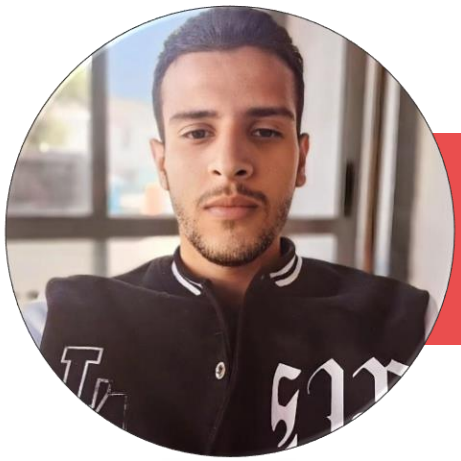


MOHAMED AMINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

OBJECTIVE

Life long learner ,Security Researcher,WEB3.0 and Devsecops enthusiast, interested in Low level applications, / Networking / Threat hunting /MERN stack Development & Blockchain related topics

SKILLS

- Static and dynamic analyzers
- Fuzzers
- ML
- Rust
- Ruby on rails
- AWS
- IBM-cloud
- CSS
- GOLANG
- C/C++
- JAVA
- DOCKER
- VMware vSphere
- VMware Horizon
- Hyper-V
- PowerShell
- batch
- autoit

EXPERIENCE

HOW I BECAME TECHIE ?

At the age of 12 I started to use 3ds max ,PS to Design visuals for my favorite game
(actually decompressing the game resource files and altering them) I was astonished
by the tens of thousands of lines of code that I cannot understand then I learned
python to create some extra functionalities these are visible only to me, using a
recently uploaded general game template files (FreeBSD Open virtualization Appliance
aka ova file, database backup ,game client) by changing some network settings and
variables and deploying the backups I was able to create my own edition without
affording domain name or stable servers I keep it running on my own computer and
using Hamachi vpn services

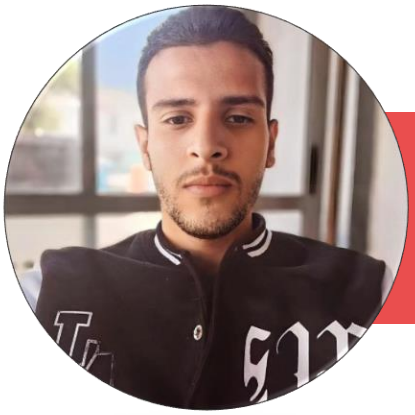
REPORTING BUGS TO ATI, ANSI • HOBBY • MAR 2017 - MAY 2017 · 3 MONTHS

Reported tons of bugs to many Tunisian website owners as a hobby some are : WEB OWASP TOP 10 others are miss use of application or not being up to date 'Linux/Windows Vulnerabilities , many of apache daemons vulnerabilities or misconfigurations of administrative content management systems '

INTRUSIF AUDITOR • SSC.NAT.TN • CONTRACT • FROM MAR 2019 - SEP 2019 · 7 MONTHS

- finding creative ways to obtain a foothold in a client's network

EMAIL | TWITTER HANDLE | TELEPHONE | LINKEDIN URL



MOHAMED AMIINE GUESMI

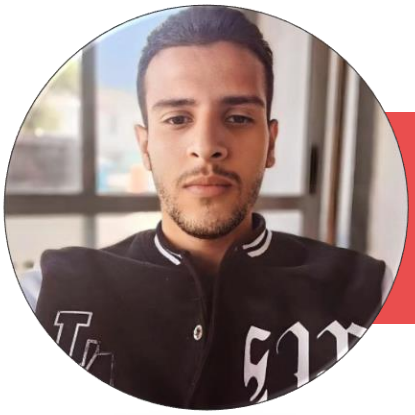
CYBER SECURITY REASERCHER
01/09/1999 NABEUL

● relational and non relational types of databases

● KOTLIN
● GROOVY
● PYTHON
● PERL
● RUBY
● LUA
● PHP
●.NET
● X64/X86 ARM Assembly
● JAVASCRIPT
● BOOTSTRAP
● Can work with advanced debuggers and disassemblers
● Can work with traffic analyzers like wireshark and burp , kismet….
● Experienced in working on Unix systems and developing databases.
● Excellent in troubleshooting skills with an ability to engineer well researched, responsive solutions after analyzing codes.
● Having knowledge of processes and tools to design state of the art software solutions

•applying an adversary mindset to simulate sophisticated actors and achieve project-specific objectives;
•stealthily move laterally, making sure not to trigger any alarms;
•performing research and develop tools my and sharpen my tradecraft
•sharing my research within the Red Team community and with the broader security community, for example writing blogs, speaking at conferences, or publishing code
•turning security weaknesses into tailored and concrete recommendations which you will present to clients
•facilitating Purple Team workshops and training defensive teams of clients in to identify tactics, techniques and procedures (TTPs) used by adversaries
•finding creative ways to obtain a foothold in a client's network
•applying an adversary mindset to simulate sophisticated actors and achieve project-specific objectives
•stealthily move laterally, making sure not to trigger any alarm
•performing research and develop tools my and sharpen my tradecraft
•sharing my research within the Red Team community and with the broader security community, for example writing blogs, speaking at conferences, or publishing code
•turning security weaknesses into tailored and concrete recommendations which you will present to clients
•facilitating Purple Team workshops and training defensive teams of clients in to identify tactics, techniques and procedures (TTPs) used by adversaries.

