# **Solent University Unit Descriptor**

## **Unit Code: COM521 Unit title: Ethical Hacking and Penetration Testing**

### **Why is this unit important?**

A security breach can have huge consequences for a company’s ability to function, reputation and causing disruption in the daily lives of millions of people. This is why the demand for security professionals continues to grow. Get on board—and develop an understanding of cybercrime, security principles, technologies, and procedures used to defend networks.

The security threat environment is constantly evolving with new tools and techniques becoming available every day.

### **What you will learn on the unit**

The unit offers an opportunity to develop the blend of understanding and skills required, including specialist technical ethical hacking skills, emphasis is placed on the ethical use of the skills acquired. Successful penetration testing is the discovery of vulnerabilities in computer systems applications and hardware and the ability to exploit them. You will use our state of art virtualised computing lab to perform ethically designed and controlled hacking on realistic systems. You will consider and define the processes for penetration testing. You will develop a technical and analytical skill set and ability to discover vulnerabilities.

### **How you will learn**

The unit will consist of all lab-based practical sessions which will allow you to gain hands-on experience of the unit topics through a series of lab activities. In most weeks, these will be preceded by a 'mini-lecture' to introduce the unit topic and to ensure that you are aware of the background to the topic before beginning the practical exercise. During the lab sessions, we will be on-hand to help you with problems.

You will perform ethical hacking on computer systems in a controlled environment using a simulated and or emulated computing environment. The skills learnt in various exercises will enable you to tackle a more realistic situation where you will perform a more systematic attack with a team.

This will involve following a complete penetration test methodology which consist of a pre-engagement phase, a practical assessment, and post engagement. You will scope the proposal of a test and perform information gathering, exploitation of part of a system, vulnerability and threat analysis and document in the deliverable which is a report.

### **How much time the unit requires**

You will need to attend and engage in 4 hours per week of timetabled practical workshops and tutorials for this unit. You will also need to engage in an additional 12 hours each week of directed and independent learning outside of these sessions in order to work towards proficiency in this subject.

**How you will be assessed**

Tasks which help you to learn and prepares you for summative tasks (Formative):

You should maintain a record of solutions to scenarios based on theoretical preparation and practical exercises. You should show this to your tutor at regular intervals

#### **Tasks which count towards your degree (Summative):**

#### For the first summative assessment, you will take a time constrained assignment consisting of theoretical questions and practical tasks that apply security solutions for a given scenario.

For the second summative assessment you will need to complete a penetration test report for a case study, which you will test and research for vulnerabilities, evaluate the severity of them and document the results.

#### 

#### **When assessment does not go to plan**

#### You will act upon the feedback provided and retake the TCA in a similar method.

You will act on the feedback provided by the tutor and resubmit the pen test report for a case study.

### **What you will be able to do after the unit**

1. Ethically perform hacking techniques to exploit a wide variety of computer systems.
2. Analyse malware & identify its mechanisms for exploitation and concealment.
3. Apply tools and methods for protecting the cybersecurity domain.
4. Communicate outcomes of research and experimentation effectively in writing.

### How this relates to the dimensions of Solent’s Real-world curriculum framework

|  |  |  |
| --- | --- | --- |
| Dimensions | How students learn | How students are assessed |
| Students are challenged to think in critical, creative and applied ways | Students will ethically hack into realistic models of systems and document penetration testing | A penetration test report for a case study |
| Students are inspired to do research through inquiry, curiosity and problem-solving | students collect data from tests and compare to known vulnerabilities | A penetration test report for a case study |
| Students experience an intellectually stimulating curriculum which inspires them to learn for life | students identify and work on authentic problems | students link theory and practice in their hacking challenges post analysis report |

### Summative assessment details

|  |  |  |
| --- | --- | --- |
| AE1 | Weighting: | 50% |
|  | Assessment type: | TCA |
|  | Aggregation: | Aggregated to AE2 |
|  | Length/duration: | 90min |
|  | Online submission: | Yes |
|  | Grade marking: | Yes |
|  | Anonymous marking: | Yes |

|  |  |  |
| --- | --- | --- |
| AE2 | Weighting: | 50% |
|  | Assessment type: | Report |
|  | Aggregation: | Aggregated to AE1 |
|  | Length/duration: | Maximum 3000 words |
|  | Online submission: | Yes |
|  | Grade marking: | Yes |
|  | Anonymous marking: | Yes |

### Unit Author:

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Title: Ethical Hacking and Pen Testing | | | |
| Credit Points: | 20 | Unit Code: | COM521 |
| FHEQ Level: | 5 | School/Service | SMAT |
| Unit Delivery Model: | CD | Max/Min student numbers | 25 |
| Unit Leader: | Warren Earle | | |
| HECOS code | 100376, 100365 | | |

### Unit change history:

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Approved/Year Implemented/Code | July 2019 | 2020/21 | COM521 |
| Unit modified/Year Implemented/Code |  |  |  |
| Add extra rows as required |  |  |  |