## **Unit README: Red Vs. Blue Team Project**

### **Unit Description**

In the second project week, you will work on a Red Team vs. Blue Team scenario in which you will play the role of both pentester and SOC analyst.

As the Red Team, you will attack a vulnerable VM within your environment, ultimately gaining root access to the machine. As Blue Team, you will use Kibana to review logs taken during their Day 1 engagement. You'll use the logs to extract hard data and visualizations for their report.

Then, you will interpret your log data to suggest mitigation measures for each exploit that you've successfully performed.

### **Unit Objectives**

Click here to view the daily unit objectives.

This week's project will prompt you to apply knowledge of the following skills and tools:

* Penetration testing with Kali Linux.
* Log and incident analysis with Kibana.
* System hardening and configuration.
* Reporting, documentation, and communication.

### **Lab Environment**

Click here to view the lab environnement.

In this unit, you will be using the Red vs Blue lab environment located in Windows Azure Lab Services. RDP into the Windows RDP host machine using the following credentials:

Username: azadmin Password: p4ssw0rd\*

Open the Hyper-V Manager to access the nested machines:

* **ELK machine credentials:** The same ELK setup that you created in Project 1. It holds the Kibana dashboards.  
  + Username: vagrant
  + Password: vagrant
  + IP Address: 192.168.1.100
* **Kali:** A standard Kali Linux machine for use in the penetration test on Day 1.  
  + Username: root
  + Password: toor
  + IP Address: 192.168.1.90
* **Capstone:** Filebeat and Metricbeat are installed and will forward logs to the ELK machine.  
  + IP Address: 192.168.1.105
  + Please note that this VM is in the network solely for the purpose of testing alerts.

**Next Week's Lab Environment**: At the end of 20.3, we will set up a new Azure Lab Environment for the Forensics unit.

### **What to Be Aware Of:**

* Throughout Day 2, it is important that you take screen shots of each step they complete. These screen shots will be used in their Day 3 Report.

### **Security+ Domains**

This unit covers portions of the following domains on the Security+ exam:

* 1.0 Attacks, Threats, and Vulnerabilities
* 2.0 Architecture and Design
* 3.0 Implementation
* 4.0 Operations and Incident Response

For more information about these Security+ domains, refer to the following resource: [Security+ Exam Objectives](https://comptiacdn.azureedge.net/webcontent/docs/default-source/exam-objectives/comptia-security-sy0-601-exam-objectives-(2-0).pdf?sfvrsn=8c5889ff_2)

### **Additional Reading and Resources**

Click here to view additional reading materials and resources.

Day 1:

* [Red Team Vs Blue Team](https://securitytrails.com/blog/cybersecurity-red-blue-team)
* [What is Vulnerability Scanning](https://www.esecurityplanet.com/network-security/vulnerability-scanning.html)
* [What is a reverse shell](https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/)

Day 2:

* [Kibana: Discover Documentation](https://www.elastic.co/guide/en/kibana/7.7/discover.html)
* [Kibana: Visualize Documentation](https://www.elastic.co/guide/en/kibana/7.7/visualize.html)
* [Elasticsearch Reference Documentation](https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html)

### **Looking Forward**

In the next week, we will cover the specialized field of digital forensics. We will cover a new set of skills and tools that allow us to analyze evidence on digital technology after an security incident or crime occurs.