ComSec 2021-22

Log and PATH poisoning

Mattia Donadelli

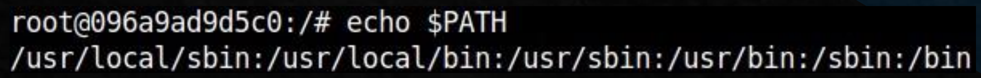
Session format

- Introduction to poisoning
- Attempt demo #1
  - Solution demo #1
- Attempt demo #2
  - Solution demo #2
- Presentation of challenges 1 and 2 (for you to solve)

What is PATH poisoning?

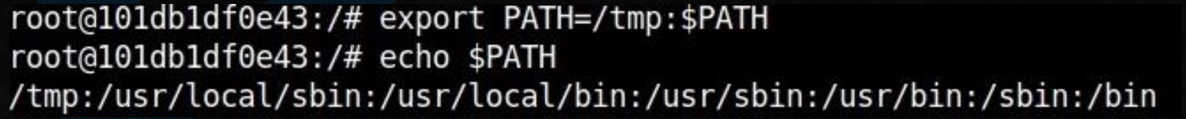
- PATH poisoning, in a Unix-like operating system, refers to the exploitation of the PATH variable in order to execute a custom payload instead of an executable binary.
- PATH is an environmental variable that tells the shell which directories to search for executable binaries in response to commands inputted by the user.
- The PATH variable can be printed using the ‘echo’ command and altered using ‘export’
- Let’s assume our PATH contains the following: /usr/local/bin:/usr/bin/:/bin

‘cat file.txt’ -> /usr/local/bin/cat -> /usr/bin/cat -> /bin/cat -> returns an error



```
root@096a9ad9d5c0:/# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

display the PATH variable



```
root@101db1df0e43:/# export PATH=/tmp:$PATH
root@101db1df0e43:/# echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

prepend ‘/tmp’ to the PATH variable

Log poisoning

- Log poisoning refers to the tampering of any kind of log file with the goal of gaining code execution.

Default location of common log files:

Apache2:

/var/log/apache2/access.log

/var/log/apache2/error.log

FTP:

/var/log/vsftpd.log

System:

/var/log/auth.log

/var/log/mail.log