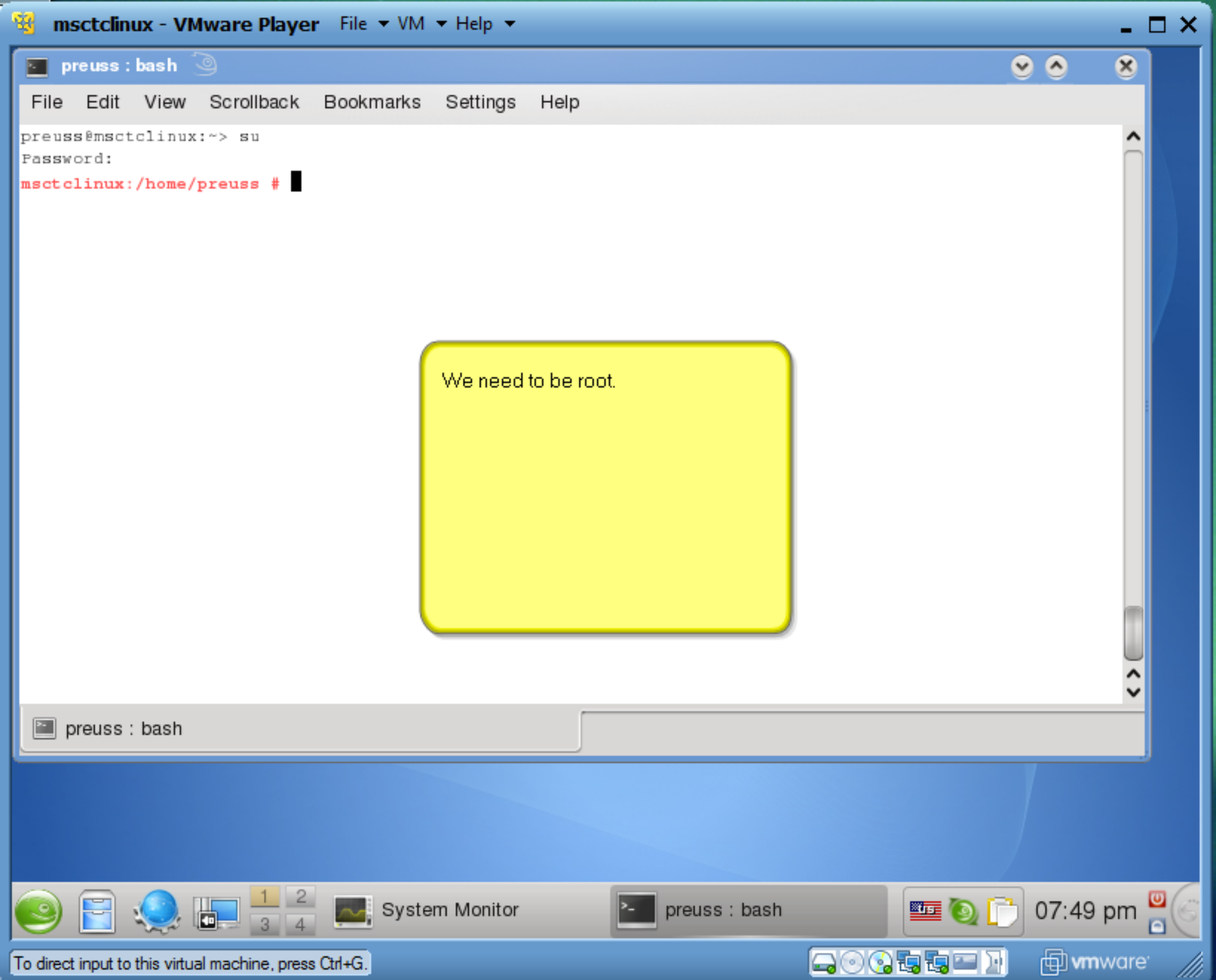
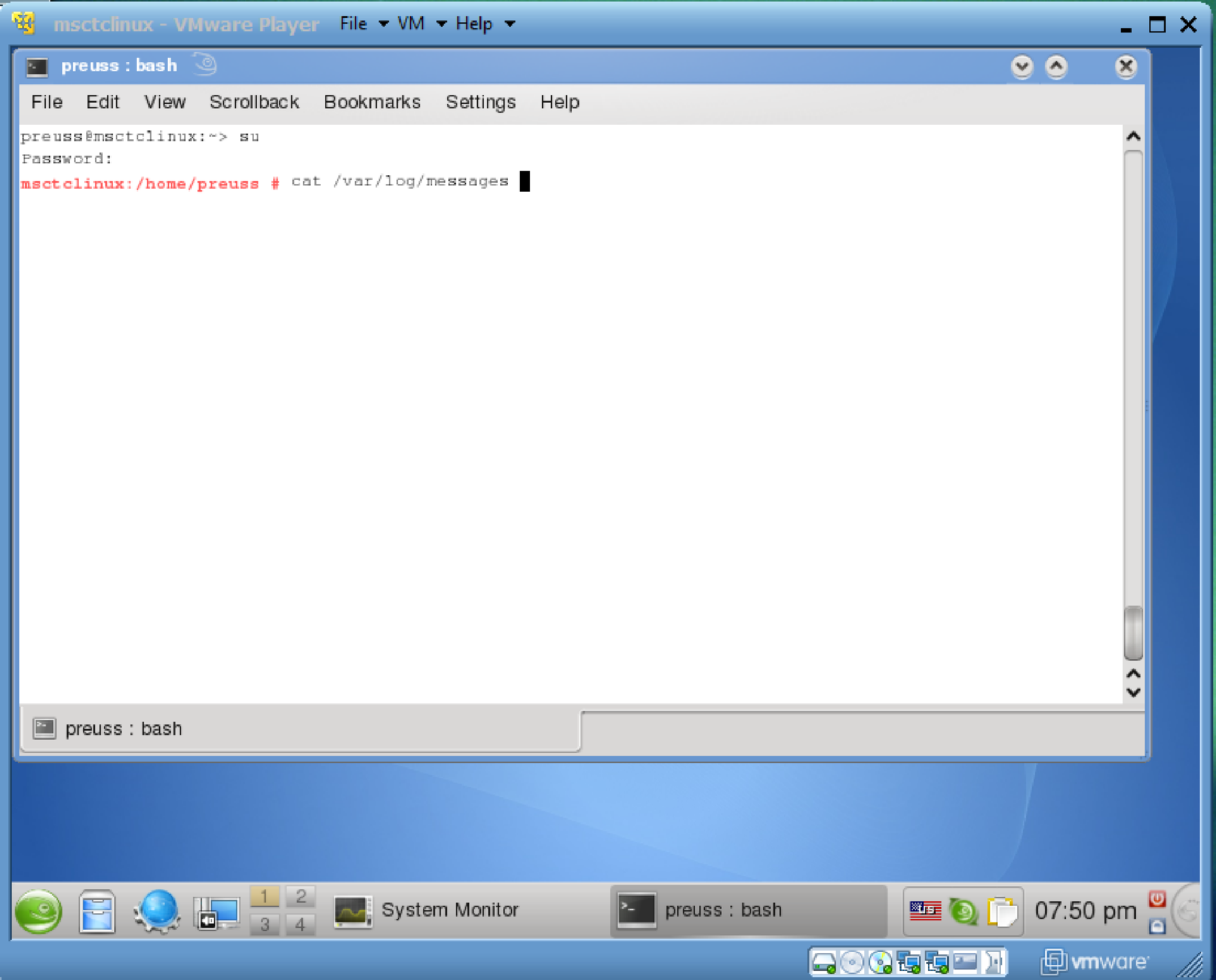
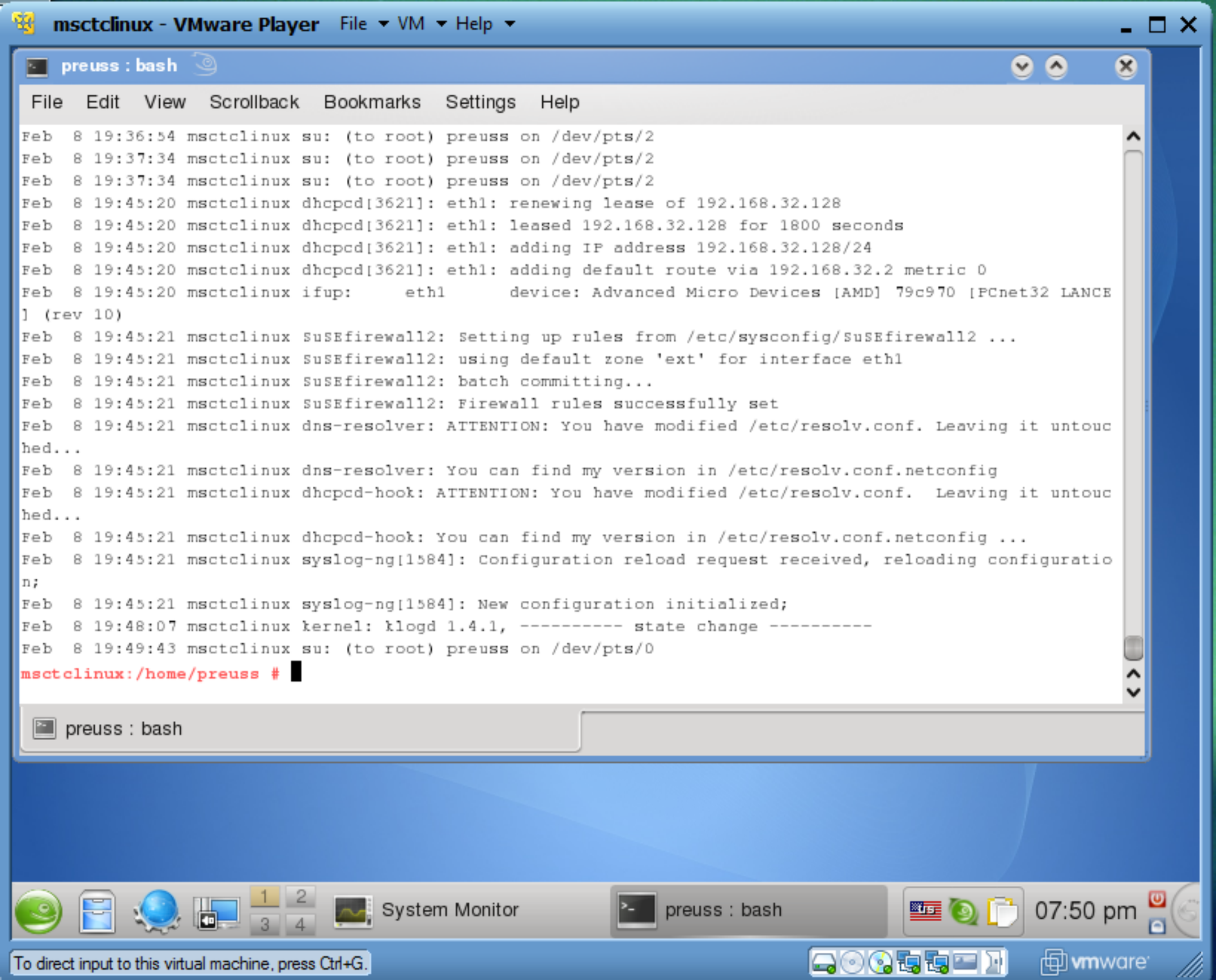
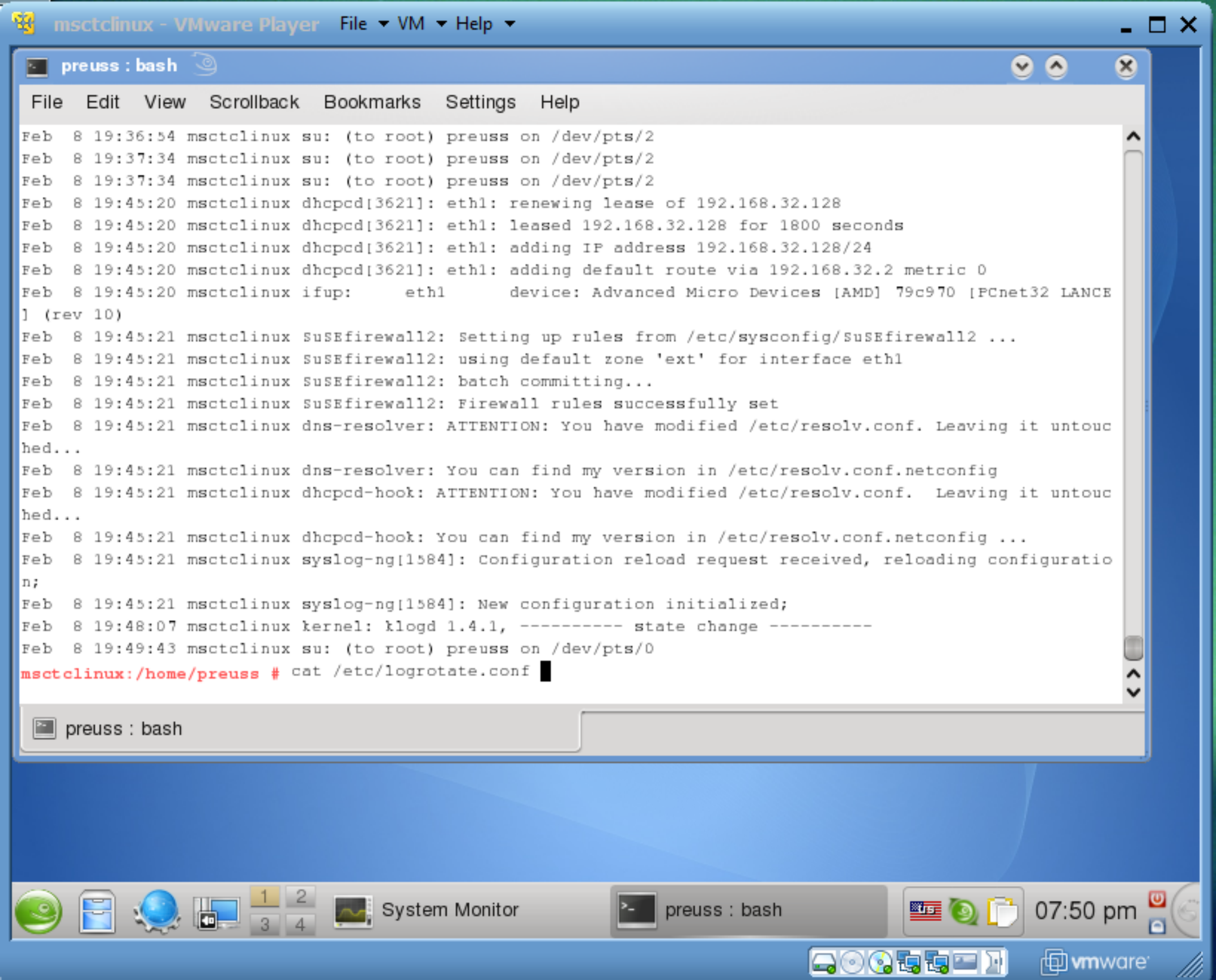
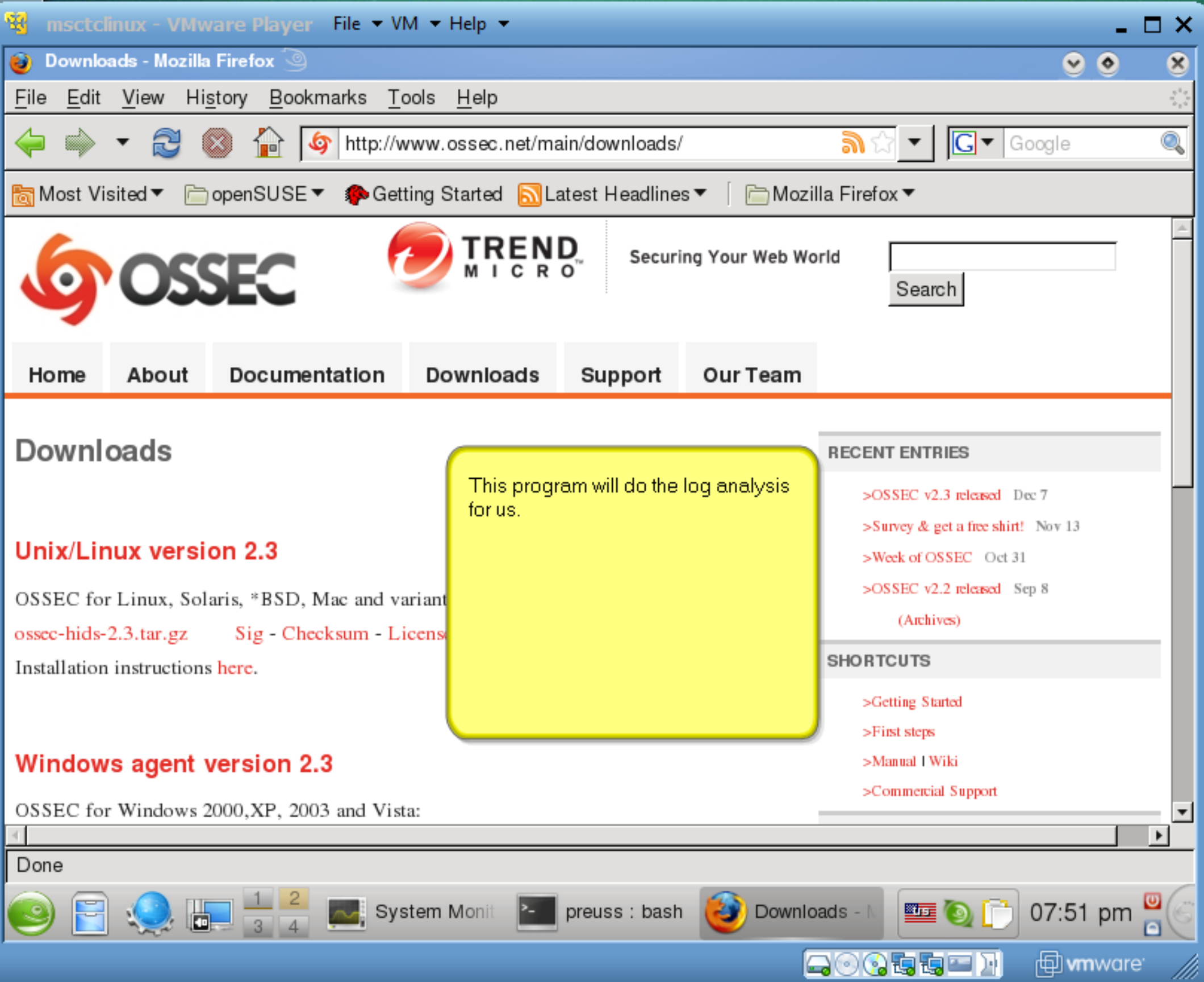
Provide a copy of your syslog or equivalent configuration on your Linux machine. Provide a copy of your log rotation. Obtain a legal program to analyze your log files. Run your log file analyzer

