PREVIEW

HAKIN9

PHYSICAL PROTECTION

IT SECURITY MAGAZINE

VOL.17, NO.12

BEST OF 2022

Smart Cities: Security, Resiliency, and Privacy Attacks

Securing a Smart Home

Metasploit from Scratch

Cyberbiosecurity: A New Context for the Fourth Industrial Revolution

AND MORE...



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

Marta Sienicka

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,

We are happy to share our Hakin9 special edition composed of the most intriguing and exciting articles published in our monthly editions in 2022! In this ‘Best of 2022’, you will find those pieces of knowledge which spiked the most interest and gained top feedback from our dear readers!

Here, you will read excellent articles on the most important and leading topics in the past few months. Those will definitely still stay relevant in 2023, so you should surely read them if you haven’t already.

Learn how to stop ransomware and how to secure your smart home! Apart from that, read about smart cities, cyberbiosecurity, Raspberry Pi, and many more! Dive in this H9 edition compiling the most compelling topics of 2022!

Stay safe,

Hakin9 Editorial Team

TABLE OF **CONTENTS**

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

26 ***CYBERBIOSECURITY: A NEW CONTEXT FOR THE FOURTH INDUSTRIAL REVOLUTION;*** *DR. ANTHONY CALDWELL*

36 **SMART CITIES: SECURITY, RESILIENCY, AND PRIVACY ATTACKS;** CHRISSA CONSTANTINE

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

79 ***STOP RANSOMWARE IN ITS TRACKS USING FILTERING AND DECEPTION;*** *KEVIN CARDWELL*

