UNMASKED

CYBRARY.IT

TAKING THE MYSTERY OUT OF CYBER SECURITY

FEBRUARY 2018 | EDITION 1

IN THIS ISSUE

EDITOR'S NOTE

As I hope most of you know, Cybrary is nothing without its members who continuously contribute their time, content, and feedback to the site. Since we just celebrated our 3 year anniversary and have grown to over 1.4 million users, our mission has become more important than ever.

Millions of jobs remained unfilled in the field, and yet proper education and training for those jobs are limited to people who have the means to pay $2,500-$5,000 for a one week class, per topic- until Cybrary.

Please vote for Cybrary in the **Cyber Security Excellence Awards for Best Education Provider.** You can do so by **clicking HERE.**

Olivia Lynch **(@Cybrary_Olivia)** is the Marketing Manager at Cybrary. Like many of you, she is just getting her toes wet in the field of cyber security. A firm believer that the pen is mightier than the sword, Olivia considers corny puns and an honest voice essential to any worthwhile blog.

CYBER SECURITY NEWS

#EXPOSED

The US military is sounding off after data was shared publicly from GPS tracker firm Strava which inadvertently revealed the locations of covert military facilities in war zones.

Strava collected more than 3 trillion coordinates from more than 27 million users of fitness trackers like Fitbit and Jawbone over 2 years. The data was anonymized and put into a global heat map, which they released in November. After a closer look by an Australian student, it appeared that they were some areas far less trafficked on the map then others, specifically in countries such as Afghanistan and Syria .Those outliers, which included military facilities in war zones and routes walked along the Mexican border by U.S. border patrols. "The security issue isn't simply that US forces are active in these locations but the level of detail Strava reveals about how they move around their environment," commented the Washington Post.

Although the risks to both foreign intelligence and military members themselves is apparent, it's important to note that Strava "offers users the ability to hide start and end points (usually a user's home address or workplace) by creating a privacy zone." However, it's an important reminder to think twice before using location sharing services. In response to this incident, many are calling for new privacy controls for soldiers in certain locations, including limiting smartphones and wearables and establishing new policies.

Social media location data can be just as dangerous. Read this post on how to craft attacks using 'Creepy.'

#HACKED

IIf cryptocurrency is the latest trend, let's hope that crypto exchange hacks don't start competing for popularity. In what's being called the largest crypto exchange hack in history, Coincheck lost over $58 billion yen.

For those unfamiliar, XEM (or NEM coins), is one of the most popular cryptocurrencies in the world. According to the Coincheck blog, they lost NEM 523,000,000 belonging to approximately 260,000 different users, of which they plan to repay ($0.81) per NEM back to those

"The Coalition is in the process of implementing refined guidance on privacy settings for wireless technologies and applications, and such technologies are forbidden at certain Coalition sites and during certain activities."
-US-led Coalition in Syria and Iraq

affected. It seems that the security of the NEM coins was lax, as they were stored in a 'hot wallet' which is especially susceptible to hackers and did not use multi-signature authentication. "Although blockchain technology has enabled Coincheck to identify the 11 addresses where the stolen coins ended up, and set up a tool for exchanges to automatically reject purchases made with them, hackers may still be able to use the funds via "tumblers."'

While the investigation into this hack is still underway, it sheds light on the growing concern over the security of cryptocurrency.In other related news, researchers from Proofpoint recently discovered a massive global botnet using EternalBlue SMB exploit to secretly mine Monero.

For those who use a public exchange, it is advised that you store much of your funds offline in a 'cold wallet.'

"In moving towards reopening our services, we are putting all of our efforts towards discovering the cause of the illicit transfer and overhauling and strengthening our security measures while simultaneously continuing in our efforts to register with the Financial Services Agency as a Virtual Currency Exchange Service Provider."
-Coincheck statement

For another story about unauthorized crypto mining, read this edition of UNMASKED.

#WIRELESS

The US National Security Council recently proposed building a 5G wireless network to protect against cyber terrorism. Although unlikely, it does raise some genuine security concerns.

Driving this proposal, is the idea that a government-run network would protect emerging technologies that will rely on super-fast 5G, like self- driving cars, and ensure the US remains a leader in wireless. Experts including the FCC Commissioners are very opposed to the idea, going as far as to say it is 'nonsense,' however, it has sparked renewed conversations over 5G, which is expected to connect more and more IoT devices. "I agree there are serious concerns relating to the Chinese government's influence into network equipment markets," said Virginia Sen. Mark Warner, a Democrat.

