual machine?'. Below this, there is a 'Virtual machine name:' label followed by a text box containing 'Ubuntu13.04|64-bit'. Below that is a 'Location:' label followed by a text box containing 'C:\Users\ATAEI\Documents\Virtual Machines\Ubuntu13.04 64-bi' and a 'Browse...' button. A note at the bottom states 'The default location can be changed at Edit > Preferences.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

New Virtual Machine Wizard

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:

Ubuntu13.04|64-bit

Location:

C:\Users\ATAEI\Documents\Virtual Machines\Ubuntu13.04 64-bi Browse...

The default location can be changed at Edit > Preferences.

< Back Next > Cancel

New Virtual Machine Wizard

Processor Configuration

Specify the number of processors for this virtual machine.

Processors

Number of processors:

1

Number of cores per processor:

1

Total processor cores:

1

Help

< Back

Next >

Cancel

New Virtual Machine Wizard

Memory for the Virtual Machine

How much memory would you like to use for this virtual machine?

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

64 GB

32 GB

16 GB

8 GB

4 GB

2 GB

1 GB

512 MB

256 MB

128 MB

64 MB

32 MB

16 MB

8 MB

4 MB

Memory for this virtual machine:

1024

MB

Maximum recommended memory:

4744 MB

Recommended memory:

1024 MB

Guest OS recommended minimum:

512 MB

Help

< Back

Next >

Cancel

**New Virtual Machine Wizard**

**Network Type**  
What type of network do you want to add?

Network connection

☐ Use bridged networking  
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

☐ Use network address translation (NAT)  
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

☐ Use host-only networking  
Connect the guest operating system to a private virtual network on the host computer.

☒ Do not use a network connection

Help < Back Next > Cancel

در قسمت network type ارتباط ماشین با شبکه مشخص می شود که گزینه آخر را انتخاب کنید.

**New Virtual Machine Wizard**

**Select I/O Controller Types**  
Which SCSI controller type would you like to use?

I/O controller types

SCSI Controller:

☐ BusLogic (Not available for 64-bit guests)

☒ LSI Logic (Recommended)

☐ LSI Logic SAS

Help < Back Next > Cancel



New Virtual Machine Wizard

Select a Disk Type

What kind of disk do you want to create?

Virtual disk type

☐ IDE

☒ SCSI (Recommended)

☐ SATA

Help

< Back

Next >

Cancel

New Virtual Machine Wizard

Select a Disk

Which disk do you want to use?

Disk

☒ Create a new virtual disk

A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

☐ Use an existing virtual disk

Choose this option to reuse a previously configured disk.

☐ Use a physical disk (for advanced users)

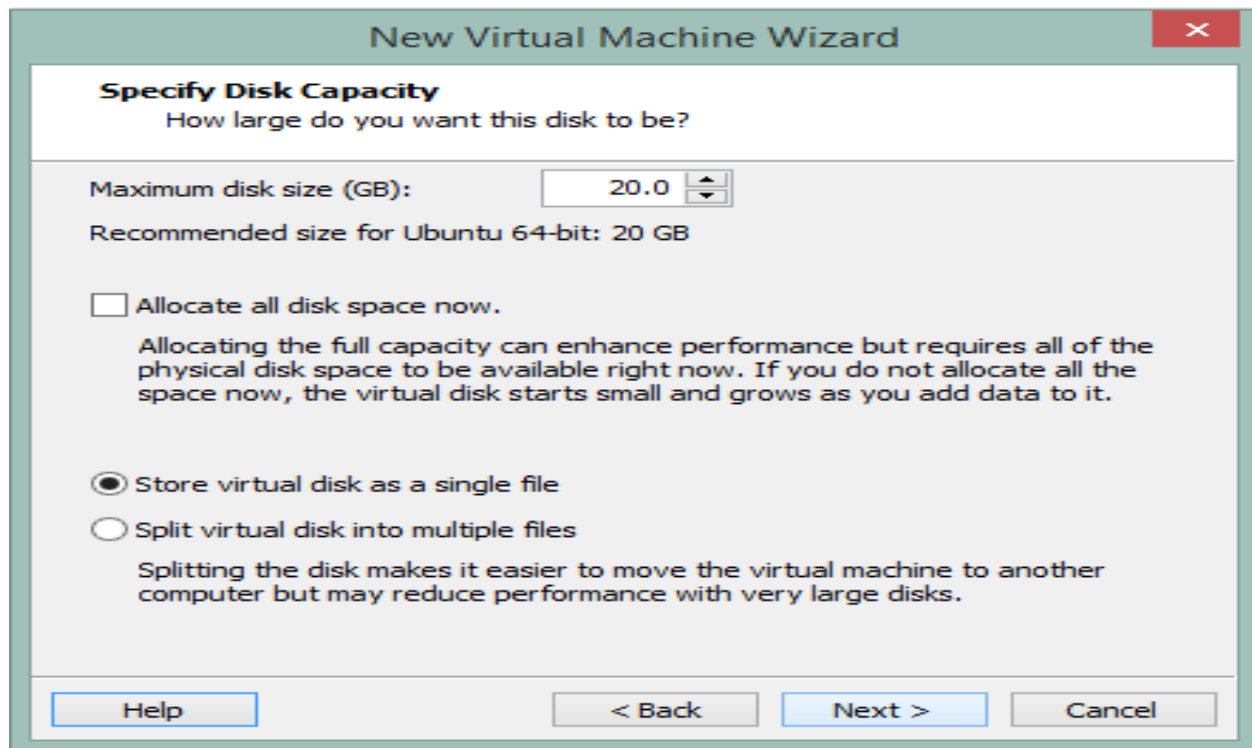
Choose this option to give the virtual machine direct access to a local hard disk.

Help

< Back

Next >

Cancel



The image shows the 'Specify Disk Capacity' step of the 'New Virtual Machine Wizard'. The title bar reads 'New Virtual Machine Wizard' with a close button. The main heading is 'Specify Disk Capacity' with the subtext 'How large do you want this disk to be?'. There is a text box for 'Maximum disk size (GB):' containing '20.0' and a spin button. Below it, it says 'Recommended size for Ubuntu 64-bit: 20 GB'. There are two radio button options: 'Allocate all disk space now.' (unchecked) and 'Store virtual disk as a single file' (checked). A descriptive paragraph explains that allocating full capacity enhances performance but requires all physical disk space. Another paragraph explains that splitting the disk makes it easier to move but may reduce performance. At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

**Specify Disk Capacity**  
How large do you want this disk to be?

Maximum disk size (GB): 20.0

Recommended size for Ubuntu 64-bit: 20 GB

☐ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

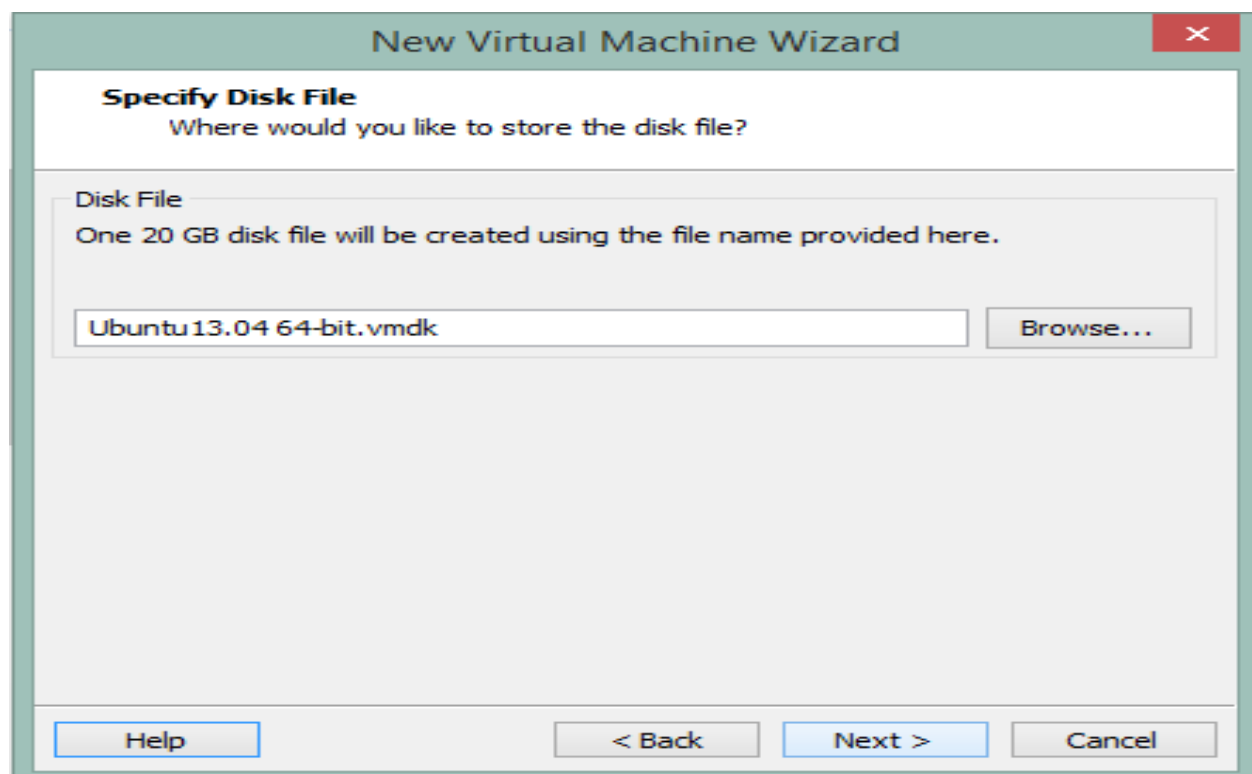
☒ Store virtual disk as a single file

☐ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help < Back Next > Cancel

در قسمت Specify disk capacity مطابق شکل زیر عمل کنید. اگر گزینه allocate all... را انتخاب کنید ماشین مجازی از همان اول تمام فضای اختصاص یافته را که خودتان مشخص کرده اید بر می دارد ولی اگر تیک این گزینه را بر دارید ماشین مجازی در صورت نیاز هر چقدر نیاز داشته باشد تا اندازه ماکزیممی که تعیین کرده اید از حافظه استفاده می کند.



