PECB Insights

ISSUE 27 ISO STANDARDS AND BEYOND JULY-AUGUST 2020

ETHICAL HACKING AND THE PRICE OF VULNERABILITY

The previous issue of the PECB Insights Magazine at a glance

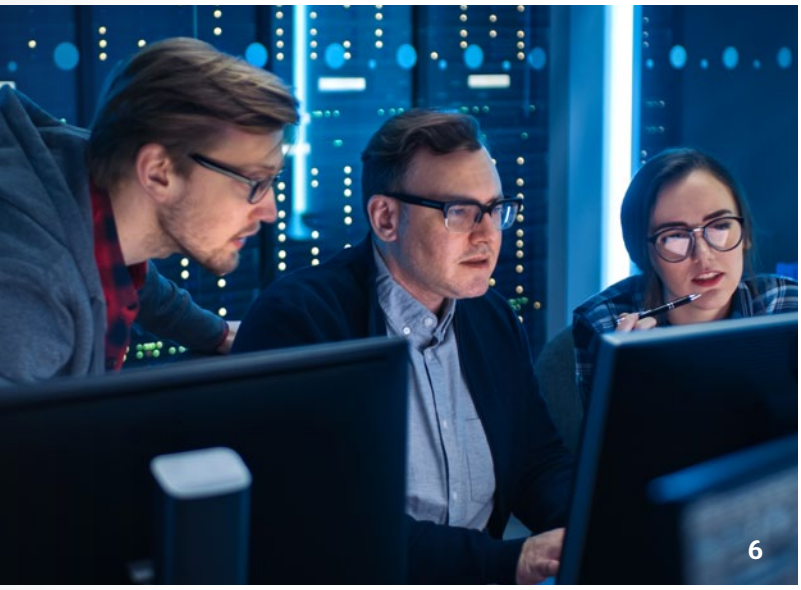
- Business Continuity Planning in a Post-COVID-19 World
- Leading with Courage through Crisis
- The Word of the Day Is Not Virus, It Is Agility
- Meet Some of the Most Secure Software Apps in Existence
- Strong Partnerships for Greater Success: Volodymyr Tkacheno's success story
- Crisis Management Lessons Learned on Embedding and Adapting Your Business Continuity Planning
- A Royal Touch of Copenhagen, Denmark
- Business Continuity: From a Best Practice to a Priority Objective
- Learn the Art of Moving on with Your Business

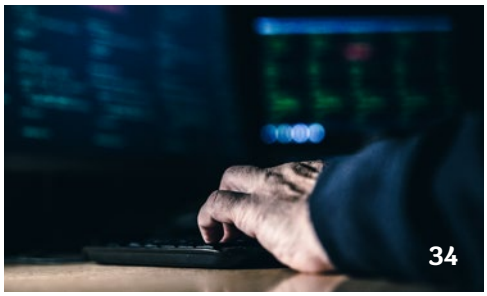
→ READ NOW

HAVE YOU SEEN
OUR RECENT ISSUES?

→

In This Issue





The views and opinions expressed in the PECB Insights Magazine do not necessarily reflect the views of PECB Group.

Copyright © PECB 2020. All rights reserved.


“There’s no silver bullet solution with cyber security. A layered defense is the only viable defense.”
James Scott
Institute for Critical Infrastructure Technology

Why Hire an Ethical Hacking Firm or Ethical Hacker?

The increasing rate of cyberattacks on organizations around the globe has produced huge financial gains for cybercriminals. The vast number of threats includes “Insider attacks,” “Malware,” and now the emergence of COVID-19 threats to mention a few. If these threats are not addressed, there is a likelihood that some organizations may be exposed to higher risks of cyberattacks for years to come.

Cybersecurity Risks and COVID-19

The unexpected outbreak of COVID-19 has increased existing threats and made some organizations defenseless as the reliance on technology grows. Threats emerging from the situation with the pandemic, malwares, remote working, phishing and business emails, and supply chain threats are escalating.

What is Ethical Hacking?

Hacking refers to exploiting weaknesses in a computer network or system to obtain unauthorized access to information; a hacker is a person who tries to hack into computer systems.

Ethical hacking is an approved and systematic process of bypassing system security to identify potential data breaches and threats in a network. The organization that owns the system will give special permission to an Ethical Hacker to perform security assessments. The core steps are: reconnaissance, scanning, exploitation, and maintaining access.

These methodologies allow common vulnerabilities that exist within a system to be discovered and remediated. Ethical hacking or penetration testing also assesses the administrative, technical, and operation controls and policies within an organization's system. These manual and automated methodologies provide thorough evaluation of assets and risk prioritization and mitigation recommendations. Penetration testing teams can also deliver customized social engineering assessments to determine the resilience of employees and processes.

The Role of an Ethical Hacker

An Ethical Hacker is a security expert that has the experience and skills in IT security and has knowledge of various programming languages such as HTML, PHP, Python, SQL, and JavaScript, networks, and computer devices. The objective of an Ethical Hacker is to support organizations in securing and protecting corporate assets. The Ethical Hacker is usually an independent consultant and does not have any affiliation with the organization.

Various Types of Hackers

There are three different types of hackers. Black Hat hackers are individuals who illegally hack into a system for monetary gain. White Hat hackers are individuals who exploit the vulnerabilities in the system by hacking into it with permission in order to defend the organization.

White hat hacking is absolutely legal and ethical. This is also often referred to as penetration testing. In addition to these hackers, we also have the Grey Hat hackers, as the name suggests, the Grey Hat hacker is a combination of both white and black hat hackers. These hackers discover vulnerabilities in the system and report it to the system's owner; Grey Hat hackers may not seek the organization’s approval. On occasions, Grey Hat hackers also ask to be compensated financially in return for the identification of vulnerabilities.

Regardless of the method used, the techniques and tools tend to be similar between the methodologies. The use of methodologies does provide some significant advantages, and can be used to find the threats to a system or network using well-known attack vectors.

Vulnerabilities discovered by Ethical Hackers include:

- Injection attacks
- Broken authentication
- Security misconfigurations
- Use of components with known vulnerabilities
- Sensitive data exposure
- Social engineering
- Input validation
- Insecure or misconfigured services

Once vulnerabilities are identified, the Ethical Hacker will exploit them and may ultimately gain access to a system. An Ethical Hacker would also attempt to break into systems that do not necessarily have a known vulnerability, but are simply exposed. Ethical Hackers will then document their findings and evidence to report back to the organization or client.

Identifying Risks Using Bug Bounties Ethical Hacking

Bug bounties can be used to strengthen an organization’s security posture. Security researchers can find out bugs to the system before the cybercriminal does. These programs are highly monetized and help reduce cybercrime and protect privacy. The rewards are paid on when the Ethical Hacker finds vulnerability and reports are submitted to the client.

The core difference between bug bounties projects and an independent Ethical Hacker is that bug bounties are open to all while Ethical Hackers are outsourced to one consulting firm.

The Threat of Cyberattack

Cyberattacks does not discriminate against the size of an organization, actually the size is quite irrelevant. Particular areas of interest include the end points on various mobile platforms, networks, and web applications. The idea is to prevent these cyberattacks occurring in the first place.

The Ethical Hacker needs to think and behave like a hacker. The Ethical Hacker has been given approval by the organization to hack their network and perform various penetration tests.

Cyberattack Research and Statistics

A research carried out by Accenture, Ninth Annual Cost of Cybercrime study, states that "The impact of these cyberattacks to organizations, industries and society is substantial. Alongside the growing number of security breaches, the total cost of cybercrime for each company

increased from $11.7 million in 2017 to a new high of $13.0 million — a rise of 12 percent" and 68% of business leaders feel their cybersecurity risks are increasing.

The Cybersecurity Challenge

Organizations will have cybersecurity controls in place to manage risk. However, there can be weaknesses in their security controls. End users are classed as easy targets by cybercriminals. There is a massive challenge in protecting all digital data, such as corporate login credentials and Personally Identifiable Information (PII). There have been several instances of these attacks. One occurrence was the highly destructive WannaCry Ransomware attack.

The emergence of WannaCry began in May 2017 in the Asian region and rapidly spread around the world. In 24 hours, more than 203,000 vulnerable computer systems were infected across 160 countries.

Data files were encrypted and users were unable to access information. A typical denial of service attack. The cybercriminals demanded a ransom payment of up to $600 Bitcoin.

The systems affected were already vulnerable — one cause of the vulnerabilities was that the systems were not updated with the latest Microsoft Operating System 2017's security updates. Organizations affected, including Nissan and FedEx, were heavily affected as this resulted in loss of production and downtime.

Cybersecurity as the practice of protecting networks and computer systems from unauthorized digital attacks, in 2018 WannaCry cyberattack cost the NHS £92m as 19,000 of appointments were canceled. The devastating global cyberattack that crippled computers in hospitals across the UK. £72m in the subsequent cleanup and upgrades to its IT systems.

How Was the WannaCry Attack Delivered?

The approach, although not unique, was delivered via email. The recipients were fooled using social engineering methods to open attachments and releasing malware onto their system through a technique known as phishing. Once a computer has been affected, it locks up the files and encrypts them in a way that cannot be accessed by the data owners. The cybercriminal then demands payment in bitcoin in order to regain access to files and data.

Probably, if an Ethical Hacker was hired in this case to conduct Penetration Testing in vulnerable systems and

operating systems, it would have identified, tested, and patched and this would have kept the network secure before the cyberattack. Customer data would have been protected, productivity would have been increased, and negative reputational damage avoided. The key thing for any organization to focus on, first off, are the threats and attention to critical and sensitive data which need protection.

Why Hire an Ethical Hacker or Ethical Hacking Firm?

1. Organization liability

Sharing the risk by hiring an Ethical Hacker or Ethical Hacking firm not only helps the organization's posture, it also demonstrates commitment to security. It can limit liability if the threat of a cyberattack is realized. Of course, based on other published attacks, the effects usually include data leakage and the publication of PII, customer, and even employee data. There are national and international regulations and standards which an organization will need to adhere to, such as GDPR, HIPPA, and PCI DSS.

2. Reduced risks and costs in the long term

The cost of testing may depend on the size and the assets of an organization. As part of testing controls and physical assets such as firewalls and servers are usually costly to maintain. However, the total cost of ownership compared to investment in protecting and managing cyberattacks can be justified to the top management and the board.

An ethical hacking firm or consultant can be hired in order for systems to be safeguarded. This is now a necessity as attacks no longer fall under "if" it will happen rather "when" they will happen.

3. Organization transition to Cloud

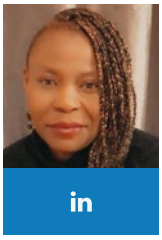
Outsourcing to the Cloud and virtualization are now the norm. There have been concerns with the security of data within the cloud and the management of security given to Cloud Service Providers. Ethical Hackers can assist in testing companies' assets without compromising security.

"Cloud testing is a form of software testing in which web applications use cloud computing environments to simulate real-world user traffic." Verification of security controls and security consulting firms already provide cloud-based testing services such as performance testing, load testing, and web-based application testing, as well as the testing of environments hosted in the cloud as WAF (web application firewall), encryption, and configuration to ensure in-depth defense within various levels are still operational.

Testing in the cloud can be quite complex. This complexity can be managed by Ethical Hackers as they possess special technical skills and are experienced in writing scripts and applying test cases.

> **As the number of cyberattacks continues to increase, ethical hacking should be considered as part of an organizations' ongoing security strategy. Utilizing third-party expert security consulting firms can enable an organization to be ahead and detect issues proactively.**

It will also help organizations avoid becoming victims of cyberattacks and serve as evidence that they are meeting their legal and contractual obligations. For more, deploying expert Ethical Hackers can help to become more proactive in managing cyber risks.



in

About the Author

Christie Ogubere
Information Security Consultant

Christie Ogubere is a Cyber Security Consultant at Intex IT and advises businesses on how to protect their networks, applications, and information assets from malicious attacks or errors from employees, criminal hackers, and unforeseen events. Christie has over 22 years of experience in different fields of information technology and security, specialized in Risk Management, Vulnerability Assessment, Penetration Testing, and Physical Security. Christie has a passion for solving business cybersecurity challenges through understanding the problem.

Christie has consulted for various companies as a Security Consultant and Trainer where she has conducted Physical Security and Pen testing reviews. She has a degree in Computer Studies and a master's degree in Computer Forensics and System Security from the University of Greenwich. Christie holds certifications in ISO/IEC 27001, ISO/IEC 27005, CISSP, and Ethical Hacking.

As a Trainer, Christie has delivered a lot of corporate training to IT as well as Infosec professionals in courses such as CISSP, CEH, CISM, ISO/IEC 27001 Lead Implementing, Lead Pen tester, Risk Management, and Cyber Security Awareness. Christie is a member of ISACA and ISC².

Cyber Risk is a Business Issue and Responsibility, Not Just a Matter for Experts

The rapid adoption of cloud and mobile technologies has significantly extended the attack surface, even the threat landscape itself has continued advancing constantly. IT organizations are feeling the squeeze to respond to business requirements while ensuring the security of corporate information.

Information and communication technologies have evolved over the last two decades and are now integrated virtually into every aspect of our lives. Innovations in business and technology have woven a rich and complex texture of network, improved through the multiplication of the internet, and lately the rise of promptly accessible cloud-based solutions.

Be that as it may, as companies become more deft and creative through the rise of digital reach, new and ever-present vulnerabilities have risen. On any given day, there are numerous media reports about significant cyber incidents. Organizations of various kinds and sizes are susceptible to cyberattacks. Which information, systems, and assets are of incentive at a specific point in time depends on the cyber attacker's motives.

Rules of Cyberspace and Territorial Sovereignty

Does the concept of sovereignty apply to cyberspace? Cyber attackers do not respect jurisdictions. All countries, especially profoundly connected ones, advantage from global participation in securing worldwide infocomm infrastructures and responding to cyber threats. Today, we have more telephone lines than individuals. Almost all households have rapid broadband internet access. Be that as it may, dependence on infocomm technologies also makes us vulnerable. Cyber threats and attacks are getting more sophisticated, with more severe consequences. We cannot underestimate cybersecurity. As a leader, you should be resolved to shield essential services from cyber threats, and to make a secure cyberspace for businesses and communities.

Leaders should work closely with different organizations and network to fabricate consensus in cyber norms, strengthen limit, and address cyber threats and crimes.

It is crucial that leaders understand the national and international aspects of sovereignty issues in cyberspace. The determination of what constitutes cyber sovereignty will greatly influence the identification and understanding of threats and the preparation of the battlefield, the development of capabilities, the identification of participants, and planning for cyberspace operations. Considering the stakes, leaders cannot afford the consequences of allowing the attacker to define the boundaries of cyber sovereignty and the rules of cyberspace engagement.

Together, leaders can manufacture a resilient and trusted cyberspace for their organization.

Fear of the Consequences — Making and Implementing Effective Cyber Strategies

In this day and age we see comments like: the attackers have so far not used their most developed cyber weapons not to uncover their actual capabilities, the consequences of a full-scale cyber war cannot be anticipated, and what

could happen could destroy a cutting-edge nation. It is of crucial significance to have a secure cyberspace and a cyber power that will also give fear of the consequences. It should not be overlooked that what is essential and significant in cyber discouragement is the execution of cyberattacks/war at the perfect time, on the correct objective, and with the correct techniques and methods. In the event that triumph is desired in case of cyber fighting, a holistic methodology, addressing cybersecurity in the entirety of its dimensions, should be received and more compelling and hindrance policies should be drafted and executed earnestly. What are the gaps and vulnerabilities caused by or resulting from a need of substantive, comprehensive cyber strategy? Are there ways to address them that may be adequate to every single applicable party? These are some questions you should answer.

Announced breaches are currently 60 times higher from a decade ago. Cybersecurity cannot remain the worry of the CISO alone. Business leaders must rather move to work with their CISO and buy large security resources to effectively check their new dependencies, and the investment in risk treatments that are justified.