Previously, Tom Wheeler of the FCC prioritized 5G cybersecurity as a top concern but the current leadership believes the FCC "should not have authority to ensure wireless providers are building secure networks." In general, wireless security is severely lacking by modern standards because it was not designed to be. No one could have imagined the kind of cyber threats that would have emerged in 2018 when these networks were built. With 5G, more data will be recorded and stored more quickly in the cloud, which has privacy advocates concerned.

"The big problem is if even one carrier decides to skimp on protecting its equipment, that could still jeopardize everyone," states a white paper written by the FCC's Public Safety & Homeland Security Bureau.

It should be noted that wireless carriers such as AT&T are already on the path to building 5G networks of their own.

What can you do to secure your wireless network? Read 'State of the Art Wifi Security' to learn more.

""What this memo shows is that cybersecurity isn't just a privacy or civil liberties issue, but a national security and competition issue. Hopefully this will spark a much-needed conversation around privacy and security in our 5G networks." -Travis Le Blanc

FACT BYTE

More than 14.5 billion emails laced with malware were sent in 2017

-AppRiver Global Security Report

MEET THE INSTRUCTOR

SHANE MARKLEY

Threats to Industrial Control Systems have only continued to increase over the years, as much the technology these systems rely on is very oudated.

In his course, **ICS Security- Intro and Recon,** Cybrarian and Instructor **Shane Markley** provides guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, and distributed control systems (DCS).

Shane has over 17 years experience in the industry and currently serves as the VP of the Southern Nevada Cyber Security Alliance. He holds many industry certifications including CCISO, CISM, CISSP, GCIH, CEH, and ITIL.

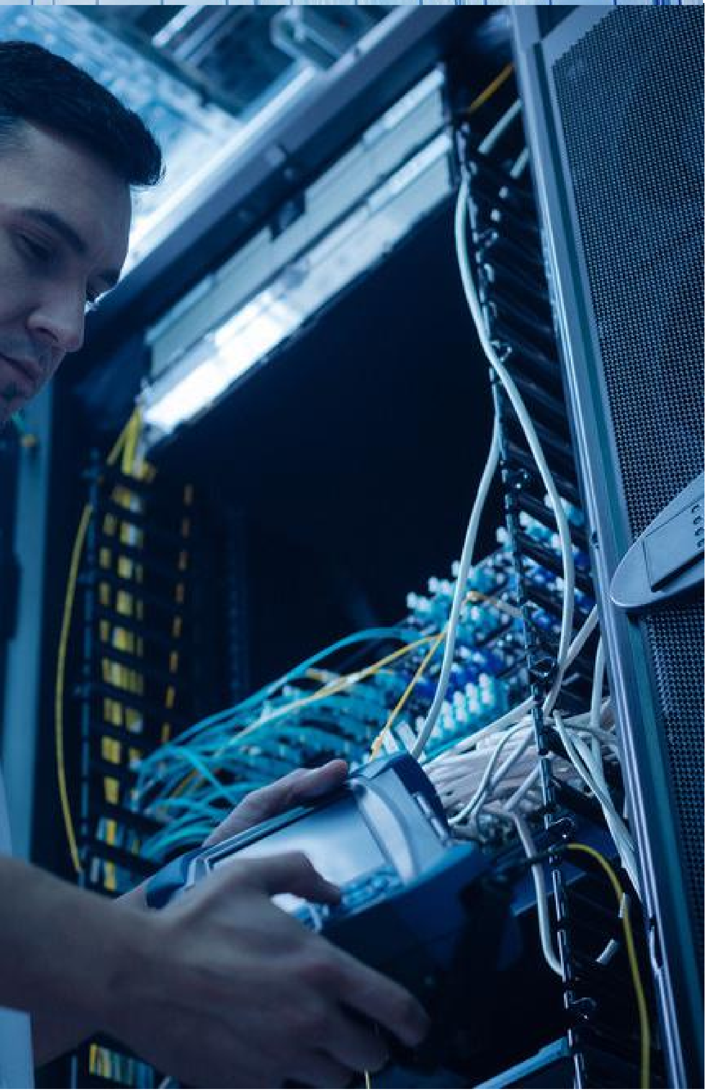
START COURSE NOW

Pivoting in Metasploit

In this Kali Linux tutorial, you will learn how to use Pivoting techniques in Metasploit. Discover vulnerable points inside your environment network using this method.

