Ethical Hacking

The Comprehensive Guide for Beginners

simplilearn

Topics Covered

Introduction: Hackers Exploit Dangerous New Threat Vectors

As the world continues to go digital in a big way, companies are allocating tremendous resources to protect their vital digital assets. Whether it's massive customer or patient databases, proprietary product specs, mission-critical applications, financial assets, or communications platforms, it's getting harder and harder to protect so many things from so many potential attack vectors.

Bad actors that include hackers and cybercriminals continue to find vulnerabilities in corporate networks and infrastructure, and there are a multitude of threat vectors that cyber security professionals must have on their radar. According to a 2020 report, malware was the top attack technique at 40 percent, account hijacking second at 21 percent, and targeted attacks third at just over eight percent.

Other attack vectors include malicious spam and script injections, IoT and device vulnerabilities, phishing and business email compromise, DDoS attacks, API exploits, and the list goes on and on. Data breaches, furthermore, cost enterprises an average of $3.92 million, according to CSO Online, so there is certainly a lot at stake.

Ethical Hacking to the Rescue

Considering the list of attack vectors, if it sounds like cyber security professionals have an uphill battle, you're absolutely right. The difficulty is that as well trained as many cyber security professionals are, they are usually playing catch-up against hackers and cybercriminals that have financial incentive and extensive experience to keep their game at peak performance. That's where Certified Ethical Hackers (CEH) become an invaluable resource for companies and government organizations.

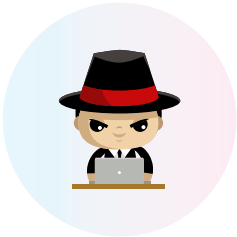
What is ethical hacking? It is the process of testing infrastructure and application vulnerabilities by using the same techniques that malicious hackers do, but in a legal, legitimate manner. The results of a CEH professional's testing can then be used to proactively enhance the strength of an organization's defensive cyber security posture. Ethical hackers learn to investigate vulnerabilities in target systems, assess security status of network systems, and master the latest hacking tools, malware codes and other tactics that hackers use every day. Suffice it to say they are among the most valuable security assets employed today. Those with CEH certifications on average earn about 10 percent higher salaries than comparable cyber security experts at the same level.

Certified ethical hackers have become the tip of the spear when it comes to building a comprehensive cyber security protocol. And the results of taking aggressive action are compelling. Accenture reports that improving cybersecurity protection can lower the cost of cybercrime and generate new revenue opportunities, with the total value of risk reaching an estimated $5.2 trillion globally in the next five years. Prioritizing cybersecurity measures by hiring CEH professionals can unlock future economic value and generate better trust with customers.

A Quick Primer on Hacking

Hackers typically fall into three basic categories, each of which identify their intentions and methods, and their names speak volumes about their objectives.

This primer highlights the key details:



Black Hat: Black hat hackers seek to steal or modify data for their own financial or illicit gain, or simply to wreak havoc on an organization. They have extensive knowledge of how to penetrate layered security protocols. Black hats are the ones you usually read about in the media and are the ones companies fear most.

White Hat: White hat hackers are the good guys, the "ethical hackers," who have permission from the organization before looking for exploits. They might either be employed by a specific company or be hired contractually to perform their work.

Grey Hat: Grey hat hackers are the middle category, not necessarily malicious but will want to be compensated for finding and reporting an exploit. They usually don't have permission to look for exploits, and they usually also don't care.

How Some Ethical Hackers Get Started

You certainly don't need to have an extensive background in hacking to become a certified ethical hacker, but knowing how some got started can put it all into perspective. Take the example of Matt Jakubowski in a recent account, who leads cybersecurity operations at the analytics company Uptake. As a younger man, in addition to spending hours digitally dissecting video games, he spent time with friends trying to hack each other's programs. They built phishing sites to bait each other into opening malicious links, which taught them to notice minor differences between legitimate and hacker sites.

