

Test Project

Cyber Security

Module D - Blue Flags

Submitted by:
Keysight Technologies, Inc.

Contents

Introduction.....	3
Description of project and tasks.....	3
Instructions to the Competitor.....	3
Infrastructure Configuration.....	4
Connection Table	4
Accessing the Environment	4

Introduction

Cyber security knowledge is becoming essential nowadays for people who want to build a successful career in any IT field. This test project 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 in the format of a Capture the Flag (CTF) event. Capture the Flag is one of, if not **THE** best way to get started in Cyber Security.

This test project is designed to test skills covering topics such as Database, enumeration, Privilege Escalation, web-based attacks and windows-based attacks. You are expected to use a variety of tools and have knowledge of various topics such as Kali Linux, Linux Vulnerabilities, Operating Systems, web servers and windows vulnerabilities.

You are required to apply your knowledge of BLUE Teaming, Tactics and Procedures (TTPs) in order to obtain flags hidden around the infrastructure. These **flags can be identified** as they use the format:

icc{ f1affb23ae939eb525b232001698fbca}

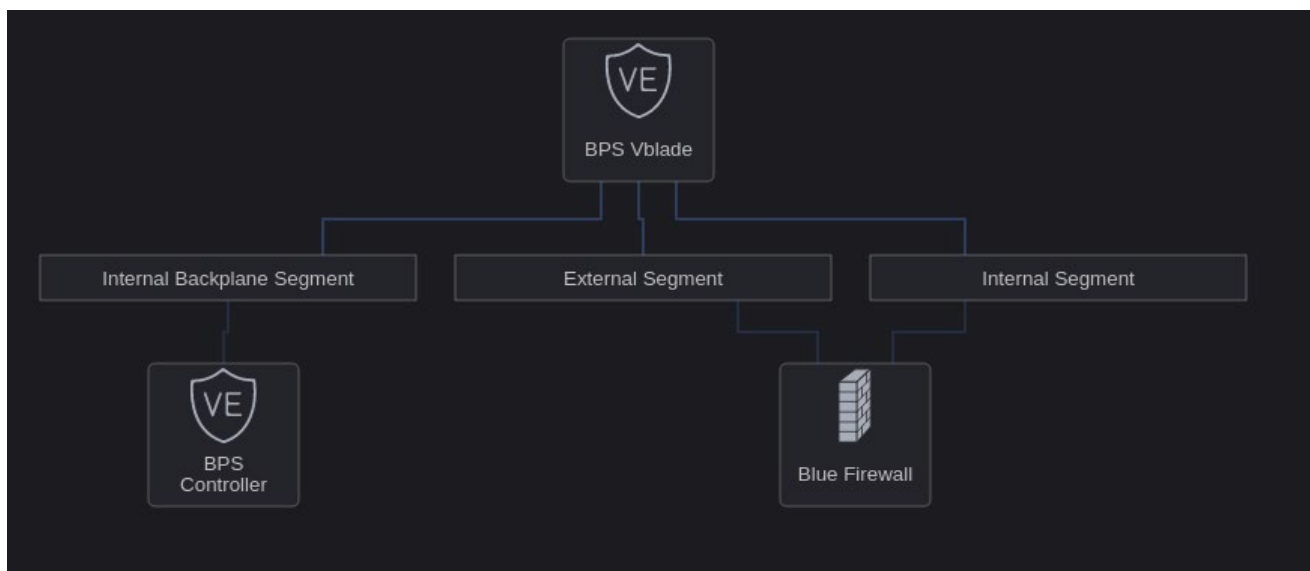
These flags may be obfuscated in various ways and may require decoding.

