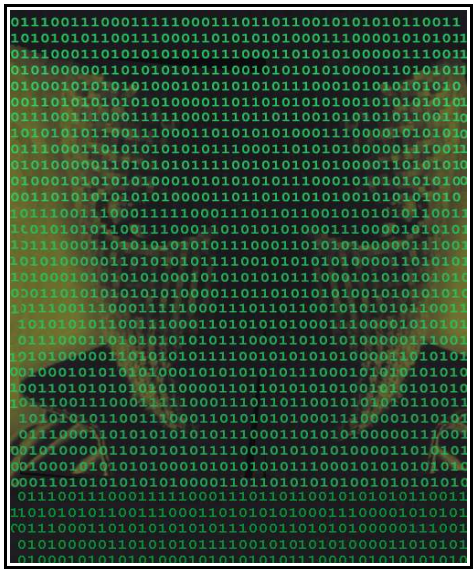
ΚΕΦΑΛΑΙΟ 3

ICMP Echo Spoofing



Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Το *ICMP* πρωτόκολλο είναι ένα πολύ χρήσιμο εργαλείο για την σωστή λειτουργία του Internet, καθώς βοηθάει στην απασφαλμάτωση λαθών που μπορούν να συμβούν κατά την ανταλλαγή IP πακέτων, που παίρνουν μέρος στην επικοινωνία μεταξύ διασυνδεδεμένων συστημάτων.
Συγχρόνως όμως το *ICMP* μπορεί να αποβεί ένα πολύ ισχυρό εργαλείο στα χέρια κακόβουλων χρηστών και να χρησιμοποιηθεί σε διάφορες δικτυακές επιθέσεις.

Όσο αναφορά τις δικτυακές επιθέσεις το *Icmp* μπορεί να χρησιμοποιηθεί για :

- Scanning – Network Mapping.
- OS Fingerprinting
- Decoy Traffic
- Denial of Service Attacks (DoS), Distributed Denial of Service Attacks (DDoS).
- Tunneling - Covert Channels.

Σε κάθε δικτυακή επίθεση και γενικότερα σε κάθε κακόβουλη ενέργεια που συμβαίνει στο Internet, ο επιτιθέμενος έχει σαν πρωταρχική έγνοια, να καλύψει τα ίχνη του ώστε να μην γίνει αντιληπτός από τον στόχο του.
Μία πολύ διαδεδομένη τεχνική για να το καταφέρει αυτό είναι το ***spoofing***, δηλαδή η χρήση ψεύτικης διεύθυνσης αποστολέα στα πακέτα που στέλνει.
Το γεγονός ότι το *Icmp* είναι ένα connectionless πρωτόκολλο κάνει ποιο εύκολη την χρήση του για *spoofing*, καθώς ο αποστολέας δεν χρειάζεται να έχει συνάψει σύνδεση με τον παραλήπτη ώστε να του στείλει κάποια πακέτα. Δηλαδή δεν απαιτείται η διαδικασία του 3 Way Handshake, όπως συμβαίνει με τις συνδέσεις που πραγματοποιούνται με το TCP πρωτόκολλο.
Φυσικά ο επιτιθέμενος δεν θα έχει την δυνατότητα να πάρει απαντήσεις για τα *spoofed* πακέτα που στέλνει, καθώς αυτές θα επιστρέφονται στον host του οποίου η IP διεύθυνση χρησιμοποιήθηκε σαν διεύθυνση αποστολέα στα *spoofed* πακέτα.
Αυτό όμως στις περισσότερες περιπτώσεις δεν είναι πρόβλημα για τον επιτιθέμενο, είτε γιατί δεν τον ενδιαφέρει να πάρει αυτές τις απαντήσεις, είτε γιατί μπορεί να παίρνει αυτές τις απαντήσεις με κάποιον άλλο τρόπο (πχ. sniffing).

Σε αυτό το Κεφάλαιο γίνεται η περιγραφή του *Icmp Echo spoofing* όταν αυτό συμβαίνει σε δικτυωμένα συστήματα.

*Ο όρος **Icmp Echo spoofing** αναφέρεται στην διαδικασία κατά την οποία κάποιος στέλνει Icmp Echo Request ή Icmp Echo Reply πακέτα σε έναν άλλο χρησιμοποιώντας ψεύτικη διεύθυνση αποστολέα.*

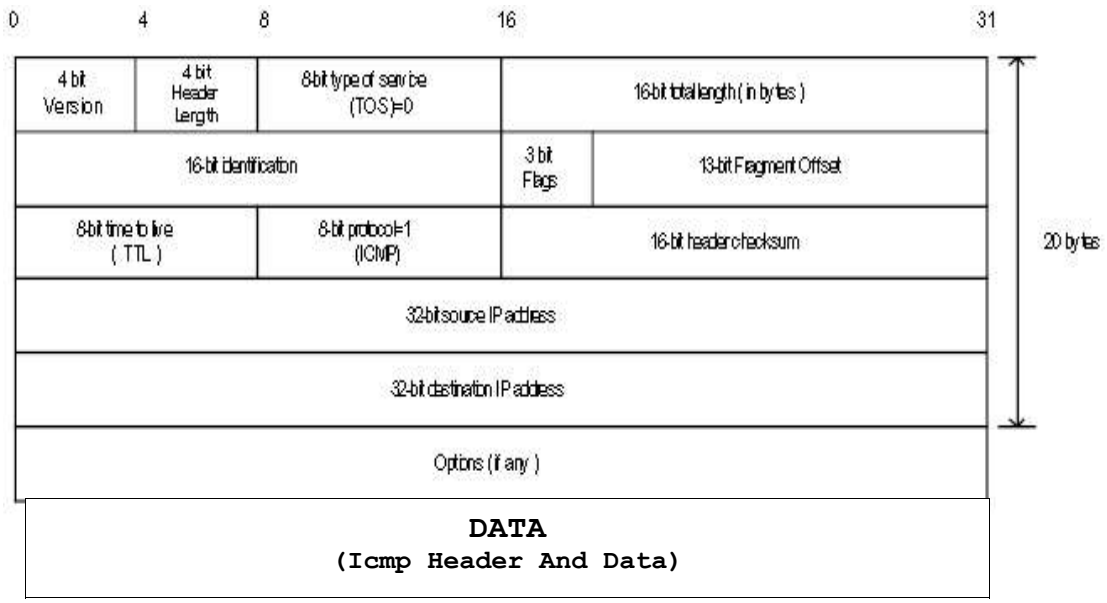
Στο ΜΕΡΟΣ Α γίνεται μία συνεπτυγμένη αναφορά στο *Icmp* πρωτόκολλο, με έμφαση στα *Icmp* πακέτα που παίρνουν μέρος στην διαδικασία του *Icmp Echo spoofing*.

Στο ΜΕΡΟΣ Β περιγράφεται το *Icmp Echo spoofing* αναλυτικά, καθώς και πως διαφέρει η λειτουργία του από την αποστολή των νόμιμων *Icmp Echo* πακέτων.
Επίσης γίνεται αναφορά στις επιπτώσεις από την χρήση του *Icmp Echo spoofing*, αναφέροντας μερικές γνωστές τεχνικές και δικτυακές επιθέσεις που στηρίζονται σε αυτό.

ΜΕΡΟΣ Α: Το *ICMP* Πρωτόκολλο

➢ Γενικά

Το *ICMP* (**I**nternet **C**ontrol **M**essage **P**rotocol) είναι ένα σχετικά απλό στην λειτουργία του πρωτόκολλο και χρησιμοποιεί το *IP* (**I**nternet **P**rotocol) για την μεταφορά του όπως και άλλα πρωτόκολλα ανωτέρων επιπέδων (πχ TCP), με την διαφορά όμως ότι θεωρείται εσωτερικό κομμάτι του *IP* και πρωτόκολλο επιπέδου δικτύου όπως και το *IP*. Στο παρακάτω σχήμα παρουσιάζεται το *IP* πακέτο που περιέχει στα data του ένα *Icmp* πακέτο.



Σχήμα Α-1: IP Header and Data

Το *IP* σαν πρωτόκολλο επικοινωνίας δεν είναι σχεδιασμένο έτσι ώστε να αποτελεί έναν απόλυτα αξιόπιστο τρόπο μεταφοράς πακέτων. Κύριος στόχος του *Icmp* είναι να αποτελέσει ένα μηχανισμό υποστήριξης του *IP* και επισήμανσης λαθών που μπορεί να συμβούν κατά την μεταφορά ενός IP πακέτου. Παρόλα αυτά το *Icmp* δεν έχει σαν στόχο να κάνει το *IP* απόλυτα αξιόπιστο, εξασφαλίζοντας την από άκρο σε άκρο (end to end) ασφαλή μεταφορά των πακέτων, καθώς ένα IP πακέτο μπορεί και πάλι να μην φτάσει στον προορισμό του χωρίς να επισημανθεί το γεγονός. Κάθε πρωτόκολλο ανωτέρων επιπέδων που χρησιμοποιεί το *IP*, όπως για παράδειγμα το TCP, είναι υπεύθυνο να υλοποιεί τους δικούς του μηχανισμούς που εξασφαλίζουν μία αξιόπιστη επικοινωνία, αν αυτή απαιτείται.
Κύρια μέριμνα του *Icmp* είναι απλά να επισημάνει κάποιο πρόβλημα που παρουσιάστηκε κατά την μεταφορά του *IP* πακέτου.

Το *ICMP* έχει δύο κύριες χρήσεις :

- Για να πληροφορήσει με *Icmp Error* μηνύματα κάποιος router ή ο παραλήπτης ενός πακέτου τον αποστολέα του πακέτου, για λάθη που συνέβησαν κατά την επεξεργασία του πακέτου αυτού.

Ένα παράδειγμα τέτοιου πακέτου είναι το *Icmp Destination Unreachable - Net Unreachable* που στέλνει ένας router στον αποστολέα κάποιου πακέτου, δηλώνοντάς του ότι το πακέτο που έστειλε δεν μπορεί να δρομολογηθεί στο δίκτυο στο οποίο το έστειλε, είτε γιατί αυτό δεν υπάρχει, είτε γιατί ο router δεν γνωρίζει πως να το δρομολογήσει σε αυτό.

- Για να διερευνηθεί κάποιο δίκτυο με *Icmp Query* μηνύματα για διάφορα χαρακτηριστικά του, με την προϋπόθεση ότι θα επιστραφούν κάποιες απαντήσεις.
  Ένα παράδειγμα τέτοιου πακέτου είναι το *Icmp Echo Request,* το οποίο στέλνεται από κάποιον Host για να ανακαλύψει αν ο υποψήφιος παραλήπτης του πακέτου υπάρχει.
  Ο παραλήπτης αυτού του πακέτου, εφόσον υπάρχει, θα απαντήσει στον αποστολέα του *Icmp Echo Request* με ένα *Icmp Echo Reply* πακέτο.

Για την υποστήριξη των παραπάνω λειτουργιών, τα *Icmp* μηνύματα χωρίζονται σε δύο κατηγορίες όπως φαίνονται στο παρακάτω σχήμα :

ICMP Query Messages	ICMP error Messages
Echo	Destination Unreachable
Router Advertisement	Source Quench
Router Solicitation	Redirect
Time Stamp	Time Exceeded
Information	Parameter Problem
Address Mask	

Σχήμα Α-2: Είδη Icmp μηνυμάτων

Μερικά γενικά χαρακτηριστικά των *Icmp* μηνυμάτων είναι :

- Κάθε *Icmp* πακέτο χαρακτηρίζεται από ένα πεδίο που δηλώνει τον τύπο του (*Type*) , ένα πεδίο που δηλώνει τον κωδικό του (*Code*) και ένα πεδίο (*Checksum*) που χρησιμοποιείται για τον υπολογισμό ενός αριθμού που δηλώνει την ορθότητα του *Icmp* πακέτου.

