

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

DNS

Email: ispinoula@ionio.gr
akourtesis@ionio.gr

Τρίτη 10/11/2026

Ιστορία DNS

- Πριν το DNS το διαδίκτυο χρησιμοποιούνταν σχεδόν αποκλειστικά σε ακαδημαϊκά πλαίσια
- Η επικοινωνία μεταξύ των υπολογιστών επιτυγχάνεται μέσω των διευθύνσεων IP, όμως η απομνημόνευσή τους δεν είναι εύκολη, για αυτό προτιμήθηκε η χρήση των domain names
- Η διαδικασία αντιστοίχισης των IP διευθύνσεων σε hostnames γινόταν μέσω ενός αρχείου (hosts.txt) που διανεμόταν στους υπολογιστές των χρηστών του διαδικτύου
- Με την ευρεία εξάπλωση του διαδικτύου, η τεχνική αυτή δεν ήταν πλέον βιώσιμη και οδήγησε το 1983 στη δημιουργία του DNS από τον Paul Mockapetris [1]

DNS

- Το Domain Name System είναι ένα πρωτόκολλο επιπέδου εφαρμογής, υπεύθυνο για την αντιστοίχιση των domain names σε διευθύνσεις IP
- Συγκεκριμένα, το DNS είναι μια κατανεμημένη βάση δεδομένων, υλοποιημένη πάνω σε μια ιεραρχία DNS servers
- Για την υποβολή ερωτημάτων στη βάση αυτή χρησιμοποιείται ένα πρωτόκολλο επιπέδου μεταφοράς (συνήθως UDP) [1][2]

DNS-Records

- Σε κάθε τύπο εγγραφής (record) σε ένα DNS zone αποθηκεύονται διαφορετικά είδη δεδομένων. Τα πιο βασικά record types είναι τα εξής:

❑ A: Αντιστοιχίζει τα domain names σε IPv4 διευθύνσεις

❑ AAAA: Αντιστοιχίζει domain names σε IPv6 διευθύνσεις

❑ CNAME: Αντιστοιχίζει ένα domain name με ένα άλλο με τη χρήση alias. (Για παράδειγμα, αντί να έχουμε ξεχωριστό A record για το www.example.com και για το product.example.com, ορίζουμε το product.example.com ως CNAME που δείχνει στο www.example.com. Έτσι, αν αλλάξει η IP, αρκεί να ενημερωθεί μόνο το A record του www.example.com[6])

DNS-Records

- MX: Ορίζει τους mail servers (με προτεραιότητα) που δέχονται email για ένα domain
- NS: Περιέχει τις ονομασίες των authoritative name servers ενός zone
- PTR: Αντιστοιχίζει μια διεύθυνση IP σε ένα domain name (αντίστροφη αναζήτηση)
- SOA: Περιέχει πληροφορίες διαχείρισης ενός domain
- TXT: Αποθηκεύει κείμενο, συνήθως για αυθεντικοποίηση email και επαλήθευση ιδιοκτησίας domain [5][6]

Table 4. Common DNS resource record types.

Type	Description
A	Maps a domain name to an IPv4 address.
AAAA	Maps a domain name to an IPv6 address.
CNAME	Specifies an alias for a name. If a CNAME exists for a name, incoming queries for that name are translated into queries for the name that the CNAME points to. For example: if there exists a CNAME that maps the name foo to the name bar, then a query for the A record for foo will effectively be treated as an A query for bar. CNAMEs may be chained, that is: a CNAME may point to another CNAME.
MX	Specifies Mail eXchange records for a name. These are the servers that handle incoming e-mail for a domain. Mail servers attempt to deliver e-mail sent to user@example.com to the servers specified in the MX records for example.com.
NS	Specifies the names of authoritative name servers for a domain name.
PTR	Pointer record from a domain name to another domain name. This record type is most commonly used for reverse DNS, to map e.g. IP addresses to domain names (see Section 2.2.1).
SOA	Start Of Authority record. The SOA record specifies metadata about a DNS zone, such as the serial number of the DNS zone. DNS zones are explained in more detail further along in the section.
TXT	Text record. TXT records may contain arbitrary text strings with a maximum length of 255 characters each. TXT records are, for example, used for the so-called Sender Policy Framework (SPF) [44], which is designed to combat e-mail forgery.

