PREVIEW

HAKIN9

PHYSICAL PROTECTION

IT SECURITY MAGAZINE

VOL.18, NO.01

GETTING OFFENSIVE WITH GO

Writing A Simple Ransomware Using Python

Application Security Testing

Tactical Wireshark: Basic Malware Analysis

Dynamic SQLIA Detection with PHP

Interview with Jason Ross and with ChatGPT! Guess which answers are AI-generated!

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

Bev Robb

Mitch Impey

Michal Jachim

Jordan M. Bonagura

Hammad Arshed

Daniela Co

David Michaud

Benjamin Aboagye

Dalibor Filipovic

Dan Dieterle

Alex Giles

Amit Chugh

Vinoth Sivasubramanian

Alex D

Paul Mellen

Jason Ross

Bhuna Selvadurai

Tom Updegrove

Craig

Frédéric Crequer

Humberto A. Sanchez II

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,

Spring is slowly approaching (at least where we're at - maybe you're blessed with the Sun already)! The improving weather always sows a seed of the will for self-development, and we hope you feel it too. Let's take advantage of it and learn new tools and concepts in the realm of cybersecurity!

Right at the beginning, you'll be able to get acquainted with a top-notch article 'Getting offensive with Go'. There, you will read about creating Reverse Shells and bypassing Anti-Virus (AV) with Golang. This will give you a brief overview of some existing Go shellcode for Pentesters and Red Teams.

In the next article, you will get to know how ransomware works, what are the parts that make it, and how you can write a simple one using the Python language (and a couple of libraries and modules). Also, you will see in action how it works and will learn how dangerous it can be for an unsuspecting victim.

To widen your knowledge, you will find out about a dynamic approach to detect an SQL Injection Attack (SQLIA) based on a static pattern matching algorithm. You will picture a PHP web server scenario including a miniature SQLIA detection system.

You will also learn about the process of developing tactics with the purpose of preparing for cyberwar. The author will try to answer such questions as: Who are the cyber military powers today? What are their doctrines? What are the military objectives in warfare?, and many more!

In another article titled 'New frontiers, new worlds, new threats', you will read an unusual piece about an idea of AI and its effect on our lives going forward. Enjoyable especially for people with interest in history ;)

Later on, we have an excellent collaborative work about the fundamental topic - application security testing. The authors share their insights about what application security testing actually is, about the importance of it, and about some key tools. Brief but essential!

In the essay 'Cyber Counter-Terrorism: Shutdown', the author makes important arguments for a counter-terrorist mindset in combating a few popular cybersecurity attacks. There, you will find some handy ideas to counter social engineering and other well-known attacks.

Next, we have a case study report which may spark your interest - 'File system fault in FAT32-formatted drives revealed by Morse-code directory names in Windows OS environment. Vulnerability in USB flash/hard drive (PenDrive, Portable External/Internal Hard Drive) case study'.

In the closing article, you will learn about the feature of Wireshark that allows you to export objects and, following that, you will explore how you can use Wireshark and extract domains as well as connections. This is a fantastic article you need to read!

Last but not least, we have an interview with Jason Ross, where we ask him about Machine Learning, Deep Learning, and AI. To spice things up, the author gave us 2 sets of answers. One delivered by him, and one by ChatGPT! It is your job to guess which ones are his original answers! If you have a clear idea why one set of answers is given by AI, try to formulate the reason. We're super curious about your opinions! Hit us at hello@hakin9.org ;)

We really hope that you will have fun reading this edition's content!

Stay safe,

Agata Staszelis and the Hakin9 Editorial Team

TABLE OF **CONTENTS**

4 ***GETTING OFFENSIVE WITH GO;*** *DANIEL W. DIETERLE*

20 ***WRITING A SIMPLE RANSOMWARE USING PYTHON;***
MOHAMMAD SAEED

30 **DYNAMIC SQLIA DETECTION WITH PHP**; *TAQIE TAQIEZADEH*

42 ***THE PROCESS OF DEVELOPING TACTICS WITH THE PURPOSE OF PREPARING FOR CYBERWAR;*** *LOCHANA KORALAGE*

49 ***NEW FRONTIERS, NEW WORLDS, NEW THREATS;***
WILSON MENDES

65 ***APPLICATION SECURITY TESTING;*** *COLLABORATIVE WORK*

73 ***CYBER COUNTER-TERRORISM: SHUTDOWN;*** *LUCAS MACLAUD*

82 ***FILE SYSTEM FAULT IN FAT32-FORMATTED DRIVES REVEALED BY MORSE-CODE DIRECTORY NAMES IN WINDOWS OS ENVIRONMENT. (...) CASE STUDY;***
ŁUKASZ GRZĄDKO

96 ***TACTICAL WIRESHARK: BASIC MALWARE ANALYSIS;***
KEVIN CARDWELL

114 ***INTERVIEW WITH JASON ROSS***

GETTING OFFENSIVE WITH GO





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.

Introduction

Creating Reverse Shells and bypassing Anti-Virus (AV) with Golang. Using Golang in security has become very popular over the last few years. In this article, I want to cover several existing Golang scripts that you can use to create Reverse Shells and possibly even bypass Anti-Virus. We will start our journey looking at a one-line reverse shell in Go, and then cover a couple apps that can generate multiple different shells. This article isn't about writing custom Go scripts or post exploit - what to do after you get a remote shell. It is simply a quick and dirty overview of some existing Go shellcode for Pentesters and Red Teams.



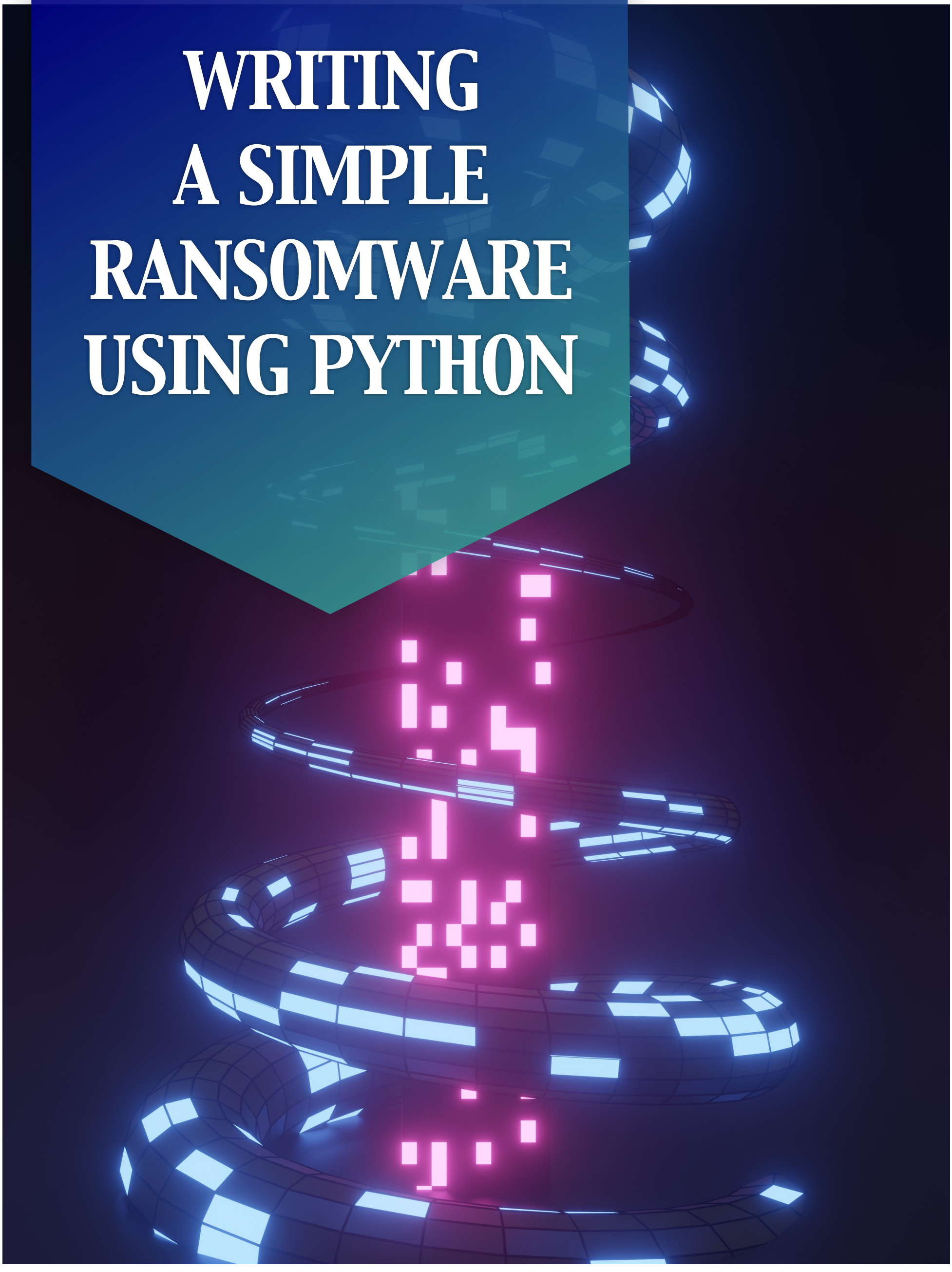
Swissky's one-line Go shell is up first. This one-line reverse shell works great against Linux based targets. Next, we will look at Girsh, a menu driven script that can create multiple different reverse shells for both Linux and Windows. Lastly, we will look at Go-Shellcode, a very good Go reverse shell that, at last testing and with the right payload, still bypasses most common Windows antivirus products.