105 ***WHAT IS A PRIVACY RED TEAM?;*** *GABRIEL CARVALHAES*

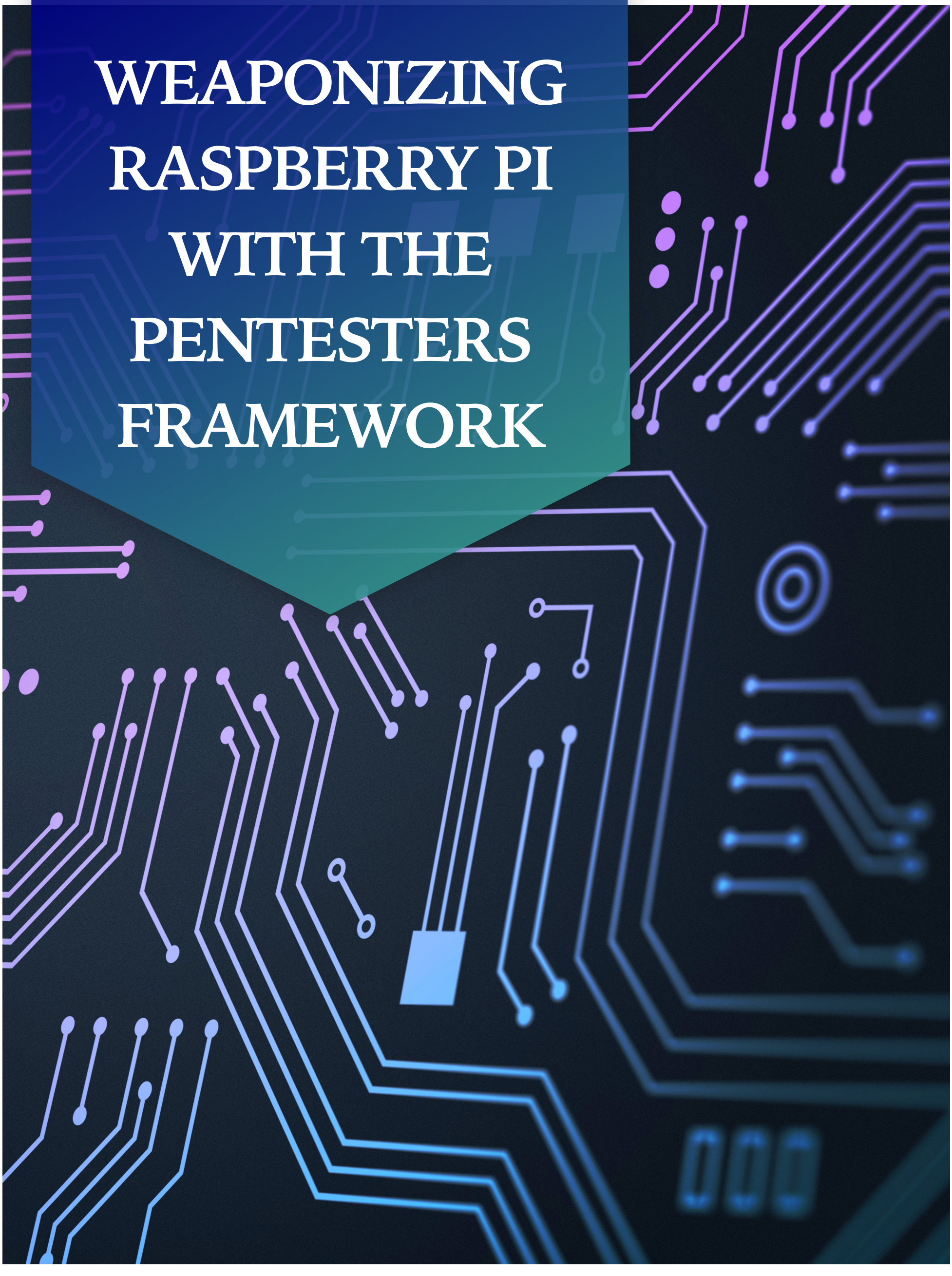
115 ***SECURING A SMART HOME;*** *MOHAMMADY ARVIN & OGANEZOV ALEXANDRE*

136 ***BASIC BETTERCAP;*** *ATLAS STARK*

154 ***GOBUSTER - BRUTE FORCE TOOL FOR HACKERS;*** *MICHAEL SOMMER & THORN DEIL*

178 ***CROSS-SITE SCRIPTING (XSS) FLAWS AND FOCUS ON BLIND XSS;*** *ROBERTO CHEMAMA & ANTOINE PLANQUE*

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

CYBERBIOSECURITY: A NEW CONTEXT FOR THE FOURTH INDUSTRIAL REVOLUTION



Dr. Anthony Caldwell

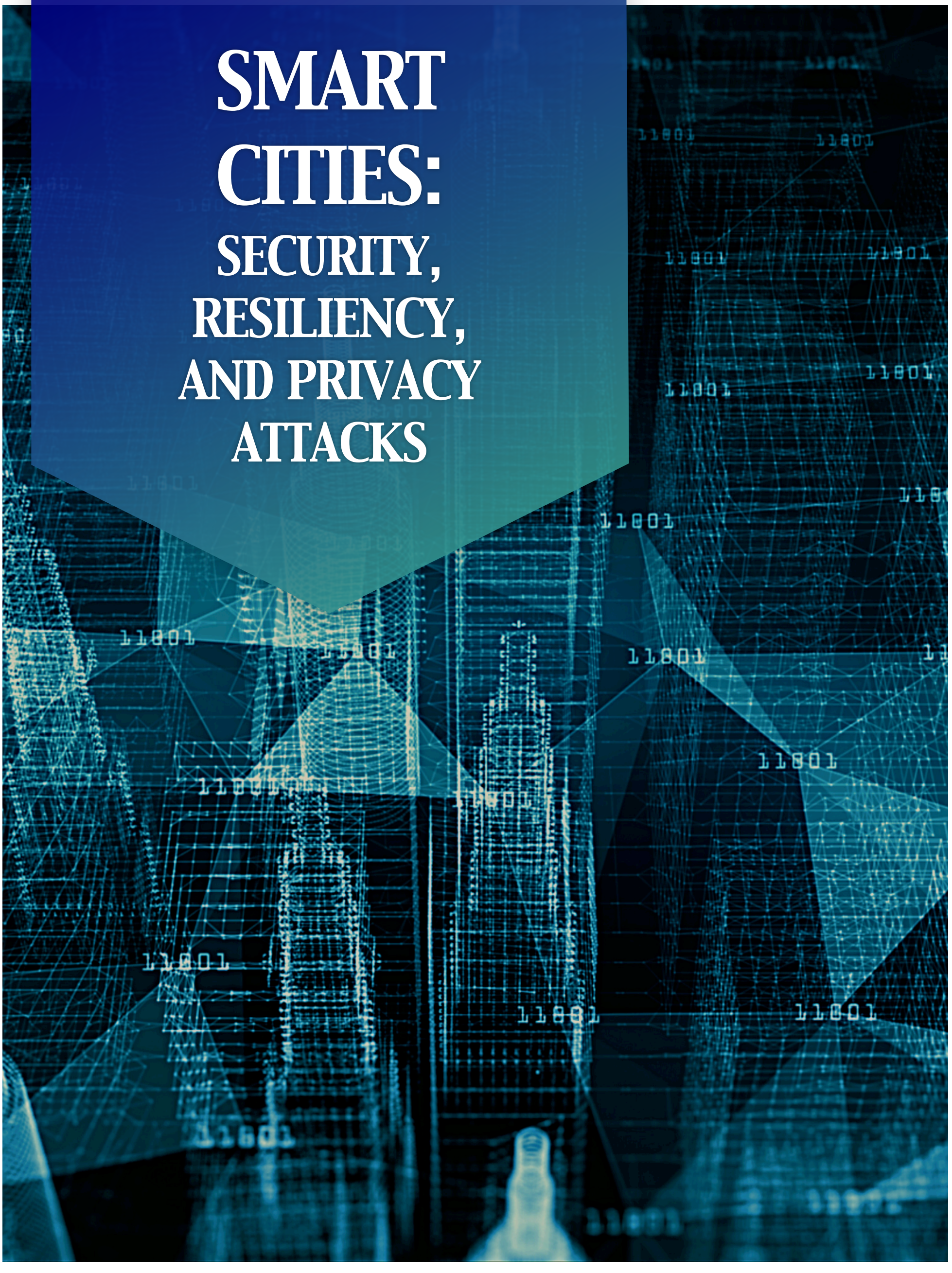
Dr. Anthony Caldwell is a cybersecurity professional and academic with over twenty years experience in industry. He is also the editor-in-chief of the international journal of information security research (IJISR).

The impressive success of the digital economy comes fraught with risks as well as rewards. In this respect, a focus of intense interest surrounding the relevance of cybersecurity has penetrated into many areas of computer science, economics, AI and law to name a few. In today's highly interconnected world, an increasingly wide variety of applications are subjected to security attacks. Of particular concern are the bioinformatic systems which store patient/customer medical data and the institutions themselves that gather it. This paper introduces some of the important themes developing within the discussions on cyberbiosecurity through the lens of the fourth industrial revolution and highlights some of the crises that may yet emerge.

