NETFLOW MANGAGMENT PROJECT

Behailu B. Bekera
Westminster College, Department of Computer Science and Mathematics
Westminster Ave., Fulton, MO, 65251
Summer Internships in Science and Technology (SIST) Program

Supervisor: Joe Klemencic
Computing Division-Network Security
Fermi National Accelerator Laboratory,
Batavia, IL 60510

OUTLINE

- Introduction
  - ✓ Objective
  - ✓ Relevance
- Tools & Methods
- Results
  - ✓ Four different cases
- Conclusion
- References

INTRODUCTION

- As a security precaution, any device that offers a network service at Fermilab must forward its logs to the central logging server.
- The Netflow Management Project is intended to identify systems that are not logging to the central logging server, and alerting the computer security team of such occurrences.
- If a device isn't sending its logs to the server, it may have been hacked in which case immediate measures need to be taken to prevent any potentially dangerous unauthorized activities and any unanticipated delay in the course of research.

TOOLS & METHODS

- Tools :
  1. PHP
  2. Linux
  3. Git Version Control System
- Flow Engine :
  - *$controller = Engine_Front::getInstance();*
  - *$controller->setFilename($flowfile);*
  - *$controller->setTimeVariant($variant);*
  - *$controller->dispatch();*

RESULTS

- **CASE ONE: Both directories associated with an IP address and hostname are found.**
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] 131.225.189.82 is the source
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] 131.225.189.82 is an IP address
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] with a hostname cmsstor82
- 2009-07-10T15:45:12-05:00 Engine_Plugin_Test [debug] Notified of preDispatch
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] /logging/syslog-ng/131.225.189.82 is a directory
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] /logging/syslog-ng/cmsstor82 is a directory
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] Files in /logging/syslog-ng/131.225.189.82
- 2009-07-10T15:45:13-05:00 Engine_Front [debug]
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] messages
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] 0 bytes
- 2009-07-10T15:45:13-05:00 Engine_Front [debug]
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] secure
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] 0 bytes

CASE ONE CONTINUED…

- 2009-07-10T15:45:13-05:00 Engine_Front [debug]
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] Files in /logging/syslog-ng/cmsstor82
- 2009-07-10T15:45:13-05:00 Engine_Front [debug]
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] messages
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] 4742729 bytes
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] Last access July 05 2009 04:03:34.
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] was last modified July 10 2009 15:45:00.
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] is in variant
- 2009-07-10T15:45:13-05:00 Engine_Front [debug]
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] secure
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] 283807 bytes
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] Last access July 05 2009 04:03:59.
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] was last modified July 10 2009 15:45:00.
- 2009-07-10T15:45:13-05:00 Engine_Front [debug] is in variant

CASE ONE CONTINUED…

- The directories associated with both the IP address and hostname do exist.
- Both message and secure files are found at least in one of the directories and contain more than 0 bytes.
- The files have also been updated within the time given by the time variant variable and
- Therefore, we can conclude that the destination with an IP 131.225.189.82 or host name of cmsstor82 is working just fine and is forwarding its log files to the central logging server.

- **CASE TWO: One of the directories exists and does contain non-zero bytes files.**
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] /logging/syslog-ng/131.225.219.144 is not a directory
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] /logging/syslog-ng/dosrv097 is a directory
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] Files in /logging/syslog-ng/dosrv097
- 2009-07-10T15:45:14-05:00 Engine_Front [debug]
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] messages
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] 375015 bytes
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] Last access July 06 2009 15:03:54.
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] was last modified July 07 2009 14:47:09.
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] Not in the given time variant
- 2009-07-10T15:45:14-05:00 Engine_Front [debug]
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] secure
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] 19707 bytes
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] Last access July 06 2009 15:03:54.
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] was last modified July 07 2009 10:33:42.
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] Not in the given time variant

CASE TWO CONTINUED…

- However, these files are not in the given time variant which means that the device has not been forwarding its log files to the central logging server during that period of time.
- Hence, this incidence will be notified to the security team for further investigation.

