UNMASKED

CYBRARY.IT

TAKING THE MYSTERY OUT OF CYBER SECURITY

JANUARY 2018 | EDITION 1

IN THIS ISSUE

EDITOR'S NOTE

2018 means a lot of new and exciting things at Cybrary. After a year of UNM4SK3D and a growing interest in cyber security news, we decided to expand the current scope and change the format to make this content more accessible for everyone.

Introducing UNMASKED 2.0, your source for the latest and greatest in the industry and at Cybrary, found in a new, easily downloadable format.

You'll still get the news updates you want, but you'll also take an inside look at tools to expand your learning experience on Cybrary and go further in your career.

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

#MALWARE

Never-before-seen features are usually a good thing, but not in the case of a complex malware strain.

Kaspersky Labs recently disclosed the new strain, 'Skygofree' which has the ability to eavesdrop on WhatsApp messages, collect private data from phones, and allow hackers to open reverse shell modules on targeted devices. It appears that the newest 'Skygofree' version has over 48 new, unique commands since its' original creation 3 years ago. One particularly nerve-wracking feature is its' ability to record audio surroundings vusing the microphone when an infected device is in a specified location.

A further look at the malware reveals traces back to the Italian firm Negg International, which provides app development, pen testing, and cybersecurity consulting services. 'Skygofree' was able to infect its victims through malicious redirects or man-in-the-middle attacks where individuals were redirected to landing pages that appeared to be from their mobile phone providers. Those landing pages then prompted victims to update their software for a speedier internet connection. Luckily, it seems only a few users in Italy have been affected. Kaspersky Lab researchers said "Skygofree's advanced spy features also included recording Skype conversations and the unique ability to capture WhatsApp end-to-end encrypted conversations via exploiting Android Accessibility Services designed to assist users with disabilities."

Protect your data from malware. Read 'Understand Unpredictable Threats: Advanced Malware.'

#SURVEILLIANCE

The US Intelligence community celebrated a small victory, while privacy advocates wallowed after the US House of Representatives passed the Foreign Intelligence Surveillance Act (FISA).

The renewal of Section 702, voted for by the majority of the House will allow for 6 more years of warrantless surveillance on US citizens which some argue is a "back door around the Fourth Amendment's prohibition against unreasonable search

"The implant's functionality has been improving and remarkable new features implemented, such as the ability to record audio surroundings via the microphone when an infected device is in a specified location; the stealing of WhatsApp messages via Accessibility Services; and the ability to connect an infected device to Wi-Fi networks controlled by cybercriminals"
-researchers Nikita Buchka and Alexey Firsh

and seizure." Those in favor of the renewal of FISA argued that it will help to prevent major foreign terrorist attacks. From a bipartisan perspective, many support the collection of information for foreign intelligence but are concerned when innocent Americans are 'incidentally' included in the surveillance.

Many in the Senate, including Rand Paul and Ron Wyden have sponsored the USA Rights Act, which "would mandate reforms to 702, including a requirement for intelligence agencies to have a warrant before they can conduct even incidental surveillance of citizens." Among the privacy advocates against FISA, data has been cited from a Washington Post examination of 160,000 emails and instant messenger conversations collected under Section 702 between 2009 and 2012, and found that 90% of them were from online accounts not belonging to foreign surveillance targets. Instead, nearly half contained information belonging to US citizens or residents. The Senate still has to vote on the renewal, but in the meantime, you can expect the debate over surveillance to continue.

"Because of these votes, broad NSA surveillance of the internet will likely continue, and the government will still have access to Americans' emails, chat logs, and browsing history without a warrant."

Concerned about your PII? Read '15 Ways to Protect Your Privacy right Now.'