- Τα *Icmp* πακέτα ενσωματώνονται στα data του IP datagram (**Σχήμα Α-1**).

- Τα *Icmp* μηνύματα δημιουργούνται είτε από κάποιον host ή κάποιον router και έχουν πάντα προορισμό τον Host που έστειλε το αρχικό πακέτο, το οποίο οδήγησε στην δημιουργία του *Icmp* μηνύματος.

- *Icmp* μηνύματα δεν μπορούν να δημιουργούνται σαν απάντηση σε άλλα *Icmp* μηνύματα, εκτός εάν τα τελευταία ανήκουν στην κατηγορία των *Icmp Query* μηνυμάτων.

- Ένα *Icmp Error* μήνυμα δεν πρέπει ποτέ να δημιουργείται ως αποτέλεσμα λήψης :

  - Ενός άλλου *Icmp Error* μηνύματος.

    Κάτι τέτοιο πρέπει να ισχύει καθώς αν ένα *Icmp Error* μήνυμα παράγει ένα άλλο, τότε και αυτό θα δημιουργήσει ένα άλλο και ού το κάθε εξής και η όλη διαδικασία θα καταλήξει σε μία αναδρομική λειτουργία, που θα συνεχίζεται επ' άπειρον με απρόβλεπτα αποτελέσματα.

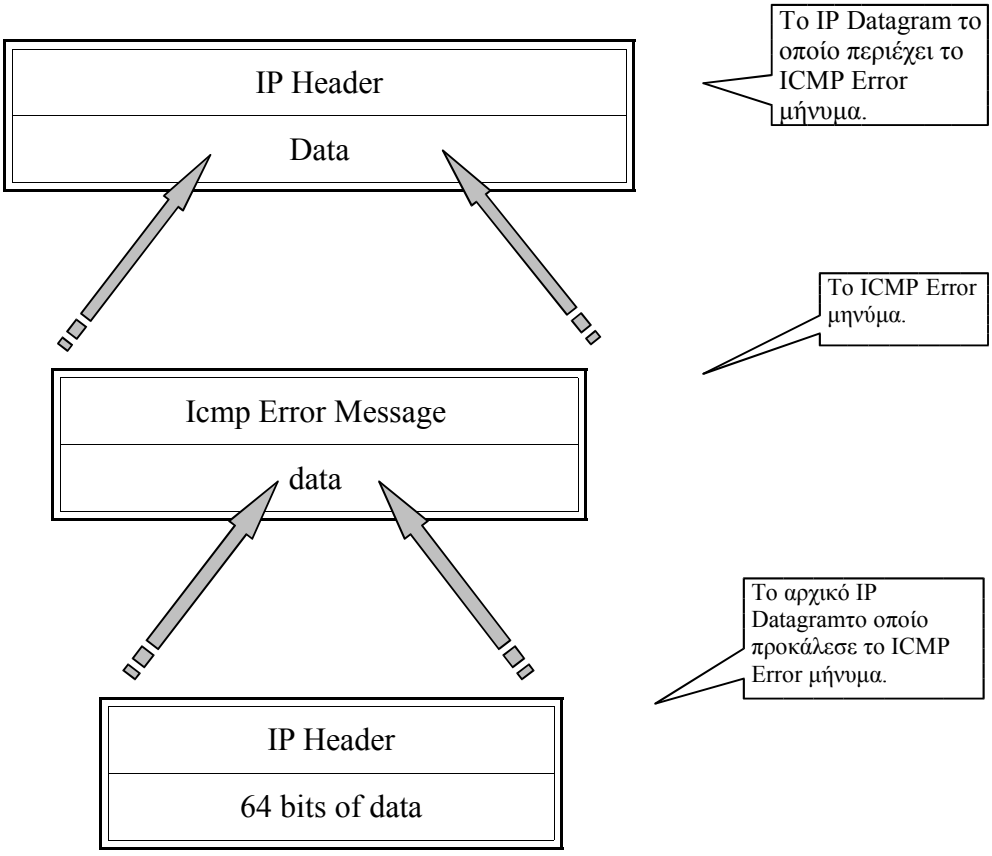
- Ενός πακέτου που δεν προορίζεται σε μία unicast address.

  Τέτοια πακέτα μπορούν να είναι αυτά που προορίζονται σε μία IP Layer , Link Layer Broadcast και Multicast address.

- Οποιουδήποτε fragment ενός IP datagram, εκτός του πρώτου (offset = 0).

- Τα *Icmp Error* μηνύματα πάντα περιέχουν στα data τους τον IP header και τα 64 πρώτα bits των data, του αρχικού IP datagram, το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος (**Σχήμα Α-3**).

Στο παρακάτω σχήμα παρουσιάζεται ο τρόπος με τον οποίο ένα *Icmp Error* μήνυμα ενσωματώνεται μέσα σε ένα IP πακέτο.
Το *Icmp Error* μήνυμα περιέχεται στα Data του IP πακέτου που το μεταφέρει.
Στα Data του *Icmp Error* πακέτου βρίσκονται ο header και τα 64 πρώτα bits των data του αρχικού IP πακέτου που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος.

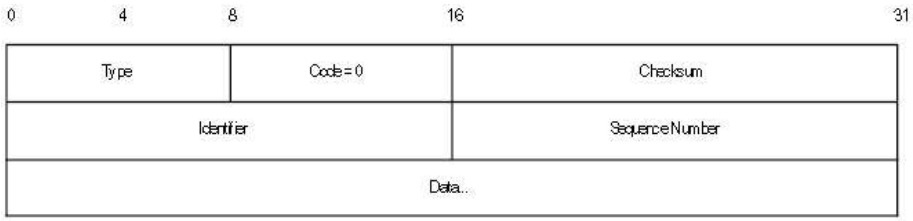


Σχήμα Α-3: Το encapsulation του ICMP Error πακέτου μέσα στο IP πακέτο.

Παρακάτω θα παρουσιαστούν με σχετική λεπτομέρεια τα *Icmp Echo* πακέτα που ανήκουν στην κατηγορία των *Icmp Query* μηνυμάτων και κάποια από τα *Icmp Destination Unreachable* πακέτα που ανήκουν στην κατηγορία των *Icmp Error* μηνυμάτων.

➢ *Το ICMP Echo* Πακέτο.

Στο **Σχήμα Α-4** φαίνεται το *ICMP Echo* πακέτο :



Σχήμα Α-4: Το Icmp Echo

Τα *Icmp Echo* πακέτα είναι τα

- *Icmp Echo Request* (Type 8 , Code 0)
- *Icmp Echo Reply* (Type 0 , Code 0)

Τα *Icmp Echo Request /Reply* πακέτα χρησιμοποιούνται για να ελεγχθεί η διασυνδεσιμότητα μεταξύ δύο hosts. Προκειμένου κάποιος host, έστω ο **A**, να διαπιστώσει αν μπορεί να επικοινωνήσει με έναν άλλο host, έστω τον **B**, θα στείλει σε αυτόν ένα *Icmp Echo Request* πακέτο και αν ο **B** είναι σε θέση να το πάρει, τότε θα απαντήσει στον **A** στέλνοντάς του ένα *Icmp Echo Reply* πακέτο, δηλώνοντας του με αυτόν τον τρόπο ότι είναι συνδεδεμένος στο δίκτυο και ικανός να λάβει μέρος σε μία επικοινωνία.

Μία ευρέως γνωστή εφαρμογή που υλοποιεί αυτή την διαδικασία ονομάζεται ***Ping*** η οποία συνοδεύει τα περισσότερα λειτουργικά συστήματα.

Όταν στέλνεται ένα *Icmp Echo Request,* το πακέτο αυτό ενσωματώνεται στα Data του IP datagram.
Ο παραλήπτης του θα αντιστρέψει την source IP με την destination IP στον IP header και θα στείλει ένα *Icmp Echo Reply*.

Αυτό σημαίνει ότι τα πεδία *Identifier* και *Sequence Number* του *Icmp Echo Reply* πακέτου, θα είναι τα ίδια με αυτά του *Icmp Echo Request*, καθώς αυτά τα πεδία χρησιμοποιούνται από τον αποστολέα του *Request* πακέτου, για να αντιστοιχεί τα *Requests* που στέλνει με τα *Replies* που λαμβάνει.

Σημείωση : Τα πεδία Sequence Number(seq) και Identifier(id) του *Icmp Echo* πακέτου.

Όταν ο Host A στείλει ένα *Icmp Echo Request* στον Host B, θα ορίσει κάποιες τιμές στα πεδία **seq** και **id** του *Icmp* πακέτου.
Ο Host B όταν πάρει αυτό το πακέτο θα δημιουργήσει ένα αντίστοιχο *Icmp Echo Reply* πακέτο με τις ίδιες τιμές (ίδιες με του *Request* πακέτου) σε αυτά τα πεδία και θα το στείλει στον Host A.

Αυτά τα δύο πεδία χρησιμοποιούνται από τον Host A (γενικότερα τον αποστολέα του *Icmp Request* πακέτου) έτσι ώστε να μπορεί να αντιστοιχίσει το κάθε Echo *Reply* που θα πάρει με το αντίστοιχο Echo *Request* που έστειλε .

Το πεδίο **id** περιέχει έναν αριθμό ο οποίος είναι ο ίδιος για κάθε *Icmp Echo Request* που ανήκει στο ίδιο session του Ping που εκτελεί ο Host A.

Το πεδίο **seq** περιέχει έναν αριθμό ο οποίος χαρακτηρίζει την ακολουθία του κάθε *Icmp Echo Request* πακέτου μέσα σε ένα Ping session.Το πρώτο πακέτο έχει **seq** = 0 (όχι πάντα) και για κάθε πακέτο που στέλνεται και ανήκει στο ίδιο session του Ping η τιμή του πεδίου αυτού αυξάνεται κατά 1.

Παράδειγμα
Ο Host A κάνει ένα Ping στον Host B στέλνοντας τρία *Icmp Echo Request* πακέτα. Τα πακέτα αυτά θα έχουν τις εξής τιμές στα πεδία **id , seq**:

Packet 1 : **id** = 04A1 , **seq** = 00 00
Packet 2 : **id** = 04A1 , **seq** = 01 00
Packet 3 : **id** = 04A1 , **seq** = 02 00

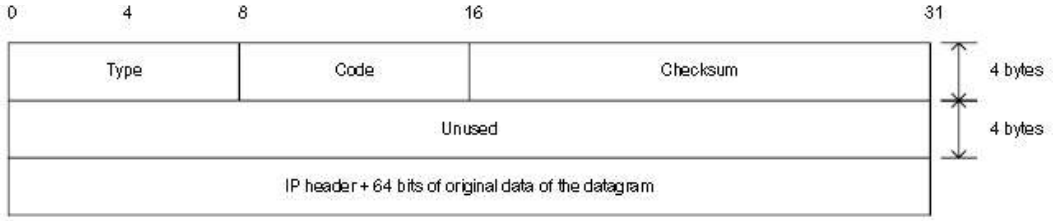
Ο Host B από την πλευρά του θα απαντήσει με τρία Echo Reply πακέτα τα οποία θα έχουν σε αυτά τα πεδία τις ίδιες τιμές με τα παραπάνω πακέτα (*Request*s).

Σημείωση

Αν περιέχονται data στο *Icmp Echo Request* πακέτο τότε αυτά πρέπει να είναι τα ίδια και στο αντίστοιχο *Icmp Echo Reply*.

➢ *Το ICMP Destination Unreachable* Πακέτο

Το *ICMP Destination Unreachable* πακέτο φαίνεται στο παρακάτω σχήμα:



Σχήμα Α-5: Γενική μορφή Icmp Error Message

Τα *Icmp Destination Unreachable* πακέτα ανήκουν στην κατηγορία των *Icmp Error* μηνυμάτων και δημιουργούνται όταν για διάφορους λόγους κάποιο πακέτο δεν ήταν δυνατόν να φτάσει στον προορισμό του ή κάποιο λάθος παρουσιάστηκε κατά την επεξεργασία του από τον παραλήπτη ή κάποιον ενδιάμεσο router που χρειάστηκε να το δρομολογήσει.
Από το **Σχήμα Α-3** φαίνεται ότι το *Icmp Destination Unreachable* πακέτο βρίσκεται μέσα στα Data του IP πακέτου που το μεταφέρει.
Επίσης τα data του *Icmp* πακέτου περιέχουν τον IP header και τα 64 πρώτα bits των data του αρχικού IP datagram που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος.

Δύο είδη τέτοιων πακέτων που παρουσιάζουν ενδιαφέρον για την παρούσα μελέτη είναι :

- Το *Icmp Destination Unreachable – Host*/*Network Unreachable* (type 3 code 0/1)

  Αν ένα τέτοιο πακέτο φτάσει στον αποστολέα ενός πακέτου, αυτό έχει προέλθει από κάποιο router που δρομολόγησε αυτό το πακέτο, δηλώνοντάς του ότι το πακέτο που έστειλε δεν έφτασε στον προορισμό του γιατί ο παραλήπτης (ή το δίκτυό του) δεν υπάρχει.
  Τέτοια πακέτα μπορούν να δημιουργήσουν μόνο routers

- Το *Icmp Destination Unreachable – Administrative Prohibited* (type 3 code 13)

  Αν ένα τέτοιο πακέτο φτάσει στον αποστολέα ενός πακέτου, αυτό έχει προέλθει από το router, δηλώνοντάς του ότι το πακέτο που έστειλε δεν έφτασε στον προορισμό του γιατί εφαρμόστηκε σε αυτό κάποιο είδος πολιτικής ασφάλειας κατά την οποία δεν επιτρέπεται η διέλευση τέτοιων πακέτων
  Τέτοια πακέτα μπορούν να δημιουργήσουν μόνο routers ή firewalls.

Σημείωση

Είναι πιθανό κάποιος router να μην έχει ρυθμιστεί να στέλνει τέτοιου είδους μηνύματα όταν δεν επιτραπεί η διέλευση κάποιου πακέτου και απλά να μην επιτρέψει στο πακέτο να φτάσει στον προορισμό του, χωρίς να πληροφορήσει τον αποστολέα για το γεγονός.

ΜΕΡΟΣ Β: Περιγραφή του *Icmp Echo Spoofing*

Στο ΜΕΡΟΣ Β περιγράφεται η λειτουργία του *Icmp Echo spoofing*, δηλαδή η διαδικασία αποστολής *Icmp Echo Request* και *Icmp Echo Reply* πακέτων που έχουν ψεύτικη διεύθυνση αποστολέα.

Στο κομμάτι **I.** περιγράφεται η φυσιολογική – νόμιμη λειτουργία του *Ping*. Δηλαδή η αποστολή ενός νόμιμου *Icmp Echo Request* πακέτου με σωστή διεύθυνση αποστολέα και τα πακέτα που θα προκύψουν από αυτό στη συνέχεια.

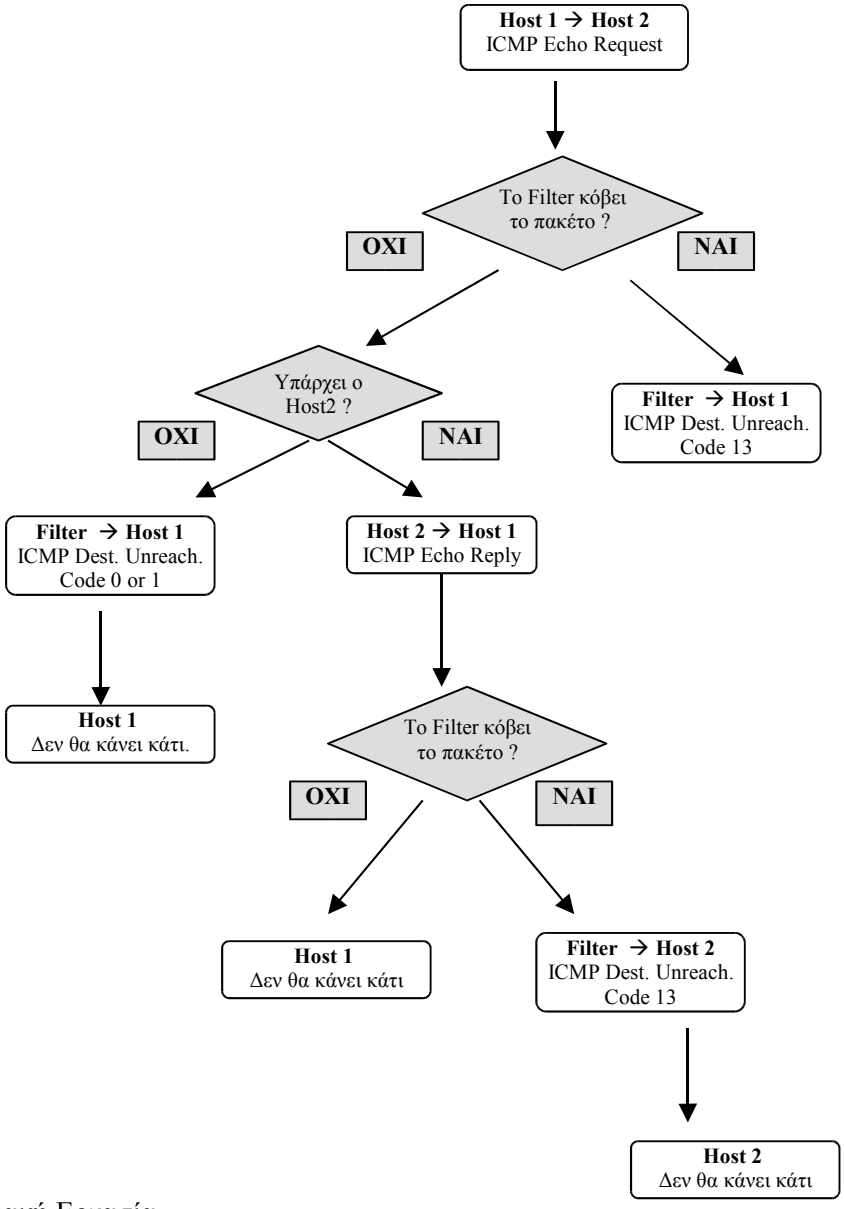
Στο κομμάτι **II.** περιγράφεται η διαδικασία κατά την αποστολή ενός *spoofed Icmp Echo Request* πακέτου (το οποίο έχει ψεύτικη διεύθυνση αποστολέα) και των πακέτων που θα προκύψουν από αυτό, ενώ στη συνέχεια περιγράφεται η διαδικασία κατά την αποστολή ενός *spoofed Icmp Echo Reply* πακέτου και των πακέτων που θα προκύψουν από αυτό.

Σε κάθε περίπτωση θα παρουσιάζεται και ένα διάγραμμα ροής των πακέτων που ανταλλάσσονται μεταξύ των εμπλεκόμενων, καθώς και ένα σχηματικό διάγραμμα, για καλύτερη κατανόηση της διαδικασίας που περιγράφεται.

Στο κομμάτι **III.** περιγράφονται μερικές από τις τεχνικές και τις επιθέσεις, στις οποίες έχει εφαρμογή το *Icmp Echo spoofing* και αναφέρονται οι επιπτώσεις τους στα δικτυωμένα συστήματα που πλήττουν.

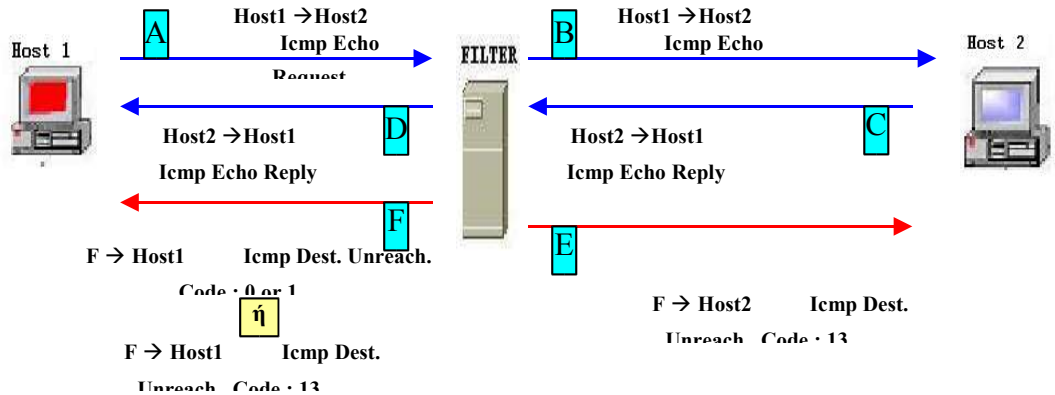
I. Η Διαδικασία κατά την Αποστολή ενός Νόμιμου *Icmp Echo Request* Πακέτου.

Στο **Σχήμα Β-1** που ακολουθεί παρουσιάζεται διαγραμματικά η ροή ενός *Icmp Echo Request* πακέτου, κατά την αποστολή του από τον `Host1` στον `Host2`, καθώς και η ροή των άλλων πακέτων που θα δημιουργηθούν εξαιτίας αυτού.
Το `Filter` (F) είναι ένα μηχάνημα το οποίο δρομολογεί και φιλτράρει τα πακέτα που στέλνονται μεταξύ των hosts που παίρνουν μέρος στην διαδικασία.



Σχήμα Β-1 : Διάγραμμα ροής κατά την αποστολή ενός νόμιμου

Στο παρακάτω σχήμα παρουσιάζεται η ίδια διαδικασία με ένα σχηματικό διάγραμμα.



Σχήμα Β-2: Σχηματικό διάγραμμα κατά την αποστολή ενός νόμιμου *Icmp Echo Request* πακέτου από τον Host1 στον Host2

Περιγραφή της Διαδικασίας

Στα παραπάνω σχήματα απεικονίζεται η λειτουργία του *Ping* που εκτελεί ο `Host1` στον `Host2`. Η διαδικασία αυτή περιγράφεται ως εξής :

[A] Ο `Host1` στέλνει ένα *Icmp Echo Request* πακέτο στον `Host2`.

[F] Αν το `Filter`, που παρεμβάλλεται στη διαδρομή μεταξύ των δύο δεν αφήσει το πακέτο να περάσει λόγω κάποιας πολιτικής ασφάλειας που εφαρμόζει, τότε θα επιστρέψει στον `Host1` ένα *Icmp Destination Unreachable – Administrator Prohibited* πακέτο. Επίσης αν δεν ισχύει αυτό, αλλά ο `Host2` δεν υπάρχει τότε το `Filter` θα επιστρέψει στον `Host1` ένα *Icmp Destination Unreachable – Host/Net Unreachable* πακέτο δηλώνοντάς του το γεγονός. Ο `Host1` στη συνέχεια δεν θα στείλει κάποιο άλλο πακέτο.

[B] Σε περίπτωση που υπάρχει ο `Host2` και το `Filter` επιτρέπει τη διέλευση των *Icmp Echo Request* πακέτων τότε το πακέτο αυτό θα φτάσει στον `Host2`.

[C] Ο `Host2` θα πάρει το πακέτο, θα δημιουργήσει ένα *Icmp Echo Reply* πακέτο και θα το στείλει στον `Host1`.

[**E**] Σε περίπτωση που το `Filter` που παρεμβάλλεται στη διαδρομή μεταξύ των δύο δεν αφήσει το πακέτο να περάσει λόγω κάποιας πολιτικής ασφάλειας που εφαρμόζει, τότε θα επιστρέψει στον `Host2` ένα *Icmp Destination Unreachable – Administrator Prohibited* πακέτο. Ο `Host2` στη συνέχεια δεν θα στείλει κάποιο άλλο πακέτο.

[**D**] Αν το `Filter` επιτρέψει σε αυτό το πακέτο να περάσει, τότε αυτό θα φτάσει στον `Host1`. Ο `Host1` με την σειρά του δεν θα στείλει κάποιο άλλο πακέτο.

Εδώ πρέπει να τονιστεί ότι το *Icmp Echo Reply* πακέτο από τον `Host2` στον `Host1`, θα δημιουργηθεί αφού προηγηθεί πρώτα ένα *Icmp Echo Request* πακέτο με την αντίθετη φορά, δηλαδή από τον `Host1` στον `Host2`.

II. Η Λειτουργία του *Icmp Echo spoofing*.

Σε αυτό το κομμάτι γίνεται η περιγραφή της διαδικασίας του *Icmp Echo spoofing* και όλα τα πιθανά σενάρια που προκύπτουν.

Αρχικά θα παρουσιαστεί ο τρόπος που υλοποιείται το *Icmp Echo Request spoofing* και στην συνέχεια θα γίνει το ίδιο για το *Icmp Echo Reply spoofing*.

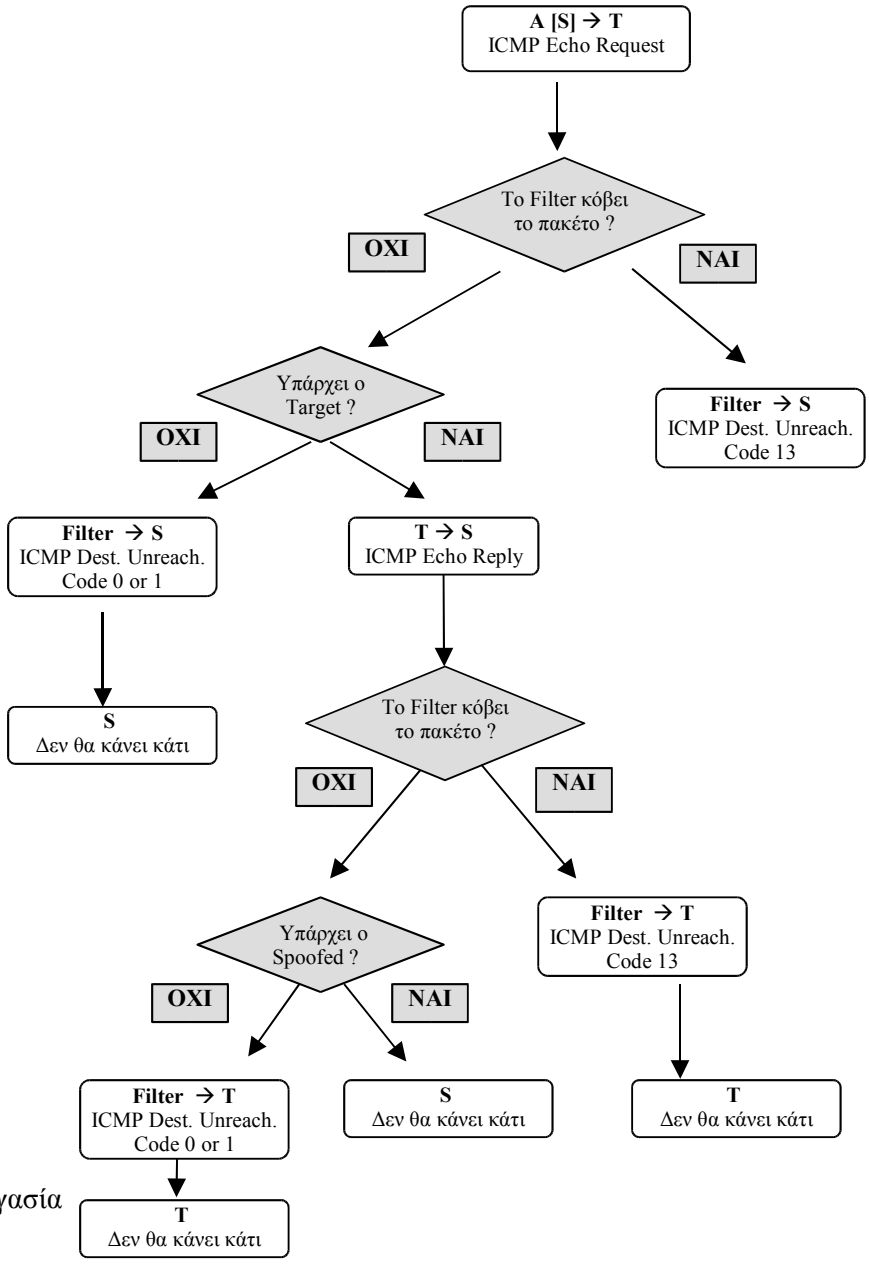
Σε κάθε περίπτωση θα παρουσιάζεται και το αντίστοιχο διάγραμμα ροής των πακέτων που προκύπτουν καθώς και ένα σχηματικό διάγραμμα της διαδικασίας που περιγράφεται.

Η διαδικασία ξεκινάει όταν κάποιος host, ο `Attacker` (A) θα στείλει ένα *Icmp Echo* πακέτο σε έναν άλλο host τον `Target` (T), χρησιμοποιώντας ψεύτικη διεύθυνση αποστολέα, η οποία ανήκει σε έναν άλλο host, τον `Spoofed` (S).

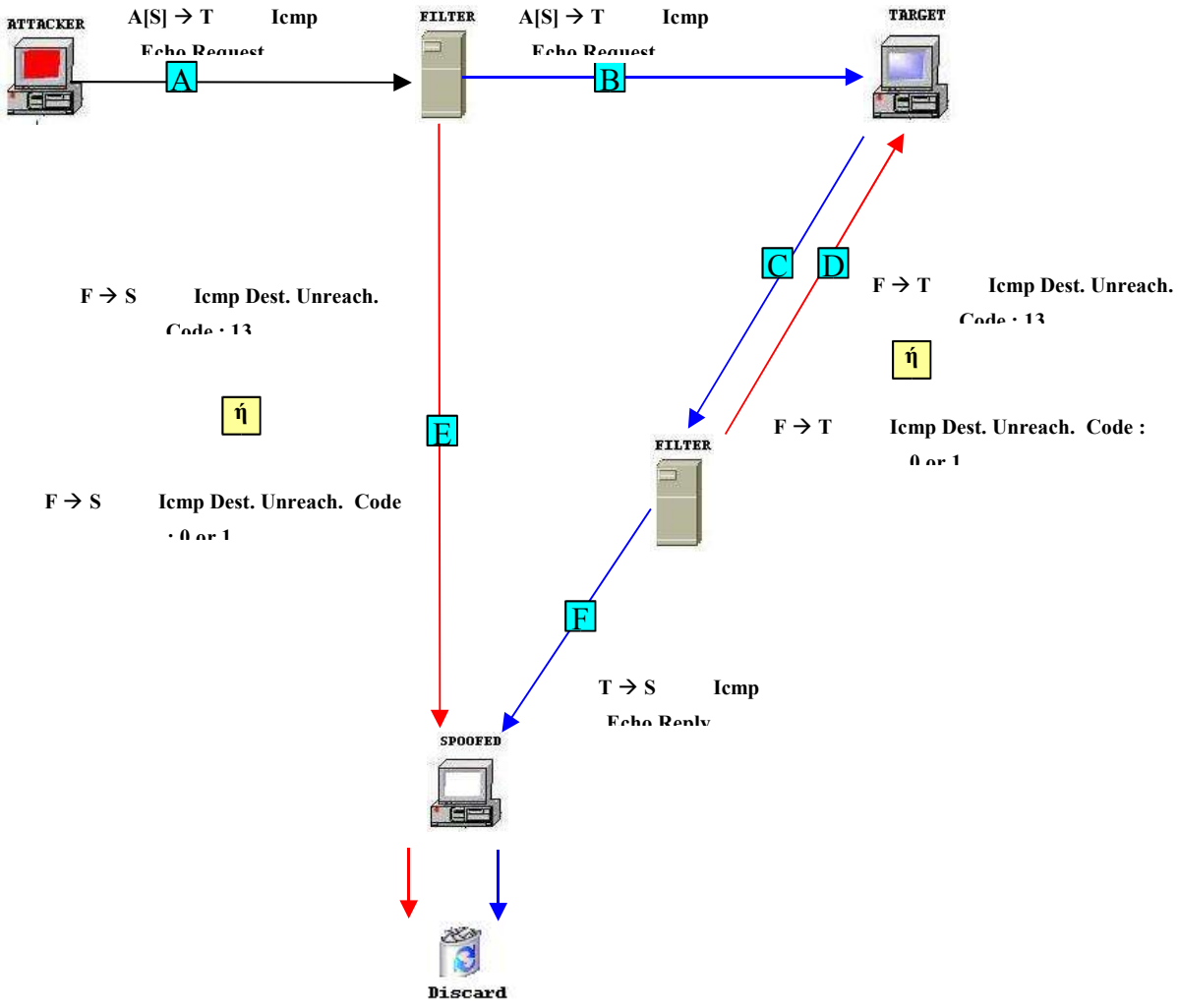
Το `Filter` (F) είναι ένα μηχάνημα που δρομολογεί και φιλτράρει τα πακέτα που στέλνονται μεταξύ των hosts που παίρνουν μέρος στην διαδικασία.

Περιγραφή του *Icmp Echo Request spoofing*

Στο παρακάτω σχήμα παρουσιάζεται η ροή του *spoofed Icmp Echo Request* πακέτου που στέλνει ο `Attacker` (A) στον `Target` (T), καθώς και των υπόλοιπων πακέτων που μπορεί να προκύψουν από αυτό.
Το *spoofed* πακέτο έχει ως διεύθυνση αποστολέα αυτή του `Spoofed` (S).



Στο παρακάτω σχήμα παρουσιάζεται η ίδια διαδικασία με ένα σχηματικό διάγραμμα.



Σχήμα Β-4: Σχηματικό διάγραμμα κατά την αποστολή ενός *spoofed* *Icmp Echo Request* πακέτου από τον Α στον Τ

Περιγραφή της Διαδικασίας

[**A**] Αρχικά ο `Attacker` στέλνει ένα *spoofed Icmp Echo Request* στον `Target` το οποίο έχει διεύθυνση αποστολέα αυτή του `Spoofed`.

[**E**] Αν στο *Request* δεν επιτραπεί από το `Filter` να περάσει, τότε ο `Spoofed` θα δεχτεί ένα *ICMP Destination Unreachable – Administrator Prohibited*, το οποίο θα περιέχει το *Icmp Echo Request* που έστειλε ο `Attacker` στον `Target`.
Ο `Spoofed` με την σειρά του δεν θα στείλει κάποιο άλλο πακέτο.

[**E**] Αν στο *Request* επιτραπεί να περάσει, αλλά ο `Target` (ή το δίκτυό του) δεν υπάρχει, τότε το `Filter` θα στείλει *Icmp Destination Unreachable – Host/Network Unreachable* στον `Spoofed`, το οποίο θα περιέχει το *Icmp Echo Request* που έστειλε ο `Attacker` στον `Target`. Ο `Spoofed` με την σειρά του δεν θα στείλει κάποιο άλλο πακέτο.

[**B**], [**C**] Αν στο *Request* επιτραπεί να περάσει και υπάρχει ο `Target`, τότε αυτός θα παραλάβει το *Icmp Echo Request* και θα στείλει ένα *Icmp Echo Reply* στον `Spoofed`.

[**D**] Αν στο *Reply* δεν επιτραπεί από το `Filter` να περάσει, τότε ο `Target` θα δεχτεί ένα *ICMP Destination Unreachable – Administrator Prohibited*, το οποίο θα περιέχει το *Icmp Echo Reply* που αυτός έστειλε στον `Spoofed`. Ο `Target` στην συνέχεια δεν θα στείλει κάποιο άλλο πακέτο.

[**D**] Αν στο *Reply* επιτραπεί από το `Filter` να περάσει αλλά ο `Spoofed` (ή το δίκτυό του) δεν υπάρχει, τότε το `Filter` θα στείλει ένα *ICMP Destination Unreachable – Host/Network Unreachable* στον `Target` το οποίο θα περιέχει το *Icmp Echo Reply* που αυτός έστειλε στον `Spoofed`. Ο `Target` στην συνέχεια δεν θα στείλει κάποιο άλλο πακέτο.

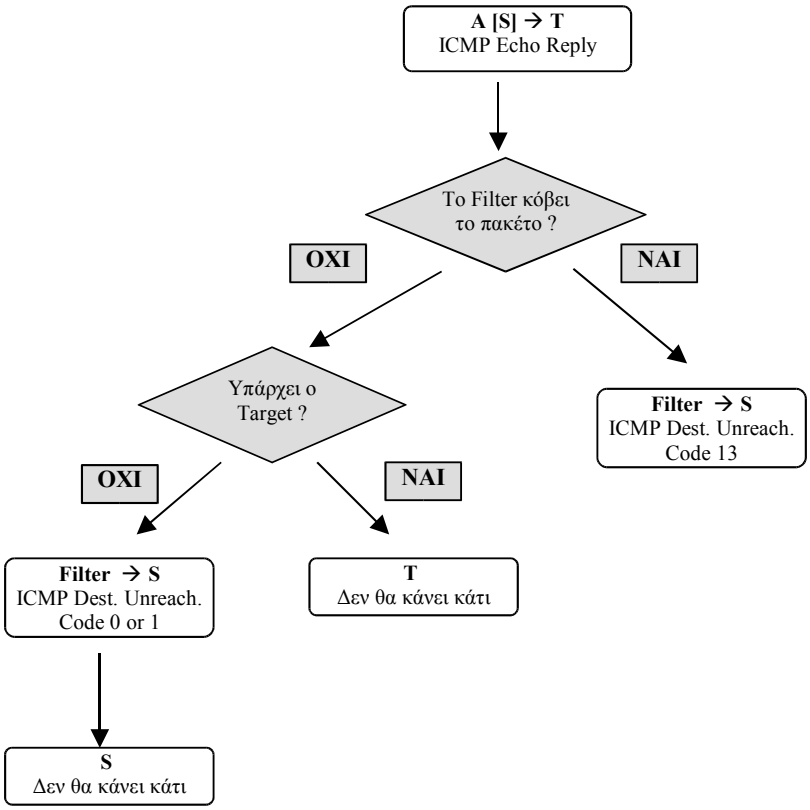
[**F**] Αν στο *Reply* επιτραπεί να περάσει και υπάρχει ο `Spoofed`, τότε το πακέτο αυτό θα φτάσει στον `Spoofed`, ο οποίος δεν θα στείλει κάποιο άλλο πακέτο.

Στη συνέχεια περιγράφεται με παρόμοιο τρόπο και το *Icmp Echo Reply spoofing*.

Περιγραφή του *Icmp Echo Reply spoofing*

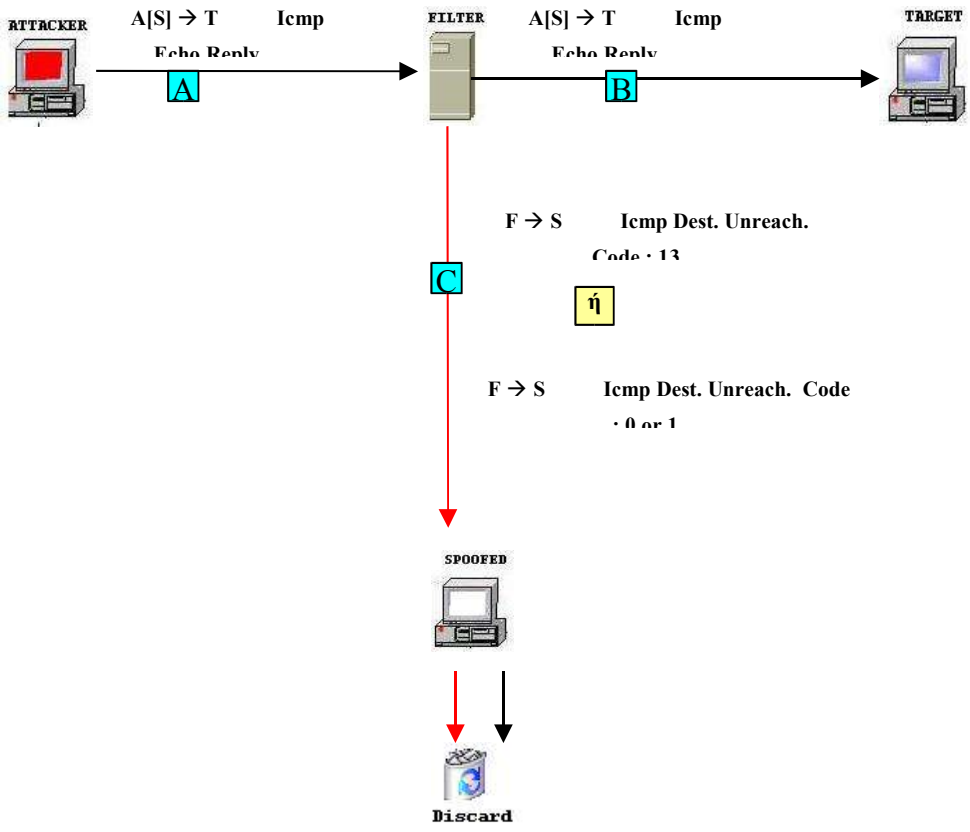
Στο παρακάτω σχήμα παρουσιάζεται η ροή του *spoofed Icmp Echo Reply* πακέτου που στέλνει ο `Attacker` (A) στον `Target` (T), καθώς και των υπόλοιπων πακέτων που μπορεί να προκύψουν από αυτό.
Το *spoofed* πακέτο έχει ως διεύθυνση αποστολέα αυτή του `Spoofed` (S).

> **Σημείωση**
>
> Υπό κανονικές συνθήκες το *Icmp Echo Reply* δεν θα μπορούσε να έχει προκύψει αν δεν είχε προηγηθεί το αντίστοιχο *Icmp Echo Request*.
> Σε αυτήν όμως την περίπτωση το *Icmp Echo Reply* είναι ένα *spoofed* πακέτο και δεν έχει προέλθει από μία νόμιμη διαδικασία.



Σχήμα B-5: Διάγραμμα ροής κατά την αποστολή ενός *spoofed* Icmp Echo Reply πακέτου από τον A στον T.

Στο επόμενο σχήμα παρουσιάζεται η ίδια διαδικασία και με ένα σχηματικό διάγραμμα.



Σχήμα Β-6: Σχηματικό διάγραμμα κατά την αποστολή ενός *spoofed* *Icmp Echo Reply* πακέτου από τον Α στον Τ

Περιγραφή της Διαδικασίας

[A] Αρχικά ο `Attacker` στέλνει ένα *spoofed Icmp Echo Reply* στον `Target`, το οποίο έχει διεύθυνση αποστολέα αυτή του `Spoofed`.

[**C**] Αν στο *Reply* δεν επιτραπεί από το `Filter` να περάσει, τότε ο `Spoofed` θα δεχτεί ένα *ICMP Destination Unreachable – Administrator Prohibited*, το οποίο θα περιέχει το *Icmp Echo Reply* που έστειλε ο `Attacker` στον `Target`. Ο `Spoofed` με την σειρά του δεν θα στείλει κάποιο άλλο πακέτο.

[**C**] Αν στο *Reply* επιτραπεί να περάσει, αλλά ο `Target` (ή το δίκτυό του) δεν υπάρχει, τότε το `Filter` θα στείλει ένα *ICMP Destination Unreachable – Host/Network Unreachable* στον `Spoofed`, το οποίο θα περιέχει το *Icmp Echo Reply* που έστειλε ο `Attacker` στον `Target`. Ο `Spoofed` με την σειρά του δεν θα στείλει κάποιο άλλο πακέτο.

[**B**] Αν στο *Reply* επιτραπεί να περάσει και υπάρχει ο `Target`, τότε αυτός θα παραλάβει το *Icmp Echo Reply* και δεν θα στείλει κάποιο άλλο πακέτο.

Από την περιγραφή του *Icmp Echo spoofing* που έγινε παραπάνω είναι φανερό ότι θύμα της αποστολής *spoofed Icmp Echo* πακέτων δεν είναι μόνο ο **`Target`** αλλά και ο **`Spoofed`** .
Ο **`Attacker`** από την στιγμή που θα στείλει το *spoofed Icmp Echo* πακέτο στον **`Target`** σταματάει να παίρνει μέρος στην όλη επικοινωνία και όλα τα πακέτα που θα προκύψουν από αυτήν θα είναι μεταξύ του **`Spoofed`**, του **`Target`** και του **`Filter`**.
Ο **`Attacker`** πλέον είναι αόρατος και δεν φαίνεται η εμπλοκή του στην όλη διαδικασία, καθώς δεν παίρνει καμία απάντηση στα πακέτα που στέλνει αφού αυτά έχουν ψεύτικο αποστολέα.

Το αποτέλεσμα της παραπάνω διαδικασίας είναι ότι ο `Spoofed`, εφόσον υπάρχει, παίρνει μέρος σε μία επικοινωνία εν αγνοία του και χωρίς την θέλησή του, ενώ ο `Target` παίρνει μέρος σε μία επικοινωνία, στέλνοντας πακέτα σε λάθος παραλήπτη χωρίς να το γνωρίζει. Το *Icmp* σαν πρωτόκολλο επικοινωνίας, λειτούργησε χωρίς λάθη και δεν συνέβη κάτι απρόβλεπτο ή παράξενο στην συμπεριφορά του.
Όλα ξεκινάνε από την στιγμή που ο `Attacker` έστειλε πακέτα με λανθασμένη πληροφορία και πιο συγκεκριμένα, ψεύτικη διεύθυνση αποστολέα.

Στη συνέχεια στο κομμάτι **III**, περιγράφονται συνοπτικά μερικές από τις περιπτώσεις στις οποίες έχει εφαρμογή το *Icmp Echo spoofing*, αναφέροντας τεχνικές και επιθέσεις οι οποίες στηρίζονται σε αυτό.

III. Τεχνικές και Επιθέσεις στις οποίες εφαρμόζεται το *Icmp Echo Spoofing*

Σε τι εξυπηρετεί τον `Attacker` το να στέλνει *spoofed Icmp Echo* πακέτα και ποιες είναι οι επιπτώσεις τους στον `Target` και στον `Spoofed` που θεωρούνται τα θύματα αυτής της διαδικασίας;

Παρακάτω δίνονται απαντήσεις στα ερωτήματα αυτά αναφέροντας μερικές από τις επιθέσεις και τις τεχνικές που στηρίζονται στο *Icmp Echo spoofing*.
Οι επιθέσεις αυτές έχουν υλοποιηθεί στο παρελθόν και έχουν δημιουργήσει σοβαρά προβλήματα, ενώ παρόμοιες ενέργειες ή και οι ίδιες σε συνδυασμό με άλλες, λαμβάνουν χώρα και σήμερα σε δικτυωμένα συστήματα, προκαλώντας την δυσλειτουργία ή και την άρνηση της χρήσης τους ή έχουν ακόμα σοβαρότερες επιπτώσεις όταν ο επιτιθέμενος καταφέρει μέσο αυτών, να αποκτήσει πρόσβαση σε κάποια σημαντικά συστήματα που περιέχουν κρίσιμες πληροφορίες.

Decoy Traffic

Το *Decoy Traffic* δεν αποτελεί κατ' ανάγκη μία επίθεση παρά είναι μία τεχνική ώστε ο επιτιθέμενος να κρύβει την δραστηριότητά του. Η χρήση του έχει κυρίως εφαρμογή σε επιθέσεις που υλοποιεί ή σε μεθόδους που χρησιμοποιεί για να συλλέξει πληροφορίες για τον στόχο του, κάνοντας δύσκολο τον εντοπισμό του.

Περιγραφή

Ο επιτιθέμενος στέλνει διάφορα *spoofed* πακέτα, σαν αντιπερισπασμό σε πραγματικά πακέτα, που στέλνει επίσης ο ίδιος.
Ο επιτιθέμενος στέλνει *Icmp Echo Request* ή *Icmp Echo Reply* πακέτα σε διάφορα συστήματα ενός δικτύου.
Ενώ τα περισσότερα από τα πακέτα αυτά είναι *spoofed,* περιέχοντας διάφορες ψεύτικες IP διευθύνσεις ως διεύθυνση αποστολέα, ένας μικρός αριθμός τους περιέχουν την πραγματική διεύθυνση του επιτιθέμενου.
Τα *spoofed* πακέτα χρησιμοποιούνται ως αντιπερισπασμός ώστε να χαθούν ανάμεσά τους τα πραγματικά πακέτα.

Επιπτώσεις

Το σύστημα ή το δίκτυο στο οποίο κάνει χρήση του *Decoy Traffic* ο επιτιθέμενος, δέχεται πακέτα που έχουν διάφορες διευθύνσεις αποστολέα και σε περίπτωση που αυτά ανήκουν σε μία επίθεση είναι δύσκολο να ανιχνευτεί ο πραγματικός ένοχος.

Χρήση του *spoofing*

Τα περισσότερα από τα πακέτα που στέλνει ο επιτιθέμενος πρέπει οπωσδήποτε να είναι *spoofed* πακέτα καθώς αυτά θα αποτελέσουν την κάλυψή του.
Το *Decoy Traffic* είναι επίσης μία τεχνική που μπορεί να χρησιμοποιήσει ο επιτιθέμενος, στην περίπτωση που δεν έχει την δυνατότητα να δει τις απαντήσεις που προκύπτουν από τα *spoofed* πακέτα που στέλνει, με κάποιον άλλο τρόπο, όπως με sniffing.
Στην περίπτωση όμως του *Decoy Traffic*, ο επιτιθέμενος αφήνει κάποιες ενδείξεις για την παρουσία του.

Scanning - Network Mapping

Ο επιτιθέμενος προσπαθεί να ανακαλύψει την τοπολογία ενός δικτύου και τα συστήματα που ανήκουν σε αυτό στέλνοντας *Icmp Echo* πακέτα.

Περιγραφή.

Πριν ο επιτιθέμενος εξαπολύσει μία επίθεση εναντίον ενός δικτύου, συνήθως προσπαθεί να συλλέξει όσο περισσότερες πληροφορίες μπορεί για αυτό το δίκτυο και τα συστήματα που ανήκουν σε αυτό, έτσι ώστε η επίθεσή του να έχει περισσότερες πιθανότητες επιτυχίας και να μην γίνει στα τυφλά.
Ο επιτιθέμενος στέλνοντας *Icmp Echo Request* πακέτα σε ένα ολόκληρο δίκτυο (πχ. σε όλες τις IP διευθύνσεις ενός C class), από τα *Icmp Echo Reply* πακέτα που θα προκύψουν θα μπορέσει να ανακαλύψει ποια συστήματα του δικτύου είναι συνδεδεμένα στο δίκτυο και να βγάλει συμπεράσματα για την τοπολογία του δικτύου. Αυτή η πληροφορία είναι χρήσιμη για τον επιτιθέμενο καθώς με αυτόν τον τρόπο κάνει μία πρώτη αναγνώριση του δικτύου, που θα τον βοηθήσει στην συνέχεια να εξαπολύσει μία επίθεση.
Η διαδικασία αυτή είναι γνωστή και με το όνομα ***Ping Sweeps***.

Το ίδιο μπορεί να προκύψει αν ο επιτιθέμενος στείλει *Icmp Echo Reply* πακέτα, καθώς από τα *Icmp Destination Unreachable – Host/Net Unreachable* πακέτα που θα προκύψουν θα μπορέσει να ανακαλύψει ποιες IP διευθύνσεις δεν αντιστοιχούν σε κάποιο σύστημα, και με την μέθοδο της αφαίρεσης να ανακαλύψει τα συστήματα που είναι συνδεδεμένα στο δίκτυο. Η τεχνική αυτή είναι γνωστή με το όνομα ***Inverse Mapping***.

Το *Inverse Mapping* μπορεί να χρησιμοποιηθεί εναλλακτικά από την αποστολή *Icmp Echo Request* πακέτων, καθώς κάποιο δίκτυο μπορεί με πολιτική ασφάλειας που υλοποιεί, να μην επιτρέπει μέσω ενός Firewall ή Router τα εισερχόμενα *Icmp Echo Requests,* αλλά να επιτρέπει τα εισερχόμενα *Icmp Echo Reply* πακέτα.

Χρήση του *spoofing.*

Τα *Icmp Echo* πακέτα που στέλνει ο επιτιθέμενος για να υλοποιήσει το *Network Mapping* συνήθως είναι *spoofed* πακέτα, έτσι ώστε σε περίπτωση που το γεγονός γίνει αντιληπτό να μην

υπάρχουν στοιχεία που να αποκαλύπτουν την ταυτότητά του. Τα πακέτα αυτά έχουν ψεύτικη διεύθυνση αποστολέα και τα πακέτα που προκύπτουν ως απαντήσεις στα *spoofed Icmp Echo* πακέτα που στέλνει ο επιτιθέμενος, δεν έχουν αυτόν ως παραλήπτη, αλλά αυτόν του οποίου η IP διεύθυνση χρησιμοποιείται στα *spoofed* πακέτα ως διεύθυνση αποστολέα.

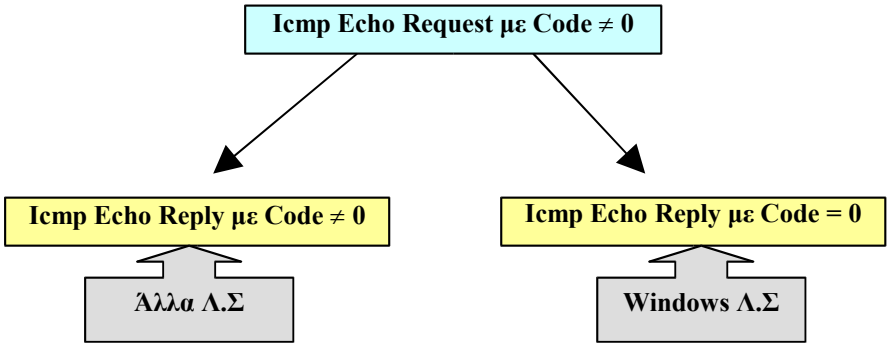
Ο επιτιθέμενος για να μπορεί να δει τα πακέτα που προκύπτουν, συνήθως κάνει sniffing σε κάποιο σημείο που περνάνε αυτά τα πακέτα.
Εναλλακτικά μπορεί να υλοποιήσει το *Network Mapping* κάνοντας χρήση του *Decoy Traffic,* στέλνοντας ανάμεσα στα *spoofed* πακέτα και μερικά *Icmp Echo* πακέτα που περιέχουν την πραγματική δική του IP διεύθυνση, έτσι ώστε οι απαντήσεις που προκύπτουν για αυτά να επιστρέφονται στον ίδιο.

OS Fingerprinting

Ο επιτιθέμενος προσπαθεί να ανακαλύψει το Λειτουργικό Σύστημα των στόχων του, ώστε να μπορέσει στη συνέχεια να εξαπολύσει σε αυτούς συγκεκριμένες επιθέσεις που σχετίζονται με το κάθε Λειτουργικό Σύστημα.

Περιγραφή.

Το *OS Fingerprinting* είναι άλλη μία μέθοδος με την οποία ο επιτιθέμενος συλλέγει πληροφορίες για τον υποψήφιο στόχο του και συνήθως υλοποιείται συγχρόνως με το *Network Mapping*.
Στέλνοντας *Icmp Echo* πακέτα σε ένα ή περισσότερα συστήματα ενός δικτύου, ο επιτιθέμενος είναι δυνατόν από τα πακέτα που προκύπτουν ως απαντήσεις, να καθορίσει το Λειτουργικό Σύστημα που τρέχουν αυτά τα συστήματα, καθώς κάθε Λειτουργικό αφήνει ίχνη στα πακέτα που στέλνει, που προδίδουν το είδος του.
Τέτοια ίχνη μπορεί να είναι μονοσήμαντες τιμές που χρησιμοποιεί το κάθε Λειτουργικό (ανάλογα με το πως υλοποιεί την IP stack) σε διάφορα πεδία του Icmp ή του IP πακέτου που δημιουργεί. Στα παρακάτω σχήματα παρουσιάζονται μερικά παραδείγματα.



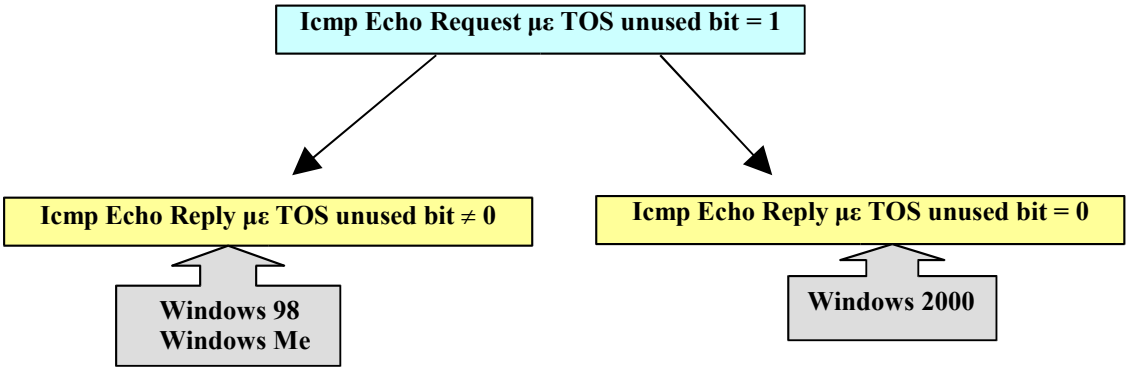
Σχήμα Β-7 : Αποστολή Icmp Echo Request με Code ≠ 0

Στο Σχήμα Β-7 παρουσιάζεται η αποστολή ενός *Icmp Echo Request* πακέτου το οποίο στο πεδίο *Code* του *Icmp header* δεν έχει την τιμή 0 που συνηθίζεται αλλά μία άλλη τιμή. Αν αυτό το πακέτο σταλεί σε μία Windows μηχανή, τότε αυτή θα απαντήσει με ένα *Icmp Echo Reply* πακέτο το οποίο θα έχει την τιμή 0 στο πεδίο *Code* του *Icmp header*.
Αν αυτό το πακέτο σταλεί σε μία μηχανή που δεν τρέχει λειτουργικό σύστημα Windows, όπως για παράδειγμα Solaris, τότε η μηχανή αυτή θα διατηρήσει την ίδια τιμή στο πεδίο *Code* του *Icmp header* στο *Reply* πακέτα που θα δημιουργήσει.

Στο Σχήμα Β-8 που ακολουθεί περιγράφεται η αποστολή ενός *Icmp Echo Request* πακέτου όπου τα unused bits του πεδίο TOS (**T**ype **O**f **S**ervice) του πακέτου έχουν την τιμή 1.
Το πεδίο TOS βρίσκεται στον *header* του IP πακέτου το οποίο περιέχει το *Icmp Echo Request* πακέτο. Τα 2 τελευταία από τα 8 bits του πεδίου αυτού υπό κανονικές συνθήκες θα έπρεπε να έχουν την τιμή 0 καθώς δεν χρησιμοποιούνται και προορίζονται για μελλοντική χρήση.

> **Σημείωση**
>
> Το πεδίο **TOS** του IP header χρησιμοποιείται από τον αποστολέα ενός πακέτου και του δίνει την δυνατότητα να ορίσει την ποιότητα μετάδοσης που επιθυμεί για αυτό το πακέτο. Για παράδειγμα μπορεί να επιλέξει αν το πακέτο θέλει να φτάσει γρήγορα στον προορισμό του ανεξαρτήτως της ποιότητας μετάδοσης ή αν θέλει να φτάσει σωστά, χωρίς λάθη ανεξαρτήτως της καθυστέρησης.

Αν ένα τέτοιο πακέτο σταλεί σε μία Windows 98 ή Windows Me μηχανή, τότε αυτή θα στείλει ένα *Icmp Echo Reply* το οποίο θα έχει την ίδια τιμή (=1) στα 2 τελευταία bits του πεδίου TOS.
Αν το πακέτο σταλεί σε μία Windows 2000 μηχανή, τότε τα 2 τελευταία bits του πεδίου TOS στο *Icmp Echo Reply* που θα σταλεί από αυτή την μηχανή θα έχουν την τιμή 0.



Σχήμα Β-8 : Αποστολή Icmp Echo Request με TOS unused bit =1

Επιπτώσεις

Η παραπάνω διαδικασία που περιγράφηκε δεν αποτελεί από μόνη της μία επίθεση άλλα μία τεχνική που μπορεί να χρησιμοποιηθεί σε προηγούμενο στάδιο, ώστε ο επιτιθέμενος να συλλέξει πληροφορίες για τον υποψήφιο στόχο του. Γνωρίζοντας το Λειτουργικό Σύστημα του στόχου του ο επιτιθέμενος μπορεί να υλοποιήσει μία επίθεση που σχετίζεται με αδυναμίες ασφάλειας του συγκεκριμένου Λειτουργικού και να έχει περισσότερες πιθανότητες επιτυχίας.

Χρήση του *spoofing*.

Και σε αυτήν την περίπτωση τα *Icmp Echo* πακέτα που στέλνει ο επιτιθέμενος για να υλοποιήσει το *OS Fingerprinting* συνήθως είναι *spoofed* πακέτα, έτσι ώστε σε περίπτωση που το γεγονός γίνει αντιληπτό να μην υπάρχουν στοιχεία που να αποκαλύπτουν την ταυτότητά του. Τα πακέτα αυτά έχουν ψεύτικη διεύθυνση αποστολέα και τα πακέτα που προκύπτουν ως απαντήσεις στα *spoofed Icmp Echo* πακέτα που στέλνει ο επιτιθέμενος, δεν έχουν αυτόν ως παραλήπτη, αλλά αυτόν του οποίου η IP διεύθυνση χρησιμοποιείται στα *spoofed* πακέτα ως διεύθυνση αποστολέα.

Ο επιτιθέμενος για να μπορεί να δει τα πακέτα που προκύπτουν, συνήθως κάνει sniffing σε κάποιο σημείο που περνάνε αυτά τα πακέτα.
Εναλλακτικά μπορεί να υλοποιήσει το *OS Fingerprinting* κάνοντας χρήση του *Decoy Traffic,* στέλνοντας ανάμεσα στα *spoofed* πακέτα και μερικά *Icmp Echo* πακέτα που περιέχουν την πραγματική δική του IP διεύθυνση, έτσι ώστε οι απαντήσεις που προκύπτουν για αυτά να επιστρέφονται στον ίδιο.

(Distributed) Denial of Service Attacks – (D)DoS

Οι (D)DoS επιθέσεις περιγράφηκαν στο Κεφάλαιο 1. Οι επιθέσεις αυτού του είδους έχουν σαν στόχο να οδηγήσουν στην δυσλειτουργία ή ακόμα και στην κατάρρευσή των συστημάτων ή των δικτύων τα οποία πλήττουν, με αποτέλεσμα να μην είναι δυνατόν να προσφέρουν τις υπηρεσίες για τις οποίες προορίζονται.
Αυτό μπορεί να επιτευχθεί με δύο τρόπους:

Icmp Nuke Attacks

Οι επιθέσεις αυτού του είδους στρέφονται σε μεμονωμένα συστήματα και σε συγκεκριμένα Λειτουργικά Συστήματα .
Ο όρος *Nuke Attack* έχει να κάνει με επιθέσεις που στηρίζονται στην αποστολή μη φυσιολογικών πακέτων, που περιέχουν πληροφορίες τις οποίες το Λειτουργικό Σύστημα του στόχου της επίθεσης δεν μπορεί να επεξεργαστεί, με συνέπεια το σύστημα αυτό να παύει να λειτουργεί κανονικά και να μην είναι δυνατόν να εξυπηρετήσει τους νόμιμους χρήστες του.
Ο λόγος που το Λειτουργικό Σύστημα αντιδρά με τέτοιο τρόπο σε αυτά τα πακέτα, είναι γιατί το κομμάτι του που υλοποιεί την επεξεργασία αυτών των πακέτων, δεν είναι από τους δημιουργούς του πιστά φτιαγμένο με τα διεθνή standards που έχουν καθοριστεί για αυτήν την διαδικασία.

> **Σημείωση**
>
> Τα διεθνή standards που πρέπει κάθε Λειτουργικό να υλοποιεί την IP stack, είναι ορισμένα από την IANA και περιγράφονται στα διάφορα RFC's που τα αφορούν.

Ping Of Death

Περιγραφή

Σε αυτήν την επίθεση ο επιτιθέμενος στέλνει ένα *Icmp Echo Request* πακέτο κατακερματισμένο σε μικρότερα πακέτα (fragments), του οποίου όμως το συνολικό μέγεθος

είναι μεγαλύτερο από το κανονικό. Το μεγαλύτερο μέγεθος που μπορεί να έχει ένα IP πακέτο είναι 65535 bytes. Ο επιτιθέμενος στέλνει ένα *Icmp Echo Request* πακέτο το οποίο έχει μέγεθος 65536 bytes σπασμένο σε πολλά μικρότερα fragments. Το σύστημα στόχος καθώς λαμβάνει τα fragments, τα επανασυγκροτεί ώστε να σχηματίσει το συνολικό IP πακέτο. Κατά την παραλαβή του τελευταίου fragment το πακέτο που προκύπτει είναι μεγαλύτερο από το φυσιολογικό κατά 1 byte και πολλά Λειτουργικά Συστήματα δεν μπορούν να το χειριστούν.

Επιπτώσεις

Το σύστημα στο οποίο στέλνεται το μεγάλο IP πακέτο σε fragments, δεν μπορεί να το επεξεργαστεί με συνέπεια να καταρρεύσει ή να εκτελέσεί επανεκκίνηση, με τελικό αποτέλεσμα να μην μπορεί να προσφέρει τις υπηρεσίες για τις οποίες είναι προορισμένο στους νόμιμους χρήστες του.
Μερικά παραδείγματα για το πως αντιδρούν κάποια λειτουργικά σε αυτήν την επίθεση παρατίθενται στον παρακάτω πίνακα.

Λειτουργικό Σύστημα	Αντίδραση
Solaris (x 86) v2.4	Reboot
Windows 95	Crash
Windows NT	Απρόβλεπτα Αποτελέσματα
Linux (kernel < 2.0.13)	Kernel Panic
Apple Mac (MacOS 7.x.x)	Crash

Πίνακας Β-1: Επιπτώσεις του Ping Of Death στα διάφορα Λειτουργικά Συστήματα

Η επίθεση αυτή είναι αρκετά παλιά και έχουν γίνει οι απαραίτητες διορθώσεις στα περισσότερα Λειτουργικά που ήταν επιρρεπή σε αυτήν.

Χρήση του *spoofing*

Η πιθανότητα ο επιτιθέμενος να χρησιμοποιεί ψεύτικη διεύθυνση αποστολέα στα πακέτα που στέλνει για να υλοποιήσει την συγκεκριμένη επίθεση είναι αρκετά μεγάλη, καθώς διαφορετικά θα πρόδιδε την ταυτότητά του. Επίσης σε αυτήν την επίθεση δεν υπάρχει η ανάγκη από τον επιτιθέμενο να παίρνει τις απαντήσεις στα *spoofed* πακέτα που στέλνει.

Icmp Floods

Οι επιθέσεις αυτού του είδους έχουν σκοπό να κατακλύσουν με πολλά πακέτα το σύστημα ή και δίκτυο το οποίο πλήττουν, έτσι ώστε να εξαντλήσουν τους πόρους του και να οδηγήσουν στην δυσλειτουργία του και στην άρνηση της χρήσης του.

Smurf Attack

Αυτή είναι μία επίθεση που έχει υλοποιηθεί στο παρελθόν με καταστροφικά αποτελέσματα, οδηγώντας ακόμα και στην κατάρρευση μεγάλων και σημαντικών δικτύων.

Περιγραφή

Ο επιτιθέμενος στέλνει μερικά *Icmp Echo Request* πακέτα στην broadcast διεύθυνση ενός δικτύου.

> **Σημείωση**
>
> Η broadcast διεύθυνση ενός δικτύου είναι αυτή, της οποίας όλα τα bit που αντιστοιχούν στο κομμάτι που αντιπροσωπεύει τους hosts του δικτύου, έχουν την τιμή 1. Για παράδειγμα η broadcast διεύθυνση ενός δικτύου Class A, του 10.0.0.0, είναι η 10.255.255.255. Τα πακέτα που στέλνονται στην broadcast διεύθυνση ενός δικτύου θα σταλούν σε όλα τα συστήματα του δικτύου αυτού.

Αν το δίκτυο αυτό επιτρέπει να στέλνονται τέτοια πακέτα στην broadcast διεύθυνσή του, τότε όλα τα συστήματα του δικτύου θα πάρουν τα *Icmp Echo Request* πακέτα που έστειλε ο επιτιθέμενος και για κάθε ένα από αυτά θα απαντήσουν με ένα *Icmp Echo Reply* στον αποστολέα των *Icmp Echo Request* πακέτων.
Τα *Icmp Echo Request* πακέτα που στέλνει ο επιτιθέμενος είναι *spoofed* πακέτα και περιέχουν σαν διεύθυνση αποστολέα την διεύθυνση του θύματος της επίθεσης.

Επιπτώσεις

Σε αυτήν την επίθεση ο κύριος στόχος είναι το σύστημα (και ίσως και το δίκτυό του) του οποίου η διεύθυνση χρησιμοποιείται στα *spoofed* πακέτα. Το σύστημα αυτό θα κατακλυστεί από έναν τόσο μεγάλο αριθμό *Icmp Echo Reply* πακέτων που θα το αναγκάσουν να εξαντλήσει τους πόρους του προκειμένου να τα επεξεργαστεί, με αποτέλεσμα να μην μπορεί να εκτελέσει άλλες λειτουργίες ή ακόμα και να καταρρεύσει. Κατ επέκταση αν ο αριθμός των πακέτων αυτών είναι πάρα πολύ μεγάλος, τότε θα δημιουργηθεί συμφόρηση και στο δίκτυο του θύματος, που θα οδηγήσει στην δυσλειτουργία του ή ακόμα και στην άρνηση της χρήσης του.
Η επιτυχία της επίθεσης στηρίζεται στον μεγάλο αριθμό των *Icmp Echo Reply* πακέτων που θα σταλούν στο δίκτυο του θύματος. Η δημιουργία αυτών των πακέτων δεν είναι πρόβλημα για τον επιτιθέμενο, καθώς τα πακέτα αυτά δεν τα στέλνει ο ίδιος άλλα τα συστήματα του δικτύου που δέχεται τα *Icmp Echo Request* πακέτα από αυτόν, στην broadcast διεύθυνσή του.
Τα δίκτυα αυτά ονομάζονται ***Ενισχυτές*** (***Amplifiers***) καθώς για ένα πακέτο που θα δεχτούν, θα δημιουργήσουν τόσα πακέτα όσα είναι και τα συστήματα που ανήκουν σε αυτά.
Για παράδειγμα αν σταλούν 100 *Icmp Echo Request* πακέτα στην broadcast διεύθυνση ενός δικτύου *Ενισχυτή* το οποίο αποτελείται από 500 συστήματα, τότε θα προκύψουν 50.000 *Icmp Echo Reply* πακέτα.
Θύμα της συγκεκριμένης επίθεσης μπορεί να είναι και το δίκτυο στο οποίο στέλνονται τα *spoofed Icmp Echo Request* πακέτα, καθώς από τα *Icmp Echo Reply* πακέτα που θα δημιουργηθούν από τα συστήματα του, θα δημιουργηθεί συμφόρηση και σε αυτό το δίκτυο.
Επίσης αν το σύστημα (ή το δίκτυό του) του οποίου η διεύθυνση χρησιμοποιείται στα *spoofed* πακέτα δεν υπάρχει, τότε το δίκτυο από το οποίο στέλνονται τα *Icmp Echo Reply* πακέτα θα κατακλυστεί και από *Icmp Destination Unreachable* πακέτα που θα δημιουργηθούν από αυτά.

Χρήση του *spoofing*

Ο επιτιθέμενος για να μπορέσει να υλοποιήσει με επιτυχία αυτή την επίθεση πρέπει να κάνει οπωσδήποτε χρήση του *spoofing*, διαφορετικά η επίθεση θα έχει τον ίδιο σαν στόχο, καθώς τα *Icmp Echo Reply* πακέτα που θα προκύψουν από το δίκτυο *Ενισχυτή* θα έχουν αυτόν ως παραλήπτη.

Σε αυτήν την επίθεση ο επιτιθέμενος δεν έχει λόγο να βλέπει τις απαντήσεις που προκύπτουν από τα *spoofed* πακέτα που στέλνει, καθώς αυτά και μόνο αρκούν από πλευράς του επιτιθέμενου για να φέρουν σε πέρας την επίθεση, που σκοπό έχει να προκαλέσει την άρνηση της χρήσης ενός συστήματος ή και ενός δικτύου.

Tunneling - Covert Channels

Περιγραφή

Ο επιτιθέμενος στέλνει *Icmp Echo Request* πακέτα σε κάποιο σύστημα-στόχο το οποίο έχει ήδη καταλάβει σε προηγούμενο στάδιο.
Τα πακέτα που στέλνει ο επιτιθέμενος περιέχουν στα data τους κωδικοποιημένες εντολές και άλλες πληροφορίες, οι οποίες αποκωδικοποιούνται από ειδική εφαρμογή που τρέχει στο σύστημα-στόχο, την οποία έχει εγκαταστήσει σε αυτό ο επιτιθέμενος σε προηγούμενο στάδιο. Έτσι ενώ τα πακέτα που στέλνονται στο σύστημα αυτό μοιάζουν με αθώα *Icmp Echo Request* πακέτα και επιτρέπεται η διέλευσή τους από το Firewall του δικτύου, στην ουσία αποτελούν μέρος κωδικοποιημένης επικοινωνίας μεταξύ του συστήματος και του επιτιθέμενου.

Επιπτώσεις

Επικοινωνία με χρήση του *Tunnelling* συνάπτει συνήθως ο επιτιθέμενος με συστήματα που έχει καταλάβει σε προηγούμενο στάδιο, ώστε να μπορεί να τα διαχειρίζεται και να τα συντονίζει χωρίς να γίνεται αντιληπτό το γεγονός, για να παίρνουν μέρος σε DDoS επιθέσεις. Ο επιτιθέμενος επικοινωνεί με αυτά τα συστήματα και από τα *Icmp Echo Reply* πακέτα που του στέλνουν ελέγχει ποια από αυτά είναι ενεργά και διαθέσιμα να πάρουν μέρος στην επίθεση. Όταν αποφασίσει να εξαπολύσει την DDoS επίθεση σε κάποιο δίκτυο, με κωδικοποιημένες εντολές, οι οποίες μπορεί να περιέχονται στα data ενός και μόνο *Icmp Echo Request* πακέτου, έχει την δυνατότητα να ενεργοποιήσει το κάθε σύστημα με το οποίο επικοινωνεί μέσω του *Tunnelling* να πάρει μέρος στην επίθεση και να ξεκινήσει να στέλνει τα πακέτα που θα την υλοποιήσουν.

Χρήση του *spoofing*

Τα *Icmp Echo Request* πακέτα που στέλνει ο επιτιθέμενος και επικοινωνεί μέσω του *Tunnelling* συνήθως είναι *spoofed* πακέτα, έτσι ώστε σε περίπτωση που γίνει αντιληπτό το γεγονός να μην υπάρχουν στοιχεία που να οδηγούν σε αυτόν.
Εκτός από τα πακέτα που θα στείλει ο επιτιθέμενος τα οποία θα αποτελέσουν το τελικό σύνθημα για να ξεκινήσει η DDoS επίθεση, για τα υπόλοιπα πακέτα που στέλνει για να ελέγξει την διαθεσιμότητα των συστημάτων αυτών, πρέπει να μπορεί να λαμβάνει τα *Icmp Echo Reply* πακέτα που του επιστρέφουν. Σε αυτή την περίπτωση ο επιτιθέμενος, θα πρέπει είτε να κάνει sniffing, ώστε να βλέπει τα *Icmp Echo Reply* πακέτα, είτε να χρησιμοποιεί *Decoy Traffic*.

Οι παραπάνω επιθέσεις είναι μόνο ένα αντιπροσωπευτικό δείγμα από το σύνολο των χρήσεων του *Icmp Echo spoofing* σε κακόβουλες ενέργειες. Παρόλο που για τις περισσότερες από αυτές έχουν βρεθεί τρόποι αντιμετώπισής τους, συνεχώς ανακαλύπτονται νέες τεχνικές που τους παρακάμπτουν, οι οποίες στηρίζονται στην αμείωτη φαντασία των επιτιθέμενων και τα ελλιπή μέτρα ασφάλειας που εφαρμόζονται στα περισσότερα δίκτυα.
Για να υλοποιηθούν αυτές οι επιθέσεις υπάρχουν διάφορα λογισμικά που δεν απαιτούν ιδιαίτερες γνώσεις στην χρήση τους και μπορεί κανείς εύκολα να τα προμηθευτεί από το διαδίκτυο. Για ευνόητους λόγους τα εργαλεία αυτά και οι δικτυακοί τόποι από τους οποίους είναι διαθέσιμα δεν αναφέρονται σε αυτήν την εργασία.

ΕΠΙΛΟΓΟΣ ΚΕΦΑΛΑΙΟΥ

Το *Icmp* ένα πολύ χρήσιμο εργαλείο για την σωστή λειτουργία του Internet, καθώς παρέχει διάφορες διαγνωστικές λειτουργίες, τόσο για την δικτύωση μεταξύ συστημάτων όσο και για την απασφαλμάτωση λαθών που μπορεί να συμβούν κατά την επικοινωνία μεταξύ τους.
Ενώ το *Icmp*, σε σχέση με άλλα πρωτόκολλα, είναι απλό στην λειτουργία του, συγχρόνως μπορεί να αποτελέσει στα χέρια κακόβουλων χρηστών ένα ισχυρό εργαλείο, μέσο του οποίου να υλοποιηθούν πολύπλοκες επιθέσεις με καταστροφικά αποτελέσματα.
Σε αυτό το Κεφάλαιο έγινε μία συνοπτική αναφορά στο *ICMP* πρωτόκολλο και στον τρόπο που λειτουργεί και έγινε αναλυτική περιγραφή στην διαδικασία του *Icmp Echo spoofing* δηλαδή στην αποστολή *Icmp Echo Request* και *Icmp Echo Reply* πακέτων που έχουν ψεύτικη διεύθυνση αποστολέα.
Στην συνέχεια παρουσιάστηκαν μερικές από τις τεχνικές και τις επιθέσεις που στηρίζονται στο *Icmp Echo spoofing* και τις επιπτώσεις που έχουν αυτές στα συστήματα και τα δίκτυα που πλήττουν. Από τις επιθέσεις που αναφέρθηκαν, έγινε κατανοητό ότι ο επιτιθέμενος μπορεί να κάνει χρήση του *Icmp Echo spoofing*, είτε για να συλλέξει πληροφορίες για την τοπολογία δικτύων και των συστημάτων που τα αποτελούν, ώστε να τις χρησιμοποιήσει σε επόμενο στάδιο σε κάποια επίθεση που θα εξαπολύσει σε αυτά, είτε για να υλοποιήσει την ίδια την επίθεση που θα θέσει συστήματα ή και ολόκληρα δίκτυα εκτός λειτουργίας.

Υπάρχει τρόπος να ανιχνευτεί το *Icmp Echo spoofing* όταν αυτό συμβαίνει, ώστε να ληφθούν κατάλληλα μέτρα προστασίας και να αποφευχθούν οι συνέπειες που μπορεί να έχουν οι παραπάνω επιθέσεις ;

Στο επόμενο Κεφάλαιο παρουσιάζεται με λεπτομέρεια, μία τεχνική ανίχνευσης των *spoofed Icmp Echo* πακέτων, έτσι ώστε αυτά να γίνονται αντιληπτά όταν υφίστανται στο traffic ενός δικτύου και το φαινόμενο να αντιμετωπίζεται ανάλογα.