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

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

- Enterprise architect user

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

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

• 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.

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

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

• 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)
•Work with the app development team to build & improve features for Edutest mobile app (React Native)

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

•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
• network vulnerability assessments, Web application security testing, network penetration testing, red teaming, security operations, or hunt

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

• 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

Currently

-bug bounty
-software development on fiver
-collecting malware
-performing reverse engineering
-Threat hunting and osint
-write info-sec articles
-Playing CTFS

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]

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

- 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

- 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

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

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

  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

MOHAMED AMIINE GUESMI

CYBER SECURITY REASERCHER
01/09/1999 NABEUL

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

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