CYBERSECURITY COURSE SYNOPSIS

The course is delivered in two formats:

⇒ a daily format

⇒ a week-long format (hybrid attendance)

The daily course aims to deliver the contents of this synopsis at a higher level, with approximately 60 minutes per module, totalling a 360-minute (6-hour) duration within an 8-hour period, allowing for adequate breaks and adaptability in case of extended class sessions.

The weekly course aims to use the daily schedule, but on a single module per day basis (5-days total).

Table of Contents

CYBERSECURITY COURSE SYNOPSIS

1. Course Synopsis

Boudica offer a course that is unique in its aims, breadth, depth, and delivery.

Everyone needs to know about cybersecurity these days, whether it's for managing online systems, GDPR compliance, or avoiding phishing and ransomware attacks; yet we have so little time and find the training dull.

So, our courses are compact, extensive, and even fun. Students will go away knowledgeable not just about working more securely, but with a good understanding of why cybersecurity is important, various attacks and defences.

We want students not just having crucial buy-in, but genuine, positive enthusiasm about the subject coming from a memorable experience of exercises and demonstrations with fun tutors.

The two courses we offer, One Day and One Week, differ only in depth. We currently spread 5 modules over the Week course but compress these into 5 hour-long lessons for the Day course.

1.1. Orientation / Cybersecurity Fundamentals

Each course begins with an orientation and introduction to the big picture of cybersecurity, outlining ideas about risk. mitigation, attack surfaces, types of security like infosec, OpSec, HumSec, network security, defence in depth as well as roles and responsibilities.

Orientation is designed to accustom you to terminology and the 'security mindset'. Here we also outline the remaining course structure and activities.

1.2. Modules

This modules section provides a comprehensive, high-level overview of the course content, detailing the thematic modules and topics covered throughout the program.

1.2.1. Networking & Defensive Security

Perhaps this is most fun part of the course because it involves the most hacking. It's also where you'll go on a deep-dive into Networking at several levels of the Open Systems Interconnection (OSI) model.
Here we'll be looking at packets, frames, addresses, sockets, and buffers, and learning to watch for strange traffic and create some mayhem of our own to defend against.

This module ends up giving you a deeper understanding or firewalls, routing, and packet filtering plus a toolbox of ideas to defend computers at the network level.

1.2.2. Interaction for Hacking

In this module we delve deeply into what a computer is, in terms or architecture, memory, processing and other components. We learn to talk to the machine via the command-line - which is an essential skill for real security engineering.

Getting see the computer from the inside, like a hacker, and getting to know the operating system and network through low-level exploration is the mission for this module.

You'll learn about "The Shell", BASH, Unix file-systems and permissions, devices, exploring the processing in real-time and getting out on to the network through a simple terminal window.

1.2.3. Ethical Hacking

We then proceed in "classical order" which is to teach RED team offensive craft first, before showing you how to defend. We like this traditional order so that all students will "know what you're up against".

Ethical Hacking module covers topics on recon, fingerprinting, mapping, exploit discovery and deployment, and the kinds of remote tools used for search, exfiltration, ransoming, maintaining access and pivoting to other systems in the quest to own an entire network and all its assets.

1.2.4. Introduction to Cryptography

There follows a challenging module that gets everyone thinking about games and puzzles in a way that's curious, logical, mathematical, and sometimes counter-intuitive. We talk about deception, camouflage, distraction, and some great battles of history. Thus, we introduce the subject of "Cryptology", which is all about Cryptographic ciphers and code breaking (cryptanalysis)

You will get to know the different types of historical and modern cryptography, and its application areas for data in transit, at rest, and under computation. We'll talk a bit about data leakage, identity, anonymity, signatures, and authentications, (non-)repudiation, keys, and get to see how more complex security devices can be built from more primitive parts and protocols.

1.2.5. Psychology and Social Engineering

Getting deeper into the mindset of the defensive and offensive digital worlds, this module delves into the intricate relationship between psychology and social engineering. We'll explore the human element in security breaches, emphasising how understanding human behaviour is crucial in fortifying digital defences.

Topics covered include Foundations of Social Engineering, defining types of social engineering attacks and the psychological principles behind manipulation and persuasion.

We also present case studies of successful social engineering tactics to explain the relation between cybersecurity and human vulnerabilities. In this module you'll be asked to think about topics on psychological triggers and techniques of influence and obtaining compliance and about decision-making processes when under pressure - so have your wits about you!

1.3. Conclude & Congratulate

Upon concluding the Boudica course, a dedicated session will be held for inquiries and feedback. During this time, attendees will have the opportunity to acquire their digital certificates, optimised for seamless sharing on LinkedIn, with your employers, and other networks.

Additionally, there will be a chance to capture memorable moments through photography.