Week 6: Consulting

The other half

Sign-In:
https://da.gd/VYxVjs

SIGN IN PLEASE

https://da.gd/VYxVjs

whoami

Gabriel Fok | baseq

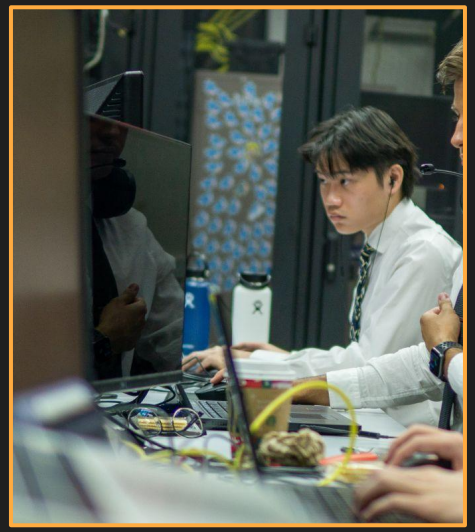
4th Year CS
ISSE @ Boeing

CCDC

Linux Team	2020-2021
Linux Lead	2021-2022
Captain	2022-2023

CPTC

Team Member	2021-2022
Co-Captain	2022-2023
Business Lead	2023-2024



Next on Bronco CPTC . . .

When	What
~~July 8th~~	~~Introduction to CPP Cyber~~
~~July 15th~~	~~Intro to Penetration Testing~~
~~July 22th~~	~~Hacking Web Applications~~
~~July 29th~~	~~Hacking Linux~~
~~August 5th~~	~~Hacking Windows~~
August 12th	Consulting
August 19th	**Tryouts**
August 26th	Full CPTC Team Selected

Agenda

1. Why Business
2. Professionalism & Ethics
3. Communication
4. Homework/Lab

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
- Something out of scope? Elaborate!

Post Engagement

- Reporting
- Presentations

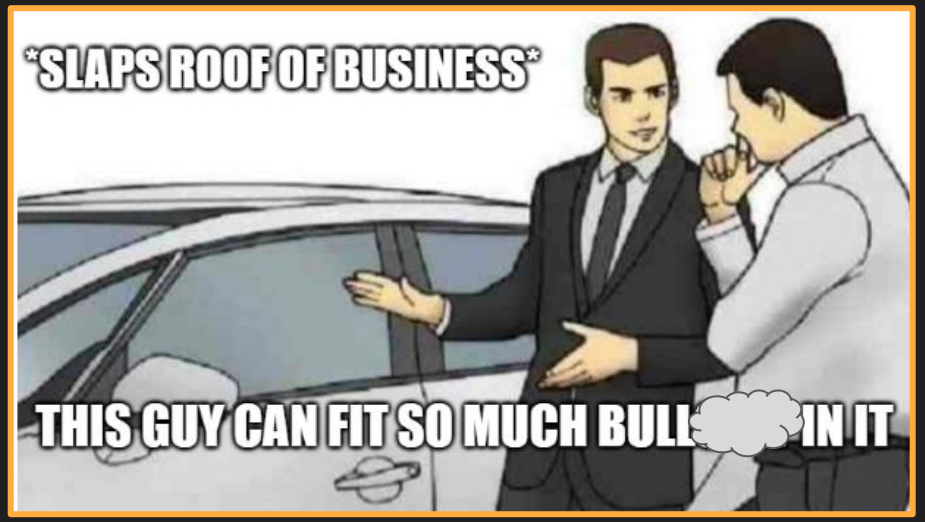
2

Professionalism & Ethics

Business Considerations

We got ...

- Clients
- Uptime
- Objectives & Scope
- 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

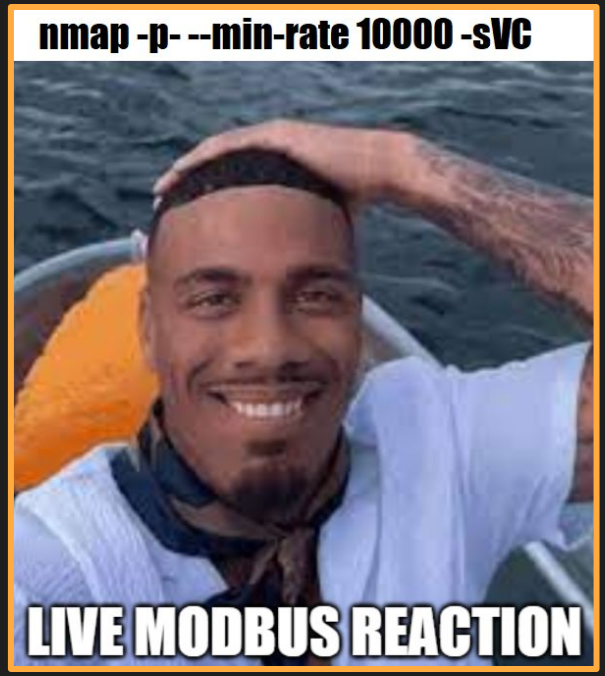
Understand your techniques

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

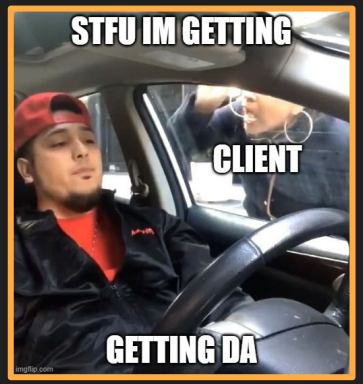
Focus on the objective & stay in scope

Prove vulnerability without downtime

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

I WANT DA RAAAAAAAAAAAAAHHHHHHHHHH

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



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://da.gd/cptcreport

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

https://da.gd/regs_2021

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

Homework/Lab

CREATE A REPORT

- Based on Lab 4 and Lab 5
  - Write up a report for the vulns found in the 2 linux machines and domain controller
- Fictional Client: Nebula Technologies
  - A Weapons Manufacturing Company
  - Private and government clientele
  - Base your business impact on this setting
- Template: https://da.gd/ntreptemp
- DM @nigerald for any questions