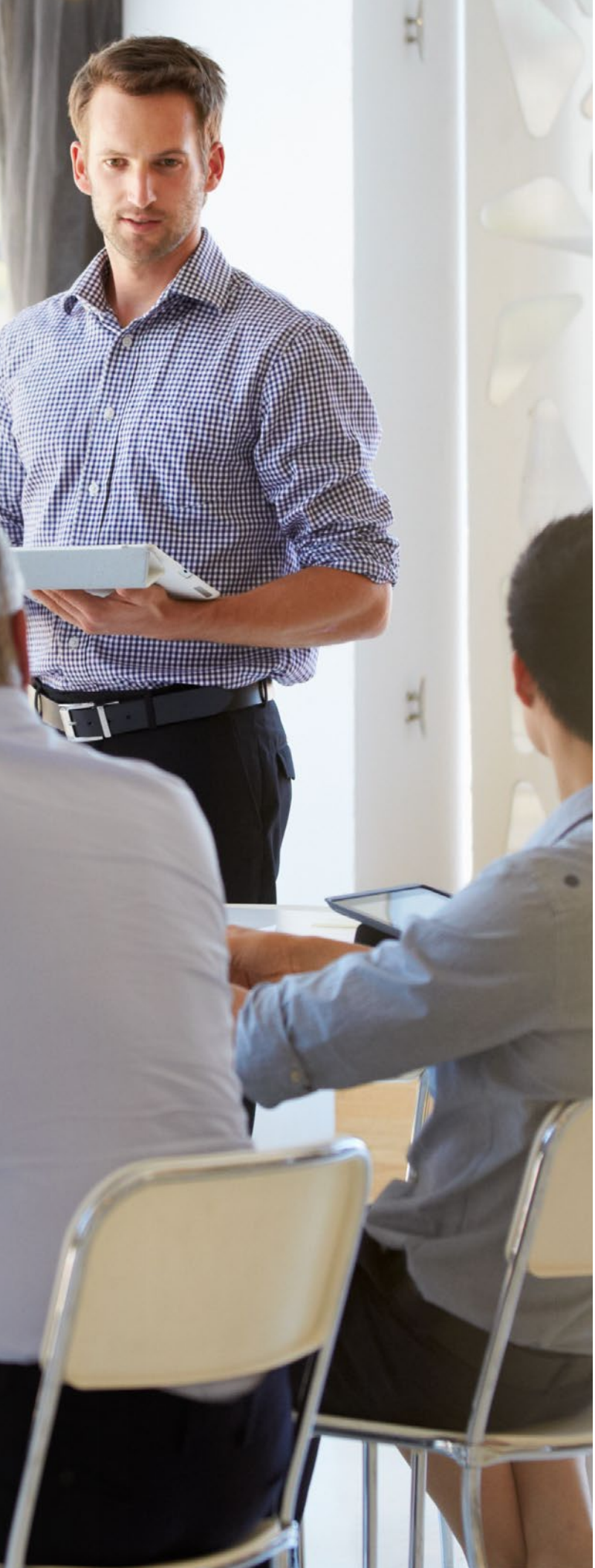
To start the process, we offer five activity points to follow:

1. Acknowledge that cyber risk is a business risk
2. Adjust cyber costs to your risk
3. Make a culture that prevents vulnerabilities
4. Ensure visibility of data
5. Ensure security and privacy are implemented "by design" to processes

The pace of progress in the present business landscape is increasing and presenting new risks that challenge our understanding of what great business practice means in an associated world. The time has come to set our organizations on an excursion to turning into a resilient flourishing worry in this world.

CEOs and boards can look to the cybersecurity profession as advisors, managers what's more, fonts of cutting edge information — however not as the bleeding edge of responsibility. Business leaders themselves must grasp the test, set the exchange, and inspire the robust understanding and response required to stand the test of genuine world cyberattack.

Cyber risk is a business issue and responsibility, not just the matter of the experts.



Be an "Iron (Wo)Man" for Your Organization during Crisis

A breach can happen to any company, at any time. So, what should you do if your defenses are penetrated? Or rather, what should you not do? Fortunately, there has been a spate of prominent cyberattacks in the course of the last years to give us some pointers.

While there is nothing the business can do to "unring" the bell after a breach, there are steps organizations can take to both limit the effect of breaches when they do happen, as well as help customers, partners, investors, and shareholders better understand the nature and effect of the occurrence. The test, for such a large number of organizations, is they need sufficient leadership and sponsorship for these efforts to grab hold and keep hold inside the enterprise. Verifying that the correct resources and priorities are set up is not something bleeding-edge and lower-level managers can do. It takes leadership and time to get ready for break response, and unquestionably not to be done in the activity. It is best to build up an arrangement ahead of time so that the playbook is composed and everybody included understands their job.

Each crisis includes numerous situations, each with various contingencies and considerations. They may incorporate security, legal, law enforcement, customer relations, media, shareholder, employees, the board, and more. While there can be overlaps, each situation has a distinct (and sometimes clashing) set of stakeholders, power structures, priorities, perspectives, interests, requirements, and values. For instance, the Communications department might need to be quickly open and transparent while the Legal department might need to hold up all, and more completely assess the risk and liabilities that such a stance could make. They each have an authentic case. Exploring this mind-boggling web of reliant relationships is overwhelming in routine times. In a crisis of this extent, the additional pressure and higher stakes can make it overpowering. In what manner can a leader successfully lead through such a mind-boggling swamp?

The first step is to ensure conviction about the values that will drive decision-making. In this case, trust should be the "genuine north" for target in its dealings with its numerous stakeholders. Obviously, shared values among leaders in the business can help forestall or resolve conflicts as operational options and objectives are gauged.

The second step is to plan the constellation of situations and their stakeholders (like a mind-map). This should be possible on a whiteboard or sheet of paper. It does not require a ton of detail; the purpose is to fix in your psyche

the awareness that you are managing a mind-boggling, dynamic issue. The edge you ignore in the crisis might be the one that causes the greatest harm at long last. Never forget that the first occasion — here, the information leakage — is only one crisis; however, the response may touch off a series of secondary crises if not dealt with well. This is especially evident in crises where the media takes an interest. Media stories will help shape the perceptions of numerous stakeholders and this will set attitudes and interactions going ahead. A considerable lot of these factors are outside your ability to control; however, they are once in a while outside of your sphere of impact.

With that mind-map drawn, search for gaps in your crisis response: something not made arrangements for or a need not met in the warmth of activity. All things considered, no action plan gets everything just right. It is basic to see the shaky areas or holes in your efforts and make mitigating strides. Make sense of who has something to provide to close a gap — from substantial assets to moral and reputational support — and who needs to get something to do likewise. Playing issue solution go between among "gives" and "gets" helps you to use and streamline resources in managing the numerous crisis situations.

Never Say Never

The crisis will develop after some time as must your view of it. Organizations likely made a move and had a disclosure plan preceding revelations in the media. In any case, a persuasive security blogger's post trailed by national and worldwide media consideration can make a huge difference.

The test for organization leaders will then be to re-situate the response to an increased pace with modified dynamics; control of messaging shifted from the organization to news outlets. Grasping the patterns of this new reality, a pioneer must foresee what is probably going to occur straight away. At exactly that point the individual in question can make the correct strides. This is a continuous circle of versatile reasoning — seeing, arranging, foreseeing, and acting — choosing, operationalizing, and conveying.

The last lesson from any incident is "never say never." An organization that takes security and customer trust seriously, Fintech industry, has a rigorous set of standards, procedures, and protocols, and penalties for resistance, that are being used with for all intents and purposes every single significant dealer across the globe. However, breaches still happen.

Times Are Tough. Micromanagement Will Not Help, Motivation Can!

At the point when times are intense, especially during crisis, leaders witness the disturbing signs like decreasing sales or high turnover. On top of that, as a result of the micromanagement, they do not feel ready to attempt to fix it. You attempt to inspire their own survival instincts and welcome them to assist you with concocting solutions. You can inspire your employees by assisting them to interface more with their end-customer and their activity's purpose.

The modern method of working that includes being constantly accessible as needs be, most of us are at the edge of burnout. You can increase your staff's profitability, innovativeness, and inspiration by doing small tweaks by the way all of you work.

Empower mid-day breaks and walking meetings. Try not to require over 40 hours of work and permit individuals to disconnect from email when they return home. Make the conditions for profound work by tolerating headphones or permitting "monk mornings" where individuals are disconnected. Exhausted employees cannot assist you with turning the business around.

> **"Leadership is not about being in charge. Leadership is about taking care of those in your charge." — Simon Sinek**

At the point when times are extreme, individuals fear losing their jobs. This dread reduces their psychological safety. They hold their head down and make an effort not to cause trouble. This can be solved by ways like the leaders taking ownership of their mistakes or the group laughing together is also significant.

Another positive response toward problems of such nature is asking the staff to focus on the issue and not the person. Ask individuals to share their concerns about what could turn out badly by doing a pre-mortem for significant projects.

> **You do not need your team to make errors because of absence of trust or communication. The time has come to order some pizzas and gather around to have a casual visit.**

In the event that you need to motivate your employees, you frequently need to conflict with your instincts. Give your staff more self-governance as opposed to less. Assist them with seeing the master plan and associate with their purpose. Urge them to work smarter instead of harder. What's more, make them feel safe instead of frightened. Not exclusively will you and your teams be more joyful, yet the results will reflect it as well.

About the Author

Nikhil Agarwal
CISM, OSCP, AWS Certified Security – Specialty, Azure Security Engineer

With over eight years of experience in cybersecurity consulting, Nikhil has expertise in both traditional cybersecurity practices like Penetration testing, DevSecOps, Cloud security, Architecture review, Cyber forensics, etc., to Next-Gen cybersecurity practices like K8s & Container Security, Red Teaming, Shadow IT, Cyber Threat Intelligence (CTI), Operational Security (OPSEC), Open Source Intelligence (OSINT), Darknet Monitoring, etc.

As a noted technology expert, who passionately shares knowledge with the community, Nikhil has proven ability to work across cultures and serve clients globally while working in Europe (Germany), Africa, MEA, APAC & ASEAN countries within various industries, both public and private.

CLICK. GET. GO.

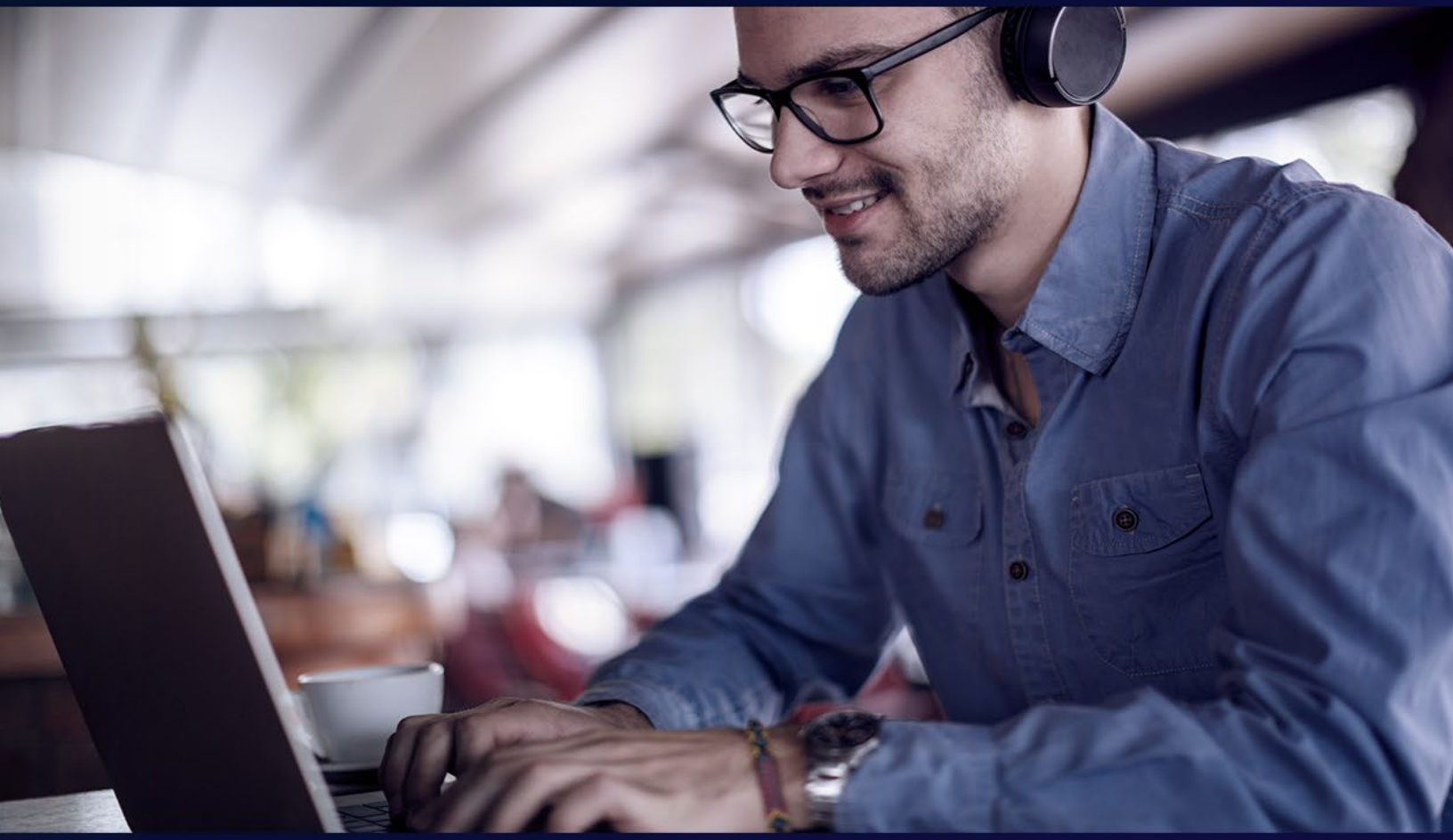
Building a booktopia with PECB eBooks!

The first PECB eBook, "ISO 22301:2019 Implementation Guide," is on its way!

Stay tuned!

PECB WEBINARS

Your Personal Roadmap to Professional Growth



Get meaningful insights from well-known experts about Digital Transformation by attending the upcoming webinar.

Digital Transformation 101 – How will it affect your business?
September 16, 3:00 PM CEST

Speakers

Anthony English

Scott Perry

Derek Stephenson

All webinar attendees are eligible for CPD credits.

REGISTER HERE

Become Cyber Resilient: Think Like a Hacker

An ethical hacker, a developer, a system engineer and an auditor walk into a bar…

…you think it's a joke, right?

It is not the typical set of people having a drink at the bar. And from a professional point of view and with 20+ years of experience in IT and security, I have not seen a lot of people or teams combining these skills.

[I didn't mention the lawyer,… he was late and paid the bill.]

But hey, you can bet on it that it will become the new normal.

What seems a completely different set of skills at first sight, is a very compatible set of skills — you will need to protect your systems and data from cybercriminals or people with malicious intent that are very persistent to get in.

Criminality has been there for ages, but what is different in the current era of cloud computing?

The Cloud Paradigm Shift

While shared and redundant infrastructure already exists from the start of computing, the X-as-a-service model is barely 10 years old — Microsoft Skydrive (predecessor of OneDrive) started in 2008, Google docs stems from October 2012. I do not want to dive into the "cloud" characteristics, but these five characteristics are relevant for this article, as defined by NIST and generally accepted as definitions: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. But most importantly, it is built on "(1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware."

For more information: https://csrc.nist.gov/projects/cloud-computing

I also recommend reading the ENISA Cloud computing risk assessment, because that is a very useful baseline to protect your IT infrastructure, both in cloud as in your physical data center.

Please also realize, at any time in the past, current, and future, that criminals have the same means at their disposal. But the dark side does not have any ethical limitations, so they always have a head start.

Of course, cloud has caused a major shift in business and IT, but most importantly in mindset. And the next technology wave is already swelling, IoT (Internet of Things).

When talking IoT, you will think about smart watches, fridges, intelligent TV's, home control devices, kids toys; in general any internet connected personal device for personal use.

But IoT (Internet of Things) in a larger interpretation is not limited to only personal devices with internet connectivity. These smart devices are also used in enterprise environments, like manufacturing, traffic control, waste control, heating systems, drinking water systems, radar systems, electricity generation and distribution. Then "simple" IoT becomes IIoT, Industrial Internet of Things. It still has to be seen where (I)IoT is going and what other waves will emerge.

But if you take a step back and look at the common denominators in these technology waves, you see that it always comes down to the same components you need to protect.