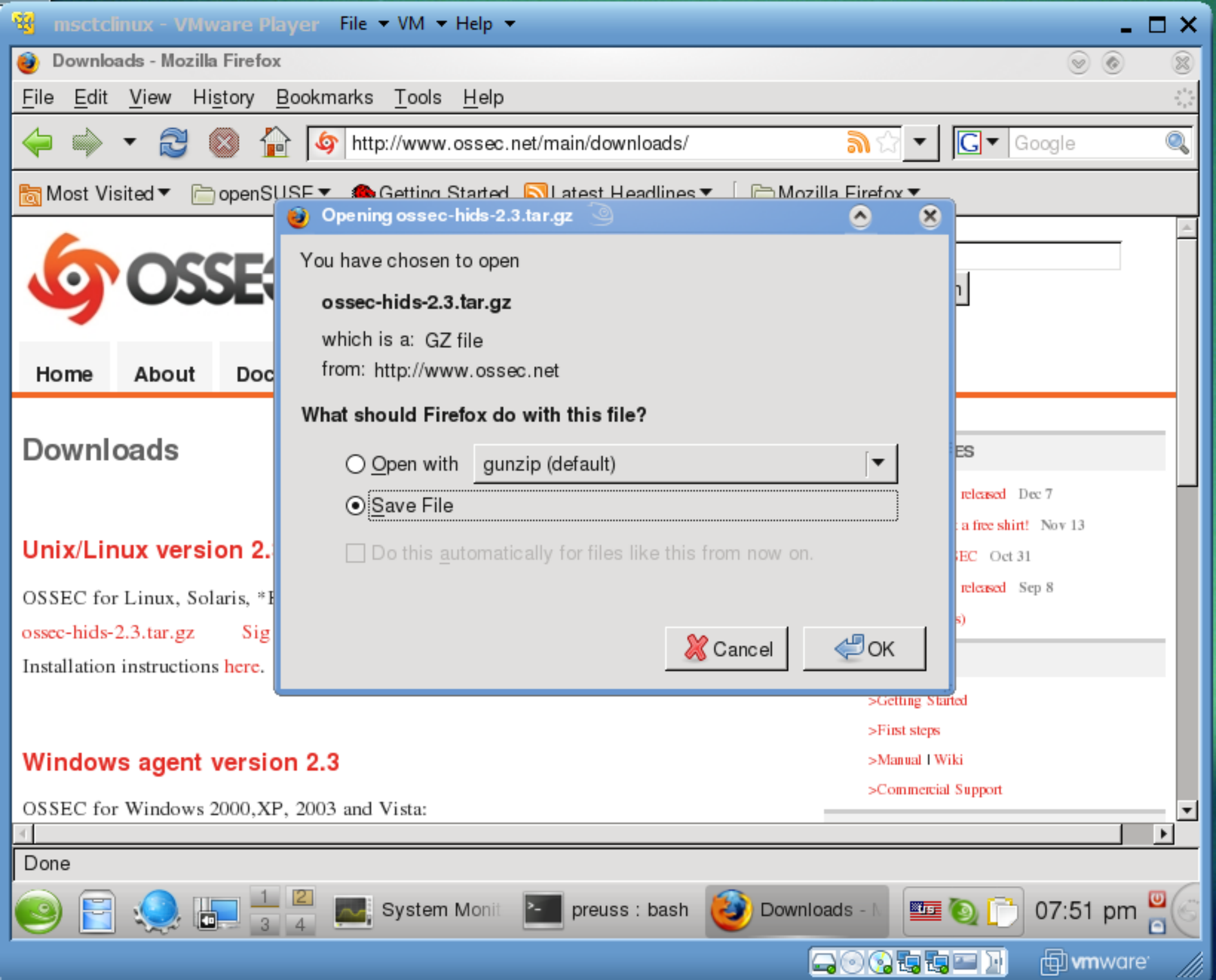

msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
preuss@msctclinux:~> su
Password:
msctclinux:/home/preuss #
We need to be root.
preuss : bash
System Monitor
preuss : bash
07:49 pm
To direct input to this virtual machine, press Ctrl+G.
vmware

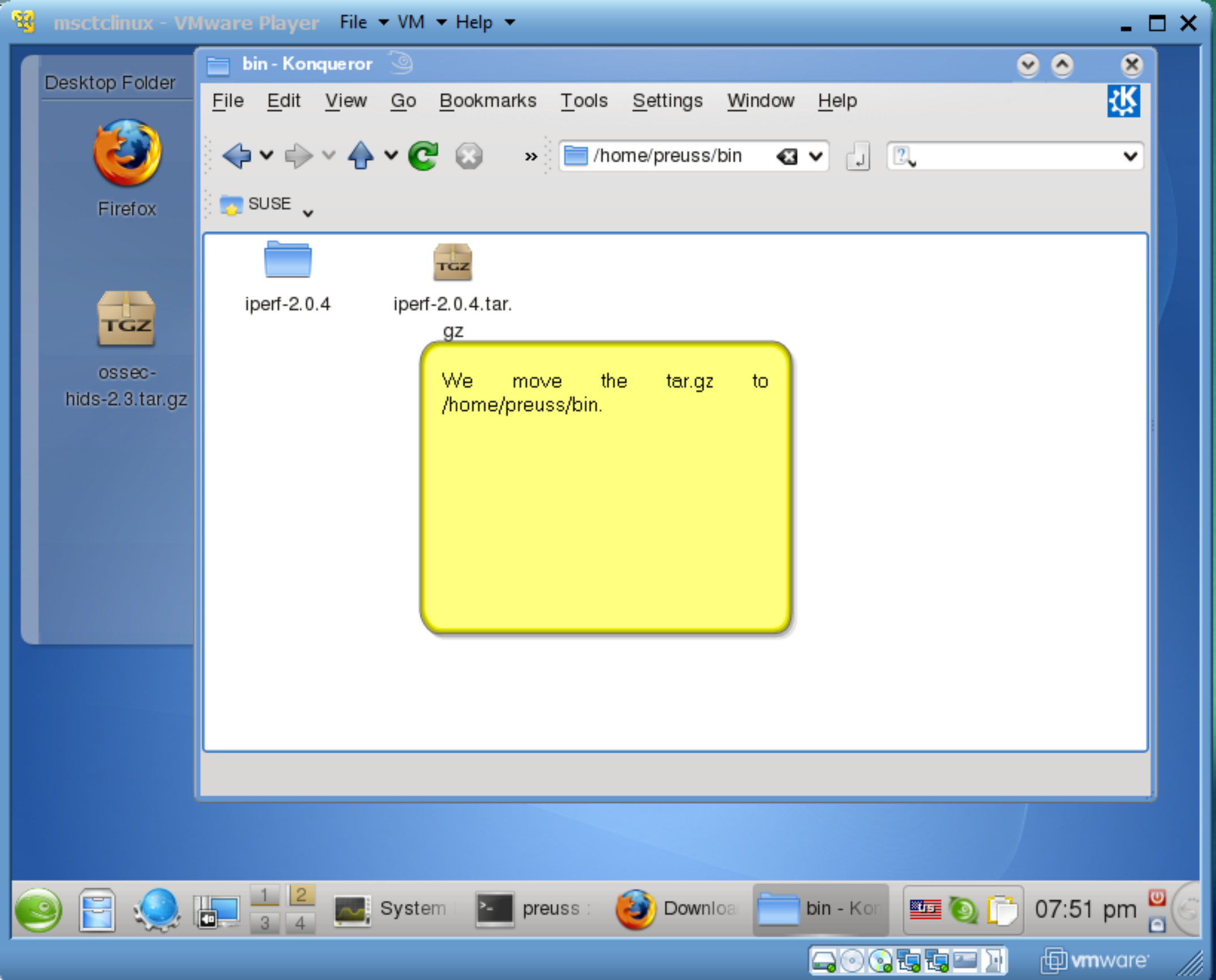

msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
preuss@msctclinux:~> su
Password:
msctclinux:/home/preuss # cat /var/log/messages
preuss : bash
1
2
3
4
System Monitor
preuss : bash
07:50 pm
vmware

