D. Y. Patil College of Engineering & Technology, Kolhapur

Experiment : 05

Title : Operating System utilities like Net Stat, FC, open files, etc.

1] * Netstat :

Netstat can be used to identify - suspicious network activity in a number of ways.

- Connections to unusal IP address / port eg. If you see a connection to an IP address that is known to be associated with malware, this could be sign of infection.
- Connections using a lot of bandwidth eg. If you see a connection using a lot of bandwidth, this could be sign that malware extracting data.
- Connection is Established but not responding eg. This could be a sign that malware is using the connection to stay in the contact with command & server.

- Dropped packets.
  eg. This could be a sign of a networking problem, such as faulty cable or switch.

* Features:

- Can help to identify malware that is communicating with command & server.
- Can help to troubleshoot network - problems, such as dropped packets and connections error.
- Can be used to monitor network - performance & identify bottlenecks.
- Displays list of all active connections
- Displays routing table information.
- Displays statistics for network - traffic, such as the number of packets send and received & the amount of bandwidth used.

* Prows

- Powerful tool for monitoring network activity & identifying suspicious connections.
- Free & open-source
- Easy to use
- Available on most operating systems.

2] FC

FC can be used to compare files for signs of infection or to verify that files have been copied correctly.

- You can compare a system file to a known-good version to identify if the file has been modified by malware.
- You can compare two versions of a file to identify differences. This can be useful for debugging software problems or for tracking changes to a file.
- You can compare two files to verify that they have be copied correctly.

* Features:

- Can help to identify malware that has modify system files.
- Used to verify that files have been copied correctly.
- Can be used to compare two versions of file to identify differences.
- Displays a list of all differences between the two files or sets of files.
- Can be configured to ignore certain types of differences, such as the differences in file size or timestamps.

* Pros:

- Powerful tool for comparing files.
- Free and open-source.
- Easy to use.
- Available on most operating systems.

3] Open files :

The open files utility can be used to identify suspicious files that may have been opened by malware or troubleshoot problems with open files.

- You can look for files that opened by the unusual processes.
  eg. If you see this happened, this could be a sign of malware injection.
- You can look for files that are located in unusual directories.
  eg. If you see a file is not associated with any known app, this could be malware.
- You can identify files that are locked by other process.
  eg. In this you can't do anything with that file even you can't delete it, this can be malware.

* Features :

- Can help to identify malware that has open system files.

- Can be used to troubleshoot problems, locked by another process problems.
- Can be used to monitor system - activity & identify suspicious - processes that have open files.
- Displays list of all open files.
- Displays information of each open files like path, process id, dates, etc
- Can be configured to filter list of open files by process, path, etc.

* Pros

- Powerful tool for identifying all open files on system.
- Free & open source
- Easy to use.
- Available on most o.s.

* Some More Commands :

- **PID :**
  Stands for Process Identifier. It is unique number that is assigned to each running process on a system.

- **TT :**
  Stands for Terminal Time. It is amount of time that a process has spent running mode.

- **STAT :**
  Stands for status. It shows the current status of process.
  R : Running
  S : sleeping
  D : uninterruptible
  Z : stopped.

- **RE :**
  Stands for Resident Memory. It is amount of physical memory that currently being used by process.

- **LIM :**
  Stands for Process Limit. It is maximum amount of CPU time that a process allowed to use.

- **% CPU :**

Stands for CPU Usage. It is the percentage of CPU time that process has used in last period of time.

- **% MEM:**

Stands for Memory Usage. It is the percentage of physical memory that process is using.

✱ Conclusion:

All are powerful OS utilities that can be used for a variety of cybersecurity purposes. By using these utilities, you can help to protect your systems & networks from cyberattacks.

✱✱✱

01/09/23