This course is intended for security enthusiasts and pentesters.

Dive Into the Course



Storm Mobile Pentesting device

Storm is a fully-loaded penetration testing platform equipped with a customized distro of Kali Linux that allows you to complete your ethical hacking training on-the-go.

A tailor-made system from **EC Council,** this piece of hardware is the next generation of practical training.

Take Hacking by Storm

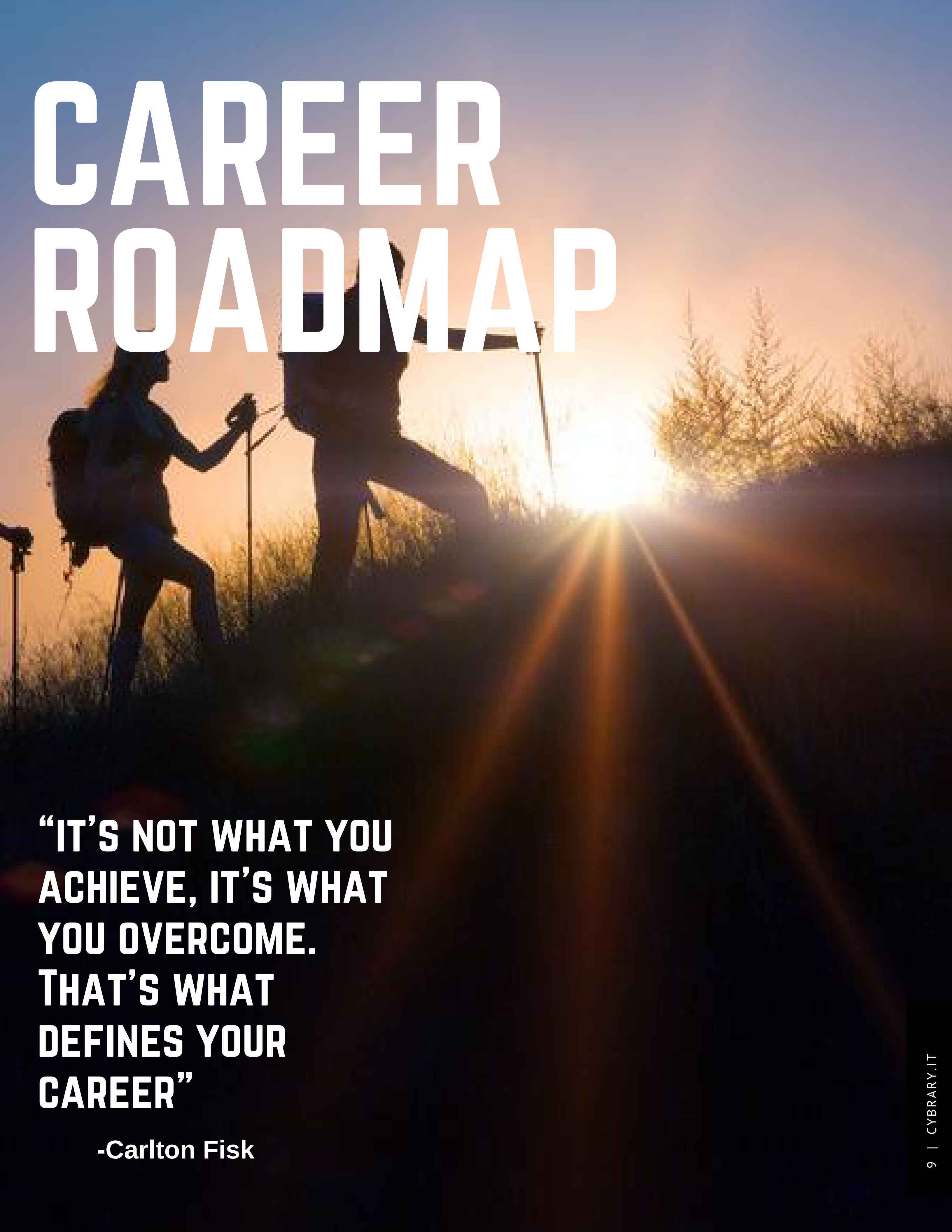
TRENDING SKILLS

Why Learn AWS?

