Meets monthly

discord.defcon908.org

defcon908.org

meetup.com/defcon908

@defcon908

Organizers

Dan Sherry

Organizer

dan@defcon908.org

@netbroom

Jeremy Chisamore

Organizer

jeremy@defcon908.org

@chazb0t

Ben Smith

Advisor

ben@defcon908.org

/in/bensmith83/

Matt K

Advisor

matt@defcon908.org

Call for Talks

30 minutes + Q&A

- Technical
- Career
- Entrepreneurship or side projects
- “War stories” or research
- Demos
- Workshops

Introductions

2 minutes each - 15 minutes

Talk

Disclaimer: photos may be taken

Call for Volunteers

The Long Game

How I Accidentally Built a Career in Pentesting

Jeremy Chisamore

Where to Find Me

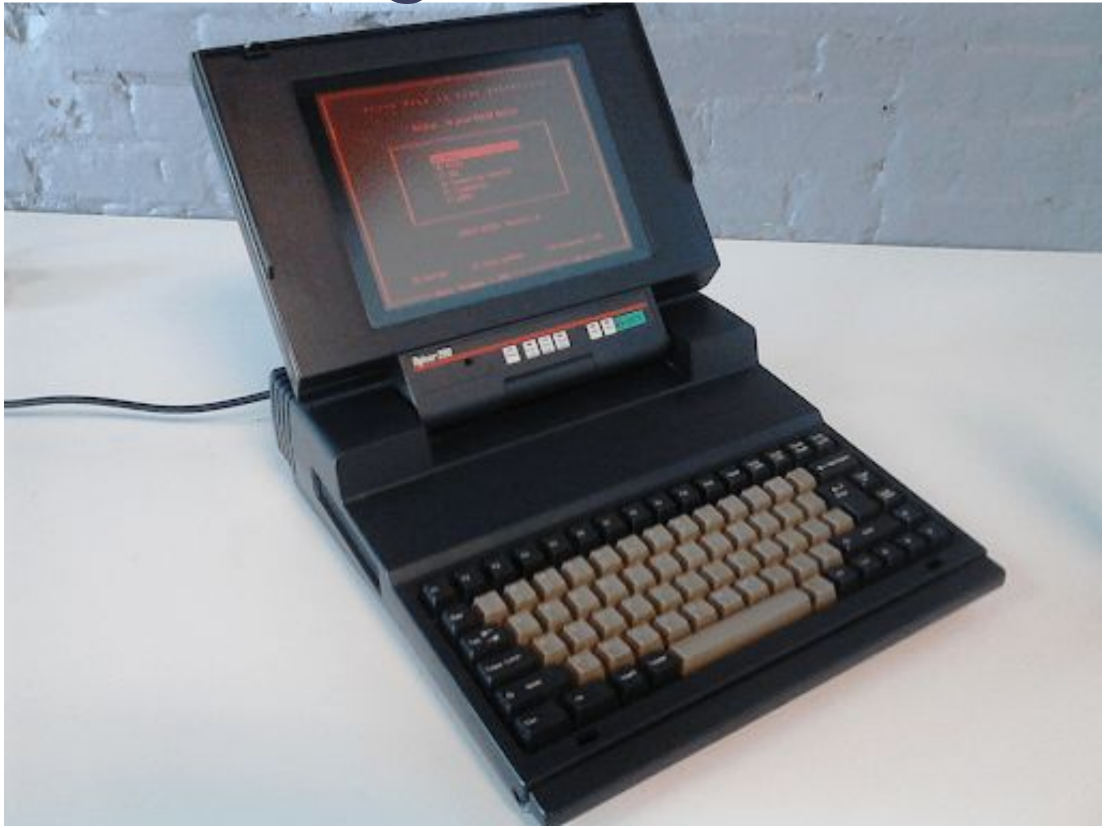
- DEFCON908 Discord: https://discord.defcon908.org/
- Linkedin: https://www.linkedin.com/in/jeremychisamore/
- Twitter: https://twitter.com/Chazb0t
- https://www.hackthebox.com/blog/poker-player-to-penetration-tester-jeremy-chisamore