As always, this article is for educational & informational purposes only.

Never try to access systems without permission.

I used two Kali Linux VMs for this article, one a target and the other an attack system. Golang was already installed on the attacking system. I also used a Windows 11 system and a Windows Server 2022 (not shown) for testing the Go-Shellcode Early Bird code.

WRITING A SIMPLE RANSOMWARE USING PYTHON



Mohammad Saeed

Mohammad graduated in the year 2021 with a bac +5, specializing in network design and architecture. I'm currently studying cybersecurity at Epita and planning to continue my studies to obtain a PhD in cybersecurity.

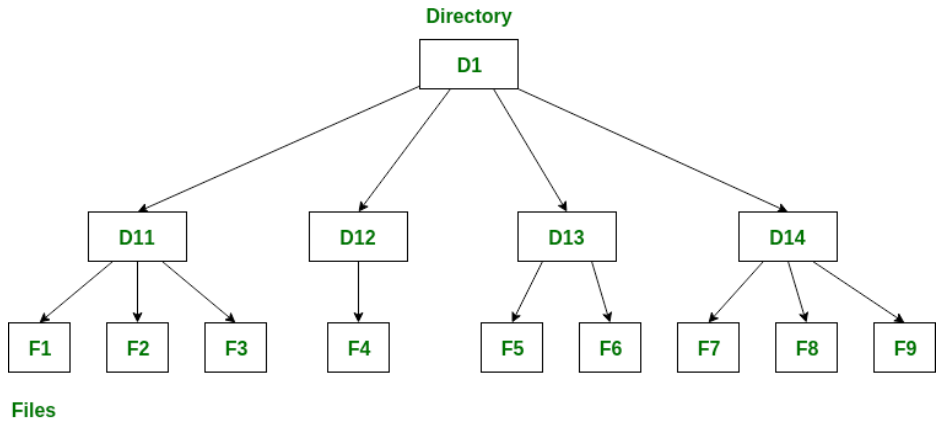
Introduction:

Ransomware is a program designed to prevent a user or organization from accessing files on their computers. It encrypts the files and demands a ransom for the decryption key; this places organizations and individuals in a position where paying the ransom is the easiest, cheapest, and quickest way to regain access to their files. Some types of ransomware have added functionalities – such as data theft too.

Recent ransomware attacks have impacted hospitals' ability to provide crucial services and crippled public services in cities. Ransomware doesn't need to be complex to cause damage, which makes it even more dangerous. Bad actors don't require a strong knowledge of programming, either. In this article, I will explore how to write a simple ransomware using Python.

How it works:

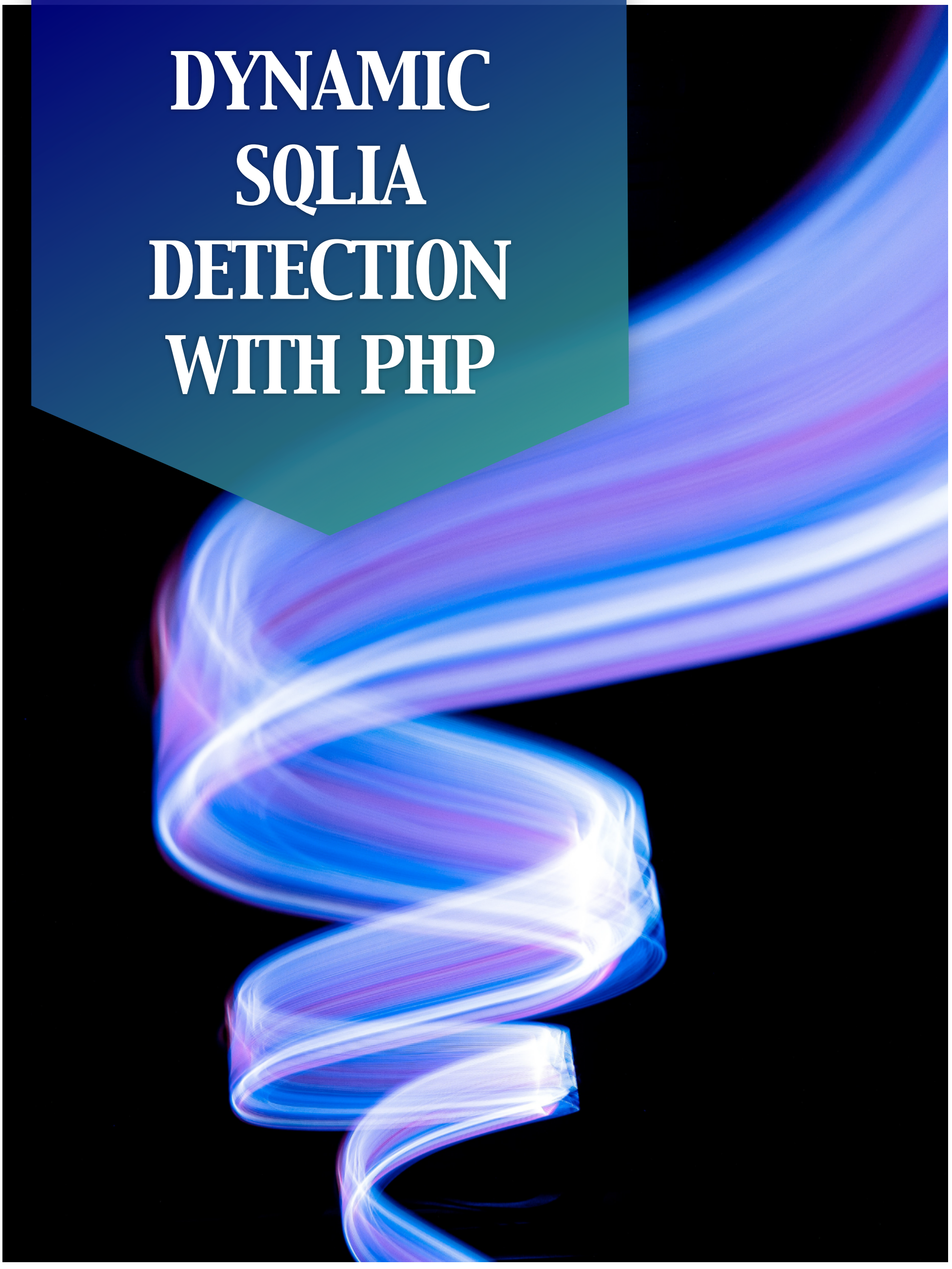
The ransomware code can be split into three parts, the directory crawler, encryption, and decryption. The first function crawls through all accessible directories within the directory that holds the malware. The crawler looks for files and other directories and will keep going until it reaches the deepest point in the directory tree and then saves the files' names and paths to be used during the encryption phase.