#VULNERABILITIES

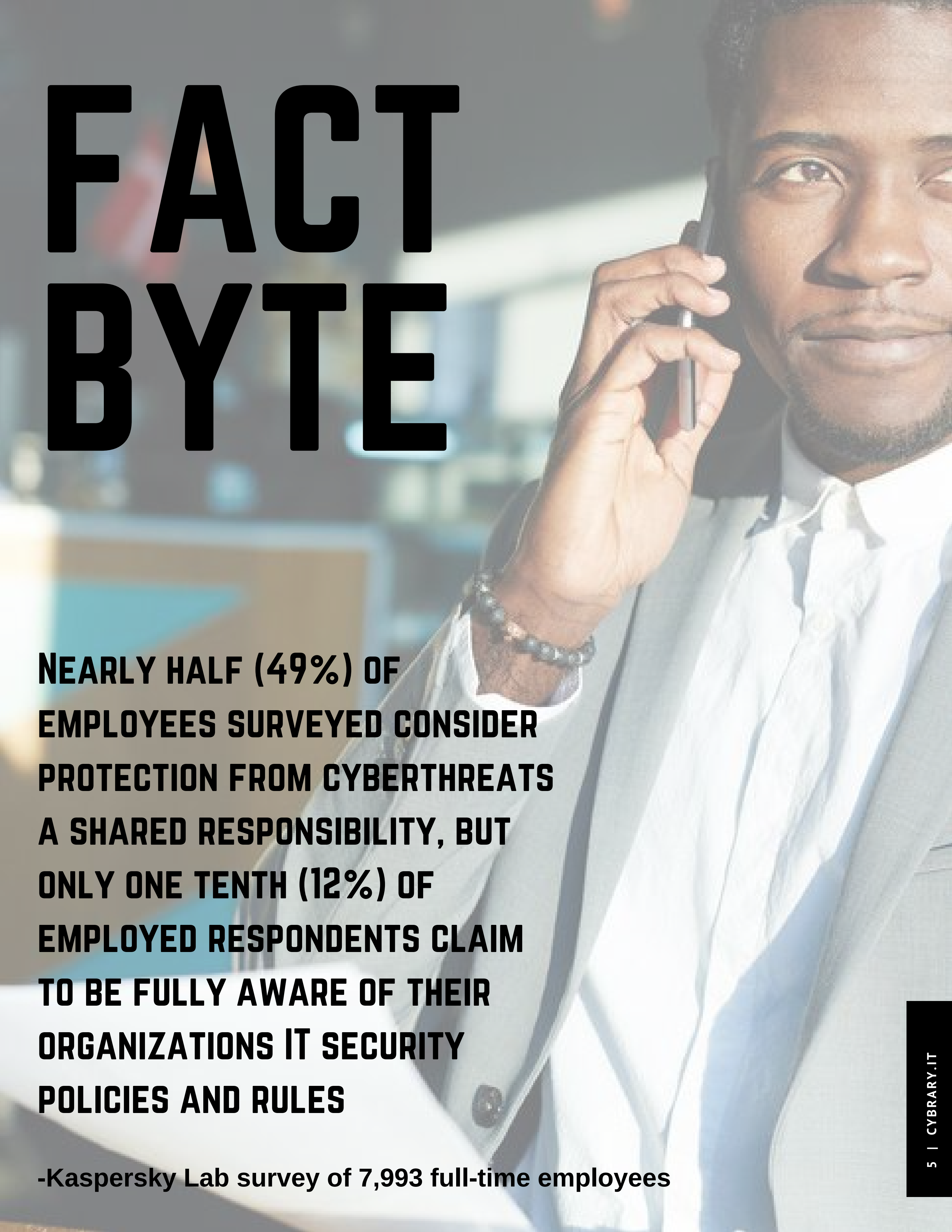
If you're a fan of browser extensions, you may want to think twice before your next download. Researchers from ICEBERG discovered 4 malicious extensions in the official Google Chrome Web Store.

With over 500,000 individuals impacted from the 4 extensions, Stickies, Nyoogle, Lite Bookmarks, and Change HTTP Request Header, the security implications are serious. Google has since removed all but Nyoogle from the extension marketplace for reasons unknown. The vulnerabilities were first discovered after ICEBERG noticed a suspicious jump in outbound network traffic from a workstation at a customer site. Likely used for click-fraud and search engine optimization manipulation, researchers wrote the extensions "provided a foothold that the threat actors could leverage to gain access to corporate networks and user information."

Although Google has been working to create enterprise-friendly security features for managing extensions, security experts are concerned that those whose extensions are not under scrutiny by company secure teams still pose a large risk."Coupling an extension marketplace style 'easy install' for users, limited understanding of the underlying risks, and few compensating controls leaves organizations vulnerable to a serious and easily overlooked attack vector," wrote researchers Justin Warner and Mario De Tore. It's important to note Chrome has about 60% of the overall browser market, making it a desirable target for criminal exploitation, but is still considered one of the safest browsers.

Want more customization for your browser? Explore further in 'Workarounds for Chrome.'

