
# Breaking in to Security

www.digininja.org

# Who Am I?



robin@digininja.org

www.digininja.org

@digininja

# What is the project about?



“I’d like to get a job in security, how do I get started?”



“What programming language do I need to learn to be a penetration tester?”

# “What certification should I get?”

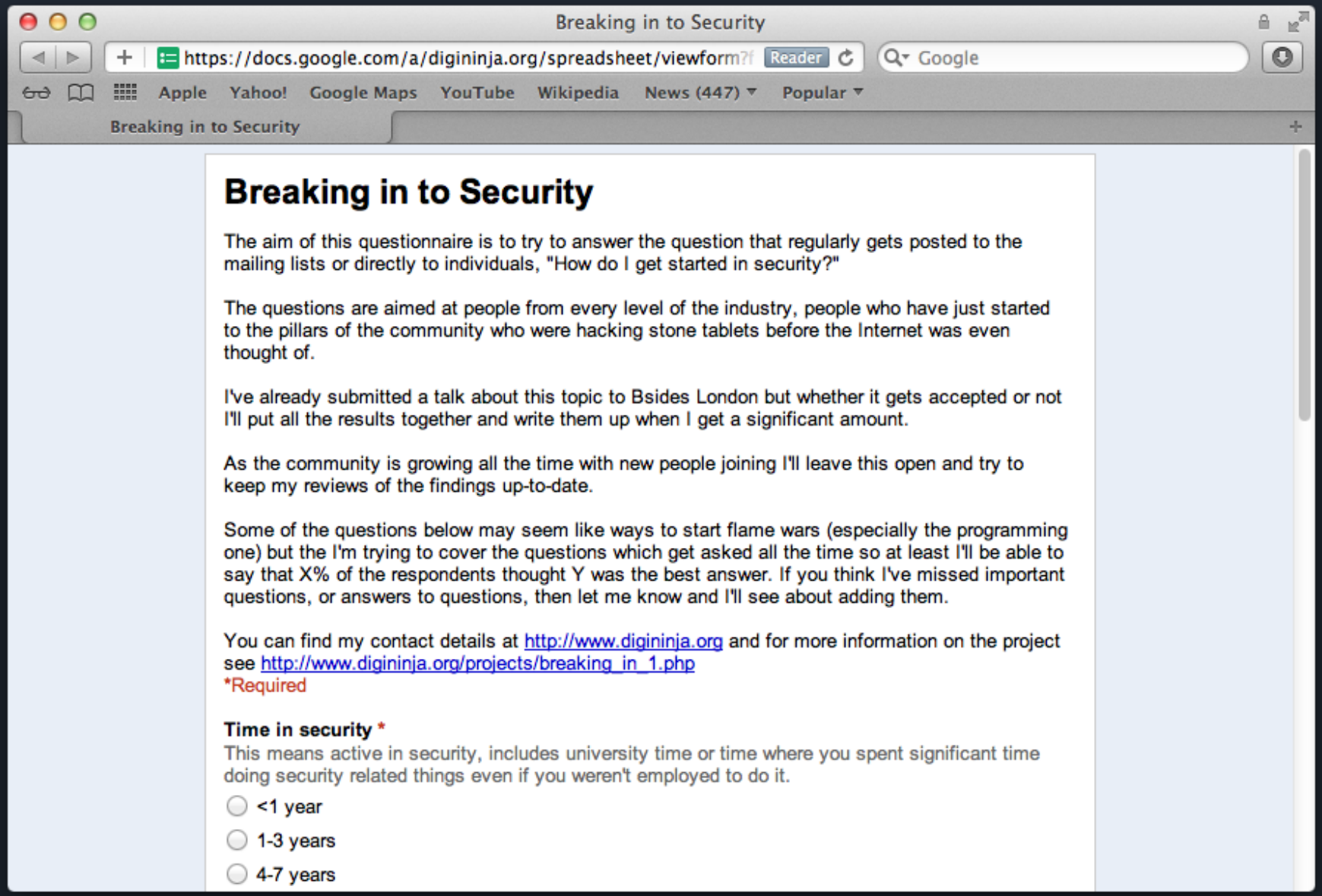


Answering these one at a time is inefficient, biased and time consuming



# Lets ask the community and get a definitive answer




Breaking in to Security
https://docs.google.com/a/digininja.org/spreadsheet/viewform?f
Reader
Google
Apple
Yahoo!
Google Maps
YouTube
Wikipedia
News (447)
Popular
Breaking in to Security
Breaking in to Security
The aim of this questionnaire is to try to answer the question that regularly gets posted to the mailing lists or directly to individuals, "How do I get started in security?"
The questions are aimed at people from every level of the industry, people who have just started to the pillars of the community who were hacking stone tablets before the Internet was even thought of.
I've already submitted a talk about this topic to Bsides London but whether it gets accepted or not I'll put all the results together and write them up when I get a significant amount.
As the community is growing all the time with new people joining I'll leave this open and try to keep my reviews of the findings up-to-date.
Some of the questions below may seem like ways to start flame wars (especially the programming one) but the I'm trying to cover the questions which get asked all the time so at least I'll be able to say that X% of the respondents thought Y was the best answer. If you think I've missed important questions, or answers to questions, then let me know and I'll see about adding them.
You can find my contact details at http://www.digininja.org and for more information on the project see http://www.digininja.org/projects/breaking_in_1.php
*Required
Time in security *
This means active in security, includes university time or time where you spent significant time doing security related things even if you weren't employed to do it.
<1 year
1-3 years
4-7 years

