So You Want to be A Pentester?

How to Transform Your Security Career

Boise ISSA Conference
May 14, 2015
Daniel DeCloss

Introduction

- In case we haven't met
  - BS/MS in CS
  - OSCP, CISSP, blah blah blah
  - Principal at Mayo Clinic
  - Formerly Principal at Veracode

DISCLAIMER

Agenda

- The Good
- The Bad
- The Ugly
- Making “The Shift”
- Demos / Resources

Why Pentesting?

- Severe skills shortage in industry
- Checkbox isn’t enough
- VA isn’t enough
- “Sexy”

The Good

- Every day is a new challenge
- Big puzzle
- Intriguing projects
- Shells

```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.64:4444
[*] Starting the payload handler...
[*] Sending stage (748544 bytes) to 192.168.1.68
[*] Meterpreter session 2 opened (192.168.1.64:4444 -> 192.168.1.68:1227) at Wed Oct 27 20:35:16 +0000 2010

meterpreter >
```

The Bad

- Hard
- Never feel like you're done
- Extreme self confidence issues (or at least you should!)
- Reporting

The Ugly

- Long hours
- Sleepless nights
- Thankless (not always)
- Constantly explaining/defending
- Reporting

“The Shift”: Basic Skills

- What does it take?
  - Comfortable with code
  - Command line (Windows and Linux)
  - Explain a protocol to a n00b (TCP/HTTP/etc.)

"The Shift": Passion

- Show initiative
- Be eager to learn
- Be patient
  - Problems take time to solve (like math)
- github (post/share)

“The Shift”: Passion

- Home Lab
  - vulnhub
  - POCs
  - MSDN

- No Excuses (might cost you some $$ out of your own pocket!)

“The Shift”: Knowledge

- Certs/Training/Knowledge
  - programming
  - networking
  - architecture / infrastructure
  - forensics/IR
  - malware

“The Shift”: Training / Certs*

- Do these for the right reasons!!
- Skills based certs:
  - OSCP, GPEN, OSCE, etc.

Nobody really cares about letters after your name if you can’t substantiate it ...

Skillz not Tools

"The Shift": Research

- Stay current on hacks, exploits, and vulnerabilities
- Never know when it comes in handy
- Understand the technical details
  - e.g. heartbleed, shellshock, etc.

“The Shift”: Community

- Go to cons
  - Don’t just be part of the hacker culture
    - Get involved
- Don’t be afraid to ask questions
  - Just ensure they are good, well thought questions (i.e. how’s your Google fu?)
  - “in my day” ...

“The Shift”: Stay or Leave

- Transform your current organization?
- Or aim for a new role elsewhere?

“The Shift”: Stay

- Go for the quick sell
  - application/mobile security
  - test baseline image
  - emphasize a partnership
  - holistic approach

“The Shift”: Stay

- Build a good team
- Collaboration
- Mentorship
- Lunch and Learns

“The Shift”: Leave

- Make sure it’s measured
- Research the background
- Seek a role that fits you

“The Shift”: Leave

- Don’t burn bridges (it’s a small community)
- Stay in touch, build your personal network
- Good people are hard to find, don’t get comfortable

Demo #1

- Quick Sell
- DLL Hijacking

Demo #2

- Quick Sell
- Application Security

Additional Resources

- https://www.owasp.org/index.php/Main_Page
- http://danielmiessler.com/projects/webappsec_testing_resources
- http://pentestmonkey.net
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- http://www.itsecgames.com/
- https://www.owasp.org/index.php/IOS_Application_Security_Testing_Cheat_Sheet
- http://vulnhub.com/

Questions?

f00forthought@wh33lhouse.net

@wh33lhouse