

# How to Design a Blue Team Scenario for Beginners on the Example of Brute-Force Attacks on Authentications

Andreas Eipper and Daniela Pöhn<sup>a</sup>  
*Universität der Bundeswehr München, Neubiberg, Germany*

**Keywords:** Cyber Range, Scenario Design, Brute-Force Attack, Training Scenario.

**Abstract:** Cyber attacks are ubiquitous and a constantly growing threat in the age of digitization. In order to protect important data, developers and system administrators must be trained and made aware of possible threats. Practical training can be used for students alike to introduce them to the topic. A constant threat to websites that require user authentication is so-called brute-force attacks, which attempt to crack a password by systematically trying every possible combination. As this is a typical threat, but comparably easy to detect, it is ideal for beginners. Therefore, three open-source blue team scenarios are designed and systematically described. They are contiguous to maximize the learning effect.

## 1 INTRODUCTION

The world is becoming more and more connected through digital systems. According to (Lord, 2020), users have between 80 and 150 online accounts, including social media, online banking, and many more. With the help of publicly available information and basic hacking skills, many authentication systems can be infiltrated or compromised, giving attackers access to users' personal information. Each user should protect their accounts with individual secure passwords. In practice, users tend to use single passwords for multiple services. This increases the impact of a security incident. Simple passwords, such as 123456, test1, qwerty, iloveyou and others in wordlists like `rockyou.txt`, can be easily cracked. Social engineering and online research, also called open source intelligence (OSINT), help hackers figure out valid passwords. The information obtained can automate brute-forcing as the attack progresses. As a result of various incidents and attacks (e. g., data leaks, brute-force attacks, and phishing), lists of user names and passwords can be found on the Internet. Credential stuffing is, for example, an attack that automatically tries these stolen credentials for other services.

The aim of this paper is to impart knowledge and skills in the field of detection and countermeasures to participants in cyber range training courses by designing and implementing open-source blue team scenarios

with the topic of brute-force attacks on authentication in a web application. Three subsequent scenarios each cover a specific part of the learning content and lay the foundation for beginners and those interested in protection against brute-force attacks.


Therefore, this paper contributes 1) the design process for beginner scenarios; 2) a description of the overall training setting and each scenario in a generic way; 3) an evaluation based on a training session.

The paper is structured as follows: Related work is introduced in Section 2. Next, the concept of the three beginner scenarios is outlined. This is the basis for the practical implementation in Section 4, which is then tested with students, as described in Section 5, and discussed in Section 6. Last but not least, the paper is concluded and future work is given in Section 7.

## 2 RELATED WORK

This chapter evaluates related work to brute-force detection and prevention as well as cyber training and training scenarios. To the best of our knowledge, there is no training for learning about brute-force detection and prevention.

**Brute-Force Detection and Prevention:** Applying detection techniques is important to detect anomalous behavior early and minimize its impact on the network. One such application is Wireshark, as de-

<sup>a</sup>  <https://orcid.org/0000-0002-6373-3637>

scribed by (Mohammed et al., 2017). The authors reason that the automatic ban function of FileZilla is not enough to stop a brute-force attack. Therefore, they recommend deactivating the targeted account. This is possible if only single or selected accounts are under attack. Other important sources for detection are log files. Apache hypertext transfer protocol (HTTP) server offers different log files, including `error.log` (diagnosis information and errors) and `access.log` (processed requests). Based on these log files, different attacks can be noticed by personnel if the attacks are known (Meyer, 2021; Simic, 2019). However, it also requires training to detect attacks, either manually or with the aid of tools. (Lopez-Araiza and Cankaya, 2017) describe tools for network security and forensics including Fail2Ban, which provides detection and ban functionalities.

**Cyber Training:** To achieve pedagogical added value, it is important to design the training competently. (Gáliková et al., 2021) provide guidelines on how training can be effectively designed using the principle of serious games. The training is intended to reproduce realistic environments that require strategic and adversarial thinking. (Knüpfer et al., 2020) categorize cyber training. (Kaschow et al., 2017) examined several training courses to determine their added value for network defense. The authors conclude that the representation of realistic and comprehensible attack scenarios with different patterns leads to a high learning effect. The training should be accompanied by specialist staff. A high proportion of practical exercises can reduce the duration of training while achieving higher learning goals. In addition, different online learning platforms provide gamified real-world labs as evaluated by (Stu et al., 2022).

**Training Scenarios:** (Al-Mohannadi et al., 2016) specify cyber attacks by applying the diamond model, consisting of an adversary, capability, infrastructure, and victim. These categories can be applied for training scenarios as well, but are not specific enough. (Nagarajan et al., 2012) give an overview of game design for cyber security training, whereas (Koutsouris et al., 2021) analyze evaluation metrics for cyber security training. (Subaşı et al., 2017) propose amongst other things a workflow diagram for training exercises, describing the main steps objectives; environment configuration; design and deploy; train test score; and analyze evaluate adjust. Although these steps can be applied, they are rather generic. The design and use cases of the KYPO cyber ranges are presented by (Vykopal et al., 2017). In their documentation, (Masaryk University, 2022) state how to

use their patterns to design use cases and workflows. Even though it is a systematic approach, it is focused on their environment. Similarly, (Arshad et al., 2021) propose a domain-specific language based on the MITRE ATT&CK framework for dynamic training in cyber range environments. The authors describe the classification, environment, execution, and evaluation in a systematic, but also high-level way.

**Summary:** Skills in network analysis is a core task for blue teams. Training designed for beginners is hardly described. We did not find any training on brute-force attacks related to authentication. Therefore, we provide a step-by-step guide and a generic description of the scenarios, which can be repurposed for other training settings.

### 3 CONCEPT

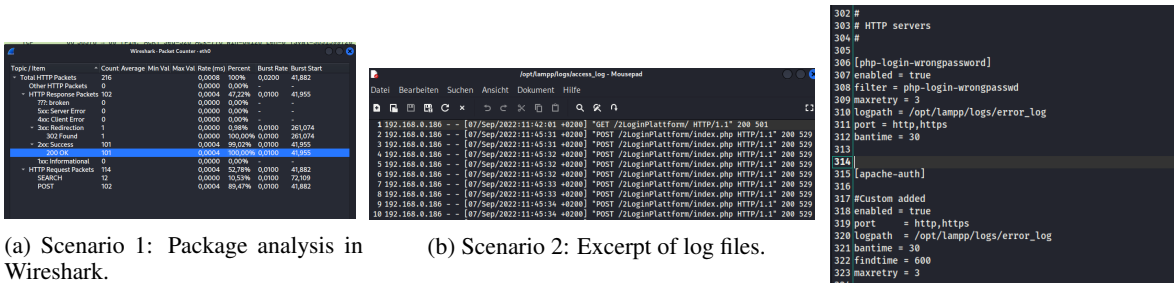
This chapter outlines the theoretical composition and structure of the designed beginner scenarios. The description of the structure of the three subsequent scenarios is based on (Knüpfer et al., 2020). Thereby, the audience, training environment, training setup, and technical setup are defined in general. In addition, the scenario, goals, and resources are explained in more detail. This is supplemented with a possible procedure based on related work, described in Section 2. Based on the received feedback, see Section 5, prerequisites are necessary to pre-access.

#### 3.1 Overview

**Audience:** The target audiences are students and other interested persons with basic cyber security knowledge. Thereby, the prerequisite consists of the knowledge gained in a bachelor's program. Hence, the sector is described as universities and the proficiency level is the related audience. The training has the purpose to increase the ability to detect brute-force attacks on authentication of websites, thereby, using log files and Wireshark, resp. understanding of intrusion prevention.

**Training Environment:** The training is carried out in dedicated computer rooms or in our cyber range. With the goal to understand brute-force attacks on authentication, their detection, and prevention, the material is divided into three distinct scenarios. Each scenario covers a certain aspect to learn basic knowledge:

1. Wireshark: As a visual instrument for analyzing and graphically processing data logs (Usha et al.,



(a) Scenario 1: Package analysis in Wireshark.

(b) Scenario 2: Excerpt of log files.

(c) Scenario 3: Rules in Fail2Ban.

Figure 1: Scenarios.

2010; Mohammed et al., 2017). In addition, Wireshark could be used in advanced scenarios with no suitable log files.

2. Log Files: As a system-related and fast source of information and supplement to Wireshark. Log files are utilized in more advanced tools. (Meyer, 2021; Simic, 2019)
3. Fail2Ban: As a simple tool for intrusion prevention (Lopez-Araiza and Cankaya, 2017).

The first two scenarios cover intrusion detection. In the last scenario, Fail2Ban is presented as an intrusion prevention system (IPS) for blue teams. Thereby, the participants first see the malicious traffic graphically, before analyzing the in-going traffic with the command line. Last but not least, a prevention possibility is explained. The topics are coherent and can, therefore, be dealt with in one go for maximum learning effect. For added pedagogical value, the diamond framework (Al-Mohannadi et al., 2016) and the cyber kill chain can be used as an aid. In addition, follow-on topics can be discussed.

**Training Setup:** No scoring is set up in these three basic scenarios as the primary goal is to introduce the participants to the concepts and handling of Kali and its tools. Scoring can be applied in advanced scenarios to challenge the participants. The participants act as a blue team in single mode at a general level.

**Technical Setup:** The scenarios try to rebuild a simplified realistic environment structure. The deployment is on-premise with a resp. several virtual machines (VMs) due to the architecture of our TAME range, as outlined by (Shin et al., 2019). Although VMware is the primary installation, VirtualBox or other products could be imported.

**Description:** The training concept can be summarized as in Listing 1. First, a description of the scenarios (name, goal, scoring, and environment) is given

(Lines 3-7). Then the set of scenarios with each scenario, intended tool, and goal are generally stated (Lines 8-20). This description language is based on related work in Section 2. It tries to balance detailed information and generic representation. The description utilizes JavaScript Object Notation (JSON) as a prominent candidate for descriptions on the Internet, similar to the related work. Depending on the cyber range, either automated provisioning with tools such as Vagrant and Puppet or VMs are set up (Shin et al., 2019). In consequence, the descriptions either result (with translation) in automated provisioning or can be used to build the VMs. The scenarios and the technical setup need to be detailed in further descriptions.

Listing 1: Training description.

```

1 {
2   "training": {
3     "description": {
4       "name": "Brute-Force AuthN",
5       "goal": "analyze",
6       "scoring": "none",
7       "environment": "cyber range",
8       "scenarios": [
9         {
10          "scenario": "network traffic",
11          "tool": "Wireshark",
12          "goal": "understand",
13        }, {
14          "scenario": "logging",
15          "tool": "log files",
16          "goal": "apply",
17        }, {
18          "scenario": "IPS",
19          "tool": "Fail2Ban",
20          "goal": "analyze",
21        }
22      ]
23    },
24  },
25 }

```

### 3.2 Scenario 1: Wireshark

**Training Environment:** The scenario provides the participants with a VM to work on. The aim is to discover abnormalities in the packet capture (PCAP) files. The following learning objectives are aimed for in this scenario.

- Wireshark basics:
  - Operation of the tool.
  - Filter application.
  - Statistics creation and evaluation.
- Detection of simple brute-force attacks.
- Awareness of log files.

**Training Setup:** The lecturer discusses the basics of Wireshark and brute-force attacks, in order to create a theoretical understanding. The participants search for and open the PCAP file in Wireshark and try to recognize the attack, shown in Figure 1a. Then, mitigation strategies are discussed.

**Technical Setup:** The participants use a stored PCAP file.

### 3.3 Scenario 2: Log Files

**Training Environment:** The aim is to discover anomalies in the log files and to include them in the analysis results of scenario 1. The following learning objectives are aimed for in this scenario.

- Basics Log Files:
  - Types of log files.
  - Locations of log files on Debian distributions.
  - Evaluation of log files.
- Detection of brute-force attacks.
- Awareness of log files.

**Training Setup:** After an introduction to log files, the participants search for and open the log files and analyze them accordingly (pattern, IP addresses, in combination with the PCAP file).

**Technical Setup:** The participants use the according log files `access.log` and `error.log`.

### 3.4 Scenario 3: Fail2Ban

**Training Environment:** The goal is to activate the Fail2Ban configuration and demonstrate the capabilities of the tool in a practical demonstration. This scenario has the following learning objectives.

- Intrusion Prevention Basics:
  - Functionality.
  - Areas of application.
- Basics Fail2Ban:
  - Theoretical functionality.
  - Practical implementation.

**Training Setup:** The lecturer summarizes the results from the previous scenarios to create a basis for discussions on ways to combat brute-force attacks. After collecting and evaluating ideas and suggestions, Fail2Ban and intrusion prevention, in general, are presented. Once the theoretical basis has been created, Fail2Ban is installed and configured. The properties of the `local.jail` file and the necessary commands for activation are shown here, see Figure 1c. The functionality is demonstrated using an example attack. Finally, possible errors and weaknesses of Fail2Ban are discussed with the participants.

**Technical Setup:** The participants use Fail2Ban with its configuration and log files.

## 4 IMPLEMENTATION

The implementations and technical precautions required to carry out the training are described in this section. The implementation can be summarized as in Listing 2. First, a description of the implementation is given (Lines 3-5). Then the environment featuring the different teams, i. e., blue team (Lines 7-19), red team (Lines 20-23), and yellow team (Lines 24-27), is summarized. This especially includes platforms, tools, IP addresses, and resources.

Listing 2: Implementation description.

```

1 {
2   "training": {
3     "description": {
4       "name": "Brute-Force AuthN",
5       "scenarios": "3",
6     }, "environment": {
7       "blueteam": {
8         "platform": "Kali Linux",
9         "tools": ["Wireshark", "log
10          files", "Fail2Ban"],
11       "ip": "192.168.1.10",
12       "infrastructure": {
13         "name": "WebApp",
14         "goal": "web application",
15         "tools": ["PHP", "Apache", "
16          phpMyAdmin"],
17       "sources": ["PHP pages",
```



```

16     "/var/log/*",
17     "/opt/lampp/logs/*",
18     "/etc/fail2ban/jail.local"]
19     },
20     "redteam": {
21       "platform": "Kali Linux",
22       "tools": ["Firefox", "Burp
23         Suite", "FoxyProxy"],
24       "ip": "192.168.2.1-100",
25     }, "yellowteam": {
26       "platform": "Windows 11",
27       "tools": ["Chrome", "Selenium"]
28     },
29     "ip": "192.168.2.1-100",
30   },
31 }

```

As a basis for the blue and red team platforms, VMs are created with Oracle VM VirtualBox and Kali Linux as the operating system. Alternatively, Debian could be used for blue teams.

The web application of the infrastructure is created with the LAMPP/XAMPP framework (PHP, Apache, MariaDB, and phpMyAdmin) by (Adobe, 2023). It consists of five PHP files: a login page, homepage, registration page, logout page, and a connection page to the database. The data required for the web application is stored in the database. The log files can be found at the default location. In addition, several tools for the analysis are available or can be installed, such as Fail2Ban.

In order to simulate the attacks (red team), the Burp Suite (Port Swigger, 2022) is utilized. Burp Suite is a tool developed by Portswigger Web Security with the ability to act as a proxy for manual testing of web applications. Other applications such as THC Hydra, Medusa, and Patator as shown by (Offensive Security, 2023a) could be used instead but Burp Suite provides a graphical interface and is often applied for website testing. Burp Suite is triggered by the browser plugin (FoxyProxy, 2023). Burp Suite Proxy and Intruder (tryhackme, 2021) catch the request to the target. The attacker then can modify it to start the brute-force attack as shown in Figure 2a. With changing IP addresses through the usage of proxies, Tor, or virtual private networks (VPNs), a distributed attack can be imitated, if no distributed setting is available. Alternatively, editing files is possible.

The tool selected to generate ordinary network traffic is Selenium (Ramya et al., 2017). Originally, Selenium is a portable testing framework primarily focused on testing web-based applications. It provides a record-playback feature that helps in recording test case executions and allows testers to

play them back at a later time as shown in Figure 2b. Thereby, simple user behavior can be simulated (Tanaka et al., 2020; Srinivasa Rao and Pais, 2017). A new test is first started and then a login process is recorded. These and other tests can be run as often as you like at later times, thereby, simulating regular user behavior. This has the advantage of a simple generation. On the other hand, it replays without much variation.

## 5 EVALUATION BASED ON TRAINING SESSION

We evaluate the training scenarios and their description through a small-scale training session with students. In order to test the learning effects of the scenarios, a training session was conducted. The participants were predominantly male, young, and technical-savvy. They had a rudimentary knowledge of cyber security. The following criteria were evaluated during the training and subsequent assessment:

**Sources of Information:** The participants had material about brute-force attacks. The material was described as comprehensive and intuitive in terms of structure and writing style. During the training, it turned out that the amount of information material becomes confusing for beginners due to the complexity and the missing knowledge about Linux and the command line.

**Training Structure:** The structuring was emphasized positively. However, the training revealed slower learning progress than expected. Nevertheless, all participants successfully completed the training within the allocated and some buffer time. One possible option could be to separate the scenarios based on their properties. Another option would be to add an informative session beforehand to explain the theory. This though would extend the training time in total (Kaschow et al., 2017). Last but not least, the Linux OS Kali and the command line could be introduced in another session. Several courses about Kali can be found online, including the official course PEN-103 by (Offensive Security, 2023b).

**Training Process:** The guide was positively received and was effective according to all participants. Here too, however, the beginner-typical deficits came clear. Basics such as operating the OS Kali, in particular using the command line to configure Fail2Ban, also had to be explained.

In summary, the training was positively received by all. The learning effect and awareness of cyber secu-



## 7 CONCLUSIONS

The number of digital accounts is ever-increasing. The same is the case with attacks on them, ranging from brute-force attacks to sophisticated supply chain attacks targeting active directory environments. In order to train beginners, we designed a series of blue team scenarios with the topic of brute-force attacks on authentication in a web application. In the first step, we evaluated related work. With the help of the results obtained, three consecutive scenarios for the cyber range were designed and implemented. These scenarios each cover a specific part of the learning content and lay the foundation for beginners and those interested in protection against brute-force attacks. Nonetheless, more scenarios are required to train future system administrators. Finally, the open-source scenarios were assessed in a small-scale training and a discussion.

In future work, we plan to extend the scenarios to cover different attacks on identities and identity management systems, such as the more advanced attacks of Kerberoasting, Golden Ticket, and Golden SAML, and other OSs, in particular Windows. In addition, we will evaluate and improve our description language with these scenarios and discuss it with other experts. For the brute-force scenarios, regular traffic was generated with Selenium. We want to investigate other techniques and represent the traffic more realistically for a better training setup in future work.

## REFERENCES

- Adeleke, O. A., Bastin, N., and Gurkan, D. (2022). Network Traffic Generation: A Survey and Methodology. *ACM Comput. Surv.*, 55(2).
- Adobe (2023). XAMPP Apache + MariaDB + PHP + Perl. <https://www.apachefriends.org/index.html>. accessed January 11, 2023.
- Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., and Disso, J. (2016). Cyber-Attack Modeling Analysis Techniques: An Overview. In *Proceedings of the 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pages 69–76. IEEE.
- Arshad, S., Alam, M., Al-Kuwari, S., and Khan, M. H. A. (2021). Attack Specification Language: Domain Specific Language for Dynamic Training in Cyber Range. In *Proceedings of the 12th Global Engineering Education Conference (EDUCON)*, pages 873–879. IEEE.
- FoxyProxy (2023). FoxyProxy. <https://getfoxyproxy.org>. accessed January 11, 2023.
- Gáliková, M., Švábenský, V., and Vykopal, J. (2021). Toward Guidelines for Designing Cybersecurity Serious Games. In *Proceedings of the 52nd Technical Symposium on Computer Science Education (SIGCSE)*, page 1275. Association for Computing Machinery.
- Kaschow, R., Hanka, O., Knüpfer, M., and Eiseler, V. (2017). Cyber Range: Netzverteidigung trainieren mittels Simulation. In *Proceedings of the D•A•CH Security 2017*, pages 126–137. syssec.
- Knüpfer, M., Bierwirth, T., Stiemert, L., Schopp, M., Seiber, S., Pöhn, D., and Hillmann, P. (2020). Cyber Taxi: A Taxonomy of Interactive Cyber Training and Education Systems. In Hatzivasilis, G. and Ioannidis, S., editors, *Model-driven Simulation and Training Environments for Cybersecurity*, pages 3–21, Cham. Springer International Publishing.
- Koutsouris, N., Vassilakis, C., and Kolokotronis, N. (2021). Cyber-Security Training Evaluation Metrics. In *Proceedings of the 1st International Conference on Cyber Security and Resilience (CSR)*, pages 192–197. IEEE.
- Lopez-Araiza, C. and Cankaya, E. (2017). A Comprehensive Analysis of Security Tools for Network Forensics. *Journal of Medical - Clinical Research & Reviews*, 1(3):1–9.
- Lord, N. (2020). Uncovering Password Habits: Are Users' Password Security Habits Improving? <https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic>. accessed January 11, 2023.
- Masaryk University (2022). KYPO Cyber Range Platform. <https://docs.crp.kypo.muni.cz>. accessed January 11, 2023.
- Meyer, R. (2021). Detecting Attacks on Web Applications from Log Files. techreport, SANS Institute.
- Mohammed, M. A., Degadzor, A. F., Effrim, B. F., and Appiah, K. A. (2017). Brute Force Attack detection and prevention on a network using wireshark analysis. *International Journal of Engineering Sciences & Research Technology*, 6(6):26–37.
- Nagarajan, A., Allbeck, J. M., Sood, A., and Janssen, T. L. (2012). Exploring game design for cybersecurity training. In *Proceedings of the International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pages 256–262. IEEE.
- Offensive Security (2023a). All Kali Tools. <https://www.kali.org/tools/all-tools/>. accessed January 11, 2023.
- Offensive Security (2023b). PEN-103 Modules. <https://portal.offensive-security.com/courses/pen-103/books-and-videos/modules>. accessed January 11, 2023.
- Port Swigger (2022). Burp Suite documentation. <https://portswigger.net/burp/documentation>. accessed January 11, 2023.
- Ramya, P., Sindhura, V., and Sagar, P. V. (2017). Testing using selenium web driver. In *Proceedings of the 2nd International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pages 1–7. IEEE.
- Shin, S., Seto, Y., Kasai, Y., Ka, R., Kuroki, D., Toyoda, S., Hasegawa, K., and Midorikawa, K. (2019). De-

- velopment of Training System and Practice Contents for Cybersecurity Education. In *Proceedings of the 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, pages 172–177. IEEE.
- Simic, S. (2019). How to View Apache Access & Error Logs. <https://phoenixnap.com/kb/apache-access-log>. accessed January 11, 2023.
- Srinivasa Rao, R. and Pais, A. R. (2017). Detecting Phishing Websites Using Automation of Human Behavior. In *Proceedings of the 3rd Workshop on Cyber-Physical System Security (CPSS)*, page 33–42. Association for Computing Machinery.
- Stu, S., Ananth, J., and de Leon Daniel, C. (2022). A Survey of Cloud-hosted, Publicly-available, Cyber-ranges for Educational Institutions. *Journal of Computing Sciences in Colleges*, 38.
- Subaşu, G., Roşu, L., and Bădoi, I. (2017). Modeling And Simulation Architecture For Training In Cyber Defence Education. In *Proceedings of the 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pages 1–4. IEEE.
- Tanaka, T., Niibori, H., Shiyinxue, L., Nomura, S., Nakao, T., and Tsuda, K. (2020). Selenium based Testing Systems for Analytical Data Generation of Website User Behavior. In *Proceedings of the 13th International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pages 216–221. IEEE.
- tryhackme (2021). Burp Suite: Intruder. <https://tryhackme.com/room/burpsuiteintruder>. accessed January 11, 2023.
- Usha, B., Ashutosh, V., and Saxena, M. (2010). Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of Computer Applications*, 6(7):1–5.
- Vykopal, J., Oslejsek, R., Celeda, P., Vizvary, M., and Tovarnak, D. (2017). KYPO Cyber Range: Design and Use Cases. In *Proceedings of the 12th International Conference on Software Technologies (ICSOFT)*, pages 310–321. INSTICC, SciTePress.
- Walden, J. (2008). Integrating Web Application Security into the IT Curriculum. In *Proceedings of the 9th SIGITE Conference on Information Technology Education (SIGITE)*, page 187–192, New York, NY, USA.