Integration of GoPhish with Moodle LMS

1. Introduction

Phishing attacks are one of the leading causes of data breaches. Organizations need to train employees to recognize and prevent phishing attempts. This document details the integration of GoPhish, an open-source phishing simulation tool, with Moodle LMS to automatically enroll employees in cybersecurity training if they fail phishing simulations.

2. Purpose of Integration

1. Automate cybersecurity awareness training based on phishing test results.
2. Identify employees who fall for phishing attempts and train them immediately.
3. Track training effectiveness and behavioral improvements over time.
4. Reduce the risk of security breaches by reinforcing phishing awareness.

3. Setting Up GoPhish

GoPhish is a phishing simulation tool that allows security teams to test phishing awareness.

Installation on Linux:

```
$ wget https://getgophish.com/releases/gophish-v0.11.0-linux-64bit.zip
$ unzip gophish-v0.11.0-linux-64bit.zip
$ cd gophish
$ sudo ./gophish
```

Access GoPhish at http://localhost:3333 and set up:

- Email templates for phishing campaigns
- Landing pages to capture credentials
- Sending profiles using SMTP servers (e.g., Gmail, Office365)

4. Capturing Failed Phishing Attempts

GoPhish tracks who clicked phishing links or submitted credentials.
We use the API to extract this data:

Command to get campaign results:

```
$ curl -H "Authorization: Bearer API_KEY" -H "Content-Type: application/json" https://gophish-server/api/campaigns
```

Extract failed users from the response JSON:

```
$ jq '.results | .[] | select(.status=="Clicked") | .email' results.json
```

These failed users will be enrolled in a cybersecurity training module.

5. Integrating GoPhish with Moodle

Moodle provides a REST API to automate user enrollment in courses.

Steps:
1. Get API Token from Moodle: Site Administration > Server > Web Services > Manage Tokens
2. Use the token to enroll users in a course.

Command to enroll a user:

```
$ curl -X POST "https://moodle-site.com/webservice/rest/server.php" \
    -d "wstoken=MOODLE_API_TOKEN" \
    -d "wsfunction=enrol_manual_enrol_users" \
    -d "moodlewsrestformat=json" \
    -d "enrolments[0][roleid]=5" \
    -d "enrolments[0][userid]=USER_ID" \
    -d "enrolments[0][courseid]=COURSE_ID"
```

6. Automating the Workflow with Python

A Python script automates the process:
- Extract failed users from GoPhish API
- Match users with their Moodle accounts
- Enroll them in cybersecurity courses

Example script:

```
import requests

GOPHISH_API_KEY = "your_gophish_api_key"
MOODLE_API_TOKEN = "your_moodle_api_token"
MOODLE_URL = "https://moodle-site.com/webservice/rest/server.php"

def get_failed_users():
    response = requests.get("https://gophish-server/api/campaigns",
                            headers={"Authorization": f"Bearer {GOPHISH_API_KEY}"}).json()
    return [r['email'] for c in response for r in c['results'] if r['status'] == "Clicked"]

def enroll_in_moodle(email):
    payload = {"wstoken": MOODLE_API_TOKEN, "wsfunction": "enrol_manual_enrol_users",
               "moodlewsrestformat": "json", "enrolments[0][roleid]": 5,
               "enrolments[0][userid]": get_moodle_user_id(email),
               "enrolments[0][courseid]": "your_course_id"}
    requests.post(MOODLE_URL, data=payload)

for user in get_failed_users():
    enroll_in_moodle(user)
```

7. Automating Execution with Cron Jobs

To automate execution, schedule the Python script to run every 10 minutes.

Edit the cron jobs:
$ crontab -e

Add this line:
*/10 * * * * /usr/bin/python3 /path/to/script.py

This ensures failed users are automatically enrolled in training.

8. Tools Used

Tool	Purpose
GoPhish	Simulating phishing attacks
Moodle	Learning management system
GoPhish API	Extracting phishing test results
Moodle API	Enrolling users in cybersecurity training
Python	Automating phishing failure response
Cron Jobs	Scheduling automation tasks

9. Summary

This integration enables organizations to:
1. Conduct phishing simulations using GoPhish.
2. Identify users who fall for phishing attacks.
3. Automatically enroll them in cybersecurity training via Moodle.
4. Automate the entire workflow using Python and Cron Jobs.
By implementing this system, organizations can strengthen security awareness and reduce phishing risks.