Active Defense

Saturday, March 11, 2023 3:51 AM

Using n**etstat** to view active connections. Netstat is installed with net-tools

yum install net-tools [On CentOS/RHEL]

apt install net-tools

Command	Output/Details
netstat | less	Show less connections
netstat -tu	Show tcp & udp
netstat -tun	-n resolves the port number of the name of the connection
netstat -tuna	The –a adds what is listening
netstat -tunap	-p will add the process ID information for active connections (run as root or sudo)
netstat -elvp	[--extend|**-e**] [--listening|**-l**] [--verbose|**-v**] [--program|**-p**]
netstat -epav	[--extend|**-e**] [--program|**-p**] [--protocol=family , -A] [--verbose|**-v**]
netstat | grep ESTABLISHED	To view established connections

The **ss** command will give similar output to netstat

Command	Output/Deteails
ss	Shows active connections

The **top** command can be used to view resources on the workstation

Command	Output/Deteails
top	View resources and processes running
htop	Another service to display process information

Use the ps command to observe process information

Command	Output/Deteails
ps	Monitor prcoesses
ps - aux	Gives detailed process ID information including users and where the process is running from
ps – aef --forest	View process tree and command line arguments that were used to launch the child processes

Use the **w** command to view the connected **users**

Command	Output/Deteails
w	Shows active users

Using **Kill** commands/signals on processes or users observed through **netstat** with –**p** or **w** for specific users

Command	Output/Deteails
kill pid#	Ends a process ID
pkill	Kill signals (must run as root or sudo)
pkill –KILL –u username	Force logout specific users

Users can broadcast messages with **wall** commands and **write** commands

Command	Output/Deteails

wall	Displays a broadcast message to users with shell sessions
write	Send messages to specific users.
write username tty	Send messages to specific users. Use the **w** command to observe the **TTY** for the specific user.

Firewall view logs:
sudo journalctl –u firewald –n 100

Enable logging:
sudo -I
nano /etc/firewalld/firewalld.conf
Find:
LogDenied=off
Replace:
LogDenied=all

sudo systemctl restart firewalld.service

Check SSH logs:
/var/log/auth.log

Check brute force attempts:
grep sshd.*Failed /var/log/auth.log | less

Search failed connections:
grep sshd.*Did /var/log/auth.log | less

Check MYSQL logs
First:
Go to this file **/etc/mysql/conf.d/mysqld_safe_syslog.cnf** and remove or comment out lines
Second:
Go to mysql conf file **/etc/mysql/my.cnf** and add following lines

To enable error log add following:
[mysqld_safe]
log_error=/var/log/mysql/mysql_error.log

[mysqld]
log_error=/var/log/mysql/mysql_error.log

To enable general query log add following:
general_log_file = /var/log/mysql/mysql.log
general_log = 1

To enable Slow Query Log add following:
log_slow_queries = /var/log/mysql/mysql-slow.log
long_query_time = 2
log-queries-not-using-indexes

Save the file and restart mysql using following commands
service mysql restart

To enable logs at runtime, login to mysql client (mysql -u root -p) and give:
SET GLOBAL general_log = 'ON';
SET GLOBAL slow_query_log = 'ON';

Web Server logging with apache
These logs can be viewed here:
/var/log/apache2/access.log

Print last 10 lines of log:
sudo tail -f /var/log/apache2/access.log