A year of gaining superpowers

Tarah Wheeler
@tarah

SANS PEN Test HackFest Summit
November 13th, 2018
THE FUTURE OF WAR

THOMAS J. CHRISTOPHER


TARAH WHEELER (@tarah) is an information security researcher and political scientist. She is a New America cybersecurity policy fellow and senior director of data trust and threat and vulnerability management at Splunk.
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not enough time. You can decrypt some of your files for free. Try now by clicking Decrypt. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click About bitcoin. Please check the current price of Bitcoin and buy some bitcoins. For more information, click How to buy bitcoins. And send the correct amount to the address specified in this window. After your payment, click Check Payment. Last time to check: 09:00am - 11:00am Central European Summer Time.

Send 2000 worth of bitcoin to this address:
1219YDPgmez29NyMLxwe019p7AA65r6SMhr

Check Payment Decrypt

About Bitcoin
How to Bitcoin?
Contact Us
Where did this all start?
I was a perfectly respectable practitioner, professor, & soc and incident commander
And then some guy showed up on this PBS Nova vidcast with me
Example of Perfectionism

(Diagram adapted from Westbrook, Kennerley and Kirk)
Lets talk about training and certification...
They matter more to under-represented populations
tarahwheeler I passed my CISSP! Thank you to @sansinstitute and @Symantec for support & Seth Miserar for awesome teaching!
frankysalinast10 Congratulations!!!
jmcquiggan Congratulations!!
curtisgram @tarahwheeler congrats!
charmunicnemyo @tarahwheeler I start my training next week for this!! Congratulations!!
charmunicnemyo @tarahwheeler did you study or was your test strategy from experience? What did you use to study? I am very curious and would love any advice you can give.
adshelp_singh That's great
romeolorenzo Awesome! Congrats! 😊

82 likes
MAY 4, 2017
Log in to like or comment.
I was surprised to pass.

Seriously.
failing is good...
YES, I'M SURE.
Public accountability is better.
I'm going to talk about something I'm afraid of. I'm afraid of failing at this haxxoring course.

3:11 PM - 16 Aug 2017

5 Retweets  85 Likes

Tarah M. Wheeler
@tarah

I just started with the @offseptraining OSCP. The @kalilinux folk are incredible. The OS folk are AWESOME. Cc @ihackstuff

8 Retweets  46 Likes

Tarah M. Wheeler
@tarah - 16 Aug 2017

I downloaded the videos. I grabbed the images. My seat in this 90-day class started on Saturday.

7 Retweets  20 Likes
I'm a 38-year old woman. I'm no hacker badass...but I'm definitely not losing my place in any *buntu file structure.

At Black Hat, I was part of the incredible @mubix & @egyp7's @metasploit Basics & Mastery trainings.

I'd never done major Ruby Dev, but I wrote my first Metasploit mod from scratch and broke a WordPress box open.

Now, for those of you that remember me asking months ago, I've started what's arguably the hardest security cert training in the world.
I love this community and my people. I'll always try to help. And now it's time for my skills to get a major upgrade.

I am here in public to tell you that for the next 87 days, I'll be working this material, and I'll take the test to be an OSCP.

I might fail. It's scary to try things, but I won't give up, and I won't stay quiet. I'll ask you all questions.

Please wish me luck, and join me in upgrading your skills every day. Admit your fear and learn to hack all the things with me.
Dear Tarah,

We regret to inform you that you did not meet the requirements to obtain the OSCP certification as we did not receive your exam documentation within the allotted time frame.

If desired, you may reschedule the exam and attempt to retake it within 12 months. If you choose to do so, please submit the exam fees via your personalized purchase link and you will be able to schedule your exam within 90 days of the Exam Retake Cooling Off Period detailed below.

**Exam Retake Cooling Off Period**

- After the 1st failed exam, a student may schedule an exam retake after 1 week.
- After the 2nd failed exam, a student may schedule an exam retake after 2 weeks.
- After the 3rd failed exam, a student may schedule an exam retake after 3 weeks.
- After the 4th failed exam onwards, a student may schedule an exam retake after 6 weeks.

If you choose to purchase a lab extension before taking the exam again, the extension fee includes a complimentary exam attempt. You will be able to schedule your exam within 90 days from your lab extension ending date.

You can make any future purchases via the following link:

[OSCE Purchase Link](#)

Sincerely,
The Offensive Security Team

[www.offensive-security.com](http://www.offensive-security.com)
IS THIS YOUR FIRST TIME?
Dear Tarah,

We regret to inform you that you did not meet the requirements to obtain the OSCP certification as we did not receive your exam documentation within the allotted time frame.

If desired, you may reschedule the exam and attempt to retake it within 12 months. If you choose to do so, please submit the exam fees via your personalized purchase link and you will be able to schedule your exam within 90 days of the Exam Retake Cooling Off Period detailed below.

**Exam Retake Cooling Off Period**

- After the 1st failed exam, a student may schedule an exam retake after 1 week.
- After the 2nd failed exam, a student may schedule an exam retake after 2 weeks.
- After the 3rd failed exam, a student may schedule an exam retake after 3 weeks.
- After the 4th failed exam onwards, a student may schedule an exam retake after 6 weeks.