1. Infrastructure (including networking, computing/processing, and storage)
2. Applications
3. Data
4. People

> **The security was, is, and will be simply the same, it is only shapeshifting.**

Just as an example, it is worth looking at the OWASP Top 10 for web application security risks (Source: https://owasp.org/www-project-top-ten/). The number one, Injection attack, is as old as we store data. That says a lot.

Why does that matter? Well, this is where the "blacks hats" will be, one way or another. And if you want to protect yourself, your peers, your infrastructure, you need to think like a hacker.

Thinking like a Hacker

What is a "black hat" exactly? They have malicious intent, to harm you, destroy, or steal data. It is the opposite of "white hat" hackers who are ethical hackers who have a code of ethics, with no intention to harm. And in between, "grey hats," that might shift between these two, not always clear on which side they are.

There are various possible reasons of existence for hackers: making money with unethical business (like extorsion, ransom, etc.), holding a grudge against someone (for example former employer or partner), etc.

Understanding the Threat Landscape

So, step 1 in building protection is to understand how this "business" works. Connect to some cyberthreat intelligence news channels.

And just a practical hint: figure out how interesting your business would be for a hacker. What are your company's crown jewels, the primary assets (services, information, technology, or people) you want to protect. That is a start of a risk management.

The Typical Steps in a Hack

I do not want to fully elaborate an ethical hacker course in this article, but if you understand the typical steps in the hacking approach, you might be able to break them or at least slow them down. Make the hacker's life as miserable as possible.

1. **Reconnaissance** (a.k.a footprinting): Gathering information about the target and the victim. This is mostly a passive phase, meaning you do not connect to the victim directly, but rather collect information via internet, search engines, social media, official records, DNS information, etc.

2. **Scanning:** Using the basic information to get more precise details where to attack. Keep in mind when you connect directly to the target systems, the chance of being detected increases, while you normally want to avoid to get detected and get caught.

3. **Enumeration:** Extracting information, collecting useful information like user names, passwords, system identification, network information, etc.

4. **Hacking:** Forcing entry into the system

5. **Escalation of privilege:** Growing the power you have, either in the system you have entered (e.g., becoming root administrator) or by moving to another system and increasing your power (e.g., moving from a member server to a domain controller with domain administrator rights)

6. **Remove evidence:** As mentioned before, you want to stay undiscovered. In many cases, interaction with or on the system, creates evidence and logs of your activity. You want to get rid of that!

7. **Persistence:** Stay in the system, keep control over the system, come back when you want. In most cases, you will open up the access or keep it open to return at a later stage. It is way more efficient than rebuilding the entire attack phase again. A bit of efficiency helps.

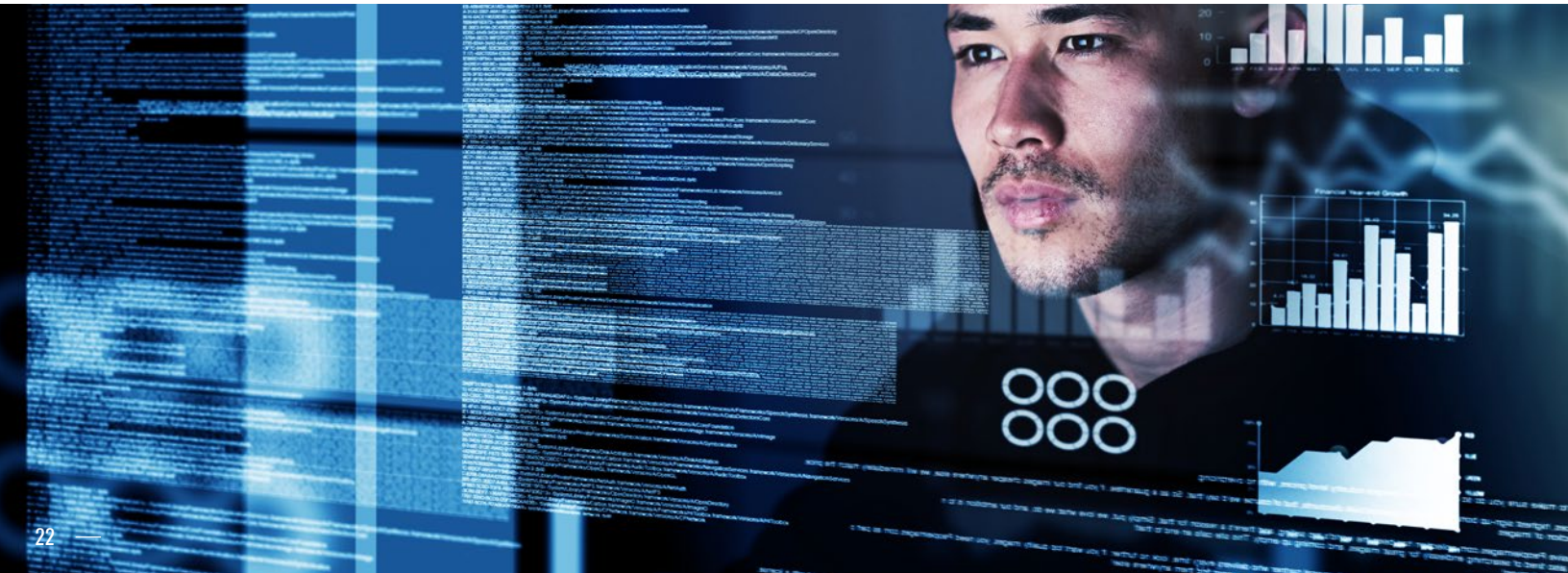
Know the Tooling

The hacker tooling is evolving continuously, so I cannot provide a full and current list. But some pointers might help, check this out:

- https://www.kali.org/
- https://www.hackerone.com/blog/100-hacking-tools-and-resources

You can easily find toolkits and ready-to-run virtual machines, which allow you to run the hacker tools with minimum effort.

Just a quick hint: Buy a wireless antenna to sniff networks in promiscuous mode (capturing traffic that is not meant of you); many of the built-in WiFi antennas do not allow promiscuous mode.



Offensive and Defensive

There are two main reasons that you need to know the most used tools and techniques.

- Defend against them (defensive mode)
- Use them against the target (offensive mode)

Just a warning here, you need to have an explicit agreement with the target for the hacking, if not, consider it as illegal. And in many countries it is considered as illegal entry with some serious consequences.

It will not surprise you that there are some best practices and guidelines for penetration testing (in short pentest), like: http://www.pentest-standard.org/index.php/Main_Page

Social Skills

While many of the aforementioned approaches demand for in-depth technical knowledge of networking, hardware, software, and system architecture, the hacker also needs an important portion of social skills. In many cases it is WAY easier: contact people directly and ask the information you need. Of course, if you tell them you are a hacker, it will not work. So "social engineering" is used to extract information under false pretenses via phone, via mail, SMS, etc., tricking the victim into disclosing the information you need.

And in some cases, you do not even need to go that far, you can enter the target building, collect information directly... so, even physical reconnaissance is an option for a hack.

Hacking in the Cloud

With cloud, the importance for ethical hacking is only growing. The same principle applies for IoT. The main reason is that cloud is highly volatile in many ways. Your environment is changing continuously.

But also, in many cases you lose physical control. Certainly, for public cloud system, you DO NOT OWN the infrastructure anymore. So you need to compensate by:

- Demanding the right to audit, and even the right to pen test (although the latter is usually difficult to achieve)
- Having contractual agreements with vendors to force them to use security best practices like SSDLC (Secure Software Development Life Cycle)

And of course, more and more data is being stored in the cloud, which increases the interest for cybercriminals, as they have a business to run too.

Vendor Management

Many public cloud providers have anticipated that demand for control by customers, to validate that their infrastructures, applications, data, and users are secure.

For example, check out the following:

- Microsoft Cloud Unified Penetration Testing Rules of Engagement, where you can pentest the Microsoft cloud platform, under certain conditions.
- Amazon AWS https://aws.amazon.com/security/penetration-testing/
- Google https://support.google.com/cloud/answer/6262505?hl=en

By the way, more and more companies, like Google, have a bug bounty program that rewards ethical hackers who find weaknesses.

The Hacker and the ISO/IEC 27001 Auditor

You see that a lot of work that the ethical hacker does, is covered by policies. This is where the ISO/IEC 27001 implementer and auditor walk in.

There is an important part of ISO/IEC 27001 and the NIST framework that provide guidance to synchronize the work of the ethical hacker, the system engineer, and the ISO/IEC 27001 LI/LA (Lead Implementer or Lead Auditor)

The NIST framework for Pentesting: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Just to be clear, ISO/IEC 27001 does cover pen testing, validation, and software security, but in a very general way.

Important auditor note here: Many security audits provide penetration testing, but on ISO level, an ISO audit should not include Pentesting. That is the customers' (auditee) responsibility, not for the auditor.

The ISO auditor is checking for compliance, they simply check if the auditee does what they say (implementing security), and say what they do (documentation).

For internal audits or specific security audits, under control of the auditee you could consider Pentesting.

The Legislative Road

Under impulse of GDPR, there has been a lot of change on legislative level.

On European level, the NIS directive and Cyberact regulation have launched. The NIS is the Directive on security of network and information systems (NIS Directive) and the CyberAct regulation establishes an EU-wide cybersecurity certification framework for digital products, services, and processes.

So, you understand that in the near future, there is also a lot of work on the agenda of ethical hackers.

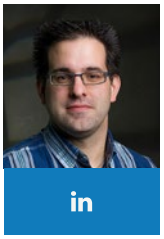
Some Hints and Tips

If you want to make the life of a black hat as difficult as possible, you really should consider the following:

- Stay informed and up to date with current evolutions in cybercrime and technology. Be aware what is coming.
- Hack yourself, before anyone else does.
- Keep your systems up to date, as unpatched systems are the most common root cause for cybercrime.
- Enforce security by design by making sure that your system is designed with security in mind, from the beginning.
- Implement security by default; change default logins and passwords
- Use the Pareto principle (20/80, 20% effort with 80% effect)
- Assume that you are breached — consider you are already hacked. How do you minimize the damage? For example, using functional or network level segmentation can avoid the collateral movement of hackers.
- Have a responsible disclosure policy; make sure that people notify you FIRST, when they find an issue on your platforms, before they publish the issue. This allows you to patch your systems before publication, minimizing impact.

> **And if you plan to become an ethical hacker, have some clear ethical guidelines and some contractual rules of engagement. Because in jail, your lawyer won't pay the bill.**

By the way, keep an eye on the PECB course agenda for the launch of their ethical hacker track: https://pecb.com/en/education-and-certification-for-individuals/ethical-hacking



About the Author

Peter Geelen
Director and Managing Consultant at CyberMinute and Owner of Quest for Security

For over more than 20 years, Peter has built a strong experience in enterprise security and architecture, identity and access management, but also privacy, information and data protection, cyber and cloud security. During the last few years, his focus is on ISO/IEC 27001 and other ISO certification mechanisms. Peter is a Certified Ethical Hacker and accredited Lead Auditor for ISO/IEC 27001, ISO 9001, a PECB Trainer and Fellow in Privacy.

Committed to continuous learning, Peter holds renowned security certificates as CEH, Certified ISO/IEC 27701 LI/LA, ISO/IEC 27001 Master, Sr. Lead Cybersecurity Manager, ISO/IEC 27002 Lead Manager, ISO/IEC 27701 Lead Implementer, CDPO, Risk management, Lead Incident Manager, Disaster Recovery, and a few more.

Ethical Hackers as "Defensive Players" to Win the "Security Battle"

In today's world, where our daily life is surrounded by smart devices, wearable electronics, IoT, and smart phones, cyber threats are always there (see Figure 1). Moreover, at the corporate level it has become something very normal to find the majority of the organizations depending on cloud solution which is usually hosted and/or operated by a third party. This, however, represents a lack of governance and may also involve weak controls, which is why both individuals and organizations are facing a very wide attack surface along with tens of attack vectors. All these technological advancements with their connected risks and threats highlighted the sudden need and importance of ethical hackers as the first line of defense. They are working proactively to detect

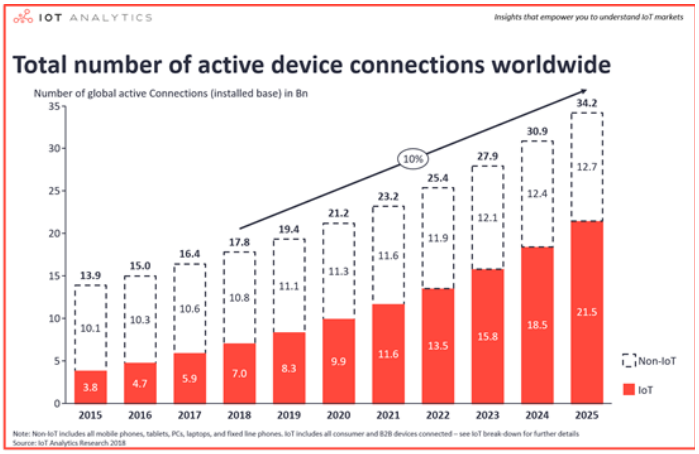


Figure 1. The dramatic increase of IoT devices expected by 2025

vulnerabilities that could exist in networks, operating systems, applications, middleware, databases, physical controls, and even human factors which often represent the weakest link in the chain.

Who Is the Ethical Hacker?

An ethical hacker, also referred to as a white hat hacker, is an information security expert who attempts to penetrate a computer system, network, application, or other computing assets in a legal way (with the owner's permission and in accordance to a predefined scope) to find security vulnerabilities that a malicious hacker could potentially exploit. With different wording, we can say that it is a simulation of an attack for a defensive purpose.

Cyberwarfare/cyber operation also has a great impact on the exponential increase on the demand of ethical hackers. During the last ten years, tens of countries including the United States, Germany, the United Kingdom, China, France, Iran, and many more have announced that they started to establish their "Cyber Army." This was mainly to protect their national security, critical infrastructure, and confidential data against cyberattacks that could be initiated from other countries (Nation Sponsored Attacks), organized criminals or cyber terrorists. In addition, in some countries like Germany they restructured the armed forces to include a sixth branch in the German military; the new branch includes 13,500 "Cyber Soldiers."

Cyber operations with both offensive and defensive targets became a necessity for all modern armies. However, based on the context of this article, I will ignore the offensive side since it is not relevant to our topic here. Cyber operations' importance will increase greatly with the release of 5G technology M2M (Machine to Machine) since billions of devices will be connected together, representing the widest ever attack surface. With the 5G technology, almost everything will be connected to the internet with hundreds of embedded systems and vendor-specific applications where control will be indeed very difficult.

Last but not the least, ethical hacking and penetration testing are necessary to achieve a wide range of certification for organizations in general or for some specific sectors, such as ISO/IEC 27001 (Information Security Management System), PCI (Payment Card Industry Standards), HIPAA (Health Insurance Portability and Accountability Act), or maybe some regulatory requirements such as GDPR (General Data Protection Regulations) where it is a must for every organization to conduct vulnerability assessment or penetration testing at least once a year.

Vulnerability Assessment versus Penetration Testing

Vulnerability assessments search systems for known vulnerabilities, while penetration testing attempts to actively exploit weaknesses — we could say that it is about checking the exploitability of the detected vulnerabilities. While a vulnerability scan can be automated, a combination of automated and manual techniques is usually utilized in conducting a penetration test where it requires a more advanced level of expertise along with a proper planning and risk assessment. Unprofessional penetration testing could result in service failure or complete denial of service.

