Week 6: Consulting

The other half

Sign-In:
https://jessh.zip/25cptcw6

SIGN IN PLEASE

https://jessh.zip/25cptcw6

Next on Bronco CPTC . . .

When	What
~~July 13th~~	~~Introduction to CPP Cyber~~
~~July 20th~~	~~Intro to Penetration Testing~~
~~July 27th~~	~~Hacking Web Applications~~
~~August 3rd~~	~~Hacking Linux~~
~~August 10th~~	~~Hacking Windows~~
August 17th	Consulting
August 24-25th	**Tryouts**
August 31st	Full CPTC Team Selected

← You are here

Agenda

1

Why Business

2

Professionalism & Ethics

3

Communication

4

Tryouts Information

1

Why Business

CTF vs IRL

- In this bootcamp/HTB/THM/etc.
  - the fundamentals
  - the methodology
  - the techniques
  - the tooling

- However, in the real world, you deal with:
  - clients (and their infrastructure)
  - red team infrastructure
  - social engineering
  - antivirus / EDR
  - accomplishing business objectives (vs. DA)

What is our purpose?

We are here to *help*

✗ "Just patch your systems" ✗

Communication & Understanding is *key*

✓ Vulnerability X has risks of Y. We suggest A to address X. Other mitigations include B and C. ✓

Providing Value

Communication

During the Engagement

- Work with the security team
- Focus on the objective
  - Be efficient
- Something out of scope? Elaborate!

Post Engagement

- Reporting
- Presentations

2

Professionalism & Ethics

Business Considerations

We got ...

- Clients
- Uptime
- Objectives & Scope
- Cost
- Ethics
- Vuln? It's a feature
- 20+ year old technology

Clients

✨**Customer Service**✨

- Technical & Non-Technical
- Be prepared to:
  - explain technical stuff to non-technical audience
  - answer tough questions
- Learn how to say "no" respectfully
- **Make sure that the client feels comfortable**

Tough Questions

Can you perform the pentest during off-hours?

Can you remove XYZ from the report? (we don't want to look bad)

How's our security compared to other companies?

Uptime

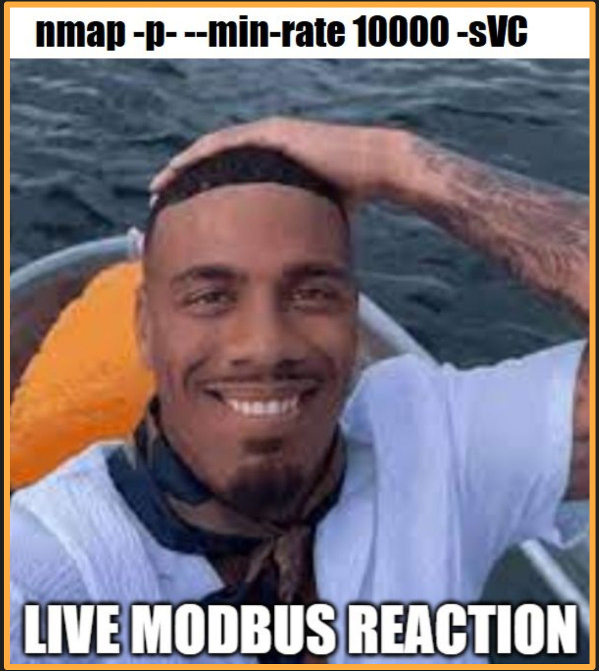
Understand your techniques

Don’t clog the pipe

Don’t lock out accounts

Don't add vulnerabilities to the environment

Communicate with your point of contact!



Objectives & Scope

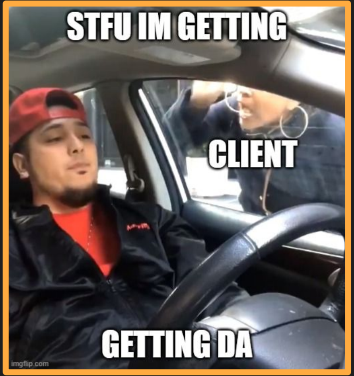
Focus on the objective & stay in scope

Prove vulnerability without downtime

A target is out of scope... but it seems vulnerable?

I WANT DA RAAAAAAAAAAAAAAHHHHHHHHHHHH

Don't be this guy =====>



Cost

You are being paid for your work

Client's don't have an infinite amount of money

- **Work efficiently**

Remediations cost time and money

3

Communication

Why listen to you?

You are the expert

Be confident

Know your attacks, the theory, and mitigations

Admit your mistakes & shortcomings

Defer if necessary

DO NOT LIE

Reporting

"Hack for show, report for dough" - BBKing

A typical format includes:

- Executive Summary
- Engagement Summary
- Methodologies
- Strategic Strengths/Weaknesses/Recommendations
- List of vulnerabilities (findings), and their remediations

Some key tips:

- Report as you go
- Understand technical writing

https://github.com/globalcptc/report_examples

Findings

Finding

Anything that affects the security posture of the client

Capable of being remediated

Criticality

Up to your interpretation

Impact + Likelihood

Remediation

Clear ways to fix finding

DO NOT MAKE PROMISES

DO NOT TRIVIALIZE, DO NOT EXAGGERATE

Technical Writing

- Be precise
- **Acronyms**
  - X performed a penetration test against **VerySecureNetworks (VSN). VSN** agreed to…
- **Terminology**
  - Definitions: exploit, vulnerability, finding, threat, etc.
  - Verbs: hacked/pwn vs exploit
- Active vs. Passive voice
- Layman's terms vs Technical terms

Presenting

Main Stuff

- Proper greeting
- Overview
- Explain* findings, steps, and methodology
- Strengths, weaknesses, recommendations
- **Prepare for questions**

Other Stuff

- Verbiage and gestures are important
- Not just what you say; also how you look saying it
- “How to prep for a presentation”

4

Tryouts Information

Your Client:
Marine Monopolies

A fictitious submarine tour company

- Small, few employees
- Recently hired 2 new employees

Yeah No

MARINE MONOPOLIES

THE NEXT AQUATIC TOURS COMP

TAKE A TOUR

Pre-register for one of our amazing tours!

LEARN MORE

https://marinemonopolies.github.io

Your Actual Client: Aquatic Armaments

A secretive underwater military company

- The actual company that hired you
- Marine Monopolies is just a front

Tryout Dates

August 24th, 10:00 AM - August 25th, 11:59 PM.

- **Briefing** will happen on August 24th at 9:30 AM.

Tryout packet will release a day before tryouts (August 23rd)

- Read packet and prep questions for briefing

Submit your report before **August 26th**.

- **No late submissions**
- Anonymize your report

5

Bonus Optional Work

CREATE A REPORT

- Use vulns found on previous labs
  - Web, Linux, AD, anything you found previously
- Fictional Client: Aquatic Armaments
  - An underwater weapons and research facility
  - Publicly known as Marine Monopolies, a tour company
  - MM: Public clients; AA: Government and private
  - Base your business impact on this setting
- Template: https://jessh.zip/aareptemp
- Past Reports: https://github.com/globalcptc/report_examples
- DM @hgwj for any questions