If you choose to purchase a lab extension before taking the exam again, the extension fee includes a complimentary exam attempt. You will be able to schedule your exam within 90 days from your lab extension ending date.

You can make any future purchases via the following link:

[OSCP Purchase Link](#)

Sincerely,
The Offensive Security Team

[www.offensive-security.com](http://www.offensive-security.com)
fail more
The end result is what matters
failing is good...
Optimize your time instead of comforting your brain meats
The law of diminishing returns

Score on test vs. Time spent studying

73-82%
The law of diminishing returns

Score on test

Emotional gratification

Useful time

Time spent studying

73-82%
Do different things to solidify this knowledge
Radically expose your ignorance. It’s the only solution.
the takeaway: we are superheroes, and we have the responsibility to learn any way we can to protect people
leave to remind the conductors of the press of their duty to apply to themselves a maxim which they never neglected to urge on the consideration of government—"that the possession of great power necessarily implies great responsibility." They stood in a high situation, and ought to consider justice and truth the great objects of their labours, and not yield themselves up to their interests or their passions. His friends would, perhaps, reproach him with instigating ministers to curb the press; but nothing, he assured them, was farther from his mind. He was aware of the great benefit the country derived from the liberty of the press, and nothing could induce him to concur in any measure that might tend to injure it; at the same time he was free to confess, that its state had an influence on the vote he gave on the present question. With regard to the statements in the reports, though his apprehensions founded on the feelings of our nature for the purpose of ruining and destroying those towards whom they were put on. It must, however, be remembered, that in human society there were many functions necessary to be discharged, many duties indispensable to be fulfilled, with regard to which the only feeling was astonishment how any persons could by any means be found, or by any motive induced to fulfil and discharge them. With respect to the affair at Huddersfield, the fact had not been denied. It was admitted that there were on the night mentioned in the report on the bridge at Huddersfield a body of armed men, the number might be disputed upon, with hostile intentions against the town. Now, if Oliver instigated the rising could it be contended that he spread throughout the country the animus the rebellious feelings which induced them thus to act according to his instigation? It was impossible to imagine, unless in itself
AND, A SHORT DISTANCE AWAY...

MY FAULT--ALL MY FAULT! IF ONLY I HAD STOPPED HIM WHEN I COULD HAVE! BUT I DIDN'T--AND NOW--UNCLE BEN--IS DEAD...

AND A LEAN, SILENT FIGURE SLO WLY FADES INTO THE GATHERING DARKNESS, AWARE AT LAST THAT IN THIS WORLD, WITH GREAT POWER THERE MUST ALSO COME--GREAT RESPONSIBILITY!

AND SO A LEGEND IS BORN AND A NEW NAME IS ADDED TO THE ROSTER OF THOSE WHO MAKE THE WORLD OF FANTASY THE MOST EXCITING REALM OF ALL!

EXT ISSUE OF AMAZING FANTASY --- FOR THE FURTHER AMERICA'S MOST DIFFERENT NEW TEEN-AGE IDOL -- SPIDERMAN!

the End
leave to remind the conductors of the press of their duty to apply to themselves a maxim which they never neglected to urge on the consideration of government—"that the possession of great power necessarily implies great responsibility." They stood in a high situation, and ought to consider justice and truth the great objects of their labours, and not yield themselves up to their interests or their passions. His friends would, perhaps, reproach him with instigating ministers to curb the press; but nothing, he assured them, was farther from his mind. He was aware of the great benefit the country derived from the liberty of the press, and nothing could induce him to concur in any measure that might tend to injure it; at the same time he was free to confess, that its state had an influence on the vote he gave on the present question. With regard to the statements in the reports, they did, in some measure, refer to the feelings of our nature for the purpose of ruining and destroying those towards whom they were put on. It must, however, be remembered, that in human society there were many functions necessary to be discharged, many duties indispensable to be fulfilled, with regard to which the only feeling was astonishment how any persons could by any means be found, or by any motive induced to fulfil and discharge them. With respect to the affair at Huddersfield, the fact had not been denied. It was admitted that there were on the night mentioned in the report on the bridge at Huddersfield a body of armed men, the number might be disputed upon, with hostile intentions against the town. Now, if Oliver instigated the rising could it be contended that he spread throughout the country the animus the rebellious feelings which induced them thus to act according to his instigation? It was impossible to imagine he could have influence
Here’s my December and January:
Dear Tarah,

We regret to inform you that you did not meet the requirement to retake the exam. We did not receive your exam documentation within the allotted time frame.

If desired, you may reschedule the exam and attempt it again. To purchase the exam fees via your personalized purchase link and reschedule the exam, please submit the exam Retake Cooling Off Period detailed below.

**Exam Retake Cooling Off Period**

- After the 1st failed exam, the cooling off period is 2 weeks.
- After the 2nd failed exam, the cooling off period is 2 weeks.
- After the 3rd failed exam, the cooling off period is 3 weeks.
- After the 4th failed exam, you may schedule an exam retake after 6 weeks.

If you choose to purchase a lab extension before taking the exam again, the extension fee includes a complimentary exam attempt. You will be able to schedule your exam within 90 days from your lab extension ending date.
Have hacking emotional support system in place
Because we know what’s coming

Be ready.