PREVIEW

HAKIN9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.17, NO.11

WEAPONIZING RASPBERRY PI WITH THE PENTESTERS FRAMEWORK?

METASPLOIT FROM SCRATCH

EXPLOITING SQL INJECTION
USING ACUNETIX VULNERABILITY SCANNER AND SQLMAP

SMART CONTRACT SECURITY AUDITING

HANDLING ENCRYPTED ASSETS

AND MORE...

Hakin9

TEAM

Editor-in-Chief:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Managing Editor:

Agata Staszelis
agata.staszelis@hakin9.org

Editors:

Bartek Adach
bartek.adach@pentestmag.com

Ewa Dudzic
ewa.dudzic@eforensicsmag.com

Bruno Zwierz
bruno.zwierz@pentestmag.com

Proofreader:

Lee McKenzie

Senior Consultant/Publisher:

Paweł Marciniak

CEO:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:

Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP:

Agata Staszelis
agata.staszelis@hakin9.org

Cover Design:

Hiep Nguyen Duc

Joanna Kretowicz

Betatesters & Proofreaders

Lee McKenzie

Amit Chugh

Jordan M. Bonagura

Alex D

Gabriel Carvalhaes

Matthew Sabin

Aashis

Hammad Arshed

Alex Giles

Ana Coman

Bev Robb

Craig

David Michaud

Nasreddine Bencherchali

Clint Garrison

John Webb

ayoeyitayo

Publisher:

Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Bielawska 6/19
1 917 338 3631

www.hakin9.org

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Hakin9

Dear Readers,

The weather and aura outside are getting bleaker and bleaker (at least in some countries). This is the best time to use those unfavorable external conditions to your advantage! Dedicate this time to expanding your knowledge and getting your hands (and brain) on our new Hakin9 Magazine issue!

You will read about such tools as Infooze or Metasploit. Also, you will follow one of our authors with exploiting SQL injection using Acunetix Vulnerability Scanner and sqlmap. To broaden your knowledge, you will find out about Smart Contract Security Auditing and handling encrypted assets.

You will also learn about weaponizing Raspberry Pi with The PenTesters Framework. Apart from this, you can take a look at a review of some encryption methodologies and an introduction to a new methodology that may challenge the National Security Agency! Sounds exciting, doesn't it? Another mysterious topic brought to you by our author is 'Hacking Destruction Algorithms'.

Last but certainly not least, we have an interview with Karan Dwivedi, a security engineering manager at Google where he leads a team of engineers to reduce risk to the company!

We really hope that you will enjoy this issue's content!

Stay safe,

Agata Staszelis and Hakin9 Editorial Team

TABLE OF **CONTENTS**

4 ***WEAPONIZING RASPBERRY PI WITH THE PENTESTERS FRAMEWORK;*** *DAN DIETERLE*

26 ***METASPLOIT FROM SCRATCH;*** *MTRO. JORGE VÁZQUEZ DEL RÍO*

39 ***INFOOZE;*** *SARTHAK THAKUR*

52 ***INTERVIEW WITH KARAN DWIVEDI***

56 ***(...) AN INTRODUCTION TO A NEW METHODOLOGY THAT MAY CHALLENGE THE NATIONAL SECURITY AGENCY;*** *PAUL F. RENDA*

63 ***HACKING DESTRUCTION ALGORITHMS;*** *WILSON MENDES*

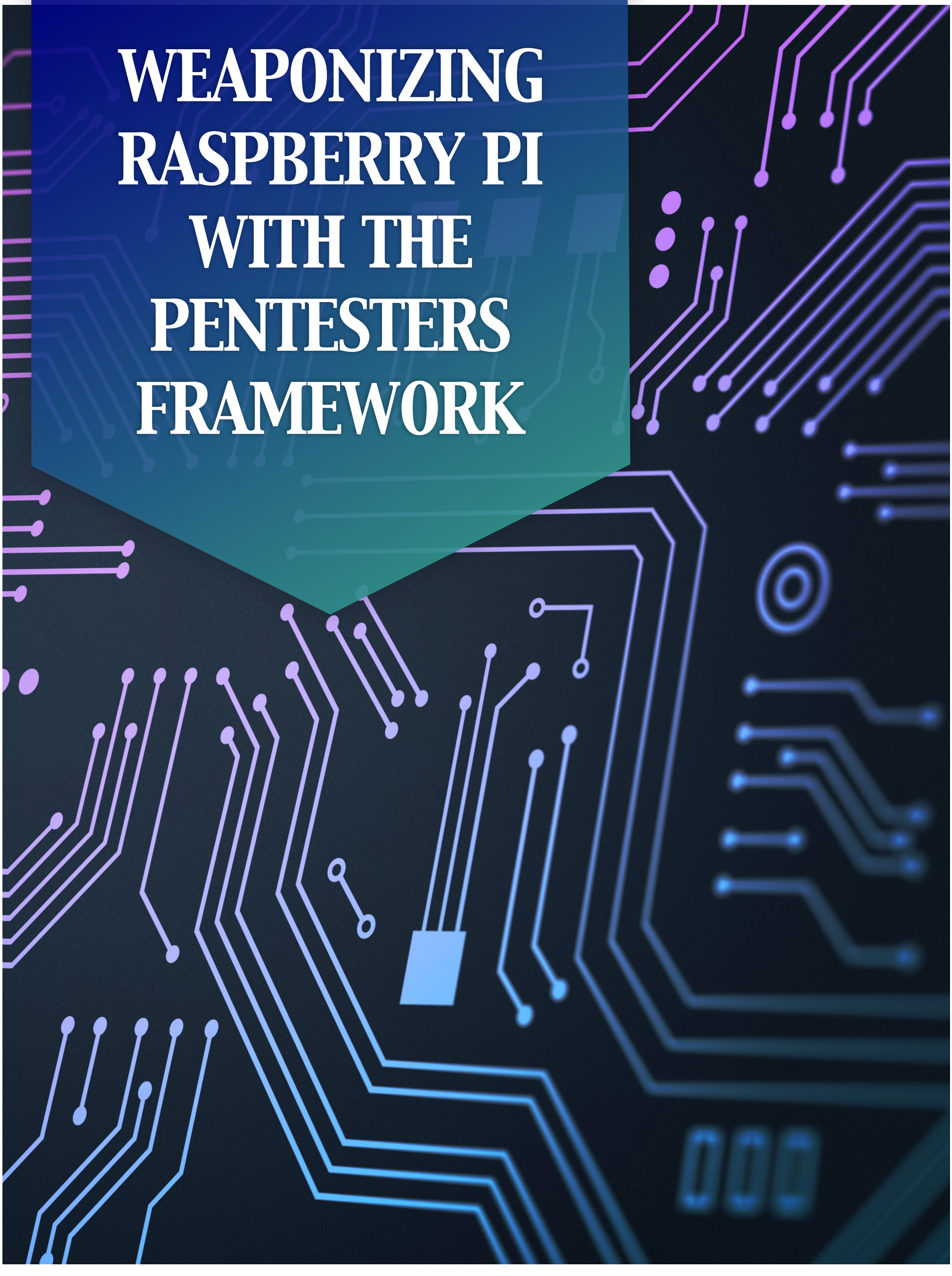
70 ***EXPLOITING SQL INJECTION USING ACUNETIX VULNERABILITY SCANNER AND SQLMAP;*** *ADAM KARIM*

85 ***SMART CONTRACT SECURITY AUDITING;*** *YOUSSEF KHAOULAJ*

94 ***HANDLING ENCRYPTED ASSETS;*** *WASHINGTON ALMEIDA*

112 ***HOW TO CONFIGURE A PHISHING SERVER WITH NGINX, GOPHISH AND SENDGRID;*** *JÚLIO CÉSAR SILVEIRA MÉLO*

WEAPONIZING RASPBERRY PI WITH THE PENTESTERS FRAMEWORK





Daniel W. Dieterle

Daniel W. Dieterle, aka “CyberArms”, has been in the computer industry for over twenty years, and currently is a Security Author, Researcher & Consultant. He is an Internationally Published Author that just released his eighth book, “Security Testing with Raspberry Pi, Second Edition”. He is also working on his next book, a complete overhaul of his original, “Basic Security Testing with Kali Linux”, which will be available next year. Daniel runs two tech blogs - cyberarms.wordpress.com & DanTheIOTMan.com, and is very active as a mentor, helping those new to the security field.

