Contents

Introduction

The project focuses on network security enhancement through system and network settings configuration and the deployment of an Intrusion Detection System (IDS) on Windows. Key features include security baseline configuration using industry best practices, IDS setup with customized rules. Additionally, Nxlogs for logging and Graylog for reporting is used . The project will rigorously test the effectiveness of security measures through simulated network attacks.

Capstone objective

To:

- Enhance the security posture of a network by configuring system and network settings to minimize vulnerabilities.
- Deploy an IDS, leveraging tools like Snort, to monitor network traffic for signs of intrusion and suspicious activities.
- Create a simple user interface or dashboard for monitoring of IDS alerts and system status
- Harden the operating system by configuring security policies, such as password policies, user rights assignments, and audit policies.

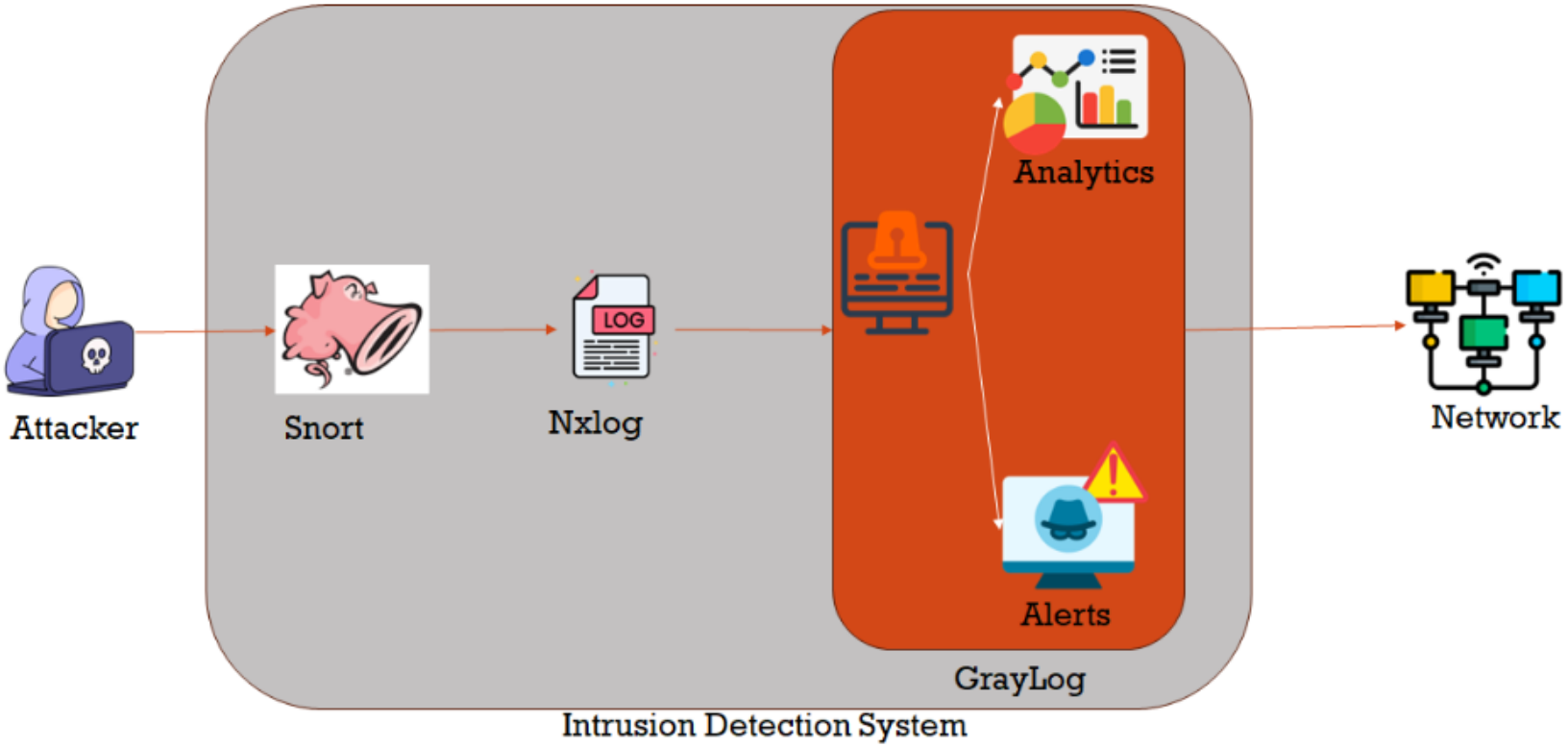
Methodology

Intrusion Detection System, which is a network security tool that monitors systems and networks for malicious activity or policy violations.