Disclaimer

- This talk is based on my anecdotal experience
- Your Mileage May Vary (YMMV)

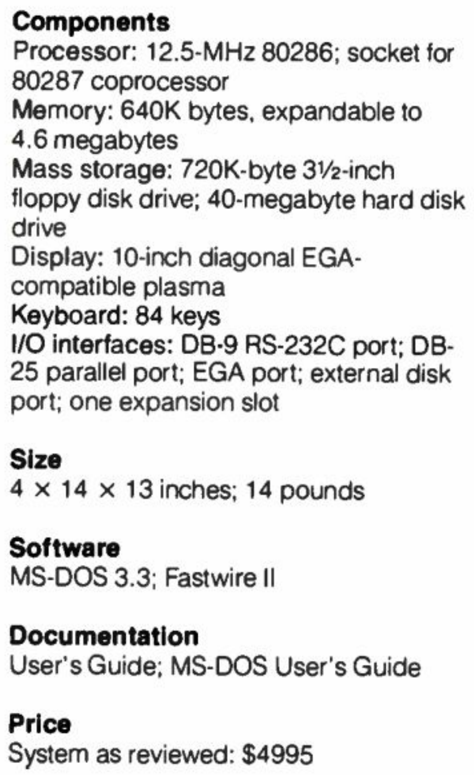
whoami

Ogivar 286



Toshiba T3100 clone

Ogivar 286, cont’d



Components
Processor: 12.5-MHz 80286; socket for 80287 coprocessor
Memory: 640K bytes, expandable to 4.6 megabytes
Mass storage: 720K-byte 3½-inch floppy disk drive; 40-megabyte hard disk drive
Display: 10-inch diagonal EGA-compatible plasma
Keyboard: 84 keys
I/O interfaces: DB-9 RS-232C port; DB-25 parallel port; EGA port; external disk port; one expansion slot

Size
4 × 14 × 13 inches; 14 pounds

Software
MS-DOS 3.3; Fastwire II

Documentation
User's Guide; MS-DOS User's Guide

Price
System as reviewed: $4995

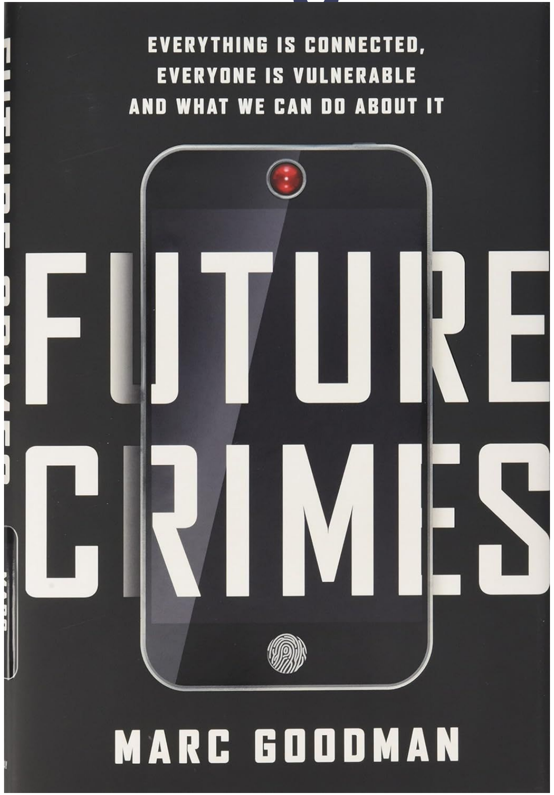
Toshiba T3100 clone

Career Path

- Lifelong Tinkerer, PC Gamer, and Tech Enthusiast
- Bachelor of Science in Management
- Financial Advisor and Stock Broker at Merrill Lynch
- Online Poker Player
- Business Development Manager at Maingear
- Senior Penetration Tester at Oracle