Cyberbiosecurity

Cyberbiosecurity is underrepresented in research articles, even among biotechnology and cybersecurity experts. What is required is a concerted effort to enhance emerging research in this field, so that we might foster awareness of these threats as the digital age of biology progresses. As an idea, cyber-biosecurity is not well-known or understood, even among biotechnology and cybersecurity experts (Millet, DosSantos and Millet, 2019). Murch et al. (2018) represents cyberbiosecurity as an interface between biosecurity, cybersecurity and cyber-physical security (Fig. 1.). Cyberbiosecurity is afflicted with its own security vulnerabilities arising from convergence of technologies in medical sciences, supply chain and infrastructure systems (Muller et al., 2021). Examples of systems in which cyberbiosecurity may become a factor when protecting the end-user are, outsourcing in biotechnology where the infrastructure becomes a target such as the equipment and service providers networked and connected online, thus leading to risk of accidental or deliberate harm (Millet, DosSantos and Millet, 2019), or misconfigured security access to medical records leading to ransom or purchase it on the black market (Mirsky et al., 2018). Medical research facilities, as well as institutional organizations, have security and engineering controls preventing environmental contamination and threats to the health of humans, plants and animals. However, these too have already fallen prey to damaging attacks such as the Irish health service in 2021 (The Journal, 2021) with consequences such as endangering public health, the environment, economy and national security (Muller et al. 2021). Indeed, the World Economic Forum (2017) published an article outlining the dangers of engineering viruses via the purchase of a used DNA synthesis machine online for less than $10,000, which has the power to engineer biological agents, such as the Canadian researchers who synthesized the horsepox virus, a relative of smallpox, from genetic pieces ordered in the mail (World Economic Forum, 2017; Science, 2017). Critical areas of attack could generally be characterized within categories such as sabotage, corporate espionage and crime/extortion (Muller et al. 2021). As pointed out by Heus et al. (2017) the scale of intellectual property losses associated with digitized biological information could rise to millions or billions (Heus et al., 2017). The more we rely on medical databases, the more likely these databases will become targets for cyber-attacks to interfere with public health and biosecurity systems (Vinatzer et al., 2019). Closer to home, the need for in-hand connection with the Internet of Things (IoT), simplified access to large databases, as well as the use of affordable hardware, may be convenient for users and health care practitioners but also more convenient to hack (Khera, 2017). Worryingly, this has already been demonstrated. Radcliffe had turned his night time hobby hours to tinkering with his own insulin pump to see

SMART CITIES: SECURITY, RESILIENCY, AND PRIVACY ATTACKS



Chrissa Constantine

Chrissa is a cybersecurity professional with a strong background in research and writing, cybersecurity, vulnerability assessment, web application testing and security training. She has experience in designing creative instructional games and interactive exercises that make learning complex concepts enjoyable. She enjoys working on OSINT investigations and helping others. She currently serves as an ISC2 CNMC Founding Member and Officer of the Board of Directors.

Certifications:

- ISC2 CISSP
- EC-Council Certified Ethical Hacker (CIEH)
- SANS GIAC GWAPT

What Makes a Smart City Smart?

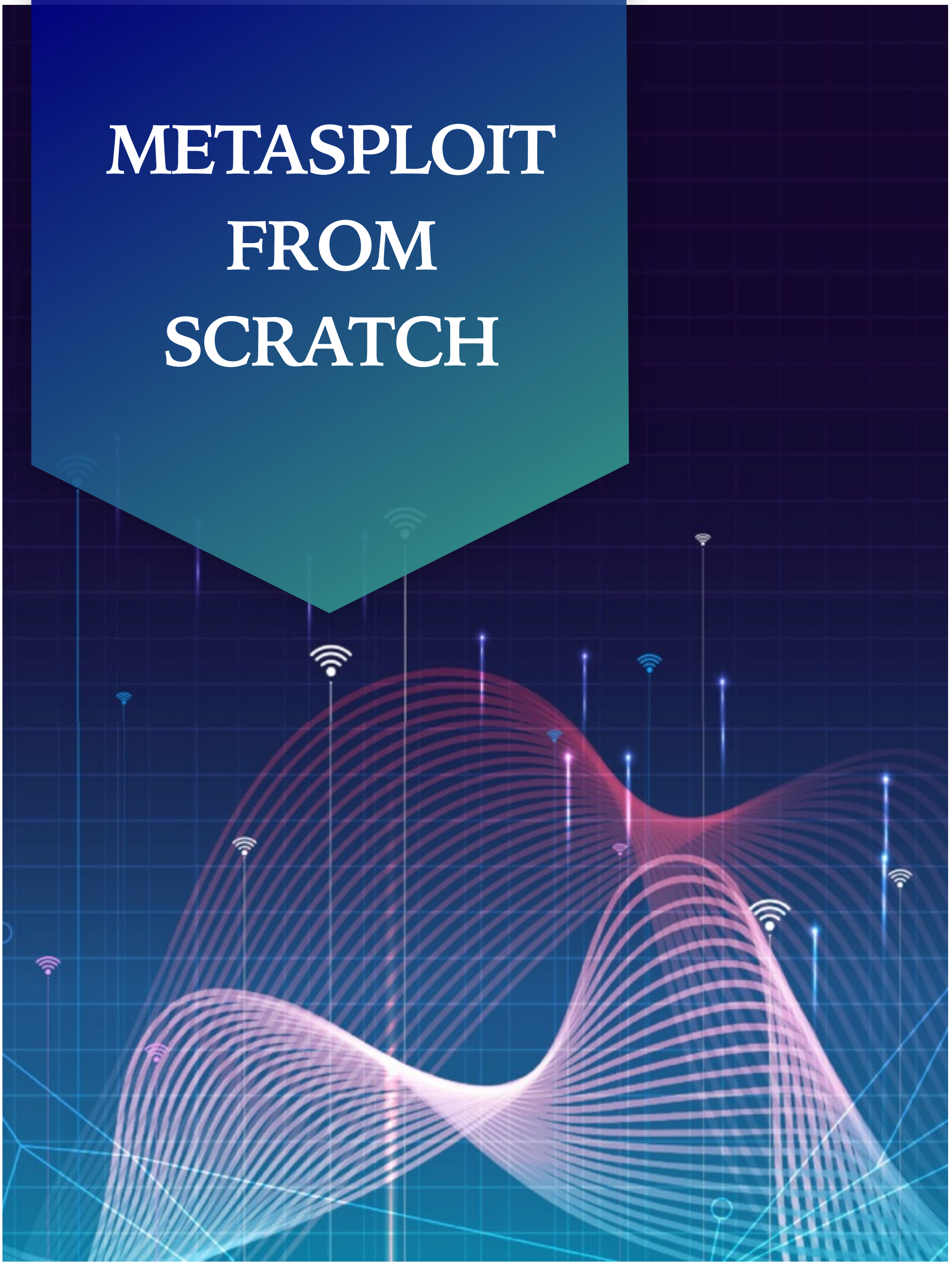
Urban centers that leverage technologies to connect and improve infrastructure that enhance the efficiency, convenience and quality of life, is a "smart" city. Smart functionality can take many forms. Some examples of intelligent technology that can be found in a city include:

