# CYBR-10025 – Lab 1: Hacking the Reavers

# Objective(s):

Gain the highest level of access you can on a fan site for The Reavers.

# Introduction:

The Reavers are a local sports team with a dedicated fan base. They have their own homegrown web forum that they use to communicate with anyone interested in the team or if they just want to connect to other Reavers fans. A few months ago, a moderator was fired and since then the site operators believe that there have been people getting high-level access to the site.

# Apparatus

* VirtualBox https://www.virtualbox.org/wiki/Downloads
* reavers.ova from Canvas.
* candidate\_passwords.zip from Canvas

# Procedure

1. Import the reavers.ova
2. ***Start the reavers VM***
3. ***Note the server IP address on the boot screen (likely 192.168.99.101)***
4. ***Point your web browser at: http://<<your server ip>>/reaver\_board***
5. ***When you reach the highest level of access. Take a screenshot (make sure it contains the “level” at the bottom of the page).***

# What To Hand In

* A MS Word file containing:
  + A written step-by-step log of the different things you investigated, information you gathered and what techniques you tried. Doing well on this assignment depends on writing clear instructions on how to gain high level access. If the person marking can’t repeat your steps and get the same effect this will cost you marks.
  + Screenshot from your browser showing the highest level of access you achieved.

# Rules

1. You may not use an automated tool like Nessus.
2. You may not use a local attack: That is an attack that would require you to be in the same room as the Linux machine if the web application was running on a physical machine instead of a VM. All attacks must be executable using remote tools (browser, ssh, netcat, etc…)
3. ***You may do just about anything else.***

# Hints:

1. Explore the web site and make note of form fields, cookies and how they are sent.
2. Examine the HTML look for other directories you might have access to.
3. Review the slide decks and videos from this course which show specific kinds of attacks.
4. The reavers site has only three levels of access: 0, 1 and 2.