ΚΕΦΑΛΑΙΟ 4

Τεχνική Ανίχνευσης του *ICMP Echo Spoofing*

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Στο Κεφάλαιο 3 έγινε η περιγραφή του Icmp Echo spoofing και αναφέρθηκαν μερικά παραδείγματα στα οποία έχει εφαρμογή. Από αυτές τις αναφορές φάνηκε ότι μπορεί να αποτελέσει ένα σοβαρό κίνδυνο για την ασφάλεια ενός δικτύου και για τον λόγο αυτόν υπάρχει η ανάγκη ανίχνευσής του όταν αυτό συμβαίνει.
Σε αυτό το Κεφάλαιο περιγράφεται μία τεχνικής ανίχνευσης του *Icmp Echo spoofing*, η οποία έχει σαν στόχο με την εφαρμογή της σε ένα δίκτυο, να εντοπίζονται και να επισημαίνονται τα *spoofed Icmp Echo Request* και *spoofed Icmp Echo Reply* πακέτα που εισέρχονται και εξέρχονται από το δίκτυο αυτό.

Η πιο διαδεδομένη τεχνική που εφαρμόζεται σήμερα για την προστασία από το *spoofing* γενικότερα, είναι το *ingress* και *egress filtering* που υλοποιείται από την πολιτική ασφάλειας των περισσότερων δικτύων.

Ο όρος ***ingress filtering*** αναφέρεται στην διαδικασία κατά την οποία ένα δίκτυο δεν επιτρέπει την διέλευση εισερχόμενων σε αυτό πακέτων, που έχουν διεύθυνση αποστολέα η οποία μπορεί να ανήκει μόνο σε συστήματα του δικτύου αυτού.
Έτσι δεν μπορεί κάποιος εκτός του δικτύου να στείλει πακέτα σε αυτό, προσποιούμενος ότι είναι ένα σύστημα που ανήκει σε αυτό το δίκτυο.

Ο όρος ***egress filtering*** αναφέρεται στην διαδικασία κατά την οποία ένα δίκτυο δεν επιτρέπει την διέλευση εξερχόμενων από αυτό πακέτων, που έχουν διεύθυνση αποστολέα η οποία δεν μπορεί να ανήκει σε συστήματα του δικτύου αυτού.
Έτσι δεν μπορεί κάποιος εντός του δικτύου να στείλει πακέτα προς τα έξω προσποιούμενος ότι είναι ένα σύστημα που δεν ανήκει σε αυτό το δίκτυο.

Οι δύο παραπάνω τεχνικές είναι απαραίτητο να υλοποιούνται σε κάθε δίκτυο και μειώνουν την πιθανότητα του *spoofing* σε μεγάλο βαθμό. Παρόλα αυτά δεν μπορούν να εξαλείψουν εντελώς την πιθανότητα του *spoofing* και υπάρχουν πολλές περιπτώσεις που δεν μπορούν να καλύψουν.

Οι δύο παραπάνω τεχνικές στηρίζονται στον έλεγχο κάθε IP πακέτου ξεχωριστά και πιο συγκεκριμένα στον έλεγχο της διεύθυνσης αποστολέα , που βρίσκεται στον header του κάθε IP πακέτου, ενώ δεν έχουν την δυνατότητα να ελέγχουν ακολουθίες πακέτων ώστε να μπορούν να επιβεβαιώσουν αν κάποιο πακέτο έχει λόγο ύπαρξης σε μία επικοινωνία, έχοντας προκύψει από κάποιο άλλο πακέτο (πχ. ένα *Icmp Echo Reply* από ένα *Icmp Echo Request*).

Στη συνέχεια θα γίνει μία μελέτη για τον τρόπο με τον οποίο μπορεί να ανιχνευτεί το *spoofing* όταν συμβαίνει, όσο αναφορά τα *spoofed Icmp Echo Request* και *Icmp Echo Reply* πακέτα.
Η εφαρμογή του *ingress* και *egress filtering* στην μελέτη που ακολουθεί θα θεωρείται δεδομένη, καθώς οι τεχνικές αυτές υλοποιούνται σήμερα σχεδόν σε όλα τα δίκτυα που εφαρμόζουν στοιχειώδη πολιτική ασφάλειας. Στόχος της μελέτης αυτής είναι καλύψει κάποιες από τις περιπτώσεις που δεν καλύπτουν οι δύο παραπάνω τεχνικές.

Η ανίχνευση του *spoofing* θα πραγματοποιηθεί από την πλευρά του `Target` (σε αυτόν στέλνονται τα *spoofed* πακέτα από τον `Attacker`) και του `Spoofed` (του οποίου η IP διεύθυνση χρησιμοποιείται στα *spoofed* πακέτα από τον `Attacker`), καθώς αυτοί είναι τα θύματα του *spoofing*.

Η γενική ιδέα στην οποία στηρίζεται η διαδικασία της ανίχνευσης που θα μελετηθεί είναι :

> ***Η ύπαρξη μίας απάντησης, προϋποθέτει ότι έχει προηγηθεί η αντίστοιχη ερώτηση.***

Για να επιτευχθεί αυτό θα πρέπει οι απαντήσεις που εντοπίζονται, να ελέγχονται για το αν αντιστοιχούν σε κάποιες από τις ερωτήσεις που έχουν προηγηθεί και για τις οποίες πρέπει να καταχωρείται ένα είδος ιστορικού.
Για την ανίχνευση του *Icmp Echo spoofing*, οι ερωτήσεις είναι τα εισερχόμενα και εξερχόμενα *Icmp Echo Request* πακέτα από το δίκτυο στο οποίο εφαρμόζεται η τεχνική της ανίχνευσης, ενώ οι απαντήσεις είναι κάποια άλλα *Icmp* πακέτα, τα οποία ελέγχονται για το αν αντιστοιχούν με κάποιο καταχωρημένο *Icmp Echo Request* πακέτο ή και αν έχουν προέλθει εξαιτίας αυτού.

Τα πακέτα που παρουσιάζουν ενδιαφέρον και θα επεξεργάζονται για την ανίχνευση του *Icmp spoofing* είναι τα παρακάτω :

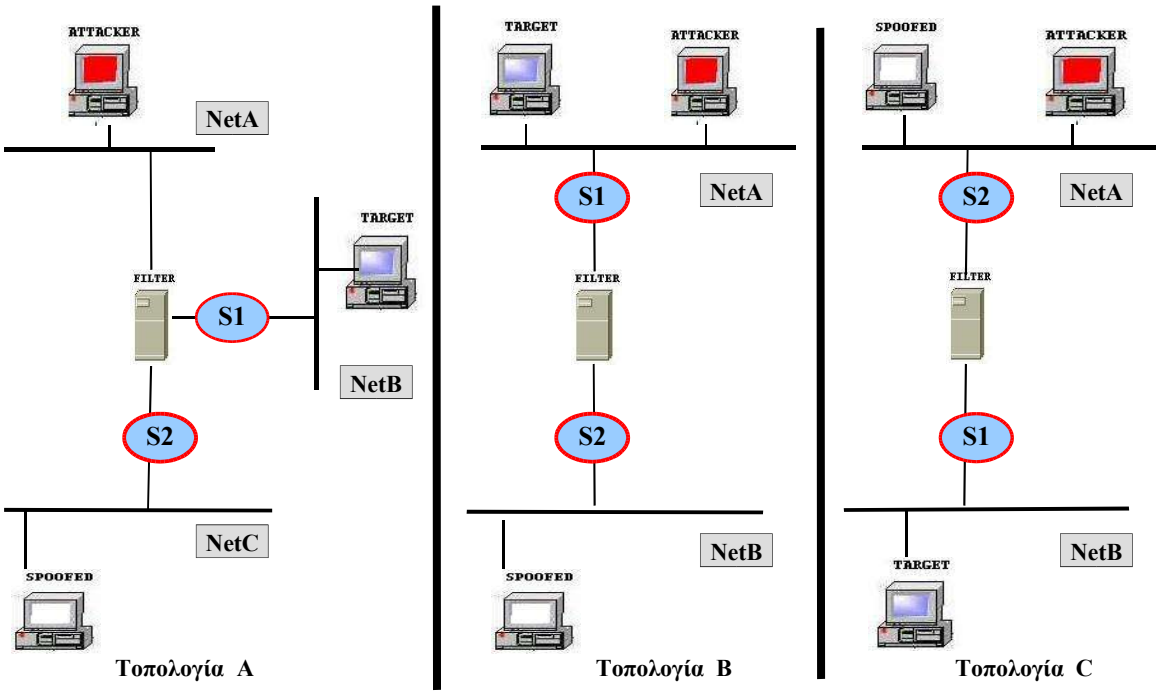
- **Icmp Echo Request** (Type 8 , Code 0)
- **Icmp Echo Reply** (Type 0 , Code 0)
- **Icmp Destination Unreachable – Host/Net Unreachable (** Type 3, Code 1/0)
  Που Περιέχουν ένα
  - ⇒ **Icmp Echo Request**
  - ⇒ **Icmp Echo Reply**
- **Icmp Destinatio*n* Unreachable – Administrative Prohibited (** Type 3, Code 13 **)**
  Που Περιέχουν ένα

Σχήμα 1 : Icmp πακέτα προς επεξεργασία

Τα *Icmp Echo Request* είναι αυτά για τα οποία πρέπει να κρατείται κάποιο ιστορικό, όταν αυτά εισέρχονται ή εξέρχονται από το προστατευόμενο δίκτυο, δηλαδή το δίκτυο στο οποίο εφαρμόζεται η τεχνική της ανίχνευσης του *Icmp Echo spoofing*.

Τα υπόλοιπα *Icmp* πακέτα είναι αυτά για τα οποία θα πρέπει να ελέγχεται για το αν είναι νόμιμη η παρουσία τους, δηλαδή αν έχει προηγηθεί κάποιο *Icmp Echo Request* που οδήγησε στην δημιουργία τους.
Στα *Icmp Destination Unreachable* πακέτα, αυτό που ενδιαφέρει προς εξέταση είναι το εσωτερικό *Icmp* πακέτο που περιέχουν, το οποίο υποτίθεται ότι οδήγησε στην δημιουργία του *Icmp Error* μηνύματος.

Στο Κεφάλαιο 3 έγινε περιγραφή της διαδικασίας του *spoofing* στην γενική μορφή του, κατά την οποία υπήρχαν τρία συστήματα που ανήκαν σε τρία διαφορετικά δίκτυα, τα οποία ένωνε ένα σύστημα το `Filter`, που έπαιζε το ρόλο ενός router ή/και firewall.
Παρόλα αυτά τα τρία συστήματα μπορούν να είναι κατανεμημένα διαφορετικά μεταξύ τους και κάποια από αυτά να ανήκουν και στο ίδιο δίκτυο. Η τοπολογία των τριών δικτύων και η θέση του κάθε συστήματος σε σχέση με τα άλλα, έχει ιδιαίτερη σημασία και όπως θα αποδειχθεί παρακάτω, διαφέρει σε κάθε περίπτωση η εξαγωγή των συμπερασμάτων για το *spoofing* όταν αυτό ανιχνευτεί.
Οι διάφορες τοπολογίες που μπορούν να ισχύουν και θα εξεταστούν για ανίχνευση του *spoofing*, μπορούν να χωριστούν σε τρεις γενικές κατηγορίες οι οποίες παρουσιάζονται σχηματικά στο **Σχήμα 2** που ακολουθεί:



Σχήμα 2 : Πιθανές Τοπολογίες

1. Τοπολογία A

Ο `Target`, ο `Spoofed` , και ο `Attacker` βρίσκονται σε τρία διαφορετικά δίκτυα.
Είναι η περίπτωση που χρησιμοποιήθηκε σαν παράδειγμα και στο Κεφάλαιο 3 για την Περιγραφή του *Icmp Echo spoofing*.

2. Τοπολογία B

Ο `Target` και ο `Attacker` βρίσκονται στο ίδιο δίκτυο ενώ ο `Spoofed` σε διαφορετικό.
Σε αυτήν την περίπτωση ο `Attacker` στέλνει *spoofed* πακέτα στον `Target`, δηλαδή μέσα στο ίδιο δίκτυο, το NetA, χρησιμοποιώντας για διεύθυνση αποστολέα αυτή του `Spoofed` που βρίσκεται εκτός του δικτύου τους.

3. Τοπολογία C

Ο `Spoofed` και ο `Attacker` βρίσκονται στο ίδιο δίκτυο ενώ ο `Target` σε διαφορετικό.

Σε αυτήν την περίπτωση ο `Attacker` χρησιμοποιεί την διεύθυνση του `Spoofed`, που βρίσκεται στο δίκτυό του, το NetA, ως διεύθυνση αποστολέα στα *spoofed* πακέτα που στέλνει στον `Target`, ο οποίος βρίσκεται εκτός του δικτύου τους.