P1 directory tree

For example, let's assume that the ransomware exists in D1. The crawler function will start going through the directories — it will go to D11, then will add all the files in D11 (F1, F2, F3) to a list and will continue to do the same for D12 through D14. Once the ransomware acquires all its targets, it is ready to start encrypting the victims' files. When the encryption begins, it will use the list made by the crawler and start encrypting all the files it can reach. When it finishes encrypting, it will show the user a message telling them that their data was compromised and give them a set of instructions that they must follow if they want to restore their data; for example, sending some cryptocurrency to get the decryption key. Once the user enters the key, all of their data may be restored, allowing them to access the data again.

DYNAMIC SQLIA DETECTION WITH PHP



Taqie Taqiezadeh

Holds MSc. On Electrical Engineering (Electronic-Microelectronics), Urmia University, Iran www.urmia.ac.ir, BSc. On Electrical Engineering (Electronics), Guilan University, Iran www.guilan.ac.ir.

About three years of work experience in the service provider as a NOC (Network Operation Center) engineer. (Metro Ethernet Network , Sonet Network and DSL Broadband Network)

About 6 years of experience as network security engineer (UTM Configuration and maintenance, router and switches security configuration and also Web Application Firewalls configuration, tuning and threat analysis).

Introduction

We're going to discuss a dynamic approach to detect an SQL Injection Attack (SQLIA) based on a static pattern matching algorithm. As we know, SQL injection attacks are malicious techniques that target your database using manipulated statements. What the proposed algorithm does is compare SQL statements with prepared static patterns and makes a decision according to the comparison result. In this paper, three basic SQL injection patterns are considered to be detected by the pattern matching algorithm. This algorithm has been implemented with PHP codes.

Pattern (String) Matching Algorithms

Simply, pattern matching algorithms, in the computer field of study, search shorter strings inside a longer one. There are numerous string-matching algorithms that are looking for the count and place of a given special pattern inside a longer string. For example, we can enumerate *Naive Pattern Searching Algorithm (NPSA)*, *Rabin-Karp Algorithm (RKA) and Aho-Corasick String Matching Algorithm (ACSMA);* each one has its own logic to fulfill the matching process. The first one, NPSA, has a straightforward algorithm. It simply checks for exact occurrences of a string inside an input text. The second one, RKA, acts similarly to NPSA, but the difference is it hashes the strings before performing the matching process. But, the ACSMA is a more sophisticated algorithm that constructs a searching tree. The tree branches represent a sequence of characters that make a string inside a dictionary.

The algorithm we're going to talk about is based on *a logical comparison*. Unlike the aforementioned algorithms it is very simple and is made up of a few lines of PHP codes. The malicious input patterns are listed and their equality is compared with the input username and password. In this approach, a separate database table is dedicated to store malicious credentials where the administrator can update it as zero-day injection patterns come out. Because it does not consider probable states, we don't encounter issues relative to false positive/negative attack detections.

Static Pattern Matching Flowchart

In this section, the flowchart of the SQLIA detection algorithm is represented. The web server, in general, is composed of a MySQL database including two tables. One of the tables maintains authorized credentials and the other is going to keep malicious SQLIA username and password patterns. Since the latter table is filled by the administrator, a submit form is designed to accept malicious patterns. On the other hand, a string matching code is written by PHP that compares the received username and password with the corresponding malicious username and password patterns listed in the second table, one by one, via a conditional loop. If the matching output is "Yes", then PHP echoes an alarm to the administrator indicating some SQLIA happened. But if the comparison result is "No", then the normal login procedure continues and it directs the user to the web server's homepage.

THE PROCESS OF DEVELOPING TACTICS WITH THE PURPOSE OF PREPARING FOR CYBERWAR

Lochana Koralage

Lochana Koralage is an experienced Systems Engineer currently working in the cybersecurity domain. The author holds an Honors Degree in Computing, and a master's degree, specializing in Cyber Security.

Who are the cyber military powers today?

Cyber military defenses are being developed by most of the developed countries in the world. However, for a country to be a military power, they must develop both offensive and defensive powers. The fine balance between the two makes those countries powerful as well as peaceful at the same time. However, this is not the case in most of the world powers. USA, UK, Russia, China, Iran, Israel, etc., can be identified as the most powerful cyber military powers in the world.

What are their doctrines? Offensive, defensive, balance?

In most of the countries, the doctrine of cyber military power exploitation is a balance between offensive and defensive. But countries like China, said to possess the largest cyber military force in the world, can be considered to have a more offensive doctrine. In contrast, countries like the UK can be considered to have a more defensive approach of protection from cyber military acts against the country or their assets. A more balanced approach can be seen in countries like the USA, where both offensive and defensive strength is high, while there is a large portion of the defense budget being allocated for cyber related power. Russia, on the other hand, can be considered as a highly offensive country in cyber military warfare. Espionage and cyber attacks are some of the most common attack techniques used in cold wars, out of which most are led by Russian groups of hackers.

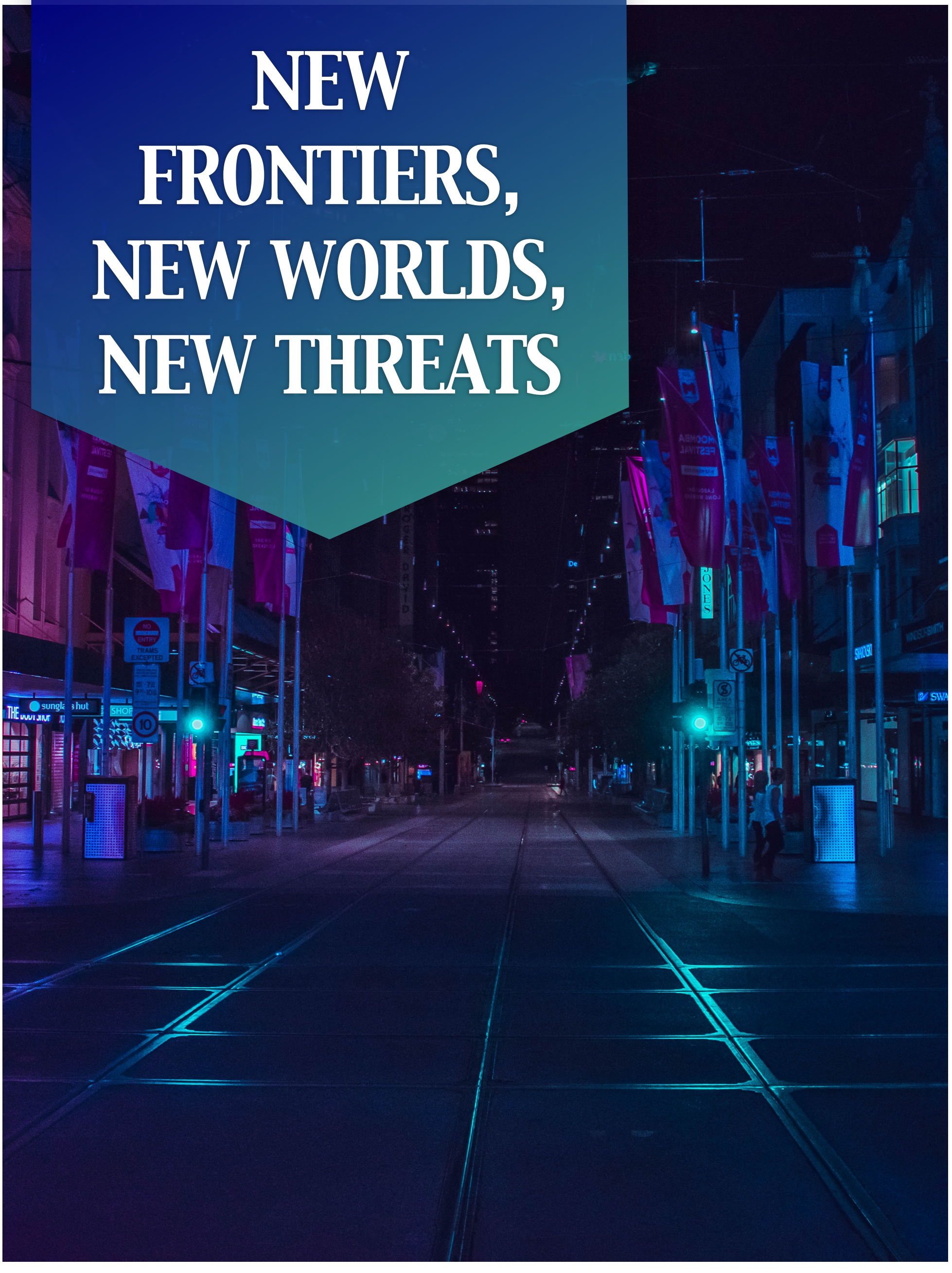
What are the military objectives in warfare? Intelligence, fake news campaigns, sabotage.

