DESAFIO 18

BOOTCAMP DEVOPS

ALUMNO: Rolando Arce

**DESAFÍO 18 – ETHICAL HACKING**

**OBJETIVO**

Realizar pruebas sobre sistemas informáticos de la misma forma que podría

hacerla una persona malintencionada.

Conocer las debilidades de la infraestructura, a fin de poder solucionarlas, antes

de que una persona malintencionada pudiera aprovecharse de ellas.

Ejecutar pruebas con un excelente nivel de ética, debido a que es muy probable

que, durante las pruebas, se descubran vulnerabilidades que podrían ser

explotadas para obtener beneficios económicos, más allá de los acordados.

Objeto de estudio: Sitio [*http://vulnweb.com/*](http://vulnweb.com/)

Comenzamos las pruebas:

1.

rarce2024@CNP-SIST028-N ~

❯ ping testhtml5.vulnweb.com

Haciendo ping a testhtml5.vulnweb.com [44.228.249.3] con 32 bytes de datos:

Respuesta desde 44.228.249.3: bytes=32 tiempo=219ms TTL=43

Respuesta desde 44.228.249.3: bytes=32 tiempo=216ms TTL=43

Respuesta desde 44.228.249.3: bytes=32 tiempo=213ms TTL=43

Respuesta desde 44.228.249.3: bytes=32 tiempo=215ms TTL=43

Estadísticas de ping para 44.228.249.3:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 213ms, Máximo = 219ms, Media = 215ms

edenon@CNP-SIST028-N ~

ping testphp.vulnweb.com

Haciendo ping a testphp.vulnweb.com [44.228.249.3] con 32 bytes de datos:

Respuesta desde 44.228.249.3: bytes=32 tiempo=214ms TTL=43

Respuesta desde 44.228.249.3: bytes=32 tiempo=217ms TTL=43

Respuesta desde 44.228.249.3: bytes=32 tiempo=210ms TTL=43

Respuesta desde 44.228.249.3: bytes=32 tiempo=214ms TTL=43

Estadísticas de ping para 44.228.249.3:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 210ms, Máximo = 217ms, Media = 213ms

❯ ping testasp.vulnweb.com

Haciendo ping a testasp.vulnweb.com [44.238.29.244] con 32 bytes de datos:

Respuesta desde 44.238.29.244: bytes=32 tiempo=212ms TTL=107

Respuesta desde 44.238.29.244: bytes=32 tiempo=216ms TTL=107

Respuesta desde 44.238.29.244: bytes=32 tiempo=217ms TTL=107

Respuesta desde 44.238.29.244: bytes=32 tiempo=216ms TTL=107

Estadísticas de ping para 44.238.29.244:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 212ms, Máximo = 217ms, Media = 215ms

edenon@CNP-SIST028-N ~

❯ ping testaspnet.vulnweb.com

Haciendo ping a testaspnet.vulnweb.com [44.238.29.244] con 32 bytes de datos:

Respuesta desde 44.238.29.244: bytes=32 tiempo=219ms TTL=107

Respuesta desde 44.238.29.244: bytes=32 tiempo=220ms TTL=107

Respuesta desde 44.238.29.244: bytes=32 tiempo=211ms TTL=107

Respuesta desde 44.238.29.244: bytes=32 tiempo=216ms TTL=107

Estadísticas de ping para 44.238.29.244:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 211ms, Máximo = 220ms, Media = 216ms

edenon@CNP-SIST028-N ~

❯ ping rest.vulnweb.com

Haciendo ping a rest.vulnweb.com [35.81.188.86] con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.

Tiempo de espera agotado para esta solicitud.

Tiempo de espera agotado para esta solicitud.

Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 35.81.188.86:

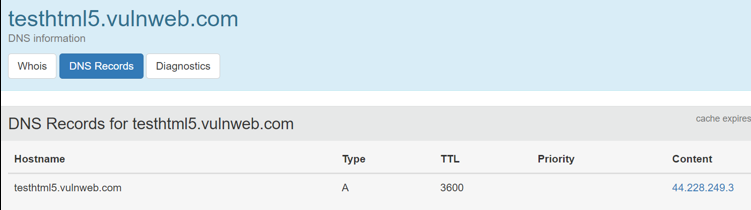
Paquetes: enviados = 4, recibidos = 0, perdidos = 4

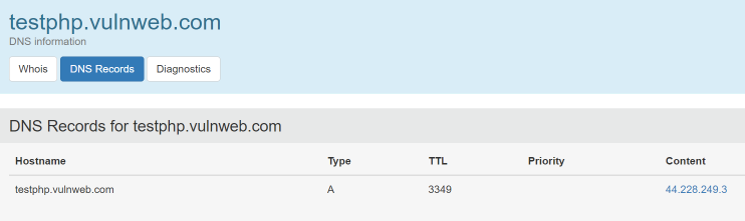
(100% perdidos),

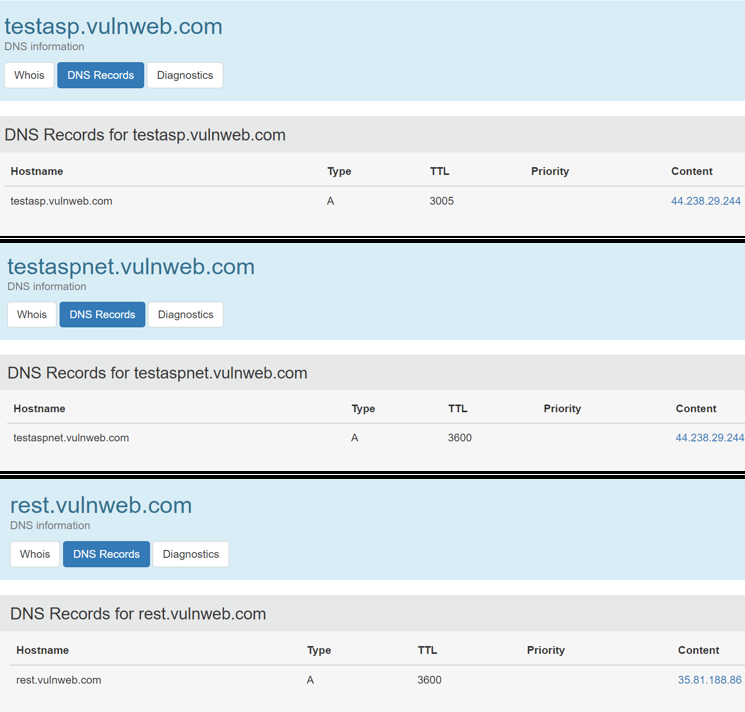
edenon@CNP-SIST028-N ~

❯

2. Who is & DIG







$ dig vulnweb.com

; <<>> DiG 9.11.9 <<>> vulnweb.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28367

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 2

;; QUESTION SECTION:

;vulnweb.com. IN A

;; ANSWER SECTION:

vulnweb.com. 2069 IN A 44.228.249.3

;; AUTHORITY SECTION:

. 86971 IN NS b.root-servers.net.

. 86971 IN NS l.root-servers.net.

. 86971 IN NS h.root-servers.net.

. 86971 IN NS j.root-servers.net.

. 86971 IN NS k.root-servers.net.

. 86971 IN NS c.root-servers.net.

. 86971 IN NS i.root-servers.net.

. 86971 IN NS e.root-servers.net.

. 86971 IN NS d.root-servers.net.

. 86971 IN NS m.root-servers.net.

. 86971 IN NS f.root-servers.net.

. 86971 IN NS g.root-servers.net.

. 86971 IN NS a.root-servers.net.

;; ADDITIONAL SECTION:

m.root-servers.net. 166160 IN A 202.12.27.33

a.root-servers.net. 164673 IN A 198.41.0.4

;; Query time: 7 msec

;; SERVER: 192.168.8.252#53(192.168.8.252)

;; WHEN: Sun Jul 07 19:54:36 -03 2024

;; MSG SIZE rcvd: 288

$ dig testhtml5.vulnweb.com

; <<>> DiG 9.11.9 <<>> testhtml5.vulnweb.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 751

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 2

;; QUESTION SECTION:

;testhtml5.vulnweb.com. IN A

;; ANSWER SECTION:

testhtml5.vulnweb.com. 2264 IN A 44.228.249.3

;; AUTHORITY SECTION:

. 87075 IN NS d.root-servers.net.