Raspberry Pi Single Board Computers are used very frequently in security. The small and inexpensive units work very well for this function. One of the most popular usage cases is to install Kali Linux and use them directly as hacking stations or configure them as stealthy Pentest Drop Boxes. They can also be used as very cheap security lab training systems. What many don't know is that you can easily use the default Raspberry Pi Operating System (Pi OS) as the base to build your Pi based security testing platform. Most of the conversion and tool installation can be done with one script - The PenTesters Framework. In this article, we will see how the PenTesters Framework can be used on a Raspberry Pi 400 to install over 300 commonly used security testing tools.

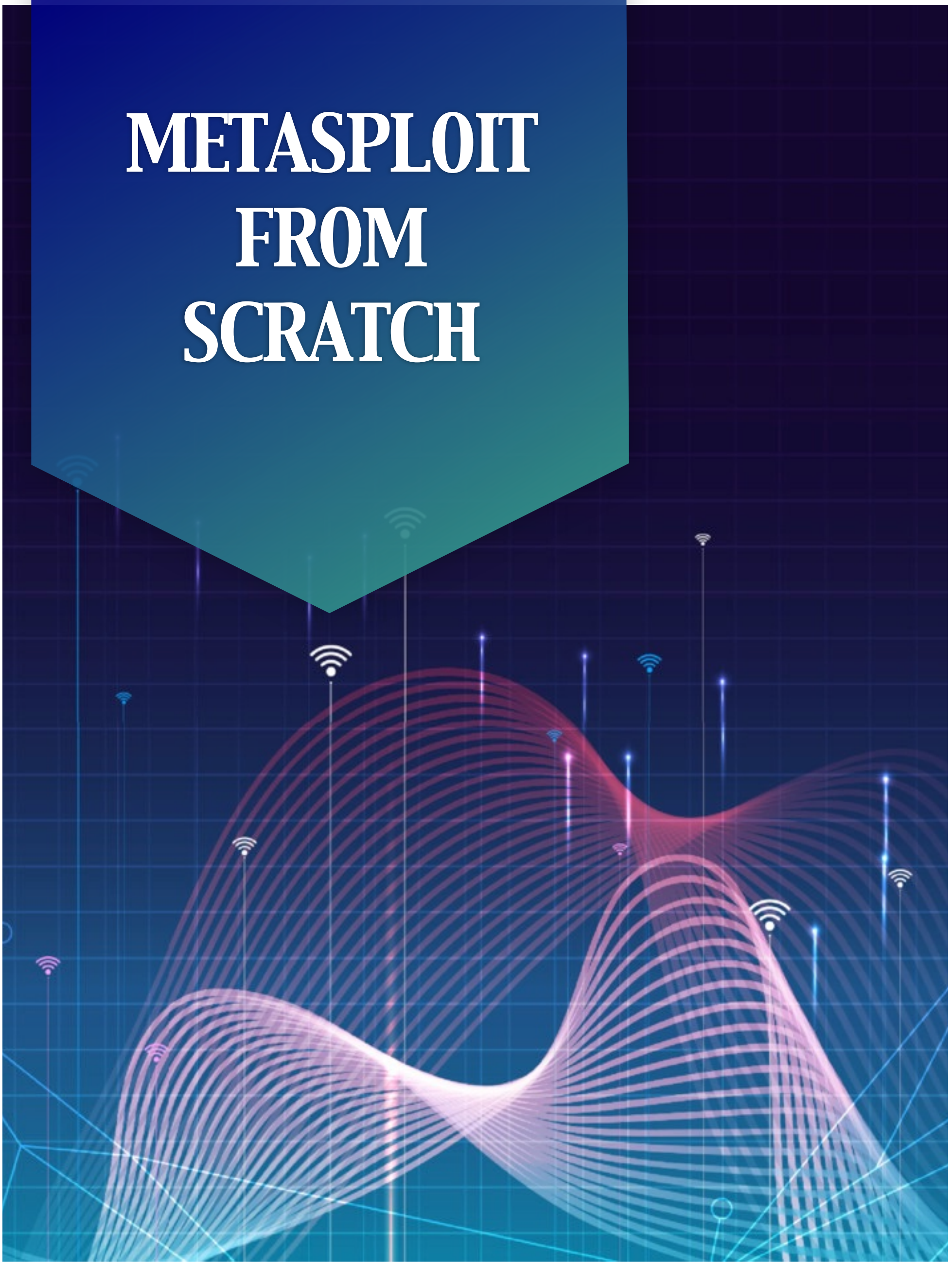


What are Raspberry PIs?

Raspberry Pis are Single Board Computers that are extremely popular in the maker field because of their small size, capabilities and cheap price. The smallest Raspberry PI, the Pi 0w2 is about the size of a stick of gum, and costs $15 USD. The Pi 4b is about the size of a credit card and costs start at $35 USD. The Pi 400, the new addition to the Raspberry Pi family, is an all-in-one keyboard unit that basically contains a modified Pi 4b inside. You can get the Pi 400 in a kit, with mouse, power supply, memory card and an introduction on how to use the Raspberry Pi book for around $100 USD.

A collection of Raspberry Pis running an assortment of Security Tools - Kali Linux, P4wnP1 ALOA, PTF

METASPLOIT FROM SCRATCH





Mtro. Jorge Vázquez del Río

He has more than 25 years of professional experience in the IT area in private initiative and federal government in Mexico. In addition, he is a professor of the master's degree in IT security at the Technological University of Mexico. His academic background is described below. ORC ID 000-0003-4620-9099

- Article published: http://dx.doi.org/10.35429/JTI.2020.21.7.1.18
- PhD Candidate in Information Technology and e-Business
    - Popular Autonomous University of the State of Puebla - UPAEP
- Master's Degree in Information Technology Security
    - Universidad Tecnologica de Mexico - UNITEC, Graduate
- Electronics and Communications Engineering, Degree in Electronics and Communications, Degree
    - Universidad Tecnológica de México - UNITEC, Graduate
- Training Workshop on Internet Drug Trafficking Investigation, INTERPOL - OAS/CICAD.
- Course on Applied Biostatistics and Epidemiology in the Field of Drugs, OAS/CICAD/COPOLAD.
- Global Lynx Ethical Hacking Foundation.
- Introduction to Artificial Intelligence with Python by Harvard University.
- Machine Learning by Stanford University.
- Machine Learning from the University of Michigan.

- Cryptography by Stanford University.
- Bitcoin and Cryptocurrency Technologies by Princeton University.
- Cybersecurity and its ten domains by the University of Georgia.
- Official Associate Certificate GNS3.
- Cisco CCNA (200-125).
- Cisco CCNA Security 210-260.
- Wireshark: Packet Analysis and Ethical Hacking.
- Linux for Network Engineers.
- CompTIA Security + (SY0-401).
- Introduction to Cisco Network Cybersecurity.
- Essential elements of cybersecurity in Cisco networks.
- Network Security.
- Pentesting with Metasploit.
- Recipes of Exploitation of the Windows API: Processes, Tokens and RW Memory.
- Exploitation of Simple Buffer Overflows in Win32.
- Scripting of Wi-Fi Pentesting Tools in Python.
- Wi-Fi Security and Pentesting.
- Wi-Fi Monitoring.
- Network Pentesting.
- Introduction to machine learning.
- Intermediate machine learning.
- Data Visualization.
- Enterprise Java Diploma.

Introduction

Metasploit Framework is a penetration testing technology that has new and enhanced capabilities, including automation APIs, evasion modules, and usability enhancements, and provides security researchers with a variety of tools and capabilities to validate the security of a given application or infrastructure deployment. With Metasploit, researchers can also test exploits against targets to see if they are at risk in an attempt to penetrate existing defensive measures.

Paragraphs:

1. Features

Among Metasploit's key new features is the extensibility of the framework's database back-end, which can now run as a REST web service. By extending the database as a web service, multiple external tools can extract data from the same database and interact with each other; it also adds a common web service framework to expose both the database and automation APIs supporting advanced authentication and concurrent operations.

