Informe de Seguridad y Recolección de Información sobre hostinger.com

---

1. Introducción

El presente informe tiene como objetivo obtener la máxima información posible sobre la organización Hostinger y sus activos tecnológicos expuestos en internet. Este análisis incluye la recopilación de subdominios, evaluación de vulnerabilidades, y técnicas OSINT para obtener información sensible sobre la organización, empleados y configuraciones críticas que pudieran estar mal implementadas o expuestas al público.

---

2. Técnicas de Footprinting

El Footprinting es la primera etapa en la que se recolecta información general sobre el objetivo. Esta etapa incluye el análisis del dominio, los subdominios y la exposición pública de los activos de la organización.

2.1 Recolección de Subdominios

Herramientas utilizadas: Sublist3r, Amass, crt.sh, ShuffleDNS, CTFR.

Comandos:

Sublist3r: sublist3r -d hostinger.com -o subdominios.txt
Amass: amass enum -d hostinger.com -o amass_subdomains.txt
Certificado Transparente (crt.sh): curl https://crt.sh/?q=hostinger.com > subdominios_crtsh.txt
ShuffleDNS: shuffledns -d hostinger.com -r resolvers.txt -o shuffledns_results.txt
CTFR: python3 ctfr.py -d hostinger.com -o ctfr_subdomains.txt

Resultados de los subdominios identificados:

- https://cart.hostinger.com
- https://cpanel.hostinger.com
- https://autodiscover.mail.hostinger.com
- https://flockmail.hostinger.com
- https://titanmail.hostinger.com
- https://support.hostinger.com

Archivos generados: subdominios_limpios.txt, subdominios_vivos.txt.

---

3. Técnicas de Fingerprinting

El Fingerprinting se refiere a identificar con precisión los sistemas y servicios que se ejecutan en el objetivo.

3.1 Escaneo de Puertos y Servicios (Nmap)

- **Herramienta utilizada**: Nmap
- **Comando**: sudo nmap -sS -T2 -Pn -iL ips_subdominios.txt -oN nmap_silent_result.txt

El escaneo de puertos reveló que la mayoría de los servicios tienen abiertos los puertos 80/tcp (HTTP) y 443/tcp (HTTPS).

Ejemplo de subdominio escaneado:

- **Host**: surveys.hostinger.com.cdn.cloudflare.net
- **Puertos abiertos**: 80/tcp, 443/tcp.

Archivo generado: nmap_silent_result.txt.

---

4. Análisis de Vulnerabilidades

El análisis de vulnerabilidades se realizó para descubrir fallas en las configuraciones de seguridad de los subdominios identificados.

4.1 Análisis de Vulnerabilidades (Nuclei)

- **Herramienta utilizada**: Nuclei
- **Comando**: nuclei -u https://subdominio -o nuclei_vulns.txt

Faltas detectadas:

- Cross-Origin Resource Policy (CORP)
- Content Security Policy (CSP)
- Strict-Transport-Security (HSTS)

Subdominios críticos:

- autodiscover.mail.hostinger.com
- autoconfig.mail.hostinger.com

Archivos generados: nuclei.txt, nuclei_vulns_https.txt.

4.2 Verificación de Configuración SSL/TLS (Testssl.sh)

- **Herramienta utilizada**: Testssl.sh
- **Comando**: testssl.sh https://subdominio > testssl_result.html

El análisis reveló configuraciones SSL/TLS débiles en algunos subdominios que podrían ser vulnerables a ataques MITM (Man-in-the-Middle).

Hallazgos:

- Algunos subdominios carecen de HSTS. Ejemplo: https://cpanel.hostinger.com no ofrece HSTS.

Archivo generado: testssl_result.html.

---

5. Técnicas OSINT

El OSINT (Open Source Intelligence) se refiere a la recolección de información pública disponible en la red. En este caso, se obtuvieron datos relevantes sobre la organización mediante herramientas OSINT.