The image shows the 'Specify Disk File' step of the 'New Virtual Machine Wizard'. The title bar reads 'New Virtual Machine Wizard' with a close button. The main heading is 'Specify Disk File' with the subtext 'Where would you like to store the disk file?'. There is a text box for 'Disk File' containing 'Ubuntu 13.04 64-bit.vmdk'. To the right of the text box is a 'Browse...' button. Below the text box, it says 'One 20 GB disk file will be created using the file name provided here.' At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

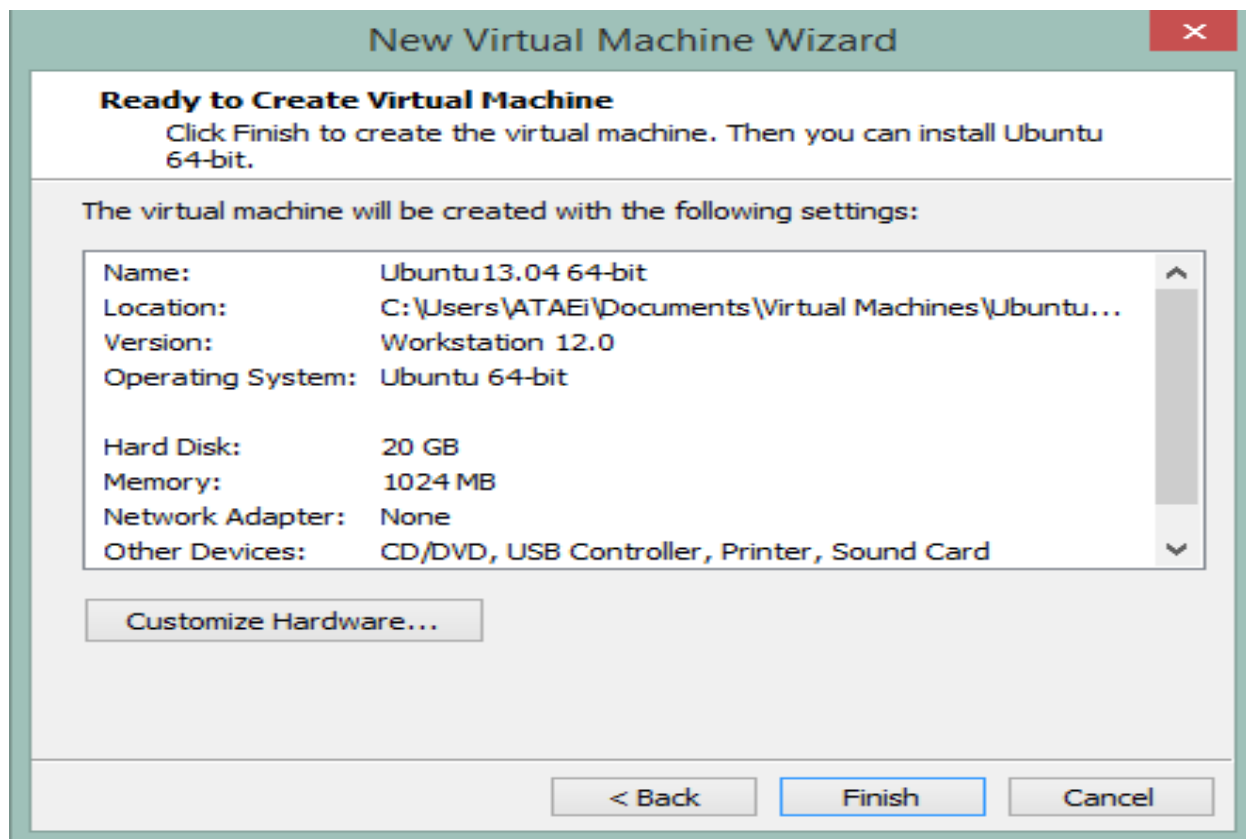
**Specify Disk File**  
Where would you like to store the disk file?

Disk File

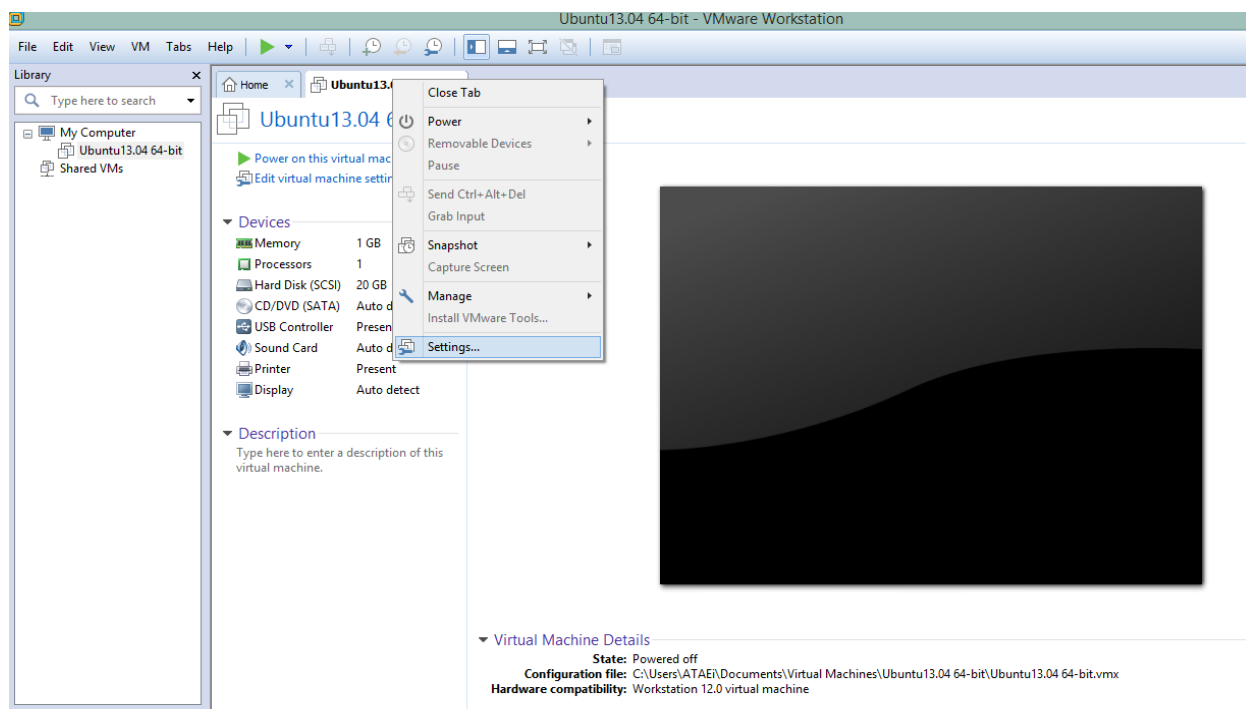
One 20 GB disk file will be created using the file name provided here.

Ubuntu 13.04 64-bit.vmdk Browse...

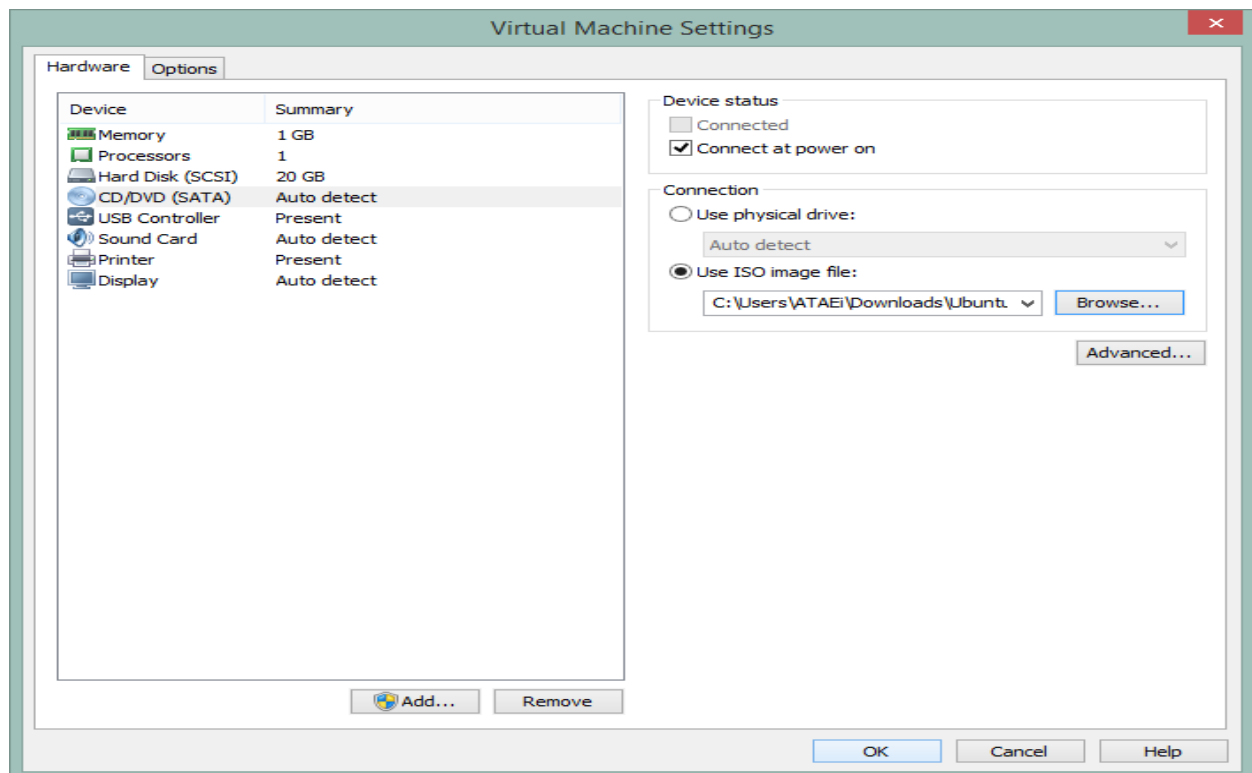
Help < Back Next > Cancel



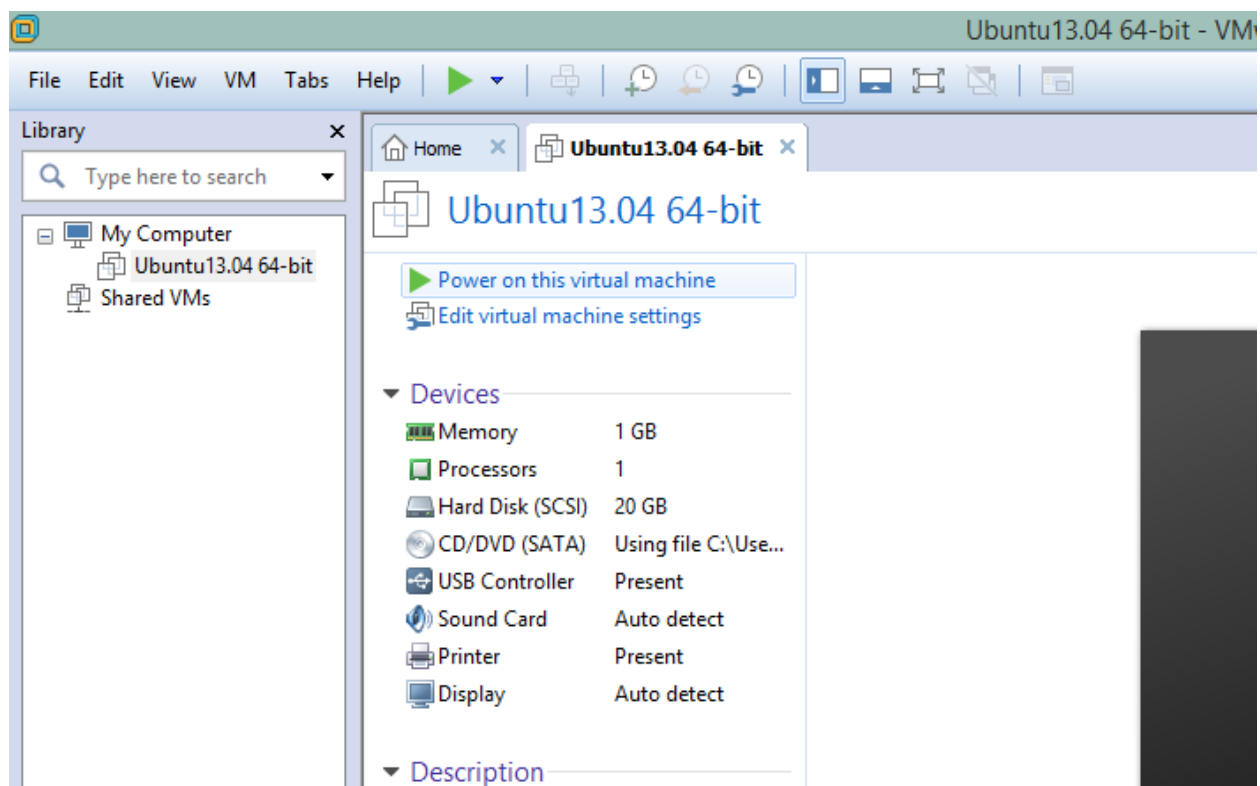
در نهایت با زدن finish ماشین مجازی آماده شده. تا اینجا کار تنها قسمت اول کار را که تهیه ماشین مجازی بود انجام داده ایم.