Ethical Hackers or Penetration Testers' Skills

According to NICCS (National Initiative for Cybersecurity Careers and Studies) and NICE (National Initiative for Cyber Education) the following KSAs (Knowledge, Skills, and Abilities) and tasks are needed for those who will conduct vulnerability assessment (Ethical Hackers and Penetration Testers)

ABILITIES

- **A0001:** Ability to identify systemic security issues based on the analysis of vulnerability and configuration data
- **A0044:** Ability to apply programming language structures (e.g., source code review) and logic
- **A0120:** Ability to share meaningful insights about the context of an organization's threat environment that improve its risk management posture
- **A0123:** Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)

KNOWLEDGE

- **K0001:** Knowledge of computer-networking concepts and protocols, and network security methodologies
- **K0002:** Knowledge of risk management processes (e.g., methods for assessing and mitigating risk)
- **K0003:** Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy
- **K0004:** Knowledge of cybersecurity and privacy principles
- **K0005:** Knowledge of cyber threats and vulnerabilities
- **K0006:** Knowledge of specific operational impacts of cybersecurity lapses
- **K0009:** Knowledge of application vulnerabilities
- **K0019:** Knowledge of cryptography and cryptographic key management concepts
- **K0021:** Knowledge of data backup and recovery
- **K0033:** Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists)
- **K0044:** Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- **K0056:** Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML)

- **K0061:** Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL])
- **K0068:** Knowledge of programming language structures and logic
- **K0070:** Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code)
- **K0089:** Knowledge of systems diagnostic tools and fault identification techniques
- **K0106:** Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- **K0139:** Knowledge of interpreted and compiled computer languages
- **K0161:** Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks)
- **K0162:** Knowledge of cyberattackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored)
- **K0167:** Knowledge of system administration, network, and operating system hardening techniques
- **K0177:** Knowledge of cyberattack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)
- **K0179:** Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth)
- **K0203:** Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model)
- **K0206:** Knowledge of ethical hacking principles and techniques
- **K0210:** Knowledge of data backup and restoration concepts
- **K0224:** Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems
- **K0265:** Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability
- **K0287:** Knowledge of an organization's information classification program and procedures for information compromise
- **K0301:** Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)
- **K0308:** Knowledge of cryptology
- **K0332:** Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
- **K0342:** Knowledge of penetration testing principles, tools, and techniques
- **K0344:** Knowledge of an organization's threat environment
- **K0624:** Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list)

TASKS

- **T0010:** Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives
- **T0028:** Conduct and/or support authorized penetration testing on enterprise network assets
- **T0138:** Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions
- **T0142:** Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing
- **T0188:** Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies or solutions
- **T0252:** Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews)
- **T0549:** Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications)
- **T0550:** Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes)

	Entry	Intermediate	Advanced
Credentials/Certifications	**Recommended:** Yes **Example types:** N/A **Example topics:** Certifications addressing new attack vectors (emphasis on cloud computing technology, mobile platforms and tablet computers), new vulnerabilities, existing threats to operating environments, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure	**Recommended:** Yes **Example types:** N/A **Example topics:** Certifications addressing managing, maintaining, troubleshooting, installing, and configuring basic network infrastructure	**Recommended:** Yes **Example topics:** Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security
Continuous Learning	**Recommended:** Yes **Examples:** 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	**Recommended:** Yes **Examples:** 40 hours annually (may include mentoring, conferences, webinars, or rotations)	**Recommended:** Yes **Examples:** 40 hours annually (may include mentoring, conferences, webinars, or rotations)
Education	**Recommended:** Yes **Example types:** Associate's **Example topics:** Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	**Recommended:** Yes **Example types:** Bachelor's **Example topics:** Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering	**Recommended:** Yes **Example types:** Master's, Ph.D. **Example topics:** Computer science, cybersecurity, information technology, software engineering, information systems, computer engineering
Experiential Learning	**Recommended:** Yes **Examples:** Prior experience in information assurance, incident handling, vulnerability management and vulnerability analysis, and assistance program	**Recommended:** Yes **Examples:** Prior experience in information assurance, incident handling, information assurance vulnerability management and analysis, and assistance programs	**Recommended:** Yes **Examples:** Prior experience in advanced information assurance and handling incidents of greater organizational impact
Training	**Recommended:** Yes **Example types:** N/A **Example topics:** Systems administration, basic cyber analysis/ operations, intermediate cyber core, cyber threat modeling	**Recommended:** Yes **Example types:** N/A **Example topics:** Network security vulnerability, advanced network analysis, basic cyber analysis/ operations, network traffic analysis, intermediate cyber core, information security, troubleshooting, information systems, quality assurance and control, SQL, network security, cyber threat modeling	**Recommended:** Yes **Example types:** N/A **Example topics:** Information system security management, information security, troubleshooting, information systems, quality assurance and control, SQL, network security, cyber threat modeling

Figure 2. Capability indicators (Source: NICCS)

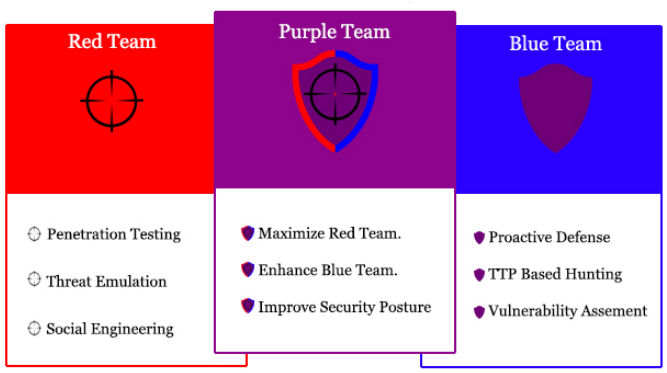
Blue Team, Red Team, or Purple Team?

Although it is obviously clear that ethical hackers, pen testers, or even malicious hackers share a very wide and common portion of knowledge and skills, they do have quite different mindsets and objectives. This is why, practically speaking, we have different teams of ethical hackers who can, for instance, work separately or coordinate to continuously detect weaknesses and improve the security posture of the organization.

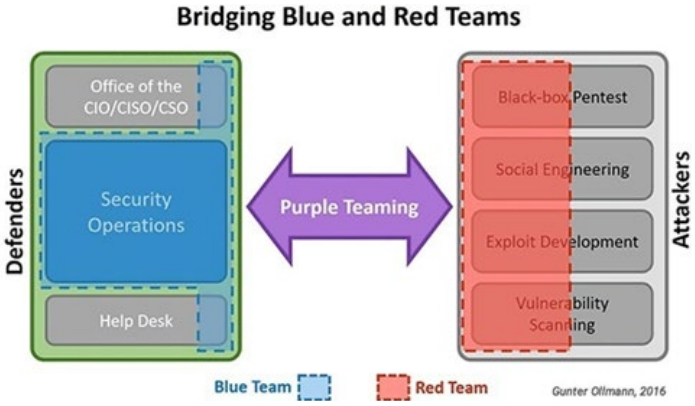
Blue team: It is an internal security team that defends against attackers. Blue team works proactively to protect the organization and defend against cybersecurity threats. It performs full-knowledge assessments of networks, systems, and applications looking for security weaknesses. It could be an internal or external (outsourced) team.

Red team: It performs no-knowledge simulations of an attack against the organization's assets with specific objectives in mind. It is sometimes staffed by people who normally work for the organization. Usually, it is authorized by the Chief Executive without notification to others within the organization (blind test/double blind test)

Purple team: It is known as the conceptual team (not a must to be a physical team). Its mindset is more towards coordinating and managing a shared goal involving red and blue teams. These coordinated joint activities improve the effectiveness of security controls, testing methodologies, and the organization's overall security posture.



Source: PTMF



Source: Cyber Defense Magazine

The world is witnessing a very high shortage in ethical hackers. According to many statistics, we have around two million vacancies in cybersecurity in general where ethical hackers/cybersecurity engineers are identified as one of the five most in-demand cybersecurity jobs for 2020 with an average of yearly salary of $106,000.

Related NICE Work Role IDs: PR-INF001, SP-SYS001

Another survey from ISC(2), an international, nonprofit membership association for information security leaders, produced a research in 2018 which estimated the cyber worker shortage at nearly 3 million — on the heels of a report they put out just a year earlier, which stated a drastically lower 1.8 million figure by 2022.

By no means, the main concern when hiring ethical hackers is their qualification and practical skills. However, well-educated and certified ethical hackers who have deep understanding of the technical and scientific concepts are representing an additional value and competitive edge for organizations from the credibility point of view. Some security guys may have great skills in one or more specific areas, but when it comes to the business perspective, this may represent a very high risk if the ethical hacker does not have sufficient knowledge, that could lead to a big problem. To put it simply, this is the difference between a professional pen tester and a script kiddie who is using hacking tools. The latter may accidentally launch an actual attack without knowing what is happening at the underlying layer, conducting a destructive test without understanding the impact on the business or the service dependencies model which could lead to denial of service or system failure. It is also worth to mention that

the different teams (red, blue, and purple) mentioned earlier, need to be connected or have joint activities and shared knowledge base with other teams such as, but not limited to, Forensics Investigators, incident handlers, or SOC (Security Operations Center) engineers.

Security has to be handled in a holistic way in order to oversee the big picture. In other words, if you have a secure operating system and a secure database in addition to secure applications, this will not, by default, lead to having a secure system since some vulnerabilities will not appear until you connect things together. My last advice for everyone is to always work in all pillars of successful security systems which are (people, process, and technology). In my humble opinion, the "People" component has a great impact on the other two.

About the Author

Adel Abdel Moneim
Registered ITU-ARCC Cybersecurity Expert

Adel Abdel Moneim, a registered ITU/ARCC Cybersecurity Expert, has over 25 years of experience in the IT/Cybersecurity, spending most of his career in Information Security consultation and training. Adel is globally recognized as "IFSEC Security thought Leadership/Global Influencer 2019."

Adel is an international certified trainer from ISC2, EC-Council, ISACA, PECB, CertNexus, and APMG. Adel works with multinational companies, academia, training companies, and law enforcement/military institutions, in the areas of Cybersecurity, Pen-Test, Digital Forensics, Data Privacy, Risk Management, ISO Standards Implementation/Audit, or GRC. Adel is PECB MS Auditor for ISMS, IPMS, BCMS.

Top Ethical Hacking Tools in 2020

BY ENDRITA MUHAXHERI, PECB

**"If I had eight hours to chop down a tree,
I'd spend the first six of them sharpening my axe."**

Abraham Lincoln

The above saying is a constant reminder that approaching a problem with the right set of tools is critical for success. In today's ever-evolving digital world, having the right hacking tools will help you find and exploit weaknesses in networks, and prevent unauthorized access to important data. It is important to think with the mind of the hacker in order to know the tools that they use. Penetration testing is now a common practice to identify the level of security.

1. Metasploit is an open-source penetration testing tool, which allows you to locate vulnerabilities on different platforms. Considered as one of the best hacker software tools, it is used by ethical hackers and cybersecurity professionals, as it allows them to perform several tasks. It helps security teams by providing them with information about vulnerabilities, strategies, and methods for exploitation. It is compatible with all major platforms including Windows, Mac OS X, and Linux. It offers two options: the free and commercial option. It also integrates with Nmap.

2. Nmap stands for Network Mapper and it is a free and open-source network scanner. It is suitable for both beginners, because it is easy to use, and experienced users, as it offers advanced features. This tool has been primarily designed to scan large networks. However, it works great for scanning single hosts too. It also has many other characteristics, as it is used by security professionals to manage the schedule of service upgrade, network inventory, monitor host, or service uptime, etc. Nmap supports all main computer operating systems such as Windows, Mac OS X, and Linux.

3. Wireshark is considered as one of the most important network security tools, used to monitor traffic in real-time, and then it displays these data in a format that is readable for the user (you can export the data in different formats). It can execute a profound analysis of many internet protocols. If you are planning to become a penetration tester, this tool is a must. There are a lot of online learning resources that can help you familiarize yourself with Wireshark. This tool is free and supports operating systems such as Windows and Linux.

4. Burp Suite is an integrated platform that has tools to perform penetration testing of web applications. It can identify over 3000 web application vulnerabilities. It is very popular due to its ease of use and is considered "a one-in-all" set of tools. You can extend the capabilities of this tool, by installing additional extensions through the store called BApp. It helps identify vulnerabilities and verify attack vectors that are affecting web applications. As a community edition, Burp Suite is available for free; however, the Professional edition costs $399/year per user and the Enterprise edition costs $3,999 per year. Supported operating systems by Burp Suite include Windows, Mac OS X, and Linux.

5. Acunetix is an automated web application security testing tool. It scans any web application or website and it can identify and report 4,500 web application vulnerabilities including all types of SQL injections and XSS. After the scans are done, Acunetix displays compliance and management reports on various web and network vulnerabilities. The crawler of this tool completely supports JavaScript, HTML5, and single-page applications and it allows auditing of complex applications. The app is compatible with different operating systems including Windows, Linux, macOS, or the cloud. The price depends on the number of websites you want to scan, and it also offers customized on the cloud or on-premises plans.

Hackers today are capable of compromising your network and stealing valuable information. This is why organizations need to take proactive measures. Employing an ethical hacker is an investment that organizations cannot miss, in order to "fight" against the growing threat of IT security.

Today's system automation is changing the way how ethical hacking is done — now is it easier and faster. By doing this, you will be able to increase the security of your systems.

The above list of ethical hacking tools is not conclusive; however, these are the most recommended tools. This will also depend on the user's preferences.

The New Academic Year Is Starting at PECB University!

Have you thought about taking your career to the next level?

Consult one of our student counselors for your path to success.

→ CONTACT NOW

Protecting Privacy and Consent Online

For everyone concerned about online privacy, ISO/IEC 29184 has just been published.

We're more connected than ever before. The growth of hi-speed connections in our homes and offices has only been outstripped by the number of smartphones in our hands and wearable devices like fitness monitors.

Devices such as these collect and process your personal data. That might include geographical and biometric data, or the frequency and timing of interactions with the device. That's legitimate, and useful for those who want to be able to get an objective insight into, say, their sleeping habits. But it also provides lucrative opportunities to companies who use such data to market their products and services, often without our informed consent.

As consumers become more aware of the type of information that's being collected, many have expressed their discomfort. From the uneasy feeling that "someone is watching" you to the flagrant sale of your personal details to third parties, people are justifiably concerned about online privacy.

The new standard, developed jointly by ISO and the IEC's committee on information security, cybersecurity and privacy protection, provides details on the implementation of privacy principles from ISO/IEC 29100. Specifically, it addresses consent and choice (Principle 1), and openness, transparency and notice (Principle 7).

Committee Chair, Dr Andreas Wolf, observes that "people are worried about the collection and use of personally identifiable information (PII) by online services. In many cases, that's because there is no clear explanation of how PII is processed, stored, maintained and managed. This new International Standard will help bring much-needed clarity and reassurance".

In addition to providing clearer information about what kind of PII is being collected and how it is being used, ISO/IEC 29184 will help people to better understand just what they're signing up to when they use connected services and, importantly, how to withdraw their consent.

Disclaimer: PECB has obtained permission to publish the articles written by ISO.

Partnerships That Spark Growth

DANIEL BLEEKER'S SUCCESS STORY

Writing a success story about our business, in the midst of the pandemic, is a challenging exercise as many smaller companies are under severe pressure. But I hope to give the reader "food for thought" and ideas to survive during these difficult times, by telling my story.

Our Story

I founded my company, STEER, with two former business colleagues. During our employment at a major global company, we had been in senior management positions in compliance, investigations, audit, and finance and had a critical role in successfully leading the company through two Deferred Prosecution Agreements with the Department of Justice (DOJ) in the USA, as a result of FCPA (anti-bribery) violations.

It was a coincidence that we all left the company within a period of a year. During one of my last days at the company I had a "farewell" coffee with the two persons who hired me years before. We talked about the previous years and the unique experience we had of working in this global company with a presence in over 100 countries, designing and implementing a compliance department and an internal investigations unit, leading the global audit function and heading the financial department of a global division. We all agreed that the best experience was the opportunity to have lived and worked in many countries around the globe.

Living in countries and being surrounded by people with different cultures, languages, views on the world, etc., is an invaluable experience. It made me even more humble and respectful towards people that had not grown up in the same environment as I did. I learned that everybody knows the basics of compliant behavior, but that it requires respect, proper communication, and patience to explain certain elements of compliance as it is known in the "Western World" and apply them in another culture.

Anyway, back to the "farewell" coffee I mentioned before. The coffee became two coffees, three coffees, and suddenly we had been talking for hours. Not a productive day for the company we worked for, but a good day for the three of us. We realized that with our combined experiences and expertise, we could be very valuable to many (global) companies. Over the next few months we all left the company and we decided to explore the possibility of starting our own boutique firm.

After multiple meetings, telephone calls, online conversations, and emails, we were convinced that there was a demand for our combined expertise and experience. However, starting a company is a stressful event, especially since we had the very ambitious plan to open offices in two different countries (Zurich, Switzerland, and New York, USA) at the same time.