2. Create a virtual laboratory

The virtualized network is conformed by a Linux distribution called Kali, which can be downloaded from https://www.kali.org/get-kali/, the other operating system used has to do with a computer built from scratch with specific vulnerabilities to perform penetration tests, or pentests, in this sense; Metasploitable 2, available at https://docs.rapid7.com/metasploit/metasploitable-2/ is used.

3. Validation of operating systems in a controlled environment

After the downloads described above and their corresponding virtualization, we proceed to validate that both operating systems are within the same network segment, therefore, a ping is performed to confirm it, as shown in Figure 1.

INFOOZE





Sarthak Thakur

I am pursuing M.Sc. in Cybersecurity from Amity University Jaipur, India. I am a certified Network Penetration Tester and also currently working as a Red Team Intern from CyberSapiens United LLP.

I enjoy trying out new tools and exploiting new vulnerabilities. The more vulnerabilities I exploit, the more my urge to learn more increases.

I am to dive more into the field of cybersecurity research and protect company security against cyber threats.

LinkedIn

INTRODUCTION:

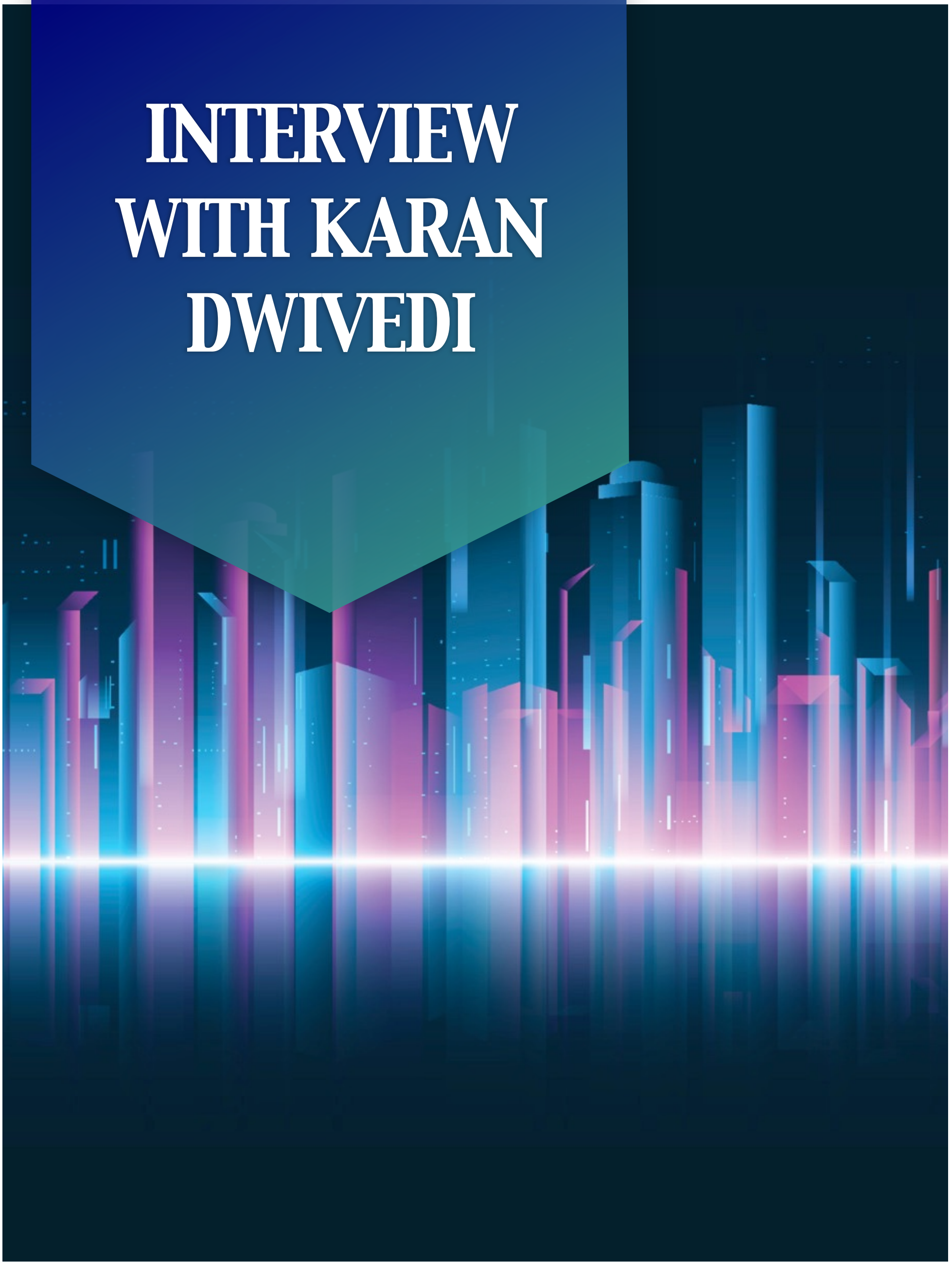
Infoooze is an open source intelligence tool built with Node.js that automates the information gathering process to help users gather information faster and more effectively. Gathering information is always important before launching an attack. This allows us to know more about the target.

Since this is a global package, it can easily be used independently from any directory. All you need is to enter information such as website, IP and username. The rest will be processed automatically.

Infoooze tool features include:

1. Insta Recon
2. Subdomain Scanner
3. Ports Scan
4. User Recon
5. Mail finder
6. URL Scanner
7. Exif metadata extract
8. Whois Lookup
9. IP Lookup
10. Header Info
11. Domain Age
12. DNS Lookup
13. UserAgent Lookup
14. Git Recon
15. Expand URL
16. YouTube Lookup
17. Instagram DP Viewer
18. Save Results to file

INTERVIEW WITH KARAN DWIVEDI



[Hakin9 Magazine]: Hello, Karan! It means a lot to us that you agreed to the interview! It would mean a lot to us if you told us something about yourself.

[Karan Dwivedi]: Thank you for having me! I am a security engineering manager at Google where I lead a team of engineers to reduce risk to the company. Prior to Google, I worked at Yahoo in their incident response team. I was one of the few people in Yahoo at the time who helped respond to the world's largest data breach. I have over seven years of experience in the information security domain specializing in detection and response – digital forensics, incident response, insider threats, network security and risk mitigation. I run a security blog named *allthingspwned.com* where I share interviewing advice for security engineers. I am a regularly invited guest speaker at security conferences, universities, and podcasts.

[H9]: We would like to know how you got started in security. What did your career path look like?

[KD]: I accidentally discovered the world of security when someone on a social media platform said that they could take over my account. At first, the sentence sparked fear in me, however, later I became really curious how they could go about doing it. It was right then that I started reading about information security, vulnerabilities, tools and techniques. Soon after, I decided to pursue the field itself to ensure that no one else falls prey to the situation I encountered. I wanted to protect people and their data without them having to be an expert in the field. I soon realized that I needed to understand the fundamentals of computer science, so I took the traditional path of pursuing a bachelor's degree in it. I started working in Honeywell after graduation in their access control and digital video management team. As I worked there, I realized I wanted to gain more knowledge so I then pursued a master's degree from Carnegie Mellon in Information Security. I landed an internship at Yahoo during my master's and joined them after graduation. Two years later, I moved to Google, which provided me with a tremendous opportunity for growth. I led several projects that impacted the security of products that have more than a billion users.

[H9]: You mentioned that you have your cybersec-oriented blog. What are its most rewarding aspects to you?

[KD]: Yes, I run the blog allthingspwned.com. I initially started the blog with the idea of having articles that help people understand vulnerabilities around us and how they can exploit them (hence the reference to the hacking term "pwned" in the domain name). I later repurposed the name to help people crack security interviews by writing about them. I provide a structured way to help people approach problems and help understand the interviewer's mindset. Writing well thought of articles with easy to understand explanations takes a lot of mental and writing work. Google's security engineering hiring team sends out a link to my blog as a preparation reference to potential candidates. The most rewarding aspect was when I have people come back after they have landed a job and tell me

that they found it really helpful in their preparation. It is messages like these that make my day and motivate me to put out more articles.

