An Innovative Approach in Digital Forensic Education and Training: the EduFors Tool

Primož Cigoj, M.Sc. and prof. Borka Jerman Blažič
Laboratory for Open Systems and Networks

Institut ”Jožef Stefan”

primoz@e5.ijs.si

Co-funded by the Prevention of and Fight against Crime Programme of the European Union
New Idea

A virtual (cloud-based) cybercrime training environment to include real life simulation and scenario analysis.
Components

**Backend**
A backend generator for different scenarios (Phishing, DDOS, SQL)

**Course and Assignments**
Use of forensic tools to solve assignments.

**Frontend**
A front-end interface which communicates with backend and assist administrator or student with user friendly dashboard.
Backend - Frontend

Frontend
Request operations on backend through endpoint URL

Backend
Responses with JSON objects
### Scenarios

<table>
<thead>
<tr>
<th>Scenario I</th>
<th>Scenario II</th>
<th>Scenario III</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phishing</strong>&lt;br&gt;Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details.</td>
<td><strong>DDOS</strong>&lt;br&gt;(DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.</td>
<td><strong>SQL Injection</strong>&lt;br&gt;SQL injection is used by hackers to steal data from organizations, in which malicious SQL statements are inserted into an entry field for execution.</td>
</tr>
</tbody>
</table>
Backend Layers

Virtual Machine
Student virtual machine with attached forensic disks (scenarios)

Data Injection
Injection of combined data (dynamic templates + dummy data)

Dynamic Templates
Nullam eu tempor purus. Nunc a leo magna, sit amet.

Dummy Data
Predefined dummy templates.
Output Template

Combined from dummy and attack templates
Backend Process

- Output Template (dummy + attack)
- Data Injection (Guest Mount)
- Virtual Machine (forensic disks)
Required Time

20% Template Generation
Time required to generate attack templates and prepare dynamic content.

80% Virtual Machine Generation
Time required to clone virtual machine template and inject pre-generated attack templates.

100% = 6 minutes
Frontend
Frontend
The Differences

Administrator / Teacher Dashboard
Courses, Students, Virtual Machines, Assignments management.

Student Dashboard
Course enrollment and assignment solving.
Scenarios Complexity

- SQL: 50%
- Phishing: 30%
- DDOS: 20%
DDOS Scenario

Various DDOS Attacks

Apache Log

Syslog
Phishing Scenario

- Brute-force Attack
- SQL Injection
- Auth Log Check
- Bash History
- MySQL / Apache logs

PHISHING
SQL Scenario

- SQL Injection
- MySQL Log
- Apache Log
- Website Code
The Estimated Time

30% PHISHING

20% DDOS

50% SQL
Phishing Scenario

Note: Use HD2 Disk in X-Ways.

Description of attack: An attacker tried to gain access to the web hosting server using brutforce tool. Through ssh he gained access to the server, where he explored the environment (mysql, apache etc.) for possible useful information. Attacker uploaded website and left it running for a while and gained victims data. At the end he deleted his uploaded data. Find the correct answers below.

Choose correct attacker IP:
- 133.240.139.53
- 207.40.75.93
- 132.253.0.70

Choose correct date of attack:
- 2010-03-16 10:06:00
- 2009-11-24 04:46:00
- 2009-11-24 18:16:00

Choose stolen data:
- user passwords
- personal photos
- credit cards
**Course Assignment**

Researched and obtained results from forensic disks answered in the online form.

---

**Student Virtual Machine**

Virtual machine with attached forensic disks / scenarios where user investigate them. Pre-installed with Windows 7 autologin and X-Ways.

---

**Forensic Disks and Tools**

Obtaining Data

X-Ways tools used to investigate each scenario (forensic) disk.

---

**Assignment**

Course Assignment

Researched and obtained results from forensic disks answered in the online form.
Assignment Success

Correct Answers
More than 50% correct answers.

Elapsed time
Time is measured while solving an assignment.
Source Lines of Code (SLOC)

- Scenario Templates: 5000
- Backend Algorithms: 2000
- Frontend Algorithms: 5000
Thank You