Interest in Penetration Testing

- Traveling in 2015/2016
- Picked up Future Crimes by Marc Goodman at an airport
- Learned that pentesting was an actual viable career path

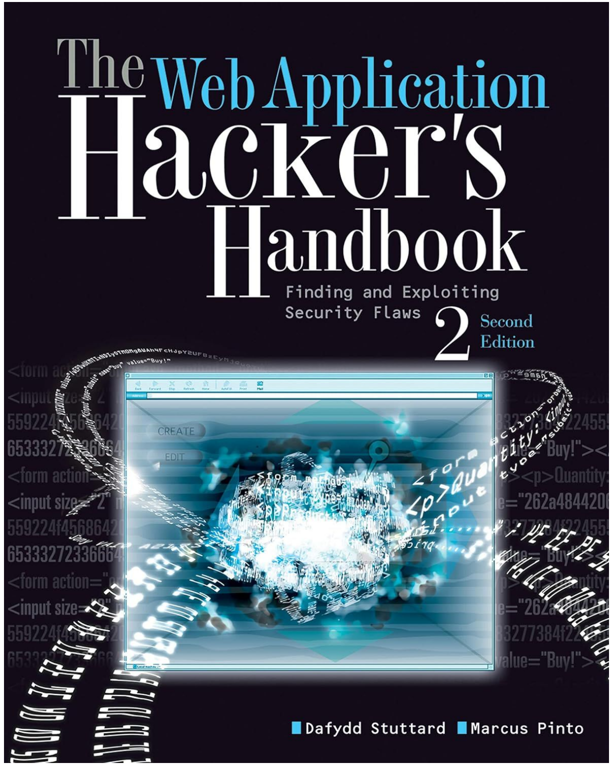


How to Get Your Foot in the Door

- Reached out to NCC Group info email account

- They mailed me a copy of the Web Application Hacker's Handbook with a handwritten letter that said "Let us know when you're ready"