It was therefore very important that we as founders decided to go through various psychological tests to better understand our inner self but also to face the strengths and weaknesses in us as a team. Based on the assessments we were able to determine how we could best complement each other and assign responsibilities.

The final step towards starting the company was to formalize our verbal agreement and address what we would do in better or worse times. The best time to talk about bad times is when things are going well. For us, that meant crafting a written partnership agreement before we officially started the business.

PECB MS

It was soon after ISO 37001 (Anti-bribery) was published in August 2016 that we realized that this ISO standard could be game changer in the world of compliance, for the private and public sector.

We had more than relevant expertise in this area and we were experienced auditors. Now we had to search for a certification body that would have a comparable vision to ours.

When we started our company, we all had the same vision about conducting business. Quality over quantity. Instead of doing multiple jobs at the same time with the risk of providing mediocre results, we focused on providing quality on each single project. Our clientele are companies that take compliance seriously and they are looking for auditors who not only have the required expertise and experience but in addition, can do an audit with a fair but critical eye, so they can further improve their compliance efforts.

After conducting due diligence on a number of certification bodies, we got in contact with PECB MS. We were instantly charmed by the fact that PECB MS is constantly looking to improve its processes and image. It is very encouraging to find that a certification body follows the requirements of most ISO standards to constantly evaluate and improve. This approach definitely keeps PECB MS at the top of the list for certification bodies.

PECB MS made clear to us that it wants to work with experts in the field of each ISO standard. They do not want to provide just a certificate; they want the client to know that PECB MS auditors are best in class. An audit conducted by experienced auditors with relevant expertise adds value to the obtained certificate. Regulators around the world, such as the Department of Justice in the USA, support the ISO 37001 standard but are trying to determine which certification bodies are serious about conducting proper audits and granting certificates. It is our experience that PECB MS is one of those certification bodies that aims to provide top-notch services to their clients in this respect.

PECB MS showed great trust in us from the very beginning. In the few years that we work with PECB MS, we have seen the continual improvements. Processes are subject to change when improvements are identified, and the training material is currently undergoing great improvements as well. Proper training provides the essential foundation for auditors so that they can provide the best value added service.

Our ISO 37001 Success

It was two years ago when we were alerted that Microsoft, who were part of the development of ISO 37001, were looking for a certification body to audit and certify a country organization and a global business unit.

Microsoft is one of the biggest companies in the world measured by market value. And it is obvious that there are very few companies that would not want to have Microsoft as a client. PECB MS was one of the certification bodies that was approached by Microsoft. As PECB MS's lead ISO 37001 auditors we were requested to do an online presentation. It was our first and only chance to convince Microsoft that the PECB MS and STEER as the PECB MS certified auditors, could provide the best value to Microsoft's commitment to audit a solid and robust Anti-bribery Management System based on ISO 37001.

We knew we had to compete with many other audit firms, all of them bigger than us and key players in the industry. In preparation for our presentation, we decided that we would approach Microsoft the same way we would approach other potential clients; not pretending we are bigger than we are, not pretending that we have the answers to all questions. We chose to describe our background and expertise, how we conduct audits, and our view on ISO 37001. By doing this in an online meeting, it gave Microsoft the chance to ask questions and get an impression of our personalities. We think it made a difference that all three STEER partners were presenting to Microsoft and that we made the commitment that all three of us would be involved in the certification audit.

A few months after our presentation, PECB MS was approached by Microsoft with the request for a financial proposal including STEER to be the auditors, for a certification audit of Microsoft Hungary's Anti-bribery Management System and a global business unit.

As with every project, if you fail on the first engagement, you will lose the client. This means, from the start of the project, the client needs to feel confident that they get value for their money. Firstly, the client needs to feel confident that the auditors have the relevant expertise to conduct a certification audit. Secondly, the client needs to feel comfortable about the audit approach.

During an online meeting the client just hears what you say. It gives a first impression. It is not until the preparation and execution of the certification audit when the client witnesses the capabilities of the auditors.

We were approaching this project with a long-term view. We put in so many (non-billable) hours to prepare for these audits, that we hardly covered our cost. However, by putting in so many hours we became very knowledgeable about Microsoft's ABMS, which gives us an advantage on future Microsoft ISO 37001 audit projects where we can offer competitive pricing.

A company like Microsoft is very serious about fighting bribery. And we were very impressed with the efforts they put in designing and implementing their Anti-bribery Management System. Microsoft's ABMS is best in class, no doubt about it, and based on their continual efforts to further improve, it will remain best in class for the foreseeable future. However, Microsoft is aware that the quality of an ABMS based on ISO 37001 can only be validated by auditors with extensive anti-bribery experience, who conduct an audit with a fair but critical eye.

After conducting certification audits at Microsoft, they had an interest in training their key employees within the global business unit to be ISO 37001 Lead Implementers. They wanted to do this to ensure that these key employees had the proper knowledge and foundation to maintain their ABMS. STEER was also chosen by Microsoft to conduct this training. As mentioned earlier, with clients like Microsoft you cannot fail to deliver on their expectations. We wanted to make sure that after auditing the global business unit, there was no (perceived) conflict of interest if we would conduct a general lead implementer training for employees of the same global business unit. We reviewed the PECB training material and contacted PECB to confirm that no conflict of interest would occur, according to ISO/IEC 17021-1.

Final Note

The pandemic has a severe impact on how business will be conducted. Times are changing and it is important to be open to new business approaches. We have been contacting clients to explore different ways to go forward with ISO projects, such as offering fully remote (online) training and (surveillance) audits. In difficult times like these it is comforting to have a business partner like PECB MS that is adapting to the new business environment and open minded to the development of solutions, so that certain services can still be provided.

We are part of the PECB family and we are always looking to partner with auditors that have a similar vision as ours. We think that combining our strengths and efforts leads to successful partnerships which will enable us to win engagements with Fortune 500 companies.

Note: PECB MS manages the audit and certification services. STEER's responsibility is to follow all policies and procedures set by PECB MS for its auditors. STEER auditors are part of PECB MS certified auditors. STEER also offers consultancy services; however, STEER does not provide management consultancy services to clients referred to PECB MS, for which STEER has conducted audit services, and STEER is not involved in any management systems certification decisions. The application process, the determination of audit days, the qualification of auditors, the reports review, and certification decisions are all conducted by PECB MS, as required by ISO/IEC 17021-1.

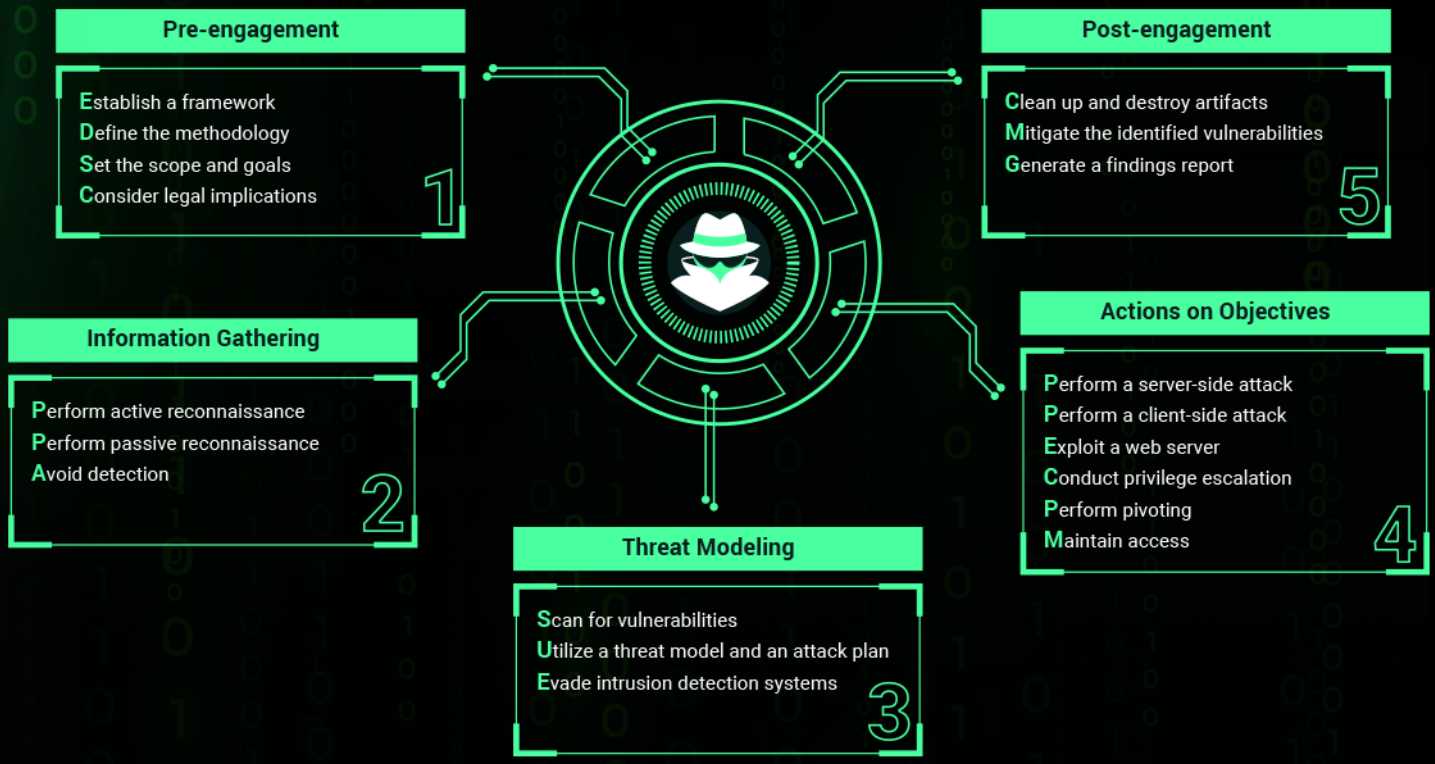
Get ready!

The long-awaited PECB Certified Lead Ethical Hacker Training Course is on its way!

Stay tuned for this one-of-a-kind, advanced CLEH training course in safeguarding the networks and systems of businesses and government agencies!

PECB's Penetration Testing Methodological Framework

Defensive Strategy with an Offensive Approach



Penetration testing provides insights into how mature the overall security of an organization is, how hackable the system is, and how to evade any attacks or breaches. It is a critial step in improving cyber defense!

COVID-19, a Window of Opportunity for Hackers

Hackers see any crisis situation as an opportunity to maximize the impact of their attacks and take advantage of the weaknesses and lack of vigilance generated by crises. The global spread of COVID-19 is not an exception to this "rule."

Ever since the first reports on the global health crisis were released, hackers have launched several campaigns of attacks, including phishing, to take advantage of the instability and uncertainty created by the situation. Several malicious programs and numerous phishing campaigns using coronavirus-related information to lure the users have been detected by cybersecurity specialists.

Businesses remain the primary target during this COVID-19 crisis, particularly medium- and small-sized businesses. Some companies had to face for the first time an unprecedented crisis, and their entire business was challenged. Hundreds of thousands other companies were facing difficulties among those were those that had not previously planned for continuity of service plans.

No effort on the part of hackers has been spared, all types of attacks have been explored, and all potential targets have been aimed, starting from Ransomware campaigns targeting hospitals, to exploiting the security vulnerabilities of web-based conference tools, such as the famous Zoom, widely used during the crisis, and finally the numerous phishing campaigns that take advantage of the human emotions and personal and professional uncertainty in which they live.

We will try to detail in this article the main reasons that led hackers to target companies and professionals during the COVID-19 health crisis. In particular, we will focus on the type of attack called Phishing, where cybercriminals try to get a person to download malware or give confidential information by email or phone by exploiting their personal information.

1. Companies occupied by the continuity of their business

Companies and professionals have faced an unprecedented crisis that has heavily impacted their businesses, so everyone was busy finding solutions to ensure the continuity of services and in particular to overcome the problem of the shift in working remotely for all or most employees and workers all over the world.

The panic and lack of vigilance did well to the hackers who took advantage of this situation to generalize the phishing attacks and double the efforts to reach the maximum number of victims.

Indeed, very few companies had a continuity plan to ensure the continuation of operations in the face of a

crisis of this magnitude. If we take the case of small- and medium-sized enterprises, ensuring the continuity of their services in the face of any crisis is in the majority of cases non-existent.

In my job as a security auditor, I have had the opportunity to audit several companies of this type, and the business continuity plan is indeed very rarely drawn up by them, and when it is written, it is never tested virtually.

Thus, during the health crisis, the level of vigilance of companies was reduced considerably and all the attention of managers, directors, and workers was focused on the business.

2. Noncompliance with internal and standard processes

During the COVID-19 health crisis, it was noted that many companies were no longer following the internal standard processes to perform the usual tasks, such as billing, accounting, supplier relations, etc. Many of these tasks that went through well-controlled workflows in normal times had to go in circuities in order to achieve the desired outcomes, which created an advantage for hackers.

Several invoicing and supplier relationship activities have been handled simply by phone calls, as the supplier is also in crisis and cannot access its internal network to use the usual invoicing tools. Phone calls that make it possible to get paid bills remind us of the famous phishing attack called “the call of the fake boss.”

In this case, people with communication skills make fraudulent calls to employees under pressure to make transfers or pay for false invoices. During the health crisis, the vigilance of employees also decreased and thus benefited malicious people to develop all possible and imaginable types of phishing.

3. Lack of employee security awareness

Another reason that may be mentioned in this article is the lack of employee security awareness. Many companies do not take enough time outside of crises to make employees aware of cybersecurity risks.

Human awareness is one of the foundations of an information security management system, because a company can put in place all possible and imaginable security tools, if it does not raise awareness among its employees, its information system will remain exposed to attacks that exploit the weakest link: the human.

Phishing attacks exploit human vulnerability in particular, employees who are not trained and made aware of these risks, or are put in extra pressure from working remotely, are an ideal target for attackers.

Normally, this type of employee is already widely targeted by hackers, but during COVID-19, this vulnerability has become even more critical. Many employees have had to manage their personal lives, take care of their children at home, and at the same time manage their professional activities with more pressure because a lot of businesses are at stake.

The lack of support for the employees was felt during this period, especially for those who saw their loved ones affected by the disease and faced an uncertain future. There have been cases that these employees focused all their attention on their personal lives and were less and less concerned with the fate of their businesses.

The sense of belonging in the company is a pillar of vigilance. Nevertheless, during this unprecedented crisis, this sense of belonging has been largely affected. In particular, the lack of contact between employees following remote working and mandatory lockdown have been substantial to this.

This is where phishing attacks come to play. The lockdown has considerably limited verbal exchanges that employees of a company or a team usually have within a company. This limitation favors isolation and then benefits hackers who exploit the most vulnerable employees, the most timid, those who do not dare to disturb others by phone to ask a question after receiving a suspicious mail or an unusual phone call.

4. Use of unusual (often free) tools

Another reason that can explain the growth of phishing attacks is the use of unusually deployed tools by companies and professionals. During this health crisis, several companies used web-conference tools, open-source, or free project management and task-sharing tools. This has significantly increased the risk of leaking and capturing sensitive data that allow hackers to collect information needed for phishing attacks.

The companies that used these tools did not have the time or resources to assess their level of security or perform a risk analysis to identify the potential risks on the internal information system and the business.

The urgency of the situation has led these companies to choose completely unknown tools by simply searching the internet search engines. The risks of making a bad meeting and deploying tools containing malicious spyware climbed to the ceiling.

Some companies, not only took the risk of deploying tools totally not controlled from a security point of view, but even when it was found that one of these tools was vulnerable, they were unable to change it or replace it because the pressure of business continuity was so strong.

Take a case that has generated a lot of ink during the COVID crisis, the case of the Zoom web-conferencing tool. As the global COVID-19 pandemic has abruptly shifted everyone's working environment from office to home, virtual meetings quickly became a necessity for just about everyone I know.

As a result, the use of Zoom reached an all-time high usage in mid-March thanks to its incredibly easy-to-use multiplatform video conferencing service. Several thousand companies around the world have opted for this tool.

