Juan Urbano Stordeur

Contact information

Email	ju@juanurs.com
Mobile Phone	+5491153237638
Site	juanurs.com

About me

I consider myself an energetic, enthusiastic person to learn, adaptable to changes, who always seeks to apply the knowledge acquired. Open to the new challenges, being these elementals for personal growth, where I always try to solve them in the most efficient and effective way possible.

Work experience

Nov 2018 – Present	**Mobile & web penetration tester**, *AFIP*, Argentina, Buenos Aires.
Feb 2016 – Oct 2018	**Networking, web & mobile penetration tester**, *ESET*, Argentina, Buenos Aires.
Feb 2016– Present	**Freelance Mobile & web penetration tester**, *ESET*, Argentina, Buenos Aires.
Jul 2013 – Ene 2016	**Penetration tester**, *Infobyte LLC*, Argentina, Buenos Aires.
Dec 2011 - Jul 2013	**(Freelance) Penetration tester**, *Infobyte LLC*, Argentina, Buenos Aires.

Studies

University	**Systems Engineering**, National Technology University (UTN), 2009 - present, currently in last years.

Personal goals 2019

- Deepen the knowledge on mobile devices in their different technologies (Android & iOS).
- Realize one of the fallowing certifications before Q4:
  - ☐ GIAC Mobile Device Security Analyst (GMOB)
  - ☐ eLearnSecurity Mobile Application Penetration Tester
- Assist to the “Advanced Frida and Radare training” next BH USA 2019, *currently registered*.
- Present at least a mobile research in a security conference.

Penetration tester knowledge

* **Experience with black, gray and white box pentesting methodologies**.
* **Analysis and risk assessment**.
* **Information gathering**.

* **Vulnerability analysis**.
  Mobile Application Security: ***Identification and exploitation of OWASP's based on the top 10 mobile vulnerabilities, OWASP mobile security testing guide*** **and MASVS**.
  - ❖ *Android skills and experience*:
    - Analyzing the internal storage (Shared Prefs and SQLIte) and external storage too.
    - De-compiling the application to .java to understand the code.
    - APK Reversing engineering and patching (Analyzing smali code and re-build the app).
    - Attacking network flags (client side): MITM through CA in the device, bypassing certificate pinning validation, hostname verifier implementation, etc.
    - Attacking network flags (server side): SQL Injection, XSS, XXE, etc.
    - Attacking components and IPC.
    - Looking for hardcoded issues like usernames, passwords, private and public IP's, etc.
    - Analyzing malware applications (passive and dynamic analysis).
    - Experience using JEB, Cuckoo, Frida, and bypassing protections.
  - ❖ *iOS skills and experience:*
    - Knowledge iOS Filesystem and Objective-C runtime.
    - Runtime analysis and manipulation.
    - Insecure Data Storage (Plist, NSUserDefaults, CoreData and Keychain).
    - Analyzing network traffic over HTTP/HTTPs and Certificate Pinning.
    - Analyzing cryptography implementations.
    - Experience bypassing anti-reversing engineering protections.
    - Dynamic Instrumentation using Frida/Xposed/Cycript/Objection, etc.

  Web Applicaton Security: Identification and exploitation of SQL/XML/HTML injections, XSS/CSRF, RCEs and more.

  Networking: External and internal network analysis;
* **Exploitation and post-exploitation**.
* **General knowledge related to cryptography**.
* **Integration of different applications and tools automated to develop tasks**.
* **Strong experience in the creation and generation of reports**.

Technical skills

Programming languages

Scripting	BASH, Python
POO	Python

Technologies

OS	Linux (ArchLinux and Debian based distros), Windows XP, Windows 7
SQL	SQLite, PostgresSQL, MySQL.

Knowledge of

Penetration Testing	Red Team penetration testing methodology

Active project

l0ckpickAR	Founder along with Juan Ignacio Bousquet. Space destined to investigation and deepening of physical security related subjects.
Ekoparty	Hacker Space contributor since 2015

Events

Conferences

Attendee	Assistant Blackhat & DEFCON 26, USA, 2018.
Attendant	Android / iOS "Offensive Mobile Application Exploitation". Blackhat USA, 2017.
Attendee	Assistant Blackhat & DEFCON 25, USA, 2017
Speaker	"Analysis of mobile applications", OWASP Latam Tour (Patagonia, Córdoba and Buenos Aires) 2017
Speaker	"Análisis de aplicaciones móviles", APPSEC Río de la Plata - december 2016.
Exponent	Physical security stand at Ekoparty security conference. 2012 - 2017.
Attendee	Ekoparty international security conference, 6th to 13th edition.
Attendee	Defcon 22, Las Vegas, USA 2014.
Speaker	Physical security. OWASP Day, Fing Uruguay 2013.
	Argentina and Uruguay chapters.

Dictated workshops

ekoparty	Android App Analysis at Ekoparty security conference 2017
ekoparty	Physical security since 2012.
ESET	Trainings, webinars and virtual classrooms, 2016.
OWASP Day	Physical security 2013, Uruguay. Physical
Risecon	security 2014, Rosario.
ESET	"Análisis de un ataque APT", corporate breakfasts 2016, Argentina y Chile.

Trainings at ekoparty security conference

Trainee	*Hacking on the Fly & Unarmed Rootkits* 2015
Trainee	*"Digital Forensics for Security Professionals 3.0"* 2014
Trainee	*"Client Side Attacks for Penetration Testers"* 2013

Personal research

2018	**Bypassing Android Anti-Emulation**, https://bit.ly/2lphJC3
2015	**Vulnerability static analyzer for Android Apps (python).**
2014	**Embedded devices, Infobyte security research,** *http://j.mp/1uFZ4Sq*
2012- present	**Biometrical devices and fingerprint cloning.**

Languages

Spanish	**Native speaker**
English	**Intermediate** (currently studying, and daily use in the workplace).