- Traffic control sensors, such as sensor-based traffic lights, vehicle and pedestrian aware sensors, roadside traffic cameras, roadside sensors for speed, weather, or volume of traffic, and automated license plate readers (ALPRs) or internet connected security cameras
- Connected "smart" vehicles that communicate to traffic meters, charging stations or other vehicles using an ad hoc mobile network called VANet for vehicle-to-vehicle or vehicle-to-roadside communications. This network enhances safety, helps with collision avoidance, traffic optimization, and locating charging stations or fuel pumps. (Brooks, Bae Yun, & Deng, 2012) Vehicles also connect for internet, phone, and entertainment purposes
- Internet-connected, sensor-based electric meters that help with energy consumption and reduce energy usage by helping people find parking
- Smartphones with digital driver's licenses or other forms of ID
- Sensors that monitor environmental events
- Intelligence medical devices and telehealth, e-government platforms with personal data
- Intelligent factories and software for industrial systems
- Smart retail with public kiosk services and payment services
- Smart homes with intelligent gas meters, sensors, solar panels
- Intelligent agricultural devices, such as tractors
- Disaster warning services
- Urban buildings can contain various sensors to measure temperature, humidity, occupancy, doors being open/closed, air quality or security

There are numerous definitions and synonyms for a smart city, such as "connected city," "digital city," "resilient city," "digital community," or "intelligent community." In this paper, these terms represent an urban center that uses technology to connect people and things.

Smart cities use vast amounts of data to efficiently manage assets, resources, and services. This data is collected from various sources, such as people, devices, and buildings, and is used to improve city-wide operations. Thoughtful city planning requires critical public safety and security for networks carrying sensitive traffic or data (e.g., police dispatches), and that operate life-critical systems (e.g., emergency services communications).

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.

STOP RANSOMWARE IN ITS TRACKS USING FILTERING AND DECEPTION

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

Introduction

If you follow any of the latest attacks that make the news, you have no doubt seen that these attacks are for the most part related to some form of a malware derivative ransomware. While it is true to some extent that these attacks have continued to increase in both sophistication and complexity. The reality is that any organization who has had the unfortunate experience of being a victim of this attack should not have lost the ability to perform either their network requirements or mission requirements in the case of military or government networks; furthermore, any organization or entity who has lost their entire network more than likely has a poor network design to blame. Even a network that follows the basic best practices tenets with respect to security would be enough to prevent the loss of the entire network capability. In this article, you will learn about these fundamental design concepts that will allow you to protect your network and/or enterprise from the majority of these attacks. You will get the most out of the article if you have a foundation and understanding of networking.

Segmentation and Isolation

The first concept we will talk about here is that of segmentation and isolation. To this day, I do not understand many of the network architectures I see. It is like most people have forgotten the simple design principles that we have been using for many years. This principle is that of separation of your user data from your services data. When you think about it, why would you ever mix your data? While this concept is not new, it is rarely followed today. Since I come from a Navy background and was part of the team to bring Internet access to US Navy ships, I will share with you one of our simple design decisions. When we started to place Internet access on Navy warships and designed our network, we made sure not to place the Tomahawk Missile Control Systems on the same network segment as the Internet. So, why is it that all of these enterprise networks have their critical data mixing with all of their other data? Again, poor network design. Let us take a look at a network architecture diagram. This is the Purdue Reference Model, and it is for Industrial Control Systems (ICS) and is an older model from the 1990s, but it is still a good reference point to start with. This model is shown in Figure 1.

WHAT IS A PRIVACY RED TEAM?



Gabriel Carvalhaes

I work as a Cyber Security Analyst for a software development company in Brazil, wearing a multitude of hats and working on internal audits, awareness materials, risk management, and a lot more. My main focus is to build an interdisciplinary career in Cyber Security and gain experience both in the OffSec world and GRC.

Reach out: https://www.linkedin.com/in/gabrielcarvalhaes10/

1. Introduction

Red teaming has been one of the most pursued careers in Cyber Security. However, many people, including IT professionals, mistake Red Team Operations for pentests and vulnerability scans. Although pentests and vulnerability scans can be part of a red team operation, they are security activities with a limited scope, whereas a true red team operation, in essence, has no limited scope in order to assess all types of flaws in a system or in a company. It can go for months on end and the goal is to emulate an Advanced Persistent Threat (APT) trying to break in through any means necessary. In short, this is what a red team is.

