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. Herramientas y Comandos Utilizados

Para llevar a cabo el análisis de seguridad, se utilizaron una variedad de herramientas de recolección de información y escaneo de vulnerabilidades. A continuación, se detallan las herramientas utilizadas y los comandos ejecutados en cada etapa del proceso.

2.1 Recolección de Subdominios

Herramientas: 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

---

2.2 Escaneo de Puertos y Servicios (Nmap)

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

---

2.3 Análisis de Vulnerabilidades (Nuclei)

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

---

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

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

---

2.5 Recolección de Información OSINT

Herramientas: The Harvester, Hunter.io, GitHub Search, DNSTwist, Google Dorks

Comandos:

The Harvester: theHarvester -d hostinger.com -b all -f emails_harvester.json
DNSTwist: dnstwist -r hostinger.com > dnstwist_results.txt
Google Dorks: site:hostinger.com filetype:pdf OR filetype:doc > google_dorks.txt

---

3. Resultados Obtenidos

3.1 Información del Dominio

El análisis del dominio hostinger.com reveló una estructura amplia de subdominios expuestos. Los subdominios más relevantes que fueron identificados son:

Subdominios:

- 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.

3.2 Escaneo de Puertos (Nmap)

El escaneo de puertos en los subdominios 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.

3.3 Análisis de Vulnerabilidades (Nuclei)

El análisis con Nuclei se centró en la detección de cabeceras de seguridad faltantes, políticas de permisos y la configuración de WAF.

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.

3.4 Configuración SSL/TLS (Testssl.sh)

El análisis de configuraciones SSL/TLS reveló configuraciones débiles en algunos subdominios que podrían ser vulnerables a ataques MITM.

Hallazgos:

- Algunos subdominios carecen de HSTS.

Ejemplo: https://cpanel.hostinger.com no ofrece HSTS.
Archivo generado: testssl_result.html.

3.5 Información OSINT

Se obtuvieron datos relevantes sobre la organización mediante técnicas OSINT, incluyendo correos electrónicos y posibles configuraciones expuestas.

Correos Electrónicos (The Harvester)

Correos recolectados:

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

Archivos generados: emails_harvester.json, emails_harvester.xml.

Variaciones de Dominio (DNSTwist)

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

Subdominios con Transparencia de Certificados (crt.sh)

Resultados: Se obtuvieron subdominios registrados mediante la plataforma de certificados públicos.
Archivo generado: subdominios_crtsh.txt.

Google Dorks

Hallazgos: Se encontraron posibles configuraciones y documentos expuestos mediante Google Dorks.
Archivo generado: google_dorks.txt.

Escaneo de Directorios (Dirsearch)

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

---

4. 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