"When an extension does enable the 'unsafe-eval' permission to perform such actions, it may retrieve and process JSON from an externally-controlled server. This creates a scenario in which the extension author could inject and execute arbitrary JavaScript code anytime the update server receives a request." -ICEBERG researchers



FACT BYTE

NEARLY HALF (49%) OF EMPLOYEES SURVEYED CONSIDER PROTECTION FROM CYBERTHREATS A SHARED RESPONSIBILITY, BUT ONLY ONE TENTH (12%) OF EMPLOYED RESPONDENTS CLAIM TO BE FULLY AWARE OF THEIR ORGANIZATIONS IT SECURITY POLICIES AND RULES

-Kaspersky Lab survey of 7,993 full-time employees

NEW TO THE CATALOG

SECURE CODING COURSE

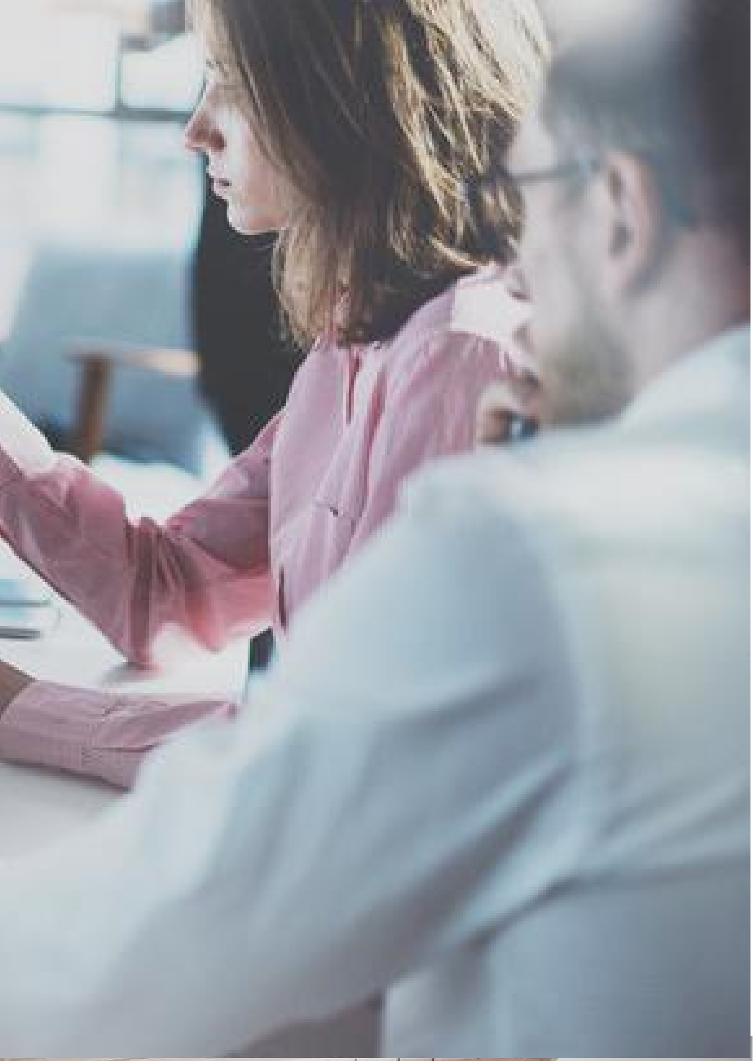
VERACODE

The Secure Development, Programming, and Coding course is comprised of a set of Application Security (AppSec) tutorials that provide information on how hackers perform a specific attack on vulnerable software and how you can fix vulnerable code to prevent those types of attacks.

Provided by Veracode, the industry's leading source code security analyzer, this course consists of 7 modules that cover a number of different application security flaws, and how to protect against them.

Cover relevant topics such as: XXS, SQL Injection, Open redirects, and Information leakage, taught by industry experts, free.

START COURSE NOW



E-Books

30BIRD MEDIA

E-Books from 30Bird Media will help you prepare for an upcoming certification or learn new skills in Microsoft Office.

With features like note taking, spoken word, and the ability to print off pages, these E-Books are excellent supplemental materials for courses.

Security+ E-Book

The Art of Exploitation Lab

Learn from scratch how to find a vulnerability or weakness in any system. This lab contains four exercises which will help you gain practical experience while taking **the Art of Exploitation Course from Mohamed Atef.**

Discover how to write an exploit using Python script and use it to hack a system affected with Buffer Overflow.