[H9]: Since you said you were a guest speaker at a few universities and institutions, we're curious what are the most difficult and rewarding aspects of that. Could you elaborate a little bit?

[KD]: Yes, the most difficult part of delivering presentations is thinking about a great idea, researching it for as long as it takes, getting the content right and refining it until you have something that's a perfect fit for the audience. In 2022, I spoke at six different conferences (Various BSides, National Cyber Summit, etc.), including one keynote talk at Northumbria University. Researching the idea for my conference talk took me a year!

The most rewarding part is recognition in the community. I get to meet and interact with people from various backgrounds and skill levels throughout the year and a lot of times they know about me through my work, talks or my blog. When someone tells me - "Hey I know you from that conference talk you presented at in June and I really liked how you went about researching that idea", it brings me absolute joy.

[H9]: Cybersecurity is changing so fast nowadays and people in it are challenged with more and more surprising problems. Could you share a few of your latest challenges? What made them interesting?

[KD]: From my personal experience, I'm observing that as technology comes closer to humans with wearables, near field communication for payments and the like, information security is becoming an integral part of our lives rather than just another aspect of technology. Securing devices like IoT, most of which talk to us through the public internet, consumers have limited options to monitor the data they are sending and receiving.

Because of how security has become so critical in our lives, another ongoing challenge is how do we, as a community, go about educating users who are generally the weakest link in the chain to not fall prey to attackers. This requires a balance between security and convenience offered by technology where users should be comfortable letting go of some convenience for the sake of security and privacy. Simply put, we can build the most sophisticated authentication systems but if users still click on that phishing link, there is not much we can do. This is the reason I continuously invest in helping out the security community, friends and family, to not only educate them on best practices but also explain why it matters for them and how we as an industry are trying to build systems that are secure by default.

[H9]: There are many people within the realm of cybersecurity that are driven by a widely understood mission. Have you encountered any incidents or dilemmas that you found thought-provoking?

[KD]: There have been several thought provoking moments for me in the last decade as I have witnessed in the security industry. Reflecting on large incidents in the cybersecurity world like log4j (which is a Java library for logging error messages in applications), it got me thinking about how impactful security vulnerabilities can be when they are found in critical pieces of a language, libraries or an application. As a result, there are two aspects which I'm always thinking about:

1) How do we secure what we already have (log4j is an example)?
2) How do we ensure we build security within the products and services?

We are reactive when we are responding to incidents like log4j whereas at the same time we need to be proactive to prevent vulnerabilities like these from happening by fixing them before they get exploited. This sometimes can lead to differing points of views on where one should invest their resources and how much.

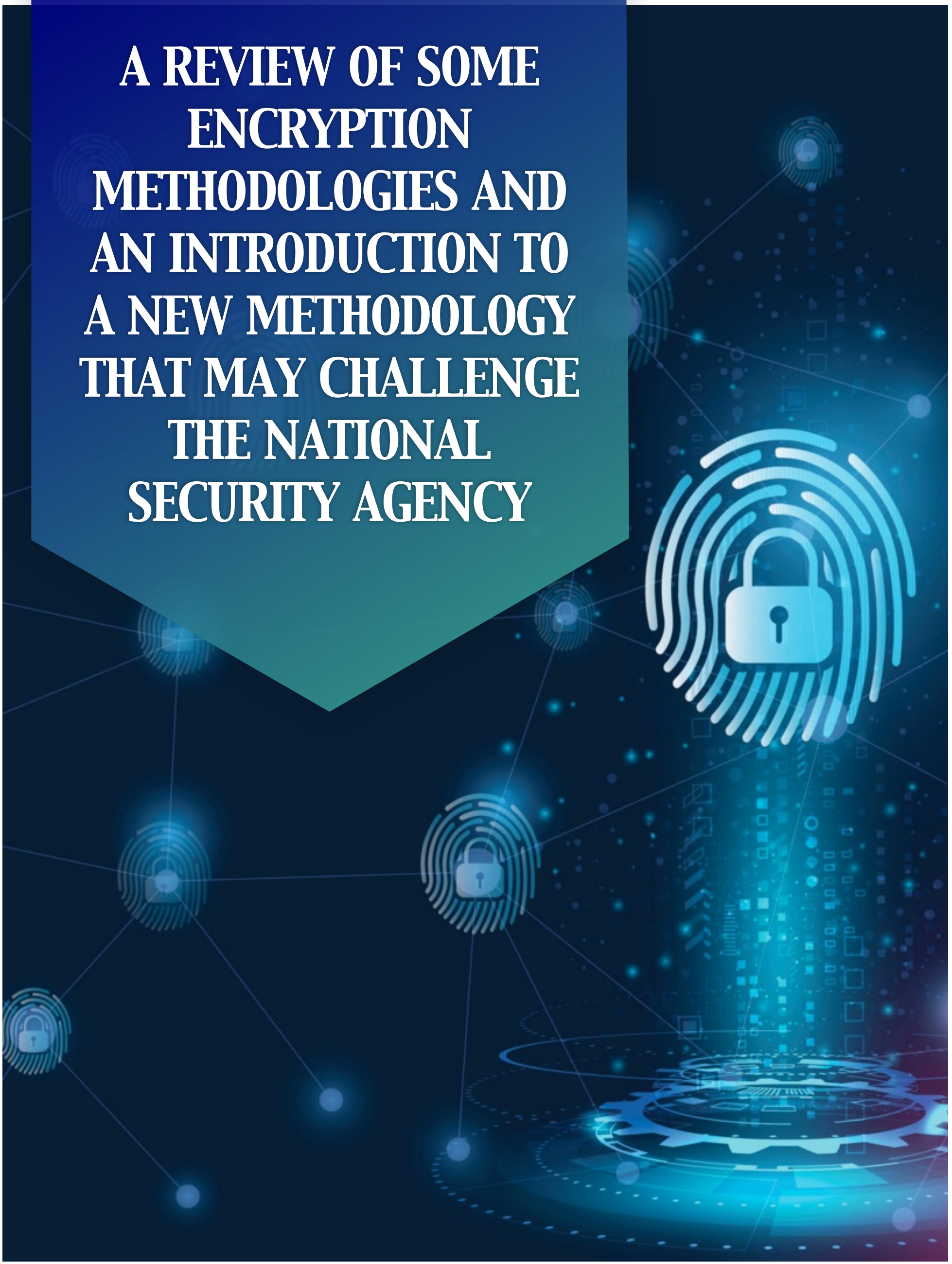
[H9]: If you were to give advice, what are some essential skills to get started in cybersecurity?

[KD]: I really love this question and this is one of the most frequently asked questions I get through my website and LinkedIn. The first thing to have within you is curiosity! The desire to know how things work and if you can make them behave differently. I would definitely say build a solid foundation of knowledge by learning about computer systems, networking and information security fundamentals. It takes work in the beginning to read and understand different (sometimes hard) concepts. Once you know these, it becomes easier to specialize, e.g. roles like incident response, application security engineering, infrastructure security engineering, etc. It also helps to be proficient in software development (or at least scripting) to automate security tasks. Practice using different tools and think about how to build them on your own!

[H9]: There's a plethora of cybersecurity tools, many new that are being created just now. Are there any preferred ones you want to recommend? Or do you use some less-known ones that are worth paying attention to?

[KD]: I've used various tools in my career at different places I've worked. Sometimes these are built internally or are provided by vendors. For personal projects, I do prefer using open source projects and tools. I really like The Sleuth Kit (and the frontend autopsy), which is a library of open source tools for investigating disk images. I also like GRR (GRR Rapid Response), which is used for remote forensic data collection. The best part about GRR is you can set it to poll a machine if it is offline and when it comes online, it can automatically collect the data you want from it.

A REVIEW OF SOME ENCRYPTION METHODOLOGIES AND AN INTRODUCTION TO A NEW METHODOLOGY THAT MAY CHALLENGE THE NATIONAL SECURITY AGENCY



Paul F. Renda

Paul F. Renda has spent over 30 years in information security. He has spoken at a number of above-ground and below-ground hacker conferences. He studied physics and math at Queens College and the University of Houston, and he has worked as a system administrator for IBM Z/OS and Linux systems. He was also recruited (recruited is a nice, friendly way to put it) by the FBI/NYPD Joint Terrorism Task Force to provide open-source high-impact information. The Russian Federation and the Department of Defense also wanted to become Paul's friend. He declined the friendship overture from the Russian Federation.