. 87075 IN NS m.root-servers.net.

. 87075 IN NS f.root-servers.net.

. 87075 IN NS g.root-servers.net.

. 87075 IN NS a.root-servers.net.

. 87075 IN NS b.root-servers.net.

. 87075 IN NS l.root-servers.net.

. 87075 IN NS h.root-servers.net.

. 87075 IN NS j.root-servers.net.

. 87075 IN NS k.root-servers.net.

. 87075 IN NS c.root-servers.net.

. 87075 IN NS i.root-servers.net.

. 87075 IN NS e.root-servers.net.

;; ADDITIONAL SECTION:

m.root-servers.net. 166264 IN A 202.12.27.33

a.root-servers.net. 164777 IN A 198.41.0.4

;; Query time: 7 msec

;; SERVER: 192.168.8.252#53(192.168.8.252)

;; WHEN: Sun Jul 07 19:52:52 -03 2024

;; MSG SIZE rcvd: 298

$ dig testphp.vulnweb.com

; <<>> DiG 9.11.9 <<>> testphp.vulnweb.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44471

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 2

;; QUESTION SECTION:

;testphp.vulnweb.com. IN A

;; ANSWER SECTION:

testphp.vulnweb.com. 2244 IN A 44.228.249.3

;; AUTHORITY SECTION:

. 87036 IN NS i.root-servers.net.

. 87036 IN NS e.root-servers.net.

. 87036 IN NS d.root-servers.net.

. 87036 IN NS m.root-servers.net.

. 87036 IN NS f.root-servers.net.

. 87036 IN NS g.root-servers.net.

. 87036 IN NS a.root-servers.net.

. 87036 IN NS b.root-servers.net.

. 87036 IN NS l.root-servers.net.

. 87036 IN NS h.root-servers.net.

. 87036 IN NS j.root-servers.net.

. 87036 IN NS k.root-servers.net.

. 87036 IN NS c.root-servers.net.

;; ADDITIONAL SECTION:

m.root-servers.net. 166225 IN A 202.12.27.33

a.root-servers.net. 164738 IN A 198.41.0.4

;; Query time: 7 msec

;; SERVER: 192.168.8.252#53(192.168.8.252)

;; WHEN: Sun Jul 07 19:53:31 -03 2024

;; MSG SIZE rcvd: 296

$ dig testasp.vulnweb.com

; <<>> DiG 9.11.9 <<>> testasp.vulnweb.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34669

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 2

;; QUESTION SECTION:

;testasp.vulnweb.com. IN A

;; ANSWER SECTION:

testasp.vulnweb.com. 2320 IN A 44.238.29.244

;; AUTHORITY SECTION:

. 87024 IN NS f.root-servers.net.

. 87024 IN NS g.root-servers.net.

. 87024 IN NS a.root-servers.net.

. 87024 IN NS b.root-servers.net.

. 87024 IN NS l.root-servers.net.

. 87024 IN NS h.root-servers.net.

. 87024 IN NS j.root-servers.net.

. 87024 IN NS k.root-servers.net.

. 87024 IN NS c.root-servers.net.

. 87024 IN NS i.root-servers.net.

. 87024 IN NS e.root-servers.net.

. 87024 IN NS d.root-servers.net.

. 87024 IN NS m.root-servers.net.

;; ADDITIONAL SECTION:

a.root-servers.net. 164726 IN A 198.41.0.4

m.root-servers.net. 166213 IN A 202.12.27.33

;; Query time: 10 msec

;; SERVER: 192.168.8.252#53(192.168.8.252)

;; WHEN: Sun Jul 07 19:53:43 -03 2024

;; MSG SIZE rcvd: 296

$ dig testaspnet.vulnweb.com

; <<>> DiG 9.11.9 <<>> testaspnet.vulnweb.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48869

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 2

;; QUESTION SECTION:

;testaspnet.vulnweb.com. IN A

;; ANSWER SECTION:

testaspnet.vulnweb.com. 2302 IN A 44.238.29.244

;; AUTHORITY SECTION:

. 87013 IN NS i.root-servers.net.

. 87013 IN NS e.root-servers.net.