Nevertheless, in April 2020, several security vulnerabilities were revealed, such as the disclosure of users' personal data to Facebook, or eavesdropping issues while holding video conferences and calls, or even exposure of the windows passwords to other users.

Well, despite all this information about the proven flaws of this tool, companies have continued to use it and continue to use it until today because of a lack of alternatives. It is of course necessary to mention that these vulnerabilities have been corrected by Zoom.

5. The technical barrier between personal and professional life is crossed

The last reason that can be mentioned in this article is crossing the barrier between personal and professional life of employees, from a technical point of view. This has been manifested clearly and concretely through the use of work tools, such as the smartphone or the computer, as personal tools, or vice-versa!

Many companies have been obliged to tolerate the personal use of the tools made available to employees. Or in the opposite case, some companies have had to rely on the advantages of BYOD (Bring Your Own Device) to enable workers to carry out their activities using their own equipment.

Unfortunately, these uses have only made things worse and therefore increased the risks of phishing attacks. Indeed, these uses were due, for example, to the attribution of the rights of employees' administrators on their professional machines, so that they could install non-standard tools such as web-conferencing tools.

Beyond this case, the use of children's entertainment tools on these machines has also become a source of threat to the information system and the business.

Concerning smartphones, for example, the explosion in the development of entertainment applications especially for children was remarkable, several cases of malware have been detected on these apps installed millions of times on smartphones used for business purposes.

Some Phishing Statistics

The sudden outburst of phishing attacks during the COVID-19 period is a fact that has been noted by many cybersecurity specialists, such as Barracuda Networks, Cisco Systems, McAfee, Symantec, Radware, etc.

In an interview conducted in France and published on their website on 5th of May 2020, France Inter welcomed Mr. Didier Schreiber, Marketing Director at Zscaler (4,000 customers worldwide, the monitoring of more than 150 data centers worldwide). In this interview, Mr. Schreiber emphasized the frightening increase in phishing attempts detected by Zscaler in saying:

> **"Our job is to analyze more than 100 billion requests every day (that's ten times more than Google, for example), and of those 100 billion, we analyze more than 150 million threats that we block every day. Since January 2020, with the coronavirus crisis, there has been an increase of over 30,000% in phishing-type computer attacks, malware, malicious sites targeting remote users. In January, there were 1,200 Covid-19-related cyber-attacks... and 380,000 cyber-attacks in early April!"**

Then, he goes on to cite the techniques used during this period: "We know that cyber hackers have used fear, fear of people with websites created in a few hours, new domain names, fake interactive cards on the number of cases infected country by country, the number of deaths... or fake masking sites."

Phishing Attempts Have Increased by 667% during COVID-19

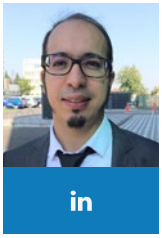
Another very interesting example, according to Barracuda, the provider of cloud-enabled security solutions, is that a 667% increase in phishing attempts was recorded in March. $12 billion has already been lost as a result of harpooning and account takeovers.

According to the report, between March 1 and March 23, Barracuda detected 467,825 spear phishing email attacks, and 9,116 of those attacks were related to COVID-19, representing about 2%. In order to make a comparison, a total of 1,188 coronavirus-related email attacks were detected in February, and just 137 were detected in January.

How Can Companies Prevent Phishing Attacks?

Crises significantly promote the growth of phishing attacks, but the risk of phishing attacks, which is becoming more and more severe, can be significantly reduced through a security approach that includes the following processes:

- Consider employees to be the first line of defense and the weak link generally targeted by attackers. Therefore, it is critical that each organization focuses on training and awareness of data security practices.
- Build and test business continuity and recovery plans to avoid panic and disruption of services during crisis periods. These plans should detail the processes and tools to be used in times of difficulty to avoid risky uses and malware.
- Implement and reinforce attack detection through the use of security detection tools or cloud-outsourced services. Cybersecurity teams should also work in conjunction with fraud risk management teams to coordinate detection and response activities.
- Perform regular security checks by auditing systems, networks, and exposed servers.



About the Author

Soufiane Tazarine
Security Auditor and Pentester at Orange France - PECB Security Certified Trainer

Soufiane has been an expert IT security engineer for 11 years and is passionate about cybersecurity. He has been involved for many years in large companies on very diverse IT topics. He has an ability to analyze systems and networks and has been able to intervene in the areas of finance, telecommunications, information technology, and other industries. He has worked on several security-related jobs during his career, including positions as a general consultant, risk manager, network solutions security architect, before currently arriving at the organizational and technical audit (pen tester).

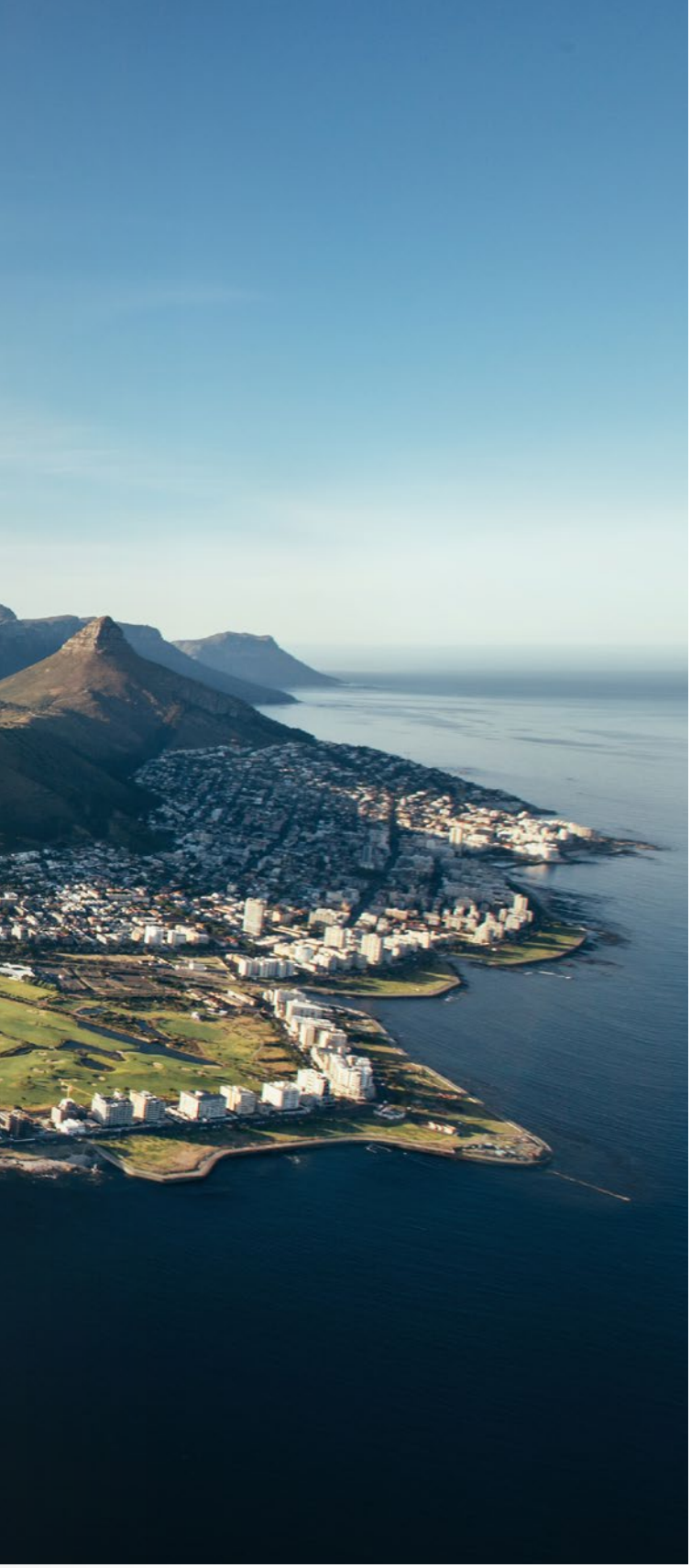
In addition to his profession, Soufiane is also a PECB-certified security trainer and has also earned several certifications such as ISO/IEC 27001 Lead Auditor, CCSP, and PECB Lead Pen tester.

Sources: SecurityBrief Asia, Barracuda, France Inter, sslstore, OECD

PECB advises you to avoid traveling nowadays due to the ongoing COVID-19 outbreak. However, make sure you add this incredible destination on your travel bucket list.

CAPE TOWN

THE TAVERN OF THE SEAS



Cape Town is a story book of some 370 years of history dating back to 1652, when the Dutch East India Company established a small outpost at the bottom of the iconic Table Mountain.

It has been voted as one of the most beautiful cities in the world — and to most South Africans it still is. It remains a favorite holiday destination for South Africans seeking a change from the frenetic pace of Johannesburg and Pretoria.

Cape Town is more than just a city. It is the starting point for most visitors, but its delights stretch well inland into the range of Sandstone Mountains along the bottom of the continent of Africa. The keen explorer may find fascinating historical places in any direction along the coast, into the interior or to the bottom of the peninsula.

Here we take a sightseeing trip around the peninsula to share some of the beauty and history. This article can only scratch at the surface and we should apologize in advance for omitting so many interesting places such as the Cape Castle, the Gardens, Groot Constantia, the V&A Waterfront, and Bloubergstrand — the list is endless.

Getting Around

The city is nestled in the bay below Table Mountain at the top of the Cape Peninsula — a long strip of sandstone mountains layered on ancient granite extrusions that separate the Indian and Atlantic ocean. The visitor soon succumbs to the notion that Cape Town means the whole peninsula and all the towns and sights across the flats to the mountains in the distance and up along the Atlantic coast to the North.

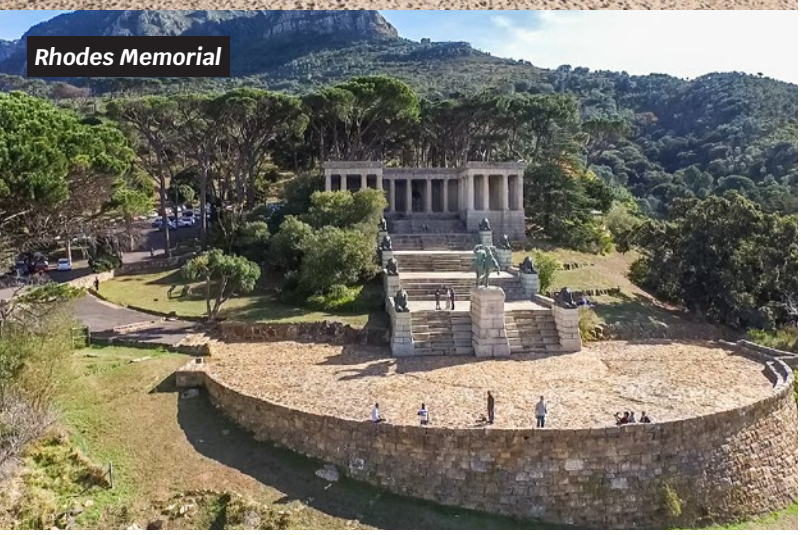
The public transport is good, and there are many tourist services such as sight-seeing bus tours and you can take the train from Cape Town station all the way to the Simon's Town Naval base, although to genuinely take in the sights, a hire car is a very good alternative. The freeways and roads are excellent, but use a GPS if you are venturing away from the peninsula as it is not difficult to get lost or end up in the wrong place. The suburban train service will take you to many places and a special journey that you can take is the trip from the city center along the coast to Simon's Town where the story of “Able Seaman Nuisance” can be found. But more of that later.

Table Mountain

The feature most associated with South Africa and the city is the view of the Table Mountain. The Table view road offers a panoramic drive across the base of the mountain, while the view from the top can be accessed if you take the Cable Way from the Eastern (right hand) end of the mountain from Kloof Nek. If you are into hiking then you can take a walk up "Platteklip Gorge" — a steep but easily accessible route to the top. It will take a morning to do this route because you will want to come down again! Just take care of the weather because the clouds can roll across the top in a matter of minutes to create the famous "tablecloth" when the visibility can drop to a few feet and you could lose sight of the restaurant and Curio shop at the Cable Station.

The view to the west overlooks some of the most valuable coastal properties in the world and the famous Clifton beaches.

Muizenberg Beach



Rhodes Memorial

A Drive around the Peninsula

If you have a car, you can take a leisurely day driving around the Peninsula to visit the seaside villages, towns, and sights. Drive out of the city westwards on the freeway towards de Waal Drive. This will take you around Devil's Peak to the east of the mountain around Rhodes Estate and past the Groote Schuur hospital where Dr. Chris Barnard performed the first heart transplant in 1967. This route passes Rhodes Estate, the University of Cape Town, and the Rhodes Memorial, and eventually to the southern reaches of the peninsula.

The drive will take you through Muizenberg, a popular surfing spot on the False Bay (Indian Ocean) coast. False Bay is some 60 km wide and is a natural habitat for Great White sharks.

Beyond Muizenberg on the main road is Rhodes Cottage Museum, which was once Rhodes' private retreat, where he also spent his last days. For those interested in history and are curious about the imperial dream, the cottage serves as a museum that commemorates his life, achievements, and death.

Our next stop is at the fishing village of Kalk Bay. If you are there early enough, you may be able to buy some of the fishing boats' catch as they barter on the harbor side. The traveler's guide claims that there are at least

25 restaurants in Kalk Bay! One of the most famous of these that offers great seafood is the Brass Bell right on the edge of the small fishing harbor and tidal pool.

Fish Hoek

Fish Hoek was a “dry” town for some 200 years until 2018 when an appeal by a major chain store was successful in overturning the historic 1818 title deed restriction. This prohibited the sale of liquor in the area which meant that visitors had to bring their own tipple to the beach.

A favorite holiday spot for families, the swimming at Fish Hoek is safe and sheltered with a shallow gently sloping seabed and a promenade along the coast over the granite boulders.

At Fish Hoek you can take a short cut across the peninsula to the Atlantic side of the peninsula with access to “die Ou Kaapse Weg” (Old Cape Road) and many hiking trails across the southern slopes of the mountain, but let’s carry on around to Simon's Town.

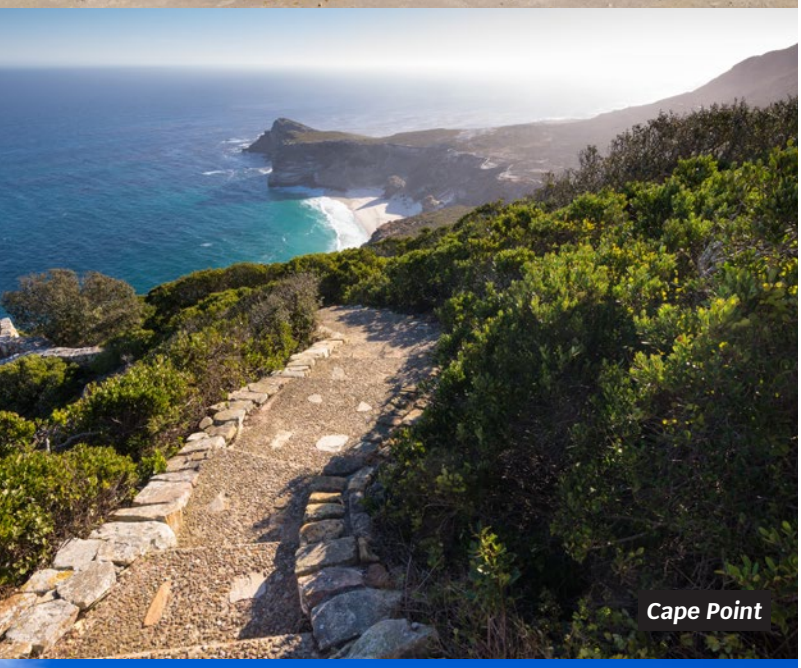
Simon's Town

From 1743, there was an influx of people of Dutch Batavian descent into area due to Simon’s Town becoming an anchorage for the Dutch East India Company.

Later it was a key Naval Base during the days of the British Empire, and especially during World War II, vital in protecting the shipping lanes between the UK and the Asia-Pacific. The coastal batteries can still be seen from those days. It is the home of the South Africa Navy and the main base for the submarine force. There are many shops, monuments, and museums, and one could spend all day exploring this historic town’s nearly 300-year history including the SA Naval Museum, the Heritage Museum and the Simon's Town Museum.

