SUMMER STUDIO B

CYBER SECURITY
AN OFFENSIVE MINDSET

Jason Ko

HIGHLIGHTS

THE 'BOOTCAMP' EXPERIENCE

A short, intense four-week course that focuses on one thing and one thing only.

CAPTURING FLAGS

That feeling of 'achieving' when you get that flag is absolutely inspiring.

INDUSTRY VISITS

Visits from professionals in the industry were amazing, the insight and knowledge they provide is invaluable.

LOWLIGHTS

GETTING STUCK

Not all machines were easy to break into, feeling stuck on a machine was demotivating.

THE STUDIO IS OVER

I really enjoyed this entire experience and I'm sad that it's finishing.

GETTING COMPLACENT

Being satisfied, resting on my achievements of completing a box and not doing more.

INSIGHTS

It's about resilience, never giving up and trying harder.
The benefits of project-based learning in terms of organisation and productivity, setting achievable but challenging goals.

WHY IS SECURITY SO IMPORTANT?

- We're in the digital age, how can we trust that the services we use are secure?
- Increasing awareness about privacy, or the lack of
- Business want to maintain consumer trust as well as reputation
- Nobody likes to be stolen from or have their data leaked and sold

WHAT CAN GO WRONG?

- Financial damage, possible to recover from
- Damage to reputation
- Customers lose faith, trust is broken, **MUCH** harder to recover from
- Possible foreclosure of business

MITIGATION

TRAINING

Make sure that employees are educated about threats or attacks that can be used against the business

CRISIS MANAGEMENT PLAN

In event of a breach, have a crisis management plan in place to minimise loss

KEEP UP TO DATE

Make sure that technology used has the latest security updates and are patched to defend against vulnerabilities

WHAT HAVE WE BEEN DOING?

SPRINT 1

Studio expectation
Group presentation
GitLab presentation
Static site blogs
OWASP Juice Shop

SPRINT 2

Web app pen testing
Bug Bounties
CTF challenges
Web app presentations

SPRINT 3

'boot2root'
Group presentations
'Own' machine(s)
(deliverable)
Deloitte presentation

SPRINT 4

More 'boot2root'
'Own' an active machine
on HackTheBox
Summer Studio Expo
Portfolio
Reverse Engineering
workshop

PROCESS

TOOLS

What are the tools I use? How do they work and why do I use them?

INFORMATION

What am I looking for? How do I find it and why do I need it?

GOAL

What do I want in this machine? Why do I want it?

Simplified Steps

LITERALLY NOTHING

Usually we're presented with a blank box/screen and we have to find out everything about it

WEB SHELL

Most vulnerable machines have a website running, we can exploit that website to gain access to a low privilege shell

USER SHELL

From a web shell, we can try to find a way to escalate our privileges to an account with more privileges

ROOT SHELL

We want to get this shell, once we're the root user, we own the machine and can do what ever we want

rm -rf /

Demo

Vulnerable Machine: "Wakanda: 1"

https://www.vulnhub.com/entry/wakanda-1,251/

Author: xMagass

https://twitter.com/@xMagass

Get ready for a lot of technical content