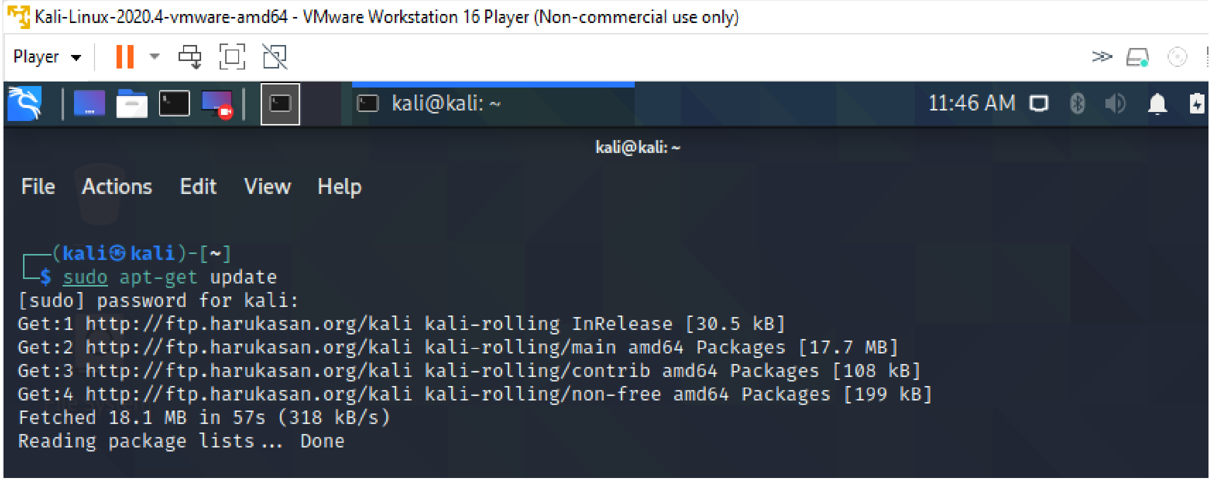
4/12/2021

LINUX, FIREWALLS AND VPN’S

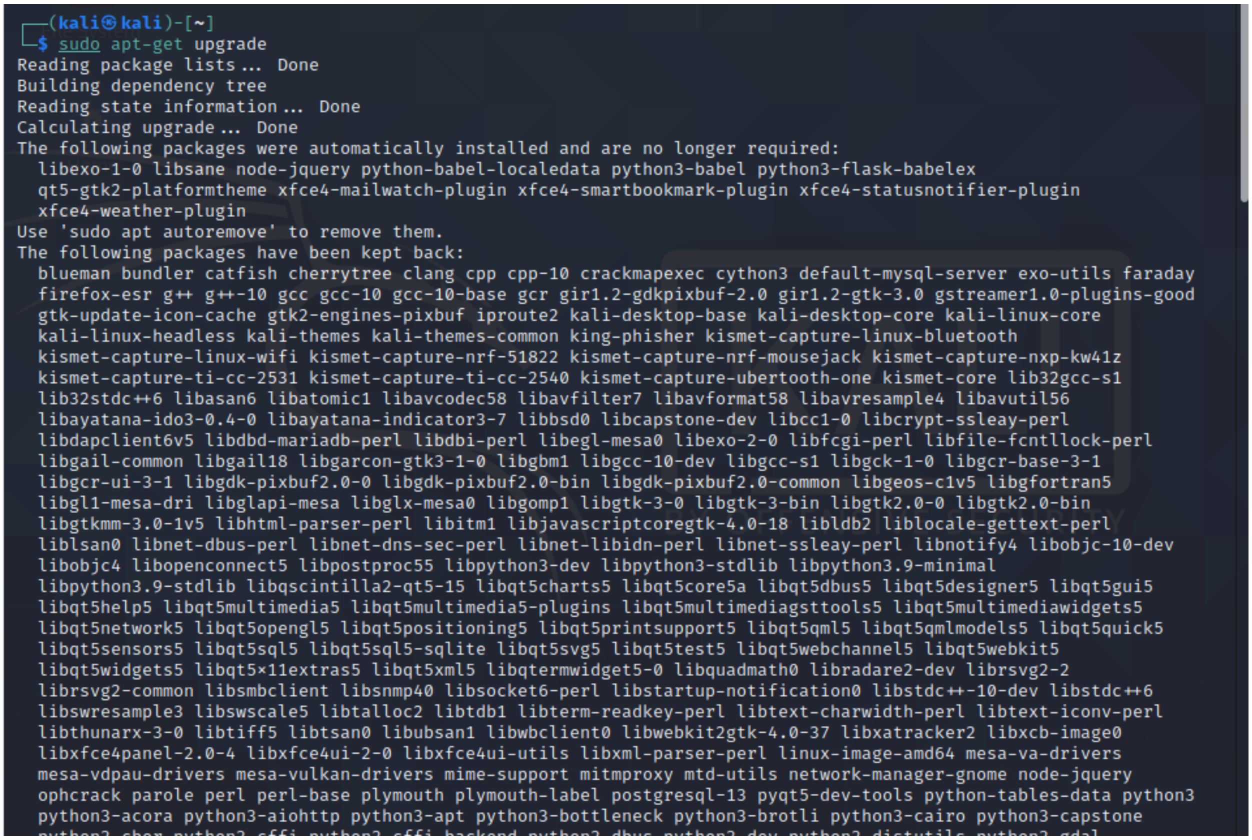
Contents

Task 1: LAB- USING LINUX FIREWALL TO BLOCK SSH AND ICMP

- UPDATE AND UPGRADE

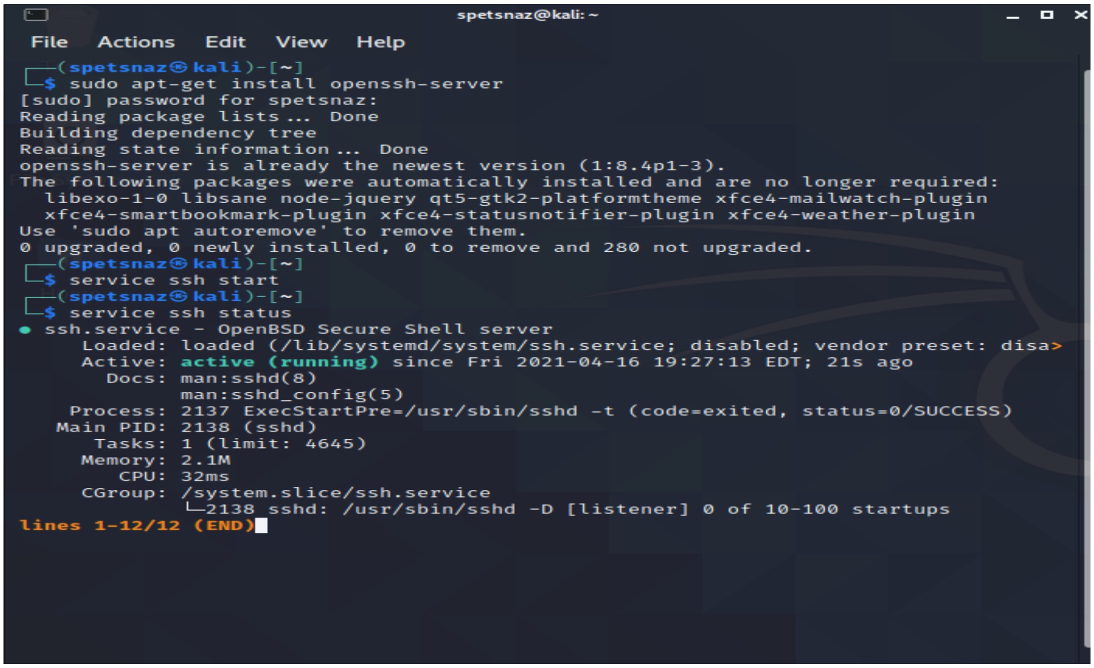

Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
11:46 AM
kali@kali: ~
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Packages [199 kB]
Fetched 18.1 MB in 57s (318 kB/s)
Reading package lists ... Done
```



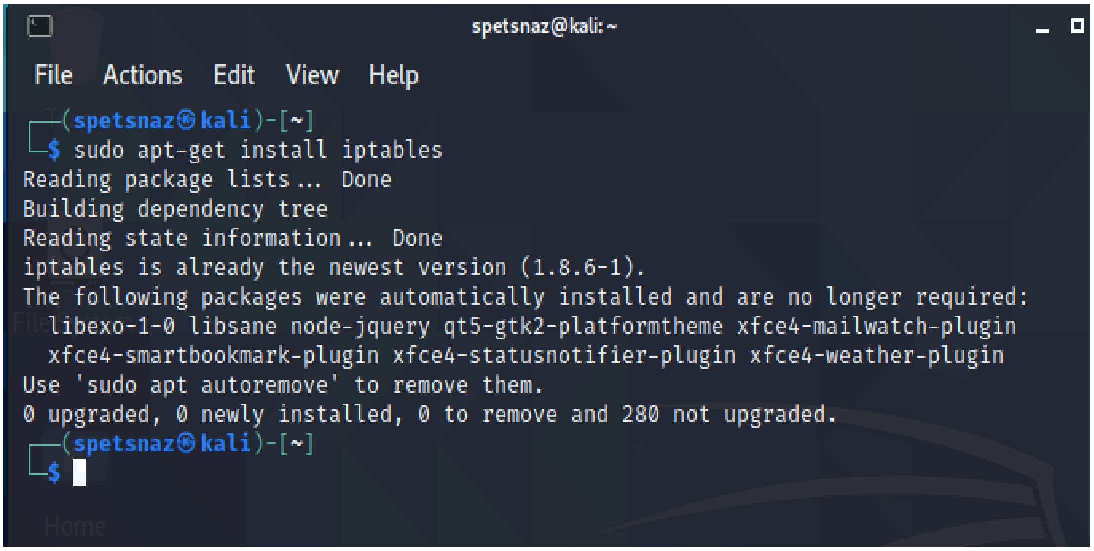
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  libexo-1-0 libsane node-jquery python-babel-localedata python3-babel python3-flask-babelex
  qt5-gtk2-platformtheme xfce4-mailwatch-plugin xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin
  xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  blueman bundler catfish cherrytree clang cpp cpp-10 crackmapexec cython3 default-mysql-server exo-utils faraday
  firefox-esr g++ g++-10 gcc gcc-10 gcc-10-base gcr gir1.2-gdkpixbuf-2.0 gir1.2-gtk-3.0 gstreamer1.0-plugins-good
  gtk-update-icon-cache gtk2-engines-pixbuf iproute2 kali-desktop-base kali-desktop-core kali-linux-core
  kali-linux-headless kali-themes kali-themes-common king-phisher kismet-capture-linux-bluetooth
  kismet-capture-linux-wifi kismet-capture-nrf-51822 kismet-capture-nrf-mousejack kismet-capture-nxp-kw41z
  kismet-capture-ti-cc-2531 kismet-capture-ti-cc-2540 kismet-capture-ubertooth-one kismet-core lib32gcc-s1
  lib32stdc++6 libasan6 libatomic1 libavcodec58 libavfilter7 libavformat58 libavresample4 libavutil56
  libayatana-ido3-0.4-0 libayatana-indicator3-7 libbsd0 libcapstone-dev libcc1-0 libcrypt-ssleay-perl
  libdapclient6v5 libdbd-mariadb-perl libdbi-perl libegl-mesa0 libexo-2-0 libfcgi-perl libfile-fcntllock-perl
  libgail-common libgail18 libgarcon-gtk3-1-0 libgbm1 libgcc-10-dev libgcc-s1 libgck-1-0 libgcr-base-3-1
  libgcr-ui-3-1 libgdk-pixbuf2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgeos-c1v5 libgfortran5
  libgl1-mesa-dri libglapi-mesa libglx-mesa0 libgomp1 libgtk-3-0 libgtk-3-bin libgtk2.0-0 libgtk2.0-bin
  libgtkmm-3.0-1v5 libhtml-parser-perl libitm1 libjavascriptcoregtk-4.0-18 libldb2 liblocale-gettext-perl
  liblsan0 libnet-dbus-perl libnet-dns-sec-perl libnet-libidn-perl libnet-ssleay-perl libnotify4 libobjc-10-dev
  libobjc4 libopenconnect5 libpostproc55 libpython3-dev libpython3-stdlib libpython3.9-minimal
  libpython3.9-stdlib libqscintilla2-qt5-15 libqt5charts5 libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5
  libqt5help5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5
  libqt5network5 libqt5opengl5 libqt5positioning5 libqt5printsupport5 libqt5qml5 libqt5qmlmodels5 libqt5quick5
  libqt5sensors5 libqt5sql5 libqt5sql5-sqlite libqt5svg5 libqt5test5 libqt5webchannel5 libqt5webkit5
  libqt5widgets5 libqt5x11extras5 libqt5xml5 libqtermwidget5-0 libquadmath0 libradare2-dev librsvg2-2
  librsvg2-common libsmbclient libsnmp40 libsocket6-perl libstartup-notification0 libstdc++-10-dev libstdc++6
  libswresample3 libswscale5 libtalloc2 libtdb1 libterm-readkey-perl libtext-charwidth-perl libtext-iconv-perl
  libthunarx-3-0 libtiff5 libtsan0 libubsan1 libwbclient0 libwebkit2gtk-4.0-37 libxatracker2 libxcb-image0
  libxfce4panel-2.0-4 libxfce4ui-2-0 libxfce4ui-utils libxml-parser-perl linux-image-amd64 mesa-va-drivers
  mesa-vdpau-drivers mesa-vulkan-drivers mime-support mitmproxy mtd-utils network-manager-gnome node-jquery
  ophcrack parole perl perl-base plymouth plymouth-label postgresql-13 pyqt5-dev-tools python-tables-data python3
  python3-acora python3-aiohttp python3-apt python3-bottleneck python3-brotli python3-cairo python3-capstone
  python3-cbor python3-cffi python3-cffi-backend python3-dbus python3-dev python3-distutils python3-gdal
```

❖ INSTALLING AND STARTING OPENSSH SERVER



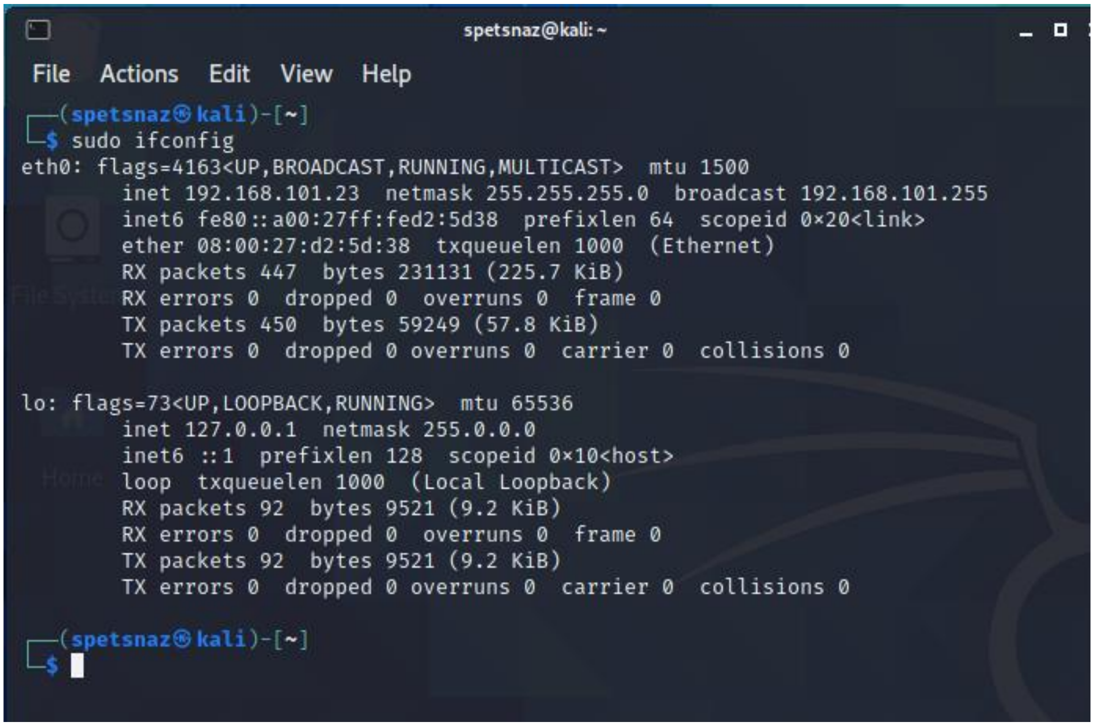
```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo apt-get install openssh-server
[sudo] password for spetsnaz:
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
openssh-server is already the newest version (1:8.4p1-3).
The following packages were automatically installed and are no longer required:
  libexo-1-0 libsane node-jquery qt5-gtk2-platformtheme xfce4-mailwatch-plugin
  xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 280 not upgraded.
┌──(spetsnaz㉿kali)-[~]
└─$ service ssh start
┌──(spetsnaz㉿kali)-[~]
└─$ service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disa>
     Active: active (running) since Fri 2021-04-16 19:27:13 EDT; 21s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 2137 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 2138 (sshd)
      Tasks: 1 (limit: 4645)
     Memory: 2.1M
        CPU: 32ms
     CGroup: /system.slice/ssh.service
             └─2138 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
lines 1-12/12 (END)
```