https://www.sciencedirect.com/science/article/pii/S1574013722000132#sec2

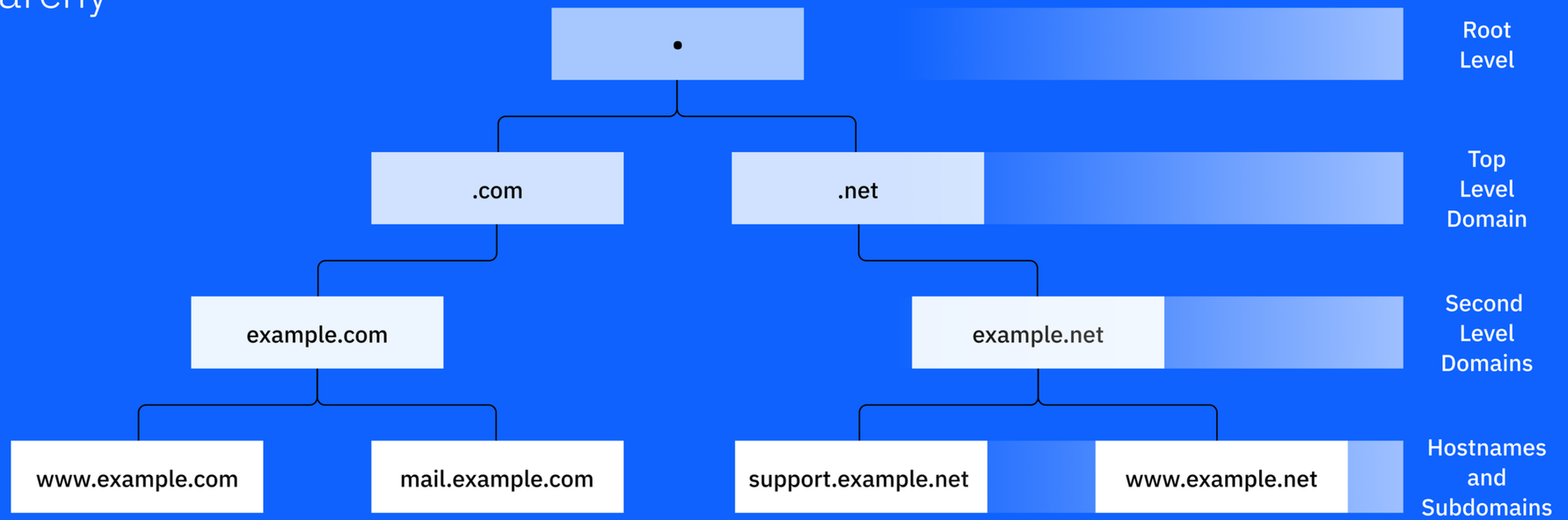
DNS - Λειτουργία

- Το DNS χρησιμοποιείται από πρωτόκολλα επιπέδου εφαρμογής, όπως το HTTP, για τη μετάφραση των domain names που δίνει ένας χρήστης (πχ example.com) σε IP διευθύνσεις
- Παράδειγμα – www.example.gr
  - Ο υπολογιστής μου πρέπει να εντοπίσει την κατάλληλη IP για να στείλει αίτημα HTTP/ HTTPS
  - 1. Ελέγχεται το DNS cache του browser/OS, αν υπάρχει εκεί η IP
  - 2. Αν δεν βρεθεί στην cache, τότε ο υπολογιστής «ρωτάει» τον recursive resolver, που αναλαμβάνει την υπόλοιπη διαδικασία εύρεσης της IP [1]

Recursive resolver/server

- Οι recursive resolvers διαχειρίζονται από ISPs ή public DNS service (πχ Google DNS (8.8.8.8))
- Οι resolvers αποθηκεύουν για ένα συγκεκριμένο χρονικό διάστημα (TTL) πρόσφατες αναζητήσεις
- Αν ο resolver δεν έχει την IP, τότε συνεχίζει τα αιτήματα ιεραρχικά μέχρι να τη βρει [1]

DNS
Hierarchy



https://www.ibm.com/think/topics/dns

DNS Hierarchy – Root (.)