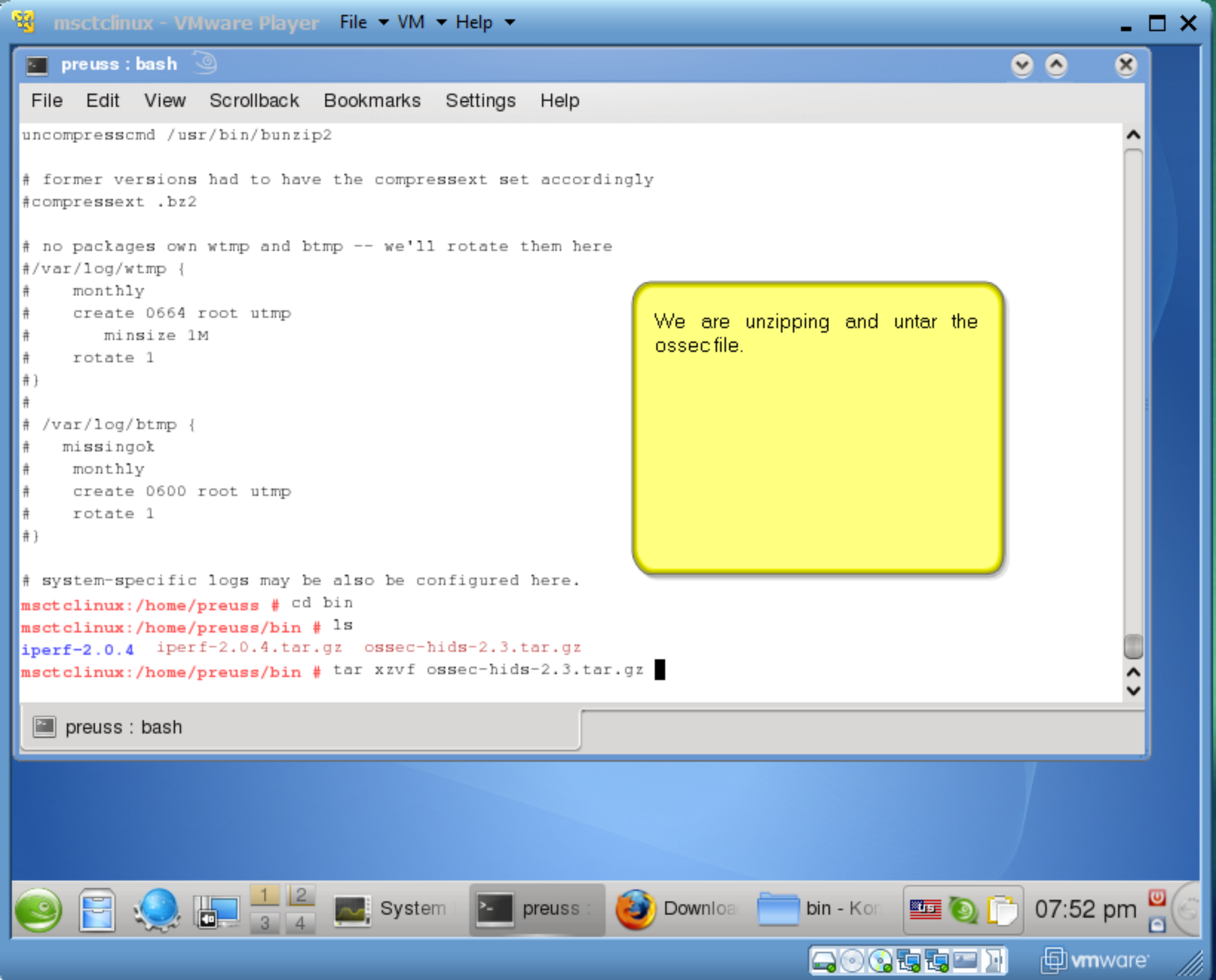

msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
Feb 8 19:36:54 msctclinux su: (to root) preuss on /dev/pts/2
Feb 8 19:37:34 msctclinux su: (to root) preuss on /dev/pts/2
Feb 8 19:37:34 msctclinux su: (to root) preuss on /dev/pts/2
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: renewing lease of 192.168.32.128
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: leased 192.168.32.128 for 1800 seconds
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: adding IP address 192.168.32.128/24
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: adding default route via 192.168.32.2 metric 0
Feb 8 19:45:20 msctclinux ifup: eth1 device: Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE
] (rev 10)
Feb 8 19:45:21 msctclinux SuSEfirewall2: Setting up rules from /etc/sysconfig/SuSEfirewall2 ...
Feb 8 19:45:21 msctclinux SuSEfirewall2: using default zone 'ext' for interface eth1
Feb 8 19:45:21 msctclinux SuSEfirewall2: batch committing...
Feb 8 19:45:21 msctclinux SuSEfirewall2: Firewall rules successfully set
Feb 8 19:45:21 msctclinux dns-resolver: ATTENTION: You have modified /etc/resolv.conf. Leaving it untouc
hed...
Feb 8 19:45:21 msctclinux dns-resolver: You can find my version in /etc/resolv.conf.netconfig
Feb 8 19:45:21 msctclinux dhcpcd-hook: ATTENTION: You have modified /etc/resolv.conf. Leaving it untouc
hed...
Feb 8 19:45:21 msctclinux dhcpcd-hook: You can find my version in /etc/resolv.conf.netconfig ...
Feb 8 19:45:21 msctclinux syslog-ng[1584]: Configuration reload request received, reloading configuratio
n;
Feb 8 19:45:21 msctclinux syslog-ng[1584]: New configuration initialized;
Feb 8 19:48:07 msctclinux kernel: klogd 1.4.1, ---------- state change ----------
Feb 8 19:49:43 msctclinux su: (to root) preuss on /dev/pts/0
msctclinux:/home/preuss #
preuss : bash
1
2
3
4
System Monitor
preuss : bash
07:50 pm
To direct input to this virtual machine, press Ctrl+G.
vmware

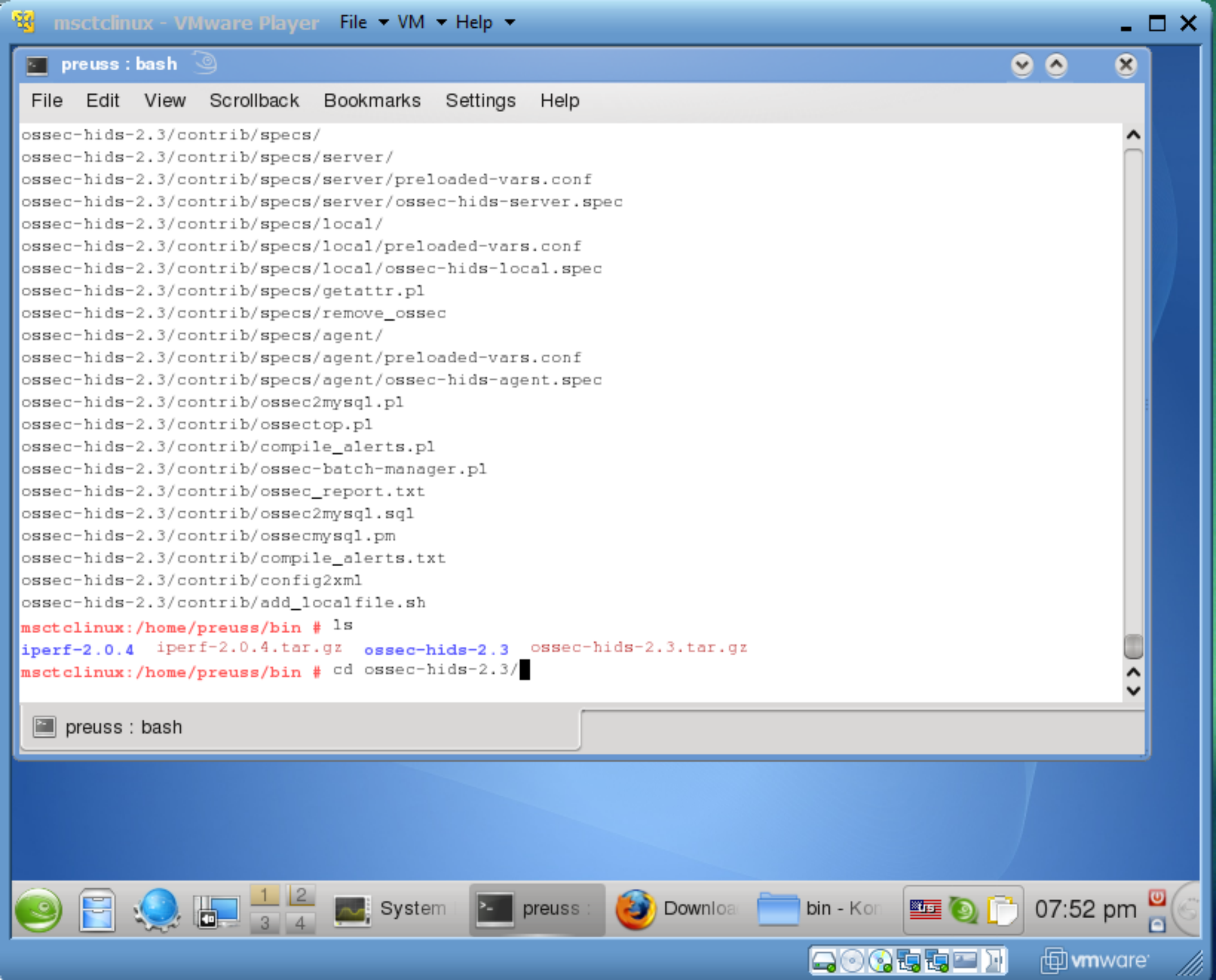

msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
Feb 8 19:36:54 msctclinux su: (to root) preuss on /dev/pts/2
Feb 8 19:37:34 msctclinux su: (to root) preuss on /dev/pts/2
Feb 8 19:37:34 msctclinux su: (to root) preuss on /dev/pts/2
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: renewing lease of 192.168.32.128
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: leased 192.168.32.128 for 1800 seconds
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: adding IP address 192.168.32.128/24
Feb 8 19:45:20 msctclinux dhcpcd[3621]: eth1: adding default route via 192.168.32.2 metric 0
Feb 8 19:45:20 msctclinux ifup: eth1 device: Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE
] (rev 10)
Feb 8 19:45:21 msctclinux SuSEfirewall2: Setting up rules from /etc/sysconfig/SuSEfirewall2 ...
Feb 8 19:45:21 msctclinux SuSEfirewall2: using default zone 'ext' for interface eth1
Feb 8 19:45:21 msctclinux SuSEfirewall2: batch committing...
Feb 8 19:45:21 msctclinux SuSEfirewall2: Firewall rules successfully set
Feb 8 19:45:21 msctclinux dns-resolver: ATTENTION: You have modified /etc/resolv.conf. Leaving it untouc
hed...
Feb 8 19:45:21 msctclinux dns-resolver: You can find my version in /etc/resolv.conf.netconfig
Feb 8 19:45:21 msctclinux dhcpcd-hook: ATTENTION: You have modified /etc/resolv.conf. Leaving it untouc
hed...
Feb 8 19:45:21 msctclinux dhcpcd-hook: You can find my version in /etc/resolv.conf.netconfig ...
Feb 8 19:45:21 msctclinux syslog-ng[1584]: Configuration reload request received, reloading configuratio
n;
Feb 8 19:45:21 msctclinux syslog-ng[1584]: New configuration initialized;
Feb 8 19:48:07 msctclinux kernel: klogd 1.4.1, ---------- state change ----------
Feb 8 19:49:43 msctclinux su: (to root) preuss on /dev/pts/0
msctclinux:/home/preuss # cat /etc/logrotate.conf
preuss : bash
1
2
3
4
System Monitor
preuss : bash
07:50 pm
vmware

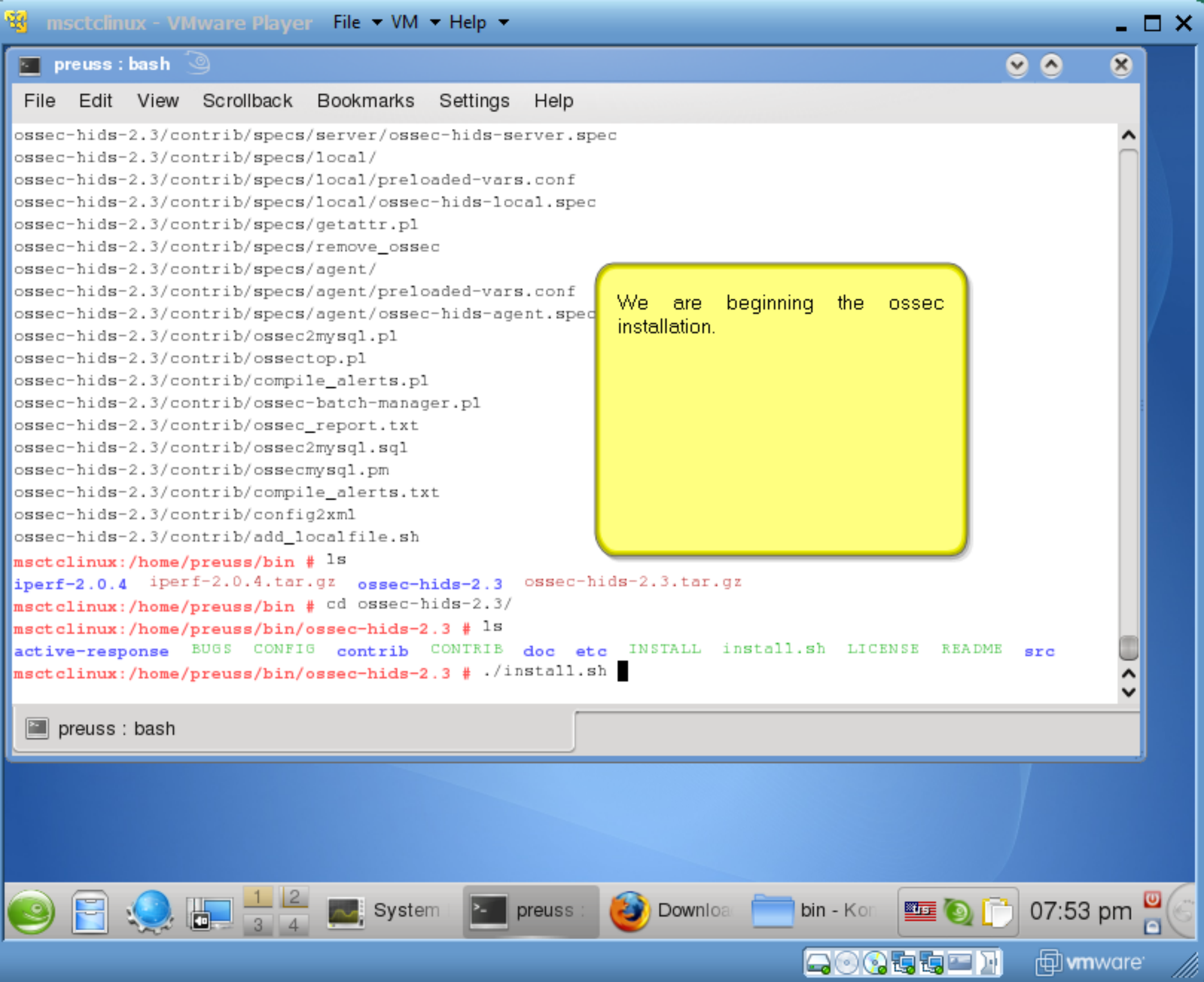

msctclinux - VMware Player
File VM Help
Downloads - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.ossec.net/main/downloads/
Google
Most Visited openSUSE Getting Started Latest Headlines Mozilla Firefox
OSSEC
TREND MICRO
Securing Your Web World
Search
Home About Documentation Downloads Support Our Team
Downloads
This program will do the log analysis for us.
Unix/Linux version 2.3
OSSEC for Linux, Solaris, *BSD, Mac and variant
ossec-hids-2.3.tar.gz Sig - Checksum - Licens
Installation instructions here.
Windows agent version 2.3
OSSEC for Windows 2000,XP, 2003 and Vista:
RECENT ENTRIES
>OSSEC v2.3 released Dec 7
>Survey & get a free shirt! Nov 13
>Week of OSSEC Oct 31
>OSSEC v2.2 released Sep 8
(Archives)
SHORTCUTS
>Getting Started
>First steps
>Manual | Wiki
>Commercial Support
Done
System Monit
preuss : bash
Downloads - M
07:51 pm
vmware