Skills: Vulnerability Scanning · Vulnerability Management · Vulnerability Research · Vulnerability



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

- Enterprise architect user

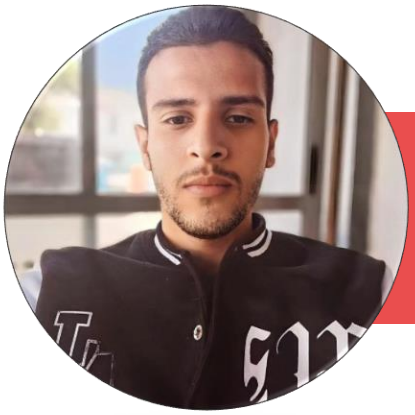
Assessment · Red Teaming · Security Information and Event Management (SIEM)

CYBER SECURITY SPECIALIST • TUNISIE CABLES • INTERNSHIP • FROM NOV 2021 - DEC 2021 · 2 MONTHS

• Secret Management
• determine the scope and align upon the approach of the technical assessment with applicable stakeholders.
• report and align upon the findings, conclusions and propose corrective actions with applicable stakeholders and will coordinate and/or conduct re-assessments after the implementation of the agreed corrective actions.
• support projects by conducting technical assessments upon project deliverables to assure newly introduced hardware and software will not introduce new vulnerabilities, security weaknesses or non-compliance issues.
• finetune pentest process description, used templates and support pentest tooling.
•Rebooting Certification Management
•Firewall policy upgrades

• OTHER SECURITY RELATED MATTERS.NE TWORK AND DEVOPS TECHNICIAN • LABORATOIRES MEDIS • INTERNSHIP • DATES FROM JAN 2020 - APR 2020 · 4 MONTHS

• Secret Management
• determine the scope and align upon the approach of the technical assessment with applicable stakeholders.
• report and align upon the findings, conclusions and propose corrective actions with applicable stakeholders and will coordinate and/or conduct re-assessments after the implementation of the agreed corrective actions.
• support projects by conducting technical assessments upon project deliverables to assure newly introduced hardware and



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

software will not introduce new vulnerabilities, security weaknesses or non-compliance issues.

• finetune pentest process description, used templates and support pentest tooling.

•Rebooting Certification Management

•Firewall policy upgrades

Skills : Red Hat Linux · Windows Server · Cisco Systems Products · Firewalls · IDS · IPS · Security Information and Event Management (SIEM) · NIST · ISO 27001

TUNISIA EDUCATION EXPOSITION • NETWORK AND SYSTEM MANAGER • CONTRACT • FROM FEB 2019 - MAY 2019 · 4 MONTHS

• Maintain essential IT operations, including operating systems, security tools, (cloud) applications, servers, email systems, laptops, computers, software, and hardware.

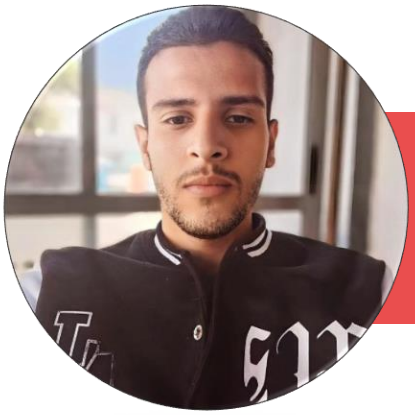
• Install and upgrade computer components and software, manage virtual servers, and integrate automation processes.

• Troubleshoot hardware and software errors by running diagnostics, documenting problems and resolutions, prioritizing problems, and assessing the impact of issues.

• Provide documentation and technical specifications to IT staff for planning and implementing new or upgrades of IT infrastructure.

• Perform or delegate regular backup operations and implement appropriate processes for data protection, disaster recovery, and failover procedures.

• Lead desktop and helpdesk support efforts, making sure all desktop applications, workstations, and related equipment problems are resolved in a timely manner with limited disruptions.



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

• Enable faster and smarter business processes and implement analytics for meaningful insights.

• Maintain essential IT operations, including operating systems, security tools, (cloud) applications, servers, email systems, laptops, computers, software, and hardware.

• Install and upgrade computer components and software, manage virtual servers, and integrate automation processes.

• Troubleshoot hardware and software errors by running diagnostics, documenting problems and resolutions, prioritizing problems, and assessing the impact of issues.

• Provide documentation and technical specifications to IT staff for planning and implementing new or upgrades of IT infrastructure.

• Perform or delegate regular backup operations and implement appropriate processes for data protection, disaster recovery, and failover procedures.

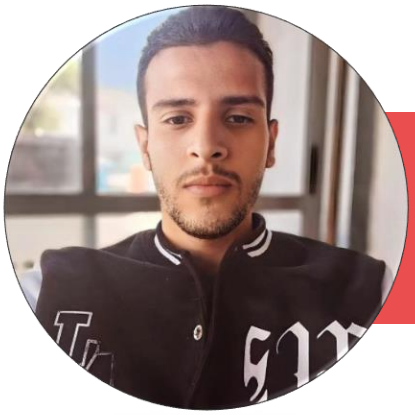
• Lead desktop and helpdesk support efforts, making sure all desktop applications, workstations, and related equipment problems are resolved in a timely manner with limited disruptions.