The image below can help explain the relation between Red Team and other areas of Cyber Security:

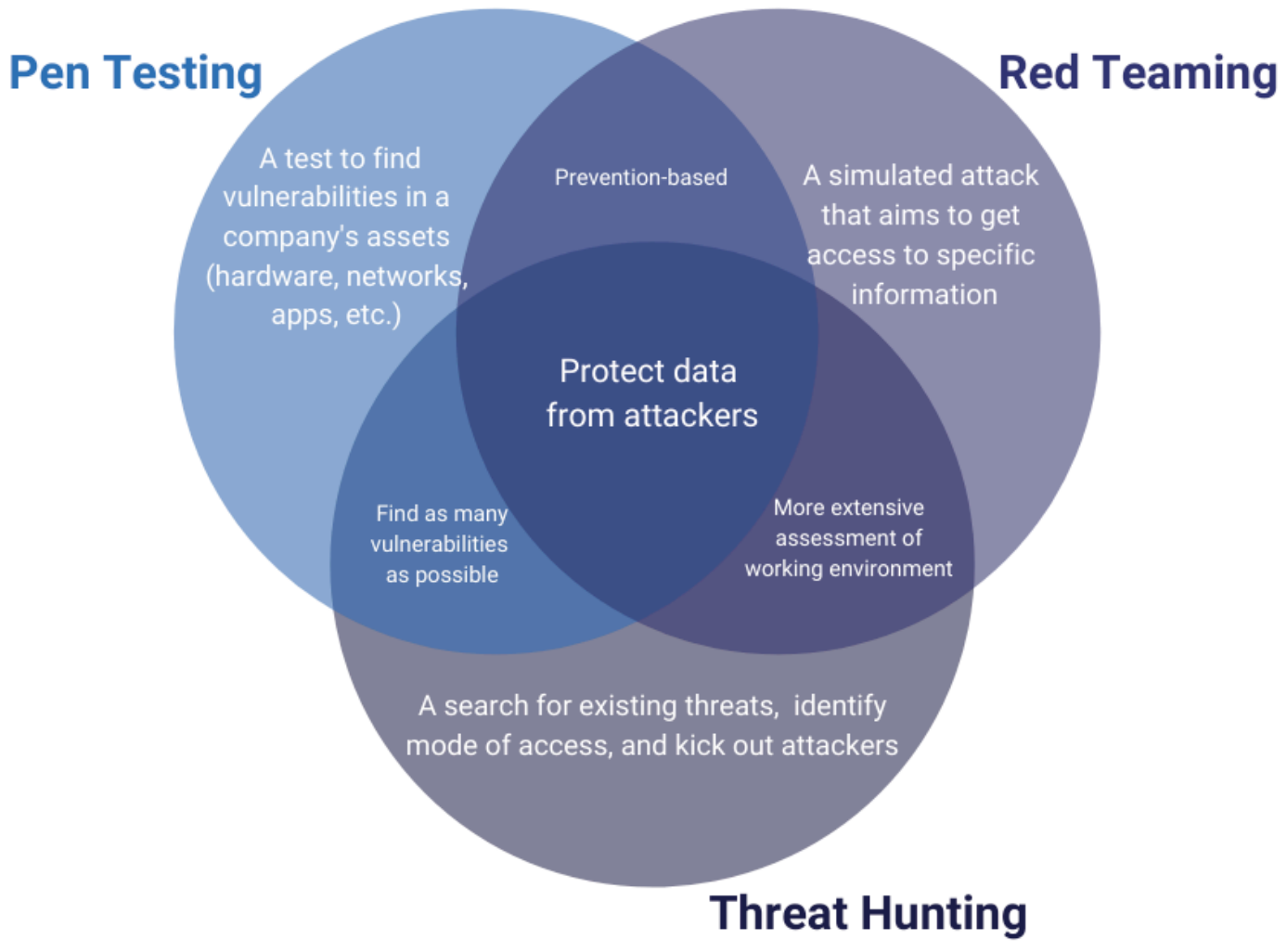


FIGURE 1 VENN DIAGRAM OF PENTESTING, THREAT HUNTING AND RED TEAM.
HTTPS://WWW.MINDPOINTGROUP.COM/BLOG/DIFFERENCE-BETWEEN-PEN-TESTING-RED-TEAMING-AND-THREAT-HUNTING

Red team operators from all over the world study the traits of APTs very deeply to elaborate the best frameworks and techniques to deal with this type of targeted attack. But they face some challenges that make it difficult to keep up with APT groups. Cybercrime is not bound by time or law limitations, and, because of that, red team operators need to make sure that their work is efficient.

SECURING A SMART HOME



Mohammady Arvin & Oganezov Alexandre

We are both first year master's degree students at Université Paris Cité in France. We both study cybersecurity. The idea of our project came from the fact that we wanted the Raspberry Pi to be the node of something but also to work on something that could potentially be useful.

INTRODUCTION

In a world where technological advances are increasingly numerous, there is an emergence of what is called "smart homes". It is a term that is beginning to be known by the public through its media coverage as in series and movies.

Perhaps some of you do not know what a smart home is. To begin with, smart houses are part of the home automation field. These are homes where the equipment is automated. It means that all actions can be programmed remotely thanks to your smartphone or tablet. For example, imagine that you come back home, tired after a long day of work and then when you arrive, the lights are already turned on, as well as the coffee machine and everything you needed. This is a considerable savings of time and energy for the owner.

However, the automation of a multitude of devices in a house inevitably involves risks, and that is precisely what this article is about. We will first study the risks that a smart house can set forth but also its advantages, then we will see how to avoid being attacked and finally, we will propose a solution to secure a smart house based on the study of human behaviour.

WHAT ARE THE ADVANTAGES AND RISKS OF OWNING A SMART HOME?

