

# Test Project

## *Cyber Security*

Module B - Enterprise Infrastructure Security

Submitted by:  
Keysight Technologies, Inc.

# Contents

Introduction .....	3
Description of project and tasks .....	3
Instructions to the Competitor .....	4
Project Tasks (Practical).....	7
Description of project and tasks .....	7
Task 1 Incident Response.....	8
Task 2 Vulnerability Detection and Repair.....	8
Task 3 Digital Forensic Investigation .....	9
Task 4 Cryptography .....	9
Task 5 IAM .....	10
Task 6 Code Review .....	10
CODE REVIEW – Python Coding .....	11
Project Tasks (Theoretical).....	15

# Introduction

Cyber security knowledge is becoming essential nowadays for people who want to build a successful career in any IT field. This Test Pct contains a lot of challenges from real life experience, primarily IT integration and IT outsourcing. If you can complete this project with the high score, you are ready to adopt enterprise security policies to the infrastructure for any multi-branch enterprise.

## Description of project and tasks

This Test Project is designed using a variety of system and network technologies with which you should be familiar includes CentOS, WebServer, Apache, MySQL, WIN OS, Linux, Wireshark, Access Control, SAML, Oauth, PHP, TLS, PKI, Open SSL, File Structure and DB – mysql, Windows, and Coding Basics – Python. Tasks are broken down into the following sections:

- Vulnerability Detection and Repair
- Incident Response
- Identity and Access Management
- Digital Forensic Investigation
- Cryptography and PKI
- Code Review

You are required to apply requested set of security hardening and policies tuning to the multi-branch enterprise with existing infrastructure. All services are functional, but security of these services is left off board. Some security aspects are very straightforward while some may leave room for different implementation options. Implement all requirements to the best of your ability, in line with industry best practices within the limitations imposed by the equipment.

## Instructions to the Competitor

1. Read all tasks in each section before proceeding with any configuration. The completion of any item may require the completion of any previous or later tasks.
2. Before starting the test project, confirm that all devices in your topology are in working order. During the test project, if any device is locked, misconfigured or inaccessible for any reason, you must recover it to the required state.
3. Knowledge of implementation and troubleshooting techniques is part of the skills being tested in the configuration section of the Test Project.
4. Test the functionality of all the requirements before you submit the documentation for the test project. Be careful, because as you configure one part, you may break a previous requirement or configuration. Points are only awarded for the implemented tasks.
5. Whenever you are required to configure a password, use password P@ssw0rd1! if otherwise is not stated.
6. All virtual machines are pre-installed. Credentials information given in the project will allow logon. Do not change these passwords
7. At end of day you will be required to submit the answer sheet, excel file with the answers to the theoretical questions, and the

### Equipment basic configuration

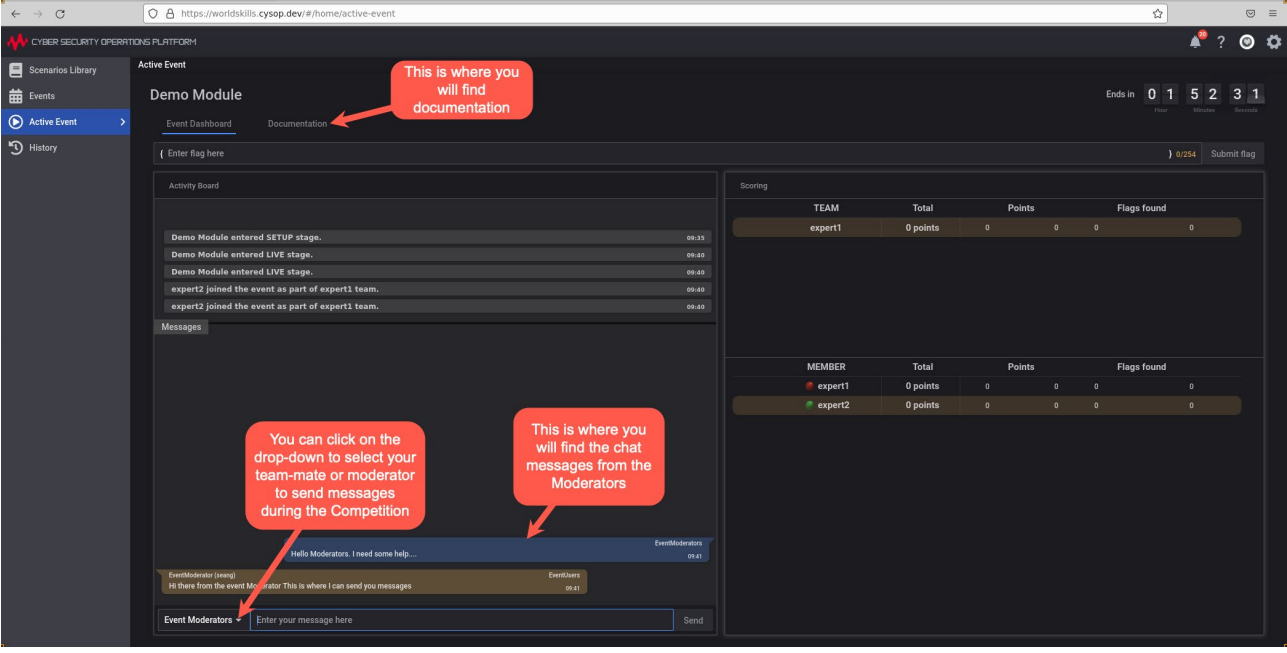
1. Hostnames for all devices and virtual machines are preconfigured according to the topology diagrams.
2. Virtual and physical switching is preconfigured according to the topology diagrams. VLAN numbers on physical switches are used in accordance with port-groups configuration (if any).
3. IP subnets are preconfigured according to the topology diagrams. For each subnet the gateway device assigned with the last IP address in this subnet and the client device assigned with the first IP address in this subnet.
4. Default routing is preconfigured.

