CYBER SECURITY FOR BEGINNERS
CYBER SECURITY FOR BEGINNERS

Program Overview

Experience hands-on training in real-time using examples of real-life scenarios that run in a live virtual environment. This course is designed to train IT professionals, such as developers, administrators or ERP personnel, who do not deal directly with cyber security on a daily basis. During the course, participants will be required to monitor, investigate and mitigate security incidents, using Cyberbit’s pre-defined scenarios.

This course includes both the technical and operational aspects of incident investigation. On the technical side, participants will learn tools and techniques used to investigate the network and will practice using these tools on the virtual environment. On the operational side, participants will learn about working as a team, dividing the tasks of monitoring and investigating between the different team members, drawing conclusions from the gathered information and applying mitigation processes.

Audience

Designed for IT personnel who are new to cyber security, the goal of this course is to introduce the cyber security domain and provide the opportunity for hands-on training in real time.

Activities

The main activities of the course include:

- **Theory:** An introduction to the theoretical background of cyber security.
- **Scenario-based training:** Investigate the virtual environment, using the Cyber Trainer System.
- **Scenario debrief:** Instructor will discuss the solution of the scenario, including an analysis of participant’s results, additional insights, mitigation plans and more.
- **Review & Preparation:** Review of prior information and preparation for the next scenario.
- **Security Utilities Training:** Training and practice with key investigation tools. Content is dynamic and may change to suit participant’s knowledge and the time available.

Required Knowledge

Participants should have basic knowledge in:

- Operating systems: General knowledge of Windows and Linux
  - Windows & Linux Command Line
  - Windows & Linux Log Management
- Networking & Logs: General understanding of networking
- Basic cyber security concepts at a high level:
  - Anti-Malware
  - Firewalls
  - IDS/IPS
  - Security Information and Event Management (SIEM)
  - Security Operations Center (SOC)

Scenarios

**Web Defacement:** In this scenario, the Cyber Training System scans the network for known services ports, once found an SSH server, uses a brute force attack to gain full access to the server. After accessing the server, it scans the server for hosted websites and replaces each with a corrupted website.

**SQL Injection:** In this scenario, the Cyber Training System attacks a known public web server using SQL injection. During the attack, the Cyber Training System enables the internal SQL stored procedure named `xp_cmdshell`, which is used to extract all employees’ computer names and e-mail addresses from the Active Directory using PowerShell scripts and to stop the internal server services using the Remote Service Control. The attack repeats until stopped by the instructor.

**Security Utilities:** List of utilities for the Security Utilities Training section (content is dynamic and may change to suit participant’s knowledge and the time available):

- Command line used for investigation (Windows & Linux)
- Firewall
- MSSQL Server Management
- Process Explorer
- SIEM
- TCP View
- Windows Event Viewer
- Wireshark

Commitment

Training is held over five days from 9 a.m. to 5 p.m.

Location

Cyber Range, College of Business, Business Building (BB) 1.01.02
Main Campus, One UTSA Circle, San Antonio, TX 78249

Cost

$5,000 | Includes tuition, course materials (printed and online), parking at UTSA, meals and refreshments

UTSA Continuing Education Units (CEUs) are available for completing this workshop.

We offer a discounted rate to support and make training accessible to not-for-profit organizations and small businesses. Group discounts for all organizations are also available, contact execed@utsa.edu for more information.

Registration

## Training Schedule

<table>
<thead>
<tr>
<th>Time</th>
<th>DAY 1</th>
<th>DAY 2</th>
<th>DAY 3</th>
<th>DAY 4</th>
<th>DAY 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 a.m.</td>
<td>Review and Preparation</td>
<td>Review and Preparation</td>
<td>Review and Preparation</td>
<td>Review and Preparation</td>
<td>Review and Preparation</td>
</tr>
<tr>
<td>9:30 a.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00 a.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30 a.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 a.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:30 a.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30 - 1:30 p.m.</td>
<td>Lunch Break</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:30 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:00 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:30 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:15 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:30 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:00 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:30 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### DAY 1
- **9:00 a.m.** Review and Preparation
- **9:30 a.m.** Cyber Security Overview
- **10:00 a.m.** Cyber Security Overview
- **10:30 a.m.** Windows Forensics
- **11:00 a.m.** Linux Forensics
- **12:30 - 1:30 p.m.** Lunch Break
- **1:30 p.m.** SIEM Overview
- **2:00 p.m.** Review and Preparation
- **2:30 p.m.** Review and Preparation
- **3:15 p.m.** Firewall Overview
- **3:30 p.m.** Firewall Overview
- **4:00 p.m.** Linux Forensics
- **4:30 p.m.** Linux Forensics
- **5:00 p.m.** Linux Forensics

### DAY 2
- **9:00 a.m.** Review and Preparation
- **9:30 a.m.** Windows Forensics
- **10:00 a.m.** Network Forensics
- **10:30 a.m.** Scenario 1: Application
- **11:00 a.m.** Scenario 2: Application
- **12:30 - 1:30 p.m.** Lunch Break
- **1:30 p.m.** Review and Preparation
- **2:00 p.m.** Review and Preparation
- **2:30 p.m.** Review and Preparation
- **3:15 p.m.** Theoretical Knowledge
- **3:30 p.m.** Theoretical Knowledge
- **4:00 p.m.** Theoretical Knowledge
- **4:30 p.m.** Theoretical Knowledge
- **5:00 p.m.** Theoretical Knowledge

### DAY 3
- **9:00 a.m.** Review and Preparation
- **9:30 a.m.** Network Forensics
- **10:00 a.m.** SC processes
- **10:30 a.m.** Scenario 1: Debrief
- **11:00 a.m.** Scenario 2: Debrief
- **12:30 - 1:30 p.m.** Lunch Break
- **1:30 p.m.** Review and Preparation
- **2:00 p.m.** Review and Preparation
- **2:30 p.m.** Review and Preparation
- **3:15 p.m.** Theoretical Knowledge
- **3:30 p.m.** Theoretical Knowledge
- **4:00 p.m.** Theoretical Knowledge
- **4:30 p.m.** Theoretical Knowledge
- **5:00 p.m.** Theoretical Knowledge

### DAY 4
- **9:00 a.m.** Review and Preparation
- **9:30 a.m.** Scenario 1: Application
- **10:00 a.m.** Scenario 2: Application
- **10:30 a.m.** Scenario 1: Debrief
- **11:00 a.m.** Scenario 2: Debrief
- **12:30 - 1:30 p.m.** Lunch Break
- **1:30 p.m.** Review and Preparation
- **2:00 p.m.** Review and Preparation
- **2:30 p.m.** Review and Preparation
- **3:15 p.m.** Theoretical Knowledge
- **3:30 p.m.** Theoretical Knowledge
- **4:00 p.m.** Theoretical Knowledge
- **4:30 p.m.** Theoretical Knowledge
- **5:00 p.m.** Theoretical Knowledge

### DAY 5
- **9:00 a.m.** Review and Preparation
- **9:30 a.m.** Review and Preparation
- **10:00 a.m.** Review and Preparation
- **10:30 a.m.** Review and Preparation
- **11:00 a.m.** Review and Preparation
- **11:30 a.m.** Review and Preparation
- **12:00 p.m.** Review and Preparation
- **12:30 - 1:30 p.m.** Lunch Break
- **1:30 p.m.** Certificate Presentation
- **2:00 p.m.** Certificate Presentation
- **2:30 p.m.** Certificate Presentation
- **3:15 p.m.** Certificate Presentation
- **3:30 p.m.** Certificate Presentation
- **4:00 p.m.** Certificate Presentation
- **4:30 p.m.** Certificate Presentation
- **5:00 p.m.** Certificate Presentation

**12:30 - 1:30 p.m. Lunch Break**

**3:30 p.m.** Certificate Presentation

**Summary and Feedback**

---

**execed.utsa.edu**

**Center for Professional Excellence**
One UTSA Circle, San Antonio, Texas 78249
Business Building 1.01.20 | 210.458.4778 | execed@utsa.edu