Advantages

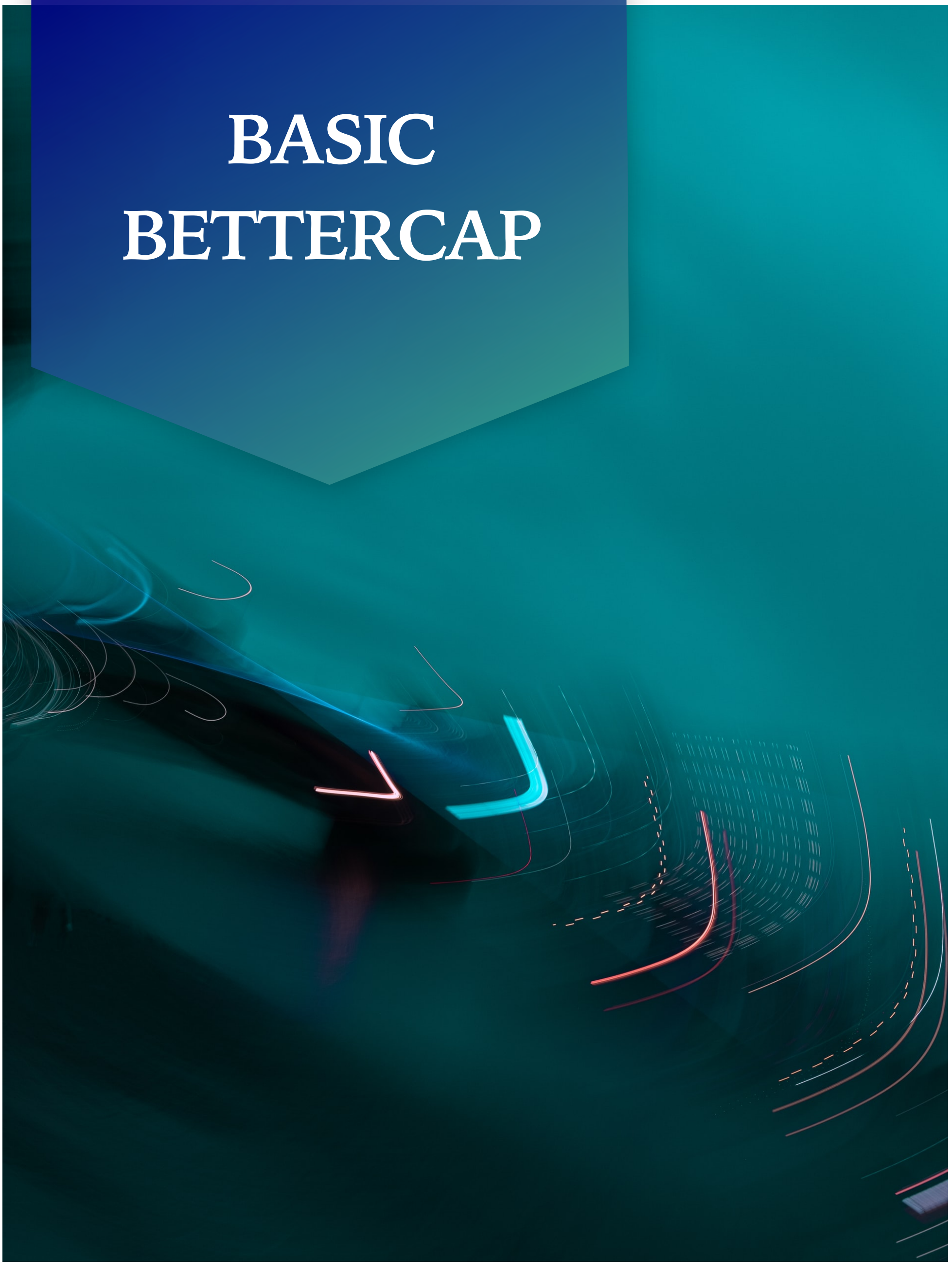
Smart homes have many advantages, in fact, a smart home greatly improves the comfort of its owner. The automation of a home's equipment and facilities allows the owner to make his life easier. Take for example a person who is at work. This person knows how long it will take to get home, so he can already start the appliances to start cooking the meal, heating the house, etc., before he gets home so that he does not waste time. He can also decide to turn off a piece of equipment at any time because he may have forgotten to do so, which could have dramatic consequences.

A smart house allows you to save money. As we have seen before, we can activate or deactivate equipment remotely at any time, whether we are home or not. Therefore, it is a savings of energy but also of money. Since we can regulate our energy consumption, there is also an environmental impact.

Another advantage is that a smart home is more secure. Indeed, the risk of breaking and entering is almost null because we have several levels of security. For example, a door can be configured so that it opens only when the owner is facing the door. We can also program alarms and/or surveillance cameras to control them from afar, to be alerted in case of intrusion and to contact the security services quickly.

Nevertheless, this security that is sold to us is not totally infallible and, on the contrary, presents many risks.

BASIC BETTERCAP



Atlas Stark

Atlas Stark is a security researcher at Stark Industries Inc. with 16+ years in the technology industry. Currently providing cyber security solutions and OSINT services to anti-human trafficking non-profits that aid in investigation and victim recovery. He also consults with state level law enforcement agencies concerning hacking related incidents. He splits his time between California and Tennessee.

Q/C:

Please email stark@starkinternational.se with any questions or concerns.

