

Para cada caso:

- mini estudio
- instalar y probar
- 1 ejemplo de la prueba

Entrega:

- Markdown en git.
- PPT sin texto.
- Exposición sin leer.

SE HACE “HASTA AQUÍ”

❖ PHISHING TOOLKIT ❖

🔍 CABECERAS 🔎

- 1Message Header Analyzer: <https://lnkd.in/d2kSS15y>
- 2Mx ToolBox: <https://lnkd.in/dtr7v9SE>
- 3WhatIsMyIP: <https://lnkd.in/dwgYTwtY>
- 4Messageheader (Google): <https://lnkd.in/dF-G8yGA>
- 5Email Header Analyzer (DNS Checker): <https://lnkd.in/dtr7v9SE>

💡 IP 💡

- 6Whois Lookup: <https://lnkd.in/dnZppsWM>
- 7Abuseipdb: <https://www.abuseipdb.com/>
- 8Ipinfo: <https://ipinfo.io/>
- 9Ipvvoid: <https://www.ipvvoid.com/>
- 10IPQualityScore: <https://lnkd.in/dEzkTcV5>

💻 LINKS 💻

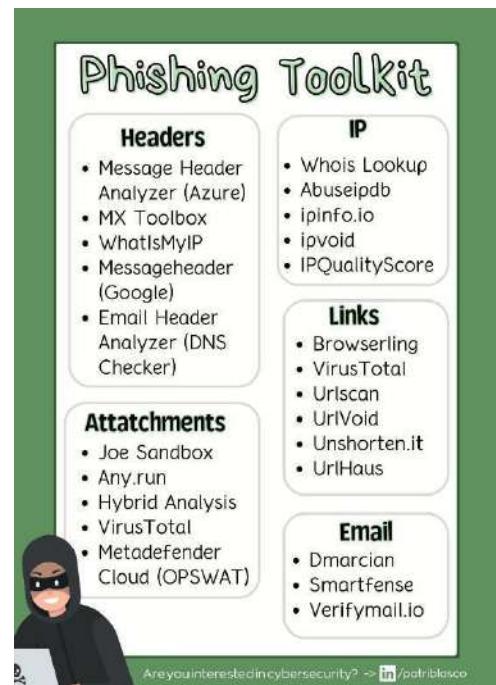
- 4Browserling: <https://lnkd.in/dgwmjMtx>
- 5VirusTotal: <https://lnkd.in/dKgBNU6n>
- 6Urlscan: <https://urlscan.io/>
- 7Urlvoid: <https://www.urlvoid.com/>
- 8Unshorten.it: <https://unshorten.it/>
- 9Urlhaus: <https://lnkd.in/dmTA9qEH>

📁 ADJUNTOS 📁

- 3Joe Sandbox: <https://lnkd.in/d77O2GMb>
- 4Any.run: <https://any.run/>
- 5Hybrid Analysis: <https://lnkd.in/d4JPnUrl>
- 6VirusTotal: <https://lnkd.in/d7XMSyPK>
- 7Metadefender Cloud: https://lnkd.in/dZwsDr_c

📩 EMAIL 📩

- 1Dmarcian: <https://lnkd.in/dYeVY4CD>
- 2Smartfense: <https://lnkd.in/d5DF4BYc>
- 3Hybrid Analysis: <https://lnkd.in/d4JPnUrl>
- 4Verify Email: <https://verifymail.io/>



OSINT

-LINKS DE LAS HERRAMIENTAS-

🔒 CONTRASEÑAS 🔒

- 5HaveIBeenPwned: <https://lnkd.in/dtYksdmm>
- 6Dehashed: <https://www.dehashed.com/>
- 7pwnedOrNot: <https://lnkd.in/dHFXrdqx>
- 1LeakCheck: <https://leakcheck.net/>
- 2Snusbase: <https://snusbase.com/>

🧠 INGENIERÍA SOCIAL 🧠

- 3Urlcrazy: <https://lnkd.in/deg7m-FY>
- 4Breach-parse: <https://lnkd.in/duYp5hyF>
- 5Wifiphisher: <https://lnkd.in/dbxxHieq>
- 6Social Engineering Toolkit: <https://lnkd.in/dVKDCiVs>
- 7Maltego: <https://www.maltego.com/>