The author can illustrate with examples.

In any form of war, key military objectives would be to get an advantage over the enemy. Even though this was a tedious task in the early days, now it is much easier with the proper cyber tools and techniques combined with the right skills. For this purpose, most countries train their military persons in cyber related activities, as well as recruit highly skilled hackers and developers to increase the strength of cyber military power of the country. Once a country possesses such assets, they can be used for espionage. Espionage is not just physical anymore; with only a digital presence in the right place at the right place, you can extract some of the most sensitive information of a country or an organization or even an individual.

Further, the correct use of tools in gaining unauthorized access can be exploited in many advantageous ways. It is then possible to extract important information. Also, with the correct access, critical systems of the enemy can be brought down in the window of a few minutes in a DOS or DDOS attack, especially with the use of the right bots and also probably with the AI based tools in their advanced form now.

NEW FRONTIERS, NEW WORLDS, NEW THREATS





Wilson Mendes

I am a cryptanalyst and work with Cyber Security Engineer | DevSecOps | Application Security | Python | FreeBSD | Red Team | Blue Team | Purple Team | Ethical Hacker, artificial intelligence and cybercrime.

http://www.wicasame.com/

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



Image created in midjourney

Where are you going?

There.

What time will you be back?

I will be back soon.

MR.CARDOSO

Introduction

Since the beginning of human history, the world has been marked by significant transformations and drastic changes.

The intersection of technology and exploration has always been a driving force behind humanity's search for new frontiers and new worlds. From the earliest tools used by our ancestors to the cutting-edge technologies of today, our ability to develop and utilize advanced technologies has enabled us to push the boundaries of what we know and discover new horizons.

Now, as we stand on the cusp of a new era, technology has become more critical than ever before. New breakthroughs in fields such as robotics, artificial intelligence, and science are allowing us to develop the necessary tools and systems to explore. Private companies and government agencies alike are investing heavily in developing the necessary technologies to make them safer, more efficient, and more affordable.

At the same time, new technologies are also opening up possibilities for exploration and discovery on other planets. The development of unmanned probes and rovers has allowed us to gather unprecedented amounts of data about the geology, atmosphere, and composition of these new worlds. This information has provided us with invaluable insights into the history and potential habitability of these other worlds, and has fueled the drive to send human explorers to these new frontiers.

However, as with any technological advancements, there are also new threats that must be considered.

In this article, we will examine the latest technological advancements driving the search for new frontiers and new worlds.

We will explore the breakthroughs in technology and discuss the potential benefits and risks of these advancements.

Join us as we delve into the exciting world of technology and explore the new frontiers that lie ahead.

Before Christ and After Christ

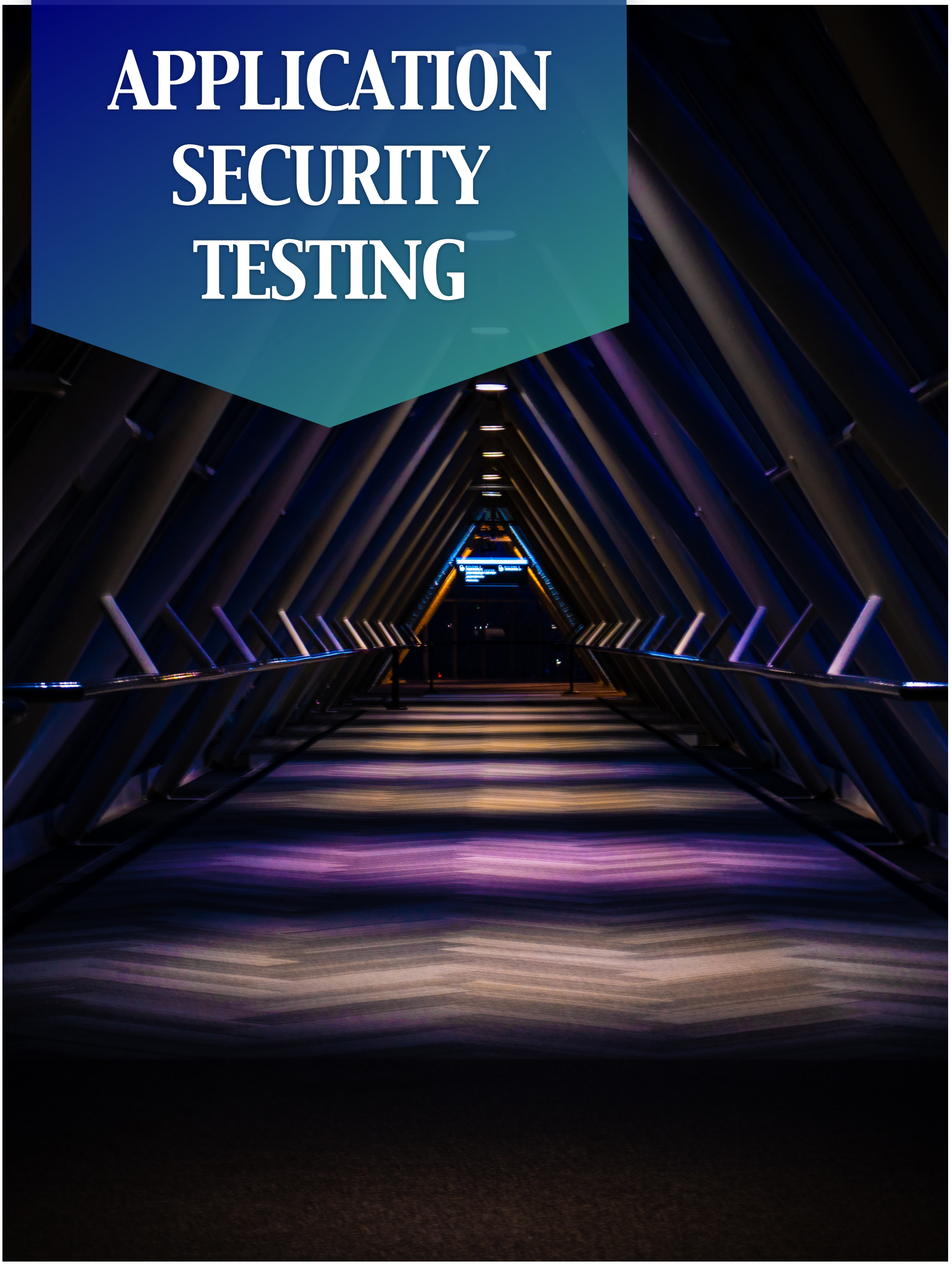
Before Christ (BC), the world was marked by different civilizations and cultures that emerged and developed in different parts of the world. Some of the most notable include the Sumerian civilization in Mesopotamia, the Egyptian civilization in Egypt, the Harappan civilization in India, the Chinese civilization, and the Mayan civilization in Central America. This period also saw important developments in mathematics, philosophy, religion, art and architecture.