Another historical landmark, located in Simon’s Town, is the statue of Able Seaman Just Nuisance. A granite headstone of the only dog ever to be officially enlisted in the Royal Navy. Between 1939 and 1944 he served at a Royal Navy shore establishment in Simon's Town called HMS Afrikander. He was a very sociable dog, which followed sailors around the town, and he started to take trips on the train. Even though he was thrown off from the train, he learned his way back to Simon’s Town, and depending on his mood, he would go back or wait to board the next train. The railway officials got tired of the dog and started to complain. This made the sailors take this case to their superiors. After this, a weird decision was made. The dog was enlisted to the Royal Navy and he would be entitled to free rail travel. This turned out to be a great idea because he became a morale booster for the troops serving in the war.

Boulders Beach



Cape Point

Slangkop Lighthouse

Boulders Beach Penguin Colony

For conservationists and wildlife lovers there is a special secluded beach in Simon's Town, great for swimming and diving among the kelp forest. It is also home to a protected colony of African (Jackass) Penguins. In 1910, the estimated number of African Penguins was around 1.5 million. Later these birds were considered as endangered species. There were only two breeding pairs remaining by 1982. In recent years, the Boulders colony has grown to over 3,000 birds due to the great preservation efforts.

Cape Point

The last southbound stop on the round trip, apart from the scenery along the coast, is the Cape Point National Park. Although not the southernmost point of Africa, it marks the division between the warm Indian Ocean and the cold Atlantic. The lighthouse and restaurant at the southernmost point are accessible through the park which is stocked with several species of African wildlife and countless baboons.

Do NOT feed the baboons if you value the external parts of your vehicle or the contents of your handbag. They can spot a tourist from a mile away!

The Two Oceans restaurant is accessible up a long steep walkway or a shuttle and offers great food and excellent views in all directions, especially across the 70kms across False Bay to Cape Hangklip, Gordons Bay, and the Winelands, where the touring explorer could spend even more time, but that is a trip for another time.

Scarborough

Carry on back to the main road from Cape Point and turn west to travel along the Atlantic coast. The small holiday resort of Scarborough Beach offers great accommodation for holidaymakers seeking quiet relaxation away from the madding crowd and some great surfing. Just a reminder: this is the cold ocean!

Keep a lookout for the curious sandstone formation aptly called “Camel Rock” and its namesake restaurant.

Kommetjie and Slangkop Lighthouse

The cast iron Slangkop lighthouse was built in 1914 and is still a key navigation aid to ships rounding the continent being visible some 33 nautical miles out to sea. It is now a tourist attraction, but you will have to book a tour. There is plenty of accommodation at Kommetjie and even a tented camp.

Camps Bay

Chapmans Peak

Beyond Kommetjie you reach the road across the peninsula to Fish Hoek, but we will keep to the coast and across Chapmans Peak Drive to Hout Bay. For the geologists amongst us, this road was built along the cliffs at the contact point between the ancient granite bedrock and the sandstone of the mountain, which is clearly visible at each of the 114 curves in the 9 km road. Considered an engineering feat when first built in 1922, it required some 1000 feet of cliff face to be excavated at various points.

Hout Bay

At the end of the drive you reach Hout Bay, so named because it was a great source of timber for the 17th century Dutch inhabitants of Cape Town. The view as you round the end of Chapmans Peak is one of the most photographed in the area, and reveals the peak known as the Sentinel. On the seaward side you can spot the old 18th century cannons guarding the entrance to bay and the bronze leopard statue on a granite boulder, sculpted by Hout Bay resident Ivan Mitford-Barberton in March 1963 as a memorial to the wildlife that once called the area home.

There is a bustling harbor for the trawler fleets of South Africa, and a great selection of restaurants and cafes all around the bay.

You can also take the boat trip around the sentinel to a seal colony on a rocky outcrop on the ocean side and commune with these inquisitive and friendly inhabitants.

For adrenaline junkies, there is Dungeons beach behind the Sentinel which is accessible only by boat.

> **According to the website of sa-venues.com, Dungeons offers "...the most ultimate extreme surfing experience for well-seasoned big wave riders and lunatics." Some say "the waves are big, but so are the sharks!"**

At this point in our journey there are two choices. We can take the road over the mountains to the oldest wine estate of Groot Constantia founded in 1685, and Wynberg, or continue along the coast to the city; but let's take the road to the coast.

Camps Bay

Over the hill, the road drops down to the sea and travels along the base of the mountain cliffs dubbed the 12 Apostles and into Camps bay with its beautiful beaches and rock pools.

This is a really beautiful (and romantic) place to stop and watch the sun set over a glass of wine or dinner at one of the restaurants such as Ocean Blue and Café Caprice.

Around Signal Hill

The road then skirts around the base of Signal hill through Clifton, through Sea Point, Green Point, past the Moullie Point Lighthouse, and World Cup 2010 Stadium, finally dropping you back in the city at the entrance to the Victoria & Alfred waterfront, just in time for dinner, and if you are lucky enough, the chance to plan the next day's excursion.

Business in Cape Town

In Cape Town, there is a strong emphasis on a healthy work-life balance with some larger organizations enabling their personnel to end their working day at four pm. Business interactions therefore tend to be open, friendly, relaxed but purposeful which is different to the competitive goal-driven and frenetic atmosphere of Johannesburg, New York, or London.

Cape Town has preserved many of its oldest buildings and made them available as business premises. The tall buildings on the city foreshore are built in land reclaimed from the sea which makes the center a curious mix of century-old architecture and modern skyscrapers. In the past few decades, satellite business centers have developed and become major hubs that attracted many large organizations and brands.

Most recently, there has been an influx of technology companies and young entrepreneurs attracted to the lifestyle and opportunities in the Cape. Those living in the hustle of business inland have dubbed them "semigrants" — those who have not left the country but escaped the rat race! Cape Town is really becoming the "Silicon Valley" of South Africa.

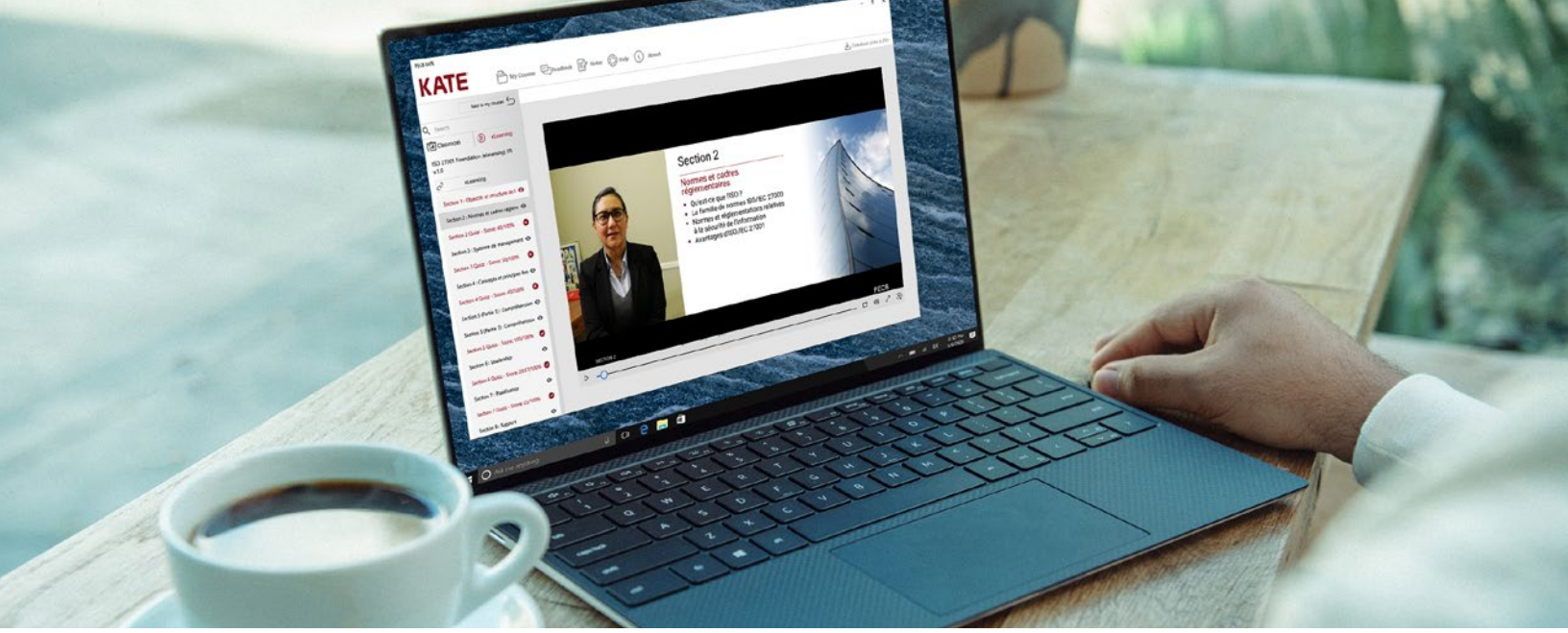
in

About the Author

Brian Henry
CEO of The Caridon Group

Brian has been involved in business and Information Technology since 1970, and has consulted in Business Continuity since 1986. He is the founder of the Caridon Group, based in Australia and South Africa, providing business and systems consulting, with skills in governance, compliance, and risk. He has served for over 17 years as a management consultant with three of the Big-4 consulting houses, providing support to client management on business systems issues including security, business continuity, risk and impact assessments, organizational restructuring, and strategic planning.

Brian holds the following certifications: ISO 9001, ISO 22301, ISO/IEC 27001 and ISO 37001 (Anti-bribery MS) Lead Auditor and Lead Implementer. He is a PECB trainer and has been delivering their internationally accredited Auditor and Implementer Certification training courses since 2013. Brian has been a founder member and Fellow of the Business Continuity Institute since 1994 and is a registered BCI Mentor. He served as Chairman of the SADC Chapter of the BCI from 2013-2019 and as a member of the ISO TC292 Working group.



The Significance of eLearning in the Modern World — What Approach Has PECB Adopted?

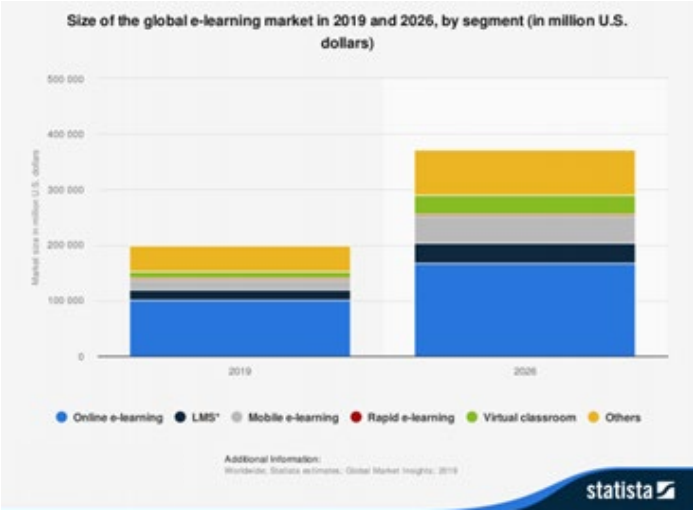
BY JETË SPAHIU HOXHA AND LUNDRIM SADIKU, PECB

What does the future of the eLearning industry look like?

The global eLearning market capital reached more than USD 200 billion last year, and this figure is expected to grow to almost USD 400 billion by 2026. This value has seen constant growth in all regions of the world, with North America and Europe being in the lead.

A study shows that the most widely distributed online courses belong to the category of "business and management" with more than 16% of the market share (the highest figure of all categories). Furthermore, the same study suggests that a growing number of companies aim at covering the cost of completing certified courses in an effort to improve productivity and performance, apply knowledge and skills into practical results, and educate employees.

With more than 60% of the training budget allocated for travel costs, it makes a lot of sense in terms of financial resources that companies are trying to find other ways to reduce the costs and increase the benefits of their training programs.



Source: Statista 2020

Taking into account the figures and trends mentioned above, it is not surprising that PECB seeks to expand the means of offering more eLearning training courses in addition to the traditional in-class training courses.

Is there a silver lining of the lockdown?

The year 2020 taught us one extremely valuable lesson. The things that we often take for granted, especially physical mobility, are in fact quite fragile. Even though the eLearning project at PECB started long before the lockdown, the new circumstances have only accelerated the pace of the project.

Now, more than ever, PECB is seeking ways that can modernize how we provide our services.

What are the benefits of taking a PECB eLearning training course?

For our candidates, the benefits are numerous! You were not paying attention to a certain section? No problem, just replay the video. You do not feel like listening to the trainers and reading the training course materials helps you learn best? No problem, just access the training course materials via PECB KATE.

Ultimately, the best thing about an eLearning training course is the unlimited accessibility. It really does not matter if you are in your office or in your bedroom for as long as you have internet access. You do not have to worry about traveling to the place where the training course session is being held or about canceling plans because schedules overlap.

What is even better is the fact that you can take control of your own time and manage your own schedule. You can return to the eLearning training course any time you want.

On the other hand, for companies themselves, eLearning reduces training costs significantly. It also enhances the knowledge retention for the employees and it provides them with crucial information sources for strategic challenges (e.g., designing and implementing an Information Security Management System (ISMS) within an organization).

Updated training courses, furthermore, are a source of cutting edge information for various fields.

In a nutshell, eLearning offers flexibility of time and place, as well as a personalized pace for your study; it reduces costs and provides solutions to strategic challenges.

How are the eLearning training courses designed?

Our eLearning training courses have been designed to meet the needs of those who have limited time and resources to attend a training course session.

Each eLearning training course that is published on PECB KATE is divided into several video sections and subsections. Videos last no longer than 20 minutes and contain animations to support what the trainer is lecturing — the animations correspond to the sections provided in Microsoft PowerPoint in the traditional mode of training. To keep our candidates engaged, we have incorporated quizzes into our eLearning training courses.

PECB has invested a great deal of capital, time, and effort in its online platforms (i.e., PECB eLearning, PECB KATE, PECB Exams) so as to offer digitalized services to our clients. Now, you can access our training courses via PECB KATE, take the exams, proctored online by PECB, and obtain our certificates FROM ANYWHERE, AT ANY TIME!

What PECB eLearning training courses are already available?

The eLearning training courses already available on PECB KATE are:

- ISO/IEC 27001 Foundation in French
- ISO/IEC 27001 Lead Implementer in French

For the success of these eLearning training courses, we collaborated with our trainers who presented not only the training courses provided by PECB, but also information from their expertise in their specific fields.

What PECB eLearning training courses to expect?

Right now, the eLearning team is working on expanding the offer. The following eLearning training courses are under way:

- ISO/IEC 27001 Lead Auditor in French
- ISO/IEC 27001 Lead Implementer in English
- ISO/IEC 27001 Foundation in English
- ISO/IEC 27001 Lead Auditor in English

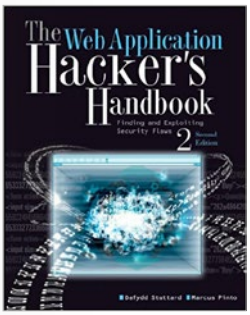
Has your local government imposed lockdown measures to contain the spread of COVID-19? Not sure if the lockdown will be lifted anytime soon? Yet, you want to continue to learn and grow professionally... You now have a choice!

Ultimate Hacking Books

As organizations are increasingly understanding the need to keep their clients' information safe, the need for cybersecurity professionals is rising. This is because in order to be able to stop hackers and cyber criminals you need to have their mindset. How to keep your organization safe from rising threats? How can you reduce the risk liability from a breach? This can be done by employing a white-hat hacker (ethical hacker) that performs activities in an attempt to penetrate the network and test the organization's network security system in order to protect the infrastructure. These activities are performed after getting permission from the organization.

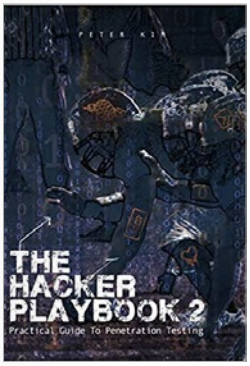
Even though ethical hacking is a practical process and requires hands-on activities, reading these books it will be a great start. Show your commitment to security by pursuing a career in Ethical Hacking, as there are plenty opportunities ahead.