- **CASE THREE: Both Directories do not exist**
- 2009-07-10T15:45:11-05:00 Engine_Front [debug] Notifying plugins of engine startup
- 2009-07-10T15:45:12-05:00 Engine_Plugin_Test [debug] Notified of dispatchLoopStartup
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] 131.225.208.243 is the source
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] 131.225.208.243 is an IP address
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] with a hostname fcdfgcb2
- 2009-07-10T15:45:12-05:00 Engine_Plugin_Test [debug] Notified of preDispatch
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] /logging/syslog-ng/131.225.208.243 is not a directory
- 2009-07-10T15:45:12-05:00 Engine_Front [debug] Both Dirs dont exist
- 2009-07-10T15:45:12-05:00 Engine_Front [debug]

CASE THREE CONTINUED…

- Both directories are not found – the system was never sending its logs
- An exception is thrown to notify the computer security team that this device was never sending its logs

- **CASE FOUR: The same file is checked to have 0 bytes in both of its locations.**
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] 131.225.207.12 is the source
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] 131.225.207.12 is an IP address
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] with a hostname cmssrm
- 2009-07-10T15:45:14-05:00 Engine_Plugin_Test [debug] Notified of preDispatch
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] /logging/syslog-ng/131.225.207.12 is a directory
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] /logging/syslog-ng/cmssrm is a directory
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] Files in /logging/syslog-ng/131.225.207.12
- 2009-07-10T15:45:14-05:00 Engine_Front [debug]
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] messages
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] 0 bytes
- 2009-07-10T15:45:14-05:00 Engine_Front [debug] /logging/syslog-ng/cmssrm/messages : 0 bytes
- 2009-07-10T15:45:14-05:00 FlowEngine [err] Files contain zero bytes

CASE FOUR CONTINUED…

- This depicts that the device in question was logging to the central server at one point in time, but has since stopped.
- If the device is no longer offering any services, this is not a problem. If it is still offering services though, the system must be reconfigured to forward its logs
- An exception is thrown to notify the computer security team about the situation.

SUMMARY

	CASE ONE	CASE TWO	CASE THREE	CASE FOUR
At least one of the directories exist	YES	YES	NO	YES
Non-zero bytes file at least in one location	YES	YES	N/A	NO
Files in a given time variant	YES	NO	N/A	N/A
DECISION	DO NOTHING	SEND ALERT	THROW EXCPETION	THROW EXCPETION

CONCLUSION

- This project can be further enhanced. It could be linked to the e-mail server so that each alert is directed to a particular technician or team of workers.
- The precondition and post condition checks enhance reliability and efficiency of the engine in terms of fully offering the intended service. The codes for these checks are expected to be included in the future.

REFERENCES

- [1] “A Full Web Building Tutorials,” Available: http://www.w3schools.com/. [Accessed: Jun. 18, 2009]
- [2] “git the fast version control system,” Available: http://git-scm.com/ . [Accessed: July 10, 2009]
- [3] Luke Welling and Laura Thomson, PHP and MYSQL Web Development, 3rd ed. Indianapolis: Sams Publishing, 2005.
- [4] “PHP Function List,” Available: http://www.php.net/quickref.php/ . [Accessed: Jun 25, 2009]
- [5] “Zend Framework,” Available: http://framework.zend.com/. [Accessed: Jun. 18, 2009]

ACKNOWLEDGEMENT

- I thank the Fermilab SIST committee for giving me the opportunity to participate in this program, chance to meet incredible people and have a great learning experience.
- I would like to extend my heartfelt gratitude to my supervisors, Joe Klemencic and Tim Rupp without whom I could not have learned so much about PHP, Linux and the Git Version Control System.
- I would also like to thank my mentor Elmie A Peoples-Evans, and David Peterson for their relentless effort to make my stay at the lab as comfortable and effective as possible.
- Further thanks go to all those who made my experience at Fermilab a memorable one.

THANK YOU!

QUESTIONS?