✉️ E-MAILS ✉️

- 1Epieos: <https://epieos.com/>
- 2Hunter: <https://hunter.io/>
- 3Norbert: <https://lnkd.in/dkAG9Eyp>
- 4Email Checker: <https://email-checker.net/>
- 5Simple Email Reputation: <https://emailrep.io/>
- 6Phonebook: <https://phonebook.cz/>
- 7iKy: <https://lnkd.in/dTmM-ghV>
- 8h8mail: <https://lnkd.in/d3439Ws3>

👤 REDES SOCIALES 🤷

- 2OSINTgram: https://lnkd.in/dKk_nYPZ
- 3SocialPwned: <https://lnkd.in/dF2un2cu>
- 4Social Bearing: <https://socialbearing.com/>
- 5BlackBird: <https://lnkd.in/dWJKVZff>
- 6Namechk: <https://namechk.com/>
- 7TweetDeck: <https://lnkd.in/d9SGXvIT>
- 8Tinfoleak: <https://tinfoleak.com/>
- 9Tweetbeaver: <https://tweetbeaver.com/>

🔍 BUSCADORES 🔎

- 3DuckDuckGo: <https://duckduckgo.com/>
- 4Baidu: <https://www.baidu.com/>
- 5Yandex: <https://yandex.com/>
- 6Tineye: <https://tineye.com/>
- 7Shodan: <https://www.shodan.io/>
- 8Spokeo: <https://www.spokeo.com/>
- 9Zoomeye: <https://www.zoomeye.org/>
- 10Google Search Guide: https://lnkd.in/dy4WR_Mj

The dashboard is organized into six sections:

- CONTRASEÑAS**: Includes HaveIBeenPwned, Dehashed, pwnedOrNot, LeakCheck, and Snusbase.
- E-MAILS**: Includes Epieos, Hunter.io, Norbert, Email Checker, Simple Email Reputation, Phonebook.cz, iKy, and h8mail.
- BUSCADORES**: Includes DuckDuckGo, Baidu, Yandex, Tineye, Shodan, Spokeo, Zoomeye, and Google Search Guide.
- INGENIERÍA SOCIAL**: Includes Urlcrazy, breach-parse, Wifiphisher, Social Engineering Toolkit, and Maltego.
- REDES SOCIALES**: Includes OSINTgram, SocialPwned, Social Bearing, BlackBird, Namechk, TweetDeck, Tinfoleak, and Tweetbeaver.
- PÁGINAS WEBs**: Includes Wayback Machine, ViewDNS, SpyOnWeb, BuiltWith, DNSlytics, Visual Ping, and Back Link Watch.

At the bottom right, there is a link: "¿Te interesa la ciberseguridad? → [/patriblasco](#)".

4google-hacking-database : <https://www.exploit-db.com/google-hacking-database>

💻 PÁGINAS WEBS 🖼

- 5Wayback Machine: <https://archive.org/web/>
- 6ViewDNS: <https://viewdns.info/>
- 7SpyOnWeb: <https://spyonweb.com/>

HASTA AQUÍ

- 1BuiltWith: <https://builtwith.com/>
- 2DNSlytics: <https://dnslytics.com/>
- 3VisualPing: <https://visualping.io/>
- 4BackLinkWatch: <https://lnkd.in/d4u-cnUW>



RED TEAM

-LINKS-

Laboratorios:

5<https://tryhackme.com/>

6<https://www.hackthebox.com/>

☒ PRIVILEGE SCALATION ☒

- 7BloodHound: <https://lnkd.in/ddxtanZV>
- 1BeRoot: <https://lnkd.in/drybarmR>

🎭 PHISHING 🎭

- 2Gophish: <https://getgophish.com>
- 3King Phisher: <https://lnkd.in/dtpMD8XZ>
- 4EvilURL: <https://lnkd.in/du82nxhD>

🕹 COMMAND AND CONTROL 🕹

- 5Empire Project: <https://lnkd.in/dafJ6WAF>
- 6Pupy: <https://lnkd.in/dQqHe8wy>
- 7Cobalt Strike: <https://lnkd.in/dw9hOtWO>