Σημείωση

Άλλες πιθανές τοπολογίες θα μπορούσε να δημιουργηθούν αν γίνονταν και οι υπόλοιποι πιθανοί συνδυασμοί μεταξύ των τριών συστημάτων. Αυτοί οι συνδυασμοί είναι οι παρακάτω και όπως αποδεικνύεται δεν έχει νόημα η μελέτη της ανίχνευσης σε αυτές τις τοπολογίες :

4. **Ο Target, ο Spoofed , και ο Attacker βρίσκονται και οι τρεις στο ίδιο δίκτυο**.

Σε αυτή την περίπτωση η συγκεκριμένη τεχνική ανίχνευσης του *spoofing* δεν έχει εφαρμογή καθώς δεν πρόκειται για εισερχόμενα ή εξερχόμενα πακέτα από το δίκτυο, αλλά για πακέτα που ανήκουν στο εσωτερικό traffic του δικτύου. Αν πρόκειται για το ίδιο τοπικό δίκτυο LAN τότε υπάρχουν άλλες τεχνικές για την ανίχνευση του *spoofing* που στηρίζονται στις Ethernet διευθύνσεις των πακέτων.

5. **Ο Target και ο Spoofed να είναι στο ίδιο δίκτυο ενώ ο Attacker σε διαφορετικό.**

Αυτή η περίπτωση καλύπτεται με την εφαρμογή του ingress filtering που θεωρείται δεδομένη. Ο Attacker στέλνει στο δίκτυο του Target *spoofed* πακέτα με την διεύθυνση του Spoofed που ανήκει και αυτός στο ίδιο δίκτυο. Το Filter θα πρέπει να κόβει αυτά τα πακέτα καθώς προορίζονται για το δίκτυο του και έχουν διεύθυνση αποστολέα που ανήκει στο δίκτυό του, ενώ προέρχονται εκτός του δικτύου.

Σε κάθε περίπτωση ο `Attacker` είναι αυτός που στέλνει *spoofed* πακέτα στον `Target`, τα οποία έχουν ως διεύθυνση αποστολέα αυτή του `Spoofed`.
Το `Filter` παίζει τον ρόλο ενός router ο οποίος ενώνει τα τρία δίκτυα και δρομολογεί τα πακέτα μεταξύ τους.

Σημείωση :

Το Filter μπορεί να θεωρηθεί μια σύμπτυξη περισσοτέρων routers που επικοινωνούν μεταξύ τους και ενώνουν αυτά τα τρία δίκτυα, έτσι ώστε να γίνεται καλύτερα αντιληπτό ότι τα τρία αυτά δίκτυα είναι ανεξάρτητα μεταξύ τους.
Μια πιο γενική εικόνα θα ήταν αν το κάθε από τα παραπάνω δίκτυα είχε τον δικό του router και οι τρεις routers να συνδέονται μεταξύ τους.
Επίσης το Filter λειτουργεί και σαν συσκευή 'φιλτραρίσματος' πακέτων (πχ.Firewall) και μπορεί να ασκεί κάποια πολιτική ασφάλειας και να φιλτράρει τα πακέτα επιτρέποντάς ή όχι την διέλευσή τους.

Τα σημεία **S1** και **S2** είναι τα πιθανά σημεία στα οποία μπορεί να εκτελείται η διαδικασία της ανίχνευσης και όπως φαίνεται και στο **Σχήμα 2**, τα σημεία αυτά βρίσκονται σε κάθε περίπτωση στα δίκτυα των πιθανών θυμάτων, δηλαδή του `Target` και του `Spoofed` .

Η διαδικασία της ανίχνευσης θα εκτελείται από τον `Sensor`. Ο `Sensor` είναι μια συσκευή η οποία θα είναι ικανή να βλέπει και να επεξεργάζεται όλα τα πακέτα που εισέρχονται και εξέρχονται από το προστατευόμενο δίκτυο.

Ο `Sensor` για την εφαρμογή της ανίχνευσης θα πρέπει να εκτελεί τις παρακάτω λειτουργίες:

I. **Αποθήκευση των Εισερχόμενων και Εξερχόμενων *Icmp Echo Request* πακέτων .**

Ο Sensor θα αποθηκεύει όλα τα *Icmp Echo Request* πακέτα που εισέρχονται και εξέρχονται από το προστατευόμενο δίκτυο. Με αυτό τον τρόπο θα διατηρεί ένα είδος ιστορικού για τα *Icmp Echo Request* πακέτα που έστειλαν ή έλαβαν τα συστήματα του δικτύου αυτού.

II. Έλεγχος των υπόλοιπων ενδιαφερόντων *Icmp* πακέτων.

Ο `Sensor` θα ελέγχει τα υπόλοιπα *Icmp* πακέτα (*Reply* , *Destination Unreachable Code 0/1*,*13*) που εισέρχονται και εξέρχονται από το προστατευόμενο δίκτυο, για το αν είναι νόμιμη η ύπαρξή τους, δηλαδή αν έχει υπάρξει κάποιο αποθηκευμένο *Icmp Echo Request* που οδήγησε στην εμφάνισή τους.

Περιορισμοί

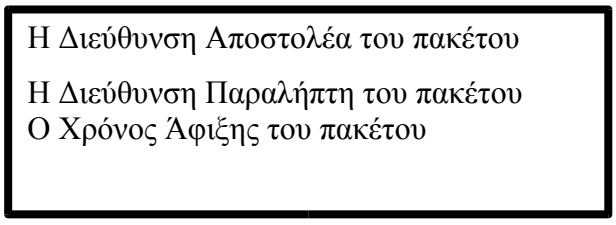
Η λειτουργία του `Sensor` πρέπει να έχει κάποιους περιορισμούς ως προς την διαδικασία της ανίχνευσης :

◊ **Ο Sensor δεν θα επεξεργάζεται το εσωτερικό traffic του προστατευόμενου δικτύου.**

Ο `Sensor` δεν θα πρέπει να είναι ικανός να βλέπει τα πακέτα που ανταλλάζουν μεταξύ τους τα συστήματα του προστατευόμενου δικτύου και αν μπορεί να τα βλέπει, τότε θα πρέπει να τα αγνοεί και να μην τα επεξεργάζεται.
Η ανίχνευση έχει στόχο να εντοπίσει τα *spoofed Icmp Echo* πακέτα που εισέρχονται ή εξέρχονται από το προστατευόμενο δίκτυο. Το *spoofing* όταν συμβαίνει μεταξύ των συστημάτων του δικτύου και εφόσον δεν επηρεάζει κάποιο άλλο σύστημα εκτός του δικτύου αυτού, δεν αφορά την συγκεκριμένη διαδικασία.

◊ **Ο Sensor δεν θα αποθηκεύει ολόκληρο το *Icmp Echo Request* πακέτο.**

Το μέγεθος της πληροφορίας για το πακέτο που θα αποθηκεύεται, έχει άμεση σχέση με την ταχύτητα της διαδικασίας της ανίχνευσης και γι ‘αυτό το σκοπό η απαραίτητη πληροφορία για κάθε *Icmp Echo Request* πακέτο που θα αποθηκεύεται θα είναι :



Σχήμα 3: Πληροφορία του Icmp Echo Request πακέτου προς αποθήκευση

Τα εισερχόμενα με τα εξερχόμενα *Icmp Echo Request* πακέτα θα αποθηκεύονται ξεχωριστά, ελέγχοντας την διεύθυνση αποστολέα του κάθε πακέτου.

◊ **Ο χρόνος αποθήκευσης του κάθε *Echo Request* θα είναι περιορισμένης διάρκειας.**

Ο χρόνος που μπορεί ένα αποθηκευμένο *Echo Request* να παραμένει αποθηκευμένο, έχει να κάνει με τον χρόνο που θεωρείται αρκετός να αναμένεται κάποιο άλλο *Icmp* πακέτο

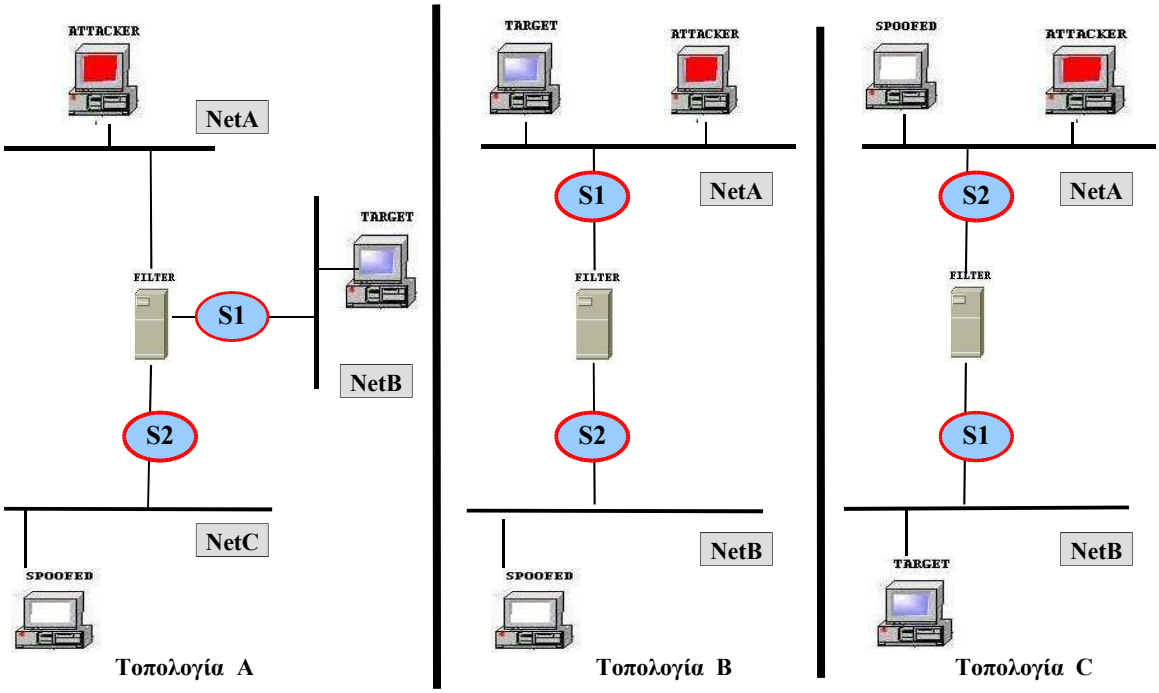
ως απάντηση σε αυτό. Ο χρόνος αυτός έχει άμεση σχέση με την τοπολογία του κάθε δικτύου και την ποιότητα των γραμμών διασύνδεσής του.

Στη συνέχεια θα εξεταστεί η λειτουργία της ανίχνευσης του *Icmp Echo spoofing*, ελέγχοντας κάθε ένα από τα *Icmp* πακέτα που παρουσιάζουν ενδιαφέρον (**Σχήμα 1**), καθώς αυτά θα εισέρχονται και θα εξέρχονται από το προστατευόμενο δίκτυο που έχει υπό την επίβλεψή του ο `Sensor`.

ΜΕΡΟΣ Α

Έλεγχος του *Icmp Echo Reply* Πακέτου (Type 0 , Code 0)

Στο σημείο αυτό παρουσιάζεται ξανά το **Σχήμα 2** έτσι ώστε να είναι πιο εύκολη η πρόσβαση σε αυτό, κατά την περιγραφή της διαδικασίας.



Σχήμα 2: Πιθανές Τοπολογίες

Ο `Sensor` εντοπίζει ένα *Icmp Echo Reply* πακέτο. Το πακέτο αυτό μπορεί να προέρχεται από το προστατευόμενο δίκτυο και να προορίζεται προς τα έξω ή το αντίθετο. Η ύπαρξη του συγκεκριμένου πακέτου μπορεί να οφείλεται σε μία από τις τρεις περιπτώσεις :

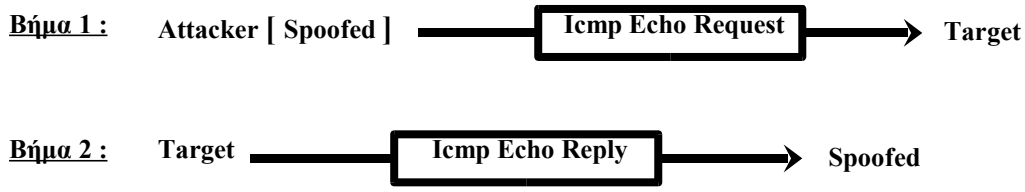
1. Να έχει δημιουργηθεί ως απάντηση σε ένα νόμιμο *Icmp Echo Request* πακέτο.
2. Να έχει δημιουργηθεί ως απάντηση σε ένα *spoofed Icmp Echo Request* πακέτο.
3. Να είναι ένα *spoofed Icmp Echo Reply* πακέτο.

Η παρουσία και μόνο, αυτού του πακέτου, δηλώνει ότι πρέπει να έχει προηγηθεί το αντίστοιχο *Icmp Echo Request* πακέτο με την αντίθετη φορά, το οποίο είχε ως αποστολέα τον παραλήπτη του *Reply* και ως παραλήπτη τον αποστολέα του *Reply*.
Η επιβεβαίωση αυτής της πρότασης ή όχι θα οδηγήσει στην ανίχνευση του *spoofing*.