Introduction:

Encrypting information is not new; it's as old as the Roman Empire and even further back than that. Today the National Security Agency tries to decrypt information from our enemies and even in some cases our allies. There are numerous schemas for encryption. The oldest was just the substitution matrix. One letter was substituted for another. The most popular schema today for commercial encryption is private key public key encryption using the RSA Algorithm. Another popular methodology is using the elliptic curve cryptography.

Before we discuss a new methodology of cryptography to seriously challenge the NSA, let's talk about Elliptic Cryptography and RSA.

Elliptic Key and RSA:

Elliptic key encryption[1] utilizes the algebra of elliptic curves as an encryption methodology. Its keys can be shorter and is considered more efficient than RSA using less CPU time to decrypt.

RSA[2] is the most widely used methodology for commercial transactions (I almost exclusively use RSA as opposed to all other encryption methodologies). It was invented by the mathematicians Rivest, Shamir and Adleman and is the oldest public/private key methodology.

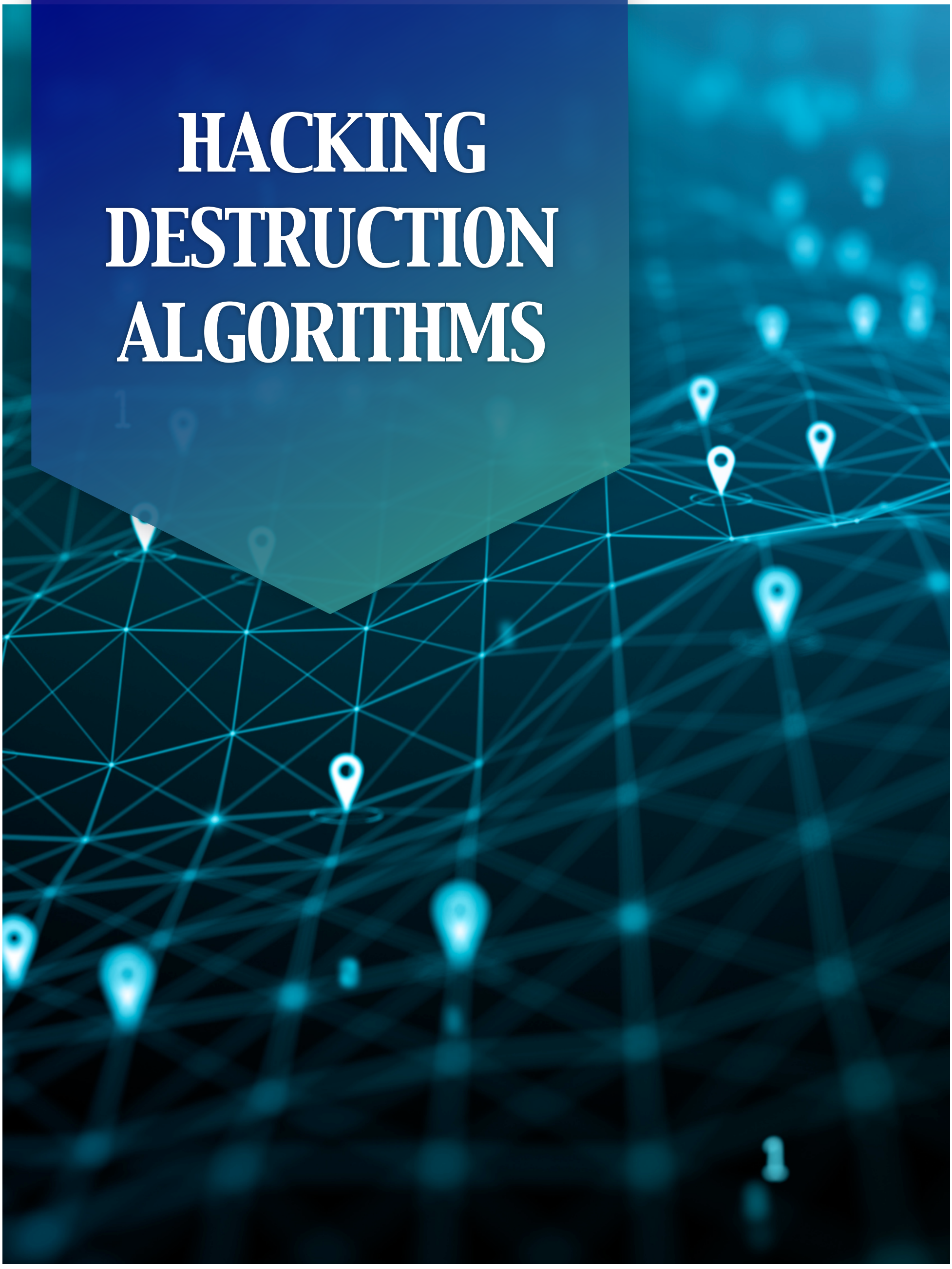
Both of these encryption methodologies involve a public key and a private key. What that means is that there's a private key that you use that you keep a secret. And a public key that you've distributed among users who need to decrypt the information. Let me give you an example of usage of public and private keys.

A company wants to put up a website and they want that website to be secure. The name of the website is www.paul.com. They would create something known as a certificate signing request (CSR)[3]. This would contain the country of origin for the website, the state or province, the city, the email address and the actual website name (www.paul.com). They would send that request to an agency known as a certificate of authority. It has a specialized authority to sign CSR to make them valid. It would also distribute the signing CA's to websites so they can validate the signed CSR.

When I create CSR for a client company, I typically use a 4096-bit key. Originally, some websites used only 128 bit key. The longer the key, the harder it is to decrypt the data and as computers become faster and faster, encryption keys have grown bigger.

You encrypt information because you wanted to keep it private and there's a long list of actors who want to steal your information. It is not only computer hackers, state governments, commercial enterprises and hacker groups. They're always brute force attacks with computers to decrypt information, and now with the possibility of quantum computing being much faster than conventional computing, it could pose a serious challenge to any type of

HACKING DESTRUCTION ALGORITHMS





Wilson Mendes

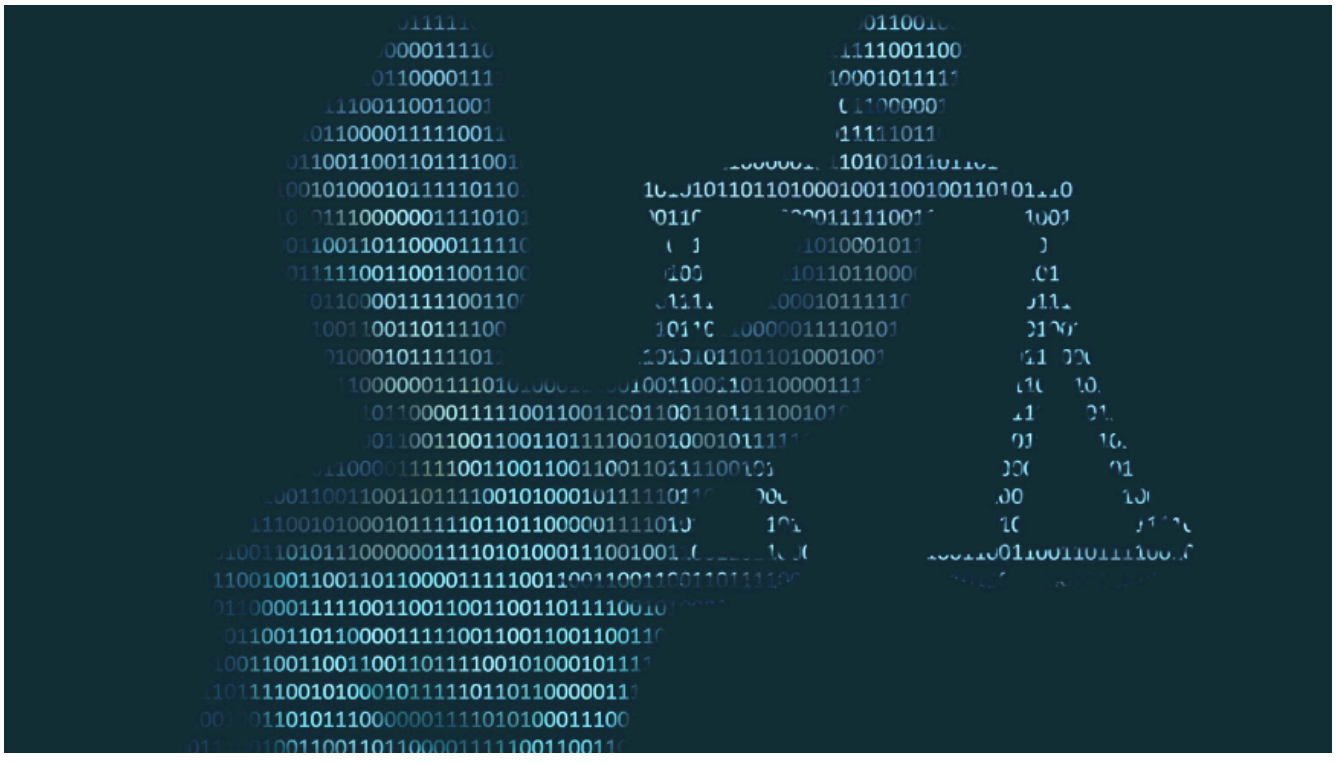
I am a cryptanalyst, researcher and advocate for digital privacy rights.