After Christ (AD), the world was profoundly influenced by the rise and expansion of the Roman Empire, which brought peace and stability to a large part of Europe, Africa and Asia. In the 4th century, the Roman Empire became Christian, which had a lasting impact on the culture and religion of Europe and other parts of the world. From the 5th century onwards, the Roman Empire began to face internal and external problems, including barbarian invasions, and ended up splitting into two in the 6th century: the Western Roman Empire and the Byzantine Empire.

In the Middle Ages, Christianity continued to expand, and new Christian nations and kingdoms emerged in Europe. This period also saw important developments in art, architecture, science and philosophy, including the emergence of the University and the Dark Ages.

The Renaissance occurred in the 15th century, and was marked by a revival of ancient knowledge, as well as the emergence of new artistic and scientific movements. This period was followed by the Enlightenment, in the 17th and 18th centuries, which valued reason and science above tradition and authority.

APPLICATION SECURITY TESTING





Ahamed Nuski has a total of 10 months of experience in both software engineering and cyber security domains. He previously worked as an Associate Software Engineer and is currently a Cyber security Trainee at AION Company. Additionally, he is armed with NDT in Information Technology and Qualys, Cybrary, Fortinet, and Cisco certified in security certification.

Contact: Nuskiahamed16@gmail.com



Wathmi Sureshika is an undergraduate studentl SC-900, Qualys, Cybrary, IT Master, Fortinet and Cisco certified in security certification.

Contact: wathmisureshi2001@gmail.com



Sandali lavanya liyanaarachchi is an undergraduate student. She is currently a Cyber security Trainee at Aion Company. She is armed with NSE 1, NSE 2, NSE 3, CISCO and Qualys Certified Security Specialist certifications.

Contact: sandali0514lavanya@gmail.com



Nipuni Sathsarani is an undergraduate student|BSc Hons in computer science | Qualys, Cybrary, IT Master, Fortinet and Cisco certified in security certification.

Contact: nipunisathsarani1234@gmail.com



Umesh Irushika is a Cyber security trainee for the past few months with hands on experience in networking and cybersecurity domain. He is armed with diploma in Cyber Security and Networking, Microsoft-SC 900, AZ 900, Qualys, Cybrary, Fortinet and Cisco Certified in security certification.

Contact: umeshirushika64@gmail.com



Chirath De Alwis is an information security professional with more than 9 years' experience in the Information Security domain. He is armed with MSc in IT (specialized in Cybersecurity) (distinction), PgDip in IT (specialized in Cybersecurity), BEng (Hons) Computer networks & Security (first class), AWS-SAA, SC-200, AZ-104, AZ-900, SC-300, SC-900, RCCE, CIEH, CIHFI and Qualys Certified Security Specialist certifications. Currently involved in vulnerability management, incident handling, cyber threat intelligence and digital forensics activities in Sri Lankan cyberspace.

Contact: chirathdealwis@gmail.com

Introduction

The digital era has made the world seem compact. Things that used to take an entire day are now completed in a matter of seconds. However, the internet also created opportunities for digital data information exploitation.

One example is cybercrime, since we know some of the applications, like Mozilla Firefox, Adobe Flash Player and Adobe Acrobat, we install on our PCs or smartphones are not secure. They are particularly vulnerable to data breaches and cybercrimes. We occasionally learn of cyber-attacks on different programs such as Microsoft Exchange Server attack and Colonial ransomware attack that happened in 2021.

The application security testing fixes any dangerous behavior it finds and alerts the user whenever it does. The method of protecting application from cyber-attacks is known as application security. [1]

What is Application Security Testing?

Application security testing is the act of assessing an application's security posture to find gaps or flaws that an attacker could take advantage of. It entails a set of tests and evaluations intended to find security holes in an application, such as desktop software, mobile applications, or web applications. [2]

Testing for application security can be done manually, automatically, or by combining both methods. A human tester aggressively explores the application during manual testing to find any potential flaws or vulnerabilities.

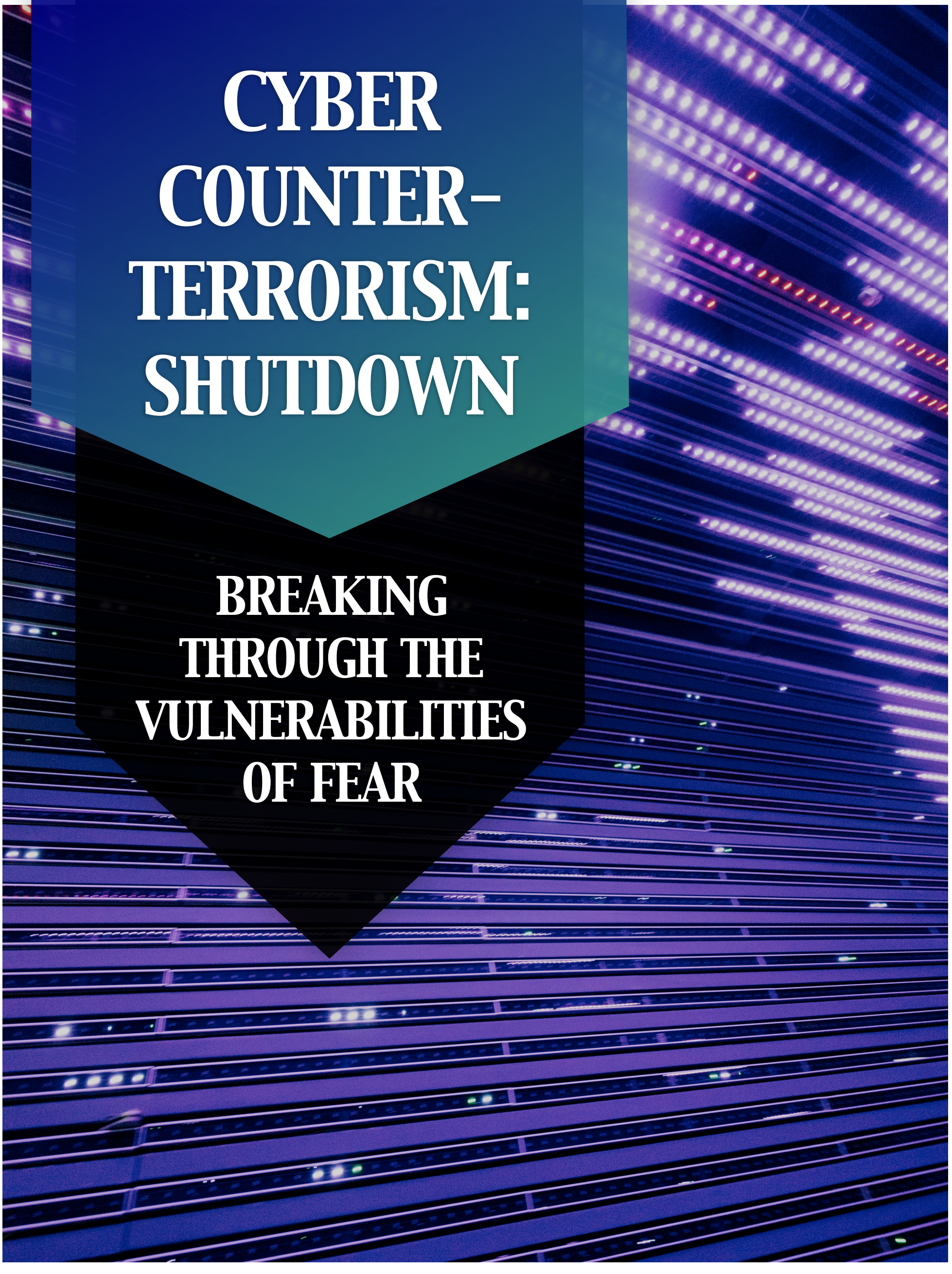
Utilizing tools and scripts to automatically test and scan the program for security flaws is known as automated testing.