Διαδικασία Ανίχνευσης
Ο `Sensor` εντοπίζει ένα *Icmp Echo Reply* πακέτο και πρέπει να ελέγξει αν προηγήθηκε το αντίστοιχο *Icmp Echo Request*. Έτσι ελέγχονται είτε τα *Εισερχόμενα* είτε τα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο που έχουν αποθηκευτεί, για να εντοπιστεί αυτό που έχει ως αποστολέα τον παραλήπτη του *Reply* και ως παραλήπτη τον αποστολέα του *Reply*.
Ένα εισερχόμενο *Reply* πρέπει να αντιστοιχηθεί με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests*, ενώ ένα εξερχόμενο *Reply* πρέπει να αντιστοιχηθεί με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests*.

A.1. Ανίχνευση του *spoofed Icmp Echo Request* πακέτου

Σενάριο



Αρχικά (Βήμα 1) ο `Attacker` στέλνει ένα *spoofed Icmp Echo Request* στον `Target`, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.
Στη συνέχεια (Βήμα 2) ο `Target` απαντάει στον `Spoofed` στέλνοντάς του ένα *Icmp Echo Reply*.

Στόχος με τον έλεγχο που θα γίνει στο *Icmp Echo Reply* πακέτο που εντοπίζεται από τον `Sensor`, είναι να ανιχνευτεί αν αυτό το πακέτο έχει δημιουργηθεί σαν απάντηση σε κάποιο *spoofed Icmp Echo Request* πακέτο.

A.1.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target` (Βήμα 1), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1, ο οποίος θα

το αποθηκεύσει στα *Εισερχόμενα Requests* προς το NetB, σαν αυτό να έχει προέλθει από τον `Spoofed`.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον *Sensor* στη θέση S1, ο οποίος εντοπίζοντας ένα εξερχόμενο *Reply* θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetB.

Ο `Sensor` στη θέση S1 θα καταφέρει να αντιστοιχήσει το εξερχόμενο *Reply* με το Εισερχόμενο *Request* που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target` και το οποίο αποθήκευσε προηγουμένως και έτσι το *spoofing* δεν θα ανιχνευτεί.

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2, ο οποίος εντοπίζοντας ένα εισερχόμενο *Reply* θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εξερχόμενα Requests* από το NetC.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το εισερχόμενο *Reply* με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests* το οποίο να έχει στείλει ο `Spoofed` στον `Target` και έτσι το *spoofing* θα ανιχνευτεί.

Τοπολογία Β

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον Target (Βήμα 1), οι οποίοι ανήκουν και οι δύο στο NetA, το πακέτο αυτό δεν θα γίνει αντιληπτό από τον `Sensor` στη θέση S1, καθώς ανήκει στο εσωτερικό traffic του δικτύου το οποίο ο `Sensor` στη θέση S1 δεν επεξεργάζεται.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1, ο οποίος εντοπίζοντας ένα εξερχόμενο *Reply* θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetA.

Ο Sensor στη θέση S1 δεν θα καταφέρει να αντιστοιχήσει το εξερχόμενο *Reply* με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests* το οποίο να έχει στείλει ο `Spoofed` στον `Target` και έτσι το *spoofing* θα ανιχνευτεί.

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2, ο οποίος εντοπίζοντας ένα εισερχόμενο *Reply* θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εξερχόμενα Requests* από το NetB.

Ο Sensor στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το εισερχόμενο *Reply* με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests* το οποίο να έχει στείλει ο Spoofed στον Target και έτσι το *spoofing* θα ανιχνευτεί.

Τοπολογία C

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον Attacker στον Target (Βήμα 1), το πακέτο αυτό θα περάσει από τον Sensor στη θέση S1, ο οποίος θα το αποθηκεύσει στα *Εισερχόμενα Requests* προς το NetB, σαν αυτό να έχει προέλθει από τον Spoofed.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον Target στον Spoofed (Βήμα 2), το πακέτο αυτό θα περάσει από τον Sensor στη θέση S1, ο οποίος εντοπίζοντας ένα εξερχόμενο *Reply* θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetB.

Ο Sensor στη θέση S1 θα καταφέρει να αντιστοιχήσει το εξερχόμενο *Reply* με το *Εισερχόμενο Request* που υποτίθεται ότι έστειλε ο Spoofed στον Target και το οποίο αποθήκευσε προηγουμένως και έτσι το *spoofing* δεν θα ανιχνευτεί.

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον Attacker στον Target (Βήμα 1), το πακέτο αυτό θα περάσει από τον Sensor στη θέση S2, ο οποίος θα το αποθηκεύσει στα *Εξερχόμενα Requests* από το NetA, σαν αυτό να έχει προέλθει από τον Spoofed.

Κατά την αποστολή του *Icmp Echo Reply* από τον Target στον Spoofed (Βήμα 2), το πακέτο αυτό θα περάσει από τον Sensor στη θέση S2, ο οποίος εντοπίζοντας ένα εισερχόμενο *Reply* θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εξερχόμενα Requests* από το NetA.

Ο Sensor στη θέση S2 θα καταφέρει να αντιστοιχήσει το εισερχόμενο *Reply* με το *Εξερχόμενο Request* που υποτίθεται ότι έστειλε ο Spoofed στον Target και το οποίο αποθήκευσε προηγουμένως και έτσι το *spoofing* δεν θα ανιχνευτεί.

A.1.2 Εξαγόμενα Συμπεράσματα

Όταν εξετάζεται ένα *Icmp Echo Reply* πακέτο για την ανίχνευση πιθανών *spoofed Icmp Echo Request* πακέτων, σημαντικό ρόλο παίζει η φορά του *Reply* ως προς το προστατευόμενο

δίκτυο. Δηλαδή εάν το πακέτο αυτό προορίζεται προς το προστατευόμενο δίκτυο (εισερχόμενο) ή αν προέρχεται από το προστατευόμενο δίκτυο (εξερχόμενο).
Σε κάθε περίπτωση, εφόσον το *spoofing* ανιχνευτεί, τα συμπεράσματα που εξάγονται είναι διαφορετικά και η πληροφορία που παράγεται, βοηθάει στην κατανόηση του τρόπου με τον οποίο το *spoofing* υλοποιήθηκε.
Έτσι εάν το πακέτο που εντοπίστηκε είναι ένα :

- **Εισερχόμενο *Icmp Echo Reply***

  - ☞ Θα γίνει έλεγχος των αποθηκευμένων *Εξερχόμενων Requests* προς αναζήτηση του αντίστοιχου εξερχόμενου από το προστατευόμενο δίκτυο *Icmp Echo Request* πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και παραλήπτη τον αποστολέα του *Reply*.

  - ☞ Σε περίπτωση που ανιχνευτεί το *spoofing*, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Spoofed`, του οποίου την διεύθυνση, χρησιμοποιεί ο `Attacker` ως διεύθυνση αποστολέα σε *spoofed Icmp Echo Request* πακέτα, που στέλνει.

  - ☞ Το *spoofing* δεν θα ανιχνευτεί στην περίπτωση που ο `Attacker` (αυτός που στέλνει τα *spoofed* πακέτα), ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Spoofed`, του οποίου την διεύθυνση χρησιμοποιεί ως διεύθυνση αποστολέα στα *spoofed* πακέτα που στέλνει.

ⓘ Έτσι όταν το *spoofing* ανιχνευτεί (Τοπολογίες A, B) το συμπέρασμα που εξάγεται είναι :

Alert a1 📣

> *Κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
> *στέλνει ένα **spoofed Icmp Echo Request** πακέτο,*
> *σε κάποιον άλλο Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
> *προσποιούμενος ότι είναι κάποιος Host **που ανήκει** στο προστατευόμενο*

Συμβολισμός

- **Εξερχόμενο *Icmp Echo Reply***

  - ☞ Θα γίνει έλεγχος των αποθηκευμένων *Εισερχόμενων Requests* προς αναζήτηση του αντίστοιχου εισερχόμενου προς το προστατευόμενο δίκτυο *Icmp Echo Request*

πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και παραλήπτη τον αποστολέα του *Reply*.

☞ Σε περίπτωση που ανιχνευτεί το *spoofing*, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Target`, στον οποίο στέλνει ο `Attacker` *spoofed Icmp Echo Request* πακέτα, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.

☞ Το *spoofing* δεν θα ανιχνευτεί στην περίπτωση που ο `Attacker` (αυτός που στέλνει τα *spoofed* πακέτα), δεν ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Target`.

ⓘ Έτσι όταν το *spoofing* ανιχνευτεί (Τοπολογία B) το συμπέρασμα που εξάγεται είναι :

Alert a2

*Κάποιος Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Request** πακέτο*
*σε κάποιον άλλο Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*προσποιούμενος ότι είναι κάποιος Host που **δεν ανήκει** στο προστατευόμενο*

Συμβολισμός

Στον επόμενο πίνακα παρουσιάζονται συγκεντρωμένα τα αποτελέσματα από την μελέτη που έγινε προηγουμένως, όσο αναφορά την ανίχνευση των *spoofed Icmp Echo Request* πακέτων, εξετάζοντας τα *Icmp Echo Reply* πακέτα που εισέρχονται και εξέρχονται από το προστατευόμενο δίκτυο.

Στη 1η στήλη του πίνακα αναφέρεται η φορά σχετικά με το προστατευόμενο δίκτυο, που έχει το *Icmp Echo Reply* πακέτο που εντοπίζει ο `Sensor`. Επίσης αναφέρεται ο αποστολέας και ο παραλήπτης του πακέτου αυτού.

Στη συνέχεια αναφέρεται η θέση του κάθε συστήματος που παίρνει μέρος στην διαδικασία σε σχέση με το προστατευόμενο δίκτυο, δηλαδή εάν βρίσκεται εντός ή εκτός από αυτό.

Η επόμενη στήλη δηλώνει την τοπολογία του σχήματος 2, που αντιστοιχεί στην συγκεκριμένη διάταξη.

Στην επόμενη στήλη δηλώνεται για ποιον host ανιχνεύεται (εάν ανιχνεύεται) το *spoofing* από τον `Sensor`.

Στην προτελευταία στήλη αναφέρεται εάν το *spoofing* είναι δυνατόν να ανιχνευτεί σε κάθε περίπτωση.

Στην τελευταία στήλη αναγράφεται το alert που παράγεται σε κάθε περίπτωση που θα ανιχνευτεί το *spoofing* όπως προέκυψε από την παραπάνω μελέτη.

Ανίχνευση των ***spoofed Icmp Echo Request*** πακέτων, εξετάζοντας τα ICMP ECHO REPLY πακέτα.								
Φορά του *Icmp Echo Reply* Πακέτου	**Θέση του κάθε Host σε σχέση με το Προστατευόμενο Δίκτυο**				**Τοπολογία**	**Ανίχνευση για τον**	**Ανίχνευση**	**Alert**
	Attacker	**Spoofed**	**Target**	**Sensor**				
Εισερχόμενο (Target → Spoofed)	Out	**In**	Out	S2	A	Spoofed	**NAI**	**a1**
	Out	**In**	Out	S2	B	Spoofed	**NAI**	**a1**
	In	**In**	Out	S2	C	Spoofed	**OXI**	--
Εξερχόμενο (Target → Spoofed)	Out	Out	**In**	S1	A	Target	**OXI**	--
	In	Out	**In**	S1	B	Target	**NAI**	**a2**
	Out	Out	**In**	S1	C	Target	**OXI**	--

Πίνακας Α-1 : Συμπεράσματα για την Ανίχνευση των spoofed *Icmp Echo Request* πακέτων, εξετάζοντας τα *Icmp Echo Reply* πακέτα.

Α.2. Ανίχνευση του *spoofed Icmp Echo Reply* πακέτου

Σενάριο

Βήμα 1 : **Attacker [Spoofed]** → **Icmp Echo Reply** → **Target**

Ο Attacker στέλνει ένα *spoofed Icmp Echo Reply* στον Target, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του Spoofed.

Στόχος είναι με τον έλεγχο που θα γίνει στο *Icmp Echo Reply* πακέτο που εντοπίζεται από τον Sensor, να ανιχνευτεί αν αυτό το πακέτο είναι ένα *spoofed* πακέτο ή αν είναι ένα νόμιμο πακέτο, με την έννοια ότι προηγήθηκε το αντίστοιχο *Icmp Echo Request* πακέτο που οδήγησε στην δημιουργία του.

Α.2.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Reply* πακέτου από τον Attacker στον Target (Βήμα 1), το πακέτο αυτό θα περάσει από τον Sensor στη θέση S1.

Εντοπίζοντας ένα εισερχόμενο *Reply* ο Sensor στη θέση S1, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εξερχόμενα Requests* από το NetB.

Ο Sensor στη θέση S1 δεν θα καταφέρει να αντιστοιχήσει το εισερχόμενο *Reply* με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests* το οποίο να έχει στείλει ο Target στον Spoofed και έτσι το *spoofing* θα ανιχνευτεί.