• Enable faster and smarter business processes and implement analytics for meaningful insights.

Skills: Microsoft SQL Server · Data Centers · Management · Linux · Windows Server

WEB AND MOBILE DEVELOPER • EDUTEST • CONTRACT • FROM 2018/02/10- 2018/09/10 · 7 MONTHS

•Work together with UX/UI'ers and other developers in an agile process to implement new features
•Build and maintain mobile app
•Monitor dev-ops process (CI with Gitlab etc)



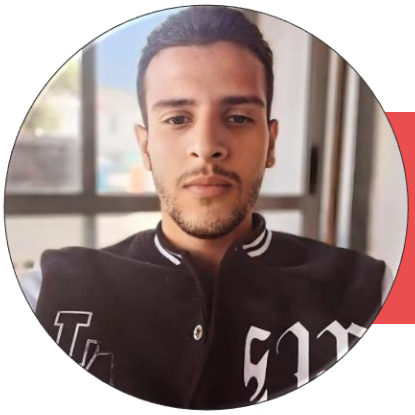
MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

•Work with the app development team to build & improve features for Edutest mobile app (React Native)
•Rapidly develop and ship full features to production,
•Further extend the capabilities of the app by delving into native iOS development
•Make the app experience slick, seamless, and delightful, with sub-second response times
•Lay the foundation for a modular and scalable codebase
•Ensure the app runs smoothly with high-performance

• KEYSTONE GROUP • INTERNSHIP • 2022/02/03 – 2022/05/03

• using, administering, and troubleshooting, including Linux
• Windows environments and with Active Directory concepts
• scripting and editing existing code and programming
• security assessment tools, including Nessus, Accunetix, Metasploit, Burp Suite Pro, Cobalt Strike, or Covenant
• application, database, and Web server design and implementation
• network vulnerability assessments, Web application security testing, network penetration testing, red teaming, security operations, or hunt
• open security testing standards and projects, including OWASP and ATT&CK
• convey results clearly in formal technical reports
• using, administering, and troubleshooting, including Linux
• Windows environments and with Active Directory concepts
• scripting and editing existing code and programming
• security assessment tools, including Nessus, Accunetix, Metasploit, Burp Suite Pro, Cobalt Strike, or Covenant
• application, database, and Web server design and implementation



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

• network vulnerability assessments, Web application security testing, network penetration testing, red teaming, security operations, or hunt
• open security testing standards and projects, including OWASP and ATT&CK
• convey results clearly in formal technical reports

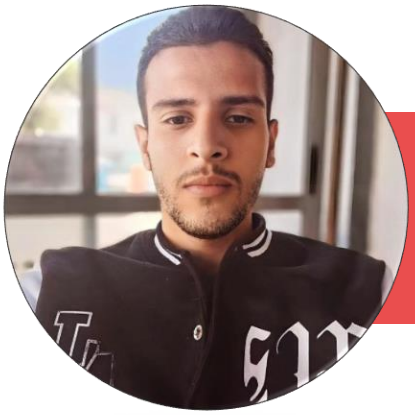
Skills: Vulnerability Assessment · Web Application Security · Penetration Testing · Ethical Hacking · Red Teaming

• ITU • FREELANCE • 2023/02/03 – 2022/07/20

Introducing the Enhanced Spectrum Management System for Developing Countries (SMS4DC 5.2) with the help of Walid Mathlouthi Head Of Infrastructure and UN team (ITU DIV)

The Spectrum Management System for Developing Countries (SMS4DC) has undergone a significant rebranding effort, now known as SMDC4. This enhanced version, SMDC4 5.2, offers a comprehensive suite of functionalities tailored to the spectrum management needs of developing nations. Building upon the legacy of SMS4DC, SMDC4 5.2 incorporates valuable contributions from MSIP (Ministry of Science and ICT), Republic of Korea.

A key highlight of SMDC4 5.2 is its alignment with the revised Article 5 of the Radio Regulations, as per the decisions made at the 2019 World Radiocommunication Conference (WRC-19). This alignment ensures that SMDC4 5.2 adheres to the latest international standards and guidelines for spectrum management.



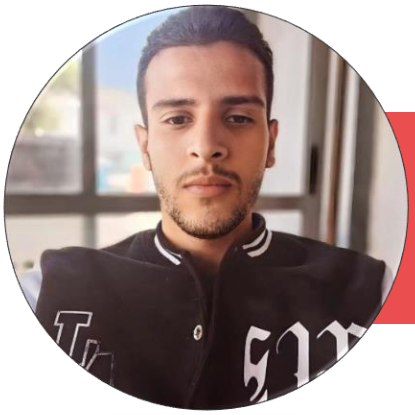
MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

SMDC4 5.2 empowers developing countries to effectively manage their radio frequency spectrum, a crucial resource for ensuring efficient communication and technological advancement. The system's functionalities span a wide range of spectrum management tasks, including:

- **Frequency allocation and assignment:** SMDC4 5.2 facilitates the optimal allocation and assignment of radio frequencies to various users, ensuring efficient utilization of this finite resource.
- **Spectrum monitoring and enforcement:** The system enables real-time monitoring of spectrum usage and enforcement of spectrum regulations, preventing unauthorized or harmful interference.
- **Spectrum planning and forecasting:** SMDC4 5.2 provides tools for long-term spectrum planning and forecasting, ensuring that spectrum availability meets future communication needs.
- **Spectrum data management:** The system maintains a comprehensive database of spectrum-related data, enabling informed decision-making and policy formulation.