# But before we get started...



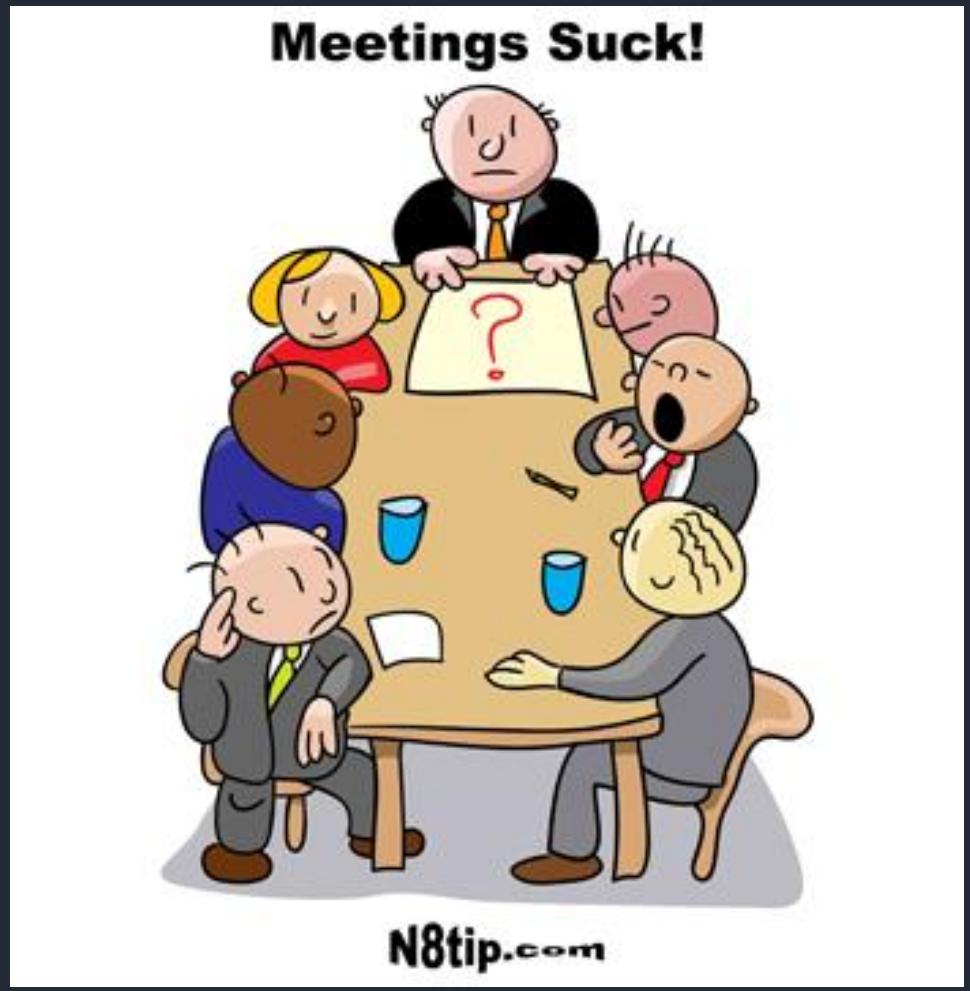
# Is this what you want to be?

# Or maybe this?

# The reality (for most testers)

# Spend a lot of time in here

# And a lot of time in these



# Still Interested?

For those still here, lets look at some stats



# Time In Industry

| | | |
|---|---|---|
| <1 year | 41 | 11% |
| 1-3 years | 92 | 24% |
| 4-7 years | 94 | 25% |
| 7+ years | 150 | 40% |

# Job Types

| | | |
|---|---|---|
| Penetration tester | 210 | 57% |
| Vulnerability auditor | 169 | 46% |
| Sys-admin | 150 | 40% |
| IDS/Firewall admin | 118 | 32% |
| Policy writer | 114 | 31% |
| Log analyst | 114 | 31% |
| Incident response | 96 | 26% |
| Other | 83 | 22% |

| | | |
|---|---|---|
| Manager | 80 | 22% |
| IT Forensics | 64 | 17% |
| Malware analyst | 57 | 15% |
| Reverse engineer | 47 | 13% |
| Helpdesk | 45 | 12% |
| Exploit developer | 42 | 11% |
| PCI auditor | 38 | 10% |

# Do you need to be able to program to be a pen-tester?

| | | |
|---|---|---|
| No, but it helps | 218 | 58% |
| Yes | 111 | 29% |
| Other | 19 | 5% |
| Don't know | 18 | 5% |
| No | 11 | 3% |