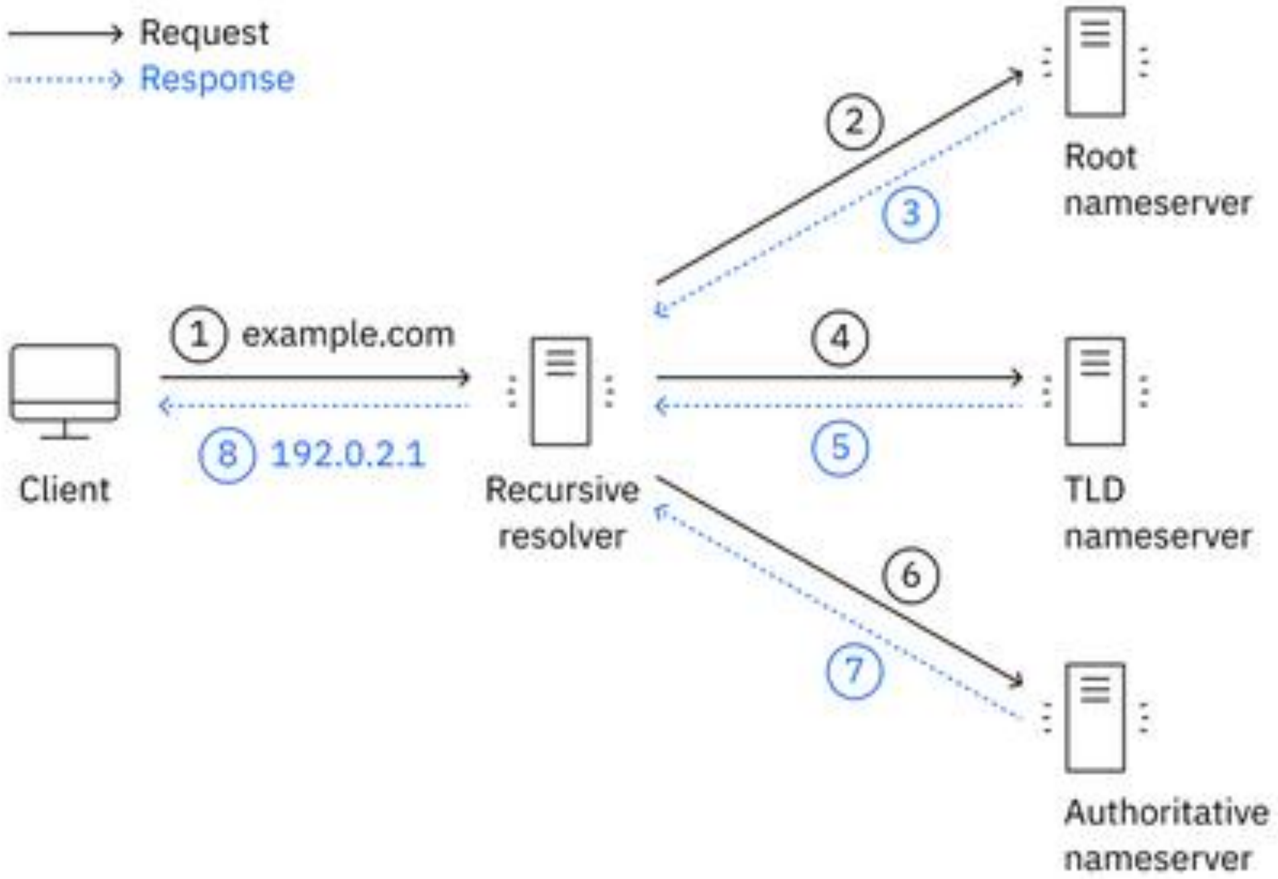
- Η αναζήτηση της IP από τον resolver ξεκινάει από τον root server
- Οι Root name servers δεν γνωρίζουν την IP αλλά γνωρίζουν τις διευθύνσεις των TLD servers (.com, .gr κτλ)
- Υπάρχουν 13 βασικά root server identities (περίπου 2000 αντίγραφά τους διασκορπισμένα στον πλανήτη), με identifiers A-M [1][2]

DNS Hierarchy – TLD (.com)

- Οι Top-Level Domain (TLD) είναι υπεύθυνοι για τα domain names που ανήκουν σε ένα συγκεκριμένο extension (.com, .gr, .gov)
- Για παράδειγμα, αν ψάχνουμε το «example.gr» (second-level domain), ο TLD server του .gr θα κατευθύνει τον resolver στον authoritative DNS server που περιέχει το domain name που ψάχνει [2]

DNS Hierarchy – Authoritative DNS Servers

- Οι Authoritative DNS Servers περιέχουν την τελική απάντηση για τα ονόματα μιας zone (π.χ. την IP του www.example.gr)
- Κάθε οργανισμός μπορεί να υλοποιήσει έναν δικό του Authoritative DNS Server ή να πληρώσει κάποιον πάροχο [2]



https://www.ibm.com/think/topics/dns

DNS- BIND

- Το πιο συνηθισμένο λογισμικό υλοποίησης DNS servers είναι το BIND9 (Berkeley Internet Name Domain). Υπάρχουν και άλλα όπως το Knot DNS, CoreDNS και το NSD, με διαφορετικές δυνατότητες
- Μπορεί να υλοποιήσει τόσο authoritative name servers όσο και resolvers, ακόμα και servers και με τις δύο ιδιότητες [7]
- Είναι open source και λειτουργεί πάνω σε Linux, BSD, macOS, και Windows
- Υποστηρίζει όλα τα DNS record types και DNSSEC
- Το βασικότερο αρχείο του είναι το named.conf στο οποίο ορίζεται ο τύπος και η συμπεριφορά του server και τα zones (domain+domain data) που εξυπηρετεί
- Επίσης σημαντικά είναι και τα zone files που περιέχουν τα records κάθε domain

