

IT Security

PASSIVE RECONNAISSANCE : DEDICATED TO DNS AND ZONE TRANSFERS

DURATION : 0'15

DNS Basics

- ▶ DNS converts human readable domain names into IP-addresses. It's easier to remember domain names than IP addresses.
- ▶ This DNS conversion process may take place through a local cache or through a zone file that is present on the server. A zone file is a file on the server that contains entries for different Resource Records (RR).
- ▶ Let's say the user opens up the browser and types "google.com". It's now the responsibility of the DNS resolver in the user's operating system to fetch the IP address.
 - ▶ First it checks his local cache.
 - ▶ If it can't find the IP address in it's cache it queries the DNS server.
 - ▶ If it still can't find the IP Address, then it goes through a process or recursive DNS query in which it queries different nameservers (NS) to get the IP-address of the domain.

DNS Record Types

- ▶ Address Mapping record (A Record) : stores a hostname and its corresponding IPv4 address.
- ▶ IP Version 6 Address record (AAAA Record) : stores a hostname and its corresponding IPv6 address.
- ▶ Canonical Name record (CNAME Record) : alias a hostname to another hostname.
- ▶ Mail exchanger record (MX Record) : specifies an SMTP email server for the domain.
- ▶ Name Server records (NS Record) : specifies that a DNS Zone, such as “example.com” is delegated to a specific Authoritative Name Server, and provides the address of the name server.
- ▶ Reverse-lookup Pointer records (PTR Record) : allows a DNS resolver to provide an IP address and receive a hostname (reverse DNS lookup).
- ▶ Certificate record (CERT Record) : stores encryption certificates (PKIX, SPKI, PGP, and so on).
- ▶ Service Location (SRV Record) : a service location record, like MX but for other communication protocols.
- ▶ Text Record (TXT Record) : typically carries machine-readable data such as opportunistic encryption, sender policy framework, DKIM, DMARC, etc.
- ▶ Start of Authority (SOA Record) : this record appears at the beginning of a DNS zone file, and indicates the Authoritative Name Server for the current DNS zone, contact details for the domain administrator, domain serial number, and information on how frequently DNS information for this zone should be refreshed.

DNS Zone file example

4

```
$ORIGIN infosecinstitute.com.;This marks the beginning of the file
$TTL 86400 ; TTL is 24 hours , it could also be 1d or 1h
infosecinstitute.com IN      SOA ns1.infosecinstitute.com. webmaster.infosecinstitute.com. (
    2002026801 ; serial number of this zone file
    2d ; refresh time for slave
    5h ; retry time for slave
    2w ; expiration time for slave
    1h ; maximum caching time
)

NS      ns1.infosecinstitute.com.      ; ns1 is a nameserver for infosecinstitute.com
NS      ns2.infosecinstitute.com.      ; ns2 is a backup nameserver for infosecinstitute.com
MX      10 mail.infosecinstitute.com.  ; mail server
ns1     A      192.168.1.1              ; Ipv4 address for ns1.infosecinstitute.com
www     CNAME  infosecinstitute.com     ; www.infosecinstitute.com is an alias for infosecinstitute.com
ftp     IN     CNAME  www.infosecinstitute.com. ; CNAME for ftp
mail    A      192.0.3.2                ; Ipv4 address for mail.infosecinstitute.com
```

DNS Basics example

5

```
C:\Users>nslookup
Default Server:  UnKnown
Address:  192.168.0.254

> set type=A
> mapmyrun.com
Server:  UnKnown
Address:  192.168.0.254

Non-authoritative answer:
Name:    mapmyrun.com
Addresses:  13.249.13.101
            13.249.13.26
            13.249.13.107
            13.249.13.86
```

- ▶ **set type=A** . This means that we are querying for the A type records which will return IP-address for the domain we query. We will look more into records in the next section.
- ▶ As soon as we type in **mapmyrun.com** we get an output showing **Non-authoritative answer**. This basically means that our DNS server queried an external DNS server to fetch the IP-address. Below we can see 4 IP-addresses associated with **mapmyrun.com**. This is usually the case with large organizations. They use multiple servers to serve the request as one server is generally not capable of handling all the requests.

DNS Basics example

6

```
> set type=NS
> mapmyrun.com
Server: UnKnown
Address: 192.168.0.254

Non-authoritative answer:
mapmyrun.com      nameserver = ns-748.awsdns-29.net
mapmyrun.com      nameserver = ns-1360.awsdns-42.org
mapmyrun.com      nameserver = ns-1621.awsdns-10.co.uk
mapmyrun.com      nameserver = ns-440.awsdns-55.com
```

- ▶ Now we have the four NS hostname.
We can make resolutions to match IP and NS.

DNS Basics example

7

```
> set type=MX
> mapmyrun.com
Server: ns-748.awsdns-29.net
Addresses: 2600:9000:5302:ec00::1
           205.251.194.236

mapmyrun.com    MX preference = 10, mail exchanger = inbound-smtp.us-east-1.amazonaws.com
mapmyrun.com    nameserver = ns-1360.awsdns-42.org
mapmyrun.com    nameserver = ns-1621.awsdns-10.co.uk
mapmyrun.com    nameserver = ns-440.awsdns-55.com
mapmyrun.com    nameserver = ns-748.awsdns-29.net
```

- ▶ I set the type to MX and again type in the domain name. What we get a mail server responsible for handling emails sent to that domain. The number before them denotes the priority with which to fetch mails. Lower the number, higher the priority.
- ▶ Note that querying from your own dns server may not give you the accurate information every time.

DNS Basics example

8

```
> fr.mapmyrun.com
Server:  UnKnown
Address: 192.168.0.254

Non-authoritative answer:
fr.mapmyrun.com canonical name = mapmyrun.com
```

- ▶ I set the type to CNAME and I search the subdomain **fr.mapmyrun.com**. I get a canonical name as **mapmyrun.com**. This means any request to the queried domain (in this case **fr.mapmyrun.com**) will be redirected to **mapmyrun.com**.

DNS Zone Transfers

9

- ▶ MX records indicate where mail should be sent, which tells us that GMail or Google is used. From this, you know that there is a minimum of spam and virus checking in place which helps when sending email for SE or client side attacks.

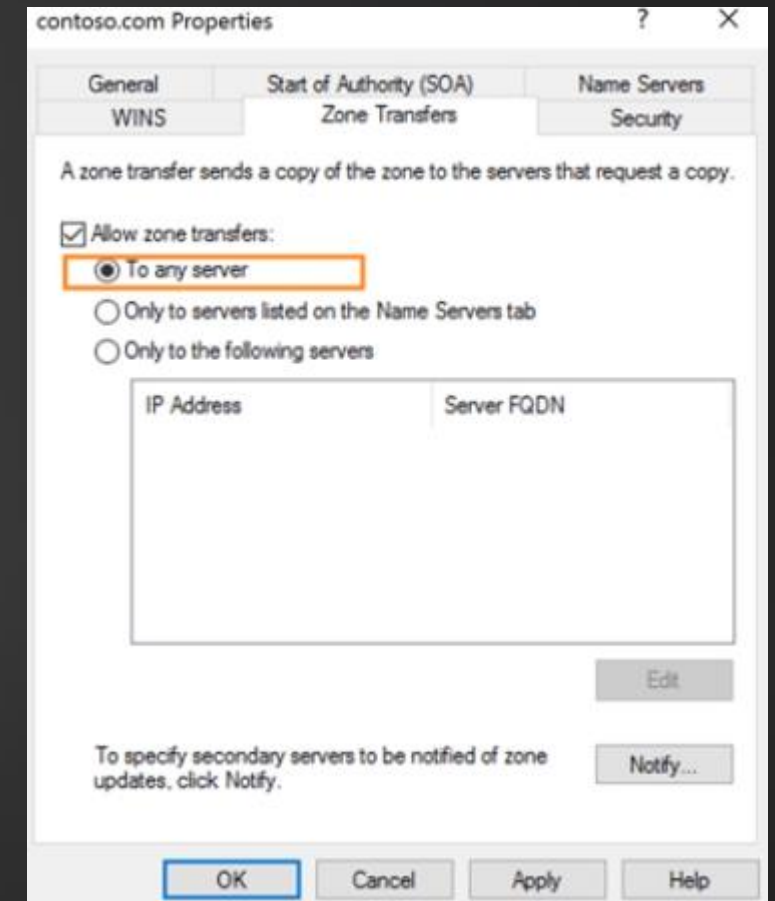
```
dig axfr @nsztml.digi.ninja zonetransfer.me

; <<>> DiG 9.9.5-3ubuntu0.6-Ubuntu <<>> axfr @nsztml.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.      7200    IN      SOA     nsztml.digi.ninja. robin.digi.ninja. 2014101601 172800 900 1209600 3600
zonetransfer.me.      300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.      301     IN      TXT     "google-site-verification=tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA"
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.
```

DNS Zone Transfers : Security issue

10

- ▶ Microsoft DNS example on bad DNS admin side with the following screenshot:
- ▶ On pentest side with an enumeration it's easy to detect all DNS lookup zones on domain controllers running DNS in a forest.



DNS Zone Transfers :

Why this matters

- ▶ DNS server contains a map of all the computers, IP addresses, services in your network and maybe a lot of other sensitive information.
- ▶ Many tools can be used to perform such activities:
 - ▶ nslookup
 - ▶ dig
 - ▶ dnsrecon
 - ▶ dnsenum
 - ▶ nmap
 - ▶ fierce
- ▶ Secure an Internal DNS server to prevent reconnaissance using DNS from occurring can be accomplished by disabling or restricting zone transfers only to specified IP addresses.

DNS Zone Transfers Security

12

- ▶ Only allow zone transfer to the trusted DNS servers (which host the secondary zones).
- ▶ Zone transfer settings are server specific and restrictions should be applied to all affected DNS servers.
- ▶ Create a process to document DNS Primary zone and secondary zone relationships.
- ▶ Create a process to document all DNS server changes: remove unwanted IP addresses from the zone transfer allowed IP addresses if the secondary servers have been retired.