🔍 OSINT 🔎

- 1Maltego: <https://www.maltego.com>
- 2Spiderfoot: <https://www.spiderfoot.net>
- 3OSINT Framework: <https://osintframework.com>

🌐 RECONNAISSANCE 🌐

- 4Nmap: <https://nmap.org>
- 5sqlmap: <https://sqlmap.org>
- 6OpenVAS: <https://www.openvas.org>
- 7Nikto: <https://lnkd.in/dZz5gzZT>
- 1Shodan: <https://www.shodan.io>
- 2Crt.sh: <https://crt.sh>
- 3RustScan: <https://lnkd.in/dOrhe8-X>
- 4Amass: <https://lnkd.in/dMU27YXS>

🔗 EXFILTRATION 🔗

- 5SharpExfiltrate: <https://lnkd.in/d8z-6HK5>
- 6DNSExfiltrator: <https://lnkd.in/dmX76kqC>
- 7Egress-Assess: <https://lnkd.in/dKljhmhY>



🔒 CREDENTIAL DUMPING 🔒

- 1Mimikatz: <https://lnkd.in/dPcBT5Fk>
- 2Dumpert: <https://lnkd.in/dH66Flj4>
- 3Lazagne: https://lnkd.in/di8zz_47
- 4forkatz: <https://lnkd.in/de-jtbjY>
- 5Pypykatz: <https://lnkd.in/dkKequy6>
- 6nanodump: <https://lnkd.in/dCHhtH3x>

BLUE TEAMS

-LINKS-

🌐 NETWORK ANALYSIS 🌐

- 7Wireshark: <https://www.wireshark.org>
- 1pfSense: <https://www.pfsense.org>
- 2Arkime: <https://arkime.com>
- 3Snort: <https://www.snort.org>

💻 OS ANALYSIS 💻

- 4Helk: <https://lnkd.in/di4rOuNb>
- 5Volatility: <https://lnkd.in/dBr4yVYa>
- 6RegRipper: <https://lnkd.in/dq2hTNOw>
- 7OSSEC: <https://www.ossec.net>
- 1osquery: <https://osquery.io>

🛡 INCIDENT MANAGEMENT 🛡

- 2TheHive: <https://lnkd.in/dkR-d4Jb>
- 3GRR Rapid Response: <https://lnkd.in/d42-6faP>

🎃 HONEYPOTS 🎃

- 4Kippo: <https://lnkd.in/d2ypa3j4>
- 5Cowrie: <https://lnkd.in/dAR68lQt>
- 6Dockpot: <https://lnkd.in/dgn7MpOg>
- 7HonSSH: <https://lnkd.in/dMKptyHz>

💡 THREAT INTELLIGENCE 💡

- 1MisP: <https://lnkd.in/dkcbKsTN>
- 2MSTICPy: <https://lnkd.in/dBjgWVqY>

🔒 EDR 🔒

- 3Cortex XDR: <https://lnkd.in/devusd8T>
- 4Cynet 360: <https://lnkd.in/dZTXUwBE>
- 5FortiEDR: <https://lnkd.in/daTMkVxb>

📎 SIEM 📋

The Blue Team Toolkit is a collection of various cybersecurity tools categorized into several sections:

- Network Analysis:** Wireshark, pfSense, Arkime, Snort.
- OS Analysis:** HELK, Volatility, Wazuh, RegRipper, OSSEC, osquery.
- Incident Management:** TheHive, GRR Rapid Response.
- Honeypots:** Kippo, Cowrie, Dockpot, HonSSH.
- Threat Intelligence:** MisP, MSTICPy.
- EDR:** Cortex XDR, Cynet 360, FortiEDR.
- SIEM:** OSSIM, Splunk, LogRhythm.

Areyouinterestedincybersecurity? -> [in/patriblasco](#)

- 6OSSIM: <https://lnkd.in/dXegU3-5>
- 7Splunk: <https://www.splunk.com>
- LogRhythm: <https://logrhythm.com>
- Wazuh: <https://wazuh.com>

-VULNERABILIDADES:

<https://nvd.nist.gov/>

<https://www.cve.org/CVERecord/SearchResults?query=cloud>

<https://cybermap.kaspersky.com/es>