Week 6: Consulting

The other half

Sign-In: https://jessh.zip/25cptcweek6

Tryouts Registration: https://jessh.zip/cptctryouts25

SIGN IN PLEASE

https://jessh.zip/25cptcweek6

Next on Bronco CPTC . . .

When	What
~~July 12th~~	~~Introduction to CPP Cyber~~
~~July 19th~~	~~Intro to Penetration Testing~~
~~July 26th~~	~~Hacking Web Applications~~
~~August 2nd~~	~~Hacking Linux~~
~~August 9th~~	~~Hacking Windows~~
August 16th	Consulting
August 23-24th	**Tryouts**

← You are here

Agenda

1

Why Business

2

Professionalism & Ethics

3

Communication

4

Tryouts Information

1

Why Business

CTF vs IRL

HTB / THM / Bootcamp / etc.
practice methodology
learn fundamentals, techniques & tools
get root & DA

Real World
clients & infrastructure
social engineering
red team infrastructure
antivirus / EDR
production environments

What is our purpose?

Our hacking is done to to *help* our clients better their defense.

We want to give them **actionable solutions and information** about the problems we found.

Just patch your systems

vs

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

We must understand

- business priorities
- service configurations
- defensive strategy

Not all fixes will be suitable for every situation and client.

Communication is key.

Providing Value

Communication with Clients

During the Engagement

- Work with the client's security & IT teams (& maybe others)
  - "What are some recently exploited vulnerabilities?"
  - "Were you the one who triggered those alerts?"
  - etc.
- Focus on the objective
  - Be efficient
  - Don't tunnel-vision for root
- Something out of scope? Elaborate!

Post Engagement

- Reporting
- Presentations

2

Professionalism & Ethics

Business Considerations

- Communication
- Uptime
- Objectives
- Scope
- Fragile & Old Technology
- Vulnerability? Or is it a feature?
- Costs

Client Communications

✨Customer Service✨

- Technical & Non-Technical
  - Be prepared to explain technical stuff to non-technical audience
- Answer tough questions
- Learn how to say "no" respectfully
- Don't shame them

Tough Questions

Some Examples

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

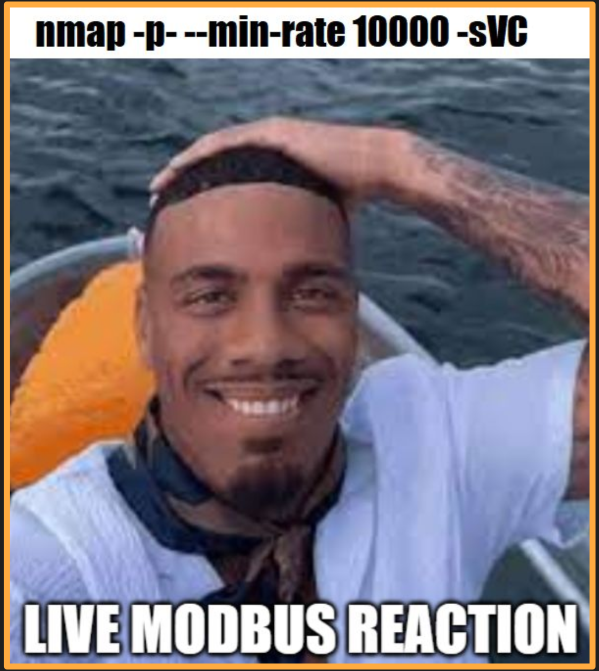
Understand your techniques

Don’t clog the pipe

Don’t lock out accounts

Don't add vulnerabilities to the environment

Communicate with your point of contact!



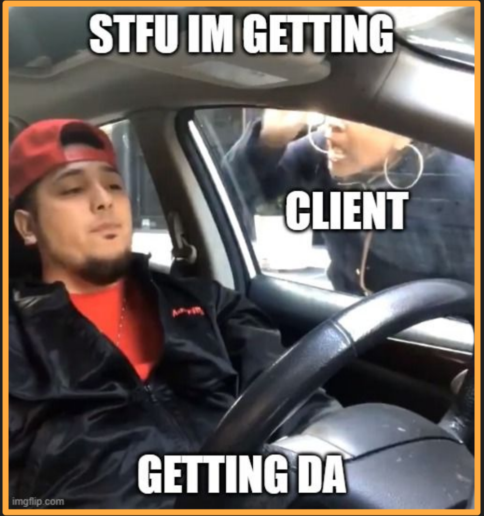
Objectives & Scope

Focus on the objective & stay in scope

Prove vulnerability without downtime

A target is out of scope…

but it seems vulnerable?



Cost

You are being paid for your work

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

- **Work efficiently**

Remediations also cost time and money

- Why hire you instead of someone to patch things?

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

Executive Summary

Engagement Summary / Attack Narrative

Methodologies

Strategic Strengths/Weaknesses/Recommendations

List of vulnerabilities (findings), and their remediations

Key tips!

Report as you go

Understand technical writing

Don't BS– they can tell!

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 (but have a reasoning to back it up)

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**
  - **Know your definitions**
    - Exploit, vulnerability, finding, threat, etc…
  - **Use professional verbs**
    - hacked/pwn vs. exploit
  - Layman's terms vs Technical terms
- **Active** vs. Passive voice

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

Tryout Dates

August 23rd, 10:00 AM - August 24th, 11:59 PM.

- **Briefing** will happen on August 23rd at 9:30 AM.

Tryout packet will release a day before tryouts (August 22nd)

- Read packet and prep questions for briefing

Submit your report before **August 25th**.

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

Sign Up!

5

Bonus Optional Work

CREATE A REPORT

- Use vulns found on previous labs
  - Web, Linux, AD, anything you found previously
- Fictional Client: Mindmend AI
  - An online AI therapy service
- Example Finding Block Template
- Past Reports: https://github.com/globalcptc/report_examples
- DM @lukedanger for any questions