There are several different types of application security testing, including:

- Static Application Security Testing (SAST): This type of testing involves analyzing the application's source code for security vulnerabilities. SAST can be performed manually or using automated tools.
- Dynamic Application Security Testing (DAST): This type of testing involves testing the application while it is running to identify security vulnerabilities. DAST can be performed manually or using automated tools.
- Interactive Application Security Testing (IAST): This type of testing involves a combination of SAST and DAST. It analyzes the application's source code and tests it while it is running to identify security vulnerabilities.
- Penetration Testing: This type of testing involves attempting to exploit vulnerabilities in the application to determine its security level. [3]

CYBER COUNTER-TERRORISM: SHUTDOWN

BREAKING THROUGH THE VULNERABILITIES OF FEAR



Lucas Maclaud

A security consultant at Ghost Level Security (Brazil), IBM Certified Cybersecurity Analyst, Veteran of the Brazilian Marine Corps, former member of the Special Operations Battalion.

ACT - Counterterrorism Certificate by the Security Industry Authority (SIA – United Kingdom), Counterterrorism Training Certificate from the Academy of Counter Terrorism (LSU/NCBRT - USA) and the Defense Counterintelligence and Security Agency (DCSA - USA) and Cyber Warfare from Charles Sturt University (AUS).

CIEH and ISC certification student and anti-terrorist investigator.

Founder of Ghost Level Security (G.L.S), a consultancy focused on complete enterprise defense, offering Blue Team and Red Team analysis as a Pentester, and offering organic security support.

Business contact:

E-mail: gl_security@protonmail.me

Instagram: @ghostlevelsecurity

From here, a perspective will be addressed regarding the power of information security as the most effective current tool in the fight against terrorism via the network.

The individual with information has a moral duty to face this global threat, which has become the virus of our generation, based on research and historical surveys that show the defense power of those who have access to information.

With the modernization of security systems, with constant anti-virus updates and increasingly advanced firewalls, we have a constant need for investments in the technological sector, due to the constant advance of malicious attacks.

According to the Cambridge dictionary, terror is:

"Violent action or threats designed to strike fear among the common people,
in order to achieve political goals"

However, it is possible to add to this definition several current motivations for terrorist actions, such as religious issues, financial issues and various personal reasons inherent in human beings with an extreme level of perversity, which may even be bullying (that's right, motivations of young people to commit acts of terror due to psychological changes in schools and the internet), that can be used to alienate terrorist groups, that is, an attempt to affect a person's freedom.



FILE SYSTEM FAULT IN FAT32-FORMATTED DRIVES REVEALED BY MORSE-CODE DIRECTORY NAMES IN WINDOWS OS ENVIRONMENT. VULNERABILITY IN USB FLASH/HARD DRIVE (PENDRIVE, PORTABLE EXTERNAL/INTERNAL HARD DRIVE) CASE STUDY

Łukasz Grządko

My computer adventure began at the age of 8, and just two years later, I started programming interactive video games in Basic language. I have participated in many maths and programming competitions, and decided to widen and strengthen my math and computer skills by attending and graduating in Computer Science at the University of Wrocław. I have interests that span from the theory and mathematics to algorithms and data structures to application and software. I have also been a TopCoder algorithm member since March 2005. Currently, I work as a Software Development Engineer in LTE and 5G Mobile Broadband technologies in Nokia. You may find interesting algorithms eg. in the “Primality tests” chapter in Nokia Book IV. You may also find other articles which were published in 'Delta Monthly', a popular computer science magazine published by the University of Warsaw, 'Programista' a magazine for software engineers, 'Chalkdust' Magazine published by the University College London, and Academia.edu.

The problem described can be reproduced in Microsoft Windows family of operating systems (i.e. Windows XP, Vista, 7, 8.1 Enterprise/Pro, 10 Enterprise 21H2, 11 Home 21H2). This is only a sample of operating systems set. Most probably, it exists in all Windows system versions but with a bit different behaviour – described later in this text. This quite unusual problem was encountered by coincidence.

Most computer users have created at least one directory on a disk and store some data in it. It is also usual that some other directory is created on the same directory-tree level. Some folder names, with special characters, may surprise the user and influence user data.

What is this problem and how can one reproduce it?

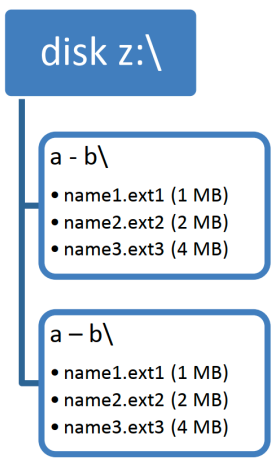


Figure 1a. Folders structure on the USB device. OS shows the same files like in "a - b" after the creation of a folder "a – b". After the entire procedure, free disk memory decreased by 7MB, not 14 MB.

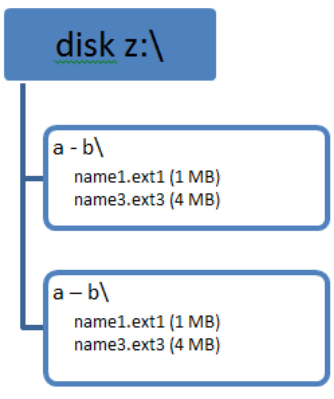


Figure 1b. Folders content after "name2.ext2" removal from exactly one of the folders. Free memory increased by 2MB.

Definitions

Denote base folder as folder name with "-" characters (short hyphen minus), e.g. "a - b" (please note that name is in quotation marks, they are not part of a name). Additional spaces around minus are required.

Denote a secondary folder as the folder name with at least one "–" character (long hyphen minus), e.g. "a – b". Please note a special dash in the middle of the word. Additional spaces characters are required too.

Reproducing a problem

We create a secondary directory with the simple name "a – b" and copy some files to it.