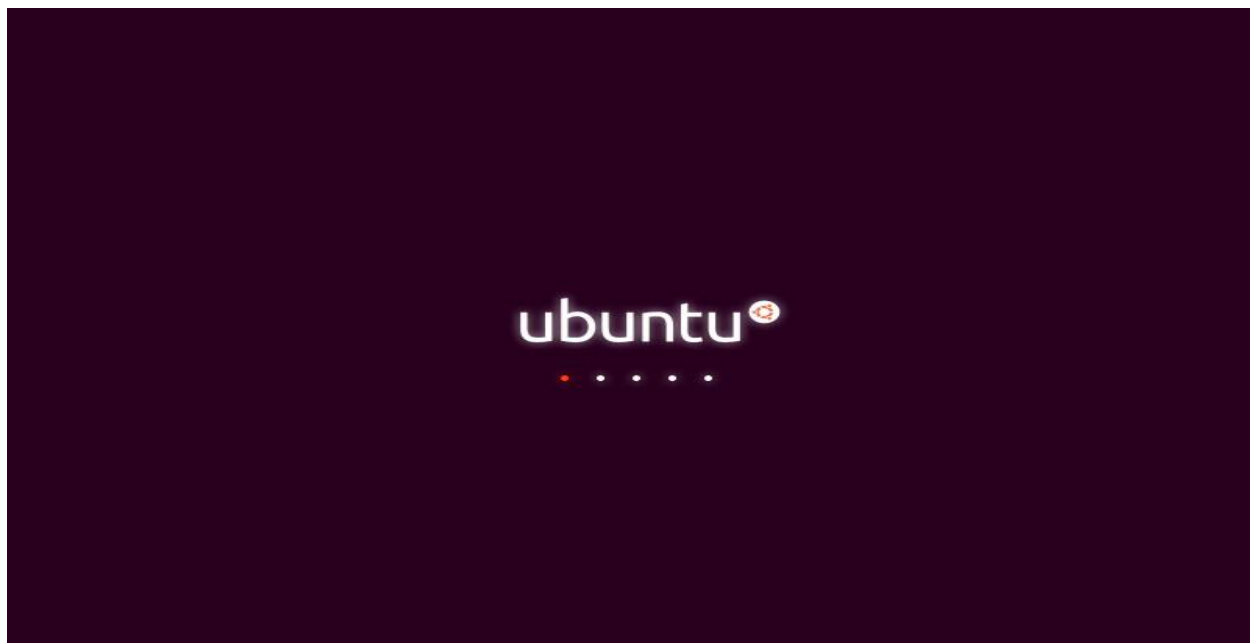
حالا نوبت نصب اوبونتوست. راست کلیک روی سربرگ ubuntu و گزینه setting را انتخاب کنید.



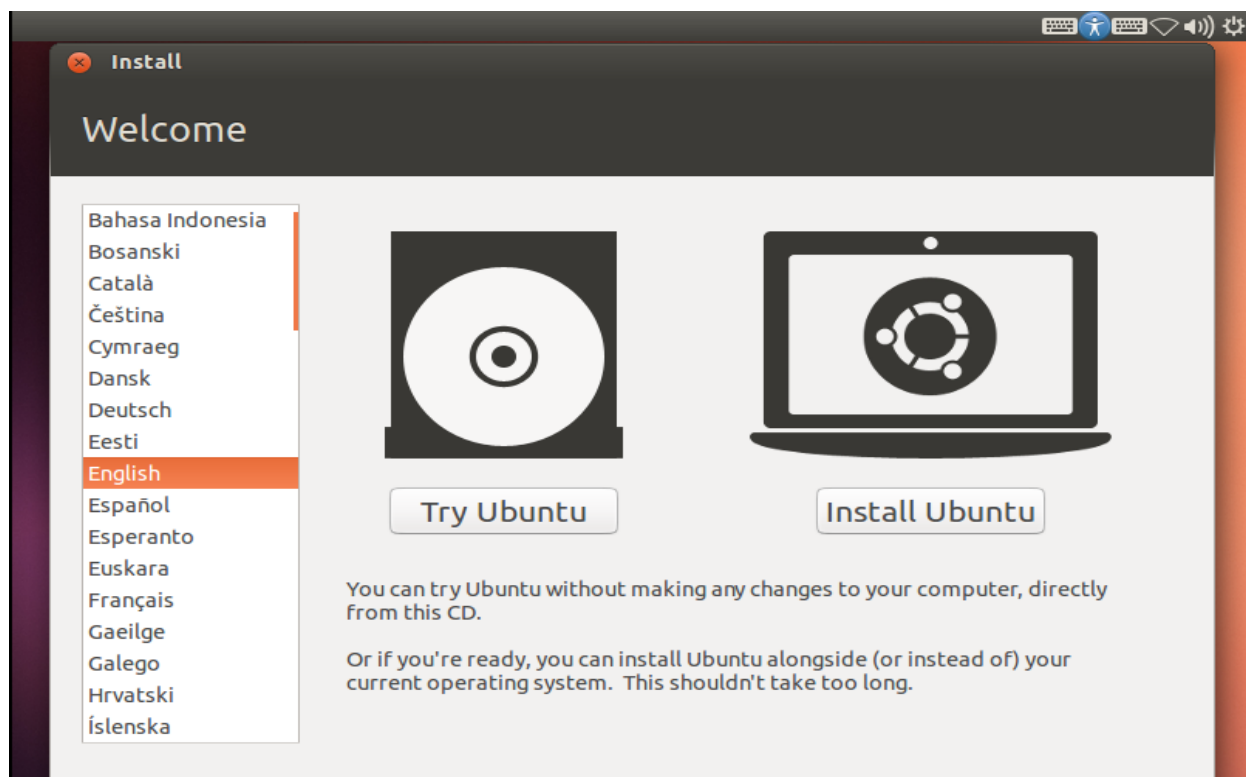
در صفحه جدید در قسمت use iso image file از قسمت browse فایل iso (فایلی اوبونتویی که قبلا دانلود کرده اید) را انتخاب کنید و همچنین تیک گزینه connect at power on را فعال کنید. سپس کلید ok را بزنید.



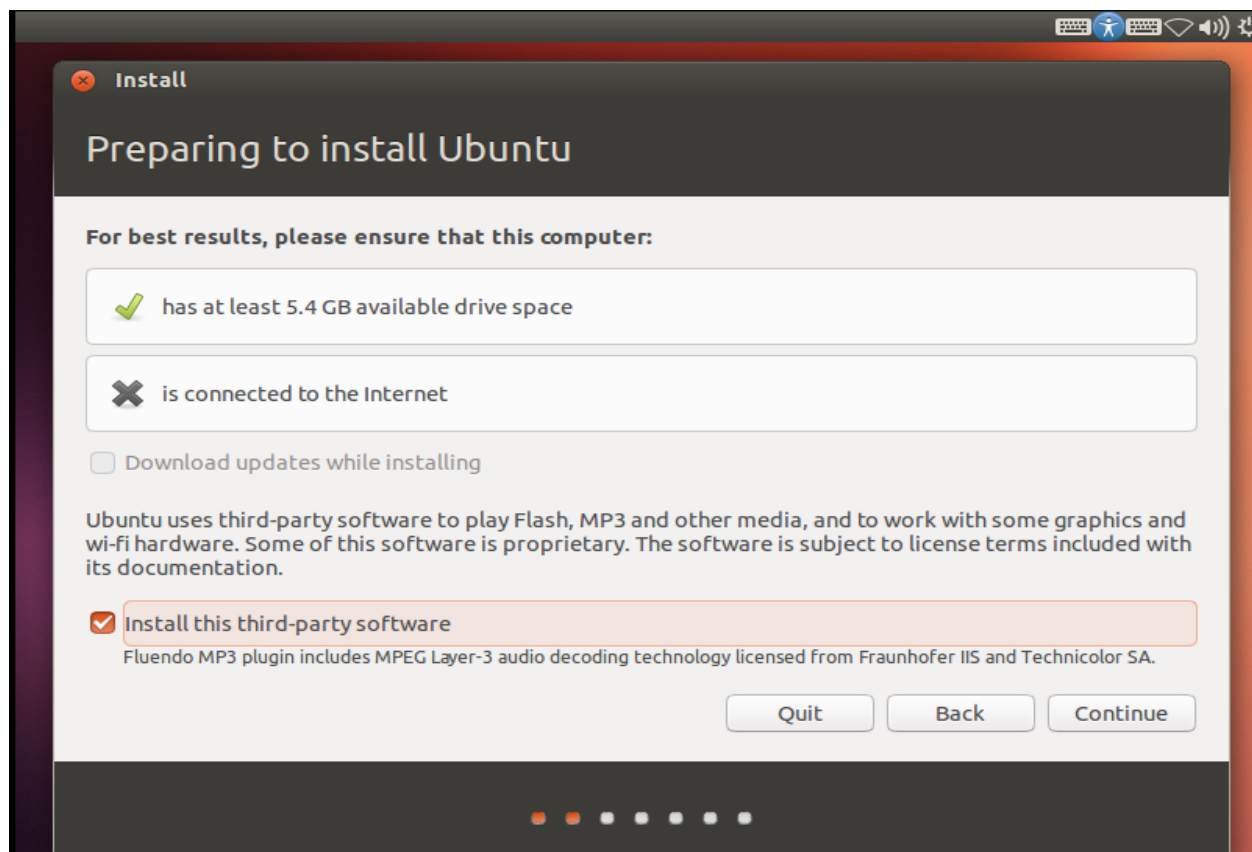
در ادامه برای ریست کردن دستگاه بر روی گزینه Power on this virtual machine کلیک می نمایم.



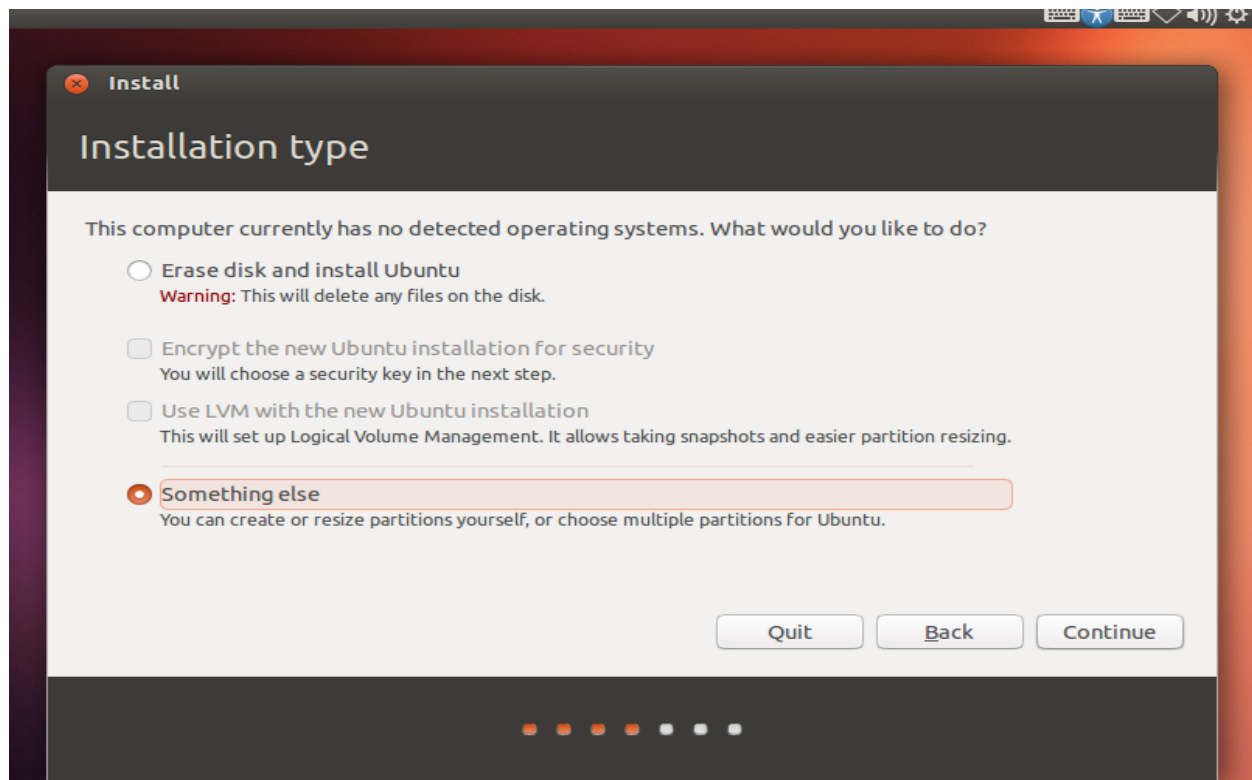
همانطور که می بینید سیستم بصورت مجازی ریست کرده و وارد مراحل نصب سیستم عامل می شود.



