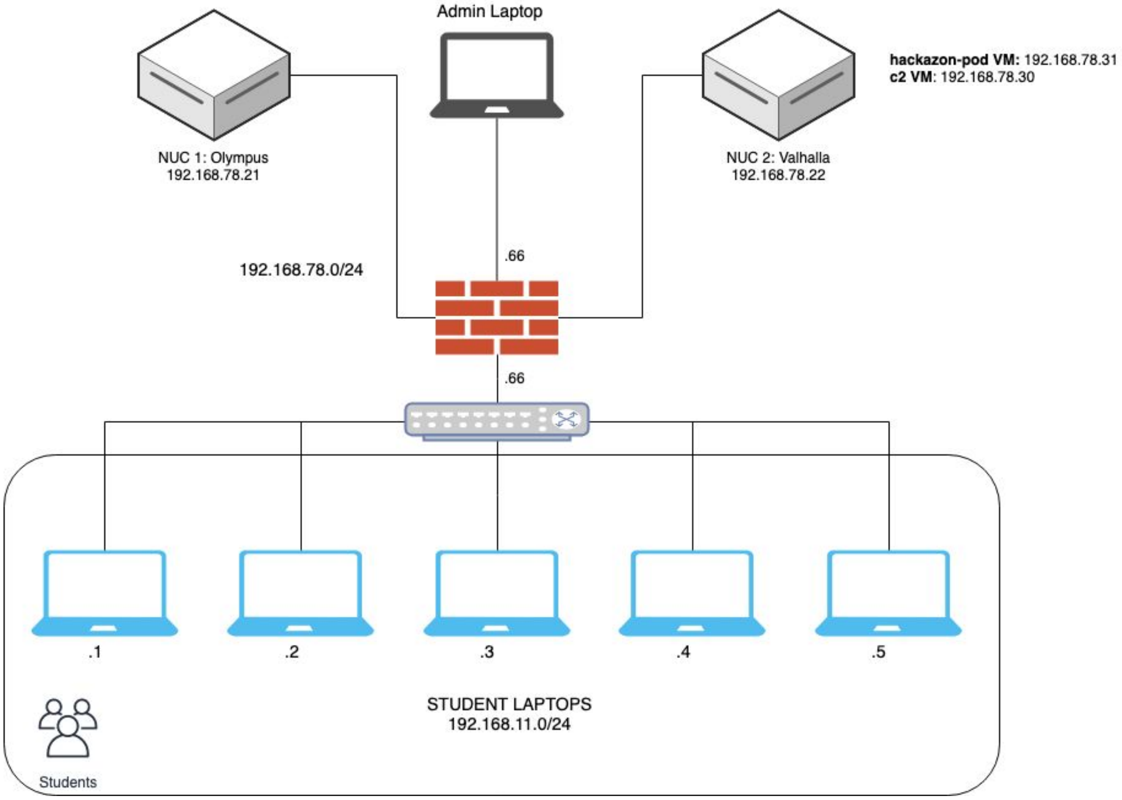
DEF CON 27 Red Team Offense Village WebApps Station Details

Station Lead: Omar Ωr Santos
Backup Leads: Ron Taylor & Joseph Mlodzianowski

Topology



NUC 1

There are two Intel NUCs. NUC 1 (Olympus) is running Ubuntu Server, Ansible, and Docker. There are 5 different containers (one for each pod) running *Juice-Shop*.

All containers can be reset using the *pod reset tool*. Details about the *pod reset tool* are included under the **Pod Reset** section of this document.

NUC 2

NUC 2 (Valhalla) is running Proxmox, and 2 VMs, Containers, and Ansible:

- **C2 VM** - where the ansible scripts are
- **Hackazon-pod VM** - with 5 containers running Hackazon

★ Contact Omar if you experience any problems with the underlying VM / container infrastructure.