Explore Lab

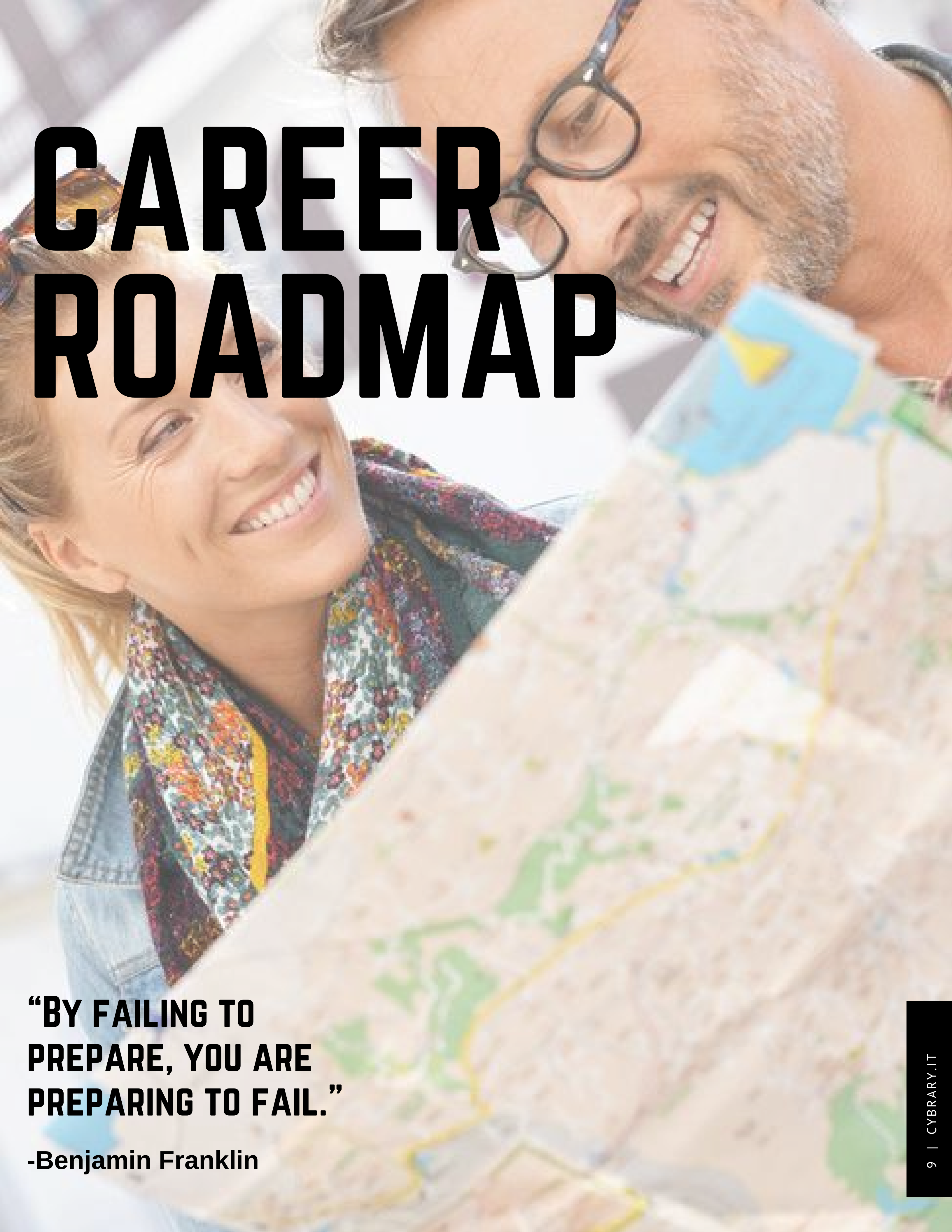
INTERVIEW ASSESSMENTS

Interview Mocha

Assessments designed by InterviewMocha Subject Matter Experts gauge the skills of professionals, so they can better tailor their learning to improve on weaknesses and determine if they are capable of filling their desired role.

Using powerful reporting, get a detailed analysis of the test results to help gauge your readiness for a position. You will get a measure of your strengths and weaknesses amongst learning objectives and industry-recognized competencies such as **Cyber Security Fundamentals, Data Science and Analytics, AWS Web Services, and Basics of Software Programming Assessment.**

Browse Assessments



CAREER ROADMAP

"By failing to prepare, you are preparing to fail."