## Connection Table

SYSTEM ACCESS	NOTES
<a href="https://worldskills.cysop.dev">https://worldskills.cysop.dev</a>	Keysight Cyber Security Operations Platform
<a href="https://evidence.cysop.dev">https://evidence.cysop.dev</a>	Evidence portal for uploading supporting configuration and evidence.

## Accessing the Environment

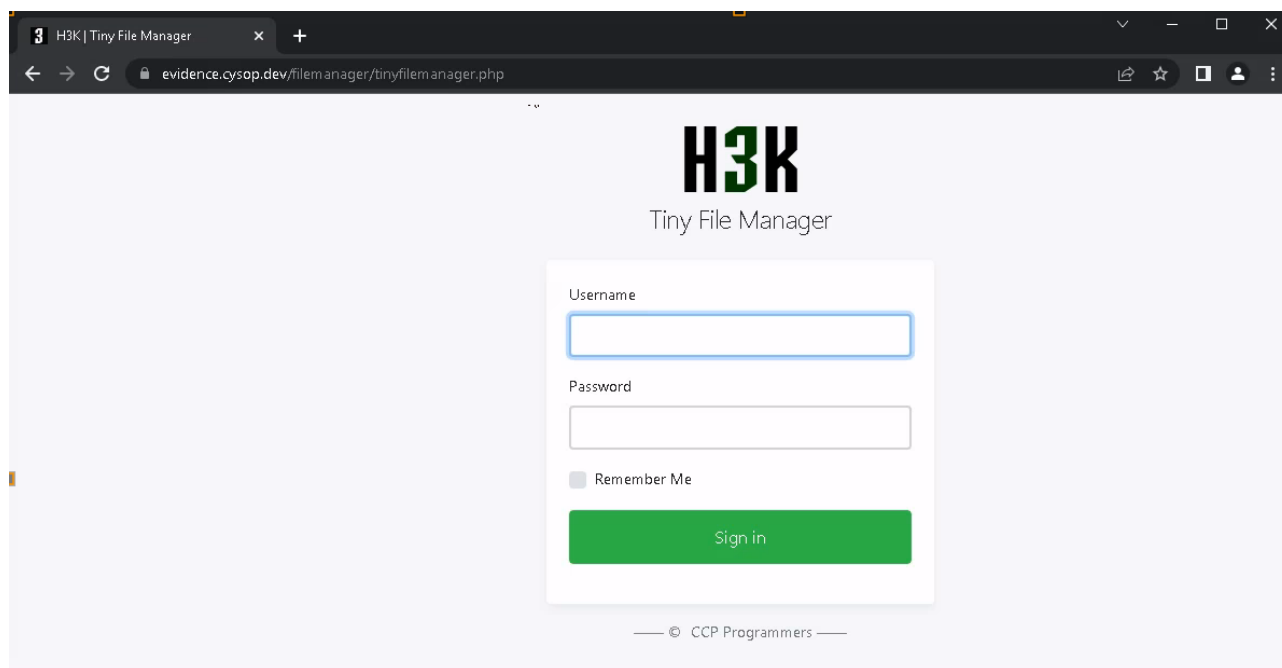
Open a web browser and connect to the Keysight Cyber Security Operations Platform mentioned in the Connection Table and login with the credentials provided to you. After a successful log in, you will be presented with a screen similar to the below screenshot:



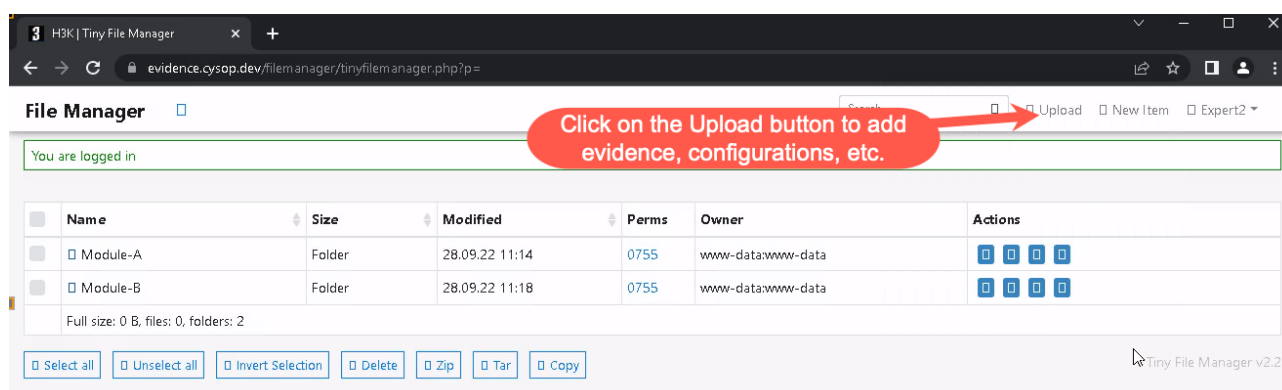
The screenshot displays the Keysight Cyber Security Operations Platform interface. The sidebar on the left contains 'Scenarios Library', 'Events', 'Active Event', and 'History'. The main content area is titled 'Active Event' and 'Demo Module'. It features an 'Event Dashboard' and a 'Documentation' tab, with a red callout indicating that documentation is found here. Below the dashboard is an 'Activity Board' showing event logs. A red callout points to a dropdown menu in the 'Messages' section, stating that it is used to select team-mates or moderators for sending messages during the competition. Another red callout points to the 'Event Moderators' section, indicating where chat messages from moderators are found. On the right side, there is a 'Scoring' section with two tables: 'TEAM' and 'MEMBER', both showing 'Total', 'Points', and 'Flags found' for 'expert1' and 'expert2'.

Once you have logged in, you will be able to access the Infrastructure that you are to use to manage the challenges.

To upload evidence into the evidence portal, connect to evidence portal mentioned in the Connection Table and login with the credentials provided to you.



After a successful log in, you will be presented with a screen similar to the below screenshot:



For Module B, all systems can be managed from Competitor 1 or Competitor 2. These infrastructure elements are duplicates of each other with different IP addresses and therefore both participants can perform tasks independently, should they so choose. To access Competitor 1 or Competitor 2, use RDP to connect to 100.100.128.50 or 100.100.128.40 with the credentials from the table below. In this module it is possible to directly access the other infrastructure elements which form part of the challenges, either using your workstation directly or via the RDP session of Competitor 1 or Competitor 2.

The credentials relevant to the test topology for Module-B can be found below:

MACHINE	MANAGEMENT LAN IP ADDRESS	TOPOLOGY IP ADDRESSES	ACCESS METHOD	USER ID / PASSWORD
Competitor 1	100.100.128.50	100.100.128.50	RDP	Competitor/Competitor
Competitor 2	100.100.128.40	100.100.128.40	RDP	Competitor/Competitor
Compromised Web Server	100.100.128.60	100.100.128.60	SSH	root/lxia!123
Compromised Windows Server	100.100.128.70	100.100.128.70	RDP	jboss/lxia!123

Module-B consists of two project parts. The first one is Practical and the second one is Theoretical. We will begin the Practical tasks in the morning, and may continue to work on them all day as required. The second is Theoretical and will involve test questions and coding challenges and these will be released after lunch time.

## Project Tasks (Practical)

### Description of project and tasks

You are part of Network Security Technical Support team for Group A. The Webserver, which is hosted by Group A, was hacked in October 2019. Your team has been called to help Group A for investigation and to trace the source of this cyber-attack. Analyze the attack methods of the hackers, find the vulnerabilities in the system, submit an incident response report for cyber security incidents (report template available in the end of this Test Project); Repair the vulnerabilities in the system, delete the backdoor dropped by the hacker in the system, and restore the system to its normal operation. It has also come to your attention that a network capture that was taken during the attack is present on the system.