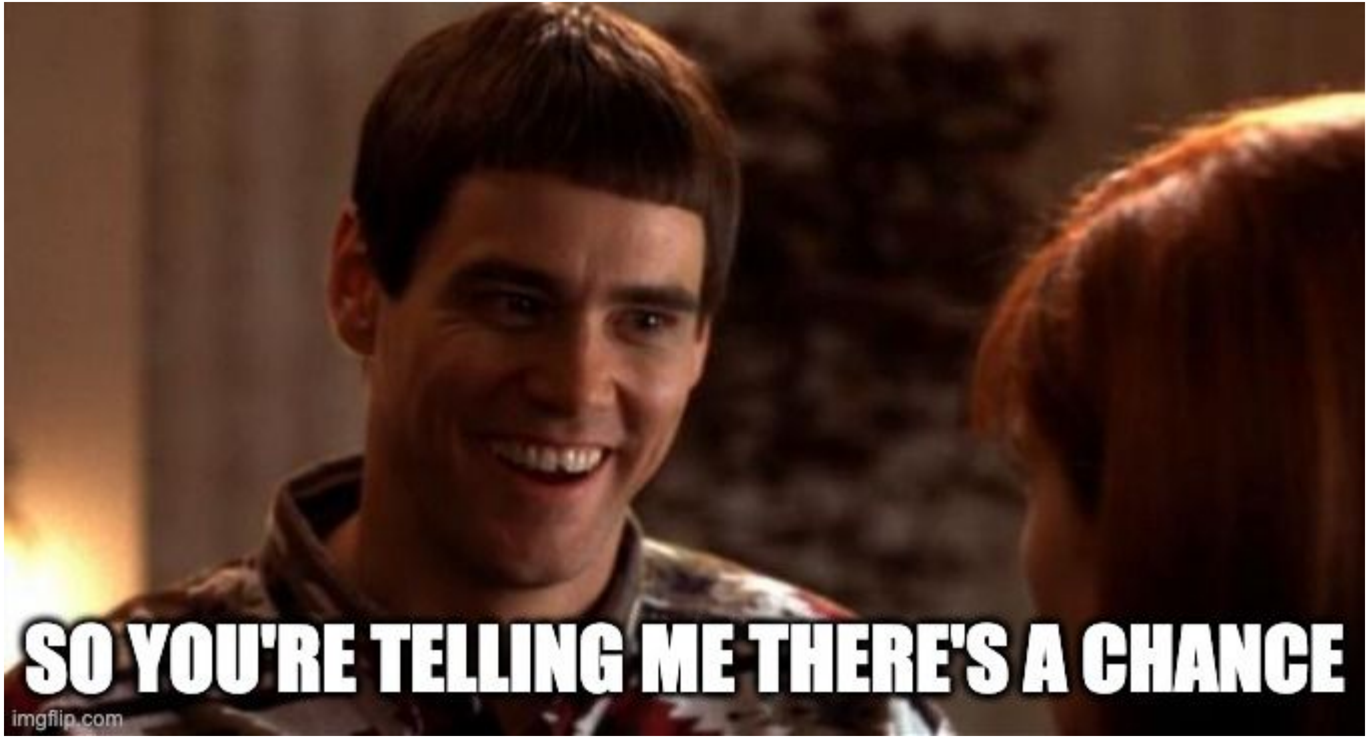
- This lit a fire under me


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard
Marcus Pinto

Networking 101

- Started getting into labs and looking into certifications and local meetups
- Met Ben and Matt at TOOOL (The Open Organisation of Lockpickers)
- Founded Central NJ Infosec group in 2016 with Ben and Matt
- Offensive Security looked too difficult for someone with no experience or education

Zero to Pentester



Certifications

- Started with eLearnSecurity (Now INE Security)

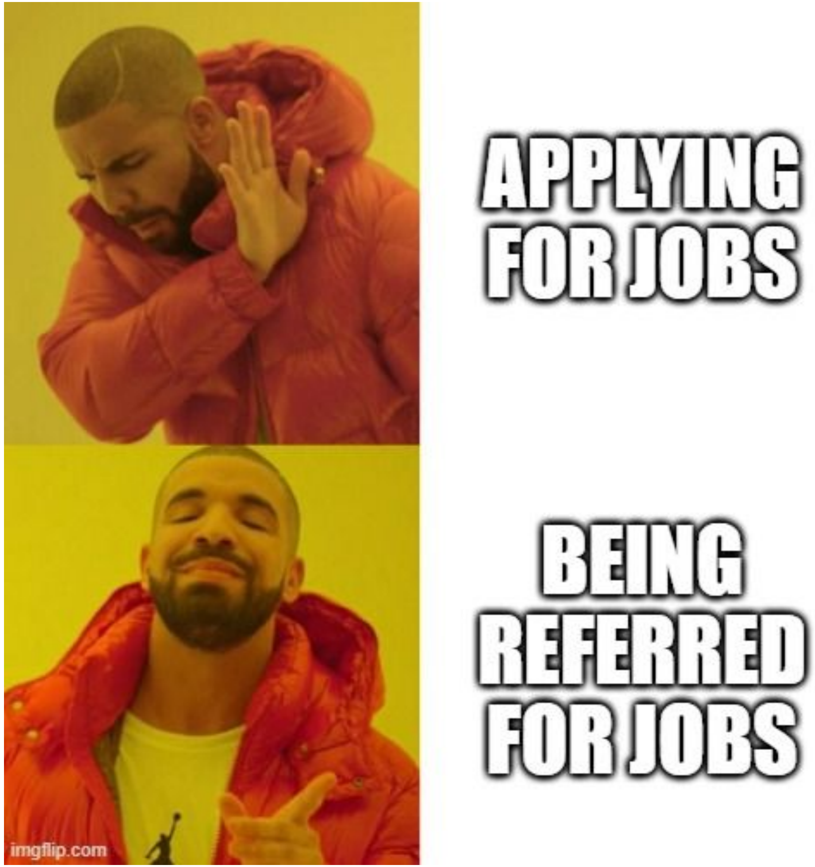
- Earned eJPT (eLearnSecurity Junior Penetration Tester)

- Earned eCPPT (eLearnSecurity Certified Professional Penetration Tester)

- Started working towards OSCP signed up for 90 day labs, failed the exam 3 times ended up taking me 292 days to pass on the 4th attempt

- In between the 3rd and 4th attempt discovered HackTheBox and it was what I needed to get over the hump and pass 4th attempt in 2018

Don’t Underestimate Networking



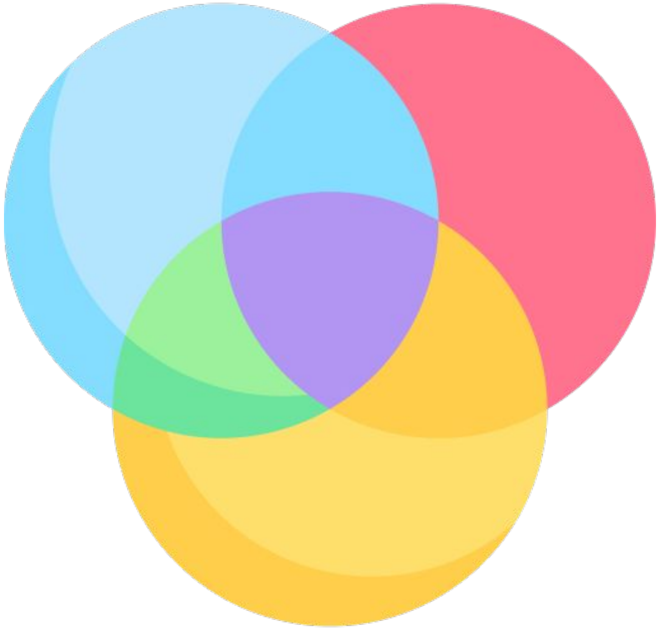
Penetration Testing Experience

- Hired as a Consultant by Context through HackTheBox Job Board in 2018
- Promoted to Lead Consultant within first 2 years
- Accenture bought Context in 2020, promoted to Senior Consultant within 2 years
- Started looking to get out of consulting and join an internal pentest team in 2022
- Got hired by Oracle as a Senior Penetration Tester on their Global Information Security (GIS) Pentest Team in 2022

Learn from My Mistakes

- Do have the right mindset
- Don’t skip the fundamentals (top down vs. bottom up) or charge headfirst into a specialization
- Don’t try to change careers or study for certifications while unemployed if you can avoid it
- Don’t get discouraged, the industry and job market is inherently overwhelming and saturated

It's Not About Catching Up



Overlapping knowledge/experience of your team

Benefits of Starting in Consulting

- Rapid-fire exposure to a wide array of technologies, industries, and clients
- Accelerated career growth and promotions
- Meet a lot of people and network in a short amount of time
- Paid certifications and training
- Compensation is good
- Strong exit opportunities

Downsides of Consulting

- Long hours/Billable hours/Timesheets
- Travel/On-site work for clients
- Lack of work/life balance
- High pressure, stress, and expectations (the other side of the exposure coin)
- Limited control of projects
- High burnout rates & attrition

Getting out of Consulting

Benefits of Internal Team

- Deeper understanding of technologies, products, and services
- Greater control of pentest targets, scope, and priorities
- Better work/life balance and less stress
- NO MORE TIMESHEETS!!!
- Job stability and security
- Full remote/zero travel except for optional conferences

Downsides of Internal Team

- Limited variety of work
- Bureaucracy & internal politics
- Slower career progression
- Less financial incentive compared to consulting
- Resource & budget constraints, much easier to charge things to clients
- Less training opportunity choices

Questions?