

# Remote DNS Cache Poisoning Attack Lab

מג'ישט: שני וhb 208584557 אילון בראשי 13

ה-IP של התקף: 10.0.2.15

ה-IP של הנתקף: 10.0.2.4

ה-IP של שרת DNS המקומי: 10.0.2.5

## Task 1: Configure the User VM

אנחנו רוצים ששרת DNS שהנטקף ישתמש בו יהיה שרת DNS המקומי שלנו, לכן אנחנו מושנים את קובץ resolv.conf שאצל הנתקף, כך שהשרת DNS שלנו יהיה שרת DNS הראשי שלו:

head.png

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#      DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN

nameserver 10.0.2.5
```

נבחן אם הפעולה הצליחה ע"י הפקודה dig:

config\_user.png

```
www.google.com.      300   IN    A     172.217.22.4
;; AUTHORITY SECTION:
google.com.          172800  IN    NS    ns2.google.com.
google.com.          172800  IN    NS    ns1.google.com.
google.com.          172800  IN    NS    ns3.google.com.
google.com.          172800  IN    NS    ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.      172800  IN    A     216.239.32.10
ns1.google.com.      172800  IN    AAAA  2001:4860:4802:32::a
ns2.google.com.      172800  IN    A     216.239.34.10
ns2.google.com.      172800  IN    AAAA  2001:4860:4802:34::a
ns3.google.com.      172800  IN    A     216.239.36.10
ns3.google.com.      172800  IN    AAAA  2001:4860:4802:36::a
ns4.google.com.      172800  IN    A     216.239.38.10
ns4.google.com.      172800  IN    AAAA  2001:4860:4802:38::a

;; Query time: 889 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Wed Dec 28 03:58:19 EST 2022
;; MSG SIZE  rcvd: 307

[12/28/22]seed@VM:~$
```

אנחנו שלחנו בקשת DNS לכתובת של גוגל, ואכן ניתן לראות שההתשובה הגיעה מ-IP של שרת DNS שלנו - הפעולה הצליחה.

## Task 2: Configure the Local DNS Server (the Server VM)

שלב ראשון - נעביר את כל השאלות של דומיין com ל-attacker32.com.  
כלומר אנחנו רוצים ש-10.0.2.15 יהיה nameserverן עבור הדומיין com.attacker32.com

22.png

```
// This is the primary configuration file for the BIND DNS server named.  
//  
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the  
// structure of BIND configuration files in Debian, *BEFORE* you customize  
// this configuration file.  
//  
// If you are just adding zones, please do that in /etc/bind/named.conf.local  
  
include "/etc/bind/named.conf.options";  
include "/etc/bind/named.conf.local";  
* include "/etc/bind/named.conf.default-zones";  
  
zone "attacker32.com"  
{  
    type forward;  
    forwarders  
    {  
        10.0.2.15;  
    };  
};
```

**מנקים את המטמון ומתחלימים את השרת:**

task2\_server.png

```
[12/28/22]seed@VM:~$ sudo rndc dumpdb -cache  
[12/28/22]seed@VM:~$ sudo rndc flush  
[12/28/22]seed@VM:~$ sudo service bind9 restart  
[12/28/22]seed@VM:~$
```

ניתן לראות שDNSSEC מבוטל (האבטחה על שרת DNS) והותן source port (DNS) מכוון להיות 33333.

2.png

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====

    // dnssec-validation auto;
    dnssec-enable no;
    dump-file "/var/cache/bind/dump.db";
    auth-nxdomain no;      # conform to RFC1035

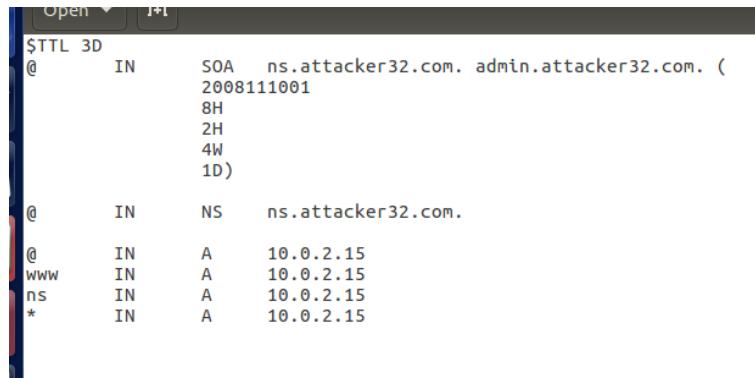
    query-source port        33333;
    listen-on-v6 { any; };

};
```

### Task 3: Configure the Attacker VM

עדכן כתובת ה-IP בקובץ zone.zone של הtokף:

3.1.png



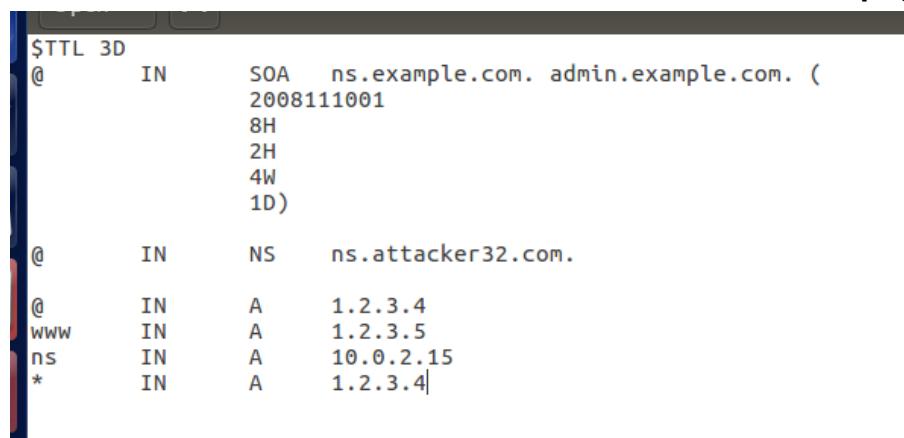
```
$TTL 3D
@ IN SOA ns.attacker32.com. admin.attacker32.com. (
2008111001
8H
2H
4W
1D)

@ IN NS ns.attacker32.com.

@ IN A 10.0.2.15
www IN A 10.0.2.15
ns IN A 10.0.2.15
* IN A 10.0.2.15
```

עדכן כתובת ה-IP בקובץ zone.zone של הtokף:

3.2.png



```
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
2008111001
8H
2H
4W
1D)

@ IN NS ns.attacker32.com.

@ IN A 1.2.3.4
www IN A 1.2.3.5
ns IN A 10.0.2.15
* IN A 1.2.3.4|
```

הווסף שתי הconfig'ות האלה לקובץ `/etc/bind/named.conf`

**png.3.4**

```
// This is the primary configuration file for the BIND DNS server named.  
//  
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the  
// structure of BIND configuration files in Debian, *BEFORE* you customize  
// this configuration file.  
//  
// If you are just adding zones, please do that in /etc/bind/named.conf.local  
  
include "/etc/bind/named.conf.options";  
include "/etc/bind/named.conf.local";  
include "/etc/bind/named.conf.default-zones";  
  
zone "attacker32.com" {  
    type master;  
    file "/etc/bind/attacker32.com.zone";  
};  
zone "example.com" {  
    type master;  
    file "/etc/bind/example.com.zone";  
};|
```

לאחר מכן הפעילו מחדש את DNS כדי שהקונפיגורציות החדשות יכנסו לתוקף.

#### Task 4: Testing the Setup

נודא שההגדרות החדשות שהכינו אכן נכוןות:

על המכונה של הנטקף נרץ את הפקודה `dig ns.attacker32.com` ונראה את ה-IP של ה-NS:

**4.5.png**

```
[2] 172796 IN A 192.41.162.30  
l.gtld-servers.net. 172796 IN AAAA 2001:500:9d37::30  
m.gtld-servers.net. 172796 IN A 192.55.83.30  
m.gtld-servers.net. 172796 IN AAAA 2001:501:b1f9::30  
  
;; Query time: 3 msec  
;; SERVER: 10.0.2.5#53(10.0.2.5)  
;; WHEN: Wed Dec 28 06:48:27 EST 2022  
;; MSG SIZE rcvd: 858  
  
[12/28/22]seed@VM:~$ clear  
[3]:J  
[12/28/22]seed@VM:~$ dig ns.attacker32.com  
  
; <>> DiG 9.10.3-P4-Ubuntu <>> ns.attacker32.com  
; global options: +cmd  
; Got answer:  
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25585  
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 27  
  
; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
; QUESTION SECTION:  
;ns.attacker32.com. IN A  
  
; ANSWER SECTION:  
ns.attacker32.com. 259195 IN A 10.0.2.15  
  
; AUTHORITY SECTION:  
com. 172791 IN NS a.gtld-servers.net.  
com. 172791 IN NS c.gtld-servers.net.  
com. 172791 IN NS m.gtld-servers.net.  
com. 172791 IN NS l.gtld-servers.net.
```

נשלח שאלתת DNS לשרת ע"י הרצת הפקודה dig www.example.com

```
[12/28/22]seed@VM:~$ dig www.example.com
; <>> DiG 9.10.3-P4-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16245
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.          IN      A
;;
;; ANSWER SECTION:
www.example.com.      86400   IN      A      93.184.216.34
;;
;; AUTHORITY SECTION:
example.com.           86400   IN      NS     a.iana-servers.net.
example.com.           86400   IN      NS     b.iana-servers.net.
;;
;; ADDITIONAL SECTION:
a.iana-servers.net.    1800    IN      A      199.43.135.53
a.iana-servers.net.    1800    IN      AAAA   2001:500:8f::53
b.iana-servers.net.    1800    IN      A      199.43.133.53
b.iana-servers.net.    1800    IN      AAAA   2001:500:8d::53
;;
;; Query time: 968 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Wed Dec 28 15:34:07 EST 2022
;; MSG SIZE rcvd: 196
```

נשלח שאלתת ישירות ל ns.attacker32.com

4.7.png

```
[12/28/22]seed@VM:~$ /bin/bash B0x33
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Dec 28 06:52:46 EST 2022
;; MSG SIZE rcvd: 108

[12/28/22]seed@VM:~$ dig @ns.attacker32.com www.example.com
; <>> DiG 9.10.3-P4-Ubuntu <>> @ns.attacker32.com www.example.com
;(1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49883
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.          IN      A
;;
;; ANSWER SECTION:
www.example.com.      259200   IN      A      1.2.3.5
;;
;; AUTHORITY SECTION:
example.com.           259200   IN      NS     ns.attacker32.com.
;;
;; ADDITIONAL SECTION:
ns.attacker32.com.     259200   IN      A      10.0.2.15
;;
;; Query time: 6 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Wed Dec 28 06:54:30 EST 2022
;; MSG SIZE rcvd: 104

[12/28/22]seed@VM:~$
```

כל הבדיקות עברו בהצלחה.

יצרנו קובץ **req.dns** - במטרה לשלוח לשרת DNS כדי שיחזיר תשובה מזויפות.

## Task 5: Spoof DNS Replies

קובץ dns.rep - זיווג תשובות DNS משרת השמות (IP מקורי) של הדומיין example.com, דרך port 53 שזה ה-port של פאקטות DNS.

## Task 6: Launch the Kaminsky Attack.

אנחנוCut רוצים להפעיל את ההתקפה (attack.c) - להרעל את מטען DNS כך שכאשר המשמש יפעיל את הפקודה dig במטרה לקבל כתשובה את כתובת ה-IP של ns.attacker32.com, שרת DNS עברו לnameserver של התוקף - כתובת שיקבע התוקף - כתוצאה מכך, המשמש לקבלת כתובת ה-IP, והכתובות שתוחזר תהיה כל כתובת שיקבע התוקף. יועבר לדף אותו קבע התוקף.

לאחר שהרכינו את הקובץ attack.c, הרכנו את הפקודה "dig" במכונה של המשמש וציפינו לראות התאמה ל- ns.attacker32.com שזה אומר שהתקפה הצליחה.