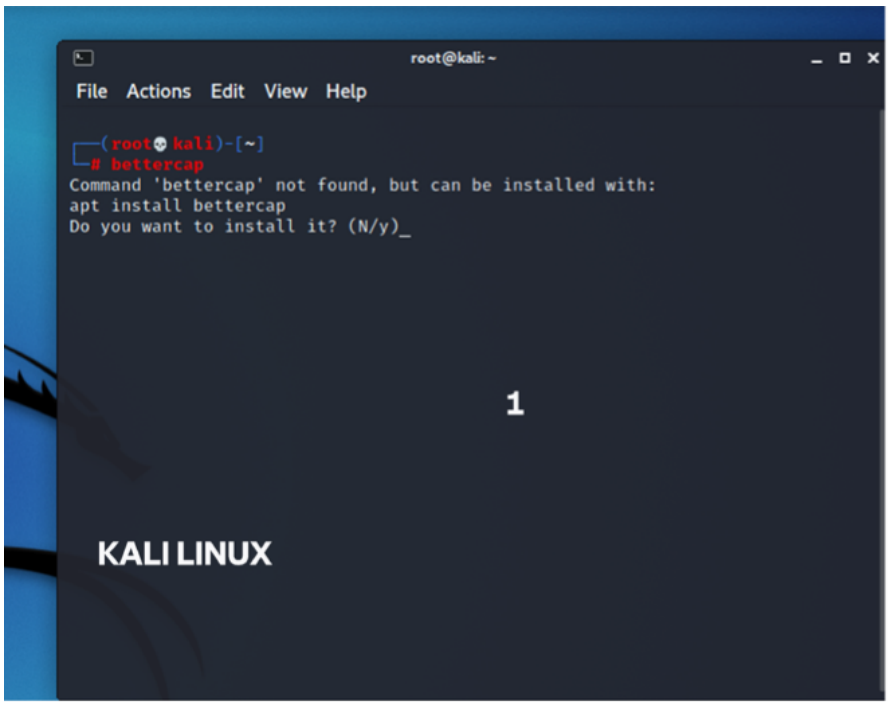
Pentesting and ethical hacking involves laborious and lengthy tasks that demand our full attention at all times, especially if you're deploying and monitoring a variety of tools simultaneously. When you discover a tool that combines a variety of extremely useful functions, you tend to utilize that tool to make your time more efficient, and if that tool is Bettercap, well, you have a keeper for sure.

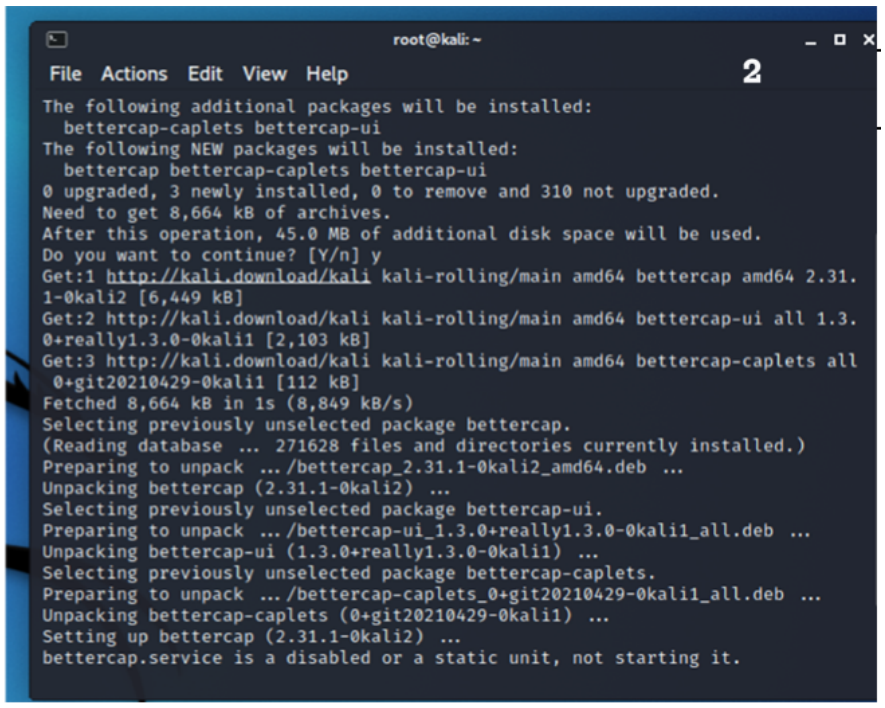
Bettercap

Bettercap, since its inception, has been referred to as the Swiss Army knife for the reconnaissance and attacking of Wi-Fi networks. It is extremely effective when conducting MITM (Man In The Middle) attacks and ARP Spoofing. The framework is written in GO which is an open source programming language that can be used to build a variety of useful applications. Check the links and resources for a recommendation for the "Black Hat GO" book from No Starch Press, it's a great resource. Bettercap can provide a variety of functions that can assist you on your next engagement so let's dive into Bettercap at the beginner level.

Bettercap Installation

Bettercap comes preinstalled in Kali Linux, however, in the event it does not there are a variety of ways to obtain Bettercap. For this article, we will be discussing Bettercap installation with Kali Linux and Fedora. The reason I choose both is that they open up some options for you, especially if you are new to Kali Linux or your daily driver OS is another Linux flavor. The following screenshots will walk you through an installation on both Kali Linux and Fedora.





As you can see, in this version of Kali Linux, Bettercap is not already installed, however, it does ask if we would like

GOBUSTER - BRUTE FORCE TOOL FOR HACKERS



Michael Sommer & Thorn Deil

Michael Sommer is a Senior Information Security Consultant and CISO at CONSULECTRA GmbH in Hamburg. He started in security in 2006. His focus is on penetration testing, critical infrastructure, live hacking, cloud security, ISMS consulting and more. He runs a YouTube channel for solution videos of web security labs.