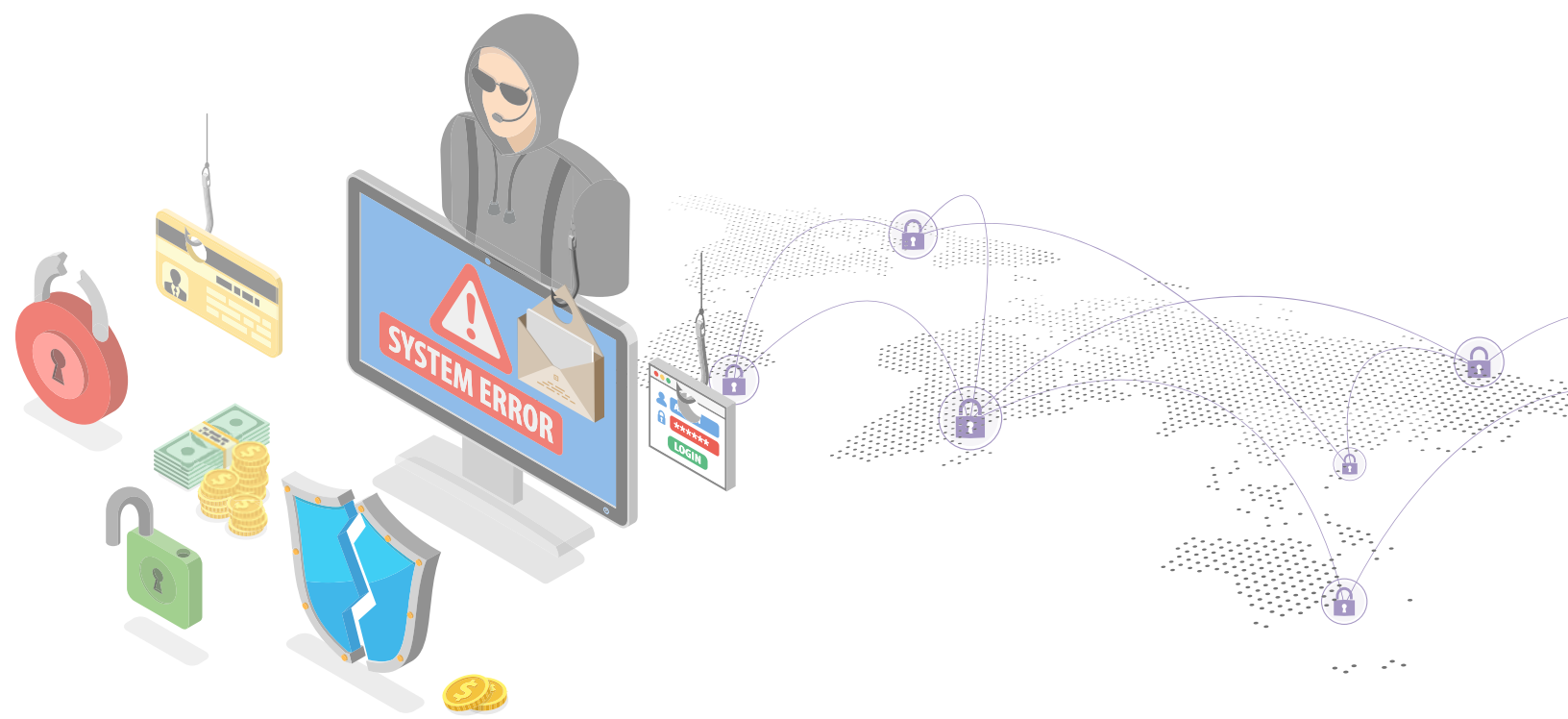
> "We learned how to secure ourselves better, but we also learned new tricks that really helped us advance in a completely legal way,"

Jakubowski says in the article. Now his job at Uptake is to prevent or mitigate that type of illicit activity. He credits his early years of friendly hacking for giving him the technical underpinning that keeps him on his toes every day.

Ethical Hacks Come at the Right Time for Many

It isn't just internal networks that can be compromised and damaged. In the new world of COVID-19 lockdowns, companies and millions of individuals have turned to video conferencing to communicate and even pass the time. Many use the Zoom product to do so, but a vulnerability was recently discovered by a security researcher. According to the news report, the vulnerability in a Mac computer's Zoom Client allowed any malicious website to initiate a user's camera and forcibly join a Zoom call without permission. It also allows a website to launch a denial of service (DoS) attack by repeatedly joining a user to an invalid call. Even if the Zoom app is uninstalled, a hacker could re-install without permission through a locally-hosted web server.

