Linux Inject How-Tos Packet

2017 Regional CCDC Edition

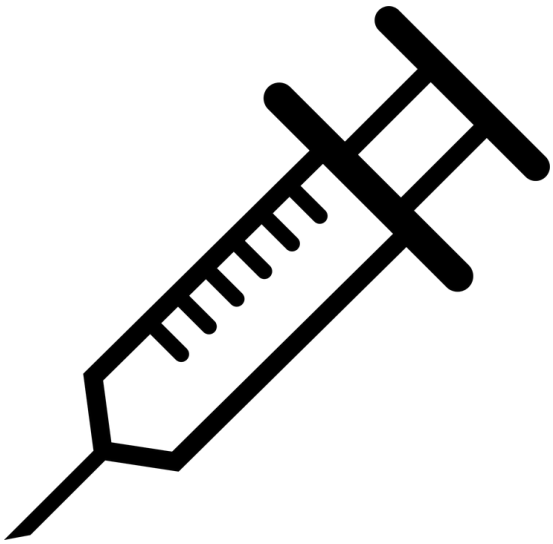

Table of Contents

TCPDump

"Include an assessment of 20 minutes of traffic as to what SNORT is finding."

Monitor all packets on eth1 interface

tcpdump -i eth1

Monitor all traffic on port 80 (HTTP)

tcpdump -i eth1 'port 80'

Monitor all traffic on port 25 (SMTP)

tcpdump -vv -x -X -s 1500 -w *filename.txt* -i eth1 'port 25'

Where,

-vv : More verbose output

-x : When parsing and printing, in addition to printing the headers of each packet, print the data of each packet.

-X : hen parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII. This is very handy for analysing new protocols.

-s 1500: Snarf snaplen bytes of data from each packet rather than the default of 68. This is useful to see lots of information.

-i eth1 : Monitor eth1 interface

TODO: Visualize TCPDump into report

http://bitthinker.com/blog/en/research/how-to-visualize-tcpdump-with-graphviz

FreePBX / Asterisk

> *“It has come to our attention that the Raspberry PI/ IOT device is not remotely accessible. Part of the problem is that its IP address is acquired via DHCP. Make the Raspberry PI/ IOT device accessible by completing the following steps:*
> *Change the IP to a static address - 172.20.241.199/24.*
> *Change the DNS server to your AD/DNS VM.*
> *...*

Static IP change through console

Login as root

cd /etc/sysconfig/network-scripts

nano ifcfg-eth0

Navigate to the line with BOOTPRONTO
Replace “dhcp" with “none”
hit return
type the following lines;

NETMASK=255.255.255.0

IPADDR=192.168.1.3 (replace this with the IP address you want)

GATEWAY=192.168.1.1 (replace this with your router gateway address)

Leave the rest.
Hit ctrl+O keys (the letter not the number zero)
Hit enter again to save the file
hit ctrl+Z to exit the text editor

service network restart

Manual DNS

/etc/resolv.conf

ClamAV

ClamAV can be installed by issuing the following command in the terminal:

apt-get install clamav

Most common problem - DatabaseMirror db.local.clamav.net - the 'local' needs to be changed to your country code.

Update ClamAV

freshclam

ClamAV is able to scan separate files or if necessary entire directories. An example of a command is demonstrated bellow.

To scan a file:

clamscan file

To scan a directory (In this instance your home directory):

clamscan --recursive=yes --infected /home

Note: If you would like ClamAV to remove the infected files add the --remove option.

By default ClamAV will not scan files larger than 20Mb. In order to override that setting the options --max-filesize=2000M --max-scansize=2000M must be appended to the command. Where the size 2000M may be replaced as necessary by the user. An example is provided bellow.

clamscan --max-filesize=2000M --max-scansize=2000M --recursive=yes

Remember to output to file!

Hashes

find / -type f -perm /u=x,g=x,o=x -exec md5sum {} \; >> hashes.txt;

diff old.txt new.txt

Bind9 DNS

- Installing Bind9
    - sudo apt-get install bind9

- Static IP and Set Itself to DNS
    - sudo vi /etc/network/interfaces
    - *set*:
        - auto eth0
        - iface eth0 inet static
        - address _____ (ex. 10.0.2.15)
        - netmask 255.0.0.0
        - dns-nameservers 127.0.0.1

- Add Forwarders
    - sudo vi /etc/bind/named.conf.options
    - *set*:
        - forwarders {
        - 8.8.8.8;
        - 8.8.4.4;
        - };

- Setting Local Configuration
    - sudo vi /etc/bind/named.conf.local
    - *add*:
        - zone "ubuntu.local" {
        - type master;
        - file "/etc/bind/db.ubuntu.local";
        - };

- Setting up db.ubuntu.local
    - cp /etc/bind/db.empty /etc/bind/db.ubuntu.local
    - sudo vi /etc/bind/db.ubuntu.local
    - *change* ubuntu.local.
    - *add* IN A _____ (ex. 10.0.2.15)
    - sudo systemctl reload bind9

NTP

I. Configure NTP server

1. Install NTP Server

```
apt-get install install ntp
```

2. Setup Restrict values in ntp.conf

Modify the /etc/ntp.conf file to make sure it has the following two restrict lines.

```
# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

The first restrict line allows other clients to query your time server. This restrict line has the following parameters

- noquery prevents dumping status data from ntpd.
- notrap prevents control message trap service.
- nomodify prevents all ntpq queries that attempts to modify the server.
- nopeer prevents all packets that attempts to establish a peer association.
- Kod – Kiss-o-death packet is to be sent to reduce unwanted queries

The value -6 in the second line allows forces the DNS resolution to the IPV6 address resolution. For more information on the access parameters list, Please refer to documentation on “man ntp_acc”

3. Allow Only Specific Clients

To only allow machines on your own network to synchronize with your NTP server, add the following restrict line to your /etc/ntp.conf file:

```
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
```

If the localhost needs to have the full access to query or modify, add the following line to /etc/ntp.conf

```
restrict 127.0.0.1
```

4. Add Local Clock as Backup

Add the local clock to the ntp.conf file so that if the NTP server is disconnected from the internet, NTP server provides time from its local system clock.

```
server  127.127.1.0 # local clock
fudge   127.127.1.0 stratum 10
```

In the above line, Stratum is used to synchronize the time with the server based on distance. A stratum-1 time server acts as a primary network time standard. A stratum-2 server is connected to the stratum-1 server over the network. Thus, a stratum-2 server gets its time via NTP packet requests from a stratum-1 server. A stratum-3 server gets its time via NTP packet requests from a stratum-2 server, and so on.

Also stratum 0 devices are always used as reference clock.

5. Setup NTP Log Parameters

Specify the drift file and the log file location in your ntp.conf file

```
driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp.log
```

driftfile is used to log how far your clock is from what it should be, and slowly ntp should lower this value as time progress.

6. Start the NTP Server

After setting up appropriate values in the ntp.conf file, start the ntp service:

```
service ntpd start
```

II. Configure NTP Client to Synchronize with NTP Server

7. Modify ntp.conf on NTP Client

This setup should be done on your NTP Client (Not on NTP-server)

To synchronize the time of your local Linux client machine with NTP server, edit the /etc/ntp.conf file on the client side. Here is an example of how the sample entries looks like. In the following example, you are specifying multiple servers to act as time server, which is helpful when one of the timeservers fails.

```
server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org iburst
server 3.rhel.pool.ntp.org iburst
```

iburst: After every poll, a burst of eight packets is sent instead of one. When the server is not responding, packets are sent 16s interval. When the server responds, packets are sent every 2s.

Edit your NTP.conf to reflect appropriate entries for your own NTP server.

```
server 19.168.1.1 prefer
```

prefer: If this option is specified that server is preferred over other servers. A response from the preferred server will be discarded if it differs significantly different from other server’s responses.

8. Start the NTP Daemon

Once the ntp.conf is configured with correct settings, start the ntp daemon.

```
/etc/init.d/ntp start
```

You will see the NTP will slowly start to synchronize the time of your linux machine with the NTP Server.

9. Check the NTP Status

Check the status of NTP using the ntpq command. If you get any connection refused errors then the time server is not responding or the NTP daemon/port is not started or listening.

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*elserver1       19.168.1.1       3 u  300 1024  377    1.225   -0.071   4.606
```

10. Set Local Date and Time

The ntpdate command can be used to set the local date and time by polling the NTP server. Typically, you'll have to do this only one time.

Your jitter value should be low, else check the drift from the clock in the driftfile. You may also need to change to some other NTP server based on the difference. This command synchronizes the time with your NTP server manually.

```
ntpdate –u 19.168.1.1
```

After this initial sync, NTP client will talk to the NTP server on an on-going basis to make sure the local time reflects the accurate time.

You can also use the following command to get the current status of ntpd.

```
# ntpdc -c sysinfo
```

Telnet / SSH Verification

1) Indicate if Telent happen to be supported on any of our servers and 2) Confirm that SSH has been implemented and VERIFIED to function properly for authorized users. Any instances of Telnet should be remedied.

Telnet

Uninstall telnet and its dependencies

```
sudo apt-get remove --auto-remove telnet
```

If you also want to delete your local/config files for telnet then this will work.

```
sudo apt-get purge telnet
```

Or similarly, like this telnet

```
sudo apt-get purge --auto-remove telnet
```

SSH Verify

First Check if the process sshd is running:

```
ps aux | grep sshd
```

This will output something like the following if it finds the process called sshd:

```
[root@server ~]# ps aux | grep sshd
root      1399  0.0  0.2   8292  1092 ?        Ss   Sep13   0:00
/usr/sbin/sshd
[root@server ~]#
```

So sshd is running with process ID 1399! It is indeed running!

Second, check if the process sshd is listening on port 22:

```
netstat -plant | grep :22
```

If ssh is listening on port 22, you will get the following:

```
[root@server ~]#
[root@server ~]# netstat -plant | grep :22
```

```
tcp        0      0 0.0.0.0:22                  0.0.0.0:*
LISTEN      1399/sshd
tcp        0      0 :::22                       :::*
LISTEN      1399/sshd
[root@server ~]#
```

So the process with ID 1399 (sshd) is listening on port 22! The second test passed!

Third, you can use the lsof command to check if the port 22 TCP file is open:

```
[root@server ~]# lsof -i
COMMAND    PID   USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
sshd      1399   root    3u  IPv4 1235481137      0t0  TCP *:ssh
(LISTEN)
httpd     6126   root    3u  IPv4 1309891499      0t0  TCP *:http
(LISTEN)
[root@server ~]#
```

So sshd (SSH daemon) and httpd (Apache web server daemon) are both running and listening on the ssh and http ports respectively! Third test passed.

Four, try to telnet to port 22:

```
telnet localhost 22
```

If the port is open, you will get the following output:

```
[root@server ~]# telnet localhost 22
Trying ::1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_5.3
```

If the port number 22 is not open, you will get the following:

```
[root@server ~]# telnet localhost 22
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
telnet: connect to address 127.0.0.1: Connection refused
[root@server ~]#
```

Five, check the status of the sshd service:
If you use Debian or Ubuntu (or CentOS or RedHat):

```
[root@server ~]# /etc/init.d/sshd status
openssh-daemon (pid  1399) is running...
[root@server ~]#
```

If the process sshd is misbehaving or not listening on port 22, one of these methods will surely fail and you should start or restart sshd using the following command:

```
[root@server ~]# /etc/init.d/sshd restart
```

Ports

To verify ports are open

Run following command:

 # netstat -tulpn | less

Make sure iptables is allowing port 80 / 110 / 143 connections:

 # iptables -L -n