Propelling Your Pen Test Career into the Next Decade

JOSHUA WRIGHT
JOSH@COUNTERHACK.COM
@JOSWR1GHT
The rogue Twitter employee who deleted Trump’s account could face hacking charges

The Computer Fraud and Abuse Act gives the government wide latitude to pursue those who have allegedly accessed a computer “without authorization” or in ways that exceed the level of authorization they’ve been given.

Brian Fung • 3 days ago
FBI arrests Chinese national connected to malware used in OPM data breach

By Evan Perez, CNN Justice Correspondent

Updated 6:29 PM ET, Thu August 24, 2017

OPM hack may be 4 times larger than government first said
ASHLEY MADISON®
Life is short. Have an affair.®

Over 56,535,000 members.*

SEE YOUR MATCHES

*The number of members who've joined Ashley Madison since 2002.
WE LIVE IN THE GOLDEN AGE OF INFOSEC EMPLOYMENT OPPORTUNITIES.*

* Also known as the Golden Age of Hacking, the Golden Age of Surveillance, the Golden Age of Ransomware, the Golden Age of Compromises, and The Golden Age of Exploiting Anything That Can Make Hackers a Buck.
Significant career growth is within your reach. * 

* If you want it, and are willing to work for it.
<table>
<thead>
<tr>
<th>Benefits</th>
<th>Benefits</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended maternity and paternity paid leave</td>
<td>Retirement benefits</td>
<td>Compensated sabbatical programs</td>
</tr>
<tr>
<td>Above average vacation allocations</td>
<td>Professional development opportunities</td>
<td>Child care programs</td>
</tr>
<tr>
<td>Premium health and dental benefits</td>
<td>Technical training budgets</td>
<td>On-site car wash, haircuts, and other conveniences</td>
</tr>
<tr>
<td>College scholarships for children of employees</td>
<td>Vertical-related independent project support</td>
<td>Family planning, fertility services</td>
</tr>
<tr>
<td>NAP ROOMS</td>
<td>Telecommuting and work from home benefits</td>
<td>On-site acupuncture, improv classes</td>
</tr>
<tr>
<td>Personal development opportunities</td>
<td>Discounted dining options</td>
<td>LGBTQ rights and diversity support</td>
</tr>
<tr>
<td>Community service sponsorship programs</td>
<td>Pet healthcare programs</td>
<td>Healthy living programs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How do you get there?
The restrictive thinking of innovation.
"widely considered one of the most successful, innovative, and influential rock groups in history."
The Lead Zeppelin

- Bring it on Home (Willie Dixon)
- Bring it on Home (Led Zeppelin)
- Killing Floor (Howlin' Wolf)
- The Lemon Song (Led Zeppelin)
- Blackwaterside (Bert Jansch)
- Black Mountain Side (Led Zeppelin)
- Dazed and Confused (Jake Holmes)
- Dazed and Confused (Led Zeppelin)
Everything is derivative. * This is a good thing.
The Alto

The Macintosh
The basic elements of creativity:

- Copy
- Transform
- Combine
By Robert Moskowitz
Senior Technical Director
ICSA Labs, a division of TruSecure Corp
November 04, 2003

Use of PSK as the key establishment method

WPA and 802.11i provide a mechanism (a PSK) as an alternative to 802.1X based key establishment. It can be a 64-bit number or a passphrase 8 to 63 bytes in length. Each AP will have its own PSK, tied to its MAC address. To do 802.11i without 802.1X, providing for one PSK for an ESS, just as they do for a 64-bit number.

When a PSK is used instead of a pre-shared key, the Pairwise Master Key (PMK) that is used to derive the Master Key and the whole Pairwise Transient Key (PTK) is constructed, there is a straightforward formula to derive PSK to the 256-bit value needed for the PMK.

This paper will look into the risks of using a PSK and particularly the risk associated with a passphrase-based PSK.

How the PSK is used in WPA and 802.11i
Copy
Transform
Combine
1. Constant learning

Develop new skills to increase your employee value proposition.

* You're here, and that's a great start.
In 1 week, figure out what Docker is.

In 1 month, convert all OPS VMs to Dockerfiles.