SMDC4 5.2 represents a significant step forward in supporting developing countries' efforts to manage their spectrum resources effectively and sustainably. The system's user-friendly interface, adaptability to diverse national contexts, and alignment with international standards make it a valuable tool for enhancing communication infrastructure and fostering technological progress in the developing world.



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

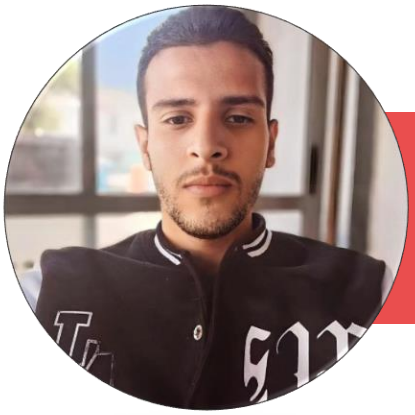
• TRIGAN • CONTRACTOR • 2023/09/19 – 2023/01/25

Enhancing Cybersecurity for Trigan's Urban Blockchain Project

As a cybersecurity specialist at Trigan, I played a pivotal role in safeguarding the integrity and security of its groundbreaking urban blockchain project. My primary responsibilities encompassed the rigorous analysis and testing of smart contracts and Web3.0 applications, ensuring their seamless integration within Trigan's comprehensive Web2 infrastructure.

Trigan's urban blockchain project stands as a decentralized powerhouse, revolutionizing the urban experience through the transformative potential of next-generation technology. Its unique platform and cutting-edge approach empower cities to embrace a future marked by enhanced intelligence, safety, and connectivity, fundamentally transforming governance, services, and transactions.

My contributions to this transformative project involved meticulously reviewing and testing smart contracts, the self-executing contracts that form the bedrock of blockchain technology. These contracts serve as the backbone of decentralized applications, ensuring secure and transparent transactions within the Trigan ecosystem. My expertise in smart contract security ensured that these contracts adhered to the highest standards of security and remained free from vulnerabilities.



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

In addition to smart contract analysis, I actively participated in the testing and evaluation of Trigan's Web3.0 applications. Web3.0, the next iteration of the internet, is built on decentralized principles, empowering users with greater control over their data and online experiences. My involvement in Web3.0 testing ensured that these applications were secure, functional, and aligned with Trigan's overall vision of a decentralized urban future.

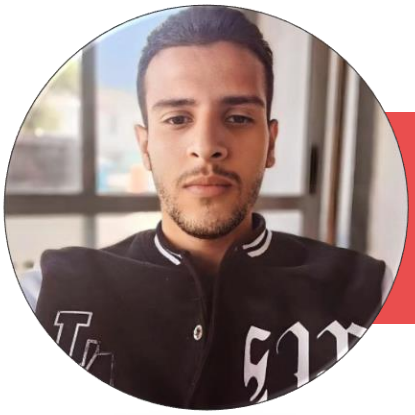
Throughout my engagement, I extensively utilized a range of tools and technologies, including Hardhat, Solidity, Golang, and IPFS. These tools played a crucial role in my ability to effectively analyze, test, and secure Trigan's smart contracts and Web3.0 applications.

Trigan's urban blockchain project represents a paradigm shift in urban governance and service delivery. By leveraging the transformative power of blockchain technology, Trigan is paving the way for smarter, safer, and more connected cities, where citizens can engage with their communities in a more secure, transparent, and empowering manner. My contributions to this project have been deeply rewarding, as I have played a part in shaping the future of urban life through the power of technology.

Currently

Collaborating with the Tunisian Navy on several promising projects:

The Tunisian Navy has embarked on a series of technological advancements to enhance its maritime security capabilities. One of the key areas of focus is collaboration with international



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

partners to acquire and implement cutting-edge technologies. In this regard, the Navy is working closely with several entities, including:

1. Albatros-class fast attack craft modernization:

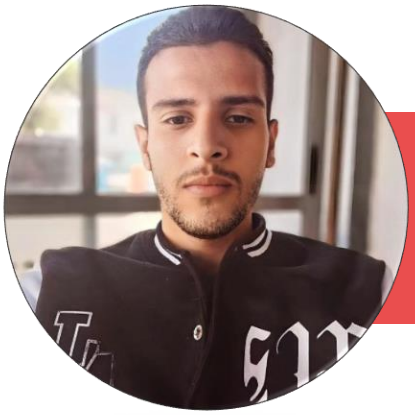
The Albatros-class fast attack craft is a versatile and effective vessel that serves as a backbone of the Tunisian Navy's coastal defense operations. To further enhance the capabilities of these vessels, the Navy is exploring modernization options that could include upgrades to their propulsion systems, electronic warfare suites, Bug fixes, potential offensive capabilities, and sensor packages.

2. GPS Spoofer for submarines:

Submarine warfare relies heavily on precise positioning and navigation capabilities. To gain an edge in this domain, the Tunisian Navy is investigating the development of GPS spoofing technology. This technology would allow the Navy to disrupt enemy submarines' GPS signals, potentially hindering their ability to navigate and engage targets effectively.