-Benjamin Franklin

Cyber Security Incident Responder

Required Knowledge & Free Courses

Click the buttons below to view courses

Computer Networking concepts, protocols, and security	▶	Network+
Cyber threats and vulnerabilities	▶	CRISC
Incident response methodologies	▶	Incident Response
System and application security threats and vulnerabilities	▶	Secure Coding
Cyber defense and information security policies	▶	CISSP
Different classes of attacks and attackers	▶	CASP
Malware analysis concepts and methodologies	▶	Malware Analysis
The Cyber Kill Chain	▶	Hacking & Forensics

Required Skills & Experiential Learning Tools

Click the buttons below to view labs

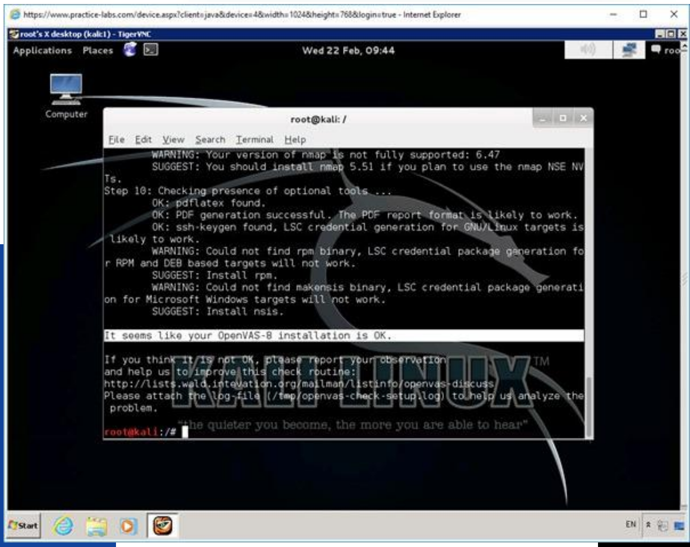
Identify, capture, contain, report malware ▶ **Hacker's Paradise**

Recognizing and categorizing types of vulnerabilities and attacks ▶ **Ethical Hacking Virtual Lab**

Protecting against malware and performing damage assessments ▶ **CYBRScore Virtual Labs**

Design incident response procedures ▶ **Security+ Virtual Lab**

Detect host and network-based intrusions ▶ **CASP Virtual Lab**


https://www.practice-labs.com/device.aspx?client=java&device=4&width=1024&height=768&login=true - Internet Explorer
root's X desktop (kali:1) - TigerVNC
Applications
Places
Wed 22 Feb, 09:44
Computer
root@kali: /
File
Edit
View
Search
Terminal
Help
KALI LINUX TM
"the quieter you become, the more you are able to hear"
Start
EN

```
        WARNING: Your version of nmap is not fully supported: 6.47
        SUGGEST: You should install nmap 5.51 if you plan to use the nmap NSE NV
Ts.
Step 10: Checking presence of optional tools ...
        OK: pdflatex found.
        OK: PDF generation successful. The PDF report format is likely to work.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is
 likely to work.
        WARNING: Could not find rpm binary, LSC credential package generation fo
r RPM and DEB based targets will not work.
        SUGGEST: Install rpm.
        WARNING: Could not find makensis binary, LSC credential package generati
on for Microsoft Windows targets will not work.
        SUGGEST: Install nsis.

It seems like your OpenVAS-8 installation is OK.

If you think it is not OK, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the
 problem.

root@kali:/#
```

> An experienced Incident Responder knows exactly what needs to be identified for an attack and where to find it. By providing accurate, informative feedback, an organization can quickly resolve any issues or threats that may presents themselves in their environment.
>
> -Chris Wreckley

A LOOK INSIDE CYBRARY

> In my opinion, preparing professionals to perform at jobs, in the fastest moving industry on the planet, required a model that could move equally as fast.

AN INTERVIEW WITH RYAN COREY, PRESIDENT AND CO-FOUNDER

"The old way of talent development in this space was to send people to over-priced, week-long training classes that cover one particular skill. The other option was to send people to a two or four-year degree program with stale, stagnant, often outdated content...

We then decided to make Cybrary completely frictionless, with free video training, because we wanted no barriers, so that those who would not participate previously, now have no barriers preventing them from participating currently. This is similar to how Uber scaled the ride-hailing market."

READ RON GULA'S FULL INTERVIEW OF RYAN ON MEDIUM, HERE.