In 3 months, roll out production Docker deployment with integrated monitoring and maintenance.
Use an RSS reader.
I'm going to let you in on a little secret. Remember AOL? I know they cancelled it, and people are all broken up about it. But did you know they have a free service? Go to reader.aol.com. You can login with your old AOL account. Oh, and there's no password. I'm pretty sure someone is going to figure it out and . Until then, hop on over there and manage all your reading from one place.
2. Login to reader.aol.com, click ••• | Import. Select the OPML file, then click Upload.
FeeddlerPro for iOS

Feedly for Android

Apply the skills you develop at work to solve problems and get noticed.
Differentiate through creation.
Start writing.

Commit to a regular writing schedule.

Work on communicating complex topics in plain language.

Work on communicating what is important to your audience.
This amount: TWELVE DOLLARS AND 85/100

Pay to the

JOSHUA WRIGHT

* This check arrived by FedEx, which cost $21.40 to ship.
If you don't code, it's time to start.
Learning to code isn't hard.

Staying motivated until you can be productive with your code is.

Solution: Build something that motivates you.
• Use Python to automate a mundane task on Unix boxes.
• Use PowerShell to do the same on Windows boxes.
• Use Swift to write a simple app for iOS.
• Use Kotlin for the same on Android.
• Use JavaScript to write a simple web app to help people choose passwords.
Awesome Password Generator!

Need an awesome password? Just click the button below for your Awesome Password!

Awesome!

Your Awesome Password is:

winter0831

Entropy for the password selection provided by the 2009 Rockyou.com compromise. See the back-end code!
Your Awesome Password is:

winter0831

Entropy for the password selection provided by the 2009 Rockyou.com compromise.
<?php
    $fp = fopen('rockyou.txt', 'r');
    // 139751900 is a little less than the total file size
    fseek($fp, rand(0, 139751900));
    fgets($fp); // Skip this possibly incomplete line
    print fgets($fp);
?>

Everyone I spoke to said their career success is tied to the contributions they have made in the infosec community.
"What are three things you've done that you feel are pivotal to your career success?"

"Information sharing has been critical for networking. ... Open collaboration to support other people and gain their support."

Kevin Finisterre

"I've participated in the infosec community - blogging and volunteering. Not only does that push me, but it makes our community of practice better as a whole."

Leslie Carhart

"Knowledge itself is not enough. I work on giving back to the community through blogging, webcasts, and speaking at conferences whenever I can."

Carrie Roberts

"Networking wherever possible and being involved with the community. I started as a volunteer for my local ISSA chapter, then joined the board, then VP, then president. While doing that, I contributed to OWASP, and I wrote a book."

Jorge Orchilles
The infosec profession, in particular, is a close-knit community that values those who excel, but reveres those who give back.
4. Choose your employer carefully.

Your employer will help you succeed, or they will hold you back.
Important Questions:

• Does your employer support your professional growth?
• Does your employer allow you to speak publicly and share outside of work?
• Is your employer more interested in making you more employable or retaining you (and holding you back)?
Leaving an employer is always scary, but an employer that doesn't support you or help you to succeed will significantly limit your chances for success.
"If people give you advice out of selfishness, then you should avoid that advice. Seek out an employer that encourages you to promote yourself and give back to the community."

John Strand, Founder
Black Hills Information Security
Actionable Steps for Moving Forward
"So Josh, tell me about your five year goals."

You should figure out your five year goals.
Write down your five year goals.
Identify how you plan to accomplish each.
Read and update the list often.
Identify your personal brand.
My personal brand:

*Technical excellence with attention to detail for high-quality, on-time delivery.*

Identify what works for your brand, and take on projects that will support it.
Regular time for tech.
Copy

Identify the practices of successful people in infosec that you want to match and exceed. Copy those ideas for your own use.

Transform

Identify what works for you, and how you can change those practices to improve your own career. Be daring, but not reckless.

Combine

Combine the practices identified in this presentation, and those you build for your own career to achieve wild success.
"Check that heavy metal
Underneath your hood
Baby, I can work all night
Believe I got the perfect tools"

Led Zeppelin
Robert Johnson (1936)
(you get the idea)
Thank you.

Joshua Wright
josh@counterhack.com
401-524-2911 (mobile)
@joswr1ght