"Whether you're a web developer, a database admin, a system admin, an IoT developer, a Big Data analyst, an AI developer (and the list goes on and on), your life will be made much easier if you take advantage of Amazon's platform. Their offerings touch almost every aspect of technology… They are constantly adding more offerings and innovating in a way that is leaving the competition in the dust."

Continue Reading

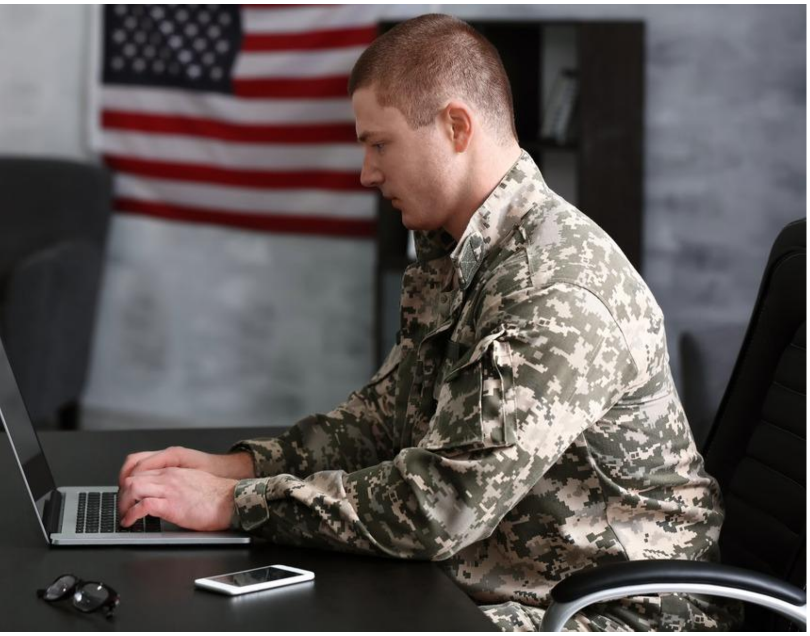
Teach an AWS Course



CAREER ROADMAP

"IT'S NOT WHAT YOU ACHIEVE, IT'S WHAT YOU OVERCOME. THAT'S WHAT DEFINES YOUR CAREER"

-Carlton Fisk



From soldier to cyber

Special Course for Transitioning military

Advice and personal journey from member Phill Kay

Whether you're transitioning from the military or just switching careers, this Cybrarian offers helpful advice on how to navigate the change. Phill shares his own experience, including the resources he used to skill-up in new areas.

While many cyber positions call for formal education and certifications, many employers are making exceptions for veterans, weighing more heavily a general experience combating threats and attacks.

Follow the Tenable Network Engineer Career Path on page 11 and prepare for a similar role using the guided coursework.

Watch Video

> Veterans are often ten steps ahead of their civilian counterparts when it comes to preparing for a career in cybersecurity. Individuals who have worked in intelligence positions during their years of service have often acquired cybersecurity training that is well suited for managing high-level IT security information.

Tenable Network Engineer

Required Knowledge & Skills

Follow the track of an industry leader's job description. Click the buttons below to view courses and supplemental materials that will put you on the path to this career

Knowledge of networks, TCP/IP ports, and protocols	▶	Network+
Knowledge of computer, network, and application security	▶	Security+
Knowledge of Tenable Nessus	▶	Nessus Fundamentals
Knowledge of Linux/Unix/Windows administration, and system configuration	▶	Administering Windows
Help customers understand vulnerability scan results, system audits, and/or log events	▶	CYBRScore
Provide technical assistance	▶	Network Troubleshooting
Recreate customer software issues in a lab environment for engineering assessment	▶	Wireshark

A LOOK INSIDE CYBRARY

Check out Cybrary's CEO and Co-Founder, Ryan Corey's latest interview on the joys and challenges of being an entrepreneur with USA Weekly

"As my role constantly evolves and new challenges arise, I need to continually shift to begin to solve the new set of problems. Therefore, reliance on amazing people who can handle the things I was previously working on, requires teaching them about the approach I took, and what may, or may not have worked. Then its key to let them take it fully over from there."

Get Insight from Ryan