. 87013 IN NS d.root-servers.net.

. 87013 IN NS m.root-servers.net.

. 87013 IN NS f.root-servers.net.

. 87013 IN NS g.root-servers.net.

. 87013 IN NS a.root-servers.net.

. 87013 IN NS b.root-servers.net.

. 87013 IN NS l.root-servers.net.

. 87013 IN NS h.root-servers.net.

. 87013 IN NS j.root-servers.net.

. 87013 IN NS k.root-servers.net.

. 87013 IN NS c.root-servers.net.

;; ADDITIONAL SECTION:

m.root-servers.net. 166202 IN A 202.12.27.33

a.root-servers.net. 164715 IN A 198.41.0.4

;; Query time: 10 msec

;; SERVER: 192.168.8.252#53(192.168.8.252)

;; WHEN: Sun Jul 07 19:53:54 -03 2024

;; MSG SIZE rcvd: 299

$ dig rest.vulnweb.com/

; <<>> DiG 9.11.9 <<>> rest.vulnweb.com/

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 55762

;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:

;rest.vulnweb.com/. IN A

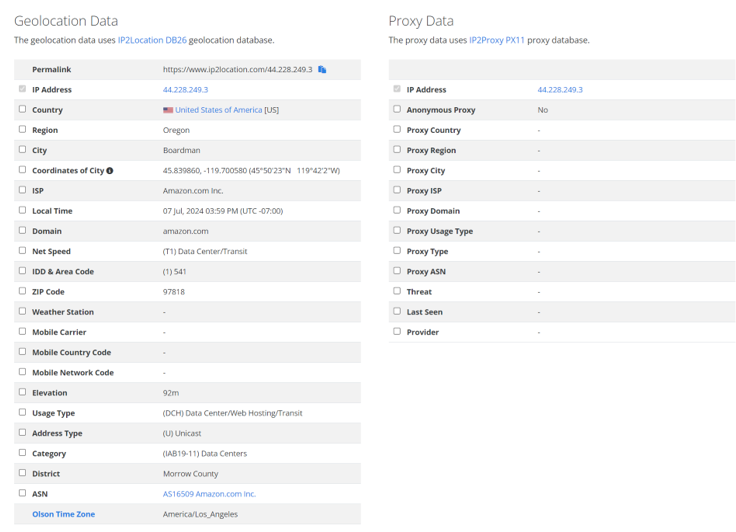
;; Query time: 43 msec

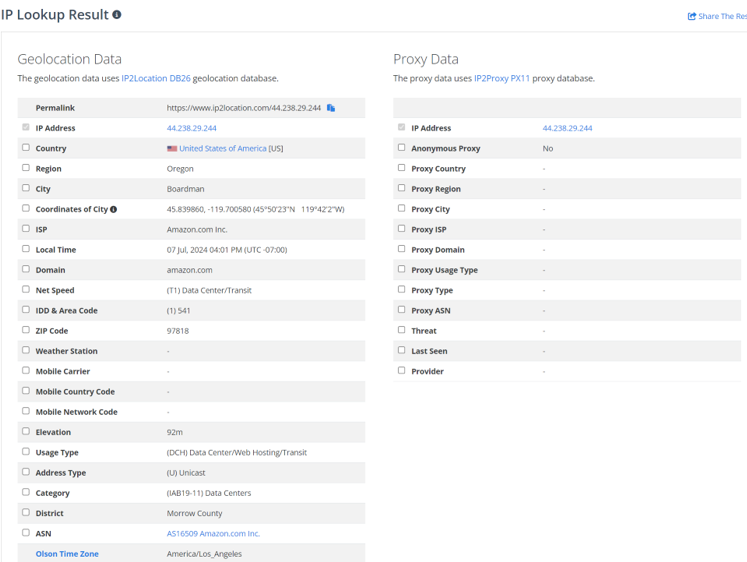
;; SERVER: 192.168.8.252#53(192.168.8.252)