The base CentOS 7 has been set up on Web Server, apache+mysql and wordpress web system has been installed; Windows Server 2012 OS has been set up on the Windows Server; Competitor machines are available on Windows 10 with Flare Tools installed as well as kali under WSL. These are identified as Competitor 1 and 2.

Answers to all questions are to be submitted in the Answer form and submitted to the evidence portal once completed.

# Task 1 Incident Response

## Work Task Incident Analysis:

### Web Server

The webserver has been exploited. Artifacts have been left on the server, which include logs and possibly a network capture.

Incident Analysis.

- Find and submit the exploit types, associated exploit URL, commands and the parameters that were used in the attacks.  
e.g. csrf: `http://ip/reset_password?user=abcd&pwd=1234`
- Submit the date and time that the hacker first successfully executed an attack command.
- Find and submit the filename and absolute path of the infected file in the web server which was used in the attack.
- Find and submit the webshell code that was used in the attack.
- Find and submit the first command that was run after the reverse-shell connection was built.
- Find and submit the username and password that the hacker used to log into the server and document all of the related actions.
- Find and submit the request URL that the hacker used for downloading files.

### Windows Server

- Find and submit the **filename and absolute path** of the malicious autorun program.
- Find and submit the **string used to create** the **mutex** for the malicious autorun program.
- Find and submit the **registry key value** that the malicious program writes as well as the file **name** that the malicious program creates.
- Find and submit the **process name and parameters** that malicious program is using.
- List the names of the registry functions that are used in this malicious executable.

# Task 2 Vulnerability Detection and Repair

## Work Task System Recovery: Web Server

During your analysis of the incident, on the Web Server, you should note the distinct issues with the web server software. Fix the bugs you found during the first task on the Web Server and provide the before/after testing result on the answer sheet. Please provide the response as well as supporting screenshots where applicable. Upload all evidence into the File share / evidence portal provided.



## Task 3 Digital Forensic Investigation

### Work Task Analysis (dump.vmem)

Analyze the memory dump and answer the questions. Providing evidence for each question, including the commands that were run as well as the relevant output (Remove any output that is not necessary to the finding). Upload all evidence into the File share / evidence portal provided.

- What is the name of the malicious program that was running?
- What is the PID and PPID of the malicious program?
- What IP addresses were attempted for connection by this malicious program and on which destination port?
- Which user executed the malicious program?
- What is the name of the other malicious program that needs to be deleted along with the main malicious program to completely clean all malicious programs from this dump file?

### Work Task Analysis (creditcard.pcap)

Three credit card details have been stolen from an Enterprise network to a Malicious Command and Control Server on the Internet. The Cyber Security Operations Centre (CSOC) team has managed to block this confidential information using their properly configured DLP system. The head of the CSOC team has found that the credit card information was being transferred over the network and the CSOC team was able to capture the outgoing traffic in multiple packet captures. The CSOC head wants the 3-credit card details to be extracted out so that these three credit cards can be blocked for further use by the company. Help the CSOC team find this confidential data at the earliest before the malicious actor could siphon out money from the credit card accounts.

The captures may be found on the Competitor 1 and Competitor 2 workstations on the desktop in a folder marked Task 3.

## Task 4 Cryptography

### Work Task Installation (Web Server)

Since the compromise of the Web Server, the team has determined that to secure the transmitted traffic over the network, the web server configuration must be changed to enforce transmission encrypted with TLS. The decision was taken to make the key very strong (4k bits), and as a temporary measure it should be set up as a self-signed certificate as a proof of concept.

Perform the following tasks and be sure to include the commands issued to create the certificate. Also make sure to upload the certificate and key into the evidence portal.

Upload all evidence into the File share / evidence portal provided.

- Create a self-signed 4K RSA certificate for the webserver. Set this certificate up so that the Server Name Indicator will respond correctly to a URI including the IP address of the host.
- Modify the configuration files of the webserver to answer on http as well as https.
- Ensure that any access via http is redirected to the https URL.

## Task 5 IAM

### Work Task Configuration (Web Server)

It was further decided that the security controls on the Web Server are not sufficient, and an audit finding found that it was possible to log into the web server remotely using the superuser account.

Please perform the following changes on the Web Server related to Identity and Access Management.

Upload all evidence into the File share / evidence portal provided.

- Make sure that the Webserver does not allow the root user to SSH directly into the server. Detail which configuration changes have been made to which configuration files.
- Change the root password to a secure password and detail the commands used to do this.
- Allow the ixia user to change to root, without needing to know the root password, and instead to use their own password.