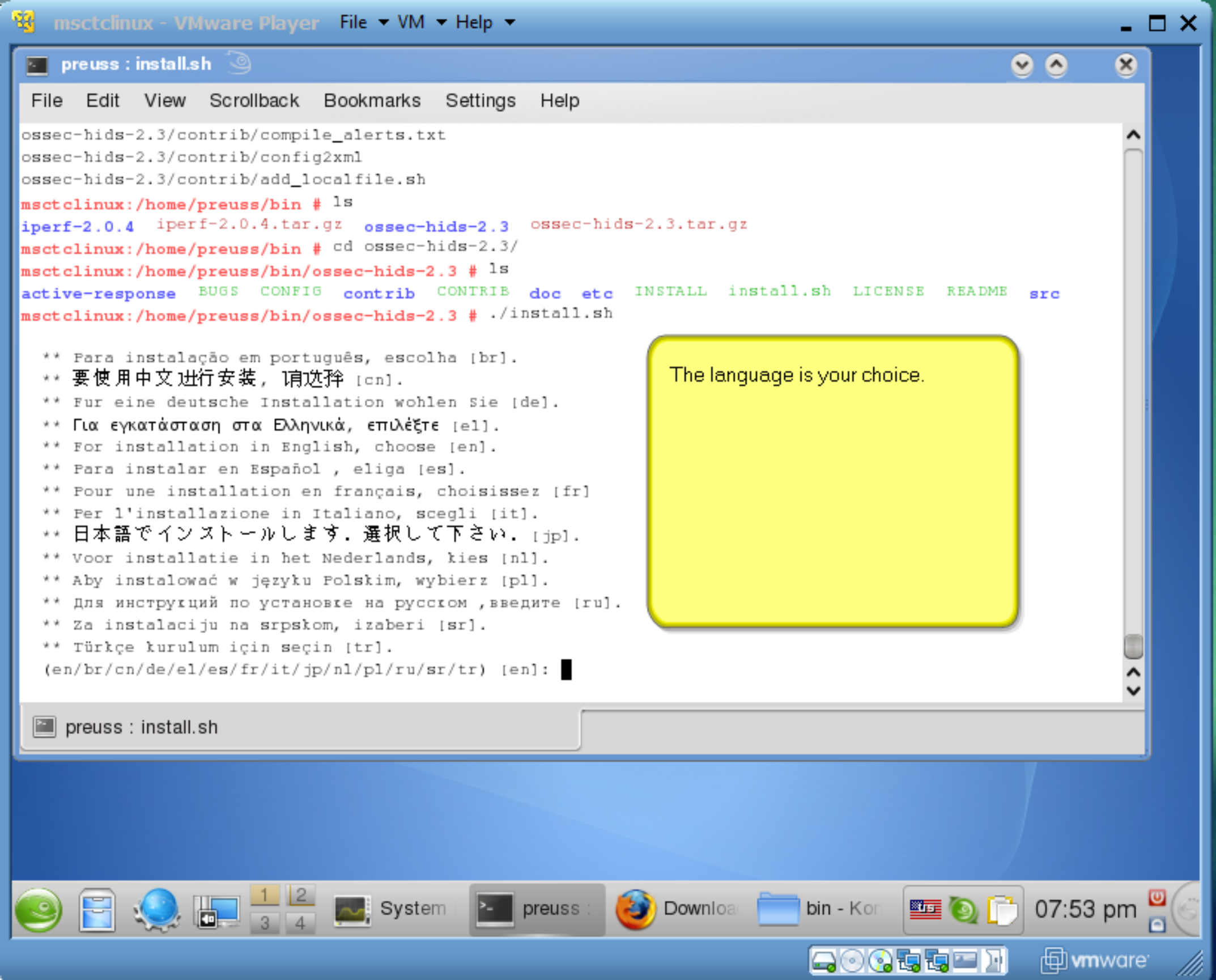

msctclinux - VMware Player
File
VM
Help
Downloads - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.ossec.net/main/downloads/
Google
Most Visited
openSUSE
Getting Started
Latest Headlines
Mozilla Firefox
Opening ossec-hids-2.3.tar.gz
You have chosen to open
ossec-hids-2.3.tar.gz
which is a: GZ file
from: http://www.ossec.net
What should Firefox do with this file?
Open with
gunzip (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK
Home
About
Downloads
Unix/Linux version 2.
OSSEC for Linux, Solaris, *
ossec-hids-2.3.tar.gz
Sig
Installation instructions here.
Windows agent version 2.3
OSSEC for Windows 2000,XP, 2003 and Vista:
released Dec 7
a free shirt! Nov 13
Oct 31
released Sep 8
>Getting Started
>First steps
>Manual | Wiki
>Commercial Support
Done
System Monit
preuss : bash
Downloads - M
07:51 pm
vmware

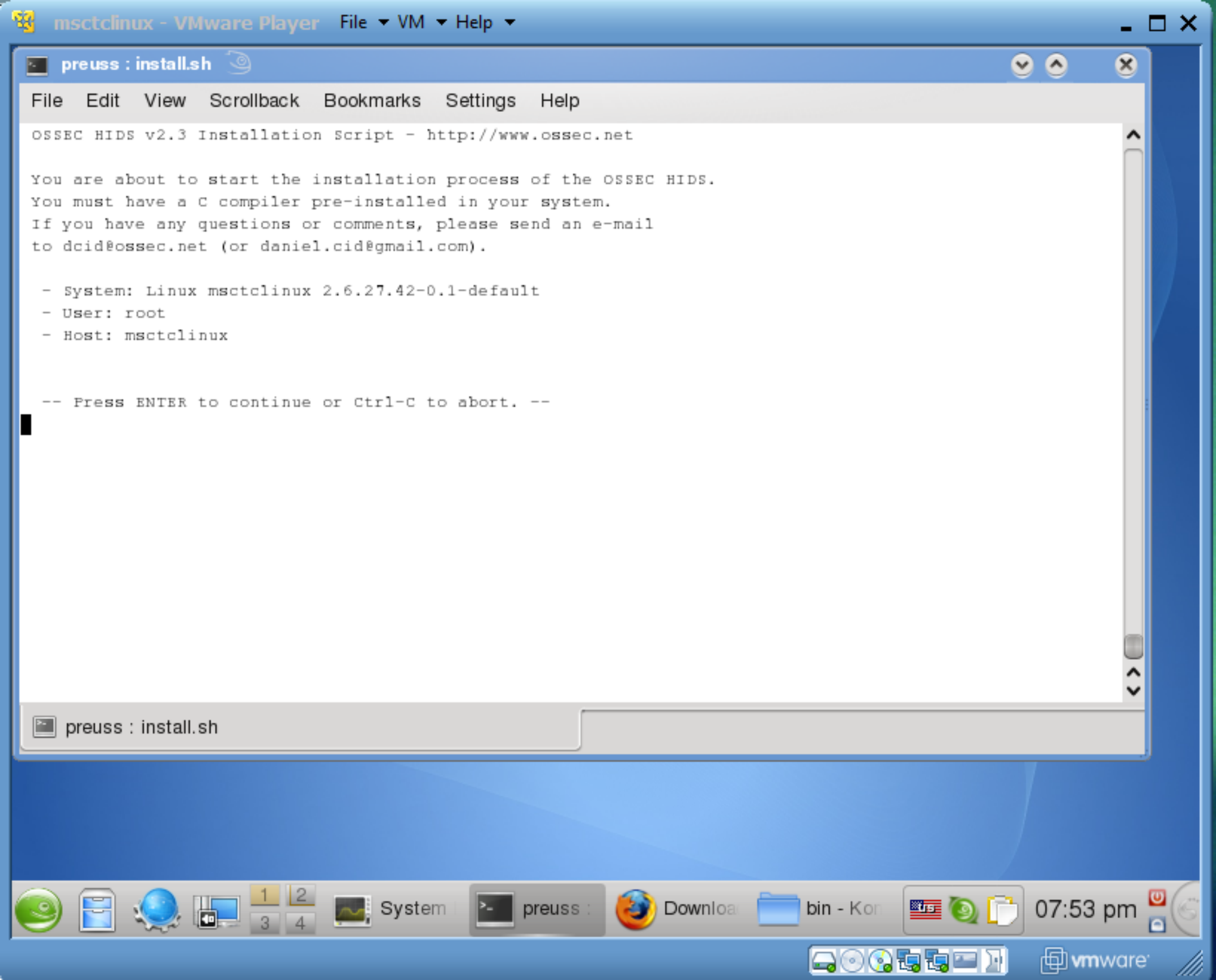

msctclinux - VMware Player
File
VM
Help
Desktop Folder
Firefox
ossec-hids-2.3.tar.gz
bin - Konqueror
File
Edit
View
Go
Bookmarks
Tools
Settings
Window
Help
/home/preuss/bin
SUSE
iperf-2.0.4
iperf-2.0.4.tar.gz
We move the tar.gz to /home/preuss/bin.
System
preuss
Downloa
bin - Kor
07:51 pm
vmware

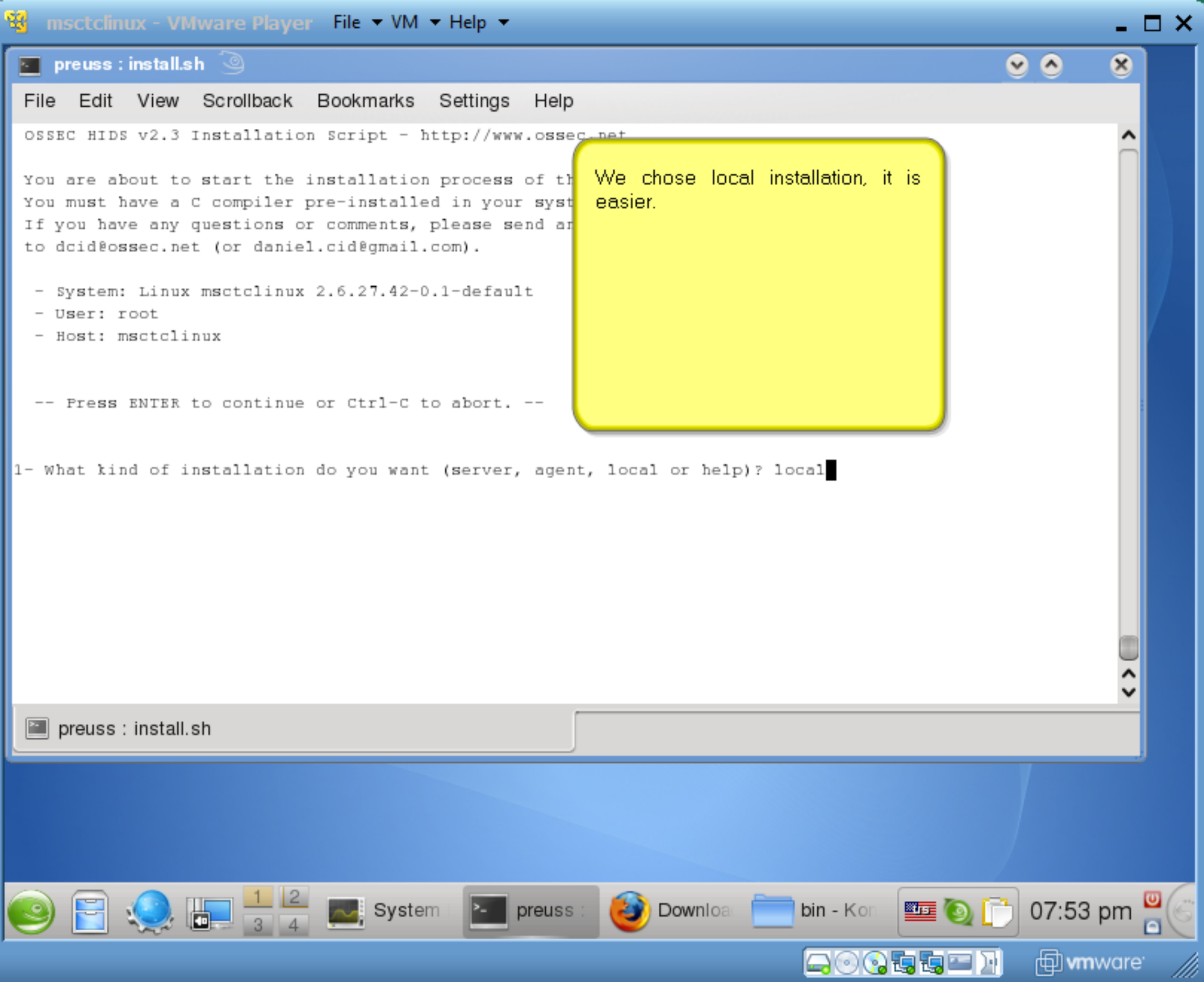

msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
uncompresscmd /usr/bin/bunzip2
former versions had to have the compressext set accordingly
#compressext .bz2
no packages own wtmp and btmp -- we'll rotate them here
#/var/log/wtmp {
monthly
create 0664 root utmp
minsize 1M
rotate 1
#}
#
/var/log/btmp {
missingok
monthly
create 0600 root utmp
rotate 1
#}
system-specific logs may be also be configured here.
msctclinux:/home/preuss # cd bin
msctclinux:/home/preuss/bin # ls
iperf-2.0.4 iperf-2.0.4.tar.gz ossec-hids-2.3.tar.gz
msctclinux:/home/preuss/bin # tar xzvf ossec-hids-2.3.tar.gz
We are unzipping and untar the ossec file.
preuss : bash
System
preuss :
Downloa
bin - Kor
07:52 pm
vmware

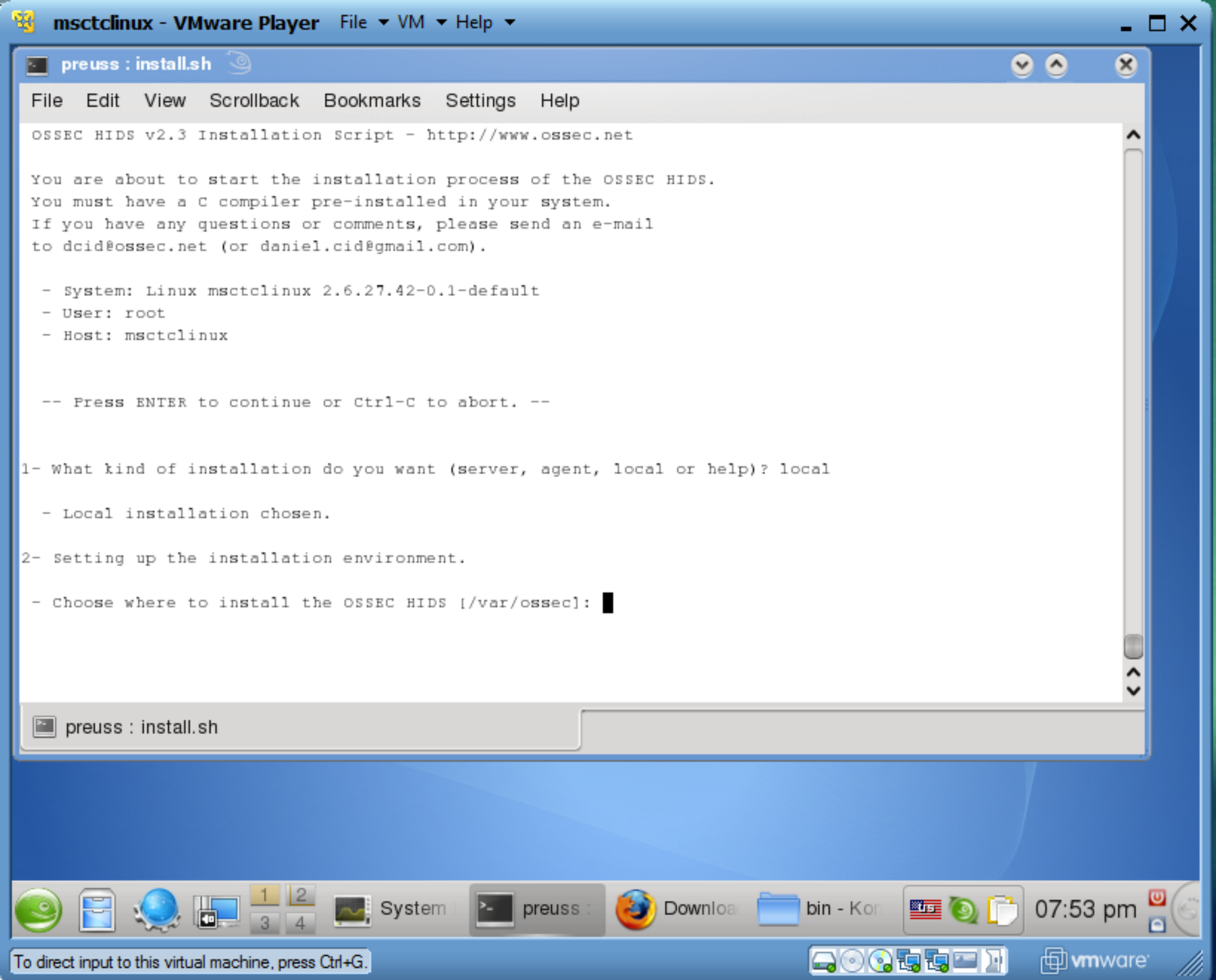

msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
ossec-hids-2.3/contrib/specs/
ossec-hids-2.3/contrib/specs/server/
ossec-hids-2.3/contrib/specs/server/preloaded-vars.conf
ossec-hids-2.3/contrib/specs/server/ossec-hids-server.spec
ossec-hids-2.3/contrib/specs/local/
ossec-hids-2.3/contrib/specs/local/preloaded-vars.conf
ossec-hids-2.3/contrib/specs/local/ossec-hids-local.spec
ossec-hids-2.3/contrib/specs/getattr.pl
ossec-hids-2.3/contrib/specs/remove_ossec
ossec-hids-2.3/contrib/specs/agent/
ossec-hids-2.3/contrib/specs/agent/preloaded-vars.conf
ossec-hids-2.3/contrib/specs/agent/ossec-hids-agent.spec
ossec-hids-2.3/contrib/ossec2mysql.pl
ossec-hids-2.3/contrib/ossectop.pl
ossec-hids-2.3/contrib/compile_alerts.pl
ossec-hids-2.3/contrib/ossec-batch-manager.pl
ossec-hids-2.3/contrib/ossec_report.txt
ossec-hids-2.3/contrib/ossec2mysql.sql
ossec-hids-2.3/contrib/ossecmysql.pm
ossec-hids-2.3/contrib/compile_alerts.txt
ossec-hids-2.3/contrib/config2xml
ossec-hids-2.3/contrib/add_localfile.sh
msctclinux:/home/preuss/bin # ls
iperf-2.0.4 iperf-2.0.4.tar.gz ossec-hids-2.3 ossec-hids-2.3.tar.gz
msctclinux:/home/preuss/bin # cd ossec-hids-2.3/
preuss : bash
System
preuss :
Downloa
bin - Kor
07:52 pm
vmware

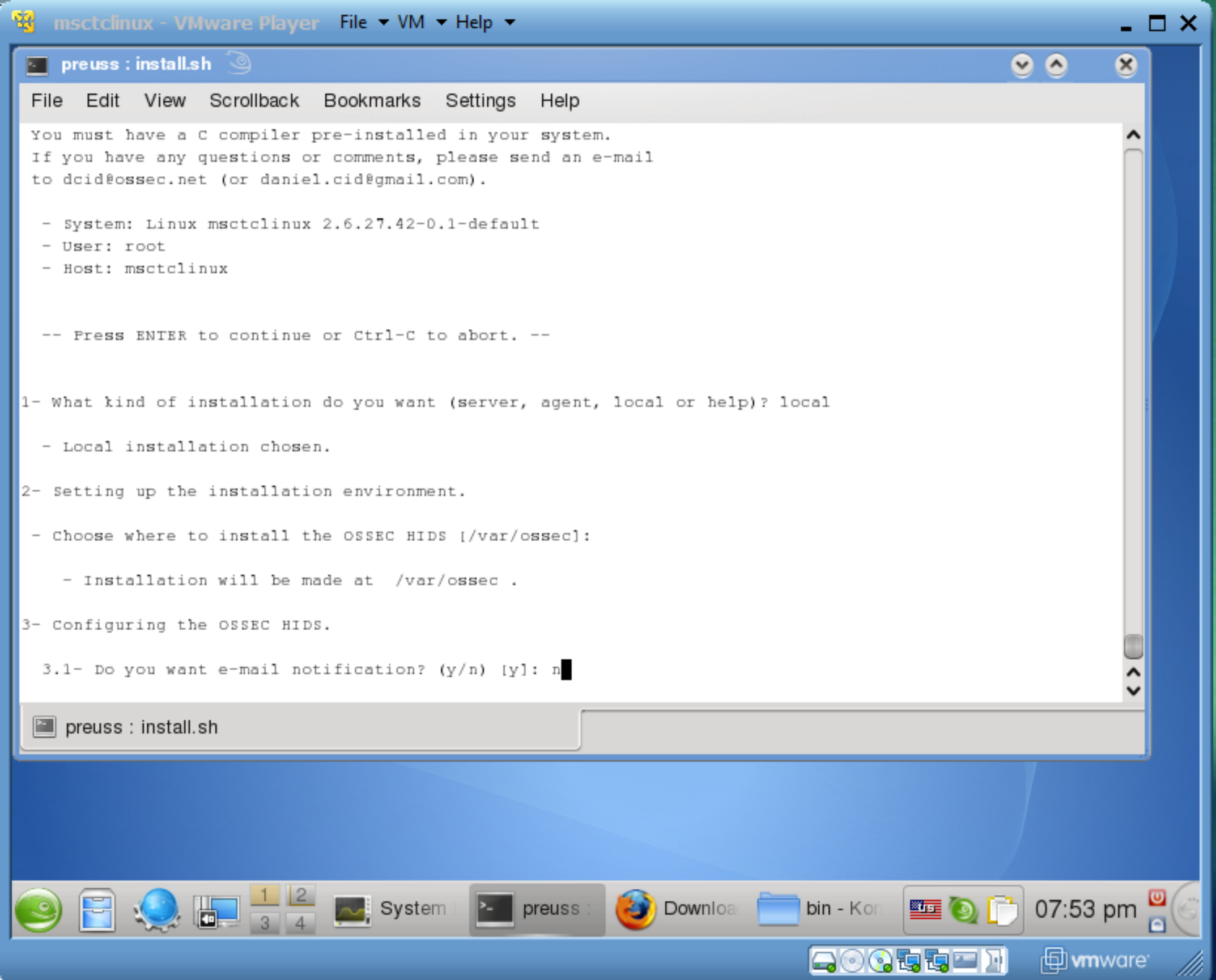

msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
ossec-hids-2.3/contrib/specs/server/ossec-hids-server.spec
ossec-hids-2.3/contrib/specs/local/
ossec-hids-2.3/contrib/specs/local/preloaded-vars.conf
ossec-hids-2.3/contrib/specs/local/ossec-hids-local.spec
ossec-hids-2.3/contrib/specs/getattr.pl
ossec-hids-2.3/contrib/specs/remove_ossec
ossec-hids-2.3/contrib/specs/agent/
ossec-hids-2.3/contrib/specs/agent/preloaded-vars.conf
ossec-hids-2.3/contrib/specs/agent/ossec-hids-agent.spec
ossec-hids-2.3/contrib/ossec2mysql.pl
ossec-hids-2.3/contrib/ossectop.pl
ossec-hids-2.3/contrib/compile_alerts.pl
ossec-hids-2.3/contrib/ossec-batch-manager.pl
ossec-hids-2.3/contrib/ossec_report.txt
ossec-hids-2.3/contrib/ossec2mysql.sql
ossec-hids-2.3/contrib/ossecmysql.pm
ossec-hids-2.3/contrib/compile_alerts.txt
ossec-hids-2.3/contrib/config2xml
ossec-hids-2.3/contrib/add_localfile.sh
msctclinux:/home/preuss/bin # ls
iperf-2.0.4 iperf-2.0.4.tar.gz ossec-hids-2.3 ossec-hids-2.3.tar.gz
msctclinux:/home/preuss/bin # cd ossec-hids-2.3/
msctclinux:/home/preuss/bin/ossec-hids-2.3 # ls
active-response BUGS CONFIG contrib CONTRIB doc etc INSTALL install.sh LICENSE README src
msctclinux:/home/preuss/bin/ossec-hids-2.3 # ./install.sh
We are beginning the ossec installation.
preuss : bash
System
preuss :
Downloa
bin - Kor
07:53 pm
vmware

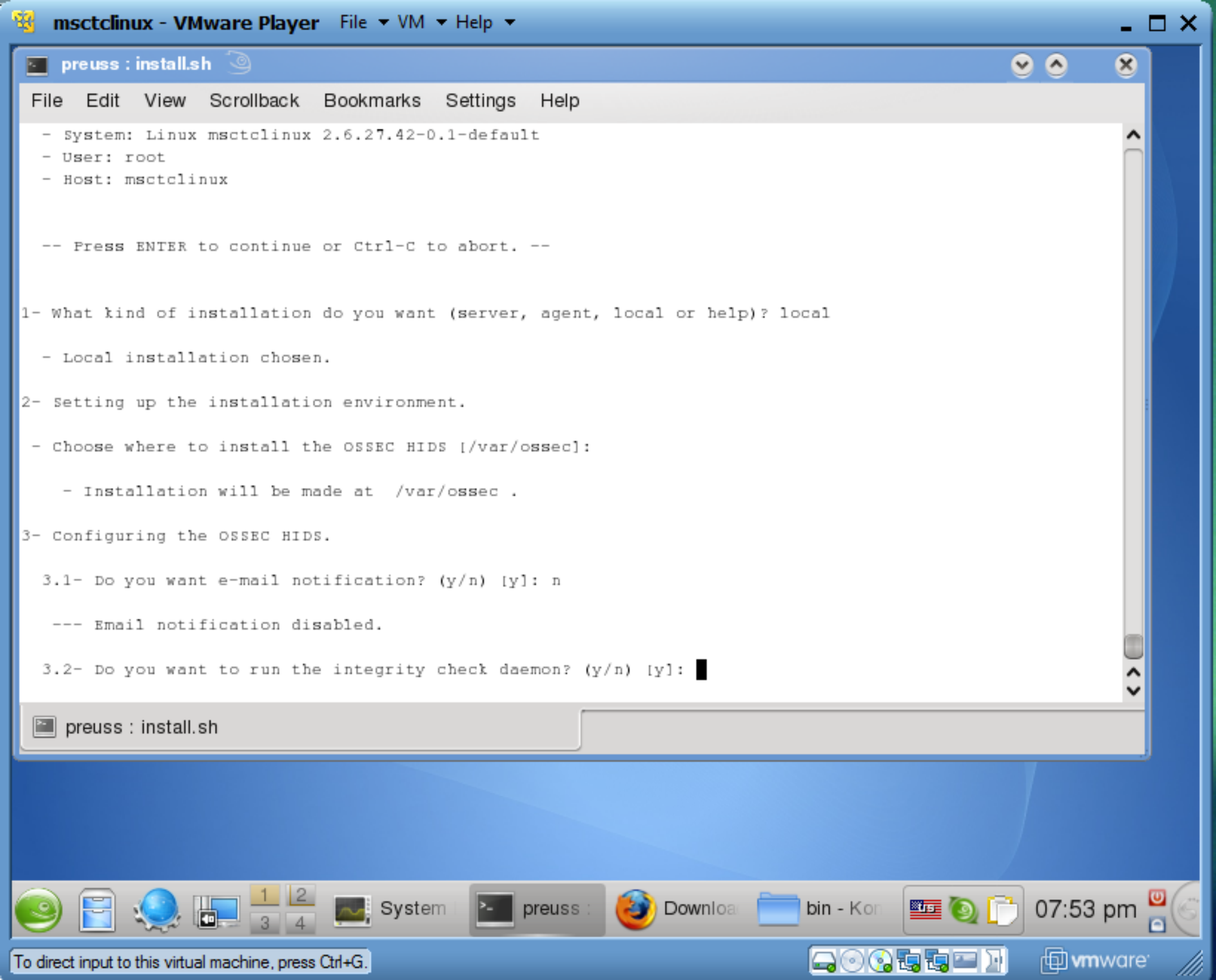

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File Edit View Scrollback Bookmarks Settings Help
ossec-hids-2.3/contrib/compile_alerts.txt
ossec-hids-2.3/contrib/config2xml
ossec-hids-2.3/contrib/add_localfile.sh
msctclinux:/home/preuss/bin # ls
iperf-2.0.4 iperf-2.0.4.tar.gz ossec-hids-2.3 ossec-hids-2.3.tar.gz
msctclinux:/home/preuss/bin # cd ossec-hids-2.3/
msctclinux:/home/preuss/bin/ossec-hids-2.3 # ls
active-response BUGS CONFIG contrib CONTRIB doc etc INSTALL install.sh LICENSE README src
msctclinux:/home/preuss/bin/ossec-hids-2.3 # ./install.sh
** Para instalação em português, escolha [br].
** 要使用中文进行安装，请选择 [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]
** Per l'installazione in Italiano, scegli [it].
** 日本語でインストールします．選択して下さい． [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/it/jp/nl/pl/ru/sr/tr) [en]:
The language is your choice.
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:53 pm
vmware

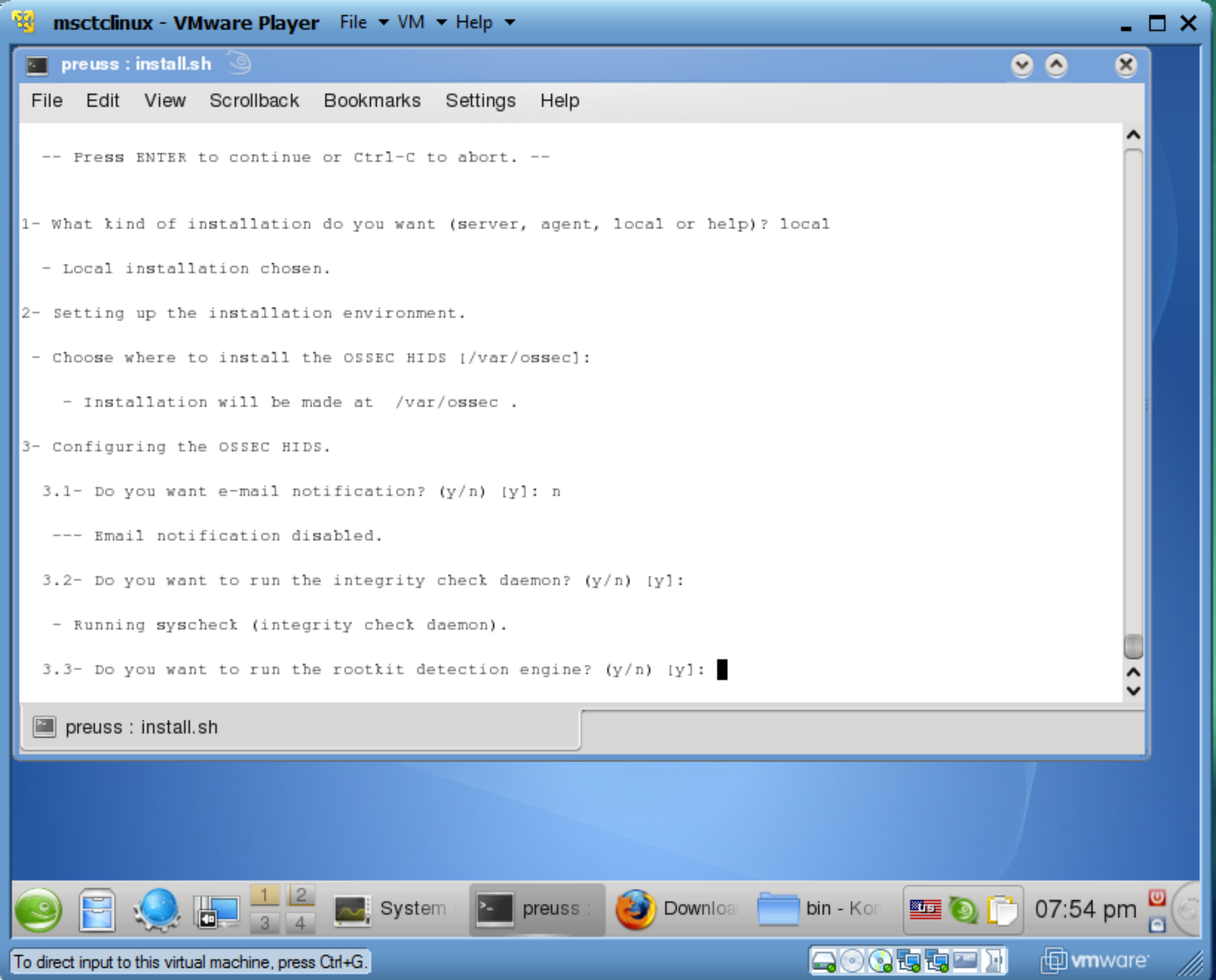

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
OSSEC HIDS v2.3 Installation Script - http://www.ossec.net
You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).
- System: Linux msctclinux 2.6.27.42-0.1-default
- User: root
- Host: msctclinux
-- Press ENTER to continue or Ctrl-C to abort. --
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:53 pm
vmware

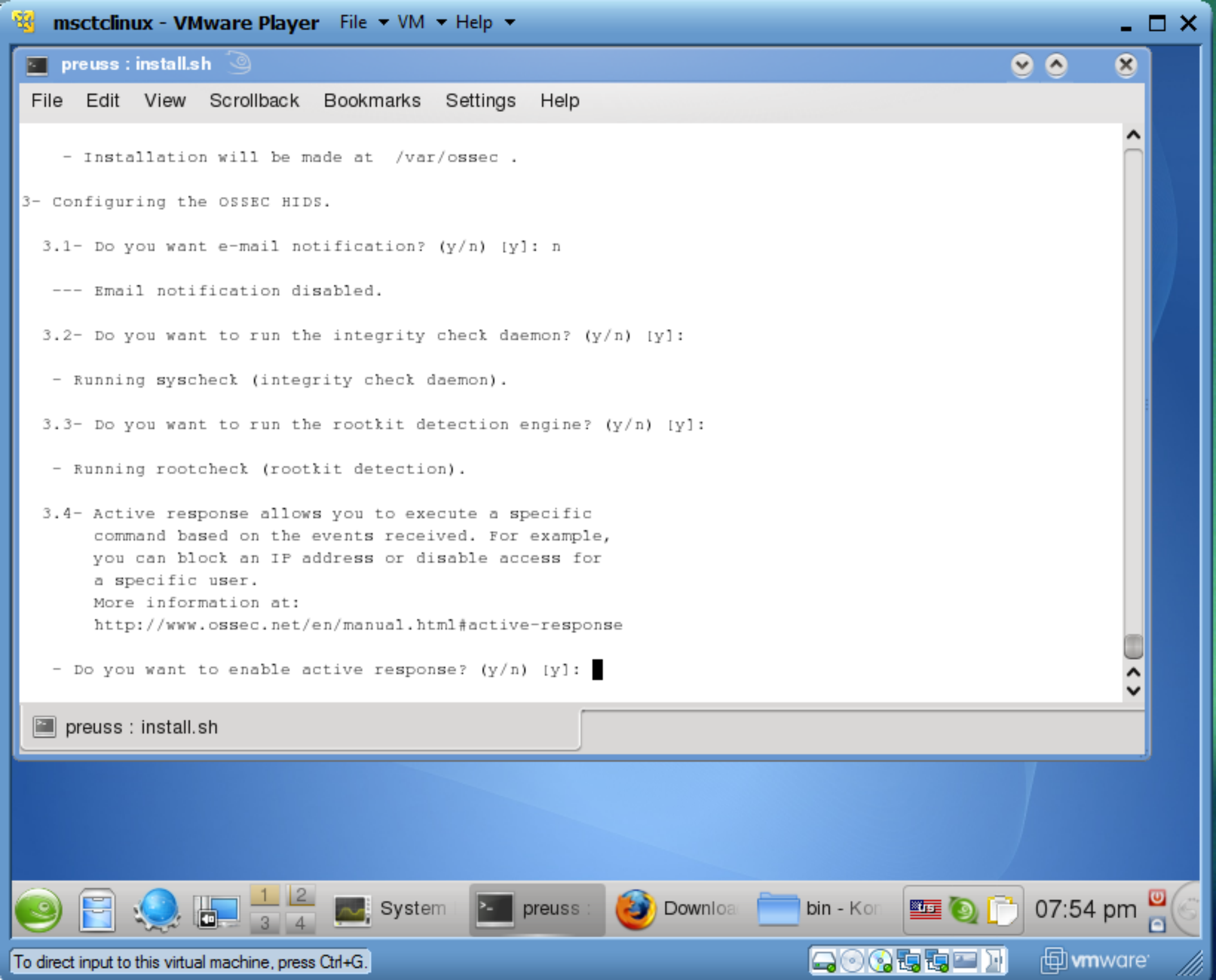

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File Edit View Scrollback Bookmarks Settings Help
OSSEC HIDS v2.3 Installation Script - http://www.ossec.net
You are about to start the installation process of th
You must have a C compiler pre-installed in your syst
If you have any questions or comments, please send an
to dcid@ossec.net (or daniel.cid@gmail.com).
- System: Linux msctclinux 2.6.27.42-0.1-default
- User: root
- Host: msctclinux
-- Press ENTER to continue or Ctrl-C to abort. --
1- What kind of installation do you want (server, agent, local or help)? local
We chose local installation, it is easier.
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:53 pm
vmware

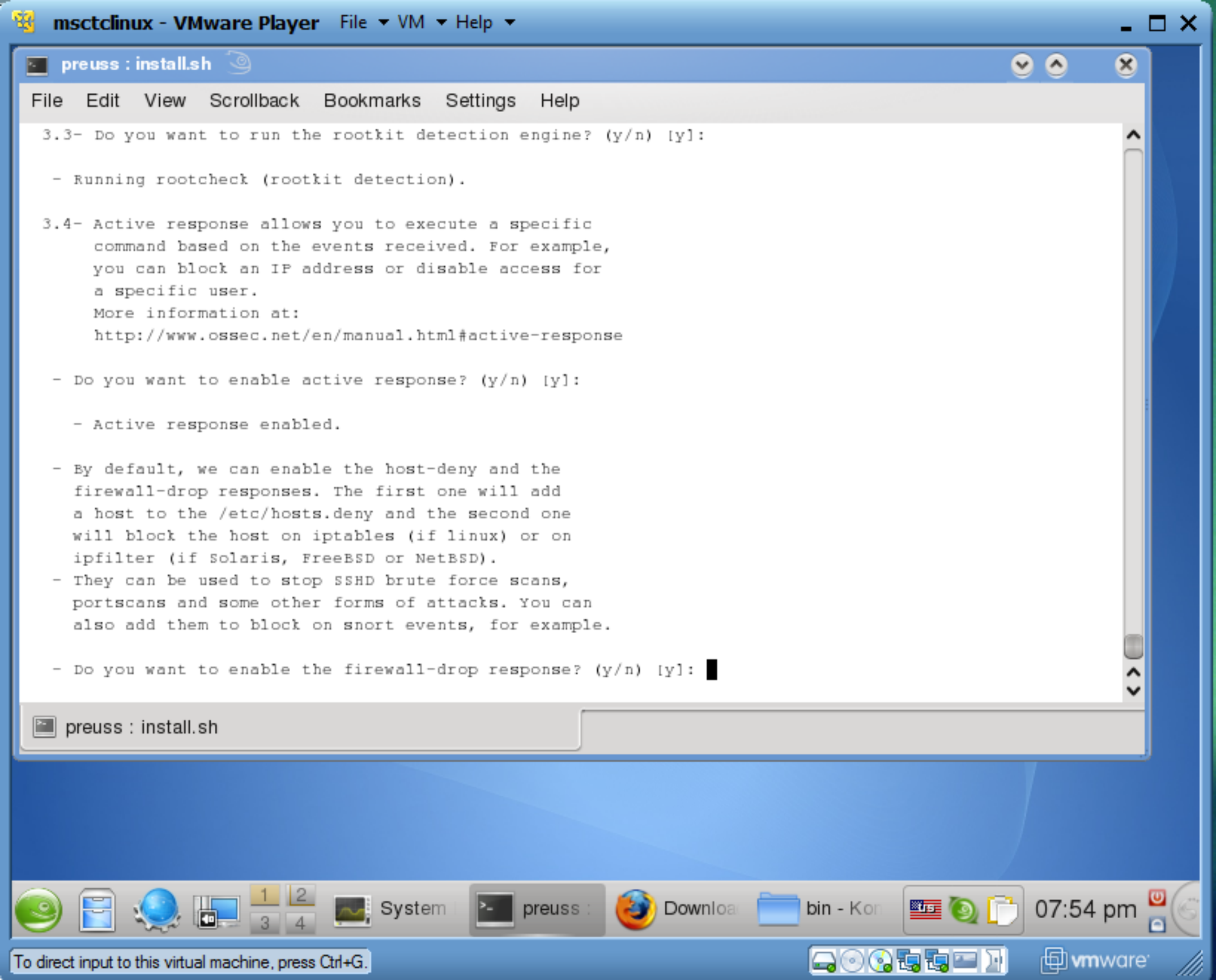

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
OSSEC HIDS v2.3 Installation Script - http://www.ossec.net
You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).
- System: Linux msctclinux 2.6.27.42-0.1-default
- User: root
- Host: msctclinux
-- Press ENTER to continue or Ctrl-C to abort. --
1- What kind of installation do you want (server, agent, local or help)? local
- Local installation chosen.
2- Setting up the installation environment.
- Choose where to install the OSSEC HIDS [/var/ossec]:
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:53 pm
To direct input to this virtual machine, press Ctrl+G.
vmware

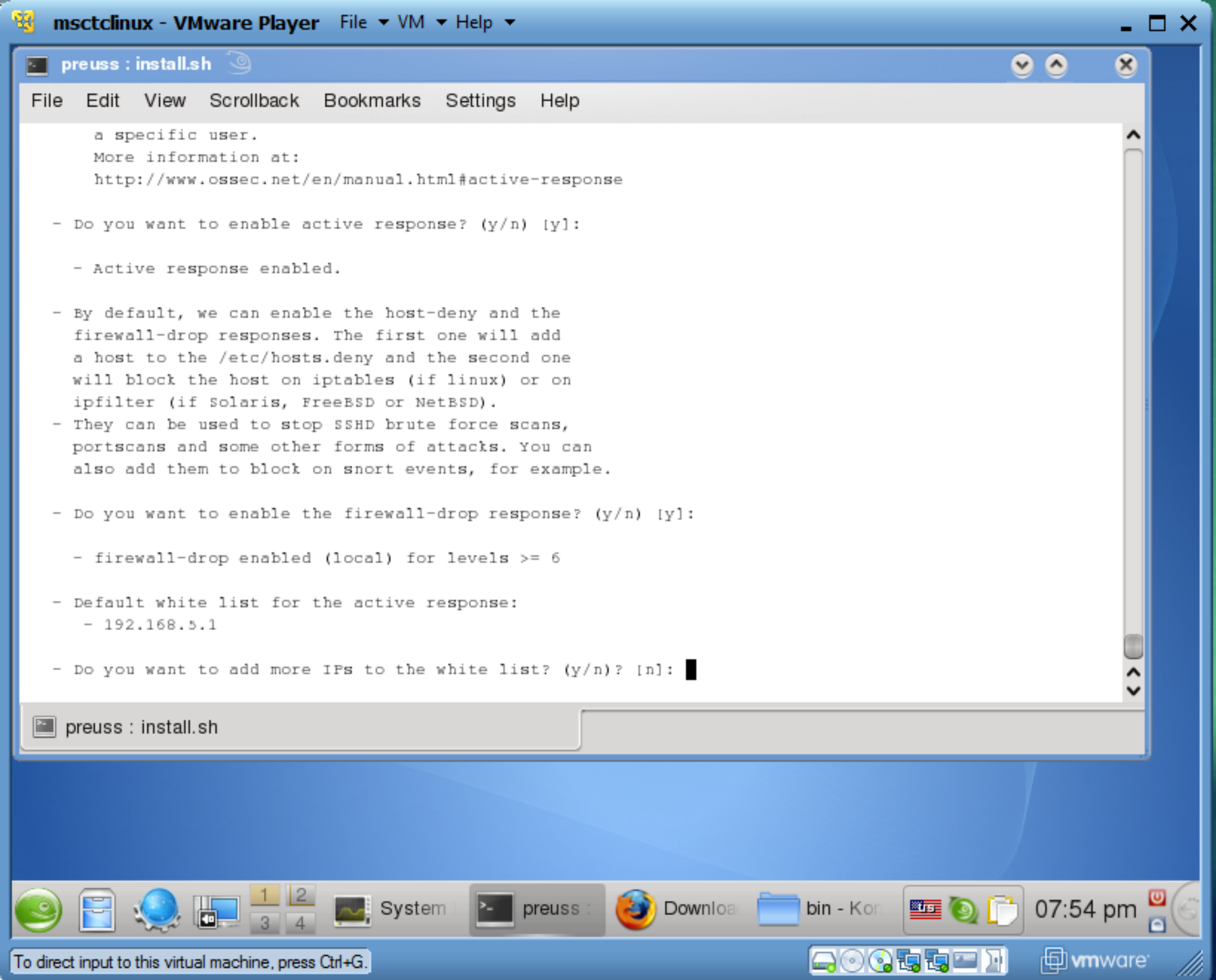

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).
- System: Linux msctclinux 2.6.27.42-0.1-default
- User: root
- Host: msctclinux
-- Press ENTER to continue or Ctrl-C to abort. --
1- What kind of installation do you want (server, agent, local or help)? local
- Local installation chosen.
2- Setting up the installation environment.
- Choose where to install the OSSEC HIDS [/var/ossec]:
- Installation will be made at /var/ossec .
3- Configuring the OSSEC HIDS.
3.1- Do you want e-mail notification? (y/n) [y]: n
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:53 pm
vmware

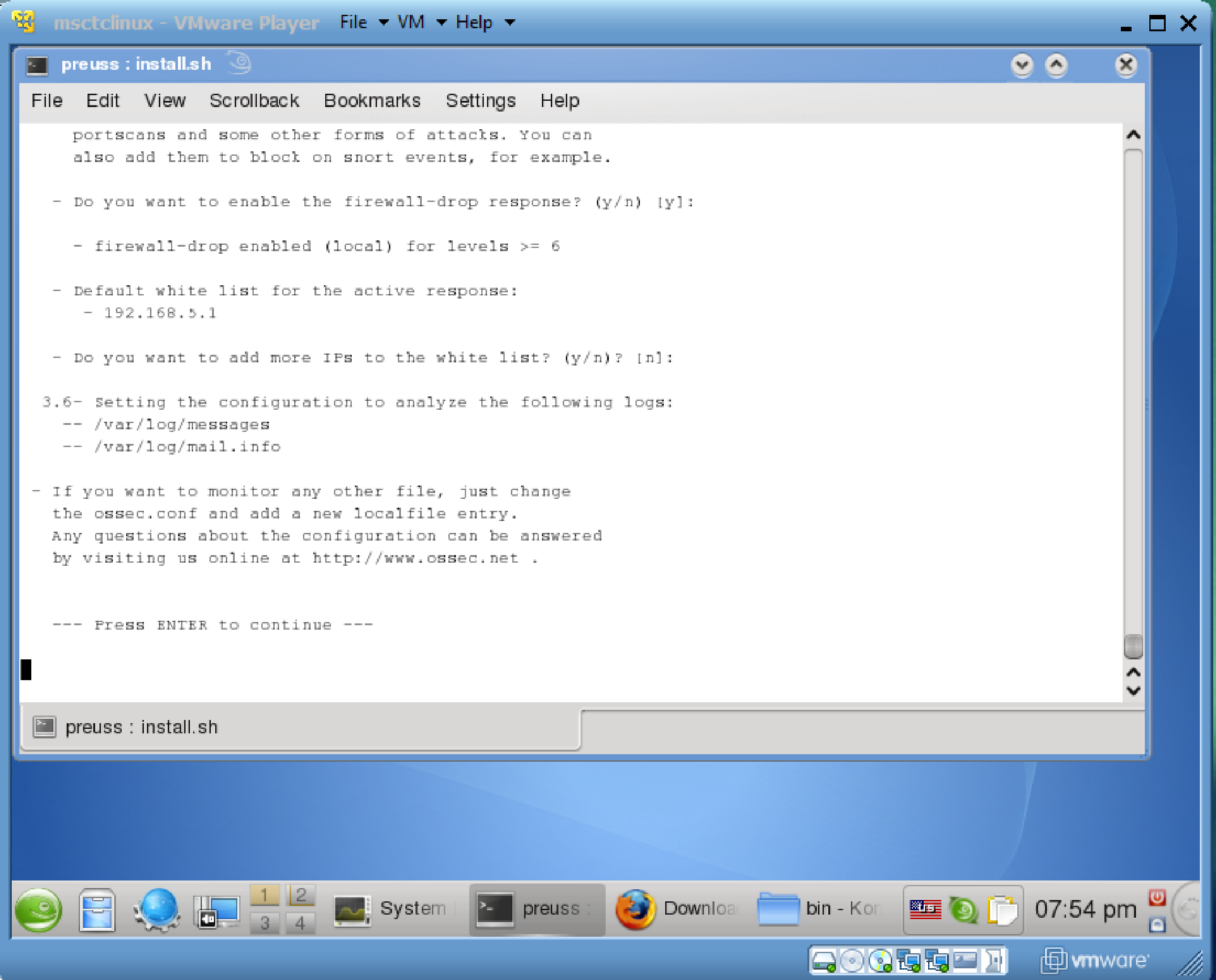

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
- System: Linux msctclinux 2.6.27.42-0.1-default
- User: root
- Host: msctclinux
-- Press ENTER to continue or Ctrl-C to abort. --
1- What kind of installation do you want (server, agent, local or help)? local
- Local installation chosen.
2- Setting up the installation environment.
- Choose where to install the OSSEC HIDS [/var/ossec]:
- Installation will be made at /var/ossec .
3- Configuring the OSSEC HIDS.
3.1- Do you want e-mail notification? (y/n) [y]: n
--- Email notification disabled.
3.2- Do you want to run the integrity check daemon? (y/n) [y]:
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:53 pm
To direct input to this virtual machine, press Ctrl+G.
vmware

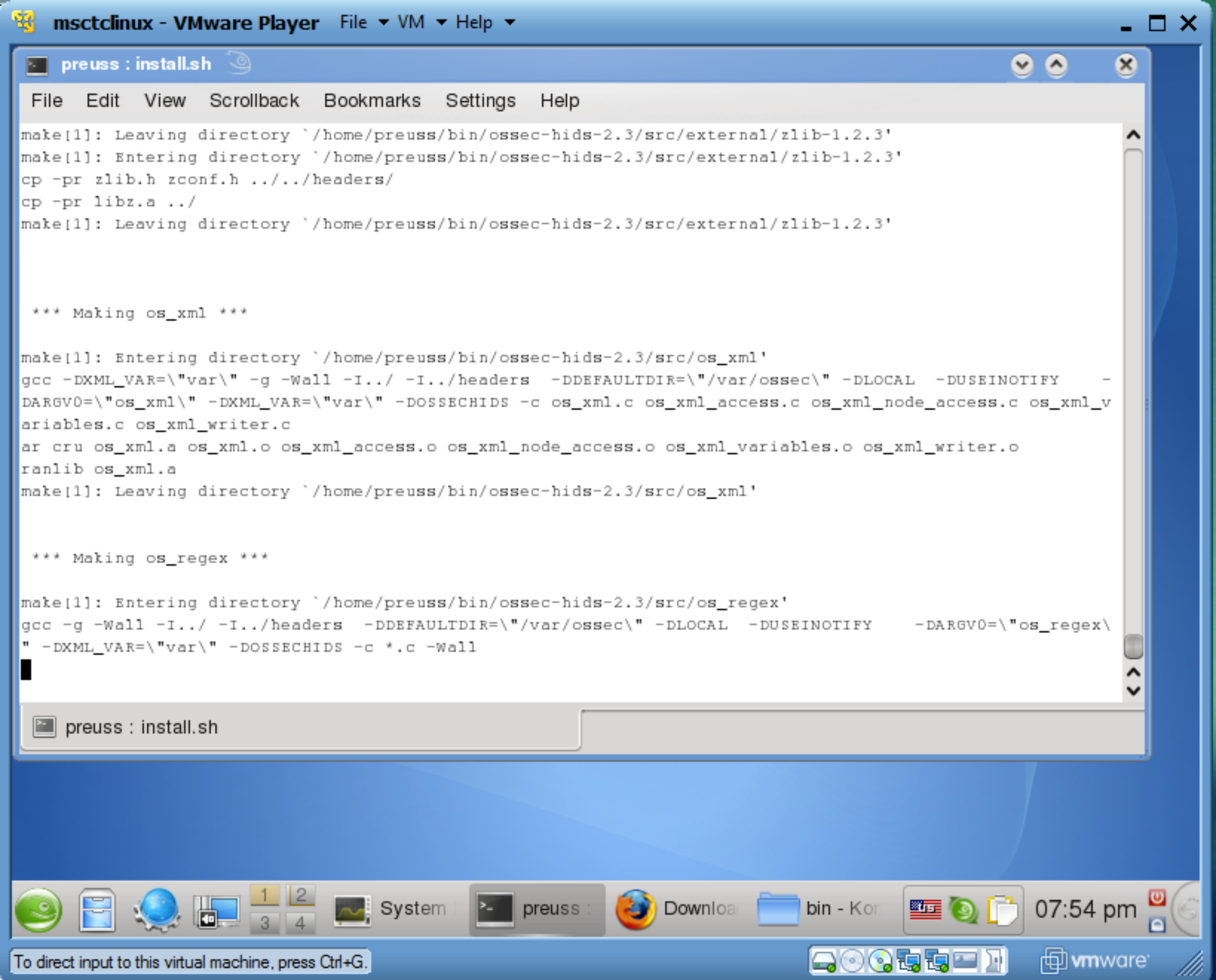

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
-- Press ENTER to continue or Ctrl-C to abort. --
1- What kind of installation do you want (server, agent, local or help)? local
- Local installation chosen.
2- Setting up the installation environment.
- Choose where to install the OSSEC HIDS [/var/ossec]:
- Installation will be made at /var/ossec .
3- Configuring the OSSEC HIDS.
3.1- Do you want e-mail notification? (y/n) [y]: n
--- Email notification disabled.
3.2- Do you want to run the integrity check daemon? (y/n) [y]:
- Running syscheck (integrity check daemon).
3.3- Do you want to run the rootkit detection engine? (y/n) [y]:
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:54 pm
To direct input to this virtual machine, press Ctrl+G.
vmware