3. IMSI Catcher:

In the realm of maritime surveillance, the ability to track and monitor vessels is crucial. The Tunisian Navy is exploring the implementation of IMSI catchers, which are devices that can capture the International Mobile Subscriber Identity (IMSI) numbers of mobile phones in their vicinity. This technology can be used to track the movements of individuals associated with



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

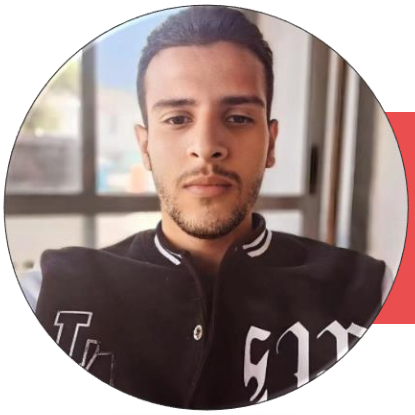
vessels of interest, providing valuable intelligence for maritime security operations.

These projects represent a significant step forward in the Tunisian Navy's efforts to modernize its capabilities and maintain a strong presence in the Mediterranean region. By collaborating with international partners and acquiring advanced technologies, the Navy is safeguarding its national interests and contributing to regional maritime security.

WARTIME WATER WORM the new definition of WWW :

I intend to conduct a thorough analysis of the ship's firmware, encompassing an in-depth examination of its Application Programming Interfaces (APIs) and internal architecture. This analysis will be facilitated through advanced techniques such as reverse engineering and decompilation, coupled with sophisticated fuzzing methodologies, including both conventional fuzzing and intelligent fuzzing strategies. The primary objective is to gain a comprehensive understanding of the system's internal workings, particularly delving into the intricacies of Ring 0, which pertains to the most privileged level of execution in the firmware, and the underlying hardware architecture.

The comprehensive analysis aims to uncover latent and nuanced vulnerabilities within the firmware. Reverse engineering will involve meticulous dissection of the firmware's codebase, while decompilation will assist in translating low-level machine code into more comprehensible higher-level languages. Fuzzing, a systematic testing approach, will be employed to evaluate the resilience of the firmware against unforeseen inputs. Intelligent fuzzing techniques, leveraging insights into the system's design and functionalities, will



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

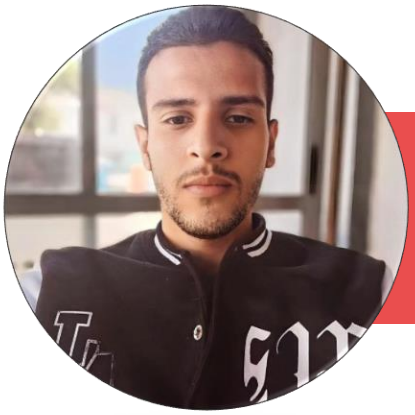
guide the generation of test cases to maximize the efficacy of the analysis.

This initiative is collaborative in nature, involving close cooperation with the Navy technical team. The collective expertise of the team will be harnessed to facilitate a holistic understanding of the firmware's operation, particularly in the context of its interaction with the underlying hardware. A meticulous exploration of Ring 0, the privileged domain of the firmware, will be paramount in uncovering potential vulnerabilities that may pose security risks.

The hardware architecture analysis will extend beyond a surface-level examination, delving into the intricate details of the ship's hardware components. This comprehensive approach seeks to identify potential weak points and susceptibilities in the system's design, contributing to a robust evaluation of its overall security posture.

Findings resulting from this analysis will be meticulously documented, encompassing identified vulnerabilities, potential exploitation scenarios, and recommendations for mitigation. A collaborative effort with the Navy technical team will then ensue to devise and implement effective strategies to address and remediate the identified vulnerabilities. Consideration will be given to the potential impact of proposed mitigations on the system's functionality, ensuring a balanced and informed approach to security enhancement.

Furthermore, this initiative emphasizes the importance of continuous monitoring and vigilance. A dynamic framework for ongoing assessment and adaptation to emerging threats will be established to fortify the ship's firmware against evolving security challenges.



MOHAMED AMIINE GUESMI

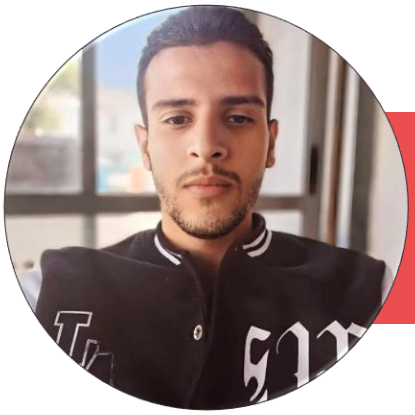
CYBER SECURITY REASERCHER
01/09/1999 NABEUL

In adherence to ethical and legal standards, a responsible disclosure approach will be followed when reporting any discovered vulnerabilities to relevant authorities or vendors. The overarching goal is to elevate the security posture of the ship's firmware comprehensively, safeguarding against potential exploits and ensuring the integrity of its operational capabilities. This endeavor also underscores the importance of fostering awareness and imparting security best practices within the Navy technical team, contributing to a culture of continuous improvement and proactive security measures.

Employing a network of smart contracts to identify and exploit low-hanging opportunities in the realm of blockchain technology

The phrase "doing a hive of smart contracts to hunt for low hanging fruits with slither and gasusage and parsers of that kind" conveys the idea of utilizing a collection of smart contracts to automate the process of identifying and capitalizing on readily available opportunities in the blockchain ecosystem. These opportunities, often referred to as "low-hanging fruits," can range from arbitrage opportunities to undiscovered tokens with promising potential.

