Dns Zone Transfer Attack

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

Dns Zone transfere imkan veren bir test ortamı vardır.

zonetransfer.me

Bu test ortamından faydalanarak dns zone transferi gerçekleştireceğiz. Öncelikle hedef web sitesinin yetkilli dns sunucu adresini öğrenelim.

> dig ns zonetransfer.me

Output:

```
; <<>> DiG 9.9.5-3ubuntu0.14-Ubuntu <<>> ns zonetransfer.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13237
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;zonetransfer.me.               IN      NS

;; ANSWER SECTION:
zonetransfer.me.        7199    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7199    IN      NS      nsztm2.digi.ninja.

;; Query time: 99 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Jun 13 08:46:31 +03 2017
;; MSG SIZE  rcvd: 96
```

Görüldüğü üzere ANSWER bölümünde dns sunucu adresleri gelmiştir. Şimdi bu dns sunucularından birine dns zone transfer yapalım ve içerdiği tüm dns kayıtlarını çekelim.

> dig axfr zonetransfer.me @nsztm1.digi.ninja

Output:

```
; <<>> DiG 9.9.5-3ubuntu0.14-Ubuntu <<>> axfr zonetransfer.me @nsztm2.digi.ninja
;; global options: +cmd
zonetransfer.me.  7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja.
zonetransfer.me.  300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.  301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2s
zonetransfer.me.  7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.  7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.  7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.  7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.  7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.  7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.  7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.  7200    IN      A       217.147.177.157
zonetransfer.me.  7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.  7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN       SRV     0 0 5060 www.zonetransfer.me.
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me. 7200 IN PTR www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN     AFSDB 1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200    IN      A       127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN      AFSDB 1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A 202.14.81.230
cmdexec.zonetransfer.me. 300      IN      TXT     "\; ls"
contact.zonetransfer.me. 2592000 IN       TXT     "Remember to call or email Pippa on +44 123
4567890 or pippa@zonetransfer.me when making DNS changes"
dc-office.zonetransfer.me. 7200   IN      A       143.228.181.132
deadbeef.zonetransfer.me. 7201    IN      AAAA    dead:beaf::
dr.zonetransfer.me.       300     IN      LOC     53 20 56.558 N 1 38 33.526
DZC.zonetransfer.me.      7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.    2222    IN      NAPTR 1 1 "P" "E2U+email" ""
email.zonetransfer.me.    7200    IN      A       74.125.206.26
home.zonetransfer.me.     7200    IN      A       127.0.0.1
Info.zonetransfer.me.     7200    IN      TXT     "ZoneTransfer.me service provided by Robin
Wood - robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php for more information."
internal.zonetransfer.me. 300     IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me. 300     IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me.   300     IN      A       167.88.42.94
intns2.zonetransfer.me.   300     IN      A       167.88.42.94
office.zonetransfer.me.   7200    IN      A       4.23.39.254
ipv6actnow.org.zonetransfer.me.   7200 IN AAAA    2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.      7200    IN      A       207.46.197.32
robinwood.zonetransfer.me. 302    IN      TXT     "Robin Wood"
rp.zonetransfer.me.       321     IN      RP      robin.zonetransfer.me.
sip.zonetransfer.me.      3333    IN      NAPTR 2 3 "P" "E2U+sip" "!^.*$!sip:customer"
sqli.zonetransfer.me.     300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me.   7200    IN      TXT     "() { :]}\; echo ShellShocked"
staging.zonetransfer.me. 7200     IN      CNAME           www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A   127.0.0.1
testing.zonetransfer.me. 301      IN      CNAME           www.zonetransfer.me.
vpn.zonetransfer.me.      4000    IN      A       174.36.59.154
www.zonetransfer.me.      7200    IN      A       217.147.177.157
xss.zonetransfer.me.      300     IN      TXT     "'><script>alert('Boo')</script>"
zonetransfer.me.  7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2014101601
;; Query time: 145 msec
;; SERVER: 167.88.42.94#53(167.88.42.94)
;; WHEN: Tue Jun 13 08:47:00 +03 2017
;; XFR size: 48 records (messages 1, bytes 1867)
```

Böylece tüm dns kayıtları çekilmiştir. Kayıtlarda dikkat edilecek olursa hedef web sitenin yetkili dns sunucusunda tanımlı subdomain'ler de gelmiştir. Bu bilgi pentest için scope'u belirlememizi sağlayan bir bilgidir.

Uygulama

Karabük üniversitesinin dns sunucularına zone transfer yapılabiliyor mu test edelim.

> dig ns karabuk.edu.tr

Output:

```
; <<>> DiG 9.9.5-3ubuntu0.14-Ubuntu <<>> ns karabuk.edu.tr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38650
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;karabuk.edu.tr.                 IN      NS

;; ANSWER SECTION:
karabuk.edu.tr.         10799   IN      NS      ns1.karabuk.edu.tr.
karabuk.edu.tr.         10799   IN      NS      ns1.ulak.net.tr.

;; Query time: 120 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Jun 13 08:59:04 +03 2017
;; MSG SIZE  rcvd: 88
```

Şimdi karabuk.edu.tr'nin yetkili dns sunucusuna zone transfer yapalım.

> dig axfr karabuk.edu.tr @ns1.karabuk.edu.tr

Output:

```
; <<>> DiG 9.9.5-3ubuntu0.14-Ubuntu <<>> axfr karabuk.edu.tr
@ns1.karabuk.edu.tr
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Görüldüğü üzere karabuk.edu.tr'nin yetkili dns sunucusu zone transfere kapalıymış.

Kaynak

LYK 2016 Ağ Güvenliği ve Sızma Testleri Defter Notları