**Lecture 22**

**Investigations on steroid cheat sheets for Windows, Linux, and BCA**

The purpose of incident response is nothing but Live Forensics. The investigation can be carried out to obtain any digital evidence. This article mainly focuses on how the incident response can be performed in a Linux system.

**Table of Contents**

* **Incident Response**
* **Logs Entries**
* **Services - Nginx, Keycloak, RabbitMQ, sftp**
* **Application -**
* **Network**
* **Incident Response**
* Whenever incident happened then on first place, please collect all the details like hostname, IP address, operating systems etc.
* Check any alert came on our Preventive detection control
* Next, Gather the information on system services.
* Check the uptime of the affected server

It will give you the details of since when the server is up and running



* Check the disk / partition size, sometimes due to disk space services may get down, check available “Avail” column for free disk space

Text

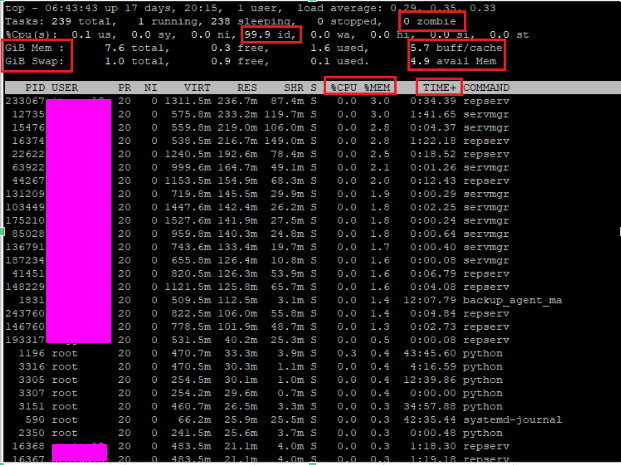
Description automatically generated with medium confidence

* Check free and available size of physical memory

Text

Description automatically generated

* Now examine the running processes by “top” command.



* If we found Cache and Buffer memory is filled up then we can release that memory by below command

*sync ; echo 3 > /proc/sys/vm/drop\_caches*

* **Sar command** will give more detailed report, like CPU, Memory, Network, HDD etc.

sar keeps all the logs under /var/log/sa database, it keeps the log for last 21 days

check the free memory space

A screenshot of a computer

Description automatically generated with low confidence

Check below Values –

**%nice** - Nice value is a user-space and priority PR is the process's actual priority that use by Linux kernel. nice value range is -20 to +19 where -20 is highest, 0 default and +19 is lowest.

**%iowait** - I/O wait (iowait) is the percentage of time that the CPU (or CPUs) were idle during which the system had pending disk I/O requests.

**%idle** - Percentage of time that the CPU or CPUs were idle during which the system had an outstanding disk I/O request.

A screenshot of a computer

Description automatically generated with medium confidence

* **ps aux | less** - A process is associated with any program running on your system, and is used to manage and monitor a program's memory usage, processor time, and I/O resources

To see the process status of your Linux and the currently running processes system and the PID. In order to identify abnormal processes that could indicate any malicious activity in the Linux system

A computer screen capture

Description automatically generated with low confidence

* iostat – This command is use to check tps and data read / write performance.

tps - The number of transfers per second that were issued to the device. Higher tps means the processor is busier.

KB\_wrtn / s - It shows the amount of data read from the device expressed in a number of blocks (kilobytes, megabytes) per second

If tps and write value will be high then there are fair chances is issue with the hdd.

A screenshot of a computer

Description automatically generated with medium confidence

* **dmesg | less -** It is useful for examining kernel boot messages and debugging hardware related issues, If booting process had issues then we can use diagnose message utility to identify hardware issue.

Graphical user interface, text

Description automatically generated

* **lsof | less -** This command provides a list of files that are opened. Basically, it gives the information to find out the files which are opened by which process.

To display more details on a particular process you can use below command, we can see the SIZE/OFF column to identify the highly utilized process. If the process is high in size it will impact the CPU performance.

A screenshot of a computer

Description automatically generated with medium confidence

* **Logs Entries**

If you find any of below error logs entry, then we can consider below action was performed at backend-

|  |  |
| --- | --- |
| **Action / Message** | **Error Log Entry** |
| Successful user login | “Accepted password”, “Accepted publickey”, “session opened” |
| Failed user login | “authentication failure”, “failed password” |
| User log-off | “session closed” |
| User account change or deletion | “password changed”, “new user”, “delete user” |
| Service failure | “failed” or “failure” |
| Failed user authentication Error code | 401 / 403 |
| Invalid request Error code | 400 |
| Internal server error Error code | 500 |