5.1 Recolección de Correos Electrónicos (The Harvester)

- **Herramienta utilizada**: The Harvester
- **Comando**: theHarvester -d hostinger.com -b all -f emails_harvester.json

Correos recolectados:

- abuse@hostinger.com
- account-recovery@hostinger.com
- domains@hostinger.com
- sales@hostinger.com

Archivos generados: emails_harvester.json, emails_harvester.xml.

5.2 Variaciones de Dominio (DNSTwist)

- **Herramienta utilizada**: DNSTwist
- **Comando**: dnstwist -r hostinger.com > dnstwist_results.txt

Variaciones detectadas: Se encontraron dominios similares que podrían ser utilizados para phishing o suplantación de identidad.

Archivo generado: dnstwist_results.txt.

5.3 Subdominios con Transparencia de Certificados (crt.sh)

Resultados: Se obtuvieron subdominios registrados mediante la plataforma de certificados públicos.

Archivo generado: subdominios_crtsh.txt.

5.4 Google Dorks

- **Comando**: site:hostinger.com filetype:pdf OR filetype:doc > google_dorks.txt

Hallazgos: Se encontraron posibles configuraciones y documentos expuestos mediante Google Dorks.

Archivo generado: google_dorks.txt.

5.5 Escaneo de Directorios (Dirsearch)

- **Herramienta utilizada**: Dirsearch

- **Comando**: python3 dirsearch.py -u https://subdominio -e php,html,txt,js -o dirsearch_result.txt

Resultados: Se intentó acceder a rutas sensibles, detectando archivos como .htaccess y .gitignore, aunque la mayoría devolvieron error 404.
Archivo generado: dirsearch_result.txt.

---

6. Capturas de Pantalla de Subdominios Críticos

En la carpeta "screenshots", se encontraron capturas de pantalla de subdominios críticos que ofrecen una visualización directa de los servicios en línea. A continuación, algunos ejemplos:

- **https://autodiscover.mail.hostinger.com**: Página de configuración de correo que podría ser vulnerable si no está debidamente protegida.
- **https://cpanel.hostinger.com**: Acceso al panel de control de servidores, un punto crítico desde el punto de vista de seguridad.
- **https://flockmail.hostinger.com**: Un servicio de correo que utiliza la tecnología Flockmail.

Estas capturas pueden ser útiles para identificar configuraciones visuales y evaluar posibles vulnerabilidades basadas en la exposición de servicios en línea.

---

7. Conclusiones

El análisis ha identificado varios puntos críticos que deben ser atendidos en el dominio hostinger.com. A continuación, se resumen los aspectos más importantes:

- **Falta de cabeceras de seguridad**: Es fundamental implementar cabeceras de seguridad como HSTS, CSP, y CORP para mitigar ataques comunes como XSS o Man-in-the-Middle.
- **Servicios relacionados con correo**: Los subdominios de correo, como autodiscover.mail.hostinger.com y autoconfig.mail.hostinger.com, presentan riesgos debido a configuraciones inseguras.
- **Variaciones de dominio**: Se detectaron posibles dominios suplantadores que podrían ser usados para ataques de phishing.
- **Subdominios protegidos por WAF**: Aunque algunos subdominios están protegidos, se recomienda revisar configuraciones adicionales para garantizar que no haya vulnerabilidades.
- **Correos y archivos expuestos**: Se encontraron correos electrónicos y rutas de archivos expuestos mediante técnicas OSINT que deben ser evaluados para mitigar riesgos.

Archivos generados:

- subdominios_limpios.txt
- subdominios_vivos.txt
- nmap_silent_result.txt
- nuclei.txt
- nuclei_vulns_https.txt
- testssl_result.html
- emails_harvester.json
- emails_harvester.xml
- dnstwist_results.txt
- subdominios_crtsh.txt
- google_dorks.txt
- dirsearch_result.txt