



The Business Side of Pentesting

What It Means To Be A Consultant

<https://da.gd/5AbL0>

Announcements

- This is the last meeting!
- Tryouts (<https://da.gd/CPTCtryout>)
- Briefing packet for tryouts <- VERY IMPORTANT
- Team selection
- Any regrade requests, ask NOW



whoami

Taylor Nguyen
4th year
Ex-CCDC 2021-2022
CPTC Team Member



Agenda

1

Why Business?

2

Reporting

3

Presentations

4

Lab





1

Why Business?

and why do I need to understand it?

Not just technical

- Pentesting requires you to understand the **business** as well as the technical stuff
- You gotta interact with clients
- Pretty big difference between doing HTB and pentesting a client environment
 - Brute-forcing AD accounts?
Don't even try. LOL
- Think before you act



The tradecraft

- In these bootcamps, HTB, THM, etc. you learn:
 - the fundamentals
 - the methodology
 - the tools
 - the problem-solving process
- However, in the real world, you deal with:
 - clients (and their infrastructure)
 - red team infrastructure
 - social engineering
 - antivirus / EDR
 - accomplishing business objectives (vs. DA)



Interacting with clients

- You're providing customer service, so **you gotta show customer service**
- Some clients might be technical, others not so much
- 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**



Some 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?





2

Reporting

very fun part of offensive security

Reporting in a nutshell

- Reporting is a **huge** part of offensive security
- Many people hate reporting, but it's part of the job
- A typical format includes:
 - Executive Summary
 - Methodologies
 - List of vulnerabilities & findings
 - Recommendations
- Some key tips:
 - Keep track of commands you ran
 - Take screenshots of findings during pentest
 - Understand technical writing (next slide)



Technical Writing Tips

- Acronyms
 - ...McDonalds performed a penetration test against **VerySecureNetworks (VSN)**. **VSN** agreed to...
- Word choice
 - Definitions: exploit, vulnerability, finding, threat, etc.
 - Verbs: hacked, attacked, exploited, etc.
- Active vs. passive voice
- How to explain technical terms



3

Presentations

also a very fun part of offensive security

Presentations in OffSec

- At the end of every pentest/red team engagement, usually you would have to do a **technical debrief presentation** with the client
 - This is also the case for CPTC
- Be able to articulate your findings and explain your steps
- Have enough knowledge about the tools you used
- And everything you see when you google "how to prep for a presentation"
- **Prepare for questions**