Τοπολογία Β

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Reply* πακέτου από τον Attacker στον Target (Βήμα 1), οι οποίοι ανήκουν και οι δύο στο NetA, το πακέτο αυτό δεν θα γίνει αντιληπτό από τον Sensor στη θέση S1, καθώς ανήκει στο εσωτερικό traffic του δικτύου το οποίο ο Sensor στη θέση S1 δεν επεξεργάζεται. Το *spoofing* δεν θα ανιχνευτεί.

Τοπολογία C

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Reply* πακέτου από τον Attacker στον Target (Βήμα 1), το πακέτο αυτό θα περάσει από τον Sensor στη θέση S1.
Εντοπίζοντας ένα εισερχόμενο *Reply* ο Sensor στη θέση S1, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εξερχόμενα Requests* από το NetB.

Ο `Sensor` στη θέση S1 δεν θα καταφέρει να αντιστοιχήσει το εισερχόμενο *Reply* με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests* το οποίο να έχει στείλει ο `Target` στον `Spoofed` και έτσι το *spoofing* θα ανιχνευτεί.

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή του *spoofed Icmp Echo Reply* πακέτου από τον `Attacker` στον `Target` (Βήμα 1), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.

Εντοπίζοντας ένα εξερχόμενο *Reply* ο `Sensor` στη θέση S2, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetA.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το εξερχόμενο *Reply* με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests* το οποίο να έχει στείλει ο `Target` στον `Spoofed` και έτσι το *spoofing* θα ανιχνευτεί.

A.2.2 Εξαγόμενα Συμπεράσματα

Όταν εξετάζεται ένα *Icmp Echo Reply* πακέτο για την ανίχνευση πιθανών *spoofed Icmp Echo Reply* πακέτων, σημαντικό ρόλο παίζει η φορά του *Reply* ως προς το προστατευόμενο δίκτυο. Δηλαδή εάν το πακέτο αυτό προορίζεται προς το προστατευόμενο δίκτυο (εισερχόμενο) ή αν προέρχεται από το προστατευόμενο δίκτυο (εξερχόμενο).
Σε κάθε περίπτωση, εφόσον το *spoofing* ανιχνευτεί, τα συμπεράσματα που εξάγονται είναι διαφορετικά και η πληροφορία που παράγεται βοηθάει στην κατανόηση του τρόπου με τον οποίο το *spoofing* υλοποιήθηκε.
Έτσι εάν το πακέτο που εντοπίστηκε είναι ένα :

➢ **Εισερχόμενο *Icmp Echo Reply***

☞ Θα γίνει έλεγχος των αποθηκευμένων *Εξερχόμενων Requests* προς αναζήτηση του αντίστοιχου εξερχόμενου από το προστατευόμενο δίκτυο *Icmp Echo Request* πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και παραλήπτη τον αποστολέα του *Reply*.

☞ Σε περίπτωση που ανιχνευτεί το *spoofing*, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Target`, στον οποίο στέλνει ο `Attacker` τα *spoofed Icmp Echo Reply* πακέτα, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.

☞ Το *spoofing* δεν θα ανιχνευτεί στην περίπτωση που ο `Attacker` ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Target` (Τοπολογία B), καθώς τα *spoofed Icmp Echo Reply* πακέτα που του στέλνει ανήκουν στο εσωτερικό traffic του δικτύου και ο `Sensor` δεν τα επεξεργάζεται.

ⓘ Έτσι όταν το *spoofing* ανιχνευτεί (Τοπολογίες A, C) το συμπέρασμα που εξάγεται είναι :

Alert a3 📣

*Κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Reply** πακέτο,*
*σε κάποιον Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*προσποιούμενος ότι είναι κάποιος άλλος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο.*

Συμβολισμός

- **Εξερχόμενο *Icmp Echo Reply***

  ☞ Θα γίνει έλεγχος των αποθηκευμένων *Εισερχόμενων Requests* προς αναζήτηση του αντίστοιχου εισερχόμενου προς το προστατευόμενο δίκτυο *Icmp Echo Request* πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και παραλήπτη τον αποστολέα του *Reply*.

  ☞ Σε περίπτωση που ανιχνευτεί το *spoofing*, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Spoofed`, του οποίου την διεύθυνση, χρησιμοποιεί ο `Attacker` ως διεύθυνση αποστολέα σε *spoofed Icmp Echo Request* πακέτα, που στέλνει.

  ☞ Το *spoofing* θα ανιχνευτεί στην περίπτωση που ο `Attacker` (αυτός που στέλνει τα *spoofed* πακέτα), ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Spoofed`, του οποίου την διεύθυνση χρησιμοποιεί ως διεύθυνση αποστολέα στα *spoofed* πακέτα που στέλνει.

ⓘ Έτσι όταν το *spoofing* ανιχνευτεί (Τοπολογία C) το συμπέρασμα που εξάγεται είναι :

Alert a4

*Κάποιος Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Reply** πακέτο*
*σε κάποιον Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
*προσποιούμενος ότι είναι κάποιος άλλος Host που **ανήκει** στο προστατευόμενο δίκτυο.*

Συμβολισμός

Στον επόμενο πίνακα παρουσιάζονται συγκεντρωμένα τα αποτελέσματα από την μελέτη που έγινε προηγουμένως, όσο αναφορά την ανίχνευση των *spoofed Icmp Echo Reply* πακέτων, εξετάζοντας τα *Icmp Echo Reply* πακέτα που εισέρχονται και εξέρχονται από το προστατευόμενο δίκτυο.

Στη 1η στήλη του πίνακα αναφέρεται η φορά σχετικά με το προστατευόμενο δίκτυο, που έχει το *Icmp Echo Reply* πακέτο που εντοπίζει ο `Sensor`. Επίσης αναφέρεται ο αποστολέας και ο παραλήπτης του πακέτου αυτού.

Στη συνέχεια αναφέρεται η θέση του κάθε συστήματος που παίρνει μέρος στην διαδικασία σε σχέση με το προστατευόμενο δίκτυο, δηλαδή εάν βρίσκεται εντός ή εκτός από αυτό.

Η επόμενη στήλη δηλώνει την τοπολογία του Σχήματος 2, που αντιστοιχεί στην συγκεκριμένη διάταξη.

Στην επόμενη στήλη δηλώνεται για ποιον host ανιχνεύεται (εάν ανιχνεύεται) το *spoofing* από τον `Sensor`.

Στην προτελευταία στήλη αναφέρεται εάν το *spoofing* είναι δυνατόν να ανιχνευτεί σε κάθε περίπτωση.

Στην τελευταία στήλη αναγράφεται το alert που παράγεται σε κάθε περίπτωση που θα ανιχνευτεί το *spoofing* όπως προέκυψε από την παραπάνω μελέτη.

Ανίχνευση των ***spoofed Icmp Echo Reply*** πακέτων, εξετάζοντας τα **ICMP ECHO REPLY** πακέτα.								
Φορά του Icmp Echo Reply Πακέτου	**Θέση του κάθε Host σε σχέση με το Προστατευόμενο Δίκτυο**				**Τοπολογία**	**Ανίχνευση για τον**	**Ανίχνευση**	**Alert**
	Attacker	**Spoofed**	**Target**	**Sensor**				
Εισερχόμενο (Attacker → Target)	Out	Out	**In**	S1	A	Target	**NAI**	**a3**
	In	Out	**In**	S1	B	Target	**OXI**	--
	Out	Out	**In**	S1	C	Target	**NAI**	**a3**
Εξερχόμενο (Attacker → Target)	Out	**In**	Out	S2	A	Spoofed	**OXI**	--
	Out	**In**	Out	S2	B	Spoofed	**OXI**	--
	In	**In**	Out	S2	C	Spoofed	**NAI**	**a4**

Πίνακας Α-2 : Συμπεράσματα για την Ανίχνευση των spoofed *Icmp Echo Reply* πακέτων, εξετάζοντας τα *Icmp Echo Reply* πακέτα.

Α.3. Επίλογος Για τον Έλεγχο των *Icmp Echo Reply* πακέτων.

Όταν εντοπιστεί ένα *Icmp Echo Reply* πακέτο, το πακέτο αυτό ελέγχεται για να ανιχνευτεί αν αυτό έχει προέλθει από κάποια διαδικασία *spoofing*, δηλαδή αν αυτό το πακέτο είναι απάντηση σε ένα *spoofed Icmp Echo Request* πακέτο ή αν το ίδιο το πακέτο είναι *spoofed*.

Η τεχνική της ανίχνευσης του *spoofing* με την εξέταση ενός *Icmp Echo Reply* πακέτου, ελέγχει την φορά του πακέτου ως προς το προστατευόμενο δίκτυο, δηλαδή εάν εισέρχεται ή εξέρχεται από αυτό.
Στη συνέχεια γίνεται προσπάθεια συσχέτισης του *Icmp Echo Reply* με το αντίστοιχο *Icmp Echo Request* από τα *Εισερχόμενα* ή τα *Εξερχόμενα Requests* που αποθηκεύονται για το προστατευόμενο δίκτυο.
Ένα εισερχόμενο *Reply* πρέπει να αντιστοιχηθεί με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests*, ενώ ένα εξερχόμενο *Reply* πρέπει να αντιστοιχηθεί με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests*.
Σε κάθε περίπτωση το υπό αναζήτηση αντίστοιχο *Request*, θα πρέπει να έχει ως διεύθυνση αποστολέα τον παραλήπτη του *Reply* και ως διεύθυνση παραλήπτη τον αποστολέα του *Reply*.

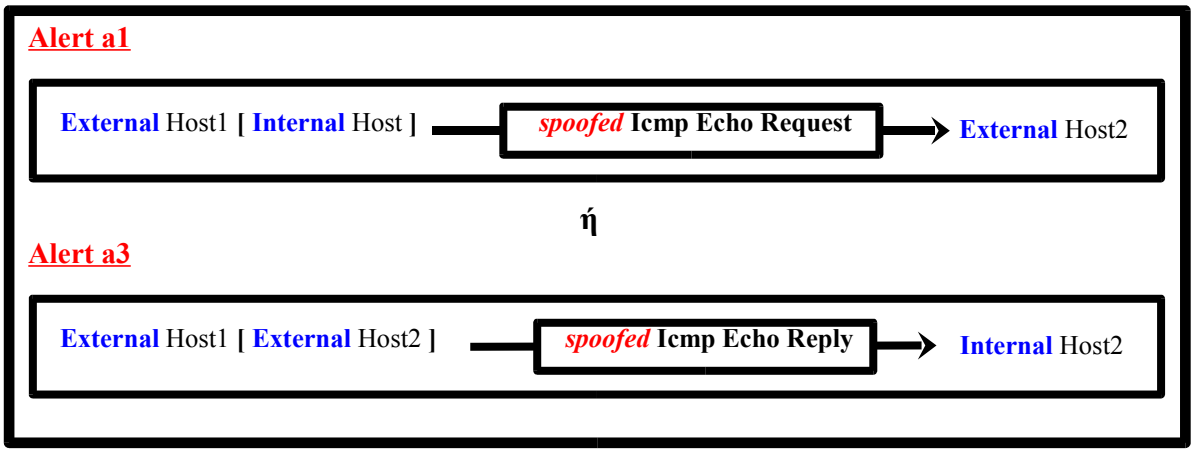
Στην περίπτωση που βρεθεί το αντίστοιχο αποθηκευμένο *Request*, η παρουσία του *Icmp Echo Reply* πακέτου θα θεωρηθεί φυσιολογική και το *spoofing* (εάν υφίσταται) δεν θα ανιχνευτεί.
Σε αντίθετη περίπτωση το *spoofing* θα ανιχνευτεί και όπως αποδείχτηκε από την παραπάνω μελέτη, ανάλογα με την φορά του πακέτου ως προς το προστατευόμενο δίκτυο τα συμπεράσματα που εξάγονται, εκτός από την επισήμανση για την ύπαρξη του *spoofing*, δίνουν επίσης σημαντική πληροφορία για το πως αυτό υλοποιήθηκε, όσο αναφορά την θέση του κάθε host, που πήρε μέρος στην διαδικασία, σε σχέση με το προστατευόμενο δίκτυο.

Έτσι τα πιθανά Alerts που μπορούν να δημιουργηθούν αν το *spoofing* ανιχνευτεί μετά τον έλεγχο ενός *Icmp Echo Reply* πακέτου, είναι τα παρακάτω :

Σημείωση

Ο host που φαίνεται μαρκαρισμένος στο κάθε alert είναι αυτός που ανήκει στο προστατευόμενο δίκτυο και για τον οποίο ανιχνεύεται το *spoofing* από τον Sensor. Ο host αυτός μπορεί να παίζει τον ρόλο είτε του Spoofed (η δικιά του διεύθυνση χρησιμοποιείται σε *spoofed* πακέτα που στέλνονται από κάποιον άλλον), είτε του Target (σε αυτόν στέλνονται τα *spoofed* πακέτα).