❖ INSTALLING IPTABLES



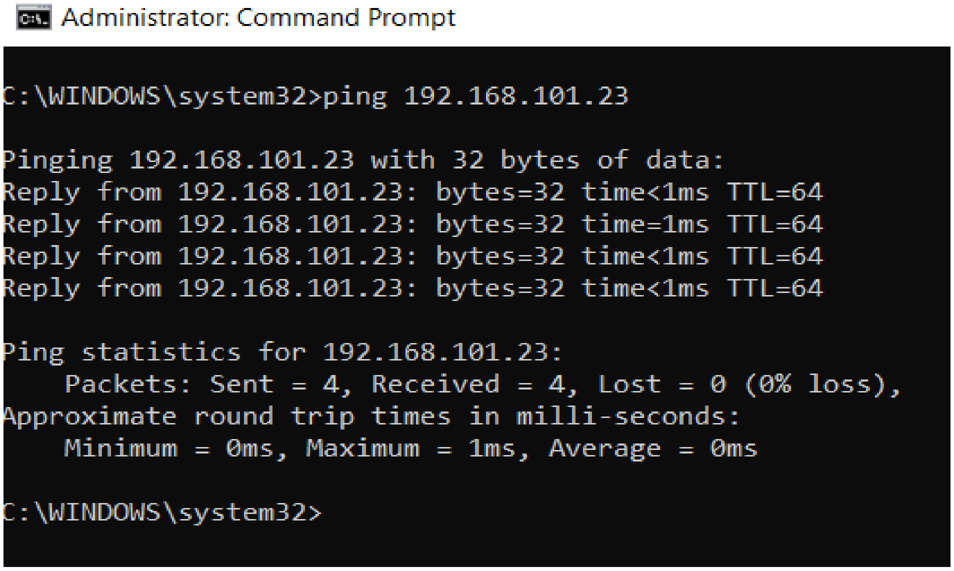
```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo apt-get install iptables
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
iptables is already the newest version (1.8.6-1).
The following packages were automatically installed and are no longer required:
  libexo-1-0 libsane node-jquery qt5-gtk2-platformtheme xfce4-mailwatch-plugin
  xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 280 not upgraded.
┌──(spetsnaz㉿kali)-[~]
└─$
```

- GETTING IP ADDRESS OF LINUX MACHINE

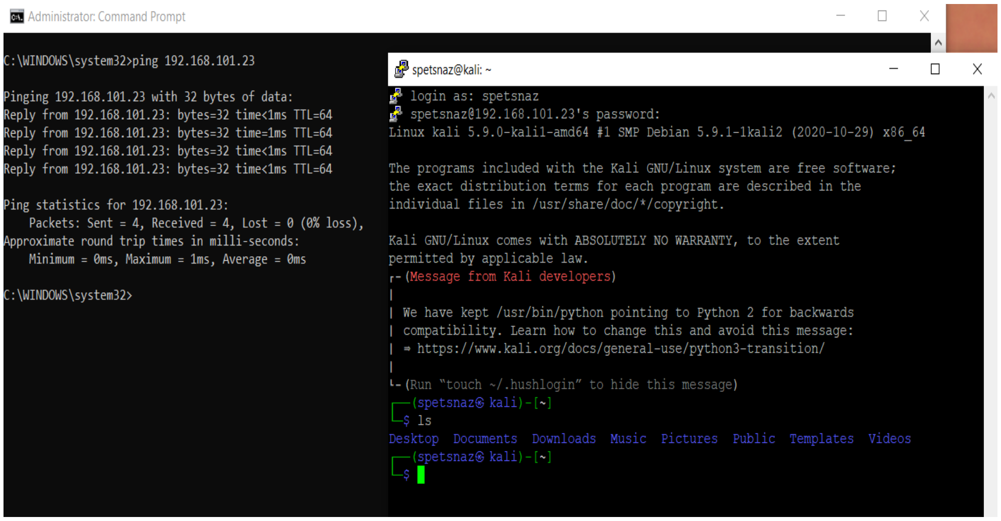


```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.101.23  netmask 255.255.255.0  broadcast 192.168.101.255
        inet6 fe80::a00:27ff:fed2:5d38  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d2:5d:38  txqueuelen 1000  (Ethernet)
        RX packets 447  bytes 231131 (225.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 450  bytes 59249 (57.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 92  bytes 9521 (9.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 92  bytes 9521 (9.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(spetsnaz㉿kali)-[~]
└─$ ▌
```

- PINGING LINUX FROM WINDOWS OR VICE VERSA



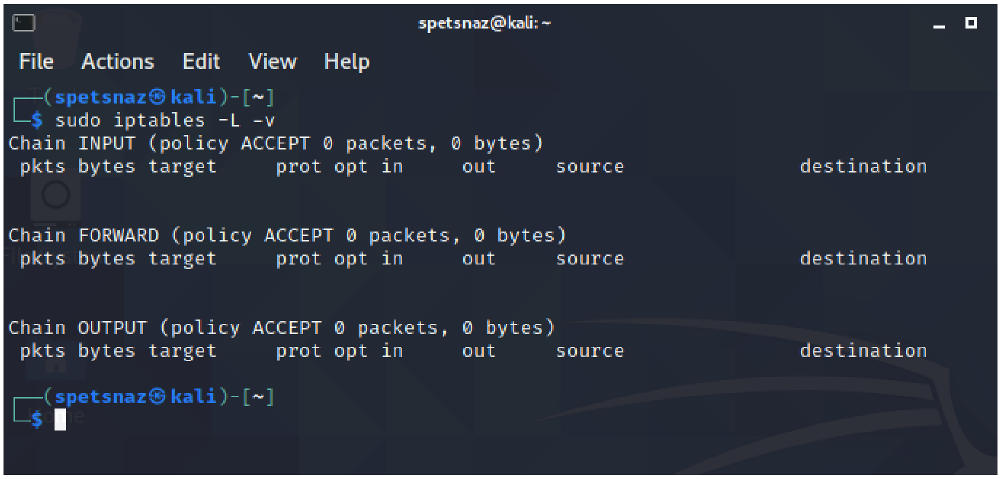
```
C:\WINDOWS\system32>ping 192.168.101.23

Pinging 192.168.101.23 with 32 bytes of data:
Reply from 192.168.101.23: bytes=32 time<1ms TTL=64
Reply from 192.168.101.23: bytes=32 time=1ms TTL=64
Reply from 192.168.101.23: bytes=32 time<1ms TTL=64
Reply from 192.168.101.23: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.101.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\WINDOWS\system32>
```



```
C:\WINDOWS\system32>ping 192.168.101.23

Pinging 192.168.101.23 with 32 bytes of data:
Reply from 192.168.101.23: bytes=32 time<1ms TTL=64
Reply from 192.168.101.23: bytes=32 time=1ms TTL=64
Reply from 192.168.101.23: bytes=32 time<1ms TTL=64
Reply from 192.168.101.23: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.101.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\WINDOWS\system32>
```

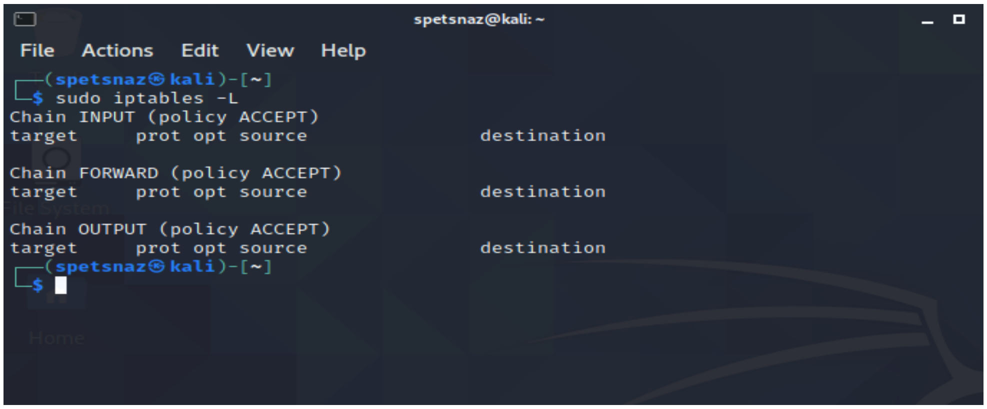
```
login as: spetsnaz
spetsnaz@192.168.101.23's password:
Linux kali 5.9.0-kali1-amd64 #1 SMP Debian 5.9.1-1kali2 (2020-10-29) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run “touch ~/.hushlogin” to hide this message)
┌──(spetsnaz㉿ kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
┌──(spetsnaz㉿ kali)-[~]
└─$ 
```

❖ CHECKING LIST OF IPTABLES



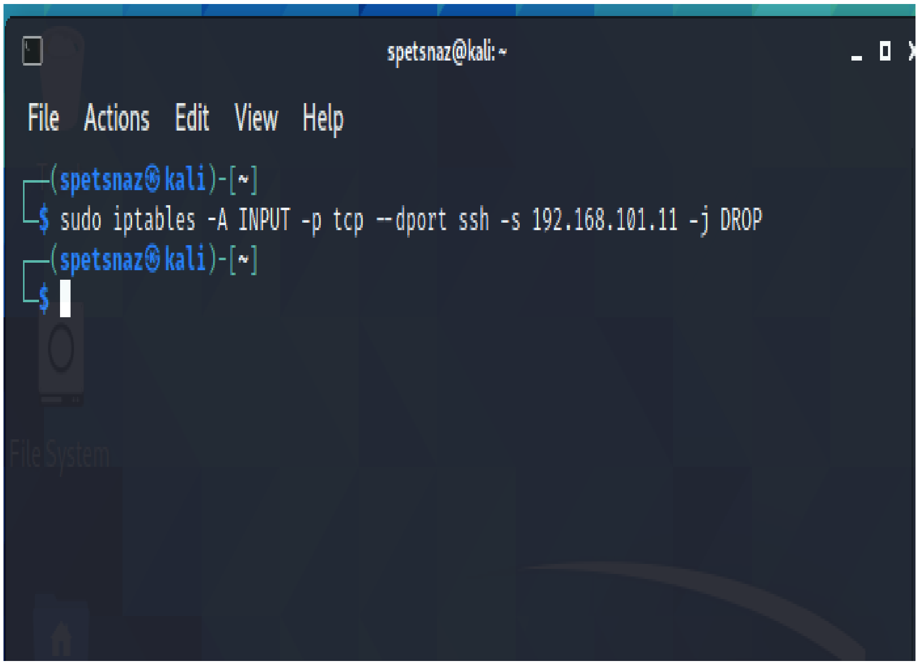
```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

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

┌──(spetsnaz㉿kali)-[~]
└─$ 
```

❖ CHECK POLICY OF THE FIREWALL

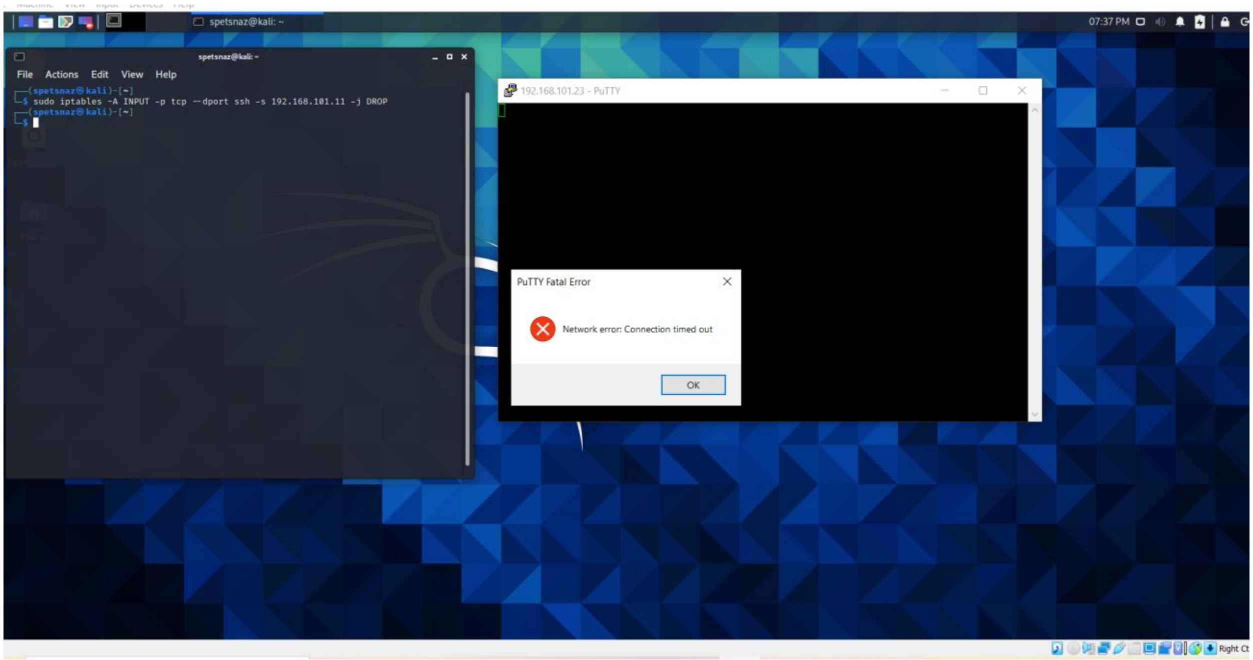


```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

❖ BLOCKING SSH CONNECTIONS

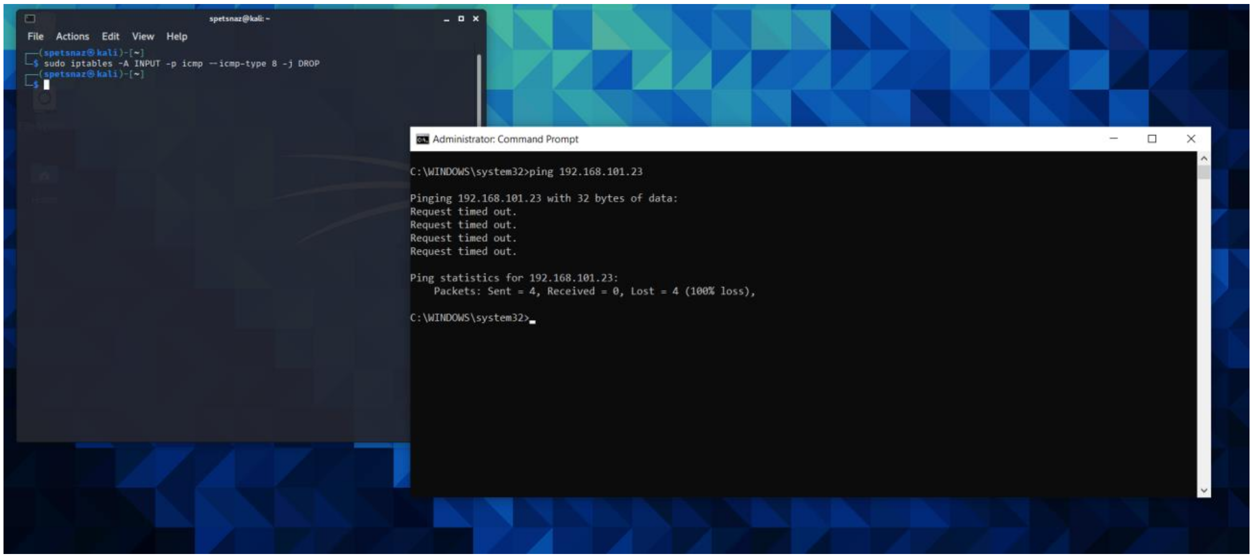


```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport ssh -s 192.168.101.11 -j DROP
┌──(spetsnaz㉿kali)-[~]
└─$ 
```



```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport ssh -s 192.168.101.11 -j DROP
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

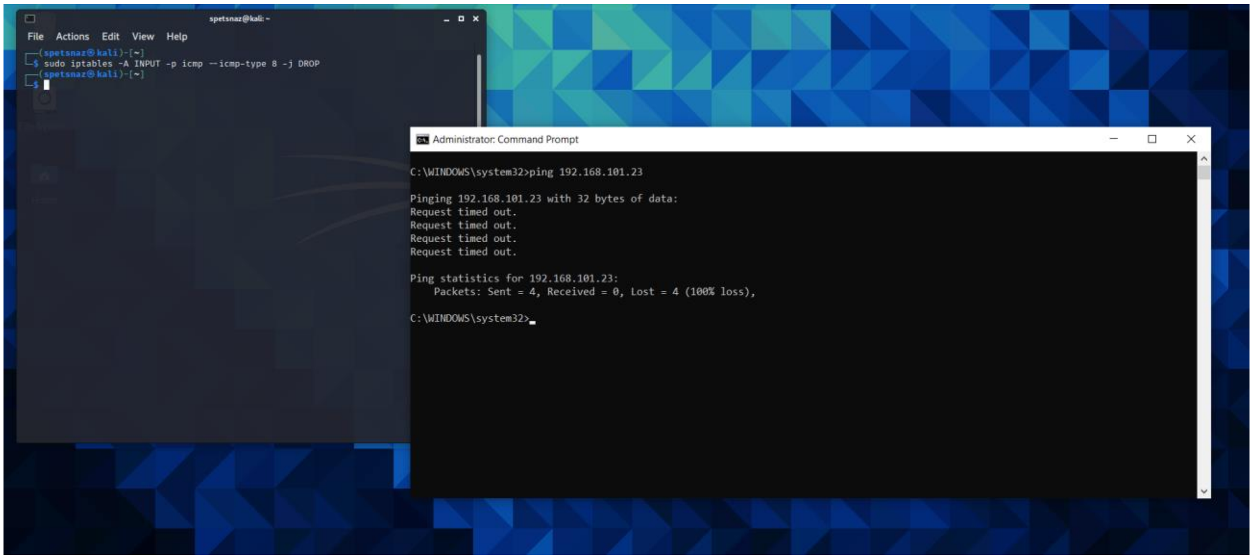
Network error: Connection timed out



```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

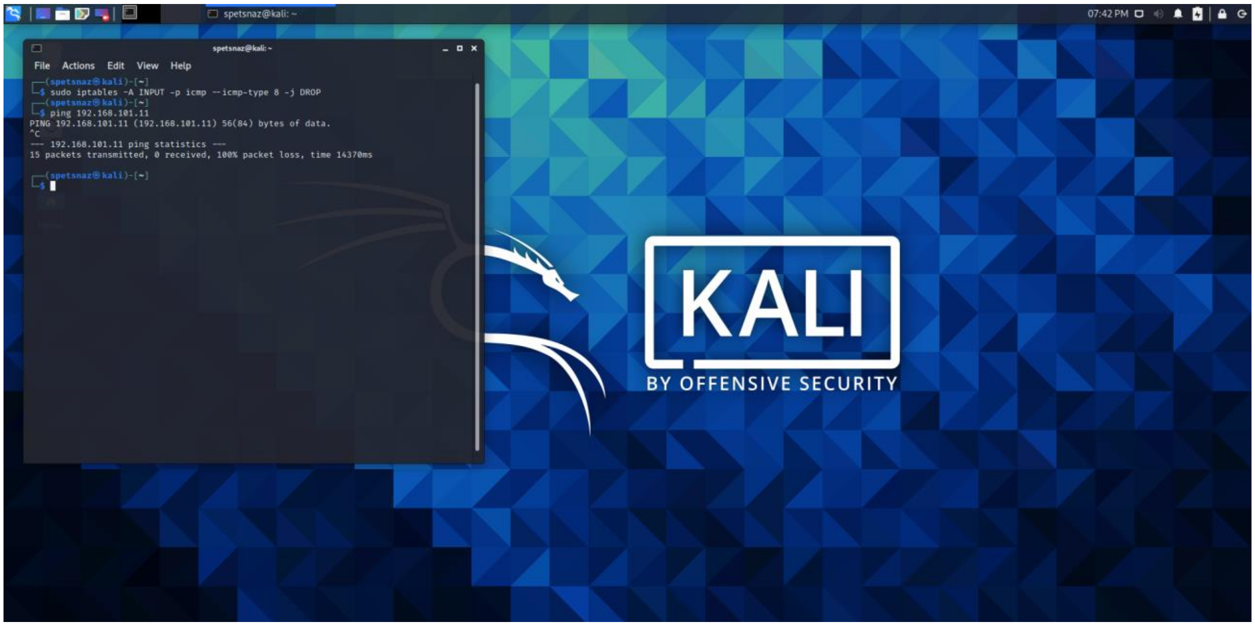
```
C:\WINDOWS\system32>ping 192.168.101.23

Pinging 192.168.101.23 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.101.23:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>_
```

- ❖ PINGING WINDOWS FROM LINUX AGAIN (ICMP PING REQUEST)



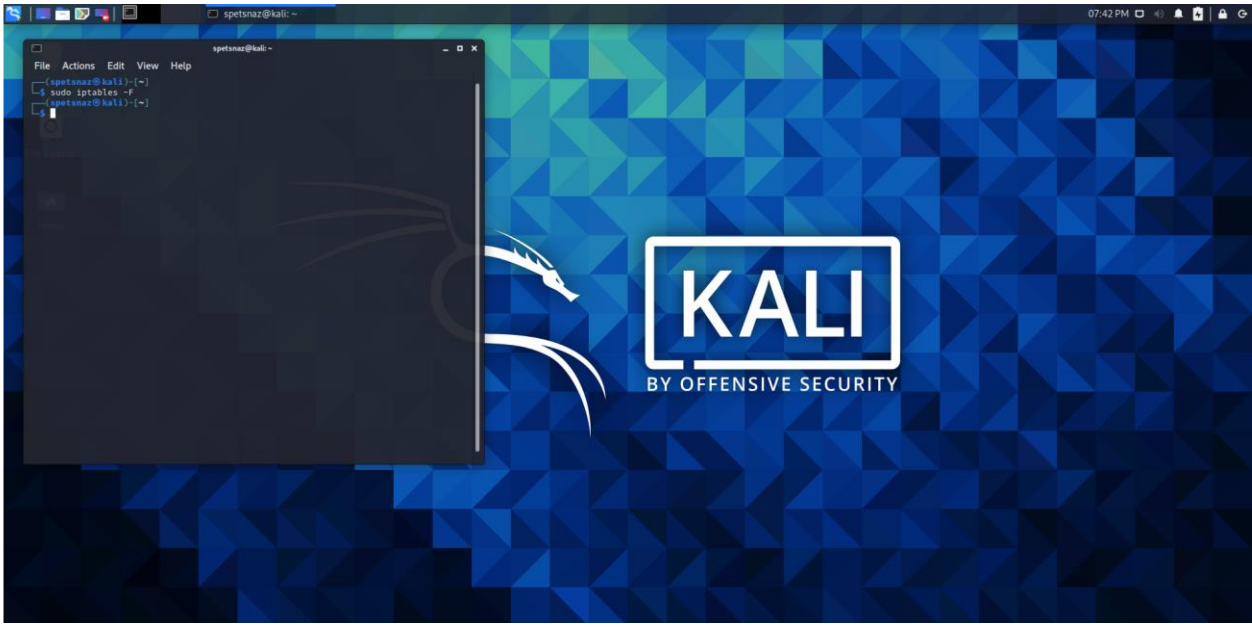
```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

```
C:\WINDOWS\system32>ping 192.168.101.23

Pinging 192.168.101.23 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.101.23:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>_
```



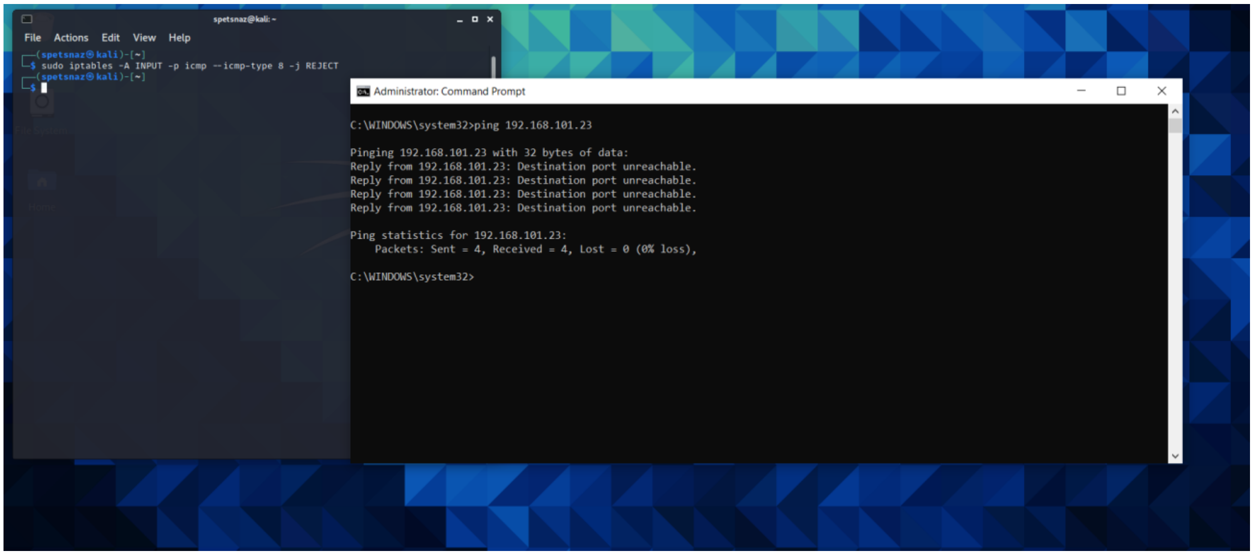
```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP
┌──(spetsnaz㉿kali)-[~]
└─$ ping 192.168.101.11
PING 192.168.101.11 (192.168.101.11) 56(84) bytes of data.
^C
--- 192.168.101.11 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14370ms

┌──(spetsnaz㉿kali)-[~]
└─$ 
```

- ❖ FLASHING THE EXISTING RULES



```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -F
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

- REJECTING ICMP PING REQUEST

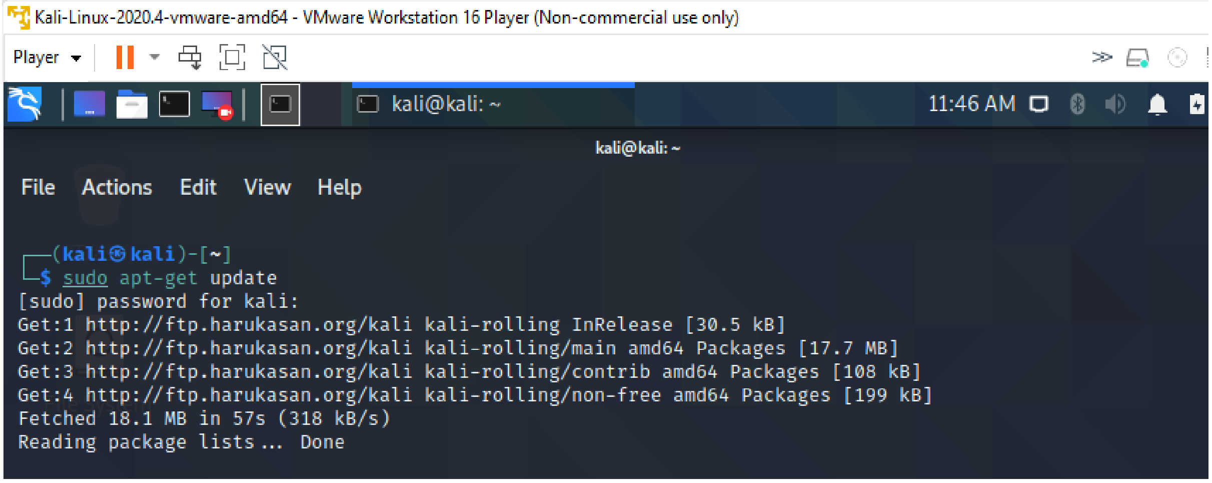


```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo iptables -A INPUT -p icmp --icmp-type 8 -j REJECT
┌──(spetsnaz㉿kali)-[~]
└─$
```

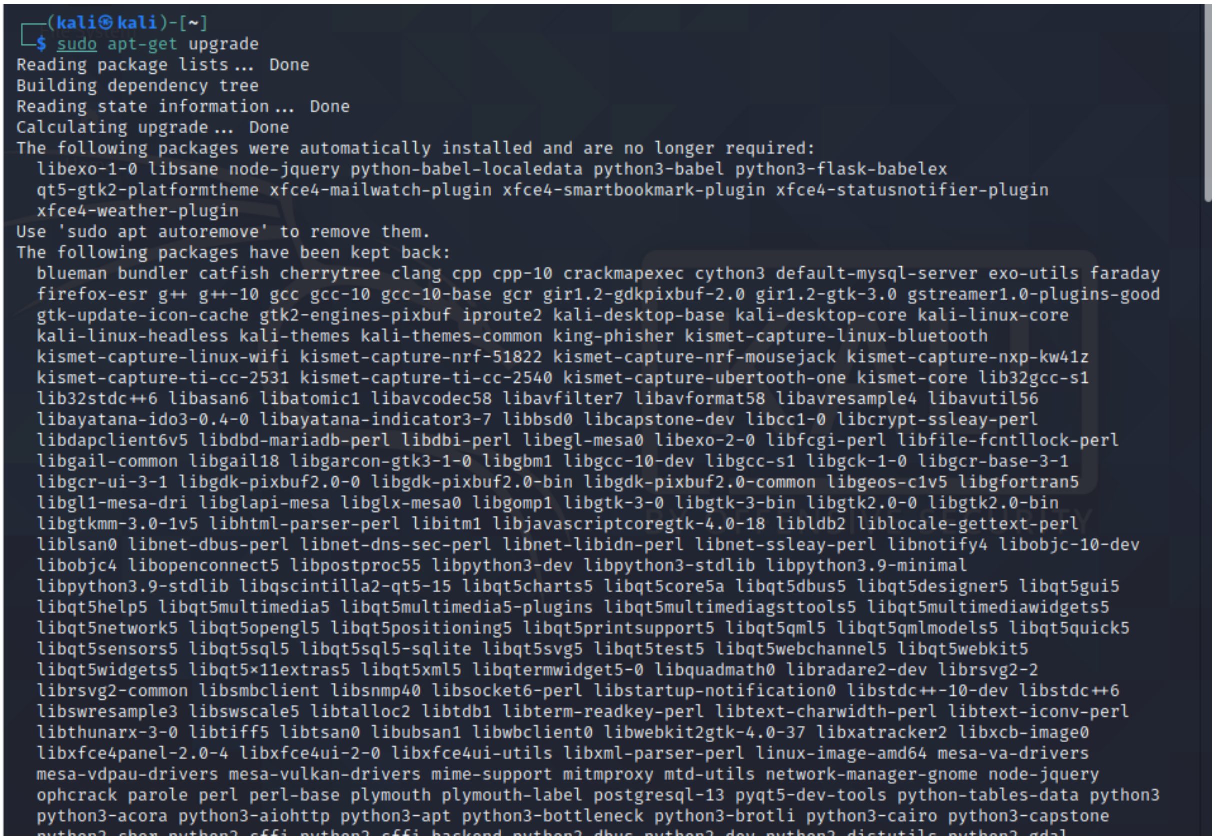
```
C:\WINDOWS\system32>ping 192.168.101.23

Pinging 192.168.101.23 with 32 bytes of data:
Reply from 192.168.101.23: Destination port unreachable.
Reply from 192.168.101.23: Destination port unreachable.
Reply from 192.168.101.23: Destination port unreachable.
Reply from 192.168.101.23: Destination port unreachable.

Ping statistics for 192.168.101.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\WINDOWS\system32>
```

Task 2: LINUX LAB 2- SNORT

- UPDATE AND UPGRADE

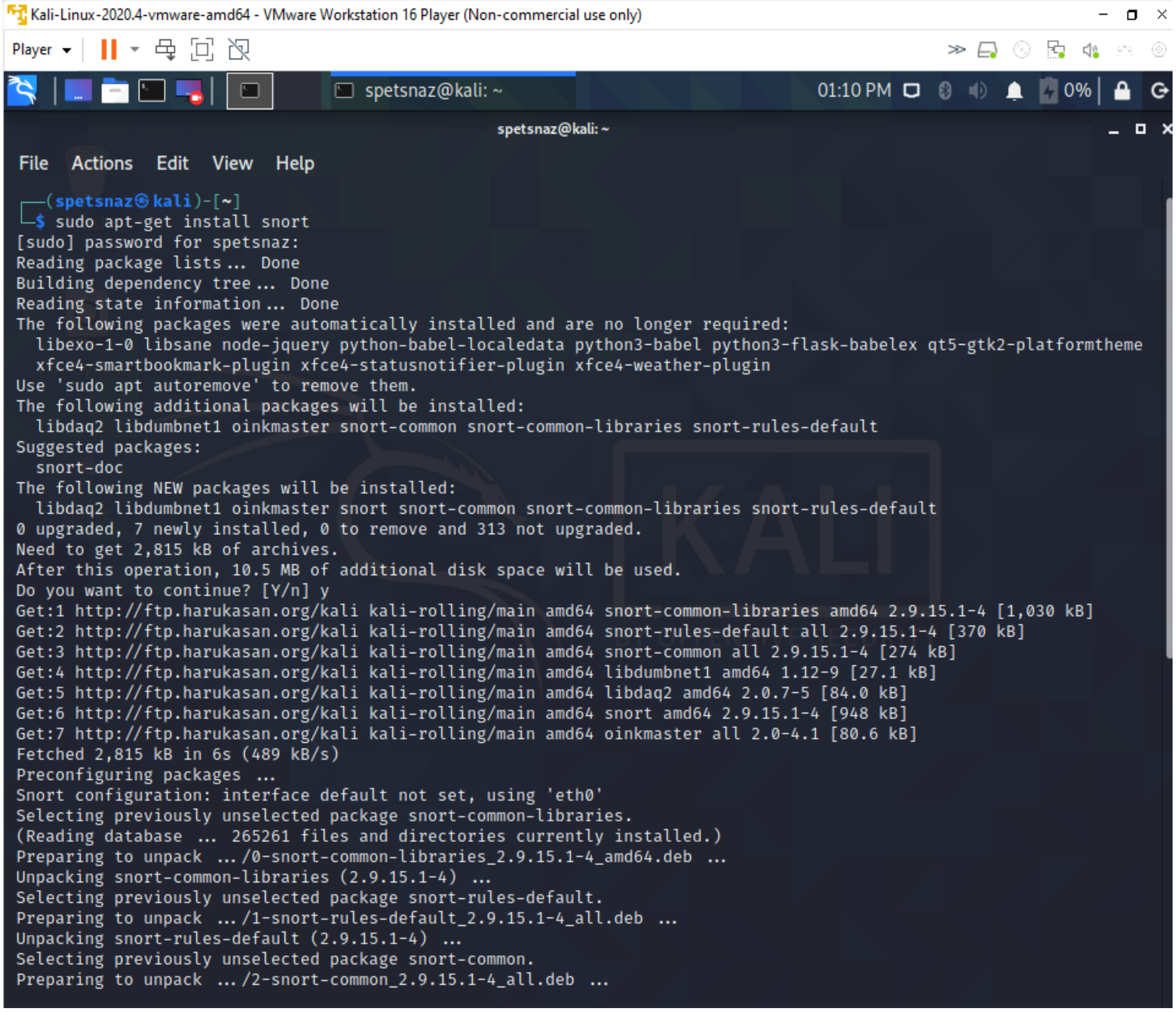

Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
11:46 AM
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/non-free amd64 Packages [199 kB]
Fetched 18.1 MB in 57s (318 kB/s)
Reading package lists ... Done
```



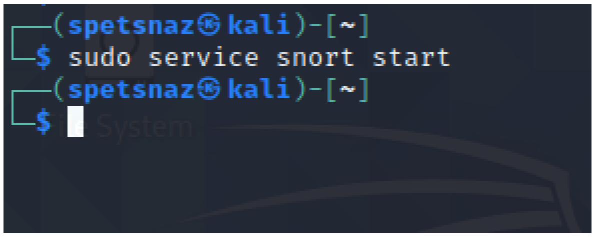
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libexo-1-0 libsane node-jquery python-babel-localedata python3-babel python3-flask-babelex
  qt5-gtk2-platformtheme xfce4-mailwatch-plugin xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin
  xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  blueman bundler catfish cherrytree clang cpp cpp-10 crackmapexec cython3 default-mysql-server exo-utils faraday
  firefox-esr g++ g++-10 gcc gcc-10 gcc-10-base gcr gir1.2-gdkpixbuf-2.0 gir1.2-gtk-3.0 gstreamer1.0-plugins-good
  gtk-update-icon-cache gtk2-engines-pixbuf iproute2 kali-desktop-base kali-desktop-core kali-linux-core
  kali-linux-headless kali-themes kali-themes-common king-phisher kismet-capture-linux-bluetooth
  kismet-capture-linux-wifi kismet-capture-nrf-51822 kismet-capture-nrf-mousejack kismet-capture-nxp-kw41z
  kismet-capture-ti-cc-2531 kismet-capture-ti-cc-2540 kismet-capture-ubertooth-one kismet-core lib32gcc-s1
  lib32stdc++6 libasan6 libatomic1 libavcodec58 libavfilter7 libavformat58 libavresample4 libavutil56
  libayatana-ido3-0.4-0 libayatana-indicator3-7 libbsd0 libcapstone-dev libcc1-0 libcrypt-ssleay-perl
  libdapclient6v5 libdbd-mariadb-perl libdbi-perl libegl-mesa0 libexo-2-0 libfcgi-perl libfile-fcntllock-perl
  libgail-common libgail18 libgarcon-gtk3-1-0 libgbm1 libgcc-10-dev libgcc-s1 libgck-1-0 libgcr-base-3-1
  libgcr-ui-3-1 libgdk-pixbuf2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgeos-c1v5 libgfortran5
  libgl1-mesa-dri libglapi-mesa libglx-mesa0 libgomp1 libgtk-3-0 libgtk-3-bin libgtk2.0-0 libgtk2.0-bin
  libgtkmm-3.0-1v5 libhtml-parser-perl libitm1 libjavascriptcoregtk-4.0-18 libldb2 liblocale-gettext-perl
  liblsan0 libnet-dbus-perl libnet-dns-sec-perl libnet-libidn-perl libnet-ssleay-perl libnotify4 libobjc-10-dev
  libobjc4 libopenconnect5 libpostproc55 libpython3-dev libpython3-stdlib libpython3.9-minimal
  libpython3.9-stdlib libqscintilla2-qt5-15 libqt5charts5 libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5
  libqt5help5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5
  libqt5network5 libqt5opengl5 libqt5positioning5 libqt5printsupport5 libqt5qml5 libqt5qmlmodels5 libqt5quick5
  libqt5sensors5 libqt5sql5 libqt5sql5-sqlite libqt5svg5 libqt5test5 libqt5webchannel5 libqt5webkit5
  libqt5widgets5 libqt5x11extras5 libqt5xml5 libqtermwidget5-0 libquadmath0 libradare2-dev librsvg2-2
  librsvg2-common libsmbclient libsnmp40 libsocket6-perl libstartup-notification0 libstdc++-10-dev libstdc++6
  libswresample3 libswscale5 libtalloc2 libtdb1 libterm-readkey-perl libtext-charwidth-perl libtext-iconv-perl
  libthunarx-3-0 libtiff5 libtsan0 libubsan1 libwbclient0 libwebkit2gtk-4.0-37 libxatracker2 libxcb-image0
  libxfce4panel-2.0-4 libxfce4ui-2-0 libxfce4ui-utils libxml-parser-perl linux-image-amd64 mesa-va-drivers
  mesa-vdpau-drivers mesa-vulkan-drivers mime-support mitmproxy mtd-utils network-manager-gnome node-jquery
  ophcrack parole perl perl-base plymouth plymouth-label postgresql-13 pyqt5-dev-tools python-tables-data python3
  python3-acora python3-aiohttp python3-apt python3-bottleneck python3-brotli python3-cairo python3-capstone
  python3-cbor python3-cffi python3-cffi-backend python3-dbus python3-dev python3-distutils python3-gdal
```

- INSTALLING SNORT-below image


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
spetsnaz@kali: ~
01:10 PM
0%
spetsnaz@kali: ~
File
Actions
Edit
View
Help

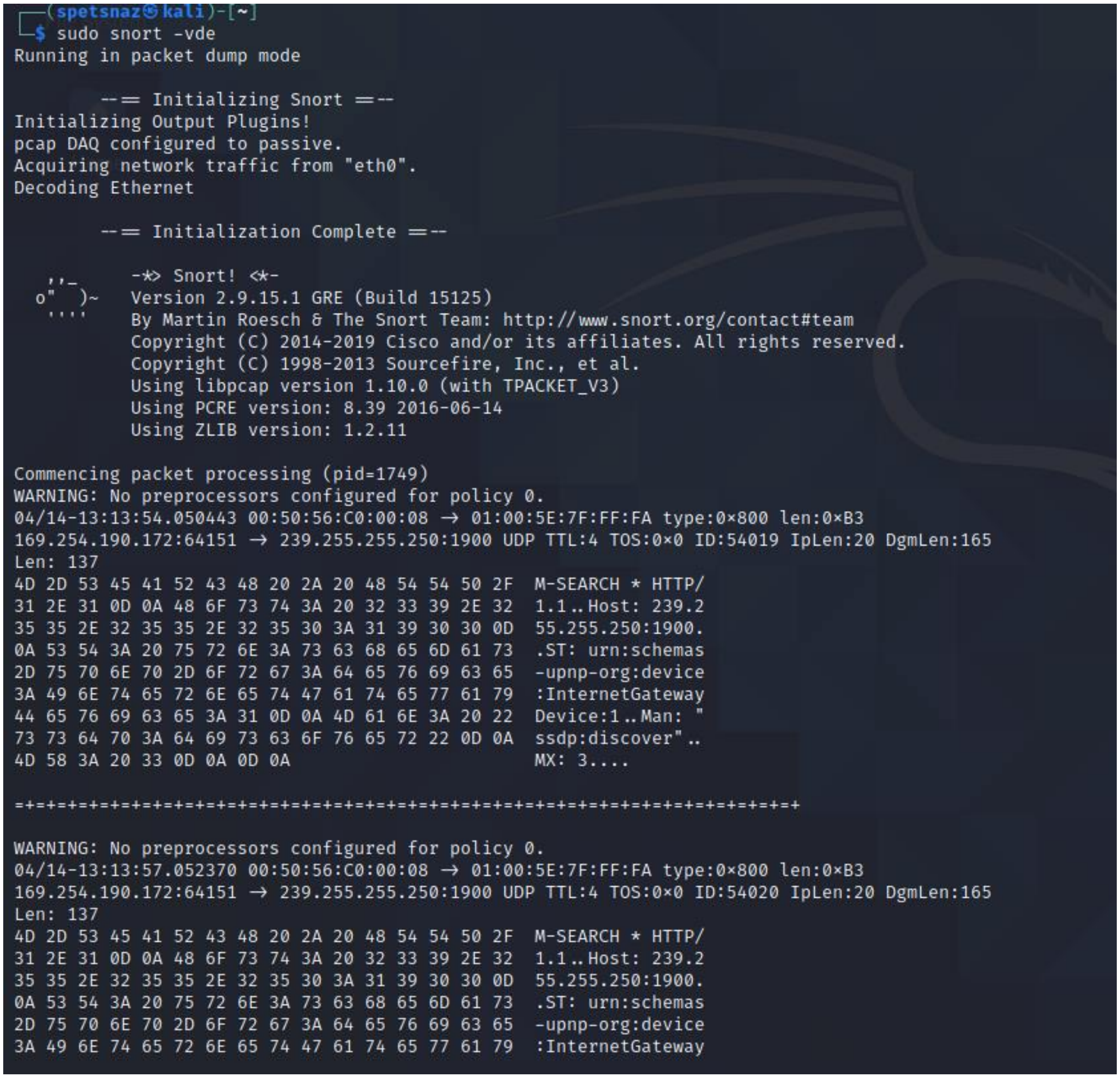
```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo apt-get install snort
[sudo] password for spetsnaz:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libexo-1-0 libsane node-jquery python-babel-localedata python3-babel python3-flask-babelex qt5-gtk2-platformtheme
  xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries snort-rules-default
0 upgraded, 7 newly installed, 0 to remove and 313 not upgraded.
Need to get 2,815 kB of archives.
After this operation, 10.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 snort-common-libraries amd64 2.9.15.1-4 [1,030 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 snort-rules-default all 2.9.15.1-4 [370 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 snort-common all 2.9.15.1-4 [274 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 libdumbnet1 amd64 1.12-9 [27.1 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 libdaq2 amd64 2.0.7-5 [84.0 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 snort amd64 2.9.15.1-4 [948 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 oinkmaster all 2.0-4.1 [80.6 kB]
Fetched 2,815 kB in 6s (489 kB/s)
Preconfiguring packages ...
Snort configuration: interface default not set, using 'eth0'
Selecting previously unselected package snort-common-libraries.
(Reading database ... 265261 files and directories currently installed.)
Preparing to unpack .../0-snort-common-libraries_2.9.15.1-4_amd64.deb ...
Unpacking snort-common-libraries (2.9.15.1-4) ...
Selecting previously unselected package snort-rules-default.
Preparing to unpack .../1-snort-rules-default_2.9.15.1-4_all.deb ...
Unpacking snort-rules-default (2.9.15.1-4) ...
Selecting previously unselected package snort-common.
Preparing to unpack .../2-snort-common_2.9.15.1-4_all.deb ...
```

- STARTING SNORT SERVICE

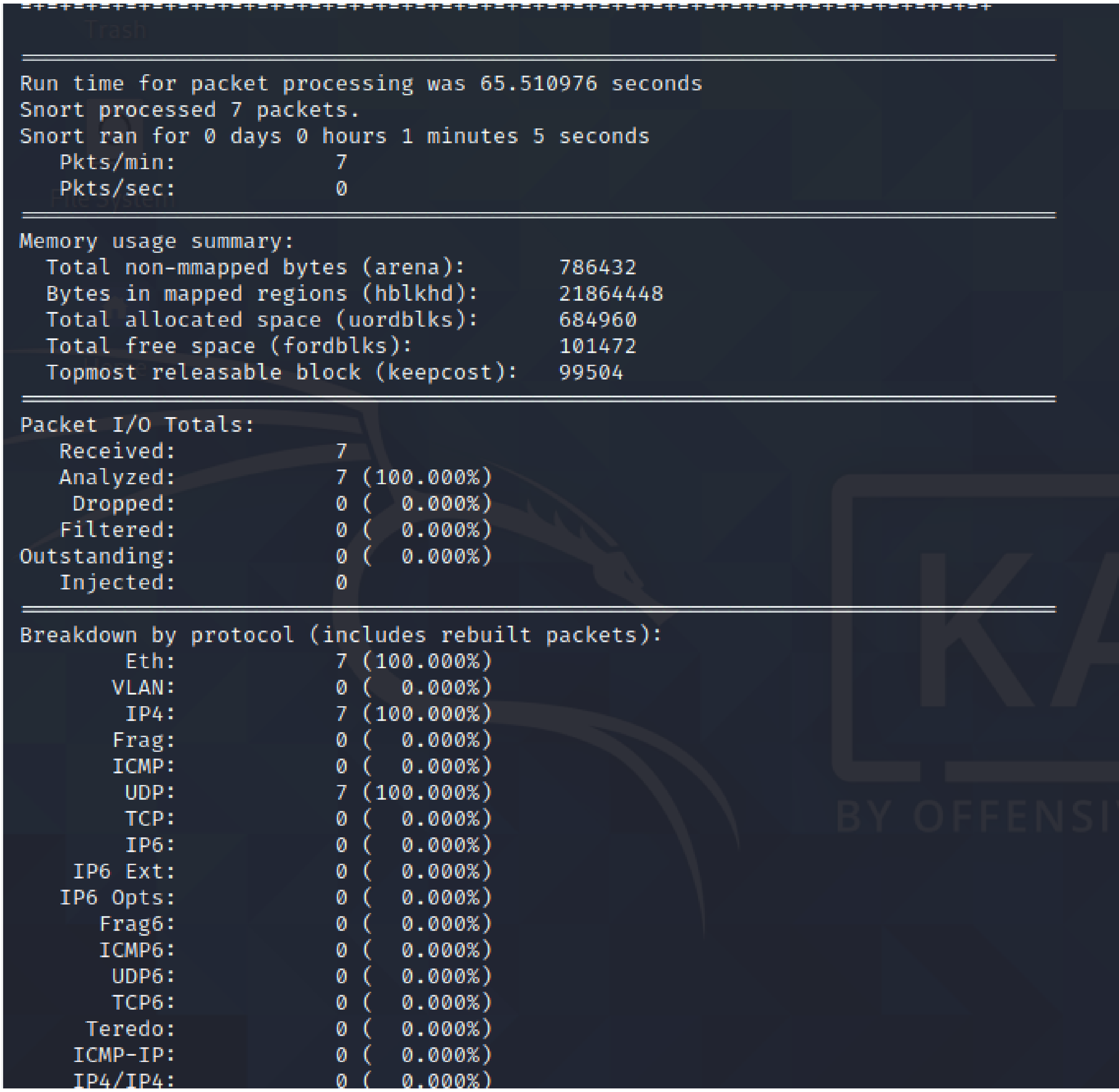


```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo service snort start
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

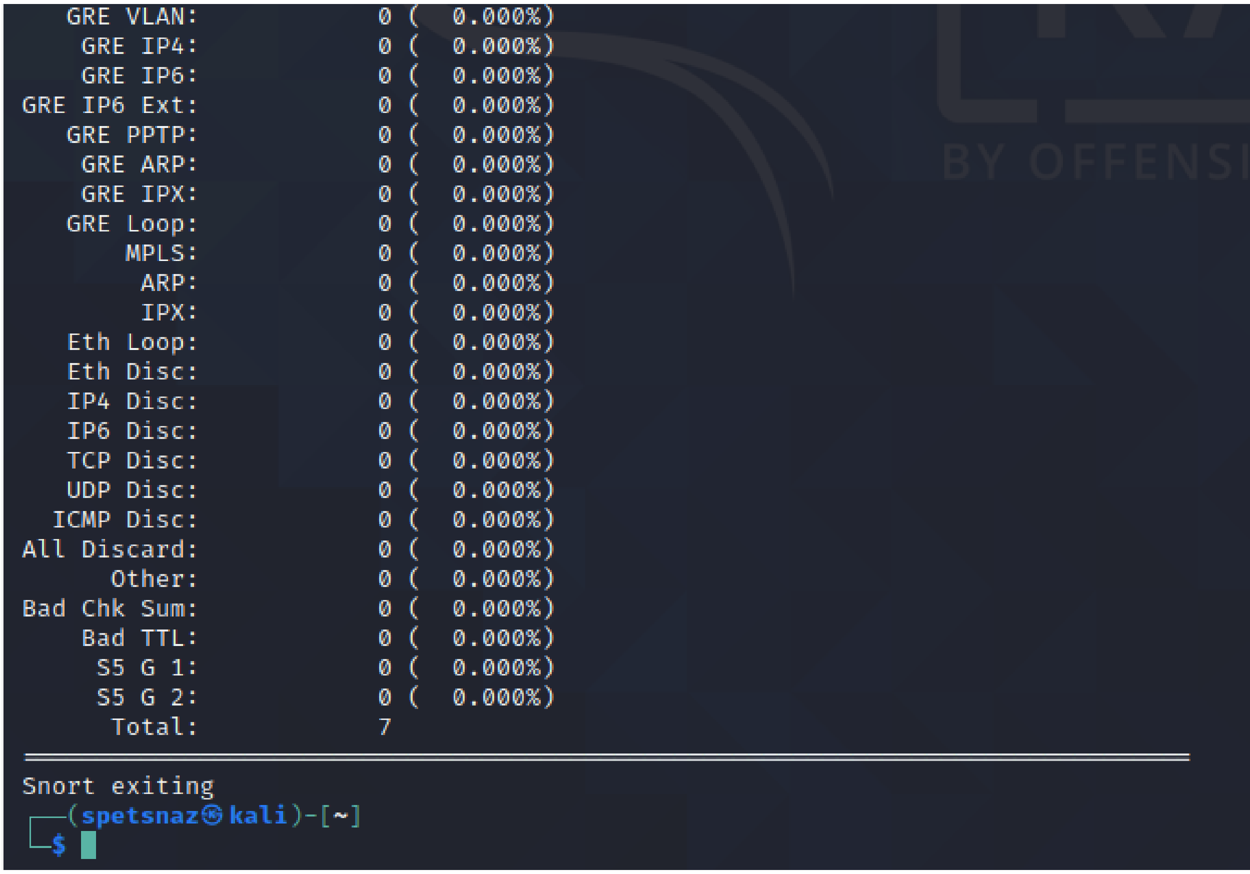
- RUNNING SNORT IN SNIFFER MODE



```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo snort -vde
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.0 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=1749)
WARNING: No preprocessors configured for policy 0.
04/14-13:13:54.050443 00:50:56:C0:00:08 → 01:00:5E:7F:FF:FA type:0×800 len:0×B3
169.254.190.172:64151 → 239.255.255.250:1900 UDP TTL:4 TOS:0×0 ID:54019 IpLen:20 DgmLen:165
Len: 137
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F  M-SEARCH * HTTP/
31 2E 31 0D 0A 48 6F 73 74 3A 20 32 33 39 2E 32  1.1..Host: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D  55.255.250:1900.
0A 53 54 3A 20 75 72 6E 3A 73 63 68 65 6D 61 73  .ST: urn:schemas
2D 75 70 6E 70 2D 6F 72 67 3A 64 65 76 69 63 65  -upnp-org:device
3A 49 6E 74 65 72 6E 65 74 47 61 74 65 77 61 79  :InternetGateway
44 65 76 69 63 65 3A 31 0D 0A 4D 61 6E 3A 20 22  Device:1..Man: "
73 73 64 70 3A 64 69 73 63 6F 76 65 72 22 0D 0A  ssdp:discover"..
4D 58 3A 20 33 0D 0A 0D 0A                       MX: 3....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
04/14-13:13:57.052370 00:50:56:C0:00:08 → 01:00:5E:7F:FF:FA type:0×800 len:0×B3
169.254.190.172:64151 → 239.255.255.250:1900 UDP TTL:4 TOS:0×0 ID:54020 IpLen:20 DgmLen:165
Len: 137
4D 2D 53 45 41 52 43 48 20 2A 20 48 54 54 50 2F  M-SEARCH * HTTP/
31 2E 31 0D 0A 48 6F 73 74 3A 20 32 33 39 2E 32  1.1..Host: 239.2
35 35 2E 32 35 35 2E 32 35 30 3A 31 39 30 30 0D  55.255.250:1900.
0A 53 54 3A 20 75 72 6E 3A 73 63 68 65 6D 61 73  .ST: urn:schemas
2D 75 70 6E 70 2D 6F 72 67 3A 64 65 76 69 63 65  -upnp-org:device
3A 49 6E 74 65 72 6E 65 74 47 61 74 65 77 61 79  :InternetGateway
```

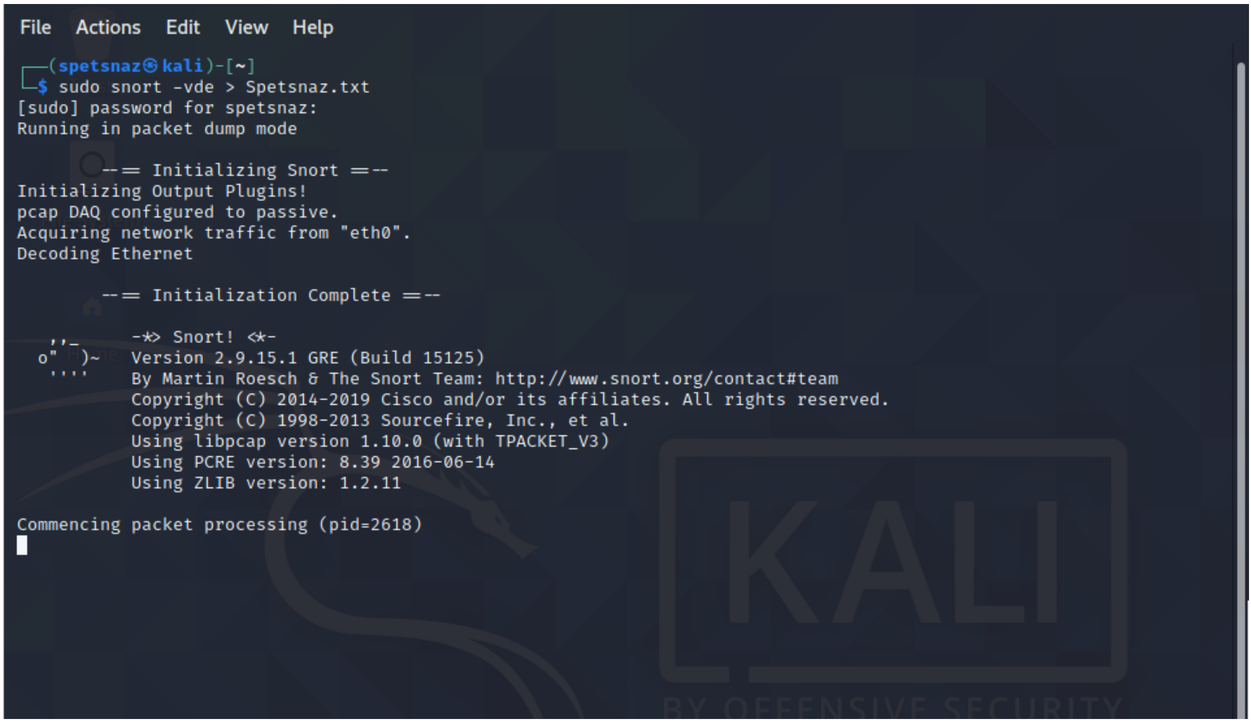


```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
===============================================================================
Run time for packet processing was 65.510976 seconds
Snort processed 7 packets.
Snort ran for 0 days 0 hours 1 minutes 5 seconds
   Pkts/min:            7
   Pkts/sec:            0
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       786432
  Bytes in mapped regions (hblkhd):      21864448
  Total allocated space (uordblks):      684960
  Total free space (fordblks):           101472
  Topmost releasable block (keepcost):   99504
===============================================================================
Packet I/O Totals:
   Received:            7
   Analyzed:            7 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:            7 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:            7 (100.000%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            7 (100.000%)
        TCP:            0 (  0.000%)
        IP6:            0 (  0.000%)
    IP6 Ext:            0 (  0.000%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            0 (  0.000%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
```



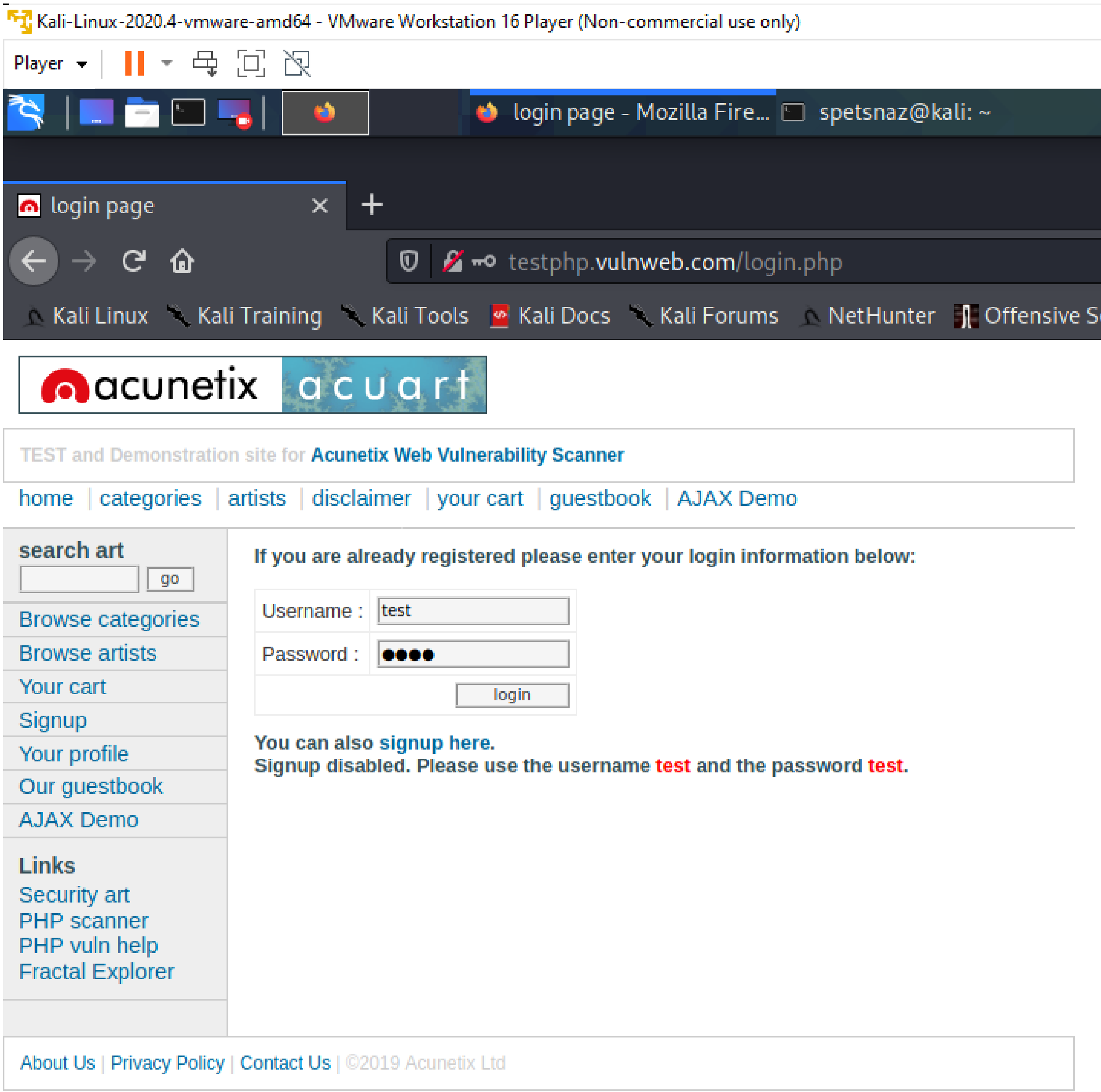
```
   GRE VLAN:          0 (  0.000%)
    GRE IP4:          0 (  0.000%)
    GRE IP6:          0 (  0.000%)
GRE IP6 Ext:          0 (  0.000%)
   GRE PPTP:          0 (  0.000%)
    GRE ARP:          0 (  0.000%)
    GRE IPX:          0 (  0.000%)
   GRE Loop:          0 (  0.000%)
       MPLS:          0 (  0.000%)
        ARP:          0 (  0.000%)
        IPX:          0 (  0.000%)
   Eth Loop:          0 (  0.000%)
   Eth Disc:          0 (  0.000%)
   IP4 Disc:          0 (  0.000%)
   IP6 Disc:          0 (  0.000%)
   TCP Disc:          0 (  0.000%)
   UDP Disc:          0 (  0.000%)
  ICMP Disc:          0 (  0.000%)
All Discard:          0 (  0.000%)
      Other:          0 (  0.000%)
Bad Chk Sum:          0 (  0.000%)
    Bad TTL:          0 (  0.000%)
     S5 G 1:          0 (  0.000%)
     S5 G 2:          0 (  0.000%)
      Total:          7
===============================================================================
Snort exiting
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

❖ SENDING OUTPUT OF SNIFFING MODE SNORT TO A FILE



```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo snort -vde > Spetsnaz.txt
[sudo] password for spetsnaz:
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.0 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=2618)
```

- LOGIN INTO THE SITE TO CAPTURE CREDENTIALS

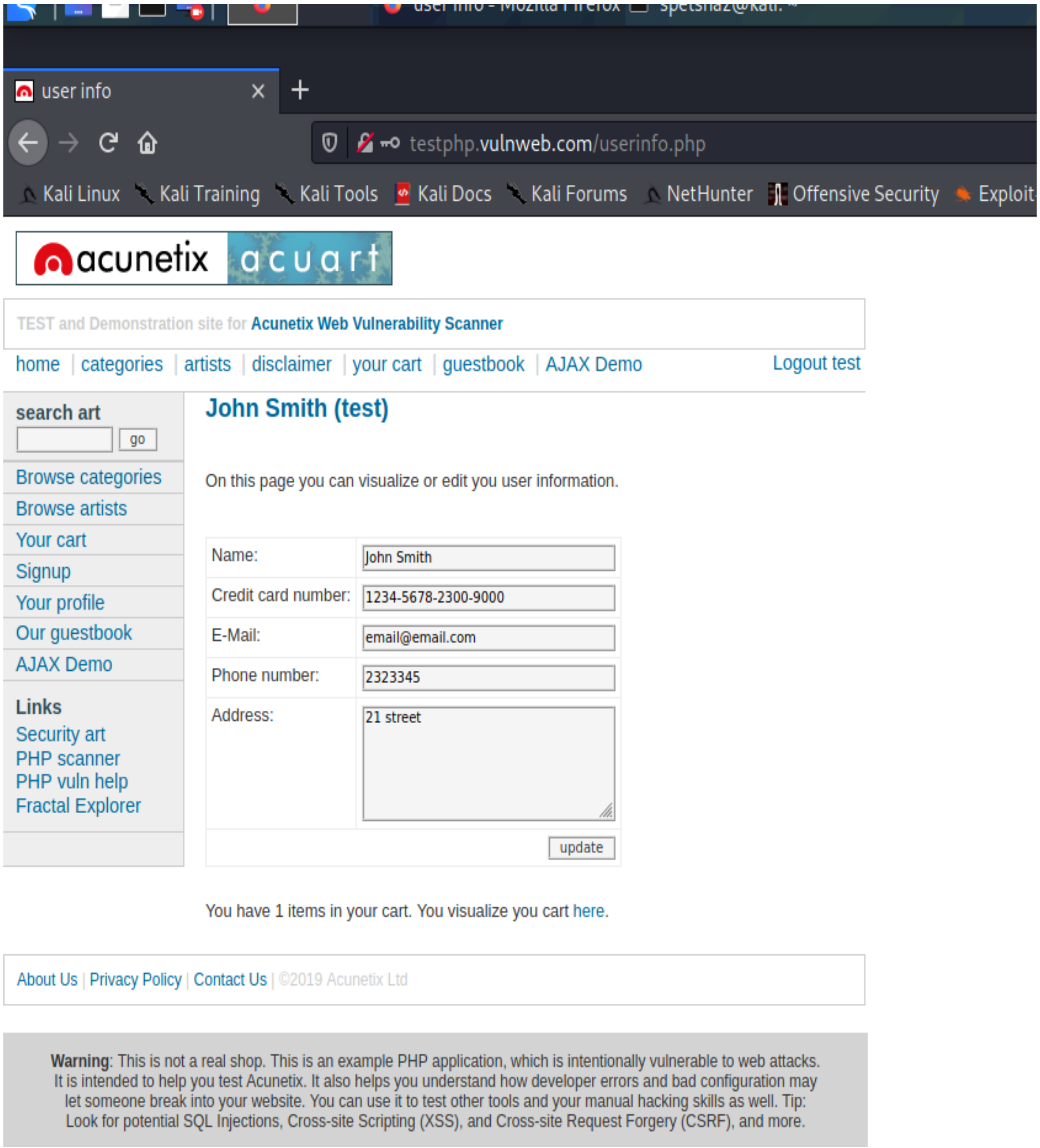


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
login page - Mozilla Fire...
spetsnaz@kali: ~
login page
testphp.vulnweb.com/login.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive S
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
login
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

If you are already registered please enter your login information below:

Username :	test
Password :	●●●●

You can also signup here.
Signup disabled. Please use the username test and the password test.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

John Smith (test)

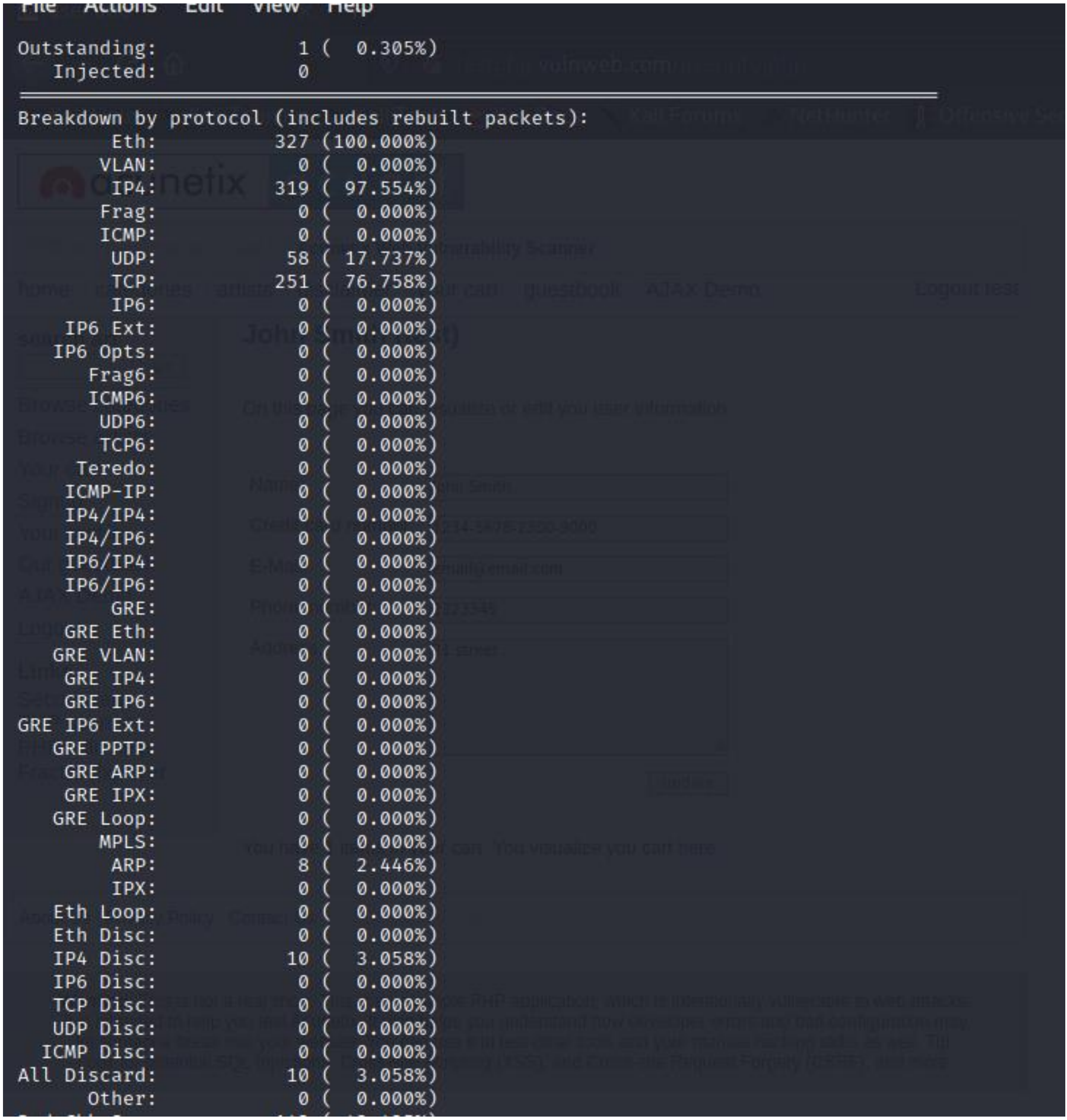
On this page you can visualize or edit you user information.

Name:	John Smith
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street

You have 1 items in your cart. You visualize you cart here.

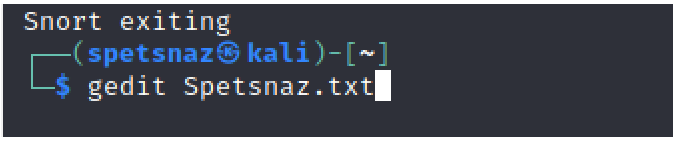
©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



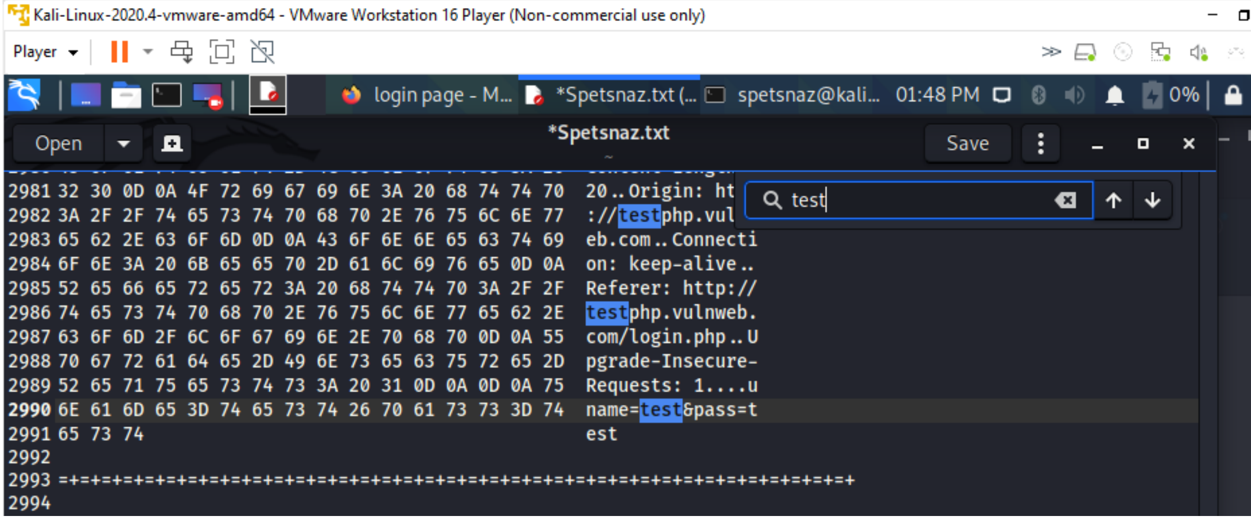
```
Outstanding:          1 (  0.305%)
  Injected:           0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:        327 (100.000%)
       VLAN:          0 (  0.000%)
        IP4:        319 ( 97.554%)
       Frag:          0 (  0.000%)
       ICMP:          0 (  0.000%)
        UDP:         58 ( 17.737%)
        TCP:        251 ( 76.758%)
        IP6:          0 (  0.000%)
    IP6 Ext:          0 (  0.000%)
   IP6 Opts:          0 (  0.000%)
      Frag6:          0 (  0.000%)
      ICMP6:          0 (  0.000%)
       UDP6:          0 (  0.000%)
       TCP6:          0 (  0.000%)
     Teredo:          0 (  0.000%)
    ICMP-IP:          0 (  0.000%)
    IP4/IP4:          0 (  0.000%)
    IP4/IP6:          0 (  0.000%)
    IP6/IP4:          0 (  0.000%)
    IP6/IP6:          0 (  0.000%)
        GRE:          0 (  0.000%)
    GRE Eth:          0 (  0.000%)
   GRE VLAN:          0 (  0.000%)
    GRE IP4:          0 (  0.000%)
    GRE IP6:          0 (  0.000%)
GRE IP6 Ext:          0 (  0.000%)
   GRE PPTP:          0 (  0.000%)
    GRE ARP:          0 (  0.000%)
    GRE IPX:          0 (  0.000%)
   GRE Loop:          0 (  0.000%)
       MPLS:          0 (  0.000%)
        ARP:          8 (  2.446%)
        IPX:          0 (  0.000%)
   Eth Loop:          0 (  0.000%)
   Eth Disc:          0 (  0.000%)
   IP4 Disc:         10 (  3.058%)
   IP6 Disc:          0 (  0.000%)
   TCP Disc:          0 (  0.000%)
   UDP Disc:          0 (  0.000%)
  ICMP Disc:          0 (  0.000%)
All Discard:         10 (  3.058%)
      Other:          0 (  0.000%)
```

- ❖ FINDING USERNAME AND PASSWORD

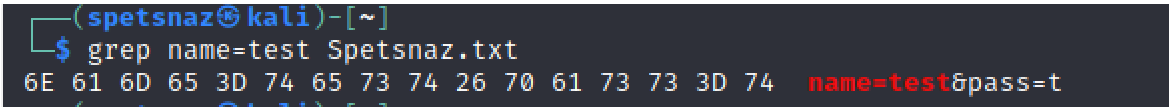


```
Snort exiting
┌──(spetsnaz㉿kali)-[~]
└─$ gedit Spetsnaz.txt
```

Two ways we can find text in command one through GUI and second through command line as shown in the images below:

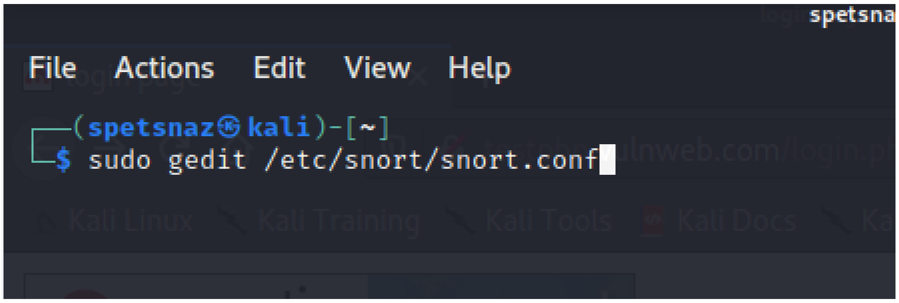


```
32 30 0D 0A 4F 72 69 67 69 6E 3A 20 68 74 74 70  20..Origin: ht
3A 2F 2F 74 65 73 74 70 68 70 2E 76 75 6C 6E 77  ://testphp.vul
65 62 2E 63 6F 6D 0D 0A 43 6F 6E 6E 65 63 74 69  eb.com..Connecti
6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D 0A  on: keep-alive..
52 65 66 65 72 65 72 3A 20 68 74 74 70 3A 2F 2F  Referer: http://
74 65 73 74 70 68 70 2E 76 75 6C 6E 77 65 62 2E  testphp.vulnweb.
63 6F 6D 2F 6C 6F 67 69 6E 2E 70 68 70 0D 0A 55  com/login.php..U
70 67 72 61 64 65 2D 49 6E 73 65 63 75 72 65 2D  pgrade-Insecure-
52 65 71 75 65 73 74 73 3A 20 31 0D 0A 0D 0A 75  Requests: 1....u
6E 61 6D 65 3D 74 65 73 74 26 70 61 73 73 3D 74  name=test&pass=t
65 73 74                                         est

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

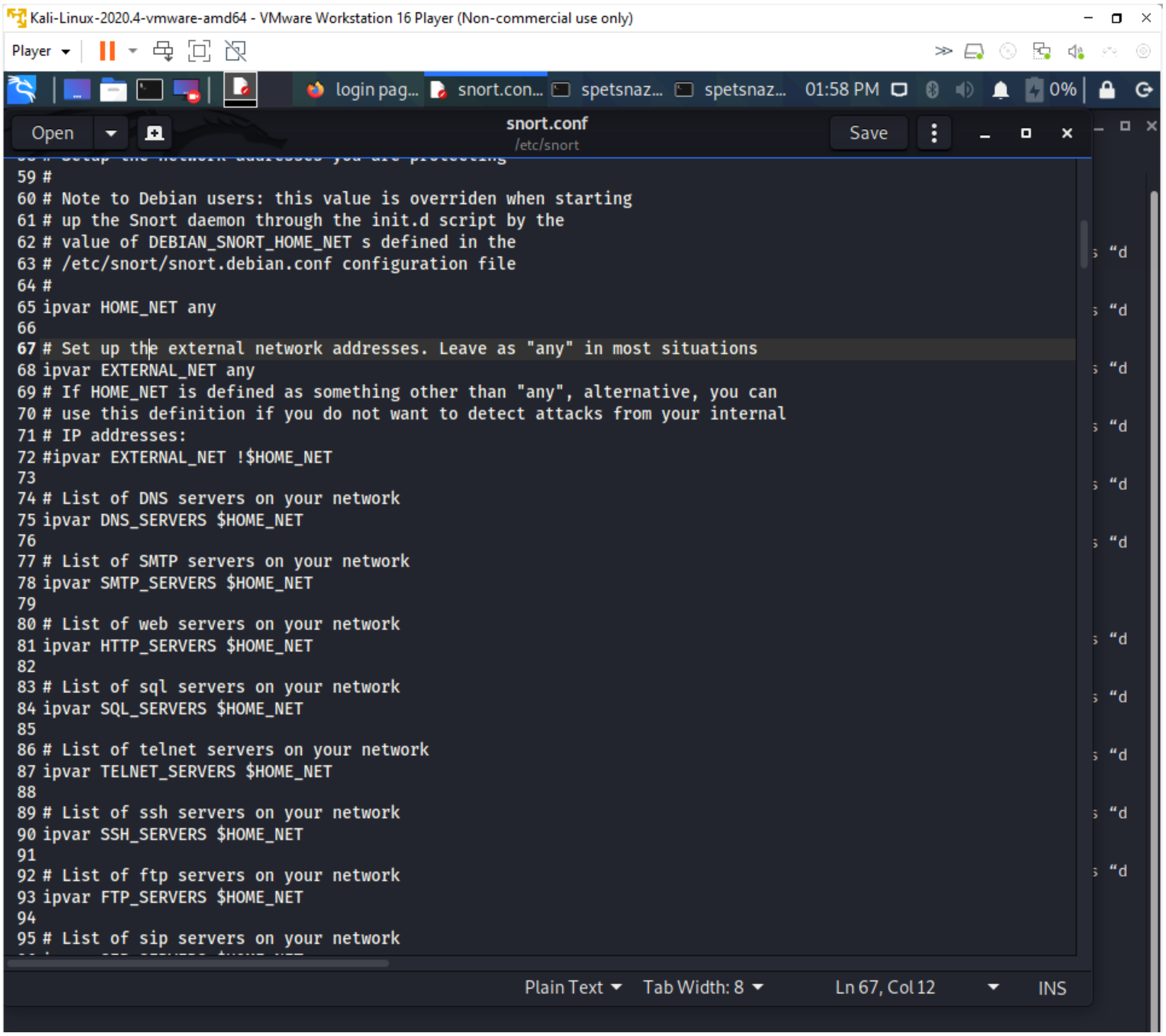


```
┌──(spetsnaz㉿kali)-[~]
└─$ grep name=test Spetsnaz.txt
6E 61 6D 65 3D 74 65 73 74 26 70 61 73 73 3D 74   name=test&pass=t
```

❖ OPENING SNORT.CONF CONFIG FILE

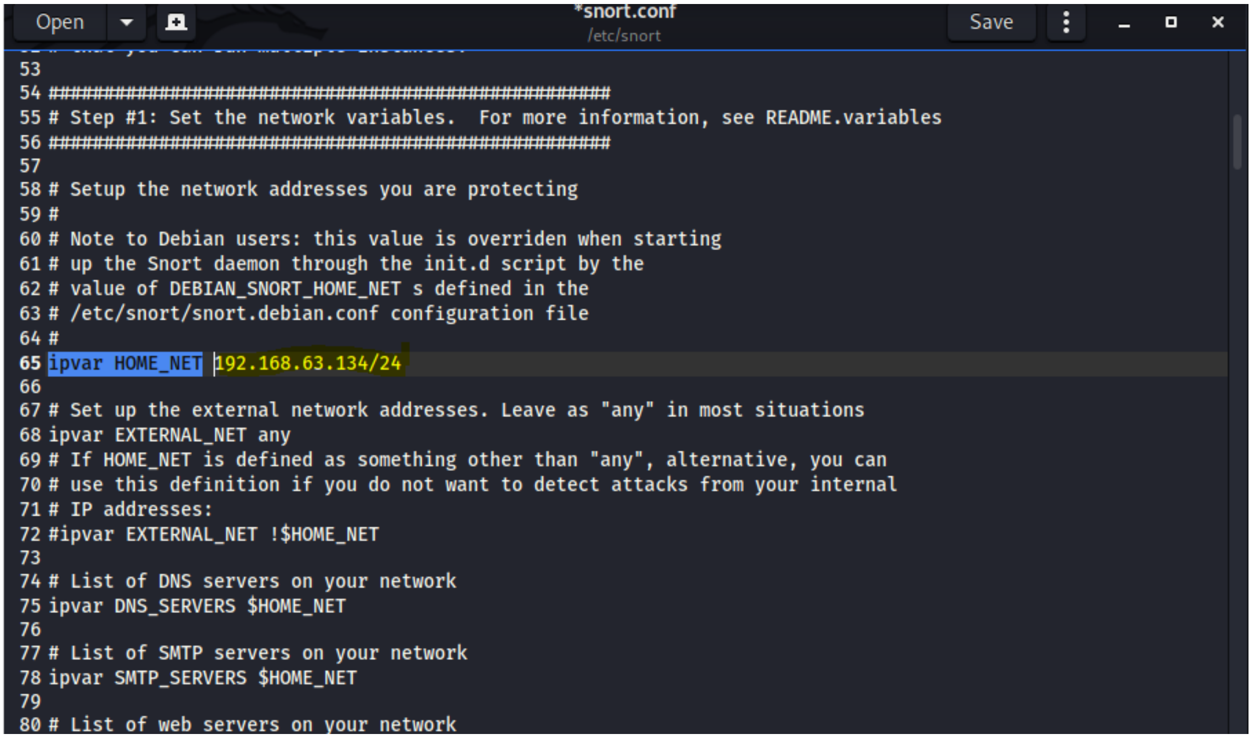


```
┌──(spetsnaz㉿kali)-[~]
└─$ sudo gedit /etc/snort/snort.conf
```



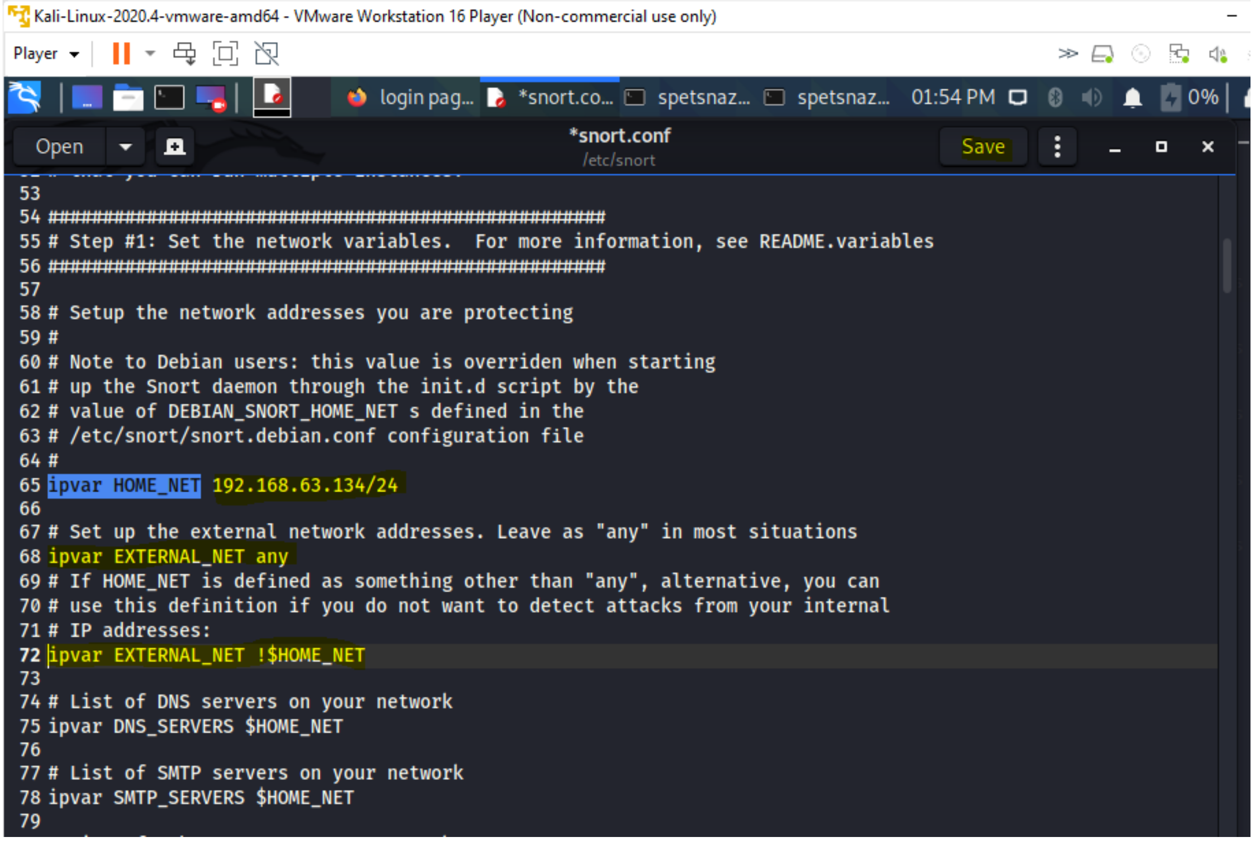
```
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET

# List of sip servers on your network
ipvar SIP_SERVERS $HOME_NET
```

❖ CHANGING VALUE OF “ipvar HOME_NET”- image below



```
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.63.134/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
```

- ❖ REMOVING # FROM “ipvar EXTERNAL_NET”

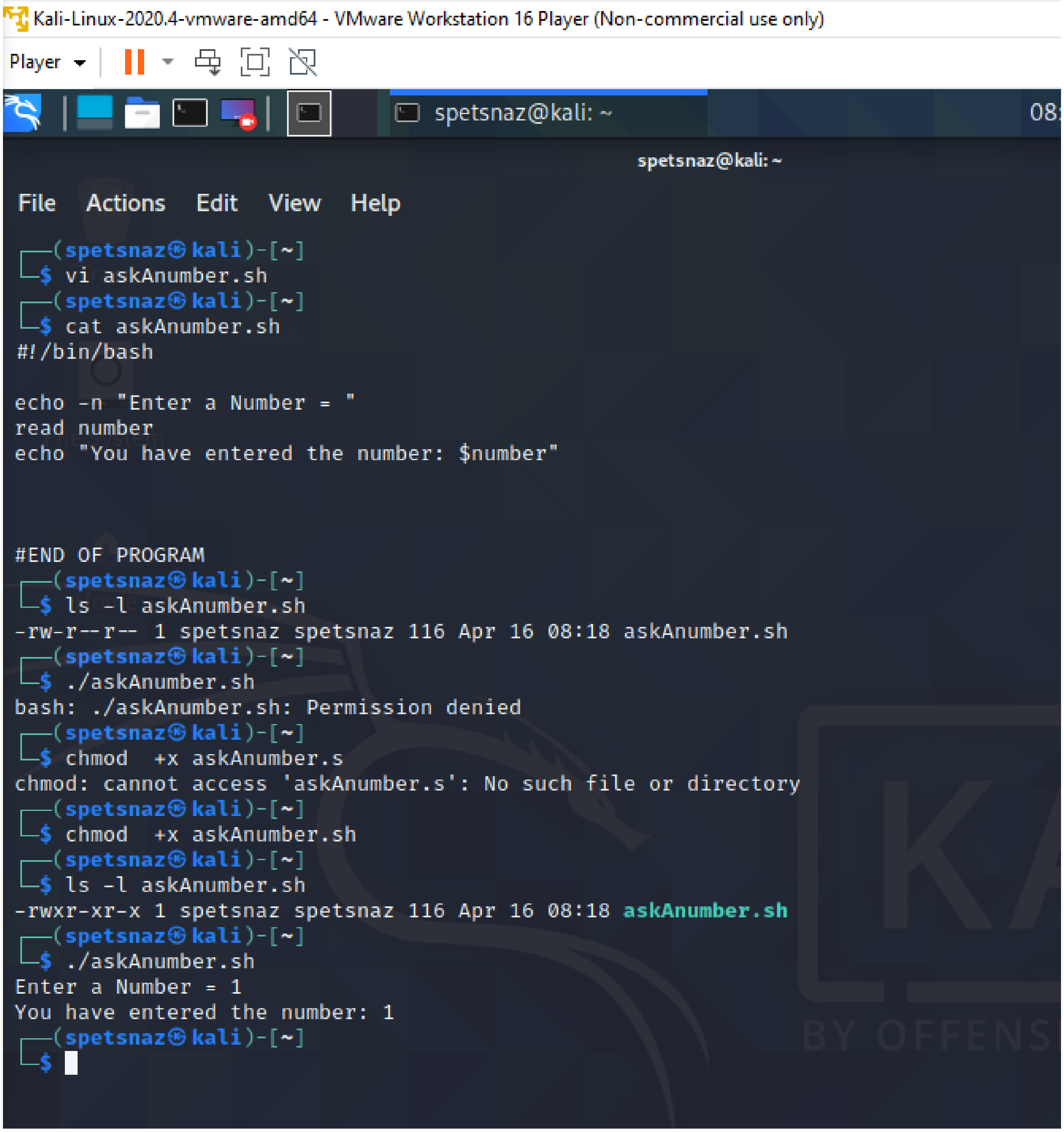


```
###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.63.134/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

```

Task 3: BASH SCRIPTING AND DISTRO WATCH

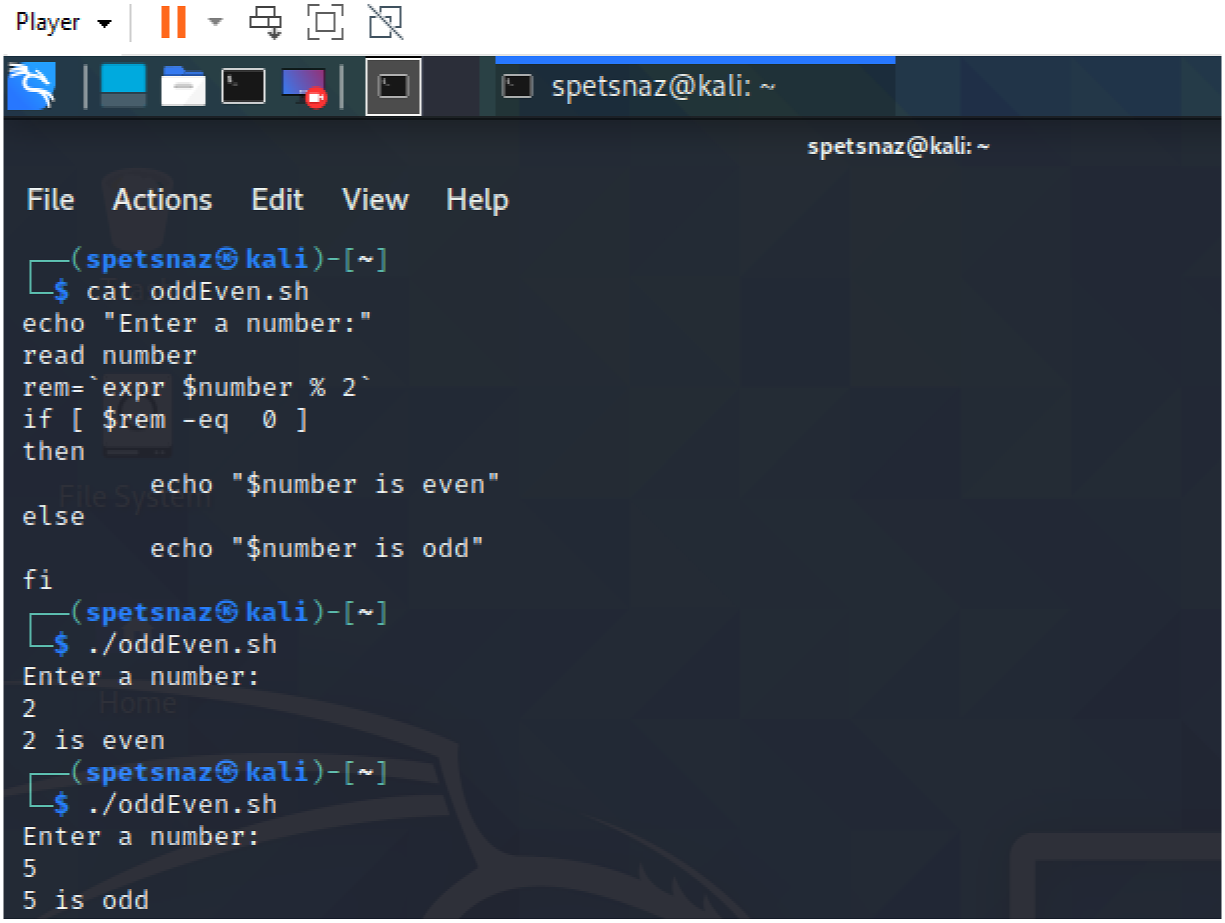
3.1 BASH SCRIPTING

3.1.1 ASKING A NUMBER FROM THE USER


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
spetsnaz@kali: ~
08:
spetsnaz@kali: ~
File
Actions
Edit
View
Help

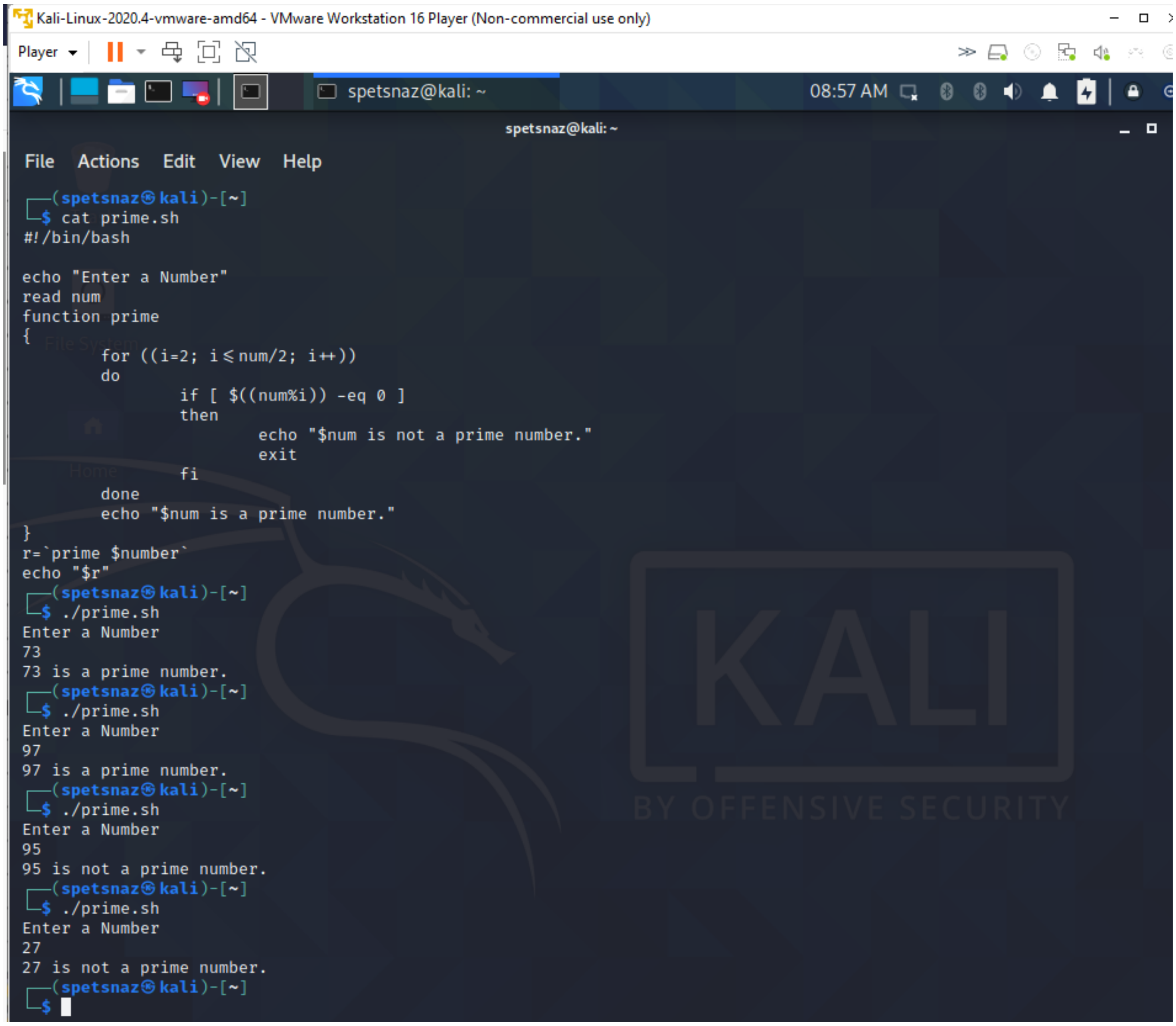
```
┌──(spetsnaz㉿kali)-[~]
└─$ vi askAnumber.sh
┌──(spetsnaz㉿kali)-[~]
└─$ cat askAnumber.sh
#!/bin/bash

echo -n "Enter a Number = "
read number
echo "You have entered the number: $number"



#END OF PROGRAM
┌──(spetsnaz㉿kali)-[~]
└─$ ls -l askAnumber.sh
-rw-r--r-- 1 spetsnaz spetsnaz 116 Apr 16 08:18 askAnumber.sh
┌──(spetsnaz㉿kali)-[~]
└─$ ./askAnumber.sh
bash: ./askAnumber.sh: Permission denied
┌──(spetsnaz㉿kali)-[~]
└─$ chmod  +x askAnumber.s
chmod: cannot access 'askAnumber.s': No such file or directory
┌──(spetsnaz㉿kali)-[~]
└─$ chmod  +x askAnumber.sh
┌──(spetsnaz㉿kali)-[~]
└─$ ls -l askAnumber.sh
-rwxr-xr-x 1 spetsnaz spetsnaz 116 Apr 16 08:18 askAnumber.sh
┌──(spetsnaz㉿kali)-[~]
└─$ ./askAnumber.sh
Enter a Number = 1
You have entered the number: 1
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

3.1.2 FINDING IF A NUMMBER IS ODD OR EVEN



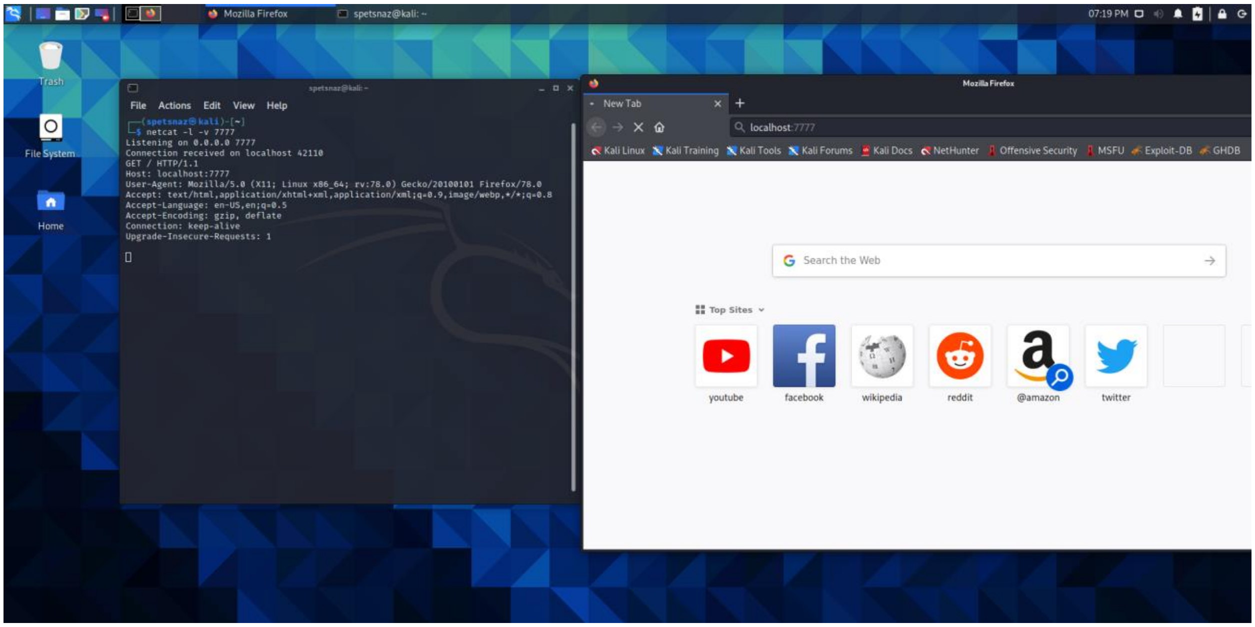
```
┌──(spetsnaz㉿kali)-[~]
└─$ cat oddEven.sh
echo "Enter a number:"
read number
rem=`expr $number % 2`
if [ $rem -eq  0 ]
then
        echo "$number is even"
else
        echo "$number is odd"
fi
┌──(spetsnaz㉿kali)-[~]
└─$ ./oddEven.sh
Enter a number:
2
2 is even
┌──(spetsnaz㉿kali)-[~]
└─$ ./oddEven.sh
Enter a number:
5
5 is odd
```

3.1.3 FINDING NUMBER IS PRIME OR NOT


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
spetsnaz@kali: ~
08:57 AM
spetsnaz@kali: ~
File
Actions
Edit
View
Help

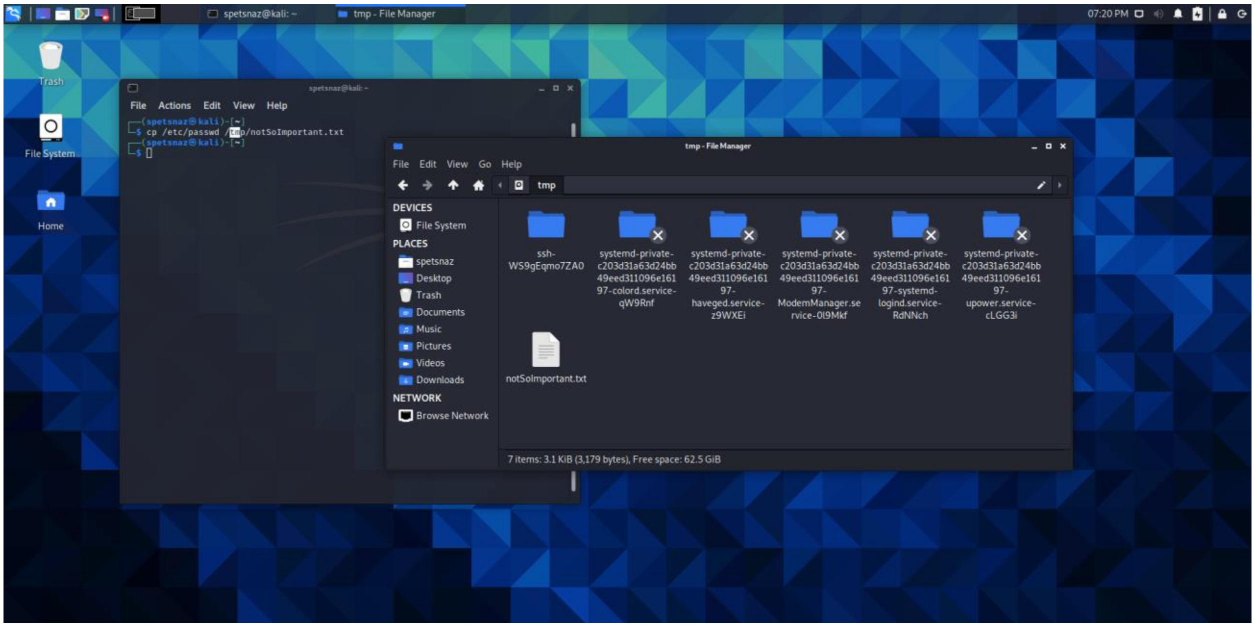
```
┌──(spetsnaz㉿kali)-[~]
└─$ cat prime.sh
#!/bin/bash

echo "Enter a Number"
read num
function prime
{
        for ((i=2; i<=num/2; i++))
        do
                if [ $((num%i)) -eq 0 ]
                then
                        echo "$num is not a prime number."
                        exit
                fi
        done
        echo "$num is a prime number."
}
r=`prime $number`
echo "$r"
┌──(spetsnaz㉿kali)-[~]
└─$ ./prime.sh
Enter a Number
73
73 is a prime number.
┌──(spetsnaz㉿kali)-[~]
└─$ ./prime.sh
Enter a Number
97
97 is a prime number.
┌──(spetsnaz㉿kali)-[~]
└─$ ./prime.sh
Enter a Number
95
95 is not a prime number.
┌──(spetsnaz㉿kali)-[~]
└─$ ./prime.sh
Enter a Number
27
27 is not a prime number.
┌──(spetsnaz㉿kali)-[~]
└─$ ▌
```

3.1.4 OPENING NETCAT PROGRAM IN LISTENING MODE ON PORT 7777



```
┌──(spetsnaz㉿kali)-[~]
└─$ netcat -l -v 7777
Listening on 0.0.0.0 7777
Connection received on localhost 42110
GET / HTTP/1.1
Host: localhost:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

3.1.5 COPY /ETC/PASSWORD TO/TMP/NOTSOMPORTANT.TXT

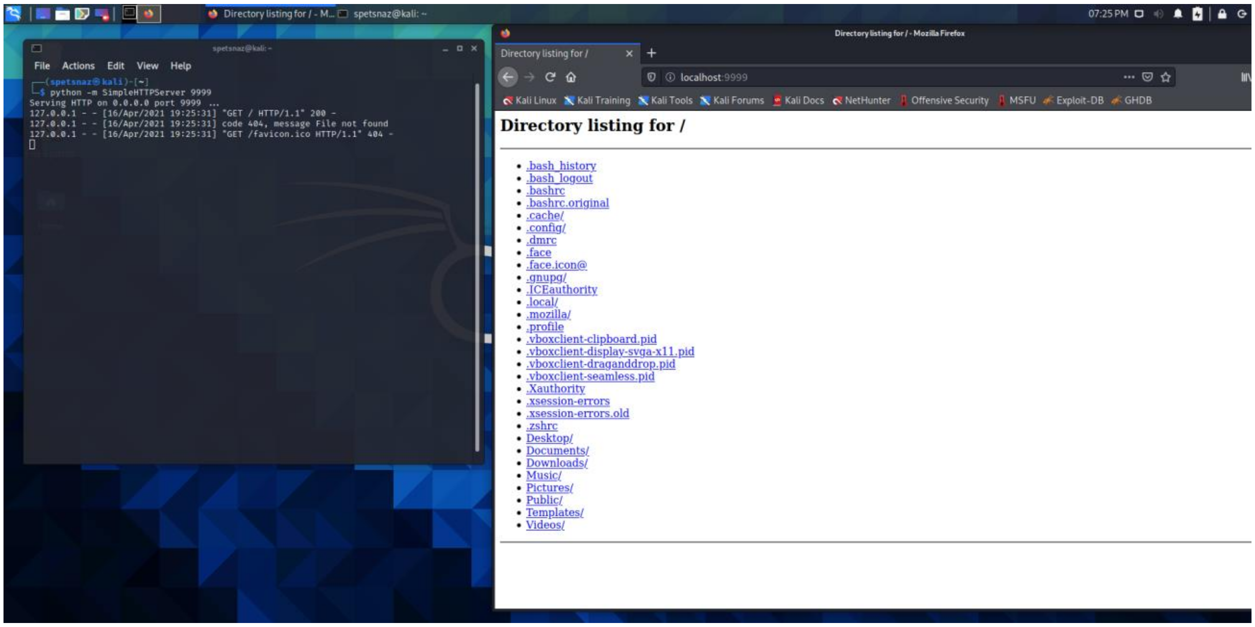


```
┌──(spetsnaz㉿kali)-[~]
└─$ cp /etc/passwd /tmp/notSoImportant.txt
┌──(spetsnaz㉿kali)-[~]
└─$ 
```

7 items: 3.1 KiB (3,179 bytes), Free space: 62.5 GiB

spetsnaz@kali: ~
tmp - File Manager
07:20 PM
Trash
File System
Home
File Actions Edit View Help
File Edit View Go Help
tmp
DEVICES
File System
PLACES
spetsnaz
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
NETWORK
Browse Network
ssh-WS9gEqmo7ZA0
systemd-private-c203d31a63d24bb49eed311096e16197-colord.service-qW9Rnf
systemd-private-c203d31a63d24bb49eed311096e16197-haveged.service-z9WXEi
systemd-private-c203d31a63d24bb49eed311096e16197-ModemManager.service-0I9Mkf
systemd-private-c203d31a63d24bb49eed311096e16197-systemd-logind.service-RdNNch
systemd-private-c203d31a63d24bb49eed311096e16197-upower.service-cLGG3i
notSoImportant.txt

3.1.6 FIRE UP A PYTHON HTTP SERVER ON THE BACKGROUND ON PORT 9999



```
┌──(spetsnaz㉿kali)-[~]
└─$ python -m SimpleHTTPServer 9999
Serving HTTP on 0.0.0.0 port 9999 ...
127.0.0.1 - - [16/Apr/2021 19:25:31] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [16/Apr/2021 19:25:31] code 404, message File not found
127.0.0.1 - - [16/Apr/2021 19:25:31] "GET /favicon.ico HTTP/1.1" 404 -
```

Directory listing for /

- .bash_history
- .bash_logout
- .bashrc
- .bashrc.original
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .local/
- .mozilla/
- .profile
- .vboxclient-clipboard.pid
- .vboxclient-display-svga-x11.pid
- .vboxclient-draganddrop.pid
- .vboxclient-seamless.pid
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zshrc
- Desktop/
- Documents/
- Downloads/
- Music/
- Pictures/
- Public/
- Templates/
- Videos/

3.2 DISTRO WATCH- PARROT LINUX

3.2.1 PARROT LINUX

Parrot OS is a type of Linux distribution whose primary focus is on security privacy and development. Parrot OS is used by many security professionals and penetration testers. There are several releases of parrot since the release date with the latest Parrot 4.11 stable version released less than a month ago on 23 March 2021.

3.2.2 WHAT IS THE SPECIALITY OF THE PARROT LINUX?

The specialty of parrot OS is that it is full of various useful tools according to the user's field of work. Parrot OS is also known for its testing abilities. There is a number of features which make it amazingly well.

- Open source- parrot is completely free and developed by the open-source community. However, it also provides the source code to users so that they can customize it as per their needs
- Lightweight- parrot is very lightweight and runs well on hardware with a smaller number of resources.
- Secure- parrot gets timely updates to keep ahead among the other tools and provide assurance that it is completely sandboxed at the same time.

3.2.3 WHEN IT WAS RELEASED? WHO IS THE AUTHOR/PARENT COMPANY?

Parrot Linux: It is a Debian-oriented distribution of Linux. It also has its penetration testing as well as security tools. The functioning and features of parrot Linux are the same as Kali Linux. It was first introduced in 2013 and hosted by the team of open-source developers, Linux, and security experts, and the team was organized by Lorenzo faletra.

It has numerous inbuilt tools most commonly are:

- Zulu crypt
- Tor
- Anonsurf.

3.2.4 WHICH DISTRIBUTION IT FOLLOW? CAN YOU USE IT IN PRODUCTION ENVIRONMENT?

- Parrot Linux is an open-source design based on Debian. It follows a rolling-release development model.

- We can use it in a production environment because is made for developers, penetration testers, security researchers, forensic investigators, and privacy-aware people.

3.2.5 LIMITATIONS OF KALI LINUX

- Without important tools built-in, users have to download testing tools from repositories

- Made for penetration test, or security testing, not made for daily operations like entertainment and gaming. Therefore, interfaces, or common applications for entertainment, will not be supported.
- Most use command and do not support many graphical test tools.
- The interface is not user friendly, though it is possible to tweak the GUI, or change the background image to make the interface more minimalistic.

3.2.6 COMPARISON OF PARROT WITH KALI

SPECIFICATIONS	**PARROT LINUX**	**KALI LINUX**
HARDWARE REQUIREMENT	No require GPU 320MB RAM or higher 1GHZ dual-core CPU Boot in both UEFI and Legacy 16GB of disc space at least	Required GPU. 1GB RAM or higher 1GHZ dual-core CPU Boot in both UEFI and Legacy 20GB of hard disc space at least
LOOK AND FEEL	All the tools installed	Get lost easily
HACKING TOOLS	More tools than kali	Lacks anonymity and crypto tools
VARIATIONS	Diverse	Not much

I recommend Parrot Linux over Kali Linux. Because this is the operating system aimed at users who are penetration testers, it will be lighter and have the necessary software built-in for specific purposes. Overall, when it comes to Parrot Linux and Kali Linux, I prefer Parrot Linux.

REFERENCES:

- **https://www.edureka.co/blog/parrot-os-vs-kali-linux/**
- **https://www.geeksforgeeks.org/difference-between-kali-linux-and-parrot-os/**
- **https://www.theknowledgeacademy.com/us/courses/linux-training/parrot-security-os-training/boise/**

- ❖ **https://en.wikipedia.org/wiki/Parrot_OS**