Παράδειγμα σύνταξης:

named.conf:

```
options {
    directory "/var/cache/bind";
    listen-on { 192.0.2.1; };
    recursion no;                 // authoritative-only, avoids open resolver abuse
    allow-transfer { 192.0.2.2; }; // only your secondary may copy zones
};

zone "example.com" {
    type primary;                 // older versions use "master"
    file "/etc/bind/zones/db.example.com";
};
```

zone file:

```
$TTL 3600
@   IN  SOA ns1.example.com. admin.example.com. (
        2026110801 ; serial
        7200       ; refresh
        3600       ; retry
        1209600    ; expire
        3600 )     ; negative cache TTL

    IN  NS   ns1.example.com.
    IN  NS   ns2.example.com.
    IN  MX   10 mail.example.com.

ns1  IN  A     192.0.2.1
ns2  IN  A     192.0.2.2
www  IN  A     192.0.2.10
mail IN  A     192.0.2.20
blog IN  CNAME www
@    IN  TXT   "v=spf1 mx -all"
```

DNS

Πώς δημιουργείται ένας DNS server;

- Για παράδειγμα, σε ένα μηχάνημα Linux με στατική IP εγκαθιστούμε το BIND9
- Συμπληρώνουμε κατάλληλα το named.conf όπως στην προηγούμενη διαφάνεια
- Στο named.conf.local φτιάχνουμε ένα zone, πχ example.com
- Μετά δημιουργούμε το zone file όπως πριν, με τα records (MX, A, NS, CNAME κτλ)
- Μετά εκκινούμε την υπηρεσία και χρησιμοποιούμε κανονικά τον server

Σχετικό εργαστήριο στο SEEDLABS: **DNS Infrastructure Lab** [8]

DNS DEMO

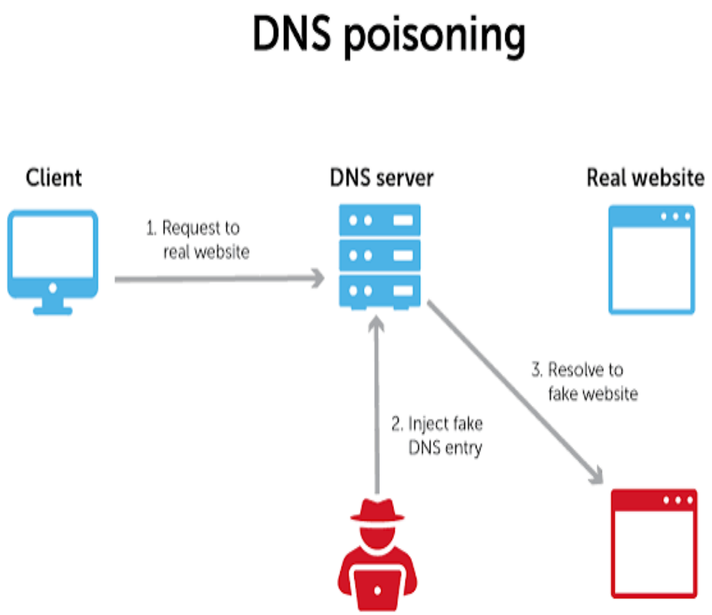
https://messwithdns.net/

https://www.whatsmydns.net/

DNS Attacks

DNS Spoofing

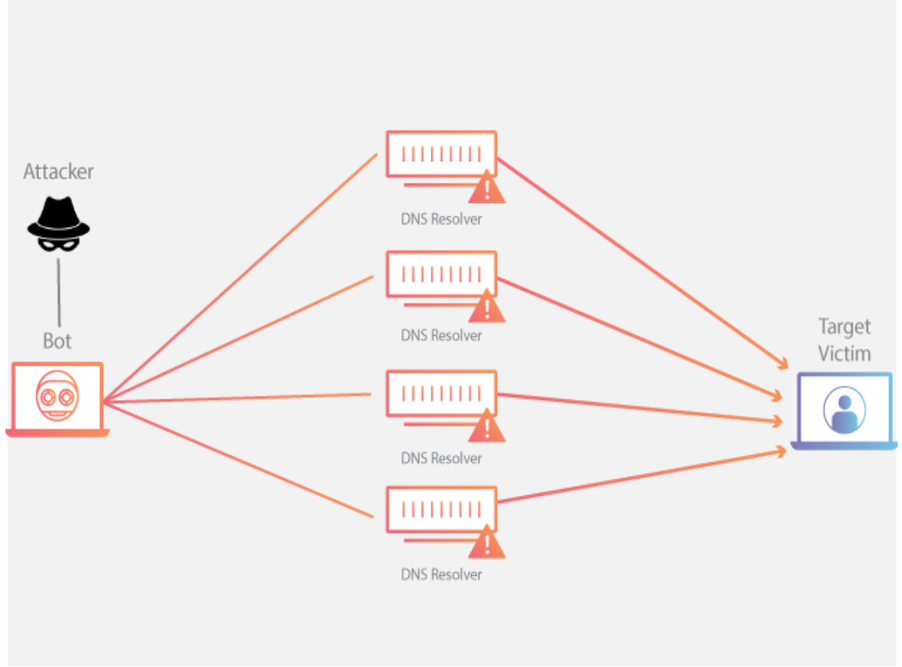
- Το DNS spoofing ή DNS cache poisoning είναι μια επίθεση στην οποία ο attacker αντικαθιστά την IP μιας έγκυρης καταγραφής της cache του DNS resolver ενός πραγματικού domain με μια άλλη που οδηγεί σε μια κακόβουλη ιστοσελίδα
- Η επίθεση αυτή έχει ως στόχο την άντληση πληροφοριών από το θύμα μέσω της κακόβουλης ιστοσελίδας (phishing, credential theft) ή της διάδοσης κακόβουλων λογισμικών [3]



https://www.imperva.com/learn/application-security/cache-poisoning/

DNS amplification attack

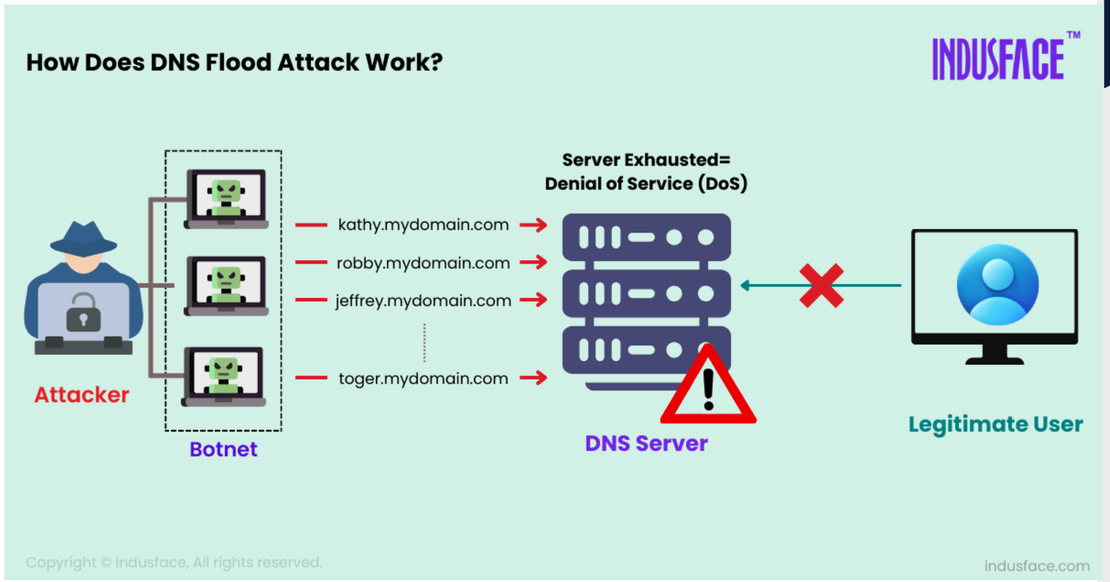
- Η επίθεση αυτή είναι μια μορφή επίθεσης τύπου DDoS
- Ο attacker μέσω spoofing, υποδυόμενος το θύμα, στέλνει πολλά μικρά αιτήματα DNS σε έναν DNS server
- Ως αποτέλεσμα ο DNS server απαντά στο victim με ένα μεγάλο πλήθος απαντήσεων, προκαλώντας αυξημένη κίνηση ή και άρνηση παροχής της υπηρεσίας



https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

DNS flooding

- Σε αυτήν την επίθεση DDoS ο επιτιθέμενος στέλνει πολλά αιτήματα DNS στον server, τόσα ώστε να μην μπορεί να τα διαχειριστεί
- Ως αποτέλεσμα, ο server είτε καθυστερεί αρκετά να απαντήσει σε έγκυρα αιτήματα, είτε δεν απαντάει σε κανένα



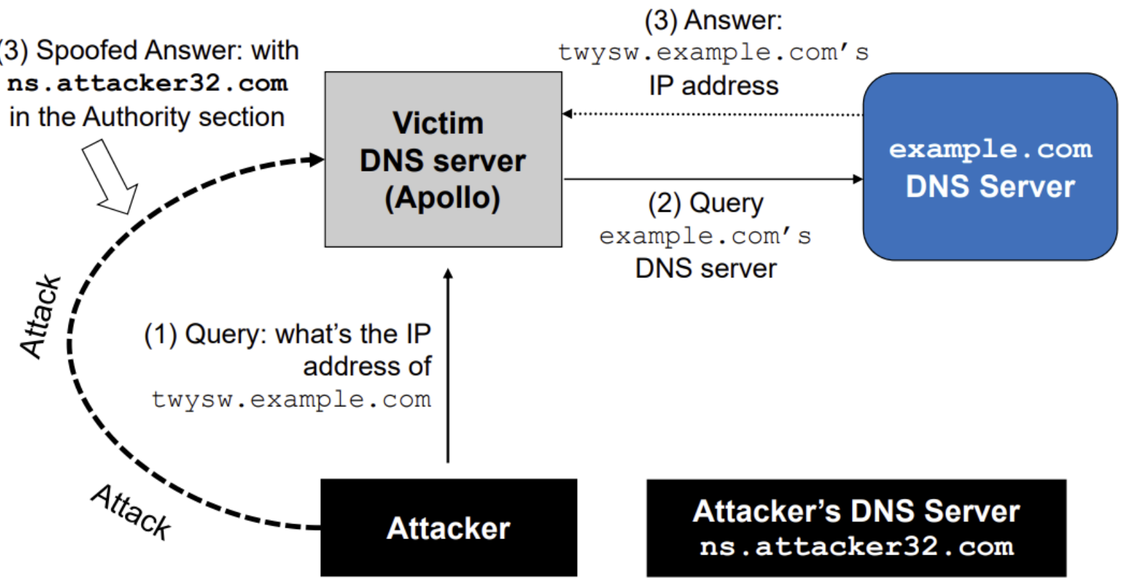
https://www.indusface.com/learning/what-is-dns-flood-attack/

DNS Kaminsky attack

- Ο επιτιθέμενος δημιουργεί έναν δικό του authoritative DNS server ο οποίος περιέχει πλαστά DNS records του domain που επιθυμεί να παραβιάσει
- Αρχικά, στέλνει πολλά αιτήματα για ένα τυχαίο, ανύπαρκτο subdomain του συγκεκριμένου domain που δεν υπάρχει στην cache του recursive DNS resolver
- Ο server θα αρχίσει να ψάχνει την ιστοσελίδα σε authoritative name servers
- Την ίδια στιγμή ο επιτιθέμενος θα αρχίσει να στέλνει πλαστά μηνύματα απάντησης στον συγκεκριμένο resolver μαντεύοντας τη σωστή θύρα και transaction ID κατευθύνοντάς τον στον δικό του ψεύτικο server

DNS Kaminsky attack

- Αν οι απαντήσεις γίνουν δεκτές από τον resolver, αποθηκεύει τις κακόβουλες εγγραφές στην cache και έτσι οποιοδήποτε νέο αίτημα γίνει για το παραβιασμένο domain θα κατευθύνεται στον ψεύτικο server και τις πλαστές IP του [3]



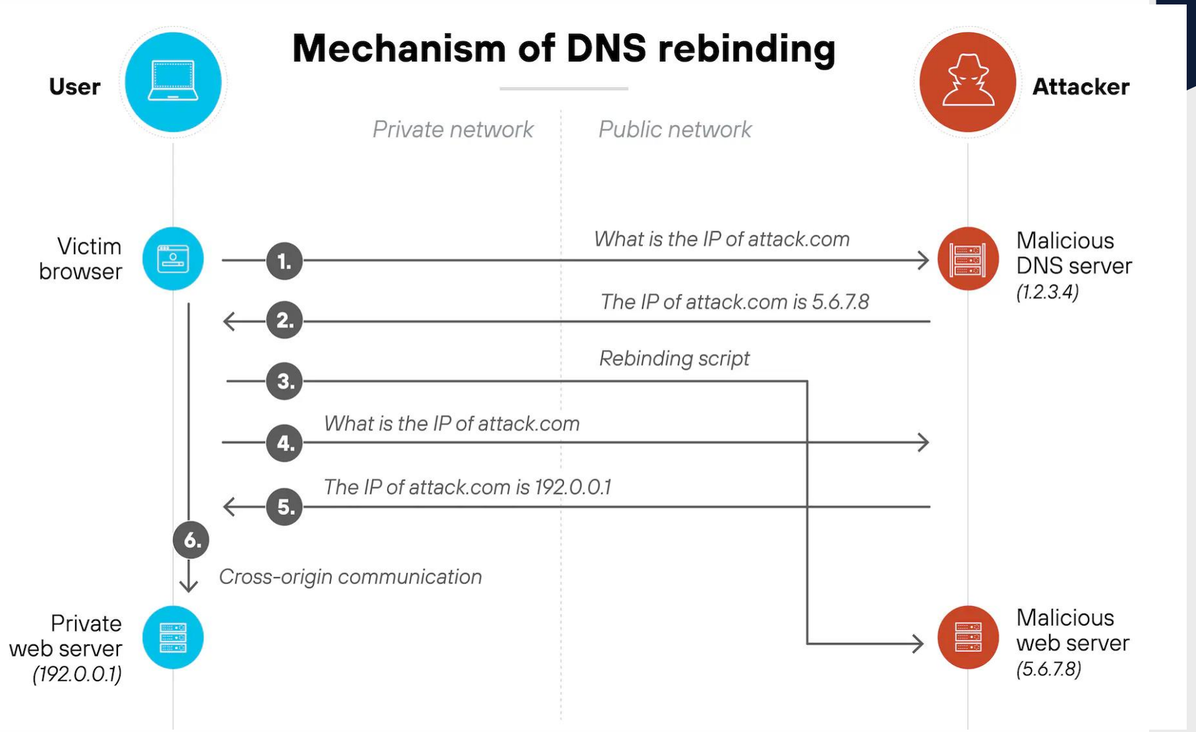
https://seedsecuritylabs.org/Labs_20.04/Files/DNS_Remote/DNS_Remote.pdf

DNS Rebinding

- Ο επιτιθέμενος δημιουργεί ένα κακόβουλο domain (πχ attack.com) και τον αντίστοιχο authoritative DNS server, ώστε να ελέγχει τις DNS απαντήσεις
- Το victim συνδέεται στην ιστοσελίδα του attacker (πχ attack.com) κανονικά με ένα DNS query. Στη σελίδα φορτώνεται κακόβουλος κώδικας JavaScript ο οποίος εκτελείται στον browser
- Ο attacker έχει ορίσει πολύ μικρό TTL, με αποτέλεσμα ο browser να κάνει ξανά DNS query
- Αυτή τη φορά ο DNS server του attacker απαντά με μια εσωτερική IP που έχει επιλέξει εκ των προτέρων (πχ του router ή το localhost)
- Ο browser εξακολουθεί να θεωρεί ότι επικοινωνεί με το attack.com, οπότε το JavaScript στέλνει αιτήματα στη συσκευή του εσωτερικού δικτύου και διαβάζει τις απαντήσεις της

DNS Rebinding

- Ο attacker αποκτά έτσι πρόσβαση σε συσκευές και υπηρεσίες πίσω από το firewall, μέσω του browser του θύματος
- Η επίθεση λειτουργεί επειδή η same-origin policy του browser ελέγχει το όνομα του domain και όχι τη διεύθυνση IP στην οποία αυτό αντιστοιχεί, οπότε η αλλαγή της DNS απάντησης, ενώ η σελίδα παραμένει ανοιχτή, δεν γίνεται αντιληπτή [9]



Mitigation strategies

DNSSEC

- Ένας τρόπος να αποφευχθούν επιθέσεις όπως το spoofing είναι η υλοποίηση του DNSSEC
- Το DNSSEC προσθέτει ψηφιακές υπογραφές σε DNS δεδομένα, συμβάλλοντας στην αυθεντικοποίηση
- Κατά βάση, αξιοποιεί το σύστημα Δημοσίου Κλειδιού, χρησιμοποιώντας ένα ιδιωτικό κλειδί για τη δημιουργία της ψηφιακής υπογραφής και το αντίστοιχο δημόσιο κλειδί που διανέμεται με τη μορφή DNSKEY record [3][4][10]

DNSSEC-Digital Signature

Διαδικασία ψηφιακής υπογραφής:

- Κάθε zone διαθέτει ένα ζεύγος κλειδιών, το ZSK, που υπογράφει τις εγγραφές της zone, και το KSK, που υπογράφει το σύνολο των DNSKEY records (τα δημόσια κλειδιά)
- Για κάθε σύνολο εγγραφών του ίδιου τύπου (πχ όλες οι εγγραφές A) δημιουργείται ένα hash το οποίο υπογράφεται με το ιδιωτικό κλειδί (ZSK). Αυτό είναι το RRSIG record
- Στη συνέχεια, ο resolver έχοντας τα DNSKEY και RRSIG ελέγχει την εγκυρότητα των δεδομένων
- Συγκεκριμένα, κάνει hash τα αντίστοιχα δεδομένα που έχει και «αποκρυπτογραφεί» το RRSIG με το DNSKEY
- Αν τα προκύπτοντα hash είναι τα ίδια τότε τα δεδομένα είναι αυθεντικοποιημένα και ακέραια

DNSSEC-Chain of Trust

- Η ψηφιακή υπογραφή από μόνη της δεν αρκεί, αφού ένας επιτιθέμενος θα μπορούσε να έχει το δικό του DNSKEY
- Για αυτό υπάρχει μια «αλυσίδα εμπιστοσύνης» στην οποία κάθε επίπεδο εγγυάται για το αμέσως επόμενο (θυγατρικό) επίπεδο στην ιεραρχία του DNS
- Σε κάθε επίπεδο της ιεραρχίας τα δεδομένα υπογράφονται ξεκινώντας από το root domain (trust anchor), συνεχίζοντας στο TLD μέχρι και τους authoritative DNS servers

DNSSEC-Chain of Trust

1. Ο resolver έχει το δημόσιο κλειδί του root zone που λειτουργεί ως trust anchor
2. Το root zone υπογράφει τα δεδομένα μαζί με ένα DS (delegation signer) record (hash DNSKEY .com) για τον πχ .com
3. Ο resolver ελέγχει ότι το DNSKEY του .com είναι ίδιο με το DS, επιβεβαιώνοντας ότι μπορεί να «εμπιστευτεί » τον .com
4. Στη συνέχεια ο .com κάνει το ίδιο, δημιουργώντας ένα αντίστοιχο DS record για το DNSKEY του πχ example.com και μετά ο resolver ελέγχει και πάλι το DS και το συγκρίνει με το DNSKEY του example.com
5. Τελικά ο example.com επιβεβαιώνει τα αρχικά δεδομένα, δηλαδή το RRSIG

DNSSEC-Attack Prevention

- Οι προαναφερθείσες επιθέσεις (cache poisoning, Kaminsky attack) δεν θα μπορούσαν να υλοποιηθούν με τη χρήση του DNSSEC, καθώς δεν θα είχαν έγκυρες υπογραφές οπότε ο resolver θα απέρριπτε τις απαντήσεις τους
- Αντίθετα, δεν εμποδίζει τις επιθέσεις flooding, amplification που κάνουν κατάχρηση πόρων χωρίς να παραποιούν DNS δεδομένα . Επίσης, δεν αντιμετωπίζει ούτε το rebinding, αφού ο attacker διαχειρίζεται τους servers, άρα έχει τα δικά του έγκυρα δημόσια κλειδιά

Other Strategies

- Rate Limiting: Περιορίζει τον αριθμό των DNS απαντήσεων προς συγκεκριμένους προορισμούς, μειώνοντας τον κίνδυνο επιθέσεων DNS Amplification και Flooding [1]
- Two-factor Authentication (2FA): Η ενεργοποίηση του 2FA στους λογαριασμούς των domain registrars δυσκολεύει την απόκτηση μη εξουσιοδοτημένης πρόσβασης και μειώνει τον κίνδυνο παραβίασης (domain hijacking). [1]

References

[1] China, C. R., & Goodwin, M. (2025, November 4). What is DNS (Domain Name System)? IBM. https://www.ibm.com/think/topics/dns

[2] Kurose, J. F., & Ross, K. W. (2021). Δικτύωση υπολογιστών: Προσέγγιση από πάνω προς τα κάτω (8η έκδ., Α. Μ. Τροχάνης, Μετάφρ.). Εκδόσεις Μ. Γκιούρδας.

[3] Kim, T. H., & Reeves, D. (2020). A survey of domain name system vulnerabilities and attacks. Journal of Surveillance, Security and Safety, 1, 34–60. https://doi.org/10.20517/jsss.2020.14

[4] IBM. (n.d.). How is DNSSEC different from encryption? https://www.ibm.com/think/topics/dnssec-vs-dns

[5] van der Toorn, O., Müller, M., Dickinson, S., Hesselman, C., Sperotto, A., & van Rijswijk-Deij, R. (2022). Addressing the challenges of modern DNS: A comprehensive tutorial. Computer Science Review, 45, Article 100469. https://doi.org/10.1016/j.cosrev.2022.100469

[6] Quiroz-Vázquez, C., & Goodwin, M. (n.d.). What are DNS records? IBM. https://www.ibm.com/think/topics/dns-records

[7] Internet Systems Consortium. (n.d.). Introduction to DNS and BIND 9. BIND 9 documentation. https://bind9.readthedocs.io/en/latest/chapter1.html

[8] SEED Project. (n.d.). DNS infrastructure lab. https://seedsecuritylabs.org/Labs_20.04/Networking/DNS/DNS_Infrastructure/

[9] Palo Alto Networks. (n.d.). What is DNS rebinding? Examples + protection tips. https://www.paloaltonetworks.com/cyberpedia/what-is-dns-rebinding

[10] IBM. (n.d.). What is DNSSEC? https://www.ibm.com/think/topics/dnssec