# What Language?

| | | |
|---|---|---|
| Python | 283 | 80% |
| Bash Scripting | 275 | 77% |
| Ruby | 142 | 40% |
| C | 145 | 41% |
| Windows Powershell | 124 | 35% |
| PHP | 122 | 34% |
| Batch Scripting | 119 | 34% |
| C++ | 86 | 24% |
| Java | 79 | 22% |
| Other | 63 | 18% |
| Perl | 74 | 21% |
| VB | 38 | 11% |
| C# | 31 | 9% |
| Lua | 25 | 7% |



# Are certifications useful?

| | | |
|---|---|---|
| Yes | 182 | 48% |
| Yes - but only to get through HR | 172 | 46% |
| No | 23 | 6% |



# Which certificates?

| | | |
|---|---|---|
| CISSP | 230 | 68% |
| SANS/GIAC | 220 | 65% |
| Offensive Security (PWB, AWE etc) | 132 | 39% |
| EC-Council (CEH etc) | 88 | 26% |
| CompTIA (Security+ etc) | 79 | 23% |
| Vendor specific | 77 | 23% |
| Other | 60 | 18% |
| CHECK Team Leader (CREST/Tiger Scheme) | 47 | 14% |
| CHECK Team Member (CREST/Tiger Scheme) | 43 | 14% |

# Other certificates included

- OSSTIM
- ISACA
- Cisco
- Microsoft
- Linux/Unix
- Whatever gets you the job
- Anything management has heard of
- Networking



# Are conferences worth attending?

| | | |
|---|---|---|
| Yes | 320 | 85% |
| Other | 32 | 8% |
| No | 25 | 7% |

# Which ones?

Any – to many to include got a mention



# That’s the end of the stats

# What do you know now that you wish you'd known when starting out?



# People skills, managing management and clients

“I think it's important to note that information security is a role in a company that involves dealing with people. Brush up on your public speaking and negotiation skills. I'm much better at hacking silicon than I am hacking carbon, but each is important. Take time to learn and practice those soft skills.”

# Business skills

"Business skills are more important than technical skills."

# Report writing skills

"It's all about the report... you can be the best penetration tester in the world, but if your report sucks, so does your test!"

# Networking is important

“Get out there and network, don't be shy we are a friendly lot”



# You can't secure everything and can't be 100% secure so live with it

"Security is a balance between risk mitigation and corporate earnings.  Companies must continue making money to pay your salary. Ergo, the best security may not be the right security."



“You will live in hotels”

“Pen testing is not so glamorous as it appears”

“Cons are bad for your liver”

What one piece advice would you give to someone wanting to start a career in security?



# Learn, learn and learn some more

"Study hard, do the labs and exercises, experiment with tools."

# You need your own lab

"Set a lab environment up to practice with, virtualization makes these easy these days."



# Get an all-round education

"Develop skills in other areas of IT (system administration, network management, development, etc.) either before or in addition to InfoSec."

# Make sure you enjoy what you do

"Do it for love of what you do, not to make money. The money is good, but if you really enjoy it, it's the best job in the world."

"Make sure its something you really want and can keep up with, not just something you enjoy on the side."



# More about soft skills and business knowledge

"Be tolerant of the non-techs, teach them, but don't talk down to them.  Be aware that sometimes, the business needs trump security best practices."



# Repeated from earlier, programming is a useful skill

"Learn to program (scripting at least)."

# Get yourself known

"To get involved in different projects and contribute, there are a lot of open source projects you can contribute to in different ways."



“It's all about reputation. Certs are useful, but if you are unknown you won't be taken seriously. Get out there, meet people, and learn from them!”

“Start a blog.. not for fame and glory but more for keeping a record of what you learn. Doesn't matter if no one reads it, do it for yourself.”



# InfoSecMentors

"Try to find a mentor. There is so many layers to information security and figuring out where and what you want to do might be very challenging."

http://www.infosecmentors.com

@InfoSecMentors



Find your local community - 2600, hackerspace, DC group

“Find your local community & online community”



# Don’t blindly trust tools

“Learn what’s going behind the tools you are using”



“Get in bed with the operations and finance people (not literally, however this might also help)”



“Work your ass off!  Everyone else does so you better get used to it.”



Is it OK to “practice” on sites/companies without permission if you don't do any damage?



Overwhelming opinion – No

There are enough resources out there you don’t need to

“Only if you want a new ‘room-mate’ called Bubba.....”



# What I've not covered

What do you see as the next up and coming area?

Is there anything you feel you did wrong that you would advise against?



# Where can I get the data?

Slides

http://www.digininja.org/projects/breaking_in_bsides.php

Data

http://www.digininja.org/projects/breaking_in_data.php

# Resources

http://infosecmentors.com/

Podcasts

Twitter

Mailing Lists

Forums

Conferences



# Conclusions

If you aren’t passionate it is just another job

Get stuck in, learn and show your interest

Don’t be afraid to ask questions - but show you’ve tried to find the answer yourself first

It isn’t all about the tech

# Big thanks to all who responded

# Any Questions?

# Who Am I?



robin@digininja.org

www.digininja.org

@digininja