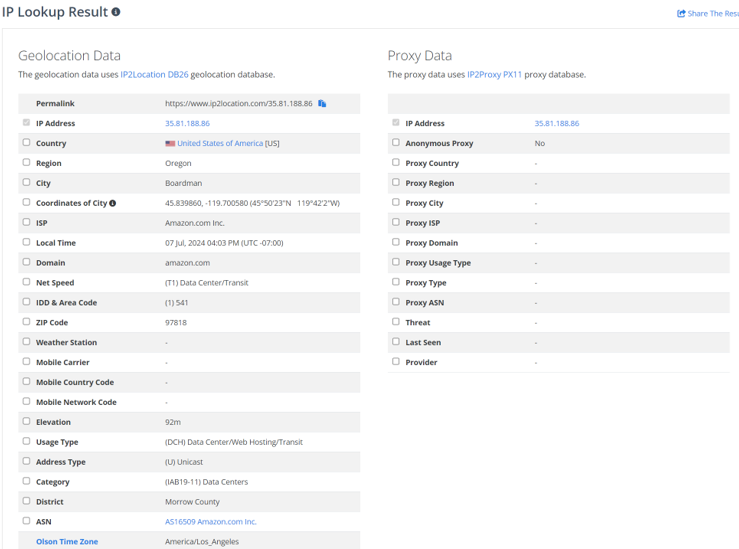
;; WHEN: Sun Jul 07 19:54:14 -03 2024

;; MSG SIZE rcvd: 35

4- GEOIP



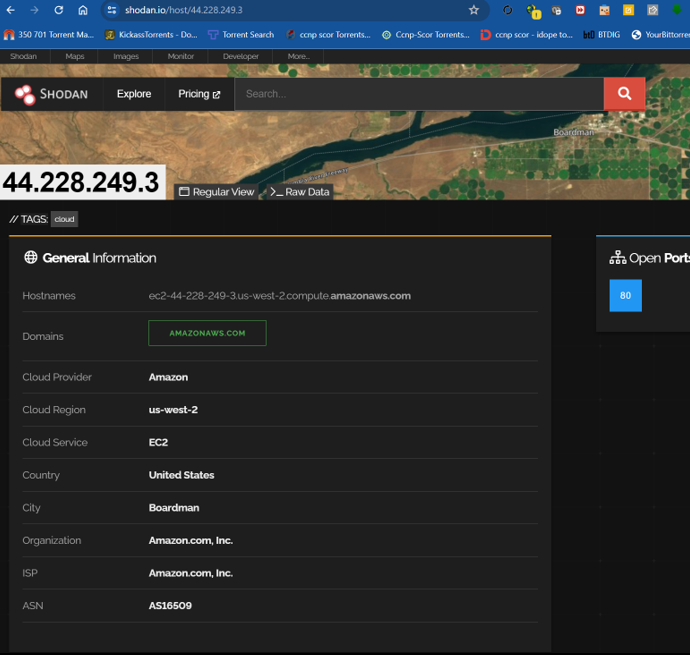


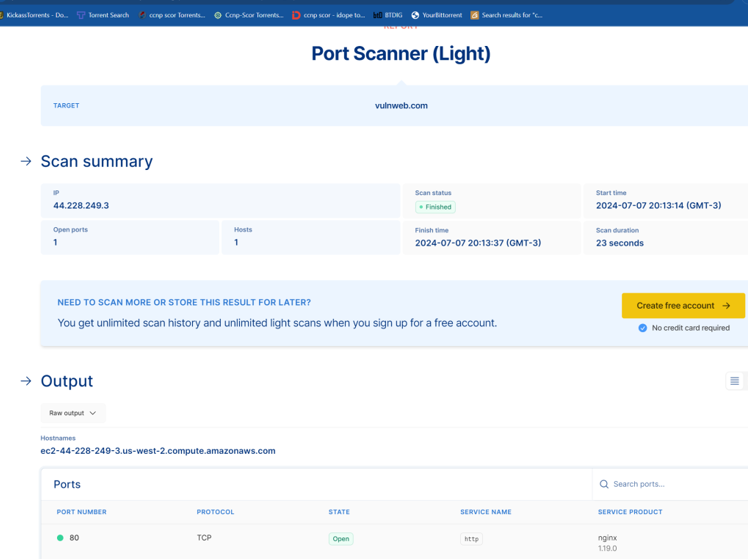


5-NMAP/SHODAN

555-NMAPN

5-NMAP/SHODAN





Fin

Repositorio.