**------------------------------------------------------------------------**

* **Services - ~~Nginx, Keycloak, RabbitMQ, sftp~~**

1. **Keycloak**

Keycloak can be used as a standalone user identity and access manager by allowing us to create users database with custom roles and groups. This information can be further used to authenticate users within our application and secure parts of it based on pre-defined roles.To ensure Keycloak working as expected below settings should be in place –

*ps -ef | grep -i keycloak*

A screenshot of a computer

Description automatically generated with medium confidence

As per above highlighted screenshot, check the configuration file and log path for potential troubleshooting –

Config file location -

*less /apps/keycloak/keycloak-10.0.2/bin/standalone.sh*

*less /apps/keycloak/keycloak-10.0.2/bin/standalone.conf*

Log file location –

*less /apps/keycloak/keycloak-10.0.2/standalone/configuration/standalone.xml*

* Check Keycloak status –

*systemctl status keycloak*



If service is not running then start the service with below command –

*systemctl start keycloak*

* Ensure below setting and AD connectivity are in place –

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

1. **Rabbitmq**

RabbitMQ simply stores messages and passes them to consumers when ready. RabbitMQ is a reliable open source message broker.

To ensure Keycloak working as expected below settings should be in place –

*ps -ef | grep -i Keycloak*

A screenshot of a computer

Description automatically generated with medium confidence

* Check the rabbitmq service should be running –

*systemctl status rabbitmq-server*

Text

Description automatically generated

If service is not running then start the service with below command –

*systemctl start rabbitmq-server*

* Check the rabbitmq log from below path –

*less /apps/rabbitmq/logs/management/access.log\_todays date*

* Check the rabbitmq conf file at below path –

*less /apps/rabbitmq/config/rabbitmq.conf*

1. **Nginx**

NGINX is commonly used as a reverse proxy and load balancer to manage incoming traffic and distribute it to slower upstream servers

To ensure nginx working as expected below settings should be in place –

*ps -ef | grep -I nginx*

Graphical user interface, text, chat or text message

Description automatically generated

* Check the nginx service should be running –

*systemctl status nginx*

Text

Description automatically generated

If service is not running then start the service with below command –

*systemctl start nginx*

* Check the nginx log from below path –

*less /apps/nginx/logs/host.access.log*

*less /apps/nginx/logs/host.error.log*

* Check the nginx conf file at below path –

*less /apps/nginx/conf/nginx.conf*

1. **SFTP**

* SFTP allows businesses to securely transfer billing data, funds, and data recovery files.
* SFTP users have been created inside “*/home*/” directory -
* Check if the account is lock by pam command

A screenshot of a computer

Description automatically generated with medium confidence

* Below command is used to reset the password of SFTP user

Text

Description automatically generated

* Check the sftp log file from below path –

*less /var/log/auth.log*

* Check the sftp conf file at below path –

*less /etc/ssh/sshd\_config*

* In below file we have define sftp log file path -

*less /etc/rsyslog.d/rsyslog.conf*

* We can check how many applications is installed in our linux box

*cd /etc/systemd/system*

* **Application -**
* When it comes to xyz then very first command we need to run is “xxx”

Text

Description automatically generated

Check status of xyz, abc, last update time and transaction log creation date should be up to date, if xyz is not active ready then you can run “def” command to recover xyz.

* Check service manager is running or not

*ps -ef | grep -i jkl*

A screenshot of a computer

Description automatically generated with medium confidence

* Check dba service manager is running or not

*ps -ef | grep -i xyz*



Note - If both services are down then first start dbaserver and then xyz manager

* Check if xyz manager port is listening or not

Text

Description automatically generated

* Check if dba port is listening or not

Graphical user interface, text

Description automatically generated

* **Network**

# To telnet specific port   
syntax: telnet 127.0.0.1 <specific port>  
 *Eg/- : telnet 127.0.0.1 80*

# To Check specific port of remote server (192.168.29.83) using telnet

*Eg/- telnet 192.168.29.83 22*   
  
  
# nc (netcat) command is also use for to check specific port like telnet

*nc 127.0.0.1 80*  
  
# netstat & ss command is used for to check NW statistics, properties, status of each reports  
 *netstat -an | grep -i 22  
 ss -tulnp | grep -i 22*  
  
  
  
# tcpdump Command # (Packet Sniffer Tool / Packet capturing tool)  
It will also identify the broadcast packet  
 *tcpdump  
 tcpdump -vvv*

#We can find out public IP of client machine which is hit on our Application hosted Windows server

1. Check your public IP (client machine public IP)

Graphical user interface, application, website

Description automatically generated

1. Now browse the URL from client machine

Chart

Description automatically generated with medium confidence

1. Open sysinternal tcp view on application hosted windows server and check the public ip and port number

Graphical user interface, application

Description automatically generated