در اینجا باید زبان سیستم عامل را انتخاب کنید که ما در این مرحله زبان ENGLISH را انتخاب می کنیم. لینوکس این امکان را فراهم کرده تا قبل از نصب سیستم عامل بصورت Live سیستم را راه اندازی کنیم تا متوجه شویم که آیا با سخت افزار سیستم ما همخوانی دارد یا نه؟ برای این کار بر روی گزینه Try Ubuntu کلیک می نمائیم. در مرحله بعد که دسکتاپ Ubuntu قابل روید خواهد بود بر روی آیکون Install Ubuntu کلیک نمائید.

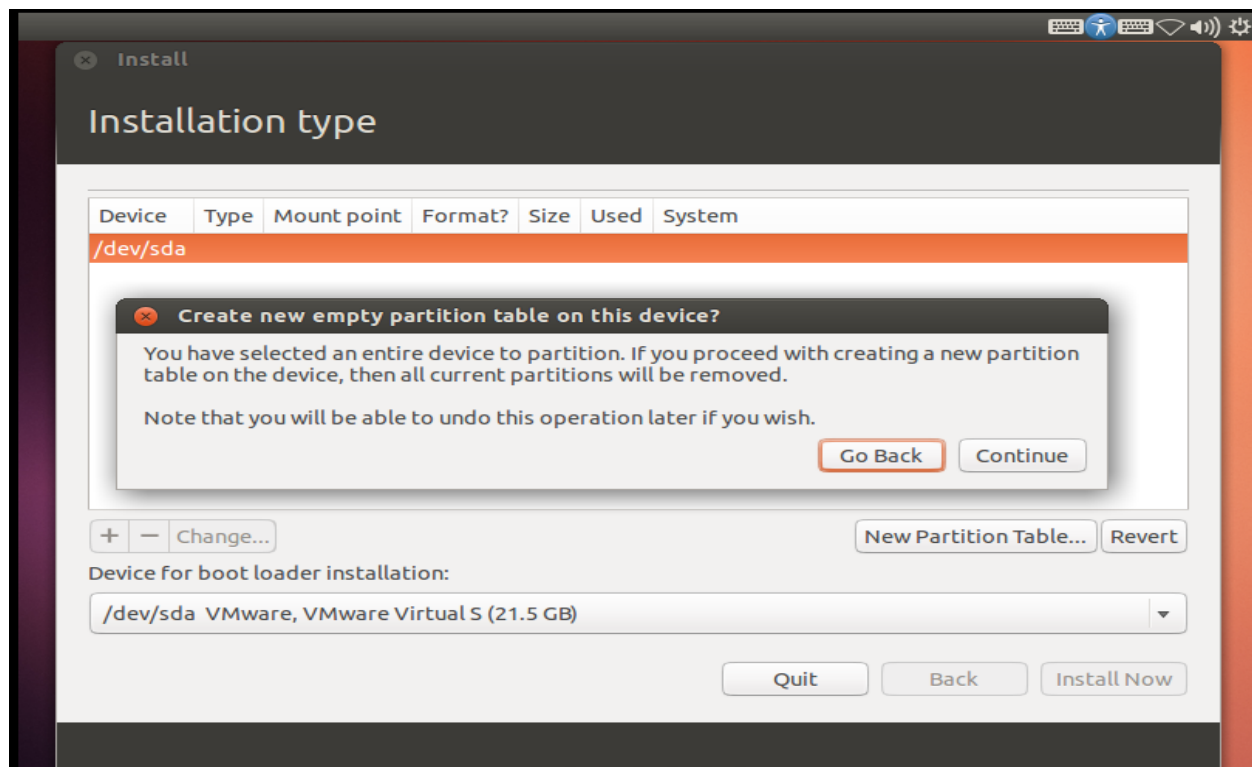


توجه داشته باشید در صورت اتصال به اینترنت مراحل نصب سیستم عامل لینوکس طولانی خواهد بود. زیرا تلاش خواهد کرد تا برنامه های خود را بروزرسانی نماید. به همین خاطر بهتر است که دسترسی به اینترنت را در زمان نصب قطع نمایید. بعد از نصب در صورت تمایل می توانید مراحل بروزرسانی را خودتان انجام دهید.

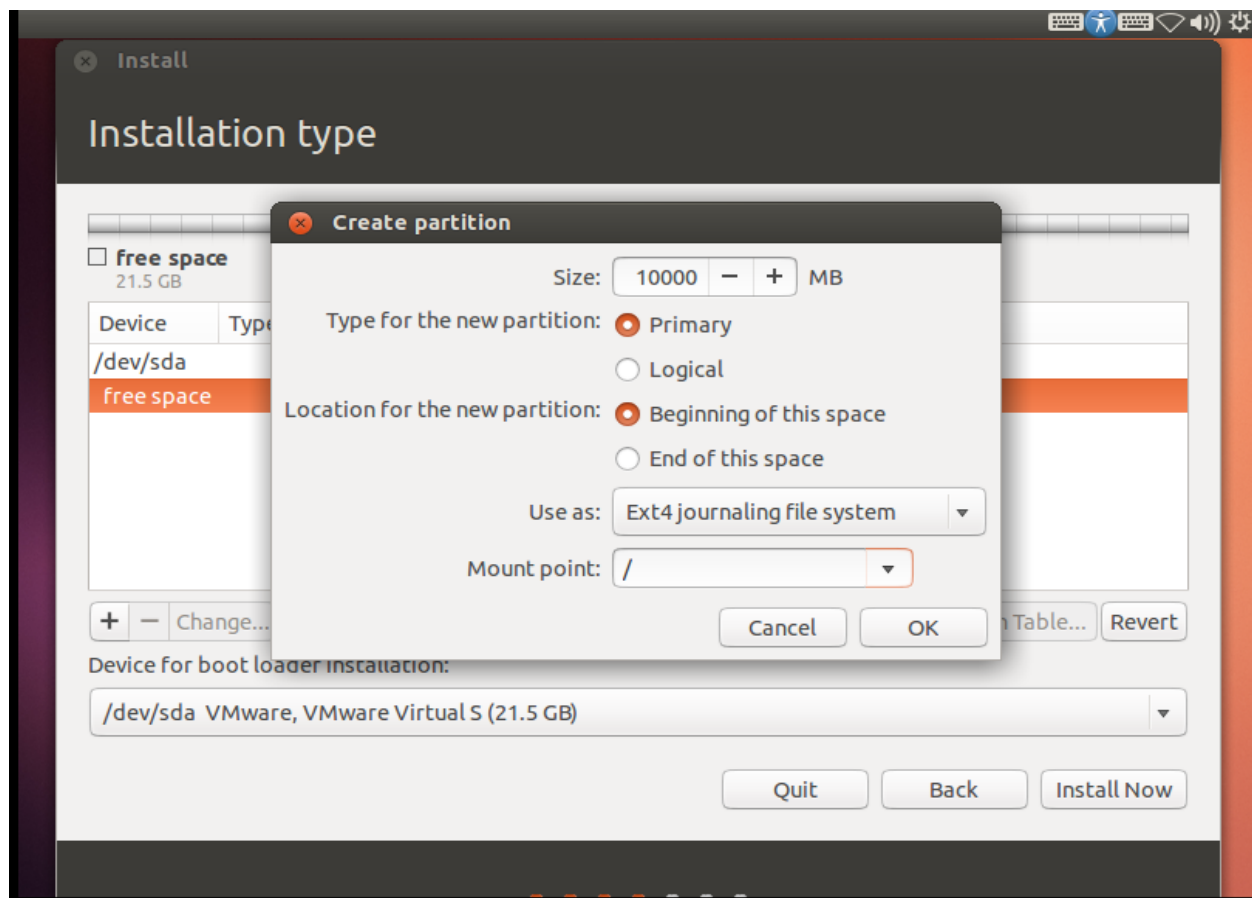


## Something else

با انتخاب این گزینه یک مرحله جدید پیش رو خواهیم داشت. این گزینه را در مواقعی که تاکنون سیستم عامل لینوکس نداشته و پارتیشن های مربوط و مخصوص به آن را ایجاد نکرده باشیم انتخاب می کنیم.



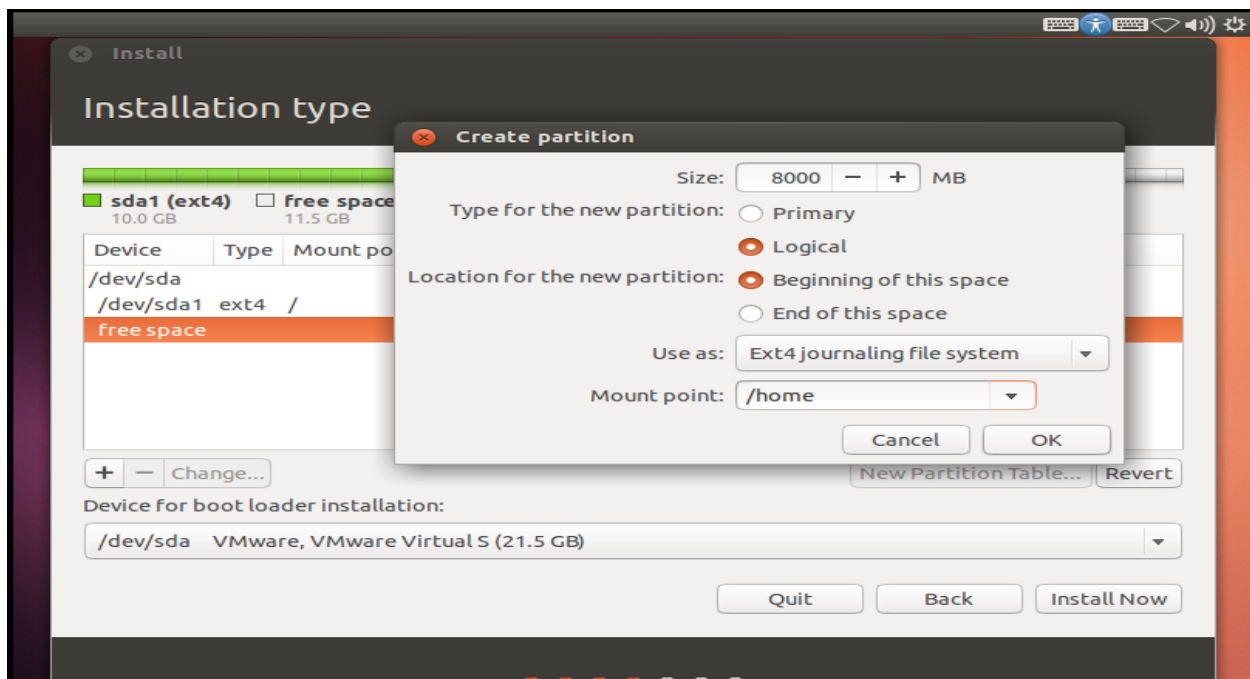
در این مرحله پیغام میدهد که آیا کل هارد پاک شود و سپس اوبونتو روی آن نصب شود یا خیر؟