The term "slither" likely refers to a tool or technique used to analyze the Ethereum blockchain and identify potential smart contract vulnerabilities or exploits. "Gasusage" refers to the concept of measuring transaction fees on the Ethereum network, which can be a crucial factor in determining the profitability of certain blockchain-based activities.



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

The phrase "parsers of that kind" suggests the utilization of tools or scripts that can interpret and extract meaningful information from blockchain data, allowing for a deeper understanding of the network and its underlying mechanics.

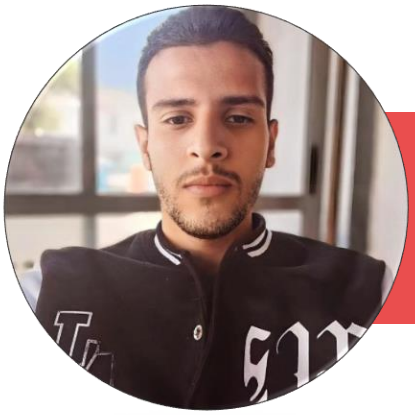
Overall, the rewritten text highlights the concept of leveraging smart contracts and specialized tools to automate the identification and exploitation of low-hanging opportunities in the blockchain space. This approach can potentially generate profits or other benefits for those who employ it effectively.
Gathering, Analyzing, and Counteracting Malware Threats

collecting malware mass decompiling mass reversing writing poc osint sharing c&c" encompasses a comprehensive approach to addressing malware threats. It involves gathering and analyzing malware samples, reverse engineering their code to understand their functionality, developing proof-of-concept (PoC) exploits or mitigation techniques, utilizing open-source intelligence (OSINT) to track malware campaigns and threat actors, and sharing information about command-and-control (C&C) servers with the security community.

1. Malware Collection:

The first step in this process is to gather a wide range of malware samples. This can be done through various means, such as honeypots, network capture analysis, or collaboration with other security researchers.

2. Mass Decompilation and Analysis:



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

Once a collection of malware samples has been assembled, the next step is to decompile and analyze them. Decompilation involves converting the malware from its machine-readable code into a more human-readable form, such as assembly language or C/C++. This allows analysts to understand the malware's functionality, identify its vulnerabilities, and develop mitigation strategies.

3. Proof-of-Concept (PoC) Development:

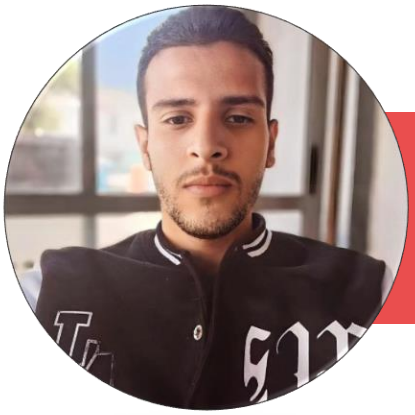
In some cases, it may be necessary to develop PoC exploits or mitigation techniques for specific malware samples. These PoCs can be used to demonstrate the malware's capabilities, test potential countermeasures, or develop tools to detect and remove the malware.

4. Open-Source Intelligence (OSINT) Gathering:

OSINT can be a valuable resource for tracking malware campaigns and identifying threat actors. By monitoring online forums, social media, and other public sources, security researchers can gather insights into the development, distribution, and targeting of malware.

5. Command-and-Control (C&C) Server Identification:

C&C servers are the central control hubs for many malware campaigns. By identifying and disrupting these servers, security researchers can effectively cripple malware operations. Sharing information about C&C servers with the security community can help to amplify this effect.



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

Engaging in Capture the Flag (CTF) Challenges on VulnHub and Root-Me

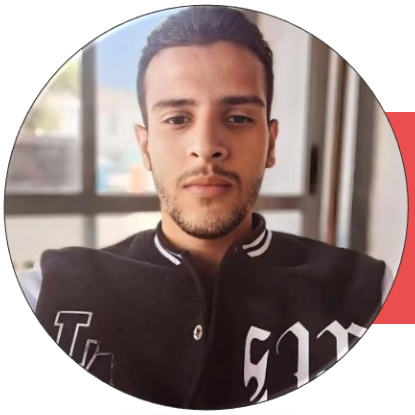
1. VulnHub:

VulnHub is a free and open-source platform that provides a collection of vulnerable virtual machines (VMs) for practicing penetration testing and hacking skills. The platform offers a diverse range of challenges, ranging from beginner-level to expert-level, catering to individuals with varying levels of experience in cybersecurity. VulnHub challenges often involve identifying and exploiting vulnerabilities in the provided VMs, gaining access to sensitive information, or achieving specific objectives within the virtual environment.

2. Root-Me:

Root-Me is another popular online platform that provides a variety of CTF challenges and training resources for cybersecurity enthusiasts. The platform offers a gamified approach to learning cybersecurity, allowing users to progress through different levels of challenges as they gain experience. Root-Me challenges cover a broad spectrum of cybersecurity topics, including web application security, cryptography, network security, and more.

Engaging in CTF challenges on platforms like VulnHub and Root-Me provides a valuable hands-on learning experience for aspiring cybersecurity professionals and enthusiasts. These challenges allow individuals to apply theoretical concepts in a



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

practical setting, enhancing their problem-solving skills, and gaining real-world experience in identifying and exploiting vulnerabilities. Additionally, CTFs provide a competitive environment for individuals to test their skills against others, fostering a sense of community and encouraging continuous learning and improvement.