Thorn Deil is a Junior Security Consultant and Pentester at CONSULECTRA GmbH since 2022. He completed an apprenticeship as an IT systems electronics technician at the Wilhelmshaven Naval Arsenal in 2018 and graduated with a bachelor's degree in applied computer science with a focus on IT security from University of Applied Sciences Mittweida in 2021.

WHAT IS GOBUSTER?

Gobuster is a brute force tool that can be used for different use cases within pentests or bug bounty programs. One of Gobuster's strengths is brute-forcing directories and files on web servers. Another use case is the brute-forcing of subdomains. There is also the possibility to identify s3 buckets and VHOSTs. In the current version of Gobuster, at the time of writing this article, it was version 3.1, the fuzzing mode has been added. In this article, all modes of Gobuster are presented and explained with practical examples. Gobuster is developed in the Go programming language by OJ Reeves and Christian Mehlmauer. The project has about 6200 stars on GitHub and quite a few supporters.

Brute-Forcing

To use Gobuster effectively, it is necessary to have an understanding of brute forcing. If brute forcing is known, then this section can be skipped.

A brute force attack is an attempt to crack a password or username, or to find a hidden web page or the key used to encrypt a message. It involves a trial-and-error approach, hoping to eventually guess the desired information. This attack method is old, but it is still effective and popular among hackers. The duration of such an attack can last from a few seconds to many years. When searching for a password, the complexity of the password determines how long it takes.

Fuzzing

In this section fuzzing is described. If fuzzing is known, then this section can be skipped.

Fuzzing is an automated technique for software testing in which random data is repeatedly sent to the programunder test at one or more input interfaces. The goal of this test is to induce unpredictable reactions of the program (e.g. program crashes) and thus to be able to identify vulnerabilities. Fuzzing was developed at the University of Wisconsin-Madison in 1989 by Barton Miller and his students.

HOW TO INSTALL GOBUSTER

There are three easy ways to install the latest Gobuster version 3.1.0, which are described in the following section. The following instructions have been tested on a Linux Kali 2022.2 system.

CROSS-SITE SCRIPTING (XSS) FLAWS AND FOCUS ON BLIND XSS

Roberto Chemama & Antoine Planque

As soon as a new subject presents itself to him, Roberto dives in to understand its workings. He is passionate about cybersecurity and intends to constantly improve his skills in this field.

roberto.chemama@etu.u-paris.fr

https://www.linkedin.com/in/roberto-chemama/

Antoine is curious to constantly learn new things about cybersecurity topics. He has a strong desire to practice more CTF and is considering certifications like the OSCP.

antoine.planque@etu.u-paris.fr

https://www.linkedin.com/in/antoine-planque-a7387320b/

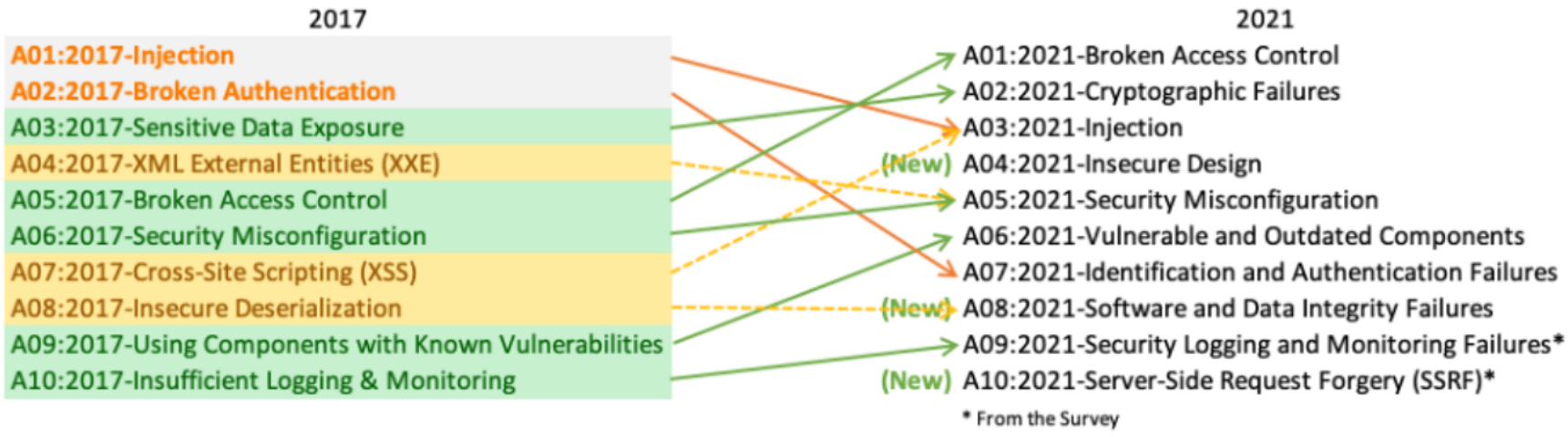
Université Paris Cité

INTRODUCTION TO XSS ATTACKS

Applications that run in a Web environment involve many technologies both on the client side (type of browser, browser version, etc.) and on the server side (type of server, database management system, etc.) and therefore generate a large attack surface.

Indeed, the OWASP, an association that works on web application security, has published a list of ten major vulnerabilities that can be found in this environment. In 2021, this list was updated for the third time to reveal a categorization of these flaws.

The one we are interested in in this article is the XSS flaw that goes from the A07:2017-Cross-Site Scripting (XSS) nomenclature to A03:2021-Injection.



OWASP TOP 10 update in 2021

It is not by chance that the XSS flaw is now categorized as an injection flaw because it consists of injecting code fragments (HTML, JavaScript) into a Web page that interprets it as something legitimate.

There are three main types of XSS flaws: Reflected XSS, DOM XSS, Stored XSS.