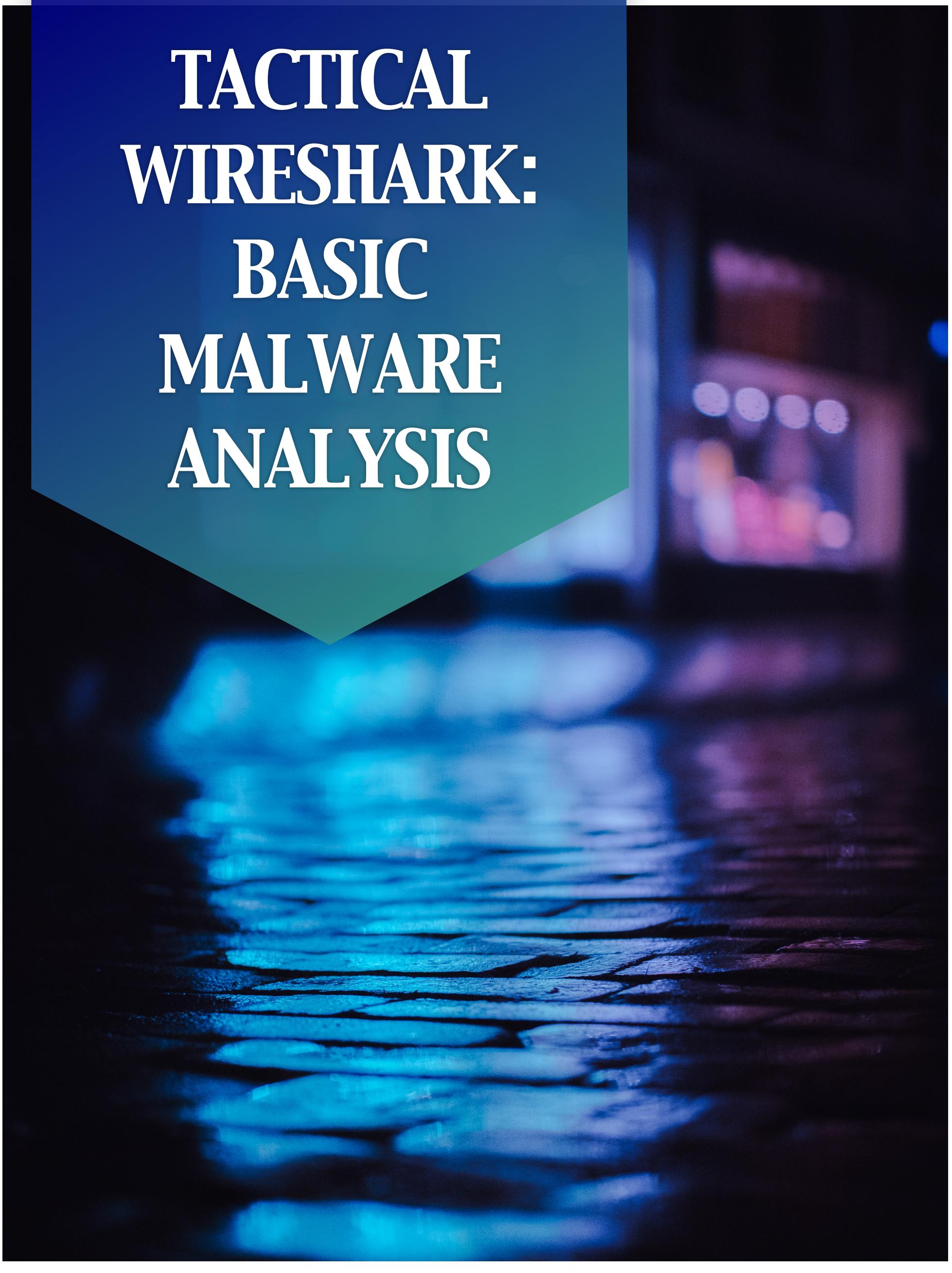
Then we return from this folder and create a new one, i.e. base folder, on the same directory-level and name it "a - b".

And now, the whole content of the secondary folder appears in the base folder too. However, it looks like a link, because memory usage does not change after base folder creation (Figure 1a). Similarly works reverse operation, i.e. file removal. If "name2.ext2" is erased from one folder, then it automatically disappears from the second folder as well (Figure 1b).

Please note it is important that the problem appears only when the base folder is created and at least one secondary folder is created.

From now on, we will also call this problem the hyphen minus problem or just minus problem.

TACTICAL WIRESHARK: BASIC MALWARE ANALYSIS



Kevin Cardwell

Kevin Cardwell spent 22 years in the U.S. Navy. He has worked as both software and systems engineer on a variety of Department of Defense projects and early on was chosen as a member of the project to bring Internet access to ships at sea. Following this highly successful project he was selected to head the team that built a Network Operations and Security Center (NOSC) that provided services to the commands ashore and ships at sea in the Norwegian Sea and Atlantic Ocean. He served as the Leading Chief of Information Security at the NOSC for six years. While there he created a Strategy and Training plan for the development of an expert team that took personnel with little or no experience and built them into expert team members for manning of the NOSC. He is an Instructor, Curriculum Developer, Technical Editor and Author for Computer Forensics, and Hacking courses. He is the author of the EC Council Certified Penetration Testing Professional, Ethical Hacking Core Skills, Advanced Penetration Testing and ICS/SCADA Security courses. He has presented at the Blackhat USA, Hacker Halted, ISSA and TakeDownCon conferences as well as many others. He has chaired the Cybercrime and Cyberdefense Summit in Oman and was Executive Chairman of the Oil and Gas Cyberdefense Summit. He is author Defense and Deception: Confuse and Frustrate the Hackers, Building Virtual Pentesting Labs for Advanced Penetration Testing 1st and 2nd edition, Advanced Penetration Testing for Highly Secured Environments 2nd Edition and Backtrack: Testing Wireless Network Security. He holds a BS in Computer Science from National University in California and a MS in Software Engineering from the Southern Methodist University (SMU) in Texas. He developed the Strategy and Training Development Plan for the first Government CERT in the country of Oman that is rated as the top CERT for the Middle East. He serves as a professional training consultant to the Oman Information Technology Authority and developed the team to man the first Commercial Security Operations Center in the country of Oman.

He has worked extensively with banks and financial institutions throughout the Middle East, Africa, Europe and the UK in the planning of a robust and secure architecture and implementing requirements to meet compliance. He currently provides consultancy to Commercial companies. He provides training and consultancy to the Oman CERT and the SOC team in monitoring and incident identification of intrusions and incidents within the Gulf region. He holds the CEH, ECSA. LPT Master, APT, CTIA , CSA CHFI, ECIH. CPENT as well as other certifications. He is currently the President and one of the founders of Cyber2Labs LLC and Cardwell Engineering Solutions International.

Major IT Projects – Kevin Cardwell Lead/Managed:

- Internet Access to U.S. Navy warships Network Operations and Security Center – European Headquarters
- Conversion of Dead Reckoning Tracer to a Fully Digital System
- Systems Engineer for the Digitization of Periscope RADAR Detection System
- Software Engineer Head for the Remote Mine Hunting Software System
- Strategy training plan for the Team to Man the CERT in Country of Oman
- Design and implementation of the first commercial Security Operations Center in the country of Oman
- Implementation of the Network Architecture for the two international airports in the country of Oman
- Security baseline development for the Oman Telephone company and the Airport Management Commission
- DoD Drone Research for Offensive tactics to counter drones as a weapon
- Strategy and Training Plan for the Algerian Army Network Security Specialists
- Strategy and Training Plan to secure multiple countries in Africa

In this article, I will review some of the concepts I explore in my book on Wireshark to be published soon.

I will briefly look at the first steps of using Wireshark in a tactical manner for the support of intrusion analysis and incident response. I am currently working with the US/Africa initiatives to try to secure multiple countries in Africa. A component of this is to train the local population to maintain and monitor a Security Operations Center (SOC) to help them protect their digital sovereignty and secure their country. These "potential" articles, including this one, will build on the concept of taking someone with a network background and molding that person into a Cyber Security SOC Analyst. We will cover:

- File Extraction
- Domain Recognition
- Determining Connections

Extracting the files

In the early days of Wireshark, we did not have the capability to automatically extract data and the carving of files could be a challenge. We had to manually locate the header, then work through the file contents until we found the trailer, which would then be combined and "hopefully" we would be successful at the extraction of the data. In many cases, it would take more than one try and it could become tedious at times. Thankfully, the versions that have come later have continued to improve the process. The capability is available from our dashboard menu. The option is located under the **File** menu; an example of the option is shown in Figure 1.