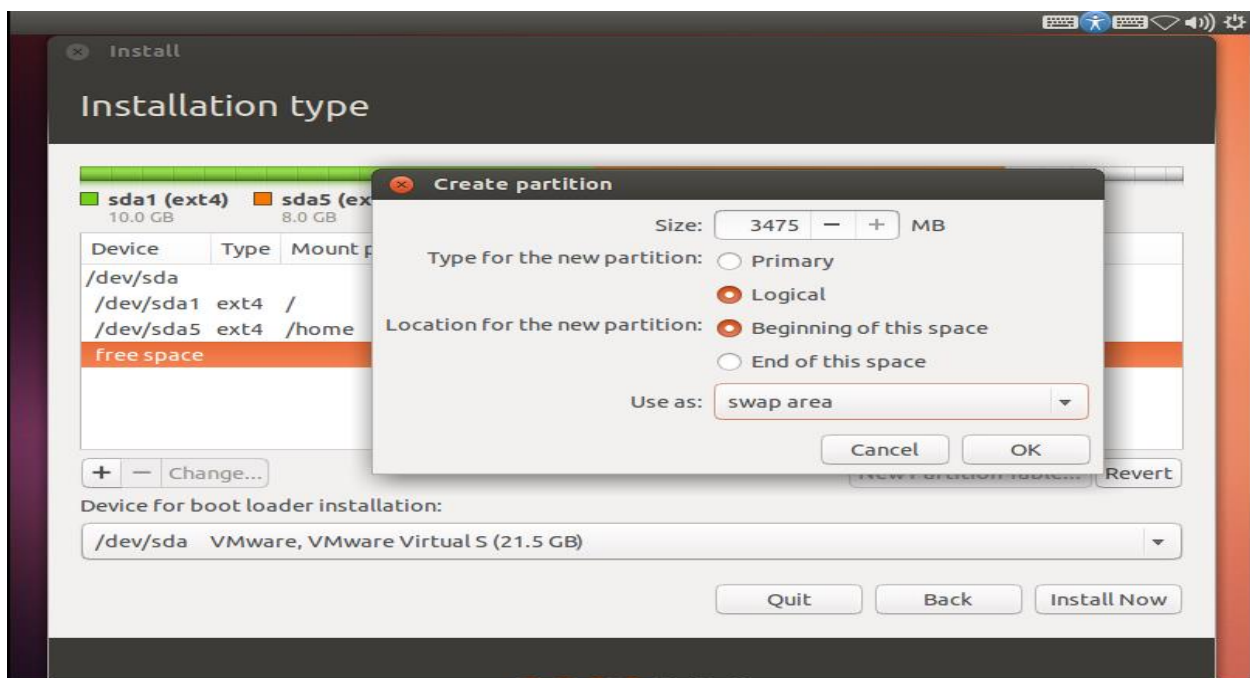
در این صفحه روی **free space** دابل کلیک می کنید. در این حالت دکمه **new partition table** را بزنید. باید صفحه ای مطابق تصویر ببینید:

فضا را 10 گیگ قرار می دهیم (10000 MB). در قسمت **use as** هم بگذارید در حالت **ext 4** قرار داشته باشد. فقط در قسمت **mount point** مطابق تصویر زیر "/" را بزنید. مدل پارتیشن بندی را **primary** قرار می دهیم.

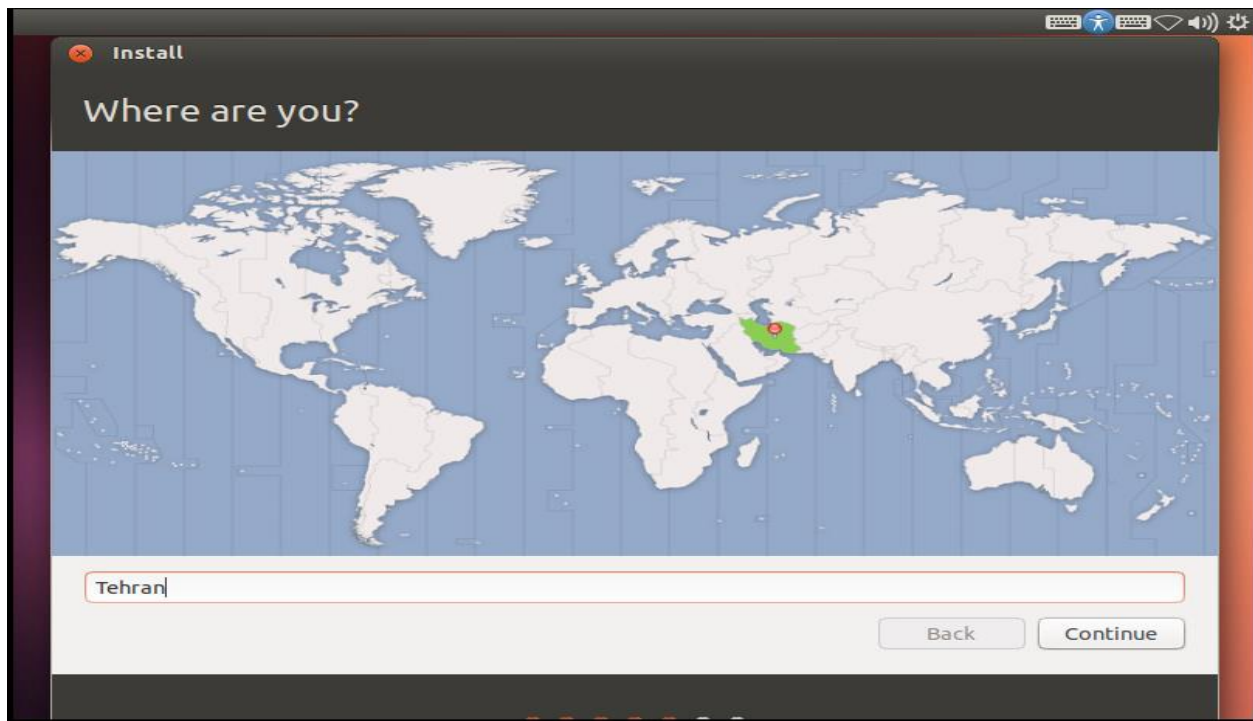




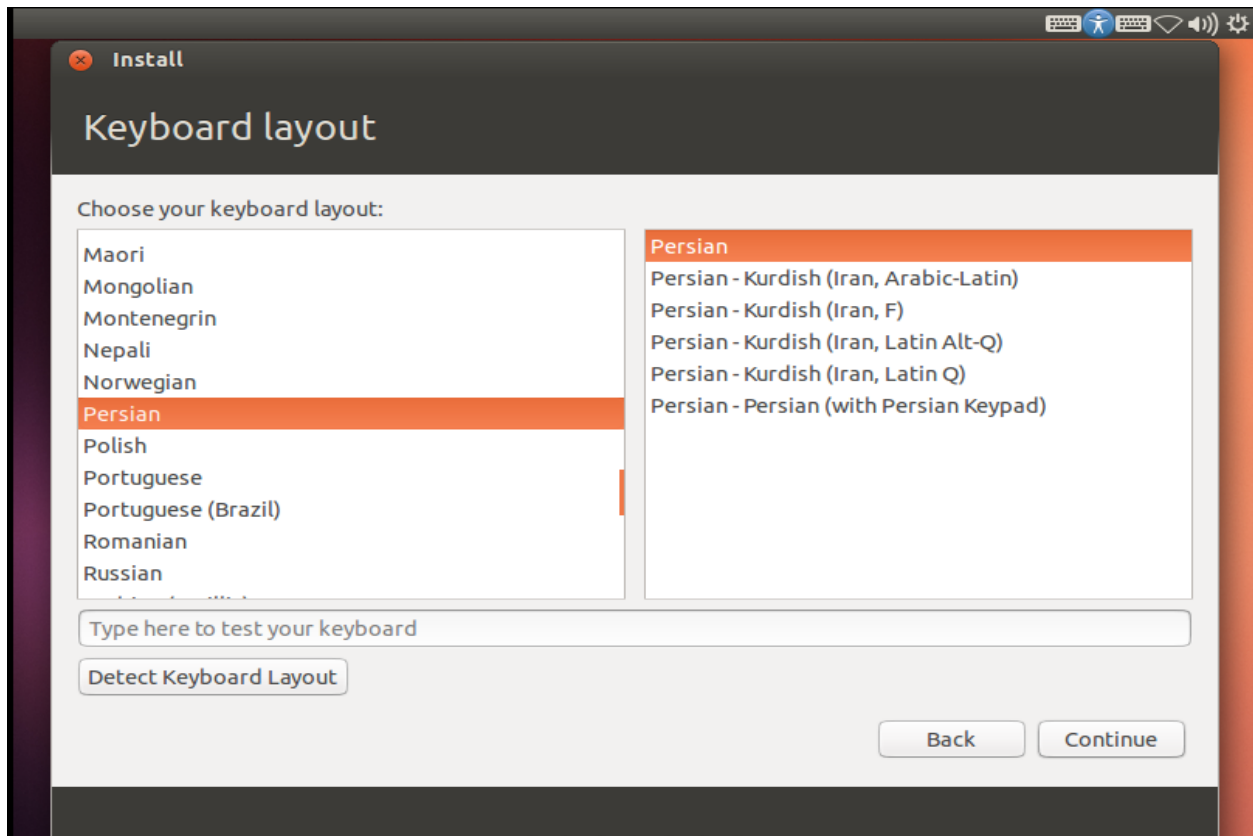
مانند مراحل پیش یک پارتیشن جدید می سازیم. فضا را 8 گیگ قرار می دهیم. در قسمت use as هم بگذارید در حالت ext 4 قرار داشته باشد. فقط در قسمت mount point مطابق تصویر زیر “/home” را بنزید. مدل پارتیشن بندی را logical قرار می دهیم.



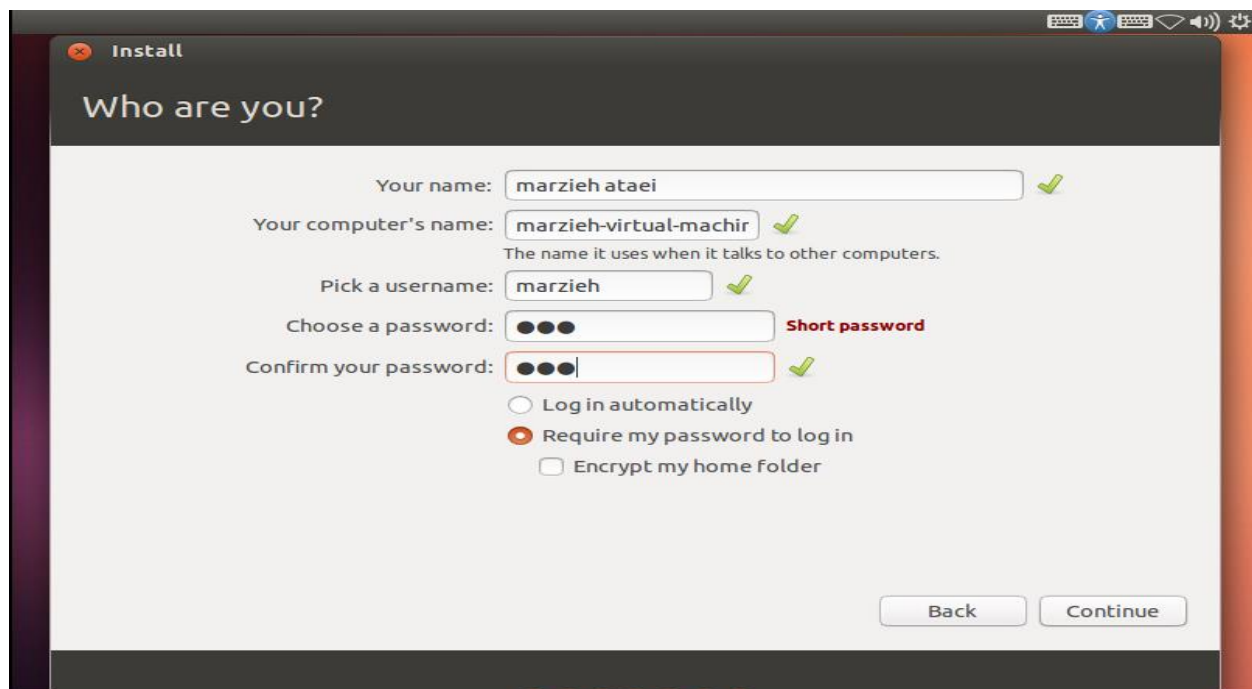
مانند مراحل پیش یک پارتیشن جدید می سازیم. این بار فضا را تغییر نمی دهیم. در قسمت use as در حالت swap area قرار داشته باشد. مدل پارتیشن بندی را logical قرار می دهیم. و در ادامه بر روی فضای ایجاد شده به عنوان Root کلیک کرده و بر روی کلید “install now” کلیک می نمائیم.



در مرحله بعد منطقه ی زمانی و شهر خود را انتخاب می نمائیم.  
در صورتی که به اینترنت متصل باشید این قسمت به صورت اتوماتیک انتخاب خواهد شد.



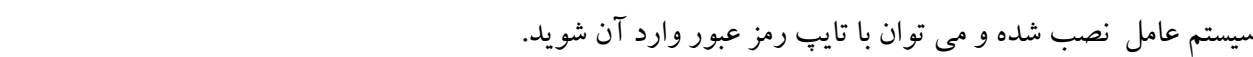
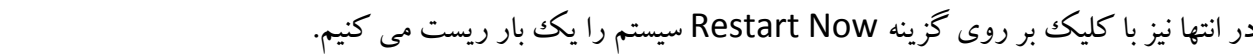
در این مرحله زبان صفحه کلید را انتخاب می کنیم.



در این صفحه یک نام و رمز عبور برای خود در نظر می گیریم.  
توجه داشته باشید که در صورت تیک زدن گزینه "encrypt my home folder" اطلاعات موجود در پوشه Home به صورت رمزنگاری شده خواهد بود.



در این مرحله لینوکس در حین نصب سیستم عامل بخش های مختلف لینوکس و همینطور قابلیت های آن را به شما معرفی می نماید. و شما با کلیک بر روی فلش کنار صفحه می توانید آنها را مشاهده کنید.





فایروال ها نقش مهمی در تامین امنیت سیستم ها و شبکه های لینوکسی ایفا می کنند. آنها با کنترل و مدیریت ترافیک شبکه های ورودی و خروجی بر اساس مجموعه ای از قوانین مانند یک محافظ امنیتی بین شبکه داخلی و خارجی عمل می کنند. مجموعه ای از قوانین فایروال تنها اجازه می دهد تا اتصالات و درخواست های مجاز از فایروال عبور کرده و آنهایی که تعریف نشده اند یا غیرمجاز تعریف شده اند مسدود می شوند. ده ها فایروال متن باز در دسترس مدیران شبکه ها و سیستم های لینوکسی قرار دارد که از آن جمله می توان به IpCop Shorewall , Iptables , UFW , Vuurmuur , pfSense , IPFire , SmoothWall , Endian و CSF اشاره کرد که در این مجال به بررسی iptables می پردازیم.

### Iptables

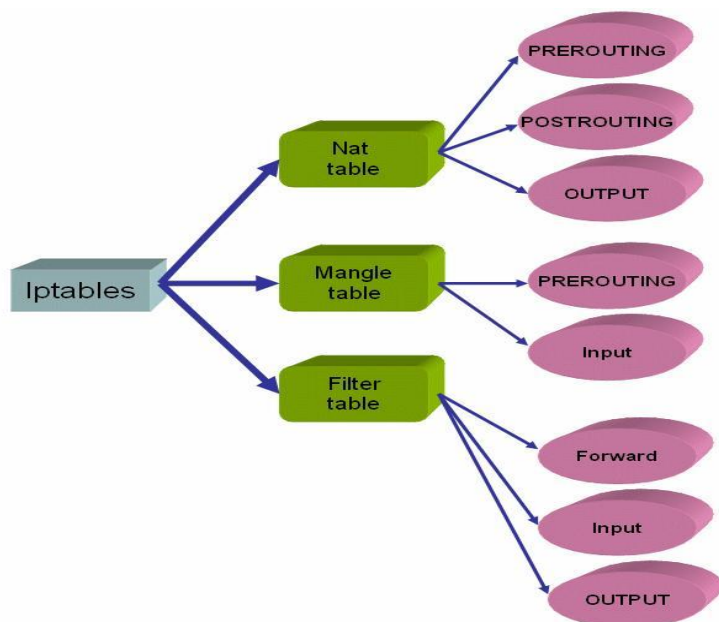
Iptables یا Netfilter محبوب ترین و پر استفاده ترین فایروال لینوکسی مبتنی بر خط فرمان است. و خط اول دفاعی سرورهای لینوکس است و بسیاری از مدیران سرورها از آن برای کانفیگ و ایجاد تنظیمات در سرورهای لینوکس استفاده می کنند.

Iptables بسته ها را درون پشته شبکه در داخل هسته لینوکس فیلتر می کند. و معمولا header هر بسته را بررسی می کند و به محتوای بسته اهمیتی نمی دهد بنابراین از سرعت بسیار زیادی برخوردار است و معمولا تاثیر چندانی در کاهش سرعت پاسخگویی سیستم ندارد، و همچنین قادر است یک رشته را درون بسته ها جستجو کند، البته این کار تا حدودی باعث کاهش سرعت سیستم خواهد شد.

iptables امکانات زیادی در اختیار یک مدیر سرور می دهد، بوسیله آن می توان پکت ها را بر اساس پروتکل مورد استفاده در ارتباط، شماره ip گیرنده و فرستنده، شماره پورت مورد در ارتباط، مک آدرس و آدرس فیزیکی سیستم ها، دامنه ای از آدرس های ip، زمان برقراری ارتباط، بخش های مختلفی از بسته ها و تنظیمات IPsec، طول بسته ها، انتخاب تصادفی بسته ها، انتخاب n امین بسته، کاربر یا گروه ارسال کننده بسته، پردازش ارسال کننده بسته، بخش های TOS و TTL هدر ip و تعداد ارتباطات در یک بازه زمانی را کنترل و فیلتر کرد.

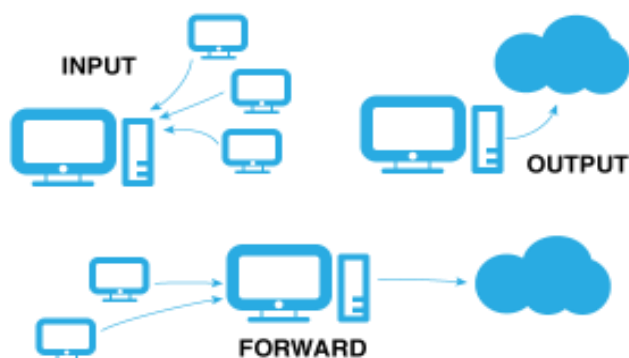
توسط iptables شما می توانید با توجه به نیاز های خود به ایجاد، حذف یا ویرایش قوانین فیلتر کردن بسته ها پردازید و حتی می توانید مجموعه قوانین جاری را بصورت لیست مشاهده کنید. iptables قابلیت انعطاف پذیری بالایی دارد و می توان با استفاده از آن نتایج کار آن را بر اساس هر قانون مشاهده یا ویرایش کرد. همچنین از قابلیت پشتیبان گیری و بازیابی قوانین با استفاده از فایل ها برخوردار است و از Load balancing نیز پشتیبانی می کند.

قوانین iptable بسته به نوع کاربرد در جداول filter table ، nat table و mangling table و در زنجیر (chain)هایی از دستورات دسته بندی می شوند.



### : Filter table

وظیفه آن سیاست گذاری و دادن مجوز برای ورود و خروج بسته های TCP/IP به سیستم است. این جدول شامل سه زنجیر INPUT برای ترافیک ورودی به سیستم، OUTPUT برای ترافیک خروجی از سیستم و FORWARD برای ترافیک فوروارد شده از سیستم است.





## : Nat table

وظیفه آن سیاست گذاری و دادن مجوز عملیات routing است و قوانین مربوط به تغییر آدرس IP و یا پورت در جدول nat قرار می گیرند. این جدول شامل سه زنجیر PREROUTING برای شبکه مقصد در ترافیک ورودی به سیستم ، POSTROUTING برای شبکه مبدا ترافیک خروجی از سیستم و OUTPUT است.

## : Mangle table

از جدول mangle می توان برای مارک دار کردن بسته ها و عملیات بررسی بسته ها قبل از ورود به جداول بالاتر استفاده کرد . کلیه اعمال پیشرفته مربوط به دستکاری فیلدهای header در بسته های ارسالی در شبکه توسط قوانین موجود در این جدول صورت می گیرد.

TABLE	INPUT	OUTPUT	FORWARD	PRE-ROUTING	POST-ROUTING
FILTER	✓	✓	✓	X	X
NAT	X	✓	X	✓	✓
MANGLE	✓	✓	✓	✓	✓

فایل های اصلی iptables :

( [/etc/init.d/iptables](#) ) اسکریپت init برای start/stop/restart و ذخیره مجموعه قوانین .

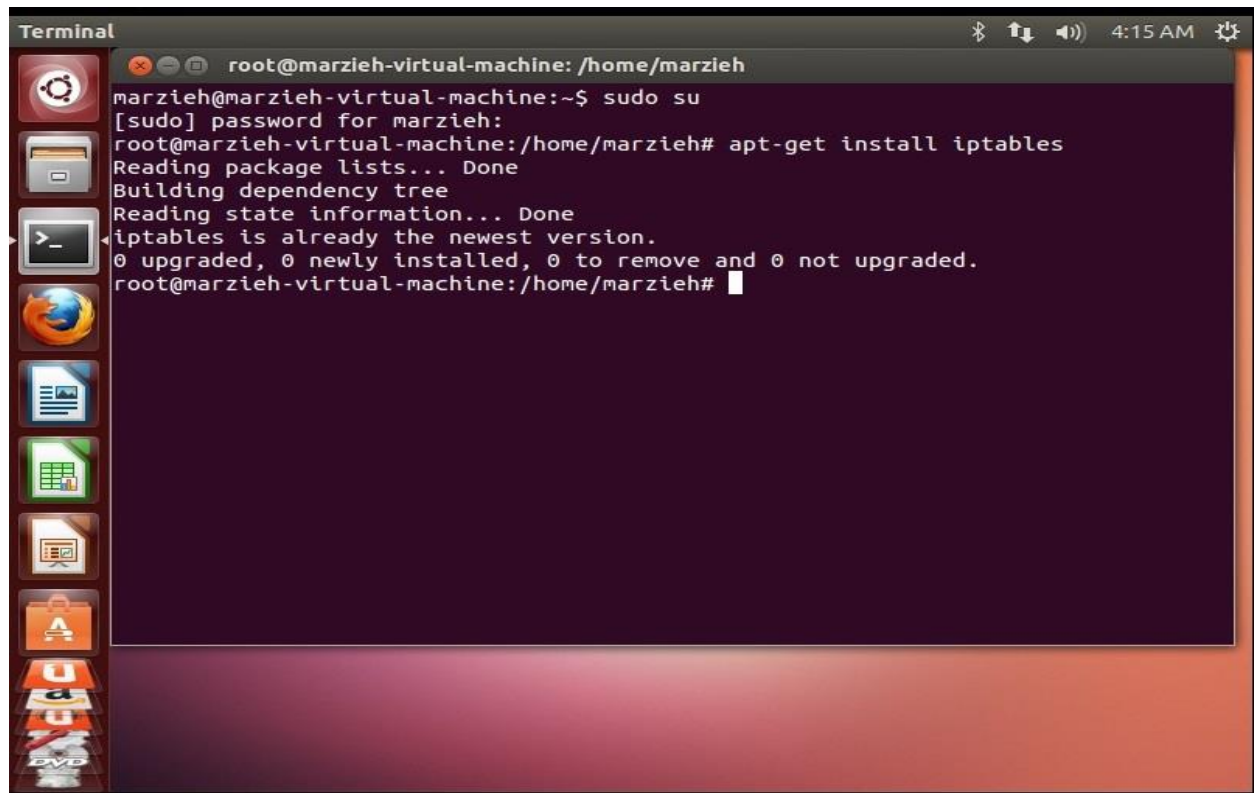
( [/etc/sysconfig/iptables](#) ) مکانی که مجموعه قوانین ذخیره میشوند .

( [/sbin/iptables](#) ) باینری

# مهم ترین و پرکاربردترین دستورات و تنظیمات iptables

## 1- طریقه نصب iptables :

```
# apt-get install iptables
```



```
Terminal
root@marzieh-virtual-machine: /home/marzieh
marzieh@marzieh-virtual-machine:~$ sudo su
[sudo] password for marzieh:
root@marzieh-virtual-machine:/home/marzieh# apt-get install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@marzieh-virtual-machine:/home/marzieh#
```

➤ برای استارت کردن iptables به هنگام بوت سیستم دستور زیر را اجرا کنید:

کد PHP

```
#chkconfig --level 345 iptables on
```

## 2 - نمایش وضعیت فایروال:

شما می توانید دستور زیر را برای بررسی وضعیت iptables استفاده کنید:

```
# service iptables status
```

```
iptables: Firewall is not running
```



➤ با دستور زیر وضعیت iptables را چک میکنیم:

L- (مجموعه قوانین را list میکند.)

v- (نمایش جزئیات)

n- (به فرمت numeric نمایش میدهد.)

کد PHP

# iptables -L -n -v

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
6	396	ACCEPT	all	-				
-	*	*	0.0.0.0/0		0.0.0.0/0		state RELATED,ESTABLISHED	
0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0
0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0
0	0	ACCEPT	tcp	-				
-	*	*	0.0.0.0/0		0.0.0.0/0		state NEW tcp dpt:22	
0	0	REJECT	all	--	*	*	0.0.0.0/0	0.0.0.0/0 reject-

with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
0	0	REJECT	all	--	*	*	0.0.0.0/0	0.0.0.0/0 reject-

with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 5 packets, 588 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

```
Terminal
root@marzieh-virtual-machine: /home/marzieh
marzieh@marzieh-virtual-machine:~$ sudo su
[sudo] password for marzieh:
root@marzieh-virtual-machine:/home/marzieh# apt-get install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@marzieh-virtual-machine:/home/marzieh# service iptables status
iptables: unrecognized service
root@marzieh-virtual-machine:/home/marzieh# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

root@marzieh-virtual-machine:/home/marzieh#
```

➤ دستور زیر قوانین iptables را به همراه شمارنده خط نمایش میدهد. با کمک گزینه `--line-numbers` شما میتوانید قوانین را حذف یا اضافه کنید:

کد PHP

`# iptables -n -L -v --line-numbers`

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination
1	51	4080	ACCEPT	all	-				
-	*	*	0.0.0.0/0	0.0.0.0/0				state RELATED,ESTABLISHED	
2	0	0	ACCEPT	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0
3	0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0
4	0	0	ACCEPT	tcp	-				
-	*	*	0.0.0.0/0	0.0.0.0/0				state NEW tcp dpt:22	
5	0	0	REJECT	all	--	*	*	0.0.0.0/0	0.0.0.0/0 reject-

with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination
1	0	0	REJECT	all	--	*	*	0.0.0.0/0	0.0.0.0/0 reject-

with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 45 packets, 5384 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination
-----	------	-------	--------	------	-----	----	-----	--------	-------------

### 3- تغییر وضعیت فایروال :

➤ طریقه start,stop,restart کردن فایروال iptables :

کد PHP

# /etc/init.d/iptables start

# /etc/init.d/iptables stop

# /etc/init.d/iptables restart

### 4- اضافه کردن کارت شبکه :

نمایش کارت شبکه های فعال

#ifconfig -a

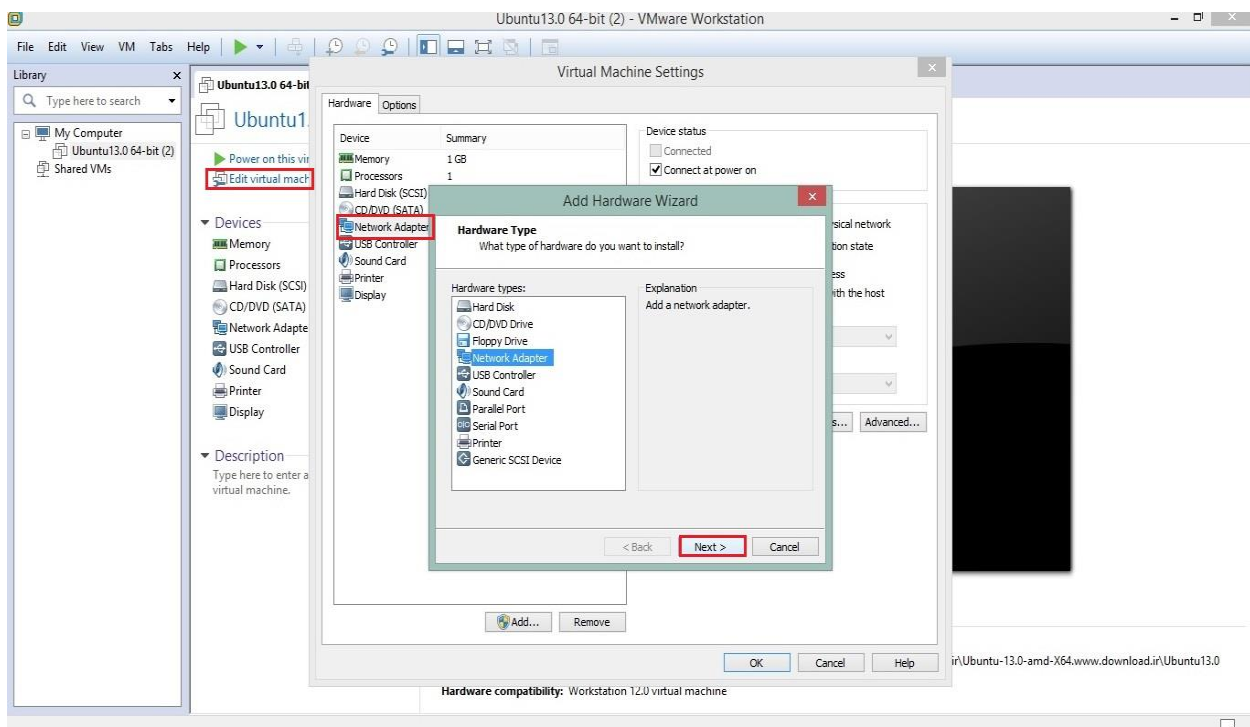
```
Terminal
root@marzieh-virtual-machine: /home/marzieh

marzieh@marzieh-virtual-machine:~$ sudo su
[sudo] password for marzieh:
root@marzieh-virtual-machine:/home/marzieh# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1e:c7:5e
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1e:c75e/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1507 errors:0 dropped:0 overruns:0 frame:0
          TX packets:398 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:214178 (214.1 KB)  TX bytes:76859 (76.8 KB)

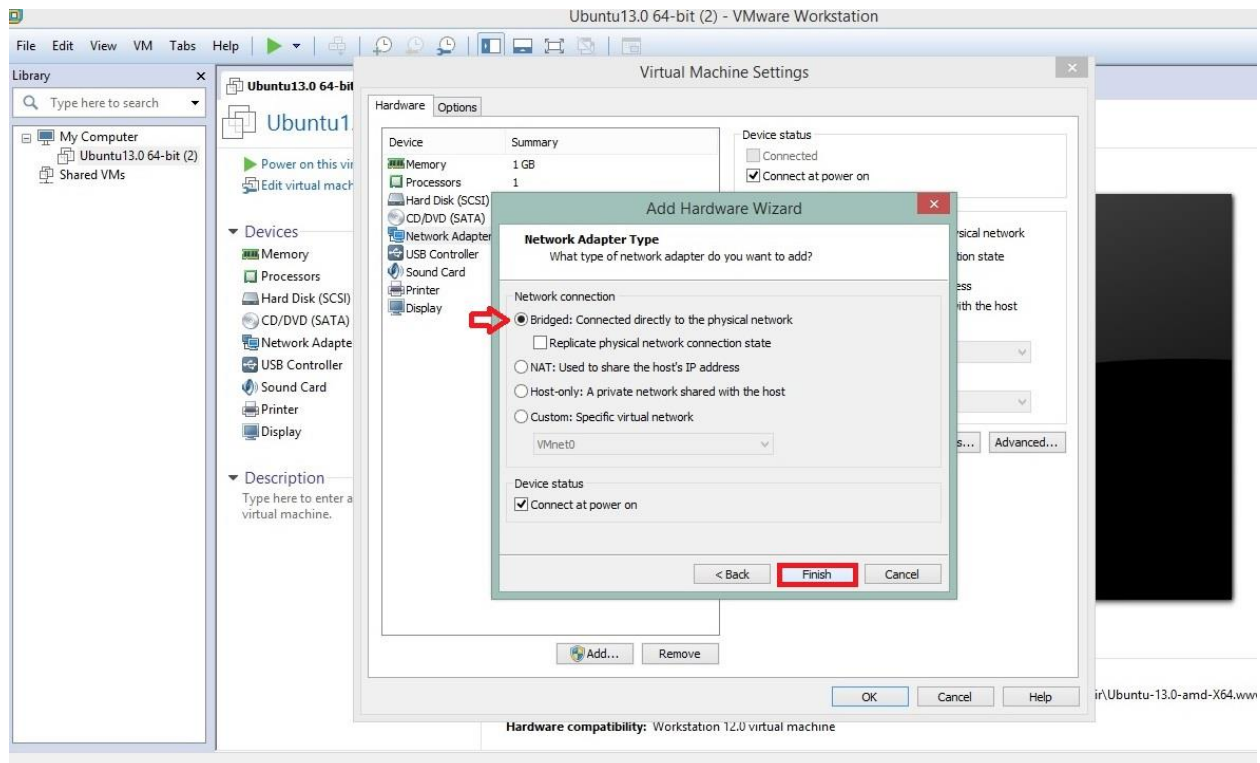
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:437 errors:0 dropped:0 overruns:0 frame:0
          TX packets:437 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31596 (31.5 KB)  TX bytes:31596 (31.5 KB)

root@marzieh-virtual-machine:/home/marzieh#
```

برای اضافه کردن کارت شبکه از لینوکس خارج شده و در محیط vmware، به صورت زیر کارت شبکه را اضافه می کنیم:







حال وارد ترمینال لینوکس می شویم و دوباره کد نمایش کارت شبکه های فعال را وارد می کنیم تا کارت شبکه اضافه شده ، نمایش داده شود:

#ifconfig -a

```

root@marzieh-virtual-machine: /home/marzieh
marzieh@marzieh-virtual-machine:~$ sudo su
[sudo] password for marzieh:
root@marzieh-virtual-machine:/home/marzieh# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1e:c7:5e
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1e:c75e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14659 (14.6 KB)  TX bytes:12300 (12.3 KB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:1e:c7:68
          inet addr:192.168.1.7  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1e:c768/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12432 (12.4 KB)  TX bytes:12037 (12.0 KB)

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:65536  Metric:1
          RX packets:83 errors:0 dropped:0 overruns:0 frame:0
          TX packets:83 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7626 (7.6 KB)  TX bytes:7626 (7.6 KB)

root@marzieh-virtual-machine:/home/marzieh#

```

## 5- حذف قوانین و رول های فایروال :

دستور زیر باید مجموعه قوانین را در chain های input و output به همراه شمارنده خطوط نمایش دهد که

کمک خواهد کرد بتوانیم قوانین را حذف یا اضافه کنیم:

ابتدا به کمک دستورات زیر شماره خط رول را بدست آورید:

➤ **Input :**

کد PHP

```
[root@tecmint ~]# iptables -L INPUT -n --line-numbers
```

Chain INPUT (policy ACCEPT)

num	target	prot	opt	source	destination
1	ACCEPT	all	-		
-	0.0.0.0/0			0.0.0.0/0	state RELATED,ESTABLISHED
2	ACCEPT	icmp	--	0.0.0.0/0	0.0.0.0/0
3	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0
4	ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0 state NEW tcp dpt:22
5	REJECT	all	--	0.0.0.0/0	0.0.0.0/0 reject-with icmp-host-prohibited

➤ **Output :**

کد PHP

```
[root@tecmint ~]# iptables -L OUTPUT -n --line-numbers
```

Chain OUTPUT (policy ACCEPT)

num	target	prot	opt	source	destination
-----	--------	------	-----	--------	-------------

➤ اگر بخواهیم قانون شماره 5 را از chain input حذف کنیم دستور زیر را باید اجرا کنیم:

کد PHP

```
[root@tecmint ~]# iptables -D INPUT 5
```

➤ برای وارد کردن یا اضافه کردن قانون به chain input بین rule شماره 4 و 5 دستور زیر را اجرا میکنیم:

کد PHP

```
[root@tecmint ~]# iptables -I INPUT 5 -s ipaddress -j DROP
```

➤ flushing یا حذف کلیه رول ها از فایروال با دستور زیر انجام میشود. در حقیقت این دستور تمامی قوانین

را از جداول پاک میکند.

کد PHP

```
# iptables -F
```

## 6- نحوه مسدود کردن ترافیک ورودی ، خروجی و یا ورود در فایروال :

برای مسدود کردن کل ترافیک می توانید از دستورات زیر استفاده فرمائید ( دقت نمائید که این دستورات می تواند مانع از دسترسی شما به سرور گردد.):

```
# iptables -P INPUT DROP
```

```
# iptables -P OUTPUT DROP
```

```
# iptables -P FORWARD DROP
```

➤ برای ذخیره نمودن تغییرات اضافه شده در فایروال می توانید از دستور زیر استفاده فرمائید:

```
# service iptables save
```

## 7- نحوه مسدود نمودن یک IP بر روی سرور :

به کمک دستورات اول شما می توانید ترافیک ورودی از سوی ای پی 1.2.3.4 و به وارد کردن دستور دوم کل ترافیک ورودی برای رنج ای پی مورد مثال مسدود می گردد.

```
# iptables -A INPUT -s 1.2.3.4 -j DROP
```

```
# iptables -A INPUT -s 192.168.0.0/24 -j DROP
```

## 8- نحوه مسدود کردن ترافیک ورودی بر روی یک پورت خاص :

➤ به کمک دستورات زیر می توان ترافیک ورودی را بر روی پورت 80 مسدود نمائید. لازم به توضیح است که معمولا وب سرور از پورت 80 برای نمایش وب سایت استفاده می کند.

```
# iptables -A INPUT -p tcp --dport 80 -j DROP
```

```
# iptables -A INPUT -i eth1 -p tcp --dport 80 -j DROP
```

➤ برای مسدود کردن ترافیک ورودی بر روی پورت 80 تنها برای یک IP و یا یک رنج IP می توانید از دستورات زیر استفاده فرمائید:

```
# iptables -A INPUT -p tcp -s 1.2.3.4 --dport 80 -j DROP
```

```
# iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --dport 80 -j DROP
```



## 9- نحوه مسدود نمودن ترافیک خروجی:

برای مسدود نمودن ترافیک خروجی برای یک IP خاص و یا یک رنج IP می توانید از دستورات زیر استفاده فرمائید:

```
# iptables -A OUTPUT -d 1.2.3.4 -j DROP
```

```
# iptables -A OUTPUT -d 192.168.1.0/24 -j DROP
```

```
# iptables -A OUTPUT -o eth1 -d 192.168.1.0/24 -j DROP
```

### مثال:

به عنوان مثال مایل هستیم که اجازه ندیم به هیچ کامپیوتری که سرور ما رو PING کنه یعنی اصطلاحاً می خوایم PING رو ببندیم...

برای این کار باید به ترافیک پروتکل ICMP اجازه ورود ندهیم... برای این منظور باید به صورت زیر عمل کنیم:  
با مجوز کاربر ROOT وارد سیستم شوید.  
فرمان زیر رو اجرا کنید:

```
#iptables -A INPUT -p ICMP -j DROP
```

فرمان فوق میگه که در انتهای ( بخاطر استفاده از سویچ A یعنی ( Append زنجیر ) INPUT یعنی ترافیک ورودی) پروتکل ICMP را DROP کن.

نوع پروتکل رو با سویچ -p مشخص می کنیم که در جلوی این سویچ می تونیم موارد TCP ، UDP ، ICMP و all رو بنویسیم.

برای مشخص کردن نحوه برخورد با ترافیک مورد نظر از سویچ -j استفاده می کنیم به معنی jump به موارد DROP ، LOG ، ACCEPT ، REJECT هستش. در اینجا تفاوتی که بین DROP و REJECT هست و اون هم این هستش که در DROP برای کاربر پیامی مبنی بر حذف بسته اش ارسال نمی شه ولی در REJECT به فرستنده پیام یک بسته عدم قبول ترافیک ارسال میشه.

در این قسمت با دو سویچ مهم از IPTABLES آشنا می شویم:

سویچ S- و d- برای مشخص کردن source و destination در یک بسته TCP/IP به ترتیب از سویچ های معرفی شده استفاده می کنیم.

فرض کنید تصمیم داریم که به کاربران شبکه 192.168.1.0/24 اجازه دهیم شبکه 192.168.2.0/24 رو PING کنند برای این کار باید یک rule در chain مربوط به خروج ( OUTPUT ) بسته ها در جدول ..... اضافه کنیم:

**#iptables -A INPUT -p ICMP -s 192.168.1.0/24 -d 192.168.2.0/24 -j ACCEPT**

```
root@marzieh-virtual-machine: /home/marzieh
num target prot opt source destination
Chain FORWARD (policy ACCEPT)
num target prot opt source destination
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
root@marzieh-virtual-machine:/home/marzieh# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@marzieh-virtual-machine:/home/marzieh# iptables -A INPUT -p ICMP -j DROP
root@marzieh-virtual-machine:/home/marzieh# iptables -A INPUT -p ICMP -s 192.168.1.0/24 -d 192.168.2.0/24 -j ACCEPT
root@marzieh-virtual-machine:/home/marzieh# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
DROP icmp -- anywhere anywhere
ACCEPT icmp -- 192.168.1.0/24 192.168.2.0/24
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@marzieh-virtual-machine:/home/marzieh#
```

به همین سادگی می توانید منبع و مقصد یک بسته TCP/IP رو در فرامین خود مشخص کنید. بدیهی است که برای مشخص کردن یک آدرس خاص نیز می توان به همین روش استفاده کرد. مثلاً می خواهیم به ماشین admin شبکه اجازه دهیم که کل شبکه رو PING کند و بقیه ماشین ها این اجازه رو در شبکه 192.168.1.0/24 نداشته

باشن آدرس ماشین Admin برابر 192.168.1.2 می باشد:  
برای این منظور از دو عدد rule به صورت زیر استفاده می کنیم:

```
#iptables -A INPUT -p ICMP -s 192.168.1.0 -d 192.168.1.0/24 -j ACCEPT  
#iptables -A INPUT -p ICMP -s 192.168.1.0/24 -j REJECT
```

## 10- غیر فعال کردن فایروال :

اگر با مشکلی در دسترسی به فایروال روبرو هستید و یا فایروال مانع از کارکرد صحیح سرویس های اصلی سرور شما شده است می توانید به کمک دستورات زیر فایروال را خاموش نمائید. با استفاده از دستور دوم نیز پس از ریستارت سرور وضعیت به همین منوال باقی خواهد ماند و فایروال مجدداً فعال نمی گردد، مگر آنکه شما از نرم افزار جانبی مانند CSF استفاده کرده باشید که بدین ترتیب فایروال مجدداً فعال می گردد و بدین شکل قابلیت غیرفعال شدن نخواهد داشت:

```
# /etc/init.d/iptables stop  
# chkconfig iptables off
```

## سوئیچ ها و دستورات iptable

- A برای افزودن دستور به انتهای یک زنجیره از جدول قوانین استفاده می شود.
- I برای افزودن به مکان خاصی از زنجیره جدول قوانین استفاده می شود.
- D برای حذف دستور از مکان خاصی از زنجیره جدول قوانین استفاده می شود.
- R برای جایگزین کردن دستور جاری یا یک دستور در مکان خاصی از زنجیره جدول قوانین استفاده می شود.
- P برای مشخص کردن نوع پروتکل مورد استفاده قرار می گیرد.
- T برای مشخص کردن جدول مورد استفاده قرار می گیرد.
- S یا --source برای مشخص کردن شماره ip مبدا مورد استفاده قرار می گیرد.
- D یا --destination برای مشخص کردن شماره ip مقصد مورد استفاده قرار می گیرد.
- i یا --in-interface برای مشخص کردن کارت شبکه ورودی مورد استفاده قرار می گیرد.

o- یا out-interface-- برای مشخص کردن کارت شبکه خروجی مورد استفاده قرار می گیرد.

Sport-- برای مشخص کردن شماره پورت مبدا مورد استفاده قرار می گیرد.

dport-- برای مشخص کردن شماره پورت مقصد مورد استفاده قرار می گیرد.

L- برای لیست کردن قوانین موجود در یک زنجیر مورد استفاده قرار می گیرد.

N- برای ایجاد زنجیر جدید مورد استفاده قرار می گیرد.

X- برای حذف یک زنجیر مورد استفاده قرار می گیرد.

F- برای پاک کردن قوانین مورد استفاده قرار می گیرد.