I work with information security, artificial intelligence and cybercrime. I am a creator of anti-tracking solutions and devices. I developed embedded systems with deep expertise in the areas of security protocol, privacy and anonymity.

www.wicasame.com

https://www.linkedin.com/in/wilsoncsmendes/

Hacking Destruction Algorithms



“Doublethink means the power to hold two contradictory beliefs in your mind simultaneously and accept both of them.”

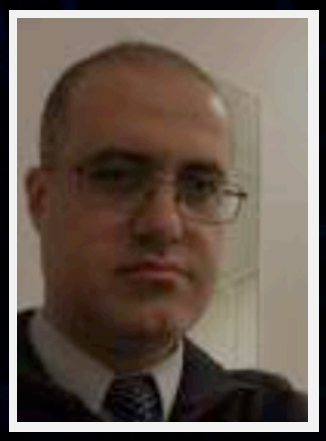
George Orwell

Prejudice has existed since the creation of the land. “Wives submit to their own husbands...” can be found in Ephesians 5 of the Bible and in the era of Big Data, through pentabytes of available information, often extracted from social media and apps, added to thousands of leaks of information, data can easily be found on the web. The algorithms are silently studying and predicting our desires, reliability, purchasing power and movements. Influencing automated decisions, often used to monitor, punish and disenfranchise, regardless of geographic region, shaping and controlling everyone's destiny, becoming a great nightmare for society.

An algorithm processes through combinations similar to those based on rolled dice, a series of statistics, thus creating probabilities. With this, we’re able to accelerate thousands of results. A person can be considered good or bad, depending entirely on the data entered in a questionnaire. This probability is distilled into a score, which might reveal a terrorist, a psychopath, a good or bad employee, or a risky loan, for example. It can change someone's life in a negative way.

Through LinkedIn, for example, when analyzing the hundreds of vacancies open for information technology, we see that the disqualification of the candidate who has an excellent curriculum, often happens due to several factors including political positioning, geographic region, salary expectation, skin color, belief and several other factors, explicit or implicit in the prejudice of the written code.

EXPLOITING SQL INJECTION USING ACUNETIX VULNERABILITY SCANNER AND SQLMAP



Adam Karim

Adam Karim is a computer engineer in Digital Forensics and IT Security. Certificates (Degree of Bachelor of Science 180 credits); 2018 Degree of Bachelor of Science in Digital Forensics and IT Security; main field of study Computer Engineering - Dalarna University in Sweden. Courses: 1) 2020 Ethical hacking I - KTH Stockholm; 2) 2019 Cyber Forensics, Stockholm University; 3) 2014 IT Security III: Computer Forensics Lab, KTH Royal Insitute of Technology - Stockholm; 4) 2012 Linux Server Administration, UMEA University in Sweden; 5) 2012 Python Programming, Stockholm; 6) 2010 HI103V Data Communications, KTH Stockholm; 7) 2008 HI119V IT Security II: Computer Forensics, KTH Sotckholm; author of articles for eForensics Magazine;

https://techworld.idg.se/2.2524/1.713397/ftk-imager-poliser-digitala-spar.

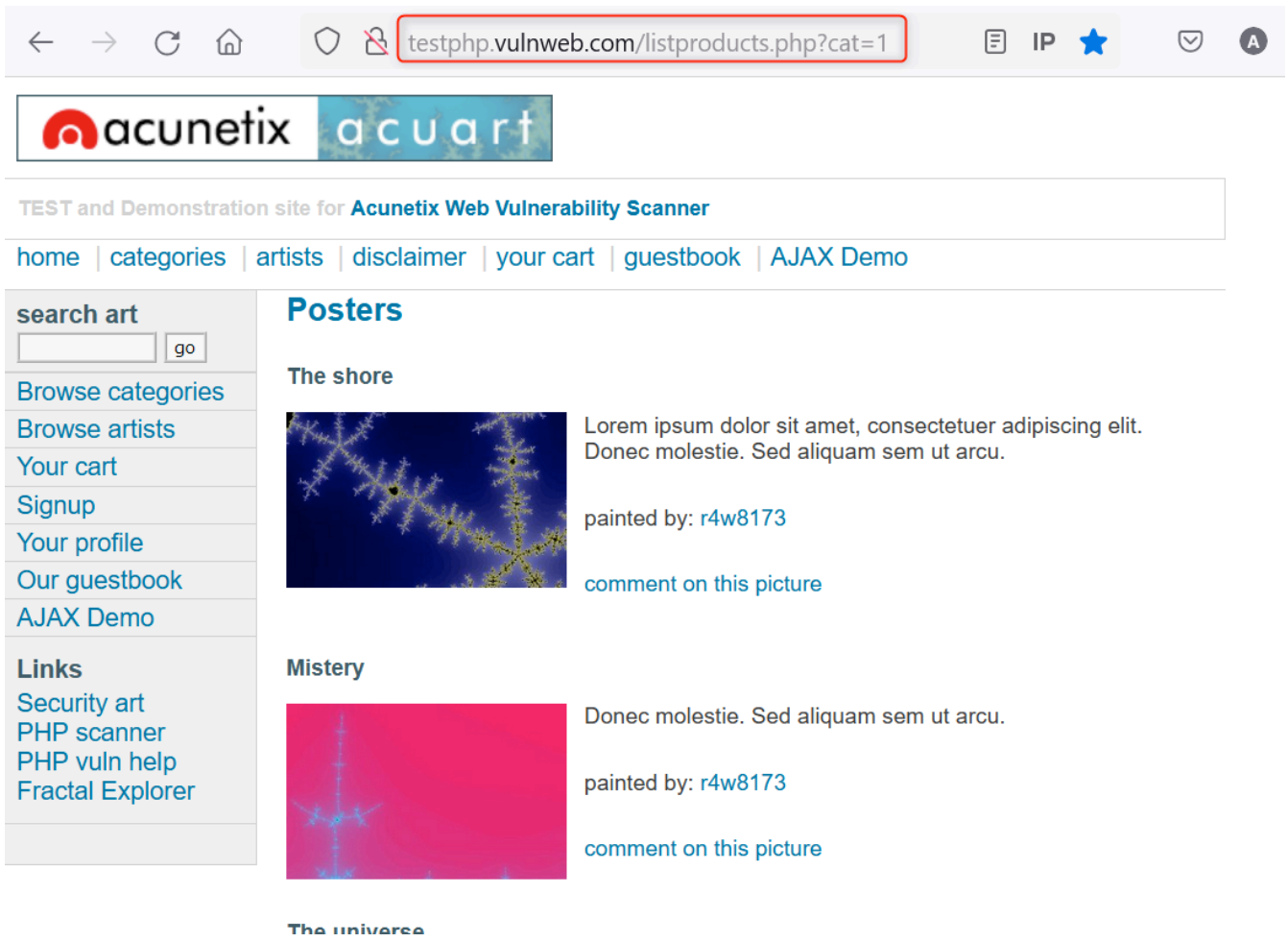
SQL injection (SQLi)



SQLi is the most well-known of all web application flaws and most web application security professionals have some familiarity with SQL injection flaws that allow a hacker's use of malicious code to bypass web application security and gain access to databases.