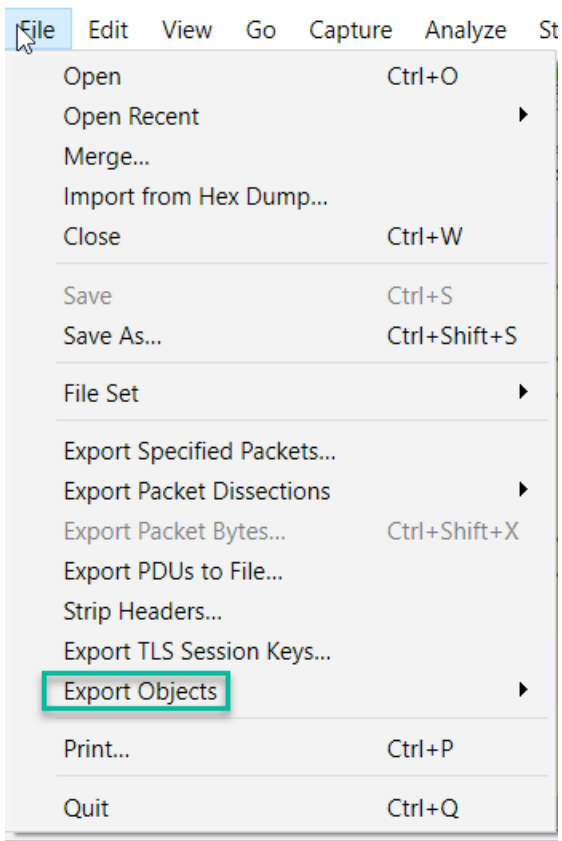
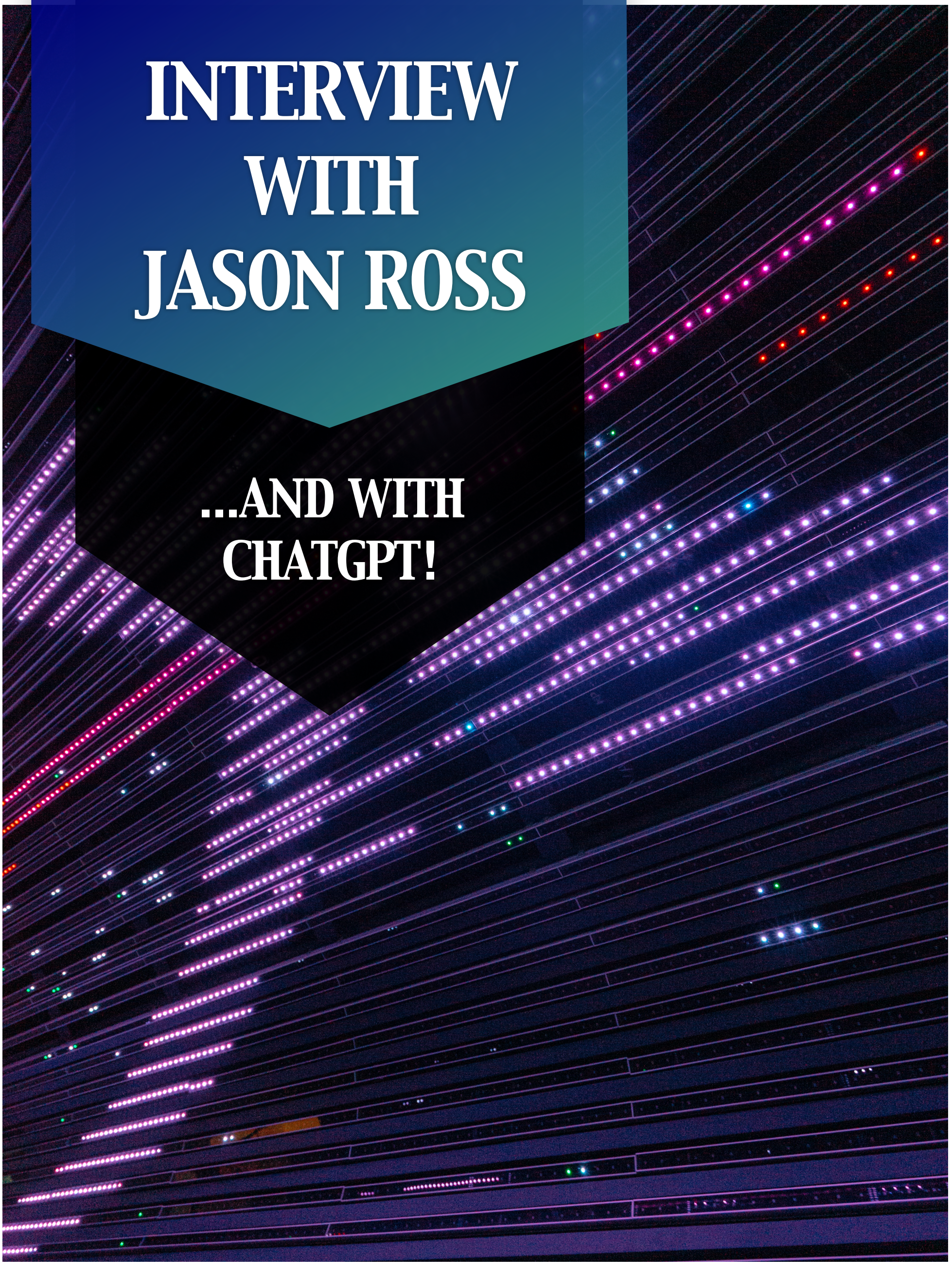


Figure 1. The Export Objects menu option

INTERVIEW WITH JASON ROSS

...AND WITH CHATGPT!



Here you will find an interview with Jason Ross, where we ask him about Machine Learning, Deep Learning, AI, and more. To spice things up, the author gave us 2 sets of answers: one delivered by him, and one by ChatGPT! It is your job to guess which ones are his original statements! If you have a clear idea why one set of answers is given by AI, try to formulate the reason. We're super curious about your opinions! Hit us at hello@haking.org ;)

1st set of answers

[Haking Magazine]: Hello, Jason! It means a lot to us that you agreed to our interview. Could you introduce yourself to our readers?

[Jason Ross]: Hi Agata! Thanks for having me. I'm an experienced security professional, and have been working in the IT/Security industry since 1998. I started out on the help desk for a telecom, then moved into system administration and network security. Eventually I ended up as a security consultant focused on penetration testing, and spent about 12 years doing that. I've recently moved out of consulting, and now perform internal security assessments and develop security policies for a Fortune 500 company. I'm also an adjunct faculty member at the Rochester Institute of Technology, and in my spare time I help out with a number of security conferences and competitions, including BSides Las Vegas, DEF CON, and the global Collegiate Penetration Testing Competition.

[H9]: You have big experience in the IT background. In hindsight, which technology was the most professionally fruitful to you?

[JR]: I've been very careful throughout my career to not specialize in any one thing, but to keep a very broad knowledge base. I think that's been the most beneficial thing for me: it's allowed me to work in a variety of positions, which overall let me be able to quickly understand how various pieces of technology fit into the environments they are deployed to, and find gaps in the security posture that may have been overlooked.

[H9]: How did the change of Internet technology affect your work from the security perspective? Was it harder several years ago or is it more difficult now?

[JR]: I definitely think it's harder now, but the reason why is an odd mix of "because things are more secure by default, generally" and "because systems are more complex generally". The complexity means that there are lots of moving parts and interconnections, often managed by different individuals or teams within an organization, and the interconnections between them are often misunderstood, or even completely overlooked. Where in the past there was a very well defined stack of technology, with simple connections between the various layers, now there is a complex mesh of interconnected strands, and while each individual piece may be secure, often the way those pieces interact is ignored, and that allows vulnerabilities to creep in.