Want to have a proactive approach and see beyond the existing network's security system? Start here by reading these top recommended books.



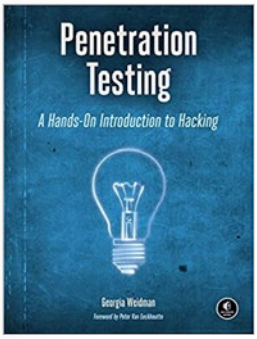
The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Marcus Pinto and Dafydd Stuttard

Web applications are the front door to most organizations, exposing them to attacks that may reveal valuable information. Considering today's significant cybersecurity exposures, it is important for organizations to take the necessary actions to prevent and mitigate malicious attacks. This book is intended to teach you how to overcome these attacks and the steps required to prevent them. Moreover, it covers discussions on remote frameworks, Hybrid File attacks, UI redress, Frame busting, HTTP Parameter Pollution, and much more.



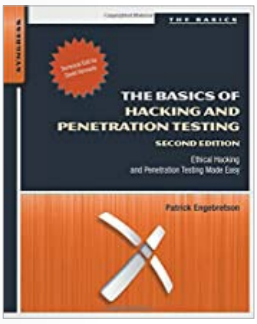
The Hacker Playbook 2: Practical Guide to Penetration Testing by Peter Kim

This is a great book which not only consists of a step by step guide of penetration hacking but also it provides practical examples and valuable advice. In the book, Peter Kim includes the latest attacks, tools, and lessons learned from these attacks. It definitely is a good baseline to start with hacking/penetration testing if you are just getting started in the field. It has simple explanations and a good approach to use with Kali Linux.



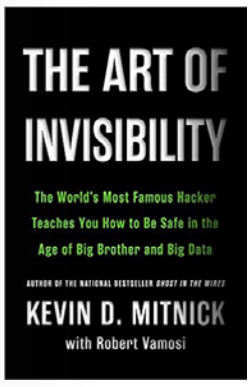
Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman

Are you new to penetration testing? This book is an excellent book if you are at a beginner level because it provides you with the required skills and techniques that you need for pen testing. By using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, the author introduces users on how to run practical lessons with tools like Nmap, Wireshark, etc. The hands-on lessons introduce you to the techniques and strategies that you can utilize for Penetration Testing.



The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy by Patrick Engebretson

In this book, Patrick Engebretson with simple explanations shows how to perform penetration testing, and how to effectively use ethical hacking tools. With practical examples and exercises, you will obtain the required knowledge to start your ethical hacking career. The book covers different tools like Nmap, Metasploit, Backtrack Linux, Netcat, Nessus, etc. If you are new to the field and you want to get a basic understanding of penetration testing and hacking, this will be a great read.



The Art of Invisibility by Kevin Mitnick

A practical book by the world's most famous hacker which shows what is happening through real-life stories. Kevin gives step-by-step instructions on how to minimize your online footprint and protect yourself and keep data safe. This book is a must-read considering today's security issues we are continuously facing. Nothing we do online is private anymore. Are we really all being tracked? Even though becoming invisible is a very challenging task, in this book you can find valuable information on how to strengthen personal security.

Visiting PAMUKKALE

Hot Springs and Ancient Ruins in Turkey

BY WANDERINGCAROL

With its healing thermal springs, white-crusted hillsides, and bird-bath sized pools terraced down the slopes, the ancient spa town of Pamukkale and the ruins of Hierapolis is one of the most unique destinations in Turkey to visit. Here's what you need to know.

PECB advises you to avoid traveling nowadays due to the ongoing COVID-19 outbreak.
However, make sure you add this incredible destination on your travel bucket list.

An Ancient Healing Town

The Pamukkale hot springs are legendary, dating back to the 2nd century BC, and the town has been a destination for healing for centuries. Other than the noxious spring in Pluto's Cave, now wisely out of bounds to tourists, the Pamukkale thermal waters are bursting with healthy minerals and are said to be good for circulation issues, skin ailments, heart conditions, and rheumatism.

One of Turkey's Most Stunning Towns

Even more impressive than the Pamukkale hot springs is the scenery. Warm water flows down the hillside above the town, leaving white calcium deposits called travertines that coat the hill like a frozen marshmallow curtain. Small pools, terraces, and stalactites add lacework to the blanket of white, and I had to blink a few times when I first saw it.

Touring Pamukkale

At my hotel I signed up for a local day tour of Pamukkale and the surrounding area. It seemed like a good way to get to know the area, meet other travelers, and ensure that my tourist dollars stayed in the local economy. Our driver's name was Mohammed, but other than that it was an all-female foray made up of Renee from California, Tai-ko from Tokyo, me and our young Turkish guide who I called Ursie because I could not pronounce her real name.

The Red Spring of Karahayit

Surprisingly, the Pamukkale hot springs that paint the hills white are not the only springs in the region. Our first destination was about five kilometers away, a natural hot spring pool in the village of Karahayit.

In contrast to Pamukkale's white hills, the ground around this small iron-rich spring was stained red, while in the distance, dry barren hills were sporadically dotted with pine.

Enjoying the thermal pools in Turkey

Ursie kicked off her sandals and waded into the water which had pooled around the spring. The water was burning hot and I gingerly high-stepped it after her to the far edge of the shallow pool where a stout woman in a headscarf was slapping clay onto her legs.

"For veins," she told Ursie in Turkish. Vein therapy? Count me in. I hiked up my pant legs and started scooping up clay. The woman shouted at me in Turkish, something that sounded like, "Ovmak! Ovmak!" "She says rub it in," Ursie translated.

Pamukkale and the ancient town of Hierapolis

After my impromptu spa treatment, we drove to the ancient ruins of Hierapolis situated high on a plateau above Pamukkale town. Because of the abundance of healing thermal water in the area, in ancient times, Hierapolis became something of a retirement destination for the elderly and a healing resort for the ill.

It was likely because so many people spent their last days here that the Necropolis of Hierapolis is so expansive and impressive — making it a UNESCO World Heritage Site today.

The Temple of Apollo

While touring the Necropolis of Hierpolis (which I like saying because it rhymes), we stopped at the Roman theatre, which was built by the Emperor Hadrian in the second century AD.

Even more interesting is the Temple of Apollo. Apollo was one of the most revered gods in ancient Hierapolis, but at the back of temple compound is where the strange and mysterious Plutonium, also known as Pluto's Cave, is located. When we were there, the grounds had been fenced off by archeologists but someone forgot to latch the gate. Ursie fiddled with it and ushered us through.

> **"I hope we don't get arrested," Renee said.**
>
> **"No problem." Ursie smiled. "My father is the police."**

Pluto's Cave

Pluto's Cave was dedicated to the god Pluto, also known as Hades, the god of the underworld. It was discovered by Italian architects in 1965 but it is probably as old as Hierapolis itself, which dates back to 190 BC. We walked over the old foundations of the temple to the stone structure built around the cave. Tucked around a corner a small weathered arch marks the entrance to a poisonous spring. It was my first realization that not all hot springs are good for you. In fact, if you breathe in the fumes, which are high concentrates of carbon dioxide, it can kill you.

Deadly as this dark grotto is, it served to establish Pamukkale's reputation as a sacred site. Priests, trained to hold their breath, would go in with an assortment of small animals, which would keel over beside them. These deadly displays contrasted with the priests' miraculous invincibility proved that Hierapolis was a place of the gods.

Ancient ruins in Hierapolis

Entrance to the poisonous Pluto's Cave

The Pamukkale Hot Springs

Our history lesson on Pamukkale and Hierapolis complete, it was time for a dip in a nearby calcium pool. And unlike Pluto's spring, this water is mineral rich and healthy. Swimming is forbidden in most of the travertine pools to protect the delicate environment today, but Ursie knew of one off-the-beaten-path spot where it was allowed. High on the hill, we stripped to our bathing suits.

"You have to rub the lime from the pools onto your body," Ursie said.

"For veins again?" I asked.

"No, exfoliation."

Hierapolis ancient theatre

This Pamukkale day tour was rapidly turning into a DIY spa tour — and I could not think of a better way to sightsee. Stepping into a small natural pool on the hillside, I started slathering soft white muck on my body.

After I had rubbed, rinsed, and repeated, I sat on the calcified curves of the hill and looked down over the throngs of tourists below, strung in a row along the travertines like a brightly-colored thread as they walked down the white hillside. There were a lot of them.

Day tourists flock to Pamukkale, so stay overnight for the real experience

Be forewarned. Bus tours arrive in Pamukkale in formidable numbers during the day en route to bigger draws like Ephesus, 215 km west. Then once the sun sets the buses move on and Pamukkale returns to its sleepy self.

But right now the crowds were at their thickest and for our last stop we could not avoid them. Cleopatra's Pool, also called the Sacred Pool or the Antique Pool (you can never have too many names!) is one of the area's biggest attractions. Fed by Pamukkale's thermal water, and known for its curative properties, the Sacred Pool has been hosting bathers for centuries.

In fact, the water is the foundation around which the healing town was based, and I do not think I have ever seen such an atmospheric pool with brilliant green water and fluted columns that lie in the water like fallen trees.

Pamukkale Hot Springs and the Sacred Pool

I waded into the water and started breast stroking over ruins untouched since they had toppled into the water after an earthquake — it was like swimming over history.

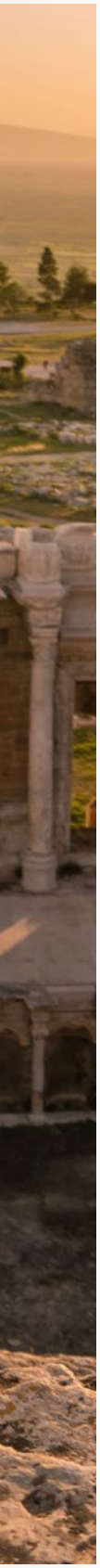
The sheen of algae covering much of the sunken marble in the Pamukkale Sacred Pool was disconcerting, but the thought of Cleopatra swimming here before me propelled me on. If this was her beauty secret I did not plan on missing out. When I questioned Ursie about whether Cleopatra was actually here, or rumored to have been here, she admitted there was no documentary evidence Cleopatra actually swam in the Pamukkale hot springs.

"But she was in the area at the time," she said brightly, "so it's possible."

And it was equally possible that right this minute Pluto was splashing around in his own dark spring up the road. But the beauty of myths is that they are hard to prove wrong. As I perched on a stump of a column, half submerged, small bubbles from the effervescent hot springs coated my body like a champagne bath.

Truly, I thought, Pamukkale is a place of the gods.

Hierapolis ancient theatre



How to Get to Pamukkale from Istanbul

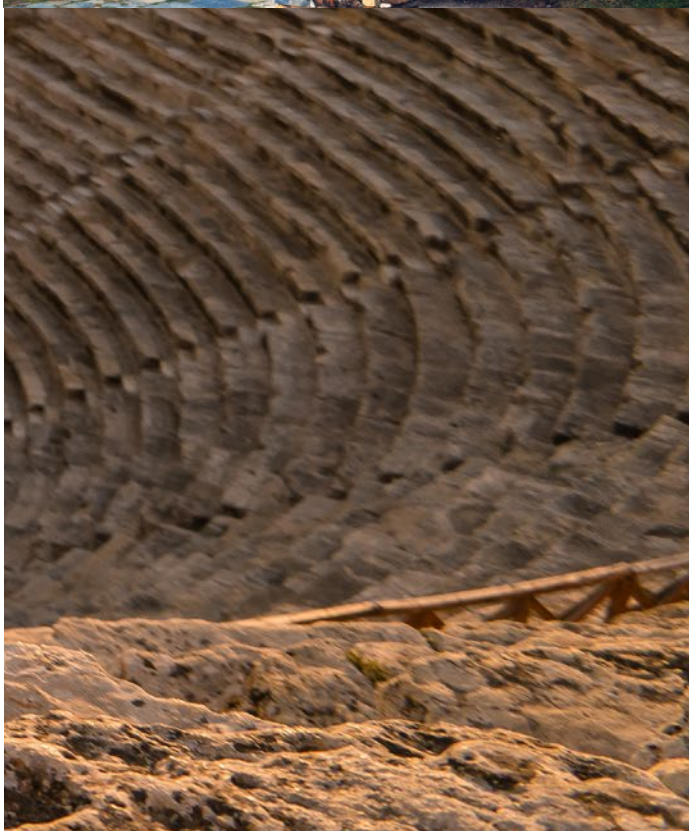
In Istanbul, you can go to just about any travel agent and buy an overnight bus ticket to Denizli. I was alone but I felt perfectly safe and the long drive was not as bad as I thought. (Though coming back the bus was much more crowded and uncomfortable. Just my luck, I guess.) If you have booked a hotel, ask for a pick up from Denizli. From Denizli, you can take a taxi.

If you are on a package tour, Pamukkale is a popular day stop, especially for those en route to Ephesus.

I highly recommend staying in Pamukkale overnight as once the crowds leave it is quite magical.

Red springs of Karahayit

The Ionic Temple of Aphrodite



Things to Do in Pamukkale

Visit Hierapolis

The Pamukkale Hierapolis ticket price is about $10 and there are three entrances — yes, it is that big: Pamukkale Town Entrance, South Entrance, and North Entrance. The cost is about $10.

Swim in the Antique Pool

For me swimming in the warm thermal springs was a highlight. The pool might float over ruins but around the pool is a modern resort complex with loungers, grass, and snack bars. The pool is seasonal, open from April to October and will cost you about $9 to enter.

Visit the Red Springs of Karahayit

My visit was to a small shallow pool, more like a fountain, and there was no fee to enter. Karahayit is about five minutes drive from Pamukkale and there are a few spa hotels here and a wellness park.

Day trip to Aphrodisias

It is easy to find day tours to Aphrodisias, a ruined city with a temple dedicated to Aphrodite, the Greek goddess of love. It is a very evocative site and worth a visit. You will want about three hours there. You can also take a dolmush, which is like a shared minibus. Ask at your hotel for times.

Where to stay in Pamukkale

Pamukkale is really small, but there are plenty of options where you can stay. One of the best hotels is Doğa Thermal Health & Spa, a five-star hotel with a great location. The rooms are spacious and comfortable, and the hotel has a very nice indoor and outdoor pool. Everything is great, especially the Turkish bath.

A great opportunity not to be missed.
Mark your calendar for 16–19 November, 2020.

Discover new ways of working in today's revolutionary digital transformation.

→ REGISTER NOW FOR FREE

PECB INSIGHTS VIRTUAL CONFERENCE 2020

For more information, contact us at events@pecb.com.

We are bringing advanced skills within your reach. Broaden your knowledge through our training courses!

Status	Training Course	Language	
Updated	ISO 22301 Lead Implementer	English	→
Updated	ISO 22301 Lead Auditor	English	→
Updated	ISO 37001 Foundation	English	→
Updated	ISO 22301 Lead Implementer	Spanish	→
Updated	ISO 22301 Lead Auditor	German	→

UNLEASHING A WORLD OF OPPORTUNITIES FOR YOUR CAREER IN AUDITING!

Attend the PECB Virtual Certified Management Systems Auditor training course and become an MS Auditor!

PECB CMSA Remote Training Course Event | American Time Zone

Trainer: Marisol Valenzuela
Date: September 8-10, 2020
Time: 09:00 AM - 5:00 PM EDT
Language: English
Register: noram@pecb.com

PECB CMSA Remote Training Course Event | European Time Zone

Trainer: Anders Carlstedt
Date: September 14-16, 2020
Time: 09:00 AM - 05:00 PM CEST
Language: English
Register: ame@pecb.com

PECB CMSA Remote Training Course Event | European Time Zone

Trainer: Serge Barbeau
Date: September 21 - 23, 2020
Time: 11:00 AM - 7:00 PM CEST
Language: French
Register: francophonie.europeenne@pecb.com

To reserve your seat, contact the organizers of the training course in the emails provided above.

SPECIAL THANKS TO

TITANIUM PARTNERS

PLATINUM PARTNERS

GOLD PARTNERS

Note that PECB Partners are listed as per the credits acquired from January 1, 2019 to December 31, 2019.

To get more information about our training courses,
contact us at marketing@pecb.com.

PECB