How Does a SQL Injection Attack Work?

SQL injection is the most dangerous security risk for web applications. Attacks usually result in data being deleted or destroyed and could lead to the entire webserver being compromised.



SMART CONTRACT SECURITY AUDITING





Youssef Khaoulaj

KHAOULAJ Youssef is the CEO and co-founder of Moroccan Blockchain Laboratory and a security researcher “bug bounty hunter” that specializes in discovering web application, cloud, blockchain, and smart contract vulnerabilities. He has over 6 years of expertise in the information security industry, with a solid grasp of Web Applications and decentralized application development.

https://www.linkedin.com/in/youssef-khaoulaj/

https://www.linkedin.com/company/moroccan-blockchain-laboratory/

Blockchain-based technologies are becoming popular. When compared to the security of typical IT systems, it is considered a novel and experimental technology. As a result, technology changes quickly, and new vulnerabilities emerge. The three key characteristics of Smart Contracts (transparency, immutability, and the ability to represent a value) can potentially jeopardize Smart Contract security, making them a target for hackers. More than 40 vulnerabilities in Smart Contracts have been uncovered so far, but as technology improves, many more will be discovered.

In this article, we will walk through the process of performing a smart contract audit, which entails a combination of multiple methodologies applied to the project together with specification and documentation. Many analyses are performed automatically using tools, while others require human intervention.

Audit is the practice of evaluating systems, apps, smart contracts, and dApps from the standpoint of an unprivileged or anonymous user "hacker" to determine legal and contractual ramifications, improve security, decrease attack surface and mitigate risk.

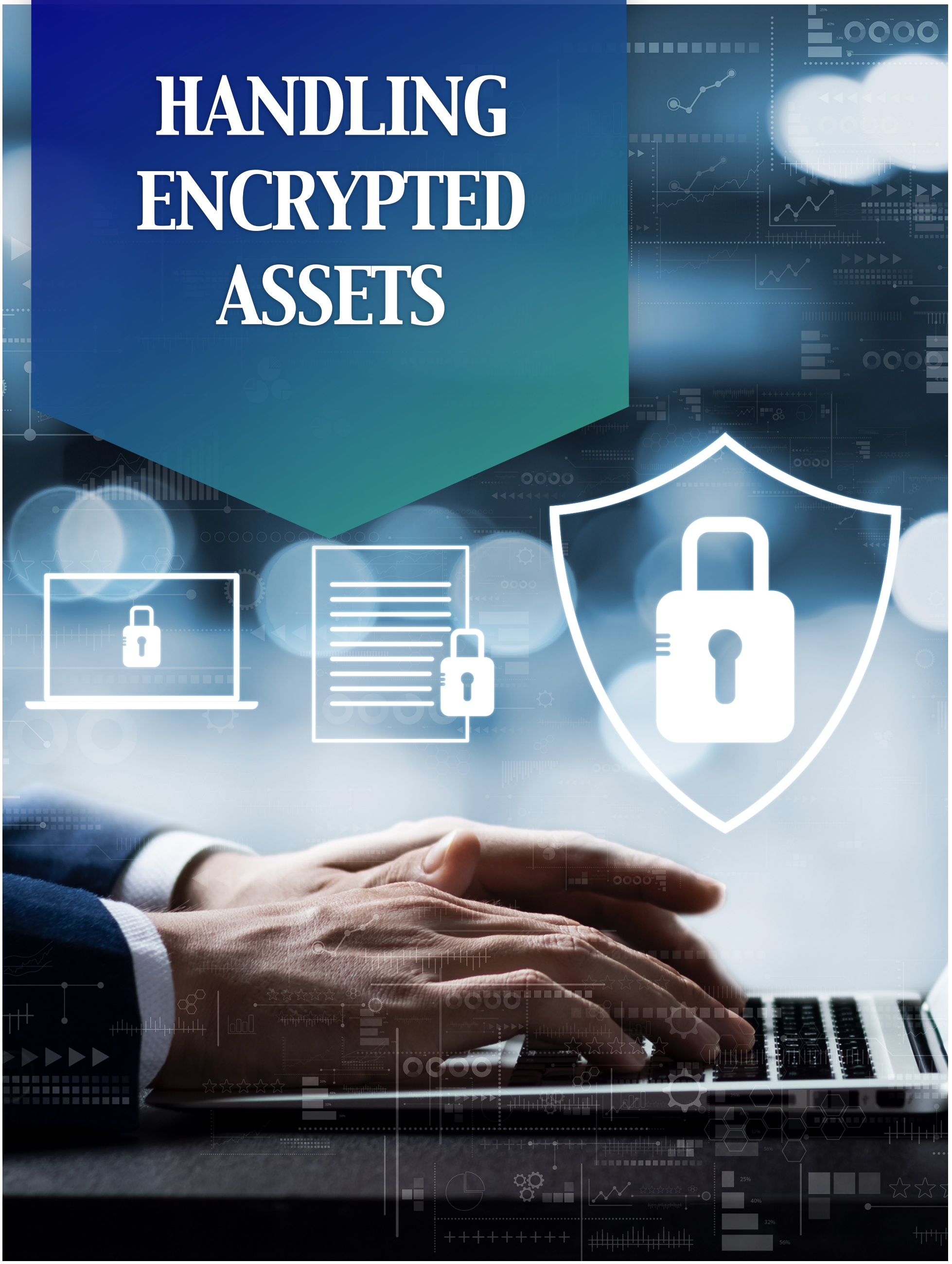
The audit scope can on-chain smart contract code and sometimes includes off-chain components that interact with the smart contracts.

According to the legislation, contracts have only been verbal or written agreements. Contracts may need the verification of a third party. Sometimes even each party to a contract acts according to what they have understood, giving rise to free interpretation. Nevertheless, "smart contracts" are self-executing contracts in which the contents of the agreement between parties are written directly in lines of code. Both agreements and code are put on a distributed and decentralized blockchain.

Smart contract enables a blockchain to move from a single purpose, such as a cryptocurrency, into a multipurpose platform used to deploy various decentralized applications and it provides full transparency in the exchange of assets between any number of parties thanks to the blockchain. Smart contract removes the need for a “middle-man” to facilitate transactions and record all exchanges and transactions of a contract onto a public ledger that can be witnessed and validated by everyone.

Smart contract platforms are designed to expand the functionality of blockchain. Instead of only implementing financial transactions, these platforms allow programs to be run on top of the distributed ledger. Transactions contain executable code that is run within each node’s copy of the blockchain’s virtual machine in order to update its state. The use of a blockchain ensures that all nodes in the network are running the exact same code in the same order, producing the same result.

HANDLING ENCRYPTED ASSETS





Washington Almeida

Washington Almeida is an Electronic Engineer and a Specialist in Law and Information Technology by the USP Polytechnic School, extension in Business Development by Fundação Dom Cabral. Founder of WE DATA SOLUTION, a company specialized in highly complex digital forensics, he is an invited Teacher at Mackenzie Presbyterian University in the Intelligence and Cyber Security, and Data Protection courses, teaching Computer Forensics and Information Security Policies respectively. Member of the Embry-Riddle Aeronautical University (ERAU) Institutional Repository (Florida-EUA), the United States High Technology Crime Investigation Association and the Italian International Forensic Association of Information Systems. Author of articles for the magazines of the "Associação Brasileira da Propriedade Intelectual" (ABPI), and the international Hakin9, Pentest Magazine and eForensics, specializing in information security, hacking and digital forensics where he also contributes as instructor. Microsoft Excellence Title as MCSE, Oxygen Forensic Detective certified (USA) and Passware Certified Examiner (EUA). More than 30 years of experience, familiar with digital forensic procedures that comprises digital forensics investigations phases as collection, examination, analysis, and reporting. Cyber security professional who also works with sophisticated systems invasion testing, helping companies to improve the security of their assets in attendance of the LGPD Brazilian legislation. In the assistance of the Justice, he is licensed by the "Tribunal de Justiça de São Paulo" and "Tribunal Regional do Trabalho da 2ª Região" acting as Witness Expert appointed by the judge.