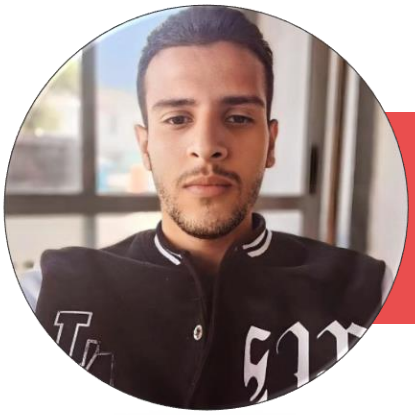
Downloaded 200GB of drivers in order to apply Reverse engineering,fuzzing AI techniques with massive decompilation and automation of codeql templates writing with IOCTL codes fuzzing in order to write OBB read and writes exploits along with common CWE threats similar to BOF and HEAP OVERFLOW
Which highlights a comprehensive approach to conducting security research and uncovering vulnerabilities in software drivers.

1. Data Preparation: Downloading a Large Volume of Drivers

The acquisition of a vast collection of drivers, amounting to 200GB, serves as the foundation for this research endeavor. This extensive dataset provides a rich source of material for subsequent analysis and vulnerability discovery.

2. Reverse Engineering and Massive Decompilation:

Reverse engineering involves examining the code of software drivers to understand their internal workings and identify potential vulnerabilities. Massive decompilation refers to the process of automatically converting the machine-readable code of multiple



drivers into a more human-readable form, enabling researchers to analyze the code on a larger scale.

3. Fuzzing:

Fuzzing is a technique for testing software by bombarding it with unexpected or invalid inputs to uncover potential crashes or vulnerabilities. In the context of driver security research, fuzzing can be used to identify vulnerabilities that could lead to system compromise or privilege escalation.

4. AI-Powered Analysis and CodeQL Automation:

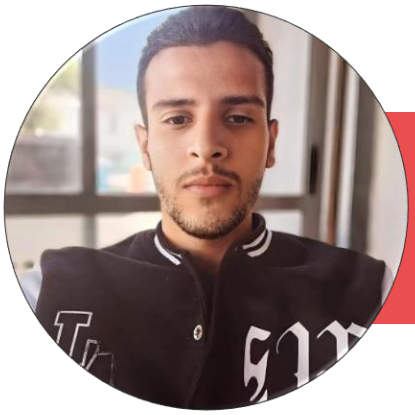
The incorporation of artificial intelligence (AI) techniques and CodeQL, a query language for identifying security vulnerabilities in code, enhances the research process. AI algorithms can assist in identifying patterns and anomalies in driver code, while CodeQL templates can streamline the automation of vulnerability detection.

5. Utilizing IOCTL Codes for Exploitation:

IOCTL (Input/Output Control Language) codes are used to communicate with device drivers, providing a means for controlling their behavior. By understanding and utilizing IOCTL codes, researchers can develop exploits that target specific vulnerabilities in drivers.

6. Exploring OBB Read and Write Exploits:

OBB (Opaque Binary Blobs) are commonly used in Android applications to store data securely. Exploiting vulnerabilities in OBB handling mechanisms can allow attackers to read or write sensitive

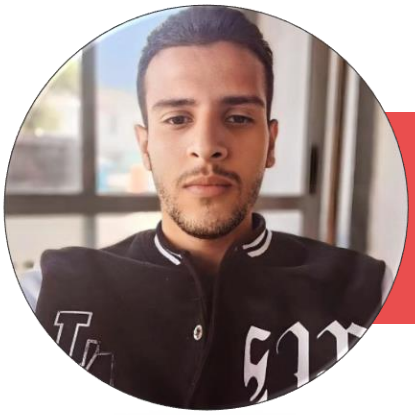


data from or to these files, potentially compromising the security of the application and the device.

7. Addressing Common CWE Threats:

CWE (Common Weakness Enumeration) is a list of standardized cybersecurity weaknesses. BOF (Buffer Overflow) and HEAP OVERFLOW are two examples of common CWE threats that can be found in software drivers. Researchers aim to identify and address these vulnerabilities to enhance the security posture of the system.

In summary, this approach to security research combines traditional techniques like reverse engineering and fuzzing with advanced AI-powered analysis and automation to uncover vulnerabilities in software drivers. By focusing on common CWE threats and exploiting techniques like IOCTL codes and OBB read and write exploits, researchers can contribute to improving the overall security of software systems.