The security issue affected as many as 750,000 companies that use Zoom on Macs. The security liability came about from a very simple feature in the product: being able to invite anyone to a meeting with a web link. After the vulnerability was disclosed, the company issued a quick-fix at first and continues to make additional modifications to keep the product safe.



Even Big-ticket Software Programs Can Be Vulnerable

Even the largest of tech companies can be prime targets to hackers, and it's up to the white hats to stay ahead before damage is done. An example of an unpatched bug in Windows' cryptographic library was recently revealed by a Google vulnerability researcher in June 2019.

As reported, the researcher revealed the security issue in SymCrypt, the core cryptographic library for Windows, a vulnerability that could potentially compromise an entire Windows fleet. He reported the vulnerability and heard back from Microsoft that they would issue a fix in an upcoming patch run. It ended up being fixed in a later run a month later, but the report had been issued and helped to solve the security issue. Cases of ethical hacking like this can positively impact millions of individuals.

How a Single Hacker Can Do So Much with So Little

We read a lot about syndicates who hack networks, but it's not always larger groups (like, say, Russian hackers that launch attacks on American companies and political organizations). It can be a single individual too, and the attacks don't even need to be very sophisticated to be successful. A great example was highlighted by cyber expert John Strand in a commentary called How I Would Hack Your Network (If I Woke Up Evil), where he summarizes the steps he would take to penetrate a corporate network. His nefarious steps were outlined as follows:

1. Bypass antivirus (AV) software. Most hackers can easily get past AV security so you can't rely on it as a firewall of protection.

2. Target the user population through social engineering-driven phishing attacks. He cites the fact that 20-30 percent of users will click on anything, so it's an easy action to exploit.

3. Couple that with a hacker's ability to research what topics you are interested in (such as your political posts on social media) and the chances for a breach go way up. Social media reconnaissance is a key way hackers find out details about users to make them easier to exploit.

4. Password-spraying web interfaces like Outlook Web Access, which is basically trying a single password on many user accounts that shouldn't be exposed externally.

5. Pivot once you're inside, by using post-exploitation tools to identify other systems to access files and folders once you've penetrated the outer defense.

Conclusion: Get on the path to becoming a Certified Ethical Hacker (CEH)

No matter what your background is, there is ample opportunity to propel your career to new heights by becoming a Certified Ethical Hacker. Even for beginners, the course curriculum for CEH certification can be challenging, exciting and rewarding. Courses are ideal for almost anyone with an interest in helping companies protect cyber assets, while learning the exploits that hackers use in today's digital world.

Certified Ethical Hacker (CEH) certification is ideal for network security officers and practitioners, site administrators, IS/IT specialists and analysts, IS/IT auditors, IT operations managers, IT security officers, network specialists, technical support engineers, senior systems engineers, and systems analysts. The learning path covers a range of fascinating topics, including:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Motivated learners can even parlay the CEH degree into an advanced learning path that can transform you into a certified cyber security expert. The Cyber Security Expert Master's program includes CEH certification as well as many more certs, including CISSP (Certified Information Systems Security Professional (long considered to be the gold standard in the field of information security), CISM (Certified Information Security Manager, a key certification for IT professionals who manage, design, oversee and assess enterprise information security), as well as CompTIA, and Certified Cloud Security.

The cyber security field is entering a golden age of activity and excitement, and opportunities abound for anyone who wants to learn how hackers ply their trade and use that knowledge for protecting cyber assets, not stealing them.

simplilearn

Founded in 2009, Simplilearn is one of the world's leading providers of online training for Digital Marketing, Cloud Computing, Project Management, Data Science, IT Service Management, Software Development and many other emerging technologies. Based in Bangalore, India, San Francisco, California, and Raleigh, North Carolina, Simplilearn partners with companies and individuals to address their unique needs, providing training and coaching to help working professionals meet their career goals. Simplilearn has enabled over 1 million professionals and companies across 150+ countries train,certify and upskill their employees.

Simplilearn's 400+ training courses are designed and updated by world-class industry experts. Their blended learning approach combines e-learning classes, instructor-led live virtual classrooms, applied learning projects, and 24/7 teaching assistance. More than 40 global training organizations have recognized Simplilearn as an official provider of certification training. The company has been named the 8th most influential education brand in the world by LinkedIn.

For more information, visit www.simplilearn.com.