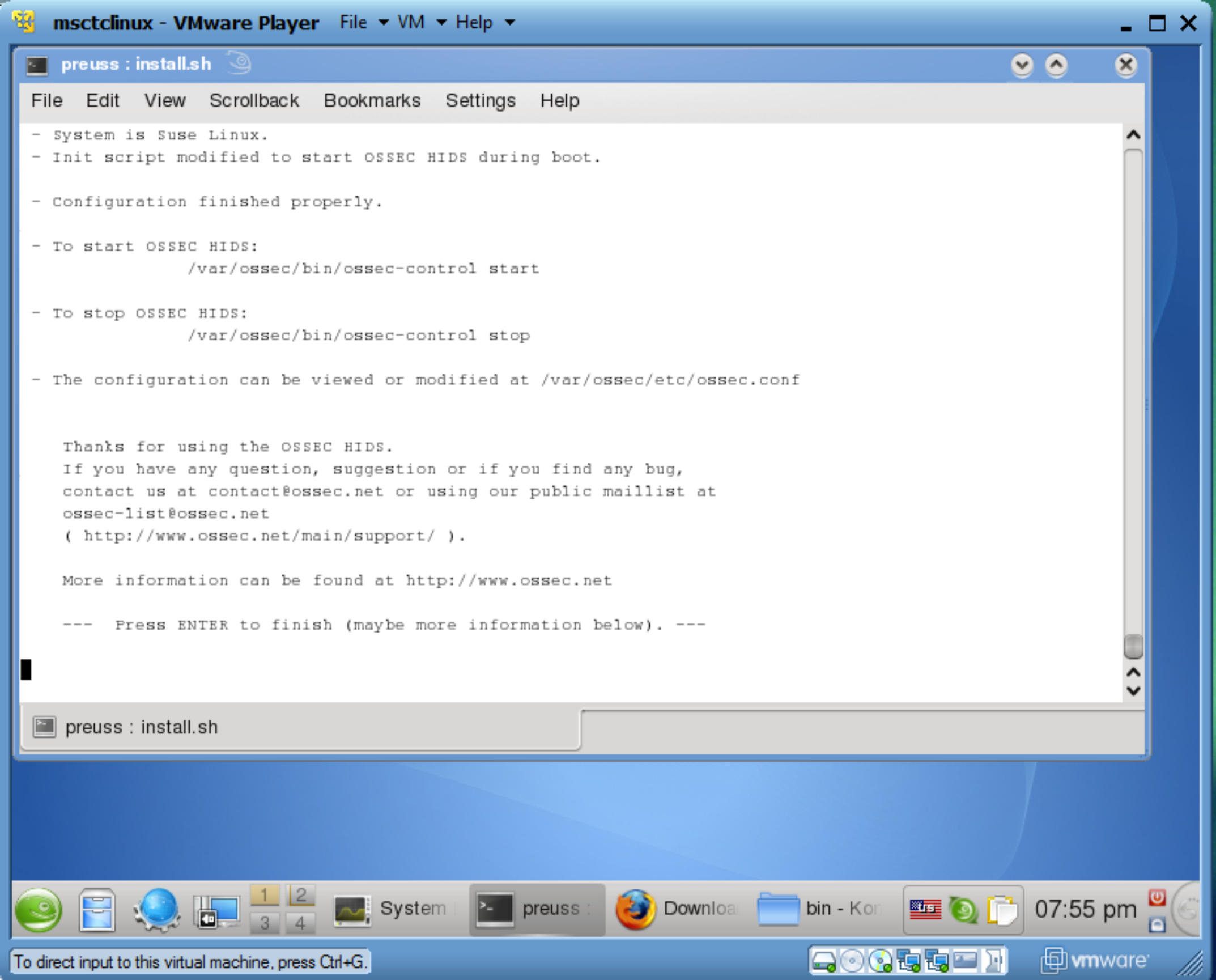

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
- Installation will be made at /var/ossec .
3- Configuring the OSSEC HIDS.
3.1- Do you want e-mail notification? (y/n) [y]: n
--- Email notification disabled.
3.2- Do you want to run the integrity check daemon? (y/n) [y]:
- Running syscheck (integrity check daemon).
3.3- Do you want to run the rootkit detection engine? (y/n) [y]:
- Running rootcheck (rootkit detection).
3.4- Active response allows you to execute a specific
command based on the events received. For example,
you can block an IP address or disable access for
a specific user.
More information at:
http://www.ossec.net/en/manual.html#active-response
- Do you want to enable active response? (y/n) [y]:
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:54 pm
To direct input to this virtual machine, press Ctrl+G.
vmware

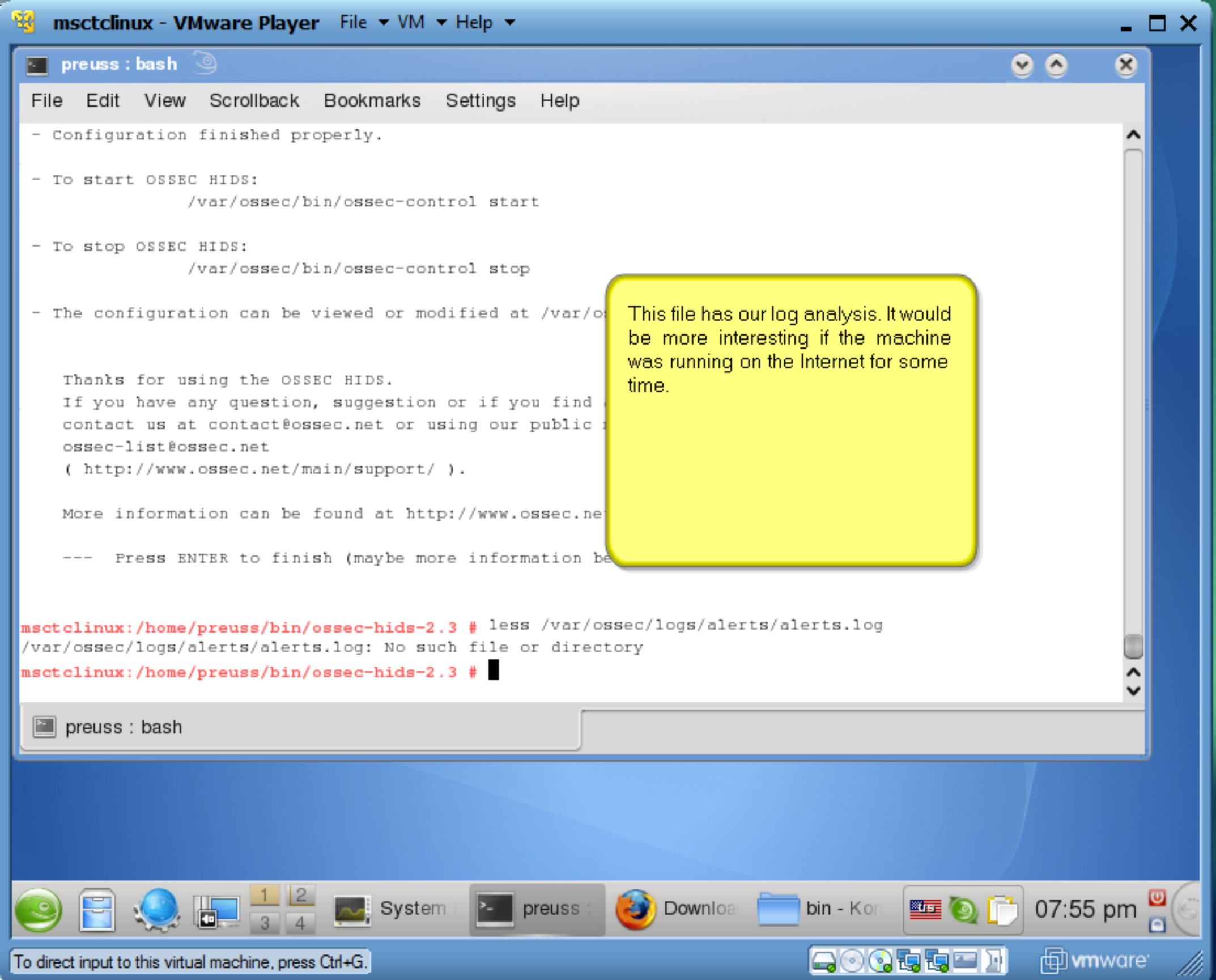

msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
3.3- Do you want to run the rootkit detection engine? (y/n) [y]:
- Running rootcheck (rootkit detection).
3.4- Active response allows you to execute a specific
command based on the events received. For example,
you can block an IP address or disable access for
a specific user.
More information at:
http://www.ossec.net/en/manual.html#active-response
- Do you want to enable active response? (y/n) [y]:
- Active response enabled.
- By default, we can enable the host-deny and the
firewall-drop responses. The first one will add
a host to the /etc/hosts.deny and the second one
will block the host on iptables (if linux) or on
ipfilter (if Solaris, FreeBSD or NetBSD).
- They can be used to stop SSHD brute force scans,
portscans and some other forms of attacks. You can
also add them to block on snort events, for example.
- Do you want to enable the firewall-drop response? (y/n) [y]:
preuss : install.sh
System
preuss :
bin - Kor
07:54 pm
To direct input to this virtual machine, press Ctrl+G.
vmware


msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
a specific user.
More information at:
http://www.ossec.net/en/manual.html#active-response
- Do you want to enable active response? (y/n) [y]:
- Active response enabled.
- By default, we can enable the host-deny and the
firewall-drop responses. The first one will add
a host to the /etc/hosts.deny and the second one
will block the host on iptables (if linux) or on
ipfilter (if Solaris, FreeBSD or NetBSD).
- They can be used to stop SSHD brute force scans,
portscans and some other forms of attacks. You can
also add them to block on snort events, for example.
- Do you want to enable the firewall-drop response? (y/n) [y]:
- firewall-drop enabled (local) for levels >= 6
- Default white list for the active response:
- 192.168.5.1
- Do you want to add more IPs to the white list? (y/n)? [n]:
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:54 pm
To direct input to this virtual machine, press Ctrl+G.
vmware


msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
portscans and some other forms of attacks. You can
also add them to block on snort events, for example.
- Do you want to enable the firewall-drop response? (y/n) [y]:
- firewall-drop enabled (local) for levels >= 6
- Default white list for the active response:
- 192.168.5.1
- Do you want to add more IPs to the white list? (y/n)? [n]:
3.6- Setting the configuration to analyze the following logs:
-- /var/log/messages
-- /var/log/mail.info
- If you want to monitor any other file, just change
the ossec.conf and add a new localfile entry.
Any questions about the configuration can be answered
by visiting us online at http://www.ossec.net .
--- Press ENTER to continue ---
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:54 pm
vmware


msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
make[1]: Leaving directory `/home/preuss/bin/ossec-hids-2.3/src/external/zlib-1.2.3'
make[1]: Entering directory `/home/preuss/bin/ossec-hids-2.3/src/external/zlib-1.2.3'
cp -pr zlib.h zconf.h ../../headers/
cp -pr libz.a ../
make[1]: Leaving directory `/home/preuss/bin/ossec-hids-2.3/src/external/zlib-1.2.3'
*** Making os_xml ***
make[1]: Entering directory `/home/preuss/bin/ossec-hids-2.3/src/os_xml'
gcc -DXML_VAR=\"var\" -g -Wall -I../ -I../headers -DDEFAULTDIR=\"/var/ossec\" -DLOCAL -DUSEINOTIFY -
DARGV0=\"os_xml\" -DXML_VAR=\"var\" -DOSSECHIDS -c os_xml.c os_xml_access.c os_xml_node_access.c os_xml_v
ariables.c os_xml_writer.c
ar cru os_xml.a os_xml.o os_xml_access.o os_xml_node_access.o os_xml_variables.o os_xml_writer.o
ranlib os_xml.a
make[1]: Leaving directory `/home/preuss/bin/ossec-hids-2.3/src/os_xml'
*** Making os_regex ***
make[1]: Entering directory `/home/preuss/bin/ossec-hids-2.3/src/os_regex'
gcc -g -Wall -I../ -I../headers -DDEFAULTDIR=\"/var/ossec\" -DLOCAL -DUSEINOTIFY -DARGV0=\"os_regex\
" -DXML_VAR=\"var\" -DOSSECHIDS -c *.c -Wall
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:54 pm
To direct input to this virtual machine, press Ctrl+G.
vmware


msctclinux - VMware Player
File
VM
Help
preuss : install.sh
File
Edit
View
Scrollback
Bookmarks
Settings
Help
- System is Suse Linux.
- Init script modified to start OSSEC HIDS during boot.
- Configuration finished properly.
- To start OSSEC HIDS:
/var/ossec/bin/ossec-control start
- To stop OSSEC HIDS:
/var/ossec/bin/ossec-control stop
- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf
Thanks for using the OSSEC HIDS.
If you have any question, suggestion or if you find any bug,
contact us at contact@ossec.net or using our public maillist at
ossec-list@ossec.net
(http://www.ossec.net/main/support/).
More information can be found at http://www.ossec.net
--- Press ENTER to finish (maybe more information below). ---
preuss : install.sh
System
preuss :
Downloa
bin - Kor
07:55 pm
To direct input to this virtual machine, press Ctrl+G.
vmware


msctclinux - VMware Player
File
VM
Help
preuss : bash
File
Edit
View
Scrollback
Bookmarks
Settings
Help
- Configuration finished properly.
- To start OSSEC HIDS:
/var/ossec/bin/ossec-control start
- To stop OSSEC HIDS:
/var/ossec/bin/ossec-control stop
- The configuration can be viewed or modified at /var/o
Thanks for using the OSSEC HIDS.
If you have any question, suggestion or if you find
contact us at contact@ossec.net or using our public
ossec-list@ossec.net
(http://www.ossec.net/main/support/).
More information can be found at http://www.ossec.ne
--- Press ENTER to finish (maybe more information be
This file has our log analysis. It would be more interesting if the machine was running on the Internet for some time.
msctclinux:/home/preuss/bin/ossec-hids-2.3 # less /var/ossec/logs/alerts/alerts.log
/var/ossec/logs/alerts/alerts.log: No such file or directory
msctclinux:/home/preuss/bin/ossec-hids-2.3 #
preuss : bash
System
preuss :
Downloa
bin - Kor
07:55 pm
To direct input to this virtual machine, press Ctrl+G.
vmware