Instructions to the Competitor

1. Login to the Keysight Cyber Security Operations Platform (CySOP) as described in the section "Accessing the Environment" below.
2. Submitting flags will get you points. Flags values should be submitted into the Keysight Cyber Security Operations Platform (CySOP) omitting the icc{} identifier. This is described in the section "Accessing the Environment" below.
3. Dummy flags may exist to confuse participants. If the scoring system does not accept the flag value, it is either already submitted or is invalid.
4. Flag scores may not be of equal value.
5. Participants have to find flags by inspecting the traffic flowing through the inside and outside interfaces of the Firewall.
6. Communication within a team as well as communication to the moderators can be achieved using Keysight Cyber Security Operation Platform (CySOP). Inter-team communication is not supported.
7. Be respectful when communicating with moderators using the platform. However, make use of this facility to report any issues that you may encounter to the moderators.
8. Intentionally bringing down, crashing and or denying of service for any other team will result in penalty or disqualification
9. Intentionally bringing down and or crashing the Keysight Cyber Security Operation Platform (CySOP) or any system on the management network (100.100.0.0/16) will result in disqualification of your team.
10. Intentionally scanning or attempting to exploit the Keysight Cyber Security Operation Platform (CySOP) for gaining points will result in penalty or disqualification.
11. Sharing or disclosing flag values, hints, or information about the challenges in the event to other teams or personnel outside of the event will result in penalty or disqualification.

Infrastructure Configuration

The infrastructure layout for Module-D contains Keysight Breaking Point System which is a traffic generator injecting benign as well as malicious traffic across the network. This traffic may contain flags or clues to find flags.

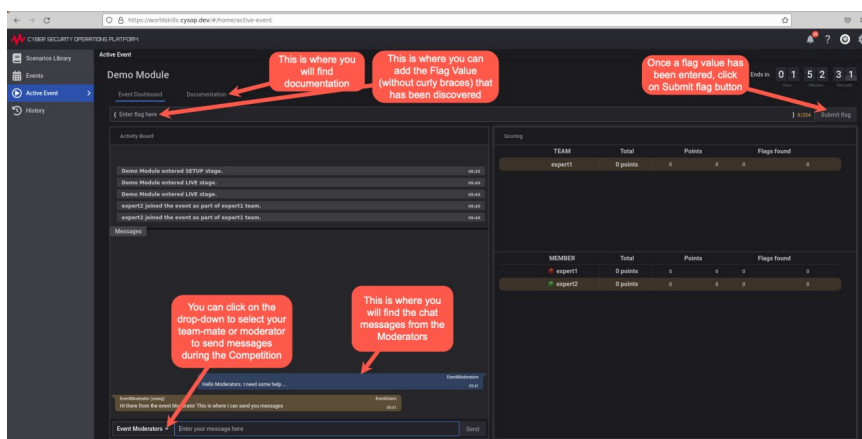


Connection Table

System Access	Notes
https://worldskills.cysop.dev	Keysight Cyber Security Operations Platform

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:



Once you have logged in, you will be able to access the Infrastructure that you are to use to manage the challenges. The systems used to access the Module-C environment can be found in the table below:

Machine	Management LAN IP address	Access Method	User ID / Password
FlareVM1	100.100.128.50	RDP	competitor/competitor
FlareVM2	100.100.128.40	RDP	competitor/competitor
Palo-Alto Firewall	100.100.128.10	HTTPS	admin/P@ssw0rd@123
Splunk SIEM	100.100.128.20	HTTPS	admin/lxia!123

To upload flags into the Keysight Cyber Security Operation Platform (CySOP), enter the flag value omitting the **icc{}** identifier and click the “**submit flag**” button as indicated in the diagram above.

For Module-D, all attacks are to be performed from either FlareVM1 or FlareVM2. To access these systems, use RDP using the credentials from the table above. FlareVM1 and FlareVM2 are functionally identical, and both are connected to the network which contains the flags. In addition, the Palo-Alto Firewall and Splunk SIEM can be directly accessed from your workstation environment.

A number of services seen in the traffic flowing through the Firewall may be found behind a Port Address Translation. Some service mappings present inside the infrastructure of BLUE Team are as mentioned below:

External IP	Internal IP	PORT	Service
60.1.10.80	100.100.128.3	1080	Php/nginx
60.1.10.81	100.100.128.3	1081	apache
60.1.10.82	100.100.128.3	1082	Php/nginx
60.1.10.83	100.100.128.3	1083	Php/nginx
60.1.10.84	100.100.128.3	1084	Php/nginx
60.1.10.85	100.100.128.3	1085	Php/nginx
60.1.10.86	100.100.128.3	1086	django