Wash Web page: www.washingtonalmeida.com.br

Wash´s Company: https://wedatasolution.com.br

Wash e-mail: wualmeida@outlook.com

1. Introduction

Most articles involving password cracking or encryption are usually associated with hacker-related activities, which is not wrong. However, this class of activity today is not solely reserved for hackers.

Police forces, Courts of Justice, intelligence agencies and other bodies linked to Public Security face daily challenges in dealing with the decryption of digital assets. From password-protected files to completely encrypted disk volumes, or accessing a machine that no longer knows the password, are just a few examples of these challenges. Linux distros, like Kali and Parrot, among others, are equipped with some powerful password attack tools, among them, the well-known John, RainbowCrack, PDFcrack for offline attacks, Ophcrack for local attack and others, like Hydra and Medusa, for online attacks.

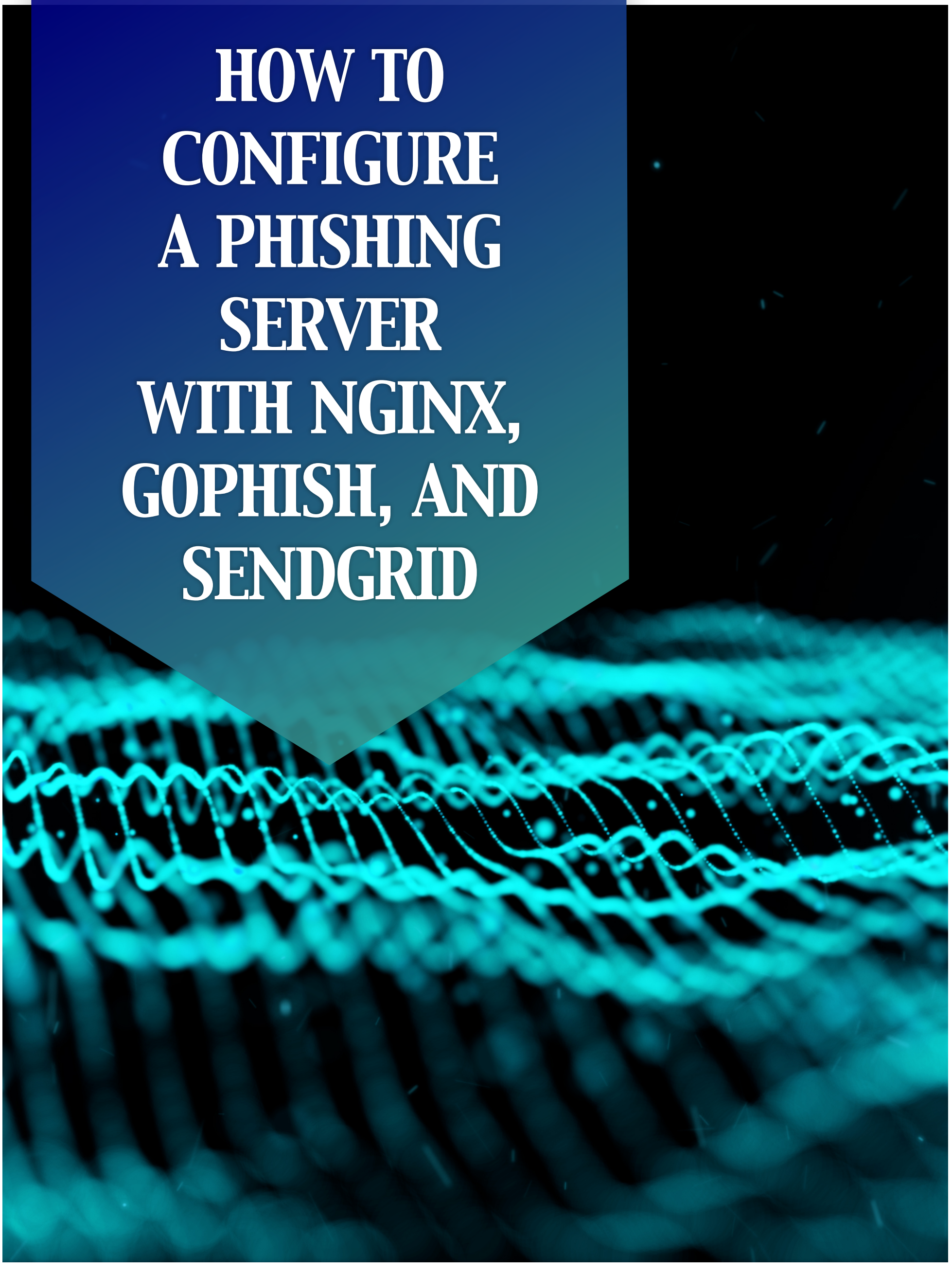
Imagine if the entire context of digital asset discovery and decryption could be put into a single suite that dealt with the sophisticated challenging scenarios. Such a tool exists. Ladies and gentlemen, I present to you "Passware Kit Forensics", the State of the Art in digital asset decryption.

2. The "Passware Kit Forensics"

Passware Kit Forensic is the complete electronic evidence discovery solution that reports all the password-protected items on a computer and decrypts them. The software recognizes 280+ file types and works in batch mode recovering their passwords. Some of the main features we find in Passware Kit Forensic (PKF for short) are:

- **All-in-one User Interface**: A single user interface for encryption discovery, password recovery and decryption for 280+ file types, mobile forensics, memory analysis, and other features.
- **Live Memory Analysis**: Extracts encryption keys for FileVault2, TrueCrypt, VeraCrypt, BitLocker, logins for Windows & Mac accounts from memory images, and hibernation files.
- **Cloud Data Acquisition**: Passware Kit acquires backups and data from cloud services: Apple iCloud and iCloud Drive, MS OneDrive, and Dropbox.
- **Mobile Forensics**: Recovers Passwords for Apple iPhone/iPad and Android backups, as well as Android images. Extracts data from Windows Phones' images. Integrated with Oxygen Forensic Suite.
- **Hardware Acceleration**: Accelerated password recovery with multiple computers, NVIDIA and AMD GPUs, Tableau Password Recovery and TACC, and Rainbow Tables.
- **Intelligent Detection**: Detects all the encrypted files and hard disk images, reports encryption type and decryption complexity.

HOW TO CONFIGURE A PHISHING SERVER WITH NGINX, GOPHISH, AND SENDGRID



Why am I writing this?

Phishing is the cause of most cyber breaches. Most successful attacks against companies start with a phishing email. And you MUST perform regular phishing training for your business.

Use with caution. You are responsible for your actions.

What you will learn here

Install and configure NGINX as a reverse proxy for multiple virtual hosts.

Install and configure GoPhish with SendGrid to send Phishing campaigns.

Requirements:

- Full access (root) to an Ubuntu server 22.04 LTS with SSH access and ports 80 and 443 open in the firewall
- Basic knowledge of git
- Basic knowledge of Vim editor

Let`s start with NGINX

NGINX, pronounced “engine-ex”, is an open-source web server that, since its initial success as a web server, is now also used as a reverse proxy, HTTP cache, and load balancer.

To install NGINX is a pretty simple task; you can do this just using the APT package manager. Go ahead and connect to your future phishing server through SSH and type the following command:

```
sudo apt update && apt install nginx -y
```

Now it's time to configure NGINX as a reverse proxy for GoPhish.

One of the best things about NGINX is the simplicity of its configuration. I love that! All NGINX configuration files are under the /etc/nginx directory. So go ahead and change to /etc/nginx directory.

To do so, type the following command in the terminal:

```
cd /etc/nginx
```

Inside this directory, you will find the files you need on your web server. Now, go ahead and create the file for your