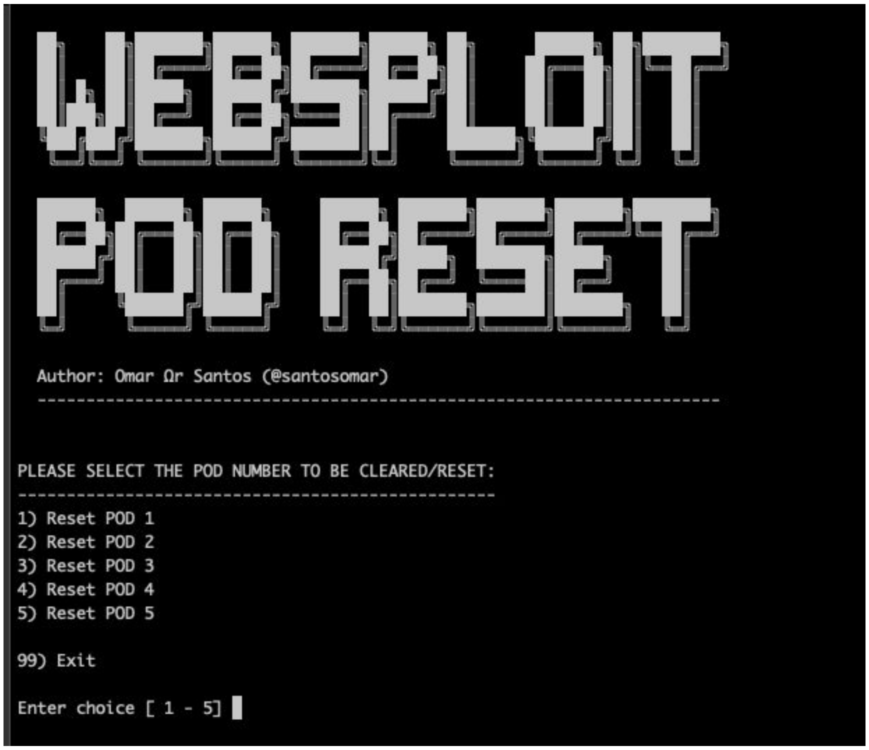
★ All pods are reset with the **pod reset tool** and there is technically no need to login to any of the VMs or containers.

Web Station Admin Laptop

The laptop is used to login to the Command and Control (C2) VM in NUC 2. On the other hand, the laptop should already be connected and the pod reset tool runs all the time. If for some reason it disconnects, the credentials are: **red/redteam!!**

Pod Reset Tool

Resetting each pod is extremely easy! You just enter the pod number, then Ansible and other scripts take care of the rest. The following is a screenshot of the pod reset tool (runs on the C2).



```
  Author: Omar Ωr Santos (@santosomar)
  -------------------------------------------------------------------


PLEASE SELECT THE POD NUMBER TO BE CLEARED/RESET:
-----------------------------------------------
1) Reset POD 1
2) Reset POD 2
3) Reset POD 3
4) Reset POD 4
5) Reset POD 5

99) Exit

Enter choice [ 1 - 5] █
```

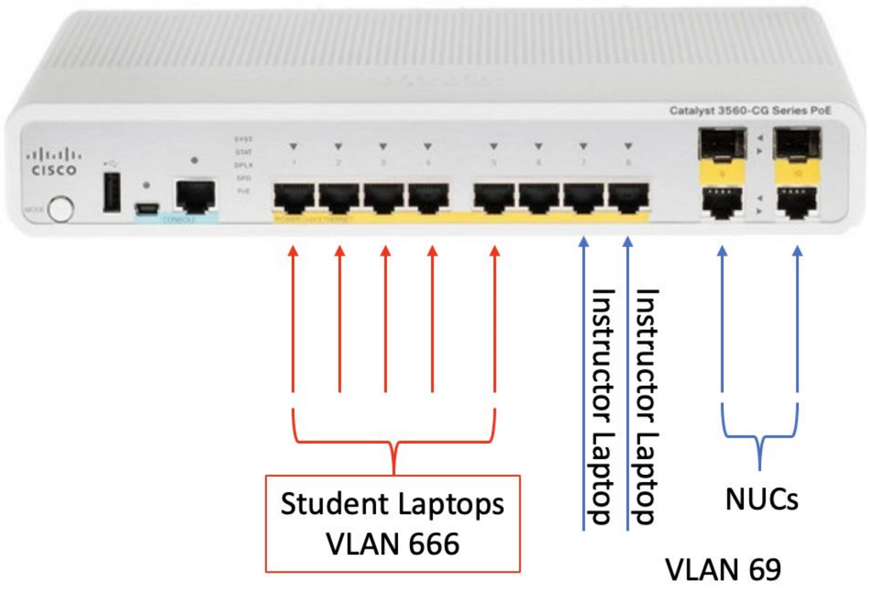
From there you can execute the pod reset scripts.

Student Laptops and Material

All student laptops are running Kali Linux. The lab guide has been posted to their desktop. The exercises should take them ~30 minutes to complete. After the student/participant completes the exercises, please give them a card that include instructions on how they can download additional material and practice in their own time. Each laptop should only have access to their respective pod.

Switch

The following is the switch port configuration. There should be no need to console or connect to the switch. If you run into any problems, please contact Omar for assistance.


Catalyst 3560-CG Series PoE
CISCO
CONSOLE
Student Laptops
VLAN 666
Instructor Laptop
Instructor Laptop
NUCs
VLAN 69