Tools and Technologies used

a. Snort – An IDS
b. Nxlog – Log shipper
c. GaryLog – Centralized log manager
d. Linux

Implementation



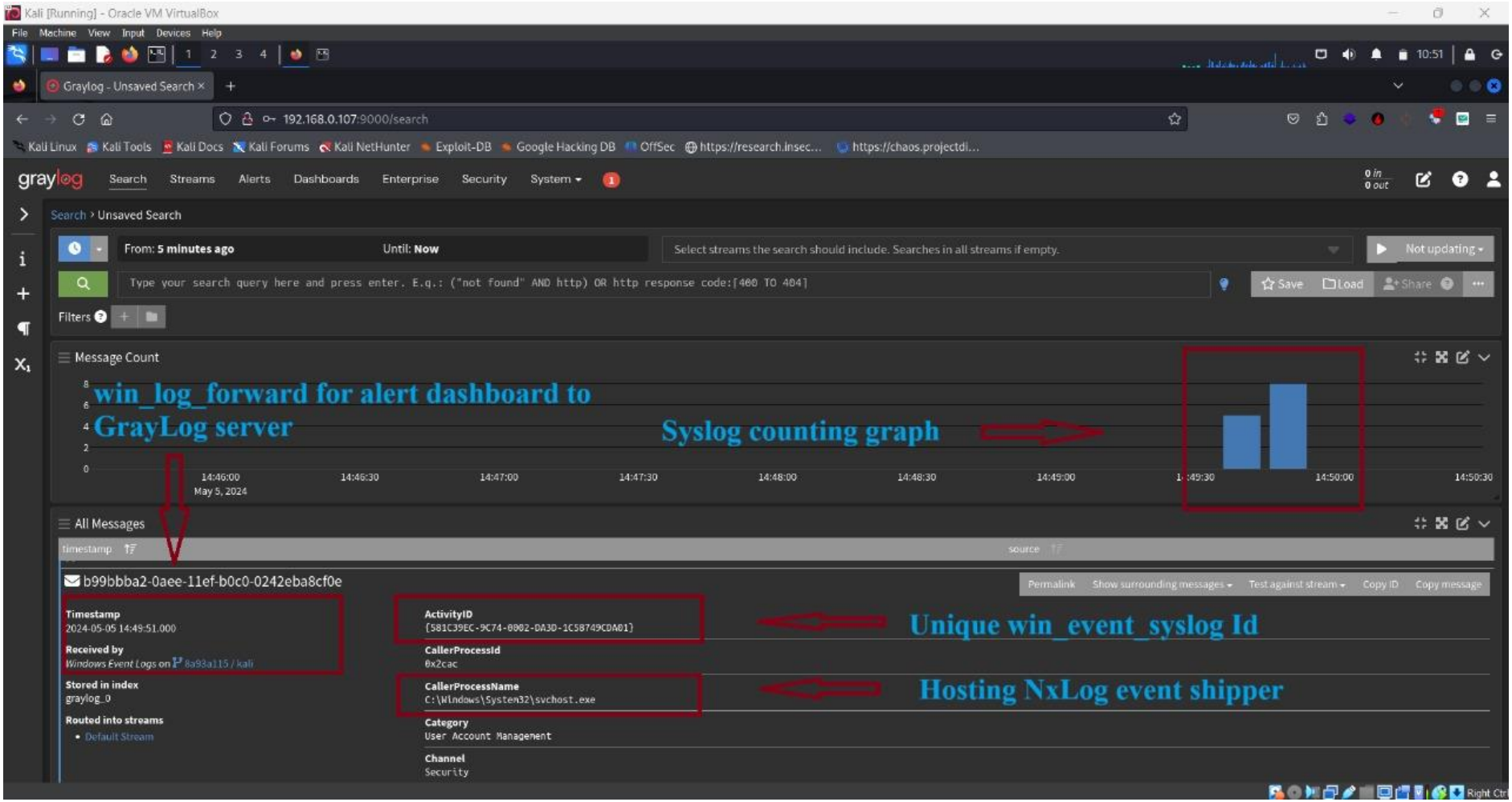
Implementation

```
#NoFreeOnExit TRUE

define ROOT     C:\Program Files\nxlog
define CERTDIR  %ROOT%\cert
define CONFDIR  %ROOT%\conf\nxlog.d
define LOGDIR   %ROOT%\data

include %CONFDIR%\\*.conf
define LOGFILE  %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data

<Extension _syslog>
   Module      xm_syslog
</Extension>

<Extension _charconv>
   Module      xm_charconv
   AutodetectCharsets iso8859-2, utf-8,
utf-16, utf-32
</Extension>
```

```
<Extension _exec>
   Module      xm_exec
</Extension>

<Extension _fileop>
   Module      xm_fileop

# Check the size of our log file hourly, rotate if larger than 5MB
   <Schedule>
      Every   1 hour
      Exec    if (file_exists('%LOGFILE%') and \
              (file_size('%LOGFILE%') >= 5M)) \
               file_cycle('%LOGFILE%', 8);
   </Schedule># Rotate our log file every week on Sunday at midnight
   <Schedule>
      When    @weekly
      Exec    if file_exists('%LOGFILE%') file_cycle('%LOGFILE%', 8);
   </Schedule>
</Extension>

# Snare compatible example configuration
# Collecting event log
 <Input in>
    Module      im_msvistalog
 </Input>
```

```
# Converting events to Snare format
and sending them out over TCP syslog
 <Output out>
    Module      om_udp
    Host        YOUR_GRAYLOG_IP
    Port
YOUR_GRAYLOG_INPUT_PORT
    OutputType  GELF
 </Output>
#
# Connect input 'in' to output 'out'
 <Route 1>
    Path        in => out
 </Route>
```

Results


win_log_forward for alert dashboard to GrayLog server
Syslog counting graph
Unique win_event_syslog Id
Hosting NxLog event shipper

Conclusion

In conclusion, the Network Security Hardening and Intrusion Detection System (IDS) project represents a significant step forward in enhancing network security posture.

By leveraging tools such as Snort, Nxlog , GrayLog with robust configurations, advanced IDS enhances the automated response mechanisms to detect and mitigate potential security threats