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

EDUCATION

BACCALAUREAT MATHEMATIQUES • 2018 • LPNK
ADVANCED PROGRAMMING WITH JAVA • 2019 • ARYSSE FORMATION
TECHNICIEN PROFESSIONNEL EN MAINTENANCE MICRO SYSTEME INFORMATIQUE
CENTRE SECTORIEL DE FORMATION MAINTENANCE NABEUL 2022

ALSO DONE, WORKED WITH

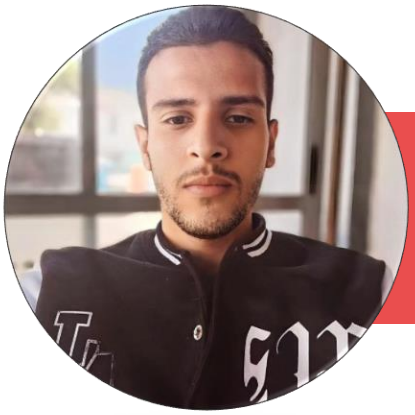
Being a bad guy and Offensive Gadget developer 2013-2016:

- Grabbing Config With [LFI]
- WordPress mass Password Change [Client Side]
- Simple Crawler Using Perl
- [PHP] WordPress mass Password Change [Server Side]
- Bash Mass Defacement
- CMS Exploitation framework for Vbulletin, joomla WordPress [python]
- Also developed tons and tons of malwares remote access tools exploits worms key loggers participated in a lot of phishing campaigns hacked a lot of networks websites and more

Being a Good guy and Offensive Gadget developer 2016-2022:

- **Xss exploit that affects all of kat.ph torrent mirrors**
- nmap and wireshark plugins development using LUA

Mainly the resulted plugins are either scanners or exploiters for newly discovered vulnerabilities or RFC definitions or even tasks automatisation



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

●Collecting active malicious softwares source codes and putting them on my GitHub account Malware researchers continually inquire about up-to-date malware samples to analyze **in order to learn, train or develop new threat techniques and defenses**

● Gns3 Privilege escalation bug discovery

GNS3 is used by hundreds of thousands of network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows you to run a small topology consisting of only a few devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud.

VM kernel which is vulnerable to dirty cow privilege escalation exploit A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. tested on the latest version : 2.1.2 VMware edition

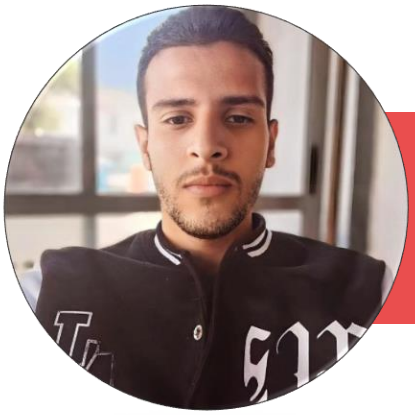
● Zipslip proof of concept

Zip Slip is a widespread critical archive extraction vulnerability, allowing attackers to write arbitrary files on the system, typically resulting in remote command execution. It was discovered and responsibly disclosed by the Snyk Security team ahead of a public disclosure on 5th June 2018, and affects thousands of projects, including ones from HP, Amazon, Apache, Pivotal and many more.

The vulnerability has been found in multiple ecosystems, including JavaScript, Ruby, .NET and Go, but is especially prevalent in Java, where there is no central library offering high level processing of archive (e.g. `zip`) files. The lack of such a library led to vulnerable code snippets being hand-crafted and shared among developer communities such as StackOverflow.

● Reddit like forum with Flask

● Pi network HTTPS traffic analysis burpsuite

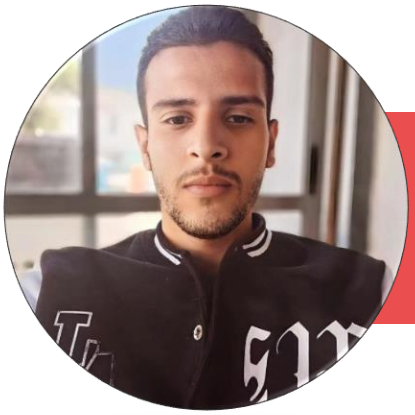


MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

Description. Pi is a new digital currency. This app allows you to access and grow your Pi holdings and serves as wallet to host your digital assets. Pi is fairly distributed, eco-friendly and consumes minimal battery power.

- Harvesting IOCs from Agent Tesla and Emotet
- On demand advanced Fuzzers using scapy and pypwn
- Deploying zabbix as monitoring framework in scada field
- Network Segmentation
- Some working on the AWS,Microsoft Azure and google Cloud
- Cloud,Godaddy
- X86 shellcode development
- Unsupervised Learning Sequence Embedding's via Sequential Patterns done by me as someone else's masters degree graduation project in data science
- An altered AI based Network intrusion detection system for benchmarking reasons done by me as someone else's masters degree graduation project in data science/cybersecurity
- Turing NGFW network gateway firewall this is mainly designed for iot and ICS environments It decrypts the traffic and analyses it with altered kitsune-NIDS and provides sandboxing integrated honeynet that can prohibit network attacks and network exfiltration and integrating signature based identification using security-onion integrated packages mainly project was proposed for Medis Laboratories
- exploitpack extracted from a honey net which is being prepared by intruders linked to Iran and thought to be used as an exploitation infrastructure immunity exploitpack is found in my honey net threat actors using the honeypot to install the exploit kit to aim it to German and Dutch targets target list kept private and networks owners has been notified
- Doing development ,security testing and network/system administration at fiverr and upwork



MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

● Found some security loopholes in Meta products (Instagram,whatsapp,facebook)

●Immersed in the World of Cybersecurity: A Comprehensive Guide to Conferences, Podcasts, YouTube Playlists, and Books

Cybersecurity is a rapidly evolving field, and staying up-to-date with the latest trends and threats is essential for anyone working in the industry. Attending cybersecurity conferences, listening to cybersecurity podcasts, watching cybersecurity YouTube playlists, and reading cybersecurity books are all great ways to learn about new developments and stay ahead of the curve