

PROJECT PLAN PROPOSAL	مقترح خطة مشروع
1) Project title VLAB	1) عنوان المشروع VLAB
2) Student(s) Name(s) and Major 1- Khalid Al-Shahri (Managing cloud infrastructure on Azure using Terraform, setting up Docker containers for running applications, supervising task execution, and coordinating the team). 2- Shabeb Al-Dosary (Supporting the setup of virtual networks and devices on Azure, managing storage and security permissions). 3- Naif Al-Marshad (Setting up and running vulnerable applications in Docker, testing the virtual environment, and ensuring the tools are ready for use).	2) اسم المتدربين والتخصص 1. خالد الشهري (إدارة البنية التحتية السحابية على Azure باستخدام Terraform وإعداد حاويات Docker لتشغيل التطبيقات ، والإشراف على تنفيذ المهام والتنسيق بين الفريق) 2. شبيب الدوسري (دعم إعداد الشبكات الافتراضية والأجهزة في Azure وإدارة التخزين والأذونات الأمنية) 3. نايف المرشد (إعداد وتشغيل التطبيقات المجيزة لاختبار الثغرات في Docker واختبار البيئة الافتراضية وضمان جاهزية الأدوات للاستخدام).
3) Supervisor Dr. Khaled Al-Yousifi – Dr. Ahmed Al-khalifa	3) المشرف الدكتور/ خالد اليوسفي - الدكتور/ أحمد الخليفة
4) Background and motivation of the project (Project Problem) - Students face challenges running ethical hacking environments on their personal devices due to limited hardware specifications. - Automating the lab setup provides a stable environment that students can access without complex configurations. Using Docker enhances resource management efficiency and reduces the time required to set up applications.	4) خلفية ومحفزات المشروع (مشكلة المشروع) - الطلاب يواجهون مشاكل في تشغيل بيئات الاختراق الأخلاقي على أجهزتهم الشخصية نظرًا لمواصفات الأجهزة المحدودة. - تمته بناء اللاب توفر بيئة مستقرة يمكن للطلاب الوصول إليها دون الحاجة إلى إعدادات معقدة. - استخدام Docker لتحسين كفاءة إدارة الموارد واختصار الوقت اللازم لإعداد التطبيقات.
5) Objectives of the project - Automating the lab-building process using Terraform and Docker to simplify the setup of a ready-made environment for penetration testing. - Providing a cloud-based virtual environment that allows students to use tools without technical complications. - Reducing the time and effort required to set up training environments.	5) أهداف المشروع - أتمته عملية بناء اللاب باستخدام Terraform و Docker لتسهيل إعداد بيئة جاهزة لاختبار الاختراق. - توفير بيئة افتراضية سحابية تتيح للطلاب استخدام الأدوات دون تعقيدات تقنية. - تقليل الوقت والجهد اللازم لإعداد بيئات التدريب.

<p>6) Expected results of the project (Final Product)</p>	<p>6) النتائج المتوقعة للمشروع (المنتج النهائي)</p>
<ul style="list-style-type: none"> <li>- A ready-made environment containing multiple vulnerable applications like Juice Shop and Metasploitable, running in Docker containers.</li> <li>- Complete automation of the lab setup process to avoid any technical issues for students, ensuring easy access through the cloud.</li> </ul>	<ul style="list-style-type: none"> <li>- بيئة جاهزة تحتوى على عدة تطبيقات ضعيفة مثل (Juice Shop - metasploitable) تعمل في حاويات Docker.</li> <li>- أتمتة كاملة لعملية إعداد المختبر لتجنب أي مشاكل تقنية للطلاب مع الوصول السهل عبر السحابة.</li> </ul>
<p>7) Prerequisites</p>	<p>7) متطلبات المشروع</p>
<p>By utilizing the university's Microsoft Azure account, where \$100 is added to the account, and services are available for 12 months.</p>	<p>بالإستفادة من حساب الجامعة في Microsoft Azure حيث يتم اضافة \$100 في حساب الطالب وتكون الخدمات متاحة لمدة 12 شهر</p>
<p>Hardware</p>	<p>متطلبات مادية وعتاد</p>
<ul style="list-style-type: none"> <li>- Microsoft Azure account to provide the required cloud resources.</li> <li>- Azure Virtual Machines (VMs)</li> <li>- Virtual Network (VNet)</li> <li>- Setting up firewall and security tools</li> </ul>	<ul style="list-style-type: none"> <li>- حساب Microsoft Azure لتوفير الموارد السحابية المطلوبة.</li> <li>- أجهزة Azure الافتراضية (VMs)</li> <li>- الشبكة الافتراضية (VNet)</li> <li>- إعداد جدار الحماية وأدوات الأمان</li> </ul>
<p>Software</p>	<p>متطلبات برمجية</p>
<ul style="list-style-type: none"> <li>- Using Terraform to automate the creation of virtual machines and cloud networks through code.</li> <li>- Using Docker to run vulnerable applications in isolated containers.</li> </ul>	<ul style="list-style-type: none"> <li>- استخدام أداة Terraform لأتمتة إنشاء الأجهزة الافتراضية والشبكات السحابية باستخدام كود</li> <li>- استخدام Docker لتشغيل التطبيقات الضعيفة في حاويات معزولة</li> </ul>
<p>8) References</p>	<p>8) المراجع</p>
<p><a href="https://azure.microsoft.com/en-us">https://azure.microsoft.com/en-us</a> <a href="https://terraform.io/">https://terraform.io/</a> <a href="https://www.docker.com/">https://www.docker.com/</a></p>	<p><a href="https://azure.microsoft.com/en-us">https://azure.microsoft.com/en-us</a> <a href="https://terraform.io/">https://terraform.io/</a> <a href="https://www.docker.com/">https://www.docker.com/</a></p>
<p>9) Additional Information</p>	<p>9) معلومات إضافية</p>
<p>Target audience: Students and learners.</p>	<p>الفئة المستهدفة : الطلاب والمتعلمين.</p>