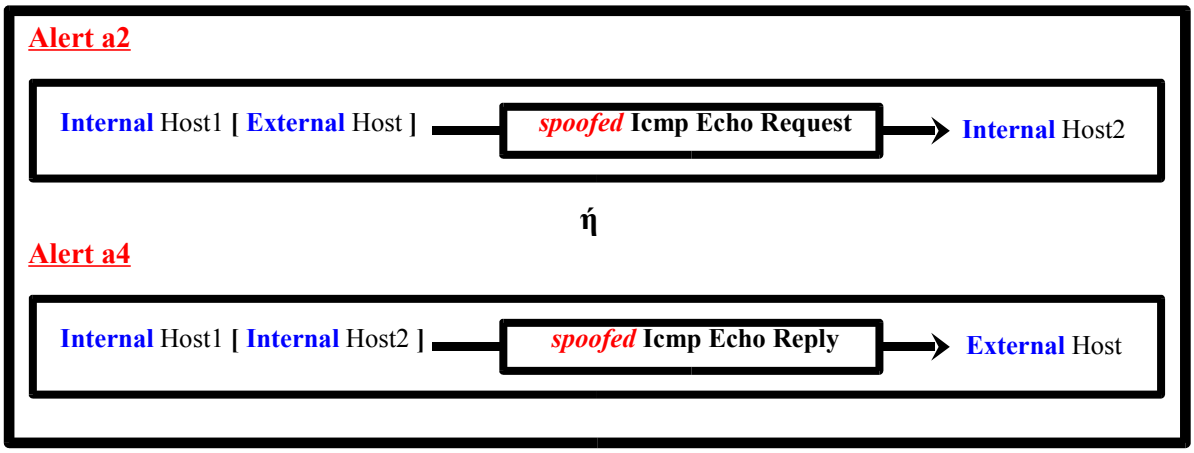
Alert A1



Το Alert A1 αποτελείται από δύο σκέλη, τα οποία είναι τα δύο πιθανά σενάρια που μπορεί να ισχύουν ώστε να δημιουργηθεί το Alert A1.
Και τα δύο αυτά alerts κατά τον έλεγχο ικανοποιούν τις ίδιες συνθήκες και γι' αυτό δεν είναι δυνατόν να γίνει ένας πιο συγκεκριμένος διαχωρισμός μεταξύ τους.
Οι συνθήκες που ικανοποιούνται κατά τον έλεγχο και δημιουργείται το Alert A1 είναι οι παρακάτω :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Echo Reply* πακέτο.
- Το *Icmp Echo Reply* πακέτο είναι ένα εισερχόμενο προς το προστατευόμενο δίκτυο πακέτο.
- Δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό το *Icmp Echo Reply* πακέτο στα αποθηκευμένα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο.

Alert A2



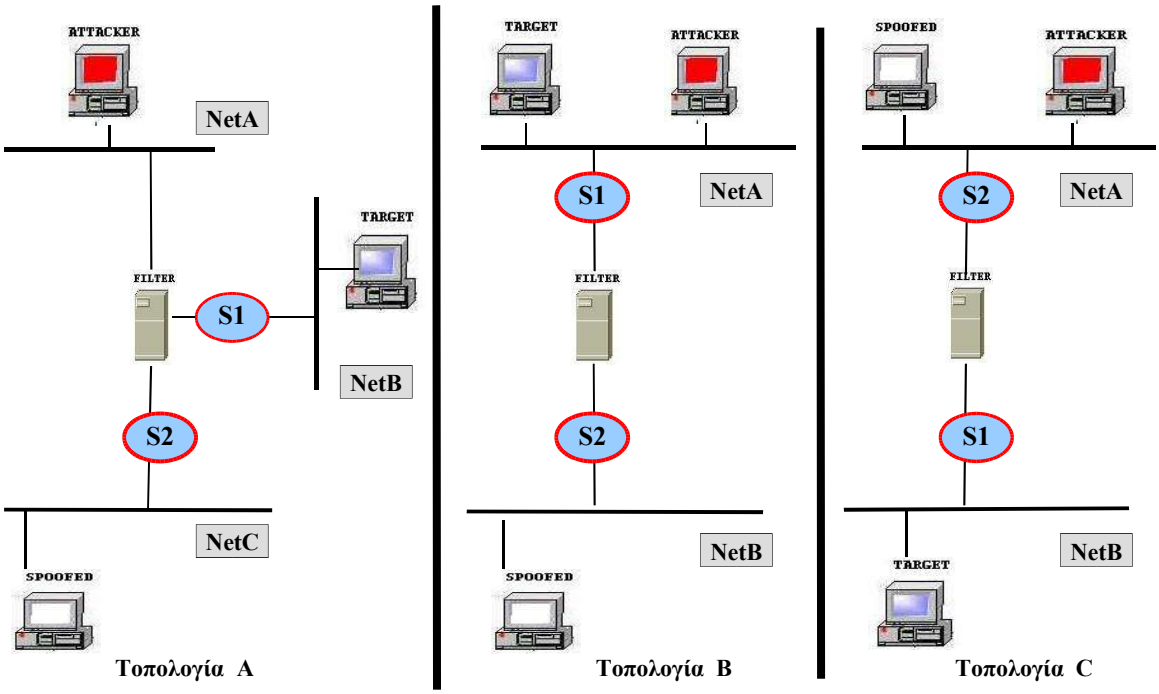
Το Alert A2 αποτελείται και αυτό από δύο σκέλη, που αντιστοιχούν σε δύο πιθανά σενάρια που μπορεί να ισχύουν, ώστε να δημιουργηθεί το Alert A2.
Και τα δύο αυτά alerts κατά τον έλεγχο ικανοποιούν και σε αυτή την περίπτωση τις ίδιες συνθήκες και γι' αυτό δεν είναι δυνατόν να γίνει ένας πιο συγκεκριμένος διαχωρισμός μεταξύ τους.
Οι συνθήκες που ικανοποιούνται κατά τον έλεγχο και δημιουργείται αυτό το Alert A2 είναι οι παρακάτω :

- Το πακέτο που ελέγχεται είναι ένα *Icmp Echo Reply* πακέτο.
- Το *Icmp Echo Reply* πακέτο είναι ένα εξερχόμενο από το προστατευόμενο δίκτυο πακέτο.
- Δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό το *Icmp Echo Reply* πακέτο στα αποθηκευμένα *Εισερχόμενα Requests* προς το προστατευόμενο δίκτυο.

ΜΕΡΟΣ Β

Έλεγχος του *Icmp Destination Unreachable –Net/Host Unreachable* Πακέτου (Type 3, Code 0/1*)*

Στο σημείο αυτό παρουσιάζεται ξανά το **Σχήμα 2** έτσι ώστε να είναι πιο εύκολη η πρόσβαση σε αυτό, κατά την περιγραφή της διαδικασίας.



Σχήμα 2: Πιθανές Τοπολογίες

Στην παρουσίαση του *Icmp* πρωτοκόλλου αναφέρθηκε ότι το *Icmp Error* μήνυμα έχει προορισμό τον αποστολέα του αρχικού πακέτου, που οδήγησε στην δημιουργία του Error μηνύματος. Έτσι αν ένα τέτοιο πακέτο εντοπιστεί από τον `Sensor` αυτό δηλώνει ότι κάποιος από το προστατευόμενο δίκτυο έστειλε το αρχικό πακέτο που το δημιούργησε.

Το *Icmp Destination Unreachable Code 0/1* που στέλνει το `Filter` σε κάποιον host του προστατευόμενου δικτύου, δηλώνει ότι κάποιο πακέτο που στάλθηκε από αυτόν τον host, δεν μπόρεσε να φτάσει στον προορισμό του γιατί ο παραλήπτης (ή το δίκτυό του) δεν υπάρχει.
Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος, θα περιέχεται στα data του *Icmp Destination Unreachable* πακέτου (μέρος του ή ολόκληρο).

Από τα *Icmp Destination Unreachable Code 0/1* πακέτα, αυτά που παρουσιάζουν ενδιαφέρον για την παρούσα μελέτη, είναι αυτά που περιέχουν ένα *Icmp Echo Request* ή ένα *Icmp Echo Reply* σαν το αρχικό πακέτο που δημιούργησε αυτό το *Icmp Error* μήνυμα.

Διαδικασία Ανίχνευσης

Ο `Sensor` εντοπίζει ένα *Icmp Destination Unreachable Code 0/1* το οποίο περιέχει στα data του ένα *Icmp Echo Request* ή ένα *Icmp Echo Reply* πακέτο (μέρος του ή ολόκληρο), το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος.
Το πακέτο αυτό προέρχεται από το `Filter` και προορίζεται προς το προστατευόμενο δίκτυο.
Η παρουσία του πακέτου αυτού δηλώνει ότι προηγήθηκε μέσα από το προστατευόμενο δίκτυο η αποστολή του αρχικού πακέτου που δημιούργησε το *Icmp Error* μήνυμα.

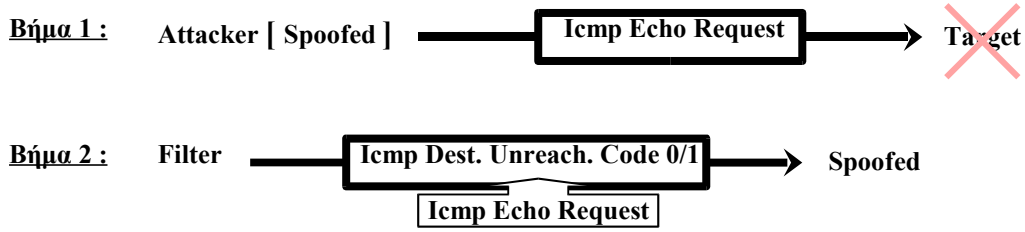
Έτσι αν το *Icmp Error* μήνυμα περιέχει ένα *Icmp Echo Request* πακέτο, το πακέτο αυτό θα πρέπει να έχει καταγραφεί και στα αποθηκευμένα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο.
Η επιτυχία ή η αποτυχία της αναζήτησης του πακέτου αυτού στα αποθηκευμένα *Εξερχόμενα Requests*, θα οδηγήσει στην ανίχνευση του *spoofing*.

Αν το *Icmp Error* μήνυμα περιέχει ένα *Icmp Echo Reply* πακέτο, θα πρέπει να έχει καταγραφεί στα αποθηκευμένα *Εισερχόμενα Requests* προς το προστατευόμενο δίκτυο, το αντίστοιχο *Icmp Echo Request* πακέτο, που έχει ως αποστολέα τον παραλήπτη του *Reply* και ως παραλήπτη τον αποστολέα του *Reply*.
Η επιτυχία ή η αποτυχία της αναζήτησης του πακέτου αυτού στα αποθηκευμένα *Εισερχόμενα Requests* θα οδηγήσει στην ανίχνευση του *spoofing*.

B.1. Ανίχνευση του *spoofed Icmp Echo Request* πακέτου

B.1.1. Το *Icmp Destination Unreachable Code 0/1* περιέχει ένα *Icmp Echo Request*

Σενάριο



Αρχικά (Βήμα 1) ο `Attacker` στέλνει ένα *spoofed Icmp Echo Request* στον `Target`, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.
Ο `Target` όμως (ή το δίκτυό του) δεν υπάρχει και το πακέτο δεν μπορεί να δρομολογηθεί στον προορισμό του.
Στη συνέχεια (Βήμα 2) το Filter καθώς δεν μπορεί να δρομολογήσει το πακέτο στον ανύπαρκτο `Target`, απαντάει στον `Spoofed` στέλνοντάς του ένα *Icmp Destination Unreachable Code 0 /1*, το οποίο περιέχει το *Icmp Echo Request* πακέτο που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target`.

Στόχος με τον έλεγχο που θα γίνει στο *Icmp Destination Unreachable Code 0/1* πακέτο που εντοπίζεται από τον Sensor, είναι να ανιχνευτεί αν το *Icmp Echo Request* που περιέχει, το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και που υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο, είναι ένα *spoofed* πακέτο.

B.1.1.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον ανύπαρκτο `Target` (ή το ανύπαρκτο δίκτυό του), το πακέτο δεν θα μπορέσει να δρομολογηθεί από το `Filter` στον προορισμό του.

Στη συνέχεια (Βήμα 2) κατά την αποστολή του *Icmp Destination Unreachable Code 0/1* από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Request* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Request* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed`, θα αναζητήσει το πακέτο αυτό στα αποθηκευμένα *Εξερχόμενα Requests* από το NetC.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το *Icmp Request* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 0/1*, με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests* το οποίο να έχει στείλει ο `Spoofed` στον `Target` και έτσι το *spoofing* θα ανιχνευτεί.

Τοπολογία Β

Σε αυτή την τοπολογία το σενάριο δεν έχει εφαρμογή καθώς το *spoofed Icmp Echo Request* από τον `Attacker` στον ανύπαρκτο `Target`, δεν θα φτάσει ποτέ στο `Filter` αλλά ούτε και στον `Sensor`.
Το πακέτο αυτό καθώς ανήκει στο εσωτερικό traffic του NetA, ο `Sensor` δεν θα το επεξεργαστεί.

Τοπολογία C

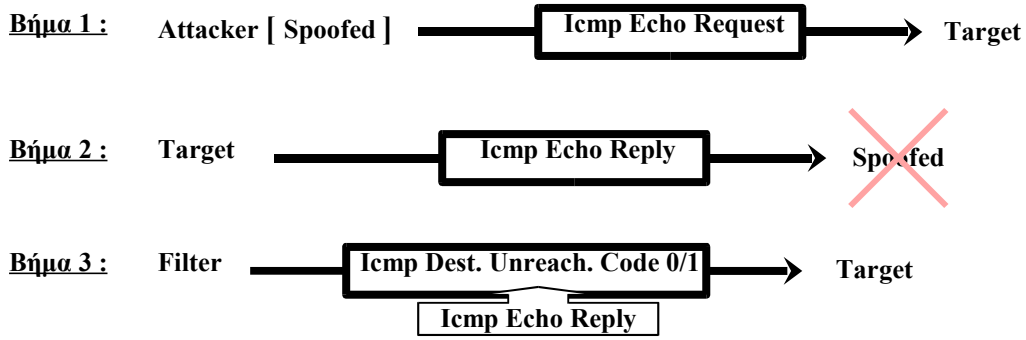
➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου (Βήμα 1) από τον `Attacker` στον ανύπαρκτο `Target` (ή το ανύπαρκτο δίκτυό του) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2, ο οποίος θα το αποθηκεύσει στα *Εξερχόμενα Requests* από το NetA, σαν αυτό να έχει προέλθει από τον `Spoofed`.

Στη συνέχεια το πακέτο θα φτάσει στο `Filter`, το οποίο δεν θα μπορέσει να το δρομολογήσει στον προορισμό του.
Κατά την αποστολή του *Icmp Destination Unreachable Code 0/1* (Βήμα 2) από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Request* πακέτο), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Request* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed`, θα αναζητήσει το πακέτο αυτό στα αποθηκευμένα *Εξερχόμενα Requests* από το NetA.
Ο `Sensor` στη θέση S2 θα καταφέρει να αντιστοιχήσει το *Icmp Request* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 0/1*, με το πακέτο που αποθήκευσε προηγουμένως στα *Εξερχόμενα Requests* το οποίο υποτίθεται ότι έστειλε ο `Spoofed` στον `Target` και έτσι το *spoofing* δεν θα ανιχνευτεί.

B.1.2. Το *Icmp Destination Unreachable Code 0/1* περιέχει ένα *Icmp Echo Reply*

Σενάριο



Αρχικά (Βήμα 1) ο `Attacker` στέλνει ένα *spoofed Icmp Echo Request* στον `Target`, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed` ο οποίος όμως (ή το δίκτυό του) δεν υπάρχει.
Στη συνέχεια (Βήμα 2) ο `Target` απαντάει στον ανύπαρκτο `Spoofed` στέλνοντάς του ένα *Icmp Echo Reply*.
Ο `Spoofed` όμως (ή το δίκτυό του) δεν υπάρχει και το πακέτο δεν μπορεί να δρομολογηθεί στον προορισμό του.
Στη συνέχεια (Βήμα 3) το `Filter` καθώς δεν μπορεί να δρομολογήσει το πακέτο στον ανύπαρκτο `Spoofed`, απαντάει στον `Target` στέλνοντάς του ένα *Icmp Destination Unreachable Code 0 /1*, το οποίο περιέχει το *Icmp Echo Reply* πακέτο που έστειλε ο `Target` στον `Spoofed`.

Στόχος με τον έλεγχο που θα γίνει στο *Icmp Destination Unreachable Code 0/1* πακέτο που εντοπίζεται από τον `Sensor`, είναι να ανιχνευτεί αν το *Icmp Echo Reply* που περιέχει το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και που υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο, έχει προέλθει από ένα *spoofed Icmp Echo Request* πακέτο.

Γενικός Κανόνας

Ένα Icmp Destination Unreachable Code 0/1το οποίο περιέχει ένα Icmp Echo Reply είναι κατεξοχήν απόρροια ενός spoofed πακέτου. Αυτό το συμπέρασμα βγαίνει καθώς δεν είναι δυνατόν κάποιος host να στέλνει ένα Reply σε κάποιον που υποτίθεται ότι του έστειλε ένα Request και αυτός (ή το δίκτυό του) να μην υπάρχει.

B.1.2.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target`, το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1, ο οποίος θα το αποθηκεύσει στα *Εισερχόμενα Requests* προς το NetB, σαν αυτό να έχει προέλθει από τον `Spoofed`.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον ανύπαρκτο `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1 και θα φτάσει στο `Filter`.

> **Σημείωση**
>
> Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S1 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων . Από αυτόν τον έλεγχο το *spoofing* δεν θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 0/1* (Βήμα 3) από το `Filter` στον `Target` (ο οποίος έστειλε το *Icmp Echo Reply* πακέτο), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1.
Ο `Sensor` στη θέση S1 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα εξερχόμενο *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Target` στον `Spoofed`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Spoofed` προς τον `Target`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetB.

Ο `Sensor` στη θέση S1 θα καταφέρει να αντιστοιχήσει το εξερχόμενο από το NetB *Icmp Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 0/1*, με το *Εισερχόμενο Request* που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target` και το οποίο αποθήκευσε προηγουμένως και έτσι το *spoofing* δεν θα ανιχνευτεί.

Ενώ μέσα από αυτή τη διαδικασία το *spoofing* δεν γίνεται αντιληπτό, είναι δυνατόν να ανιχνευτεί από την ισχύ του Γενικού Κανόνα , καθώς δεν είναι δυνατόν ο `Target` να στέλνει ένα *Reply* σε κάποιον που υποτίθεται ότι του έστειλε ένα *Request* και αυτός (ή το δίκτυό του) να μην υπάρχει. Έτσι το *spoofing* θα ανιχνευτεί.

Τοπολογία Β

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target` (Βήμα 1), οι οποίοι ανήκουν και οι δύο στο NetA, το πακέτο αυτό δεν θα γίνει αντιληπτό από τον `Sensor` στη θέση S1, καθώς ανήκει στο εσωτερικό traffic του δικτύου το οποίο ο `Sensor` στη θέση S1 δεν επεξεργάζεται.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον ανύπαρκτο `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1 και θα φτάσει στο Filter.

Σημείωση

Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S1 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων. Από αυτόν τον έλεγχο το *spoofing* θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 0/1* (Βήμα 3) από το `Filter` στον `Target` (ο οποίος έστειλε το *Icmp Echo Reply* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1.
Ο `Sensor` στη θέση S1 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Target` στον `Spoofed`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Spoofed` προς τον `Target`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetA.

Ο `Sensor` στη θέση S1 δεν θα καταφέρει να αντιστοιχήσει το εξερχόμενο *Icmp Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 0/1*, με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests* το οποίο να έχει στείλει ο `Spoofed` στον `Target` και έτσι το *spoofing* θα ανιχνευτεί

Παράλληλα με αυτήν τη διαδικασία το *spoofing* είναι δυνατόν να ανιχνευτεί και από την ισχύ του Γενικού Κανόνα

Τοπολογία C

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target` (Βήμα 1), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1, ο οποίος θα το αποθηκεύσει στα *Εισερχόμενα Requests* προς το NetB, σαν αυτό να έχει προέλθει από τον `Spoofed`.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον ανύπαρκτο `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1 και θα φτάσει στο `Filter`.

Σημείωση

Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S1 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων. Από αυτόν τον έλεγχο το *spoofing* δεν θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 0/1* (Βήμα 3) από το `Filter` στον `Target` (ο οποίος έστειλε το *Icmp Echo Reply* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1.
Ο `Sensor` στη θέση S1 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα εξερχόμενο *Icmp Echo Reply*, το οποίο υποτίθεται ότι έχει στείλει ο `Target` στον `Spoofed`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Spoofed` προς τον `Target`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetB.

Ο `Sensor` στη θέση S1 θα καταφέρει να αντιστοιχήσει το εξερχόμενο από το NetB *Icmp Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 0/1*, με το *Εισερχόμενο Request* που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target` και το οποίο αποθήκευσε προηγουμένως και έτσι το *spoofing* δεν θα ανιχνευτεί.

Ενώ μέσα από αυτή τη διαδικασία το *spoofing* δεν γίνεται αντιληπτό, είναι δυνατόν να ανιχνευτεί από την ισχύ του Γενικού Κανόνα , καθώς δεν είναι δυνατόν ο `Target` να στέλνει ένα *Reply* σε κάποιον που υποτίθεται ότι του έστειλε ένα *Request* και αυτός (ή το δίκτυό του) να μην υπάρχει. Έτσι το *spoofing* θα ανιχνευτεί.

B.1.3. Εξαγόμενα Συμπεράσματα

Όταν εξετάζεται ένα *Icmp Destination Unreachable Code 0/1* πακέτο για την ανίχνευση πιθανών *spoofed Icmp Echo Request* πακέτων, σημαντικό ρόλο παίζει το πακέτο που περιέχεται στα data του, και το οποίο είναι αυτό που δημιούργησε το *Icmp Error* μήνυμα.
Το εσωτερικό πακέτο μπορεί να είναι ένα *Icmp Echo Request* ή ένα *Icmp Echo Reply* και υποτίθεται ότι στάλθηκε από το προστατευόμενο δίκτυο.
Σε κάθε περίπτωση, εφόσον το *spoofing* ανιχνευτεί, τα συμπεράσματα που εξάγονται είναι διαφορετικά και η πληροφορία που παράγεται βοηθάει στην κατανόηση του τρόπου με τον οποίο το *spoofing* υλοποιήθηκε.
Έτσι εάν το *Icmp Destination Unreachable Code 0/1* πακέτο που εντοπίστηκε περιέχει ένα :

- ***Icmp Echo Request***

  - Το *Icmp Error* μήνυμα δημιουργήθηκε γιατί το *Icmp Echo Request* που περιέχει, δεν έφτασε στον προορισμό του καθώς ο `Target` (ή το δίκτυό του) δεν υπάρχει.

  - Το *Icmp Echo Request* υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο και πρέπει να γίνει έλεγχος των αποθηκευμένων *Εξερχόμενων Requests*, προς αναζήτηση του πακέτου αυτού.

  - Σε περίπτωση που ανιχνευτεί το spoofing, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Spoofed`, του οποίου την διεύθυνση, χρησιμοποιεί ο Attacker ως διεύθυνση αποστολέα σε *spoofed Icmp Echo Request* πακέτα, που στέλνει.

  - Το spoofing θα ανιχνευτεί στην περίπτωση που ο `Attacker` (αυτός που στέλνει τα spoofed πακέτα), δεν ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Spoofed`,

του οποίου την διεύθυνση χρησιμοποιεί ως διεύθυνση αποστολέα στα spoofed πακέτα που στέλνει.

ⓘ Έτσι όταν το *spoofing* ανιχνευτεί (Τοπολογίες A) το συμπέρασμα που εξάγεται είναι :

Alert b1

*Κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Request** πακέτο,*
*σε κάποιον άλλο Host που **δεν ανήκει** στο προστατευόμενο δίκτυο και **δεν υπάρχει**,*

Συμβολισμός

➢ ***Icmp Echo Reply***

☞ Το *Icmp Error* μήνυμα δημιουργήθηκε γιατί το *Icmp Echo Reply* που περιέχει δεν έφτασε στον προορισμό του καθώς ο `Spoofed` (ή το δίκτυό του) δεν υπάρχει.

☞ Το *Icmp Echo Reply* υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο και πρέπει να γίνει έλεγχος των αποθηκευμένων *Εισερχόμενων Requests*, προς αναζήτηση του αντίστοιχου εισερχόμενου προς το προστατευόμενο δίκτυο *Icmp Echo Request* πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και παραλήπτη τον αποστολέα του *Reply*.

☞ Σε περίπτωση που ανιχνευτεί το spoofing, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Target`, στον οποίο στέλνει ο `Attacker` spoofed *Icmp Echo Request* πακέτα, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.

☞ Το spoofing θα ανιχνευτεί σε κάθε περίπτωση με την ισχύ του Γενικού Κανόνα. Επιπρόσθετα όμως στην περίπτωση που ο `Attacker` ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Target`, στον οποίο στέλνει τα spoofed πακέτα , το spoofing θα ανιχνευτεί και με την καθιερωμένη διαδικασία της ανίχνευσης .

ⓘ Έτσι αν ισχύει μόνο ο Γενικός Κανόνας (Τοπολογίες A, C) το συμπέρασμα που εξάγεται είναι:

Alert b2

*Κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο, στέλνει ένα **spoofed Icmp Echo Request** πακέτο σε κάποιον Host που **ανήκει** στο προστατευόμενο δίκτυο, προσποιούμενος ότι είναι κάποιος άλλος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο και **δεν υπάρχει**.*

Συμβολισμός

ⓘ Στην περίπτωση που το *spoofing* ανιχνευτεί από την καθιερωμένη διαδικασία και έχει ανιχνευτεί και σε προηγούμενο έλεγχο (Τοπολογία B), το συμπέρασμα που εξάγεται είναι :

Alert b3

*Κάποιος Host που **ανήκει** στο προστατευόμενο δίκτυο, στέλνει ένα **spoofed Icmp Echo Request** πακέτο σε κάποιον άλλο Host που **ανήκει** στο προστατευόμενο δίκτυο, προσποιούμενος ότι είναι κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο και **δεν υπάρχει**.*

Συμβολισμός

Στον επόμενο πίνακα παρουσιάζονται συγκεντρωμένα τα αποτελέσματα από την μελέτη που έγινε προηγουμένως, όσο αναφορά την ανίχνευση των *spoofed Icmp Echo Request* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 0/1* πακέτα που εισέρχονται στο προστατευόμενο δίκτυο.

Στην 1η στήλη του πίνακα αναφέρεται το περιεχόμενο του πακέτου (αν περιέχει ένα *Icmp Echo Request* ή *Reply*). Επίσης αναφέρεται ο αποστολέας και ο παραλήπτης του πακέτου αυτού.

Στη συνέχεια αναφέρεται η θέση του κάθε συστήματος που παίρνει μέρος στην διαδικασία σε σχέση με το προστατευόμενο δίκτυο, δηλαδή εάν βρίσκεται εντός ή εκτός από αυτό.

Η επόμενη στήλη δηλώνει την τοπολογία του σχήματος 2, που αντιστοιχεί στην συγκεκριμένη διάταξη.

Στην επόμενη στήλη δηλώνεται για ποιον host ανιχνεύεται (εάν ανιχνεύεται) το *spoofing* από τον `Sensor`.

Στην προτελευταία στήλη αναφέρεται εάν το *spoofing* είναι δυνατόν να ανιχνευτεί σε κάθε περίπτωση.

Στην τελευταία στήλη αναγράφεται το alert που παράγεται σε κάθε περίπτωση που θα ανιχνευτεί το *spoofing* όπως προέκυψε από την παραπάνω μελέτη.

Το ✗ σε κάποια πεδία του πίνακα, δηλώνει ότι ο Host που αναγράφεται στο συγκεκριμένο πεδίο δεν υπάρχει. Αυτός είναι ο λόγος που δημιουργήθηκε το *Icmp Destination Unreachable Code 0/1* πακέτο, μετά την αποστολή του πακέτου που περιέχεται στα data του (1η στήλη του πίνακα), στον Host που αναγράφεται στο πεδίο αυτό.

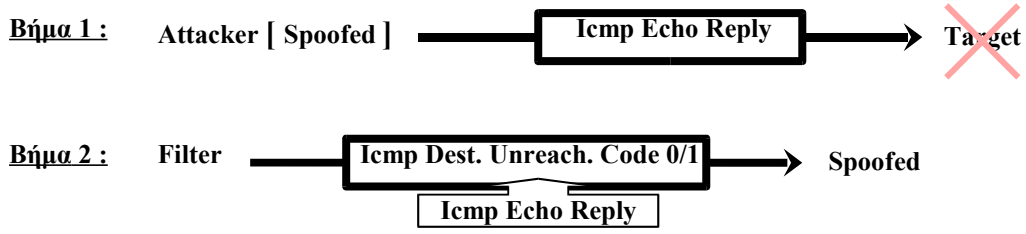
Ανίχνευση των ***spoofed Icmp Echo Request*** πακέτων, εξετάζοντας τα ***Icmp Destination Unreachable Code 0/1*** πακέτα.								
Περιεχόμενο, Κατεύθυνση του *Icmp Dest. Unreach. Code 0/1* Πακέτου	**Θέση του κάθε Host σε σχέση με το Προστατευόμενο Δίκτυο**				**Τοπολογία**	**Ανίχνευση για τον**	**Ανίχνευση**	**Alert**
	Attacker	**Spoofed**	**Target**	**Sensor**				
Icmp Echo Request (Filter → Spoofed)	Out	**In**	~~Out~~	S2	A	Spoofed	**NAI**	**b1**
	Out	**In**	~~Out~~	S2	B	Spoofed	**Δεν Ισχύει**	--
	In	**In**	~~Out~~	S2	C	Spoofed	**ΟΧΙ**	--
Icmp Echo Reply (Filter → Target)	Out	~~Out~~	**In**	S1	A	Target	***NAI**	**b.2**
	In	~~Out~~	**In**	S1	B	Target	**NAI**	**b.3**
	Out	~~Out~~	**In**	S1	C	Target	***NAI**	**b.2**

Πίνακας Β-1 : Συμπεράσματα για την Ανίχνευση των spoofed *Icmp Echo Request* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 0/1* πακέτα.

* **Ανιχνεύτηκε γιατί ισχύει ο Γενικός Κανόνας.**

B.2. Ανίχνευση του spoofed Icmp Echo Reply πακέτου

Σενάριο



Αρχικά (Βήμα 1) ο `Attacker` στέλνει ένα *spoofed Icmp Echo Reply* στον `Target`, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.
Ο `Target` όμως (ή το δίκτυό του) δεν υπάρχει και το πακέτο δεν μπορεί να δρομολογηθεί στον προορισμό του.
Στη συνέχεια (Βήμα 2) το `Filter` καθώς δεν μπορεί να δρομολογήσει το πακέτο στον ανύπαρκτο `Target`, απαντάει στον `Spoofed` στέλνοντάς του ένα *Icmp Destination Unreachable Code 0 /1*, το οποίο περιέχει το *Icmp Echo Reply* πακέτο που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target`.

Στόχος με τον έλεγχο που θα γίνει στο *Icmp Destination Unreachable Code 0/1* πακέτο που εντοπίζεται από τον `Sensor`, είναι να ανιχνευτεί αν το *Icmp Echo Reply* που περιέχει, το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και που υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο, είναι ένα *spoofed* πακέτο.

B.2.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Reply* πακέτου από τον `Attacker` στον ανύπαρκτο `Target` (ή το ανύπαρκτο δίκτυό του), το πακέτο δεν θα μπορέσει να δρομολογηθεί από το `Filter` στον προορισμό του.

Στη συνέχεια (Βήμα 2) κατά την αποστολή του *Icmp Destination Unreachable Code 0/1* από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Request* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed` στον `Target`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Target` προς τον `Spoofed`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetC.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το *Icmp Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 0/1*, με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests* το οποίο να έχει στείλει ο `Target` στον `Spoofed` και έτσι το *spoofing* θα ανιχνευτεί

Τοπολογία Β

Σε αυτή την τοπολογία το σενάριο δεν έχει εφαρμογή καθώς το *spoofed Icmp Echo Reply* από τον `Attacker` στον ανύπαρκτο `Target`, δεν θα φτάσει ποτέ στο `Filter` αλλά ούτε και στον `Sensor`.
Το πακέτο αυτό καθώς ανήκει στο εσωτερικό traffic του NetA, ο `Sensor` δεν θα το επεξεργαστεί.

Τοπολογία C

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Reply* πακέτου από τον `Attacker` στον ανύπαρκτο `Target` (ή το ανύπαρκτο δίκτυό του), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2 και θα φτάσει στο `Filter`.

Σημείωση

Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S2 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων. Από αυτόν τον έλεγχο το *spoofing* θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 0/1* (Βήμα 3) από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Reply* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed` στον `Target`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Target` προς τον `Spoofed`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetA.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το *Icmp Echo Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 0/1*, με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests* το οποίο να έχει στείλει ο `Target` στον `Spoofed` και έτσι το *spoofing* θα ανιχνευτεί.

B.2.2. Εξαγόμενα Συμπεράσματα

Όταν εξετάζεται ένα *Icmp Destination Unreachable Code 0/1* πακέτο για την ανίχνευση πιθανών *spoofed Icmp Echo Reply* πακέτων, το πακέτο αυτό προέρχεται από το `Filter` και περιέχει στα data του το *spoofed Icmp Echo Reply*.
Σε κάθε περίπτωση, εφόσον το *spoofing* ανιχνευτεί, τα συμπεράσματα που εξάγονται είναι τα παρακάτω:

- Το *Icmp Error* μήνυμα δημιουργήθηκε γιατί το *Icmp Echo Reply* που περιέχει, δεν έφτασε στον προορισμό του καθώς ο `Target` (ή το δίκτυό του) δεν υπάρχει.

- Το *Icmp Echo Reply* υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο και πρέπει να γίνει έλεγχος των αποθηκευμένων *Εισερχόμενων Requests*, προς αναζήτηση του αντίστοιχου εισερχόμενου προς το προστατευόμενο δίκτυο *Icmp Echo Request* πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και ως παραλήπτη τον αποστολέα του *Reply*.

- Το *spoofed Icmp Echo Reply*, είναι το πακέτο που περιέχεται στα data του *Icmp Error* μηνύματος που στέλνει το `Filter` στο προστατευόμενο δίκτυο.

- Σε περίπτωση που ανιχνευτεί το *spoofing*, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Spoofed`, του οποίου την διεύθυνση, χρησιμοποιεί ο `Attacker` ως διεύθυνση αποστολέα σε *spoofed Icmp Echo Reply* πακέτα, που στέλνει.

- Αν ανιχνευτεί το *spoofing*, τότε αν ο `Attacker` ανήκει επίσης στο προστατευόμενο δίκτυο με τον `Spoofed`, το *spoofing* θα έχει ανιχνευτεί και σε προηγούμενο στάδιο κατά τον έλεγχο του *Icmp Echo Reply* όταν αυτό εξέρχεται από το προστατευόμενο δίκτυο.

ⓘ Αν μετά από τον έλεγχο του *Icmp Destination Unreachable Code 0/1* που περιέχει ένα *Icmp Echo Reply*, αποδειχτεί ότι το *Icmp Echo Reply* είναι *spoofed* και αν αυτό το πακέτο δεν έχει επισημανθεί και νωρίτερα ως *spoofed* από προηγούμενο έλεγχο (Τοπολογία A), τότε το συμπέρασμα που εξάγεται είναι :

Alert b4

*Κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Reply** πακέτο,*
*σε κάποιον άλλο Host που **δεν ανήκει** στο προστατευόμενο δίκτυο και **δεν υπάρχει**,*
*προσποιούμενος ότι είναι κάποιος Host που **ανήκει** στο προστατευόμενο δίκτυο.*

Συμβολισμός

ⓘ Αν μετά από τον έλεγχο του *Icmp Destination Unreachable Code 0/1* που περιέχει ένα *Icmp Echo Reply* αποδειχτεί ότι το *Icmp Echo Reply* είναι *spoofed* και αν αυτό το πακέτο έχει επισημανθεί και νωρίτερα ως *spoofed* από προηγούμενο έλεγχο (Τοπολογία C), τότε το συμπέρασμα που εξάγεται είναι :

Alert b5

*Κάποιος Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Reply** πακέτο,*
*σε κάποιον Host που **δεν ανήκει** στο προστατευόμενο δίκτυο και **δεν υπάρχει**,*
*προσποιούμενος ότι είναι κάποιος άλλος Host που **ανήκει** στο προστατευόμενο δίκτυο.*

Συμβολισμός

Στον επόμενο πίνακα παρουσιάζονται συγκεντρωμένα τα αποτελέσματα από την μελέτη που έγινε προηγουμένως, όσο αναφορά την ανίχνευση των *spoofed Icmp Echo Reply* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 0/1* πακέτα που εισέρχονται στο προστατευόμενο δίκτυο.

Στην 1η στήλη του πίνακα αναφέρεται το περιεχόμενο του *Error* πακέτου. Επίσης αναφέρεται ο αποστολέας και ο παραλήπτης του πακέτου αυτού.

Στη συνέχεια αναφέρεται η θέση του κάθε συστήματος που παίρνει μέρος στην διαδικασία σε σχέση με το προστατευόμενο δίκτυο, δηλαδή εάν βρίσκεται εντός ή εκτός από αυτό.

Η επόμενη στήλη δηλώνει την τοπολογία του σχήματος 2, που αντιστοιχεί στην συγκεκριμένη διάταξη.

Στην επόμενη στήλη δηλώνεται για ποιον host ανιχνεύεται (εάν ανιχνεύεται) το *spoofing* από τον `Sensor`.

Στην προτελευταία στήλη αναφέρεται εάν το *spoofing* είναι δυνατόν να ανιχνευτεί σε κάθε περίπτωση.

Στην τελευταία στήλη αναγράφεται το alert που παράγεται σε κάθε περίπτωση που ανιχνεύεται το *spoofing* όπως προέκυψε από την παραπάνω μελέτη.

Το ✗ σε κάποια πεδία του πίνακα, δηλώνει ότι ο Host που αναγράφεται στο συγκεκριμένο πεδίο δεν υπάρχει. Αυτός είναι ο λόγος που δημιουργήθηκε το *Icmp Destination Unreachable Code 0/1* πακέτο, μετά την αποστολή του πακέτου που περιέχεται στα data του (1η στήλη του πίνακα), στον Host που αναγράφεται στο πεδίο αυτό.

Ανίχνευση των ***spoofed Icmp Echo Reply*** πακέτων, εξετάζοντας τα ***Icmp Destination Unreachable Code 0/1*** πακέτα.								
Περιεχόμενο, Κατεύθυνση του *Icmp Dest. Unreach. Code 0/1* Πακέτου	**Θέση του κάθε Host σε σχέση με το Προστατευόμενο Δίκτυο**				**Τοπολογία**	**Ανίχνευση για τον**	**Ανίχνευση**	**Alert**
	Attacker	**Spoofed**	**Target**	**Sensor**				
Icmp Echo Reply (Filter → Spoofed)	Out	**In**	~~Out~~	S2	A	Spoofed	**NAI**	**b.4**
	Out	**In**	~~Out~~	S2	B	Spoofed	**Δεν Ισχύει**	--
	In	**In**	~~Out~~	S2	C	Spoofed	**NAI**	**b.5**

Πίνακας B-2 : Συμπεράσματα για την Ανίχνευση των *spoofed Icmp Echo Reply* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 0/1* πακέτα.

Β.3. Επίλογος Για τον Έλεγχο των *Icmp Destination Unreachable Code 0/1* Πακέτων.

Όταν εντοπιστεί ένα *Icmp Destination Unreachable Code 0/1* πακέτο, το πακέτο αυτό ελέγχεται για να ανιχνευτεί αν αυτό έχει προέλθει από κάποια διαδικασία *spoofing*, δηλαδή αν αυτό το πακέτο είναι απάντηση σε ένα *spoofed Icmp Echo Request* ή *Icmp Echo Reply* πακέτο.

Η τεχνική της ανίχνευσης του *spoofing* με την εξέταση ενός *Icmp Destination Unreachable Code 0/1* πακέτου, ελέγχει το πακέτο που περιέχεται στα data του, το οποίο είναι το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος.
Στη συνέχεια γίνεται προσπάθεια συσχέτισης του αρχικού πακέτου το οποίο μπορεί να είναι ένα *Icmp Echo Reply* ή ένα *Icmp Echo Request*, με κάποιο από τα *Εισερχόμενα* ή τα *Εξερχόμενα Requests* που αποθηκεύονται για το προστατευόμενο δίκτυο.

Αν το αρχικό πακέτο είναι ένα *Icmp Echo Request*, τότε αυτό θα πρέπει να αντιστοιχηθεί με κάποιο από τα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο και αν αυτό δεν συμβεί, τότε προκύπτει ότι το *Icmp Error* μήνυμα έχει δημιουργηθεί ως απάντηση σε ένα *spoofed Icmp Echo Request* πακέτο.
Στην περίπτωση που βρεθεί το αντίστοιχο αποθηκευμένο *Request*, η παρουσία του *Icmp Error* μηνύματος θα θεωρηθεί φυσιολογική και το *spoofing* (εάν υφίσταται) δεν θα ανιχνευτεί.

Αν το αρχικό πακέτο είναι ένα *Icmp Echo Reply*, τότε αυτό θα πρέπει να αντιστοιχηθεί με κάποιο από τα *Εισερχόμενα Requests* προς το προστατευόμενο δίκτυο και αν αυτό δεν συμβεί, τότε προκύπτει ότι το *Icmp Error* μήνυμα έχει δημιουργηθεί ως απάντηση σε ένα *spoofed Icmp Echo Request* ή ένα *spoofed Icmp Echo Reply* πακέτο.
Ακόμα και στην περίπτωση που βρεθεί το αντίστοιχο αποθηκευμένο *Request*, το *Icmp Error* μήνυμα θεωρείται ότι προήλθε ως απάντηση σε ένα *spoofed* πακέτο καθώς ισχύει ο Γενικός Κανόνας.

Γενικός Κανόνας

Ένα Icmp Destination Unreachable Code 0/1το οποίο περιέχει ένα Icmp Echo Reply είναι κατεξοχήν απόρροια ενός spoofed πακέτου. Αυτό το συμπέρασμα βγαίνει καθώς δεν είναι δυνατόν κάποιος host να στέλνει ένα Reply σε κάποιον που υποτίθεται ότι του έστειλε ένα Request και αυτός (ή το δίκτυό του) να μην υπάρχει.

Στην περίπτωση που το *spoofing* ανιχνευτεί, όπως αποδείχτηκε από την παραπάνω μελέτη ανάλογα με το αρχικό πακέτο που περιέχεται στα data του *Icmp Error* μηνύματος, τα συμπεράσματα που εξάγονται, εκτός από την επισήμανση για την ύπαρξη του *spoofing*, δίνουν επίσης σημαντική πληροφορία για το πως αυτό υλοποιήθηκε, όσο αναφορά την θέση του κάθε host, που πήρε μέρος στην διαδικασία, σε σχέση με το προστατευόμενο δίκτυο.

Έτσι τα πιθανά Alerts που μπορούν να δημιουργηθούν αν το *spoofing* ανιχνευτεί μετά τον έλεγχο ενός *Icmp Destination Unreachable Code 0/1* πακέτου, είναι τα παρακάτω :

Σημείωση

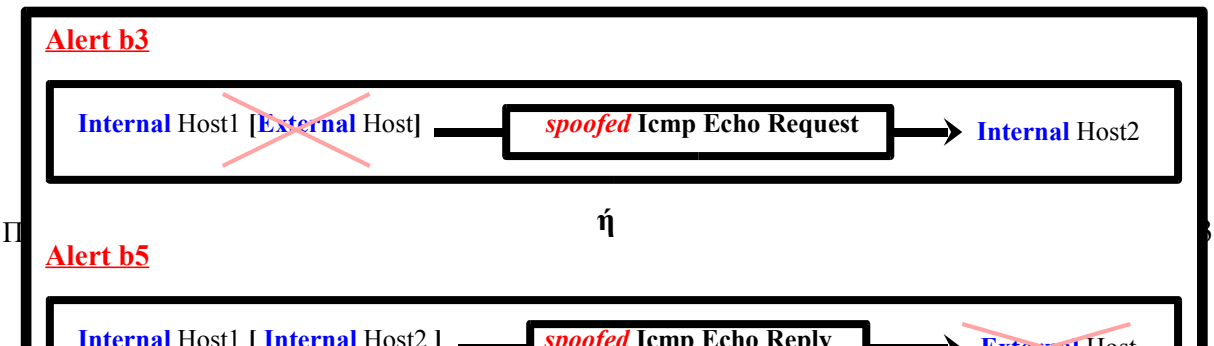
Ο host που φαίνεται μαρκαρισμένος στο κάθε alert είναι αυτός που ανήκει στο προστατευόμενο δίκτυο και για τον οποίο ανιχνεύεται το *spoofing* από τον Sensor.
Ο host αυτός μπορεί να παίζει τον ρόλο είτε του Spoofed (η δικιά του διεύθυνση χρησιμοποιείται σε *spoofed* πακέτα που στέλνονται από κάποιον άλλον), είτε του Target (σε αυτόν στέλνονται τα *spoofed* πακέτα).
Ο host που είναι διαγραμμένος έχει την έννοια ότι αυτός δεν υπάρχει.

Alert B1

Το Alert B1 είναι το Alert b1 όπως παρουσιάστηκε στην παραπάνω μελέτη. Το alert αυτό δημιουργήθηκε μετά από τον έλεγχο του *Icmp Destination Unreachable Code 0/1* πακέτου, καθώς ικανοποιήθηκαν οι παρακάτω συνθήκες :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Destination Unreachable Code 0/1* πακέτο.
- Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και το οποίο περιέχεται στα data του *Icmp Destination Unreachable Code 0/1* πακέτου, είναι ένα *Icmp Echo Request* πακέτο.
- Κατά τον έλεγχο του αρχικού πακέτου που περιέχεται στα data του το *Icmp Destination Unreachable Code 0/1*, δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό, στα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο.

Alert B2



Το Alert B2 αποτελείται από δύο σκέλη, τα οποία είναι τα δύο πιθανά σενάρια που μπορεί να ισχύουν ώστε να δημιουργηθεί το Alert B2.
Και τα δύο αυτά alerts κατά τον έλεγχο ικανοποιούν τις ίδιες συνθήκες και γι' αυτό δεν είναι δυνατόν να γίνει ένας πιο συγκεκριμένος διαχωρισμός μεταξύ τους.
Οι συνθήκες που ικανοποιούνται κατά τον έλεγχο και δημιουργείται το Alert B2 είναι οι παρακάτω :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Destination Unreachable Code 0/1* πακέτο.
- Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και το οποίο περιέχεται στα data του *Icmp Destination Unreachable Code 0/1* πακέτου, είναι ένα *Icmp Echo Reply* πακέτο.
- Κατά τον έλεγχο του αρχικού πακέτου που περιέχεται στα data του το *Icmp Destination Unreachable Code 0/1*, δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό, στα *Εισερχόμενα Requests* από το προστατευόμενο δίκτυο.
- Το *spoofing* έχει ανιχνευτεί σε προηγούμενο στάδιο, με ξεχωριστό έλεγχο που έχει γίνει στο *Icmp Echo Reply* πακέτο, που περιέχεται στα data του *Icmp Error* μηνύματος.

Alert B3

Το Alert B3 είναι το Alert b4 όπως παρουσιάστηκε στην παραπάνω μελέτη. Το alert αυτό δημιουργήθηκε μετά από τον έλεγχο του *Icmp Destination Unreachable Code 0/1* πακέτου, καθώς ικανοποιήθηκαν οι παρακάτω συνθήκες :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Destination Unreachable Code 0/1* πακέτο.
- Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και το οποίο περιέχεται στα data του *Icmp Destination Unreachable Code 0/1* πακέτου, είναι ένα *Icmp Echo Reply* πακέτο.

- Κατά τον έλεγχο του αρχικού πακέτου που περιέχεται στα data του το *Icmp Destination Unreachable Code 0/1*, δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό, στα *Εισερχόμενα Requests* από το προστατευόμενο δίκτυο.

- Το *spoofing* δεν έχει ανιχνευτεί σε προηγούμενο στάδιο, με ξεχωριστό έλεγχο που έχει γίνει στο *Icmp Echo Reply* πακέτο, που περιέχεται στα data του *Icmp Error* μηνύματος.

Alert B4

Το Alert B4 είναι το Alert b2 όπως παρουσιάστηκε στην παραπάνω μελέτη. Το alert αυτό δημιουργήθηκε μετά από τον έλεγχο του *Icmp Destination Unreachable Code 0/1* πακέτου, καθώς ικανοποιήθηκαν οι παρακάτω συνθήκες :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Destination Unreachable Code 0/1* πακέτο.

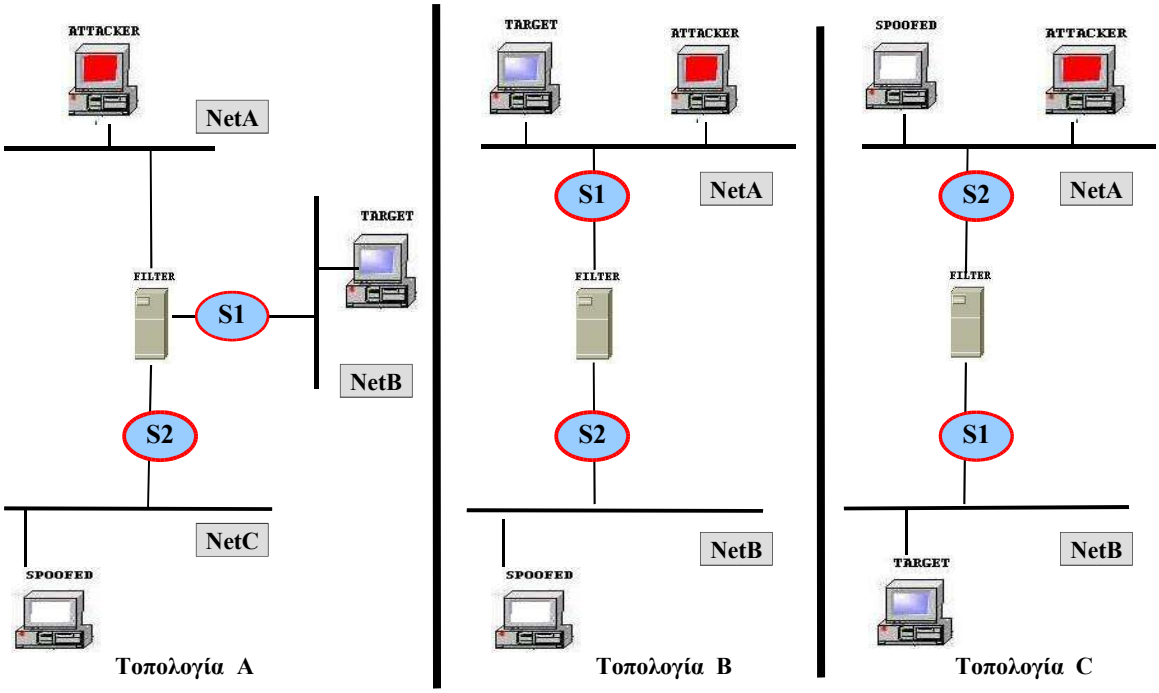
- Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και το οποίο περιέχεται στα data του *Icmp Destination Unreachable Code 0/1* πακέτου, είναι ένα *Icmp Echo Reