Getting Into Pentesting

Izdihar Sulaiman


Getting Into Pentesting
Izdihar Sulaiman

whoami

- Izdihar Sulaiman
- Husband, Father, Avid CTF Player
- Principal Consultant @ Swarmnetics
- CVE-2022-40317
- CISSP, GXPN, OSEP, OSWE, OSCP, OSWA, OSWP, CRT, CPSA, BSCP, eMAPT, ...

Contact Information ==> https://izdiwho.com

agenda

- starting point
- industry demand
- foundations
- tools & skills
- career path
- next?


starting point

what is pentesting?

Pentesting (Penetration Testing) is when companies hire us to legally hack their systems to find security problems before the bad guys do.

To break it down even further:

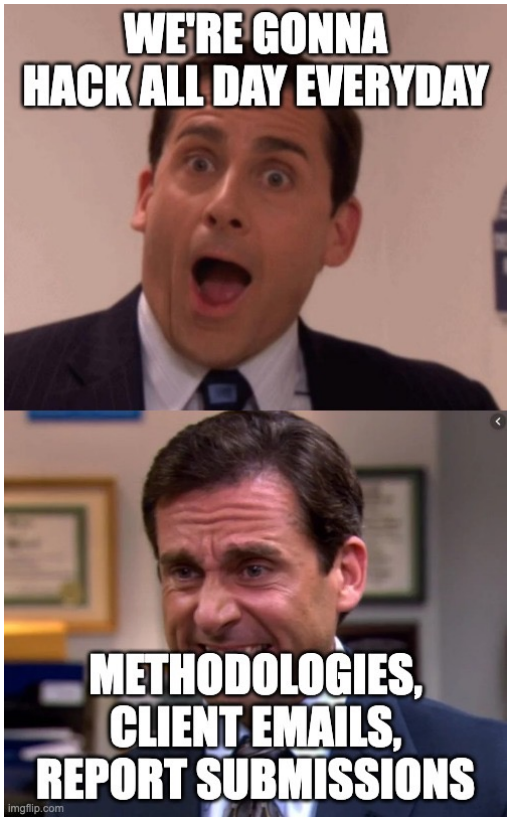
- We get permission (super important!)
- We try to break in
- We document what we found
- We explain how to fix it

my first finding

- Local Financial Institution
- Insecure Direct Object Reference
- Get statements of other people’s bank accounts
- Hooked!

reality check

- Methodical process, not just random hacking
- A LOT of documentation
- Effective client communication required
- ~~Continuous~~ Never-ending learning



day in the life of...

- Morning: Client calls, scope review, daily updates
- Mid-day: Active testing (hacking) + documentation
- Afternoon: Report writing and writing and writing


industry demand

why do you need pentesting?

- Regulatory Compliance
- Business Driven
- Risk Management
  - Proactive security
  - Breach prevention

current landscape

- Growing focus on cybersecurity everywhere
- Banking sector digital transformation
- Rise in cloud adoption
- Critical infrastructure protection needs
  - Cyber Security Order (Cyber Security Brunei)
- Personal Data Protection needs
  - Personal Data Protection Order (AITI)

compensation

- Locally
  - Junior: $30,000 - $42,000
  - Mid Level: ??
  - Senior: ??
- Globally (SG example)
  - Junior: $48,000 – $65,000
  - Mid Level: $65,000 – $120,000
  - Senior: $120,000 – $180,000


foundations

technical: Linux Fundamentals

- Essential commands
- File system navigation
- Permissions
- Bash basics

technical: Networking Basics

- TCP/IP understanding
- Common ports and services
- Network protocols
- Basic routing

technical: Web Technologies

- HTTP/HTTPS
- Common vulnerabilities
- API basics
- Web architecture

learning platform: TryHackMe

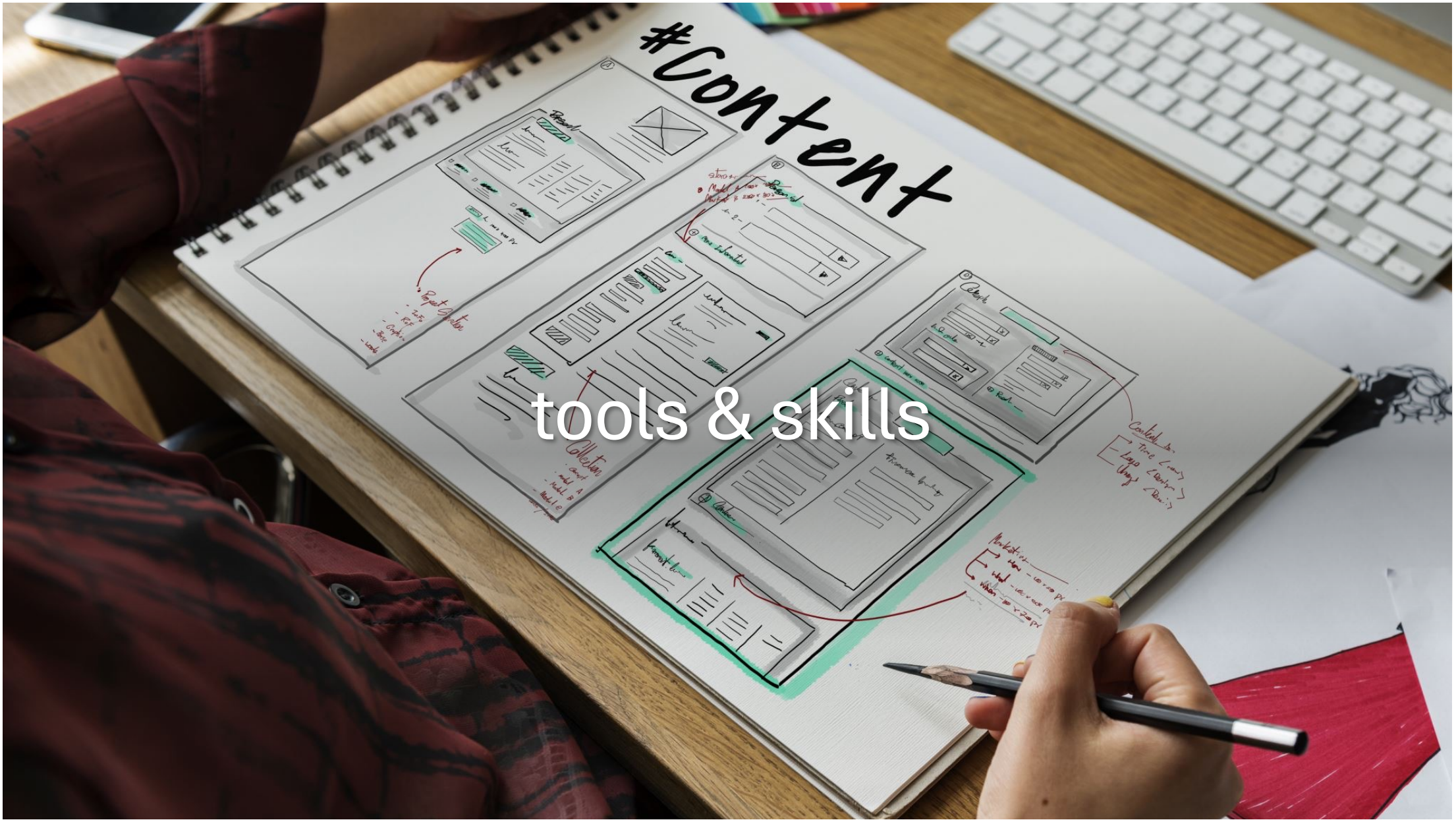
- Complete Beginner Path
- Web Fundamentals Path
- Network Fundamentals Path

learning platform: HackTheBox

- Starting Point machines
- HTB Academy

learning platform: VulnHub

- DIY Hosting
- Beginner-friendly VMs
- Created by community


#Content
tools & skills

tools

- Kali Linux
- NMAP
- Metasploit
- Nessus
- Burp Suite

skills (building)

- Home lab setup
  - Virtual Machine setup
  - Network configuration
- Capture the Flag competitions
  - Brunei CyberBattle CTF
  - PicoCTF
  - OverTheWire
  - HackTheBox challenges
- Bug Bounty programs
  - HackerOne


career path

technician build

- Transferable Skills:
  - Troubleshooting methodology
  - System administration basics
  - Active Directory experience
  - User behavior understanding
  - Incident documentation
  - Communication with non-technical users

technician build (cont.)

- Learning Focus Areas:
  - Security tools and techniques
  - Network fundamentals
  - Basic scripting (Python/Bash)
  - Web application security
  - Security methodologies

- Timeline Expectations:
  - 6 months: Basic security concepts & tools
  - 12 months: Junior security role
  - 18-24 months: Junior pentester position

developer build

- Leveraging Coding Knowledge:
  - Understanding application logic
  - Code review expertise
  - API security testing
  - Custom tool development
  - Automation capabilities
  - Debug skill application

developer build (cont.)

- Application Security Focus:
  - OWASP Top 10
  - Secure coding practices
  - Common vulnerabilities
  - Authentication/Authorization flows
  - API security testing

developer build (cont.)

- Transition Strategy:
  - Start with web app security
  - Join bug bounty programs
  - Build security tools
  - Contribute to open source
  - Focus on secure coding first

graduate build

- Building Experience:
  - Home lab setup
  - CTF participation
  - Bug bounty programs
  - Open source contributions
  - Personal projects

graduate build (cont.)

- Internship Strategies:
  - Target security companies (ITPSS/Swarmnetics)
  - Remote internship opportunities (Swarmnetics)
  - Security research positions
  - SOC analyst roles

graduate build (cont.)

- Portfolio Development:
  - Document all projects
  - Write technical blogs
  - Share CTF write-ups
  - Create GitHub repos
  - Record tool demos

common success factors

- Continuous Learning
  - Online platforms (TryHackMe, HTB)
  - Certifications (Pentest+, OSCP, CPTS, PNPT)
  - Community involvements (Meetups)
- Building Proof of Skills
  - Portfolio
  - GitHub presence
  - Blog posts

common success factors (cont.)

- Networking
  - LinkedIn presence
  - Local communities
  - Discord communities
- Practical Experience
  - CTFs
  - Bug bounties
  - Vulnerability research


next?

4 week action plan (sample)

- Week 1:
  - Set up Kali Linux (Virtual Machine)
  - Complete TryHackMe beginner path
  - Join security communities
- Week 2:
  - Create a home lab
  - Practice basic tools
    - nmap
    - Burp suite
  - Try out CTFs (ctftime.org)

4 week action plan (cont.)

- Week 3:
  - Web App Security basics (OWASP Top Ten)
  - Practice documentation
  - Check bug bounty platform (read H1 reports)
- Week 4:
  - Vulnerability assessment practice (OpenVAS)
  - Network scanning basics
  - …

resources

- https://tryhackme.com
- https://hackthebox.com
- https://academy.tcm-sec.com/
- https://book.hacktricks.xyz/

shameless plugs

https://izdiwho.com

Brunei Cybersecurity Talk
(WhatsApp Group by BCSA)

Upcoming:
18 Dec 7PM
HackTheBox Meetup


Q&A