## Task 6 Code Review

### Work Task Code Review

As a senior software developer, code security is of utmost importance to you. It is part of your daily job to review codes developed by junior programmers. This is to ensure that the codes developed have no vulnerabilities. It is a daunting task at times because most of the codes are syntactically and semantically correct. You have to rely on your eye power and experiences to get you through. The code snippets are included below. For each one of these please answer the following questions.

- Identify the vulnerable line of code that poses a security threat.
- Describe why it's not safe.
- Explain how one can make the code secure.
- Modify the code (or lines of code) to make the code to guard against the vulnerability.

Note: Observe and apply all safety rules and precautions

# CODE REVIEW – Python Coding

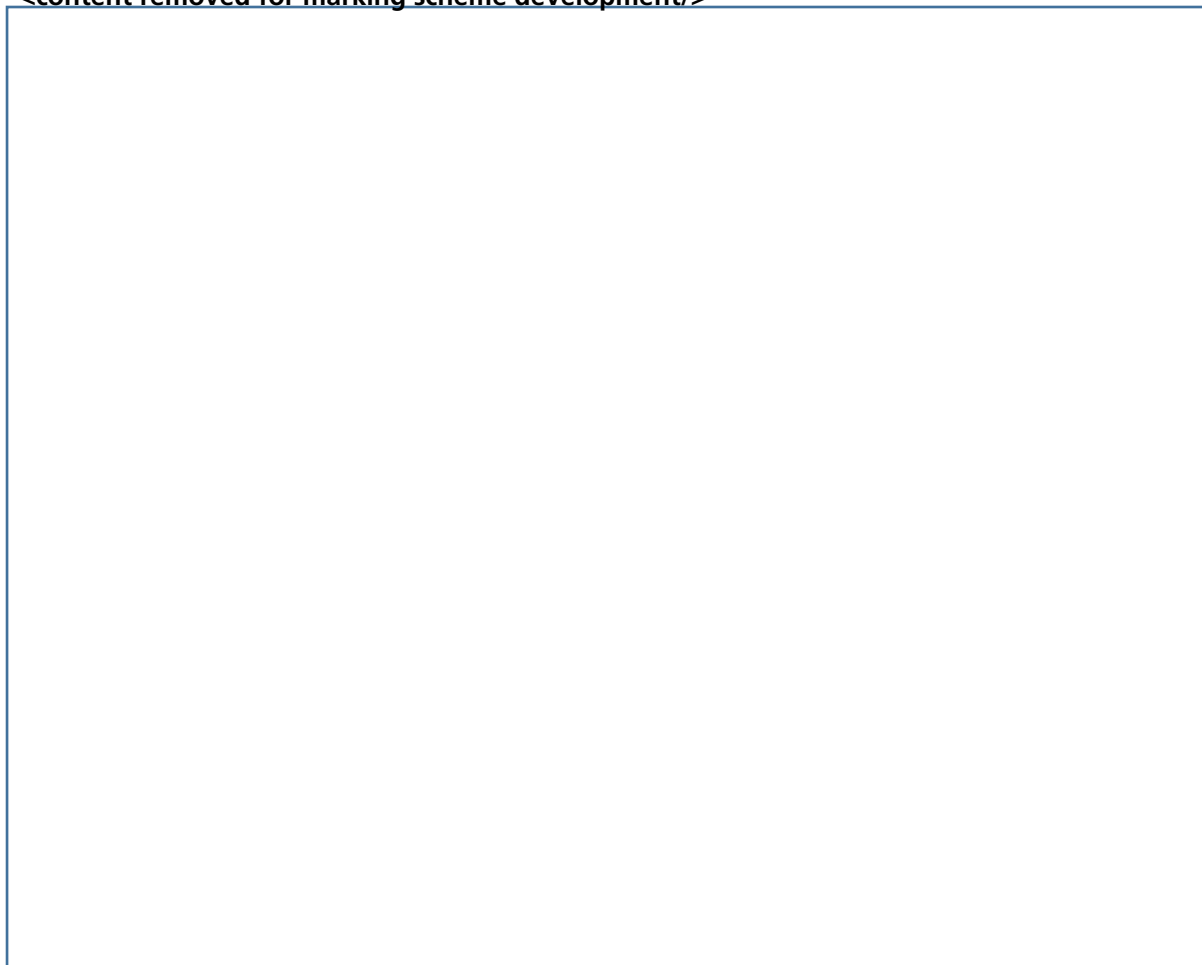
## Code Snippets

### Code 1

**<content removed for marking scheme development,  
will be distributed after lunch/>**

## Code 2

<content removed for marking scheme development/>



### Code 3

<content removed for marking scheme development/>



#### Code 4

<content removed for marking scheme development/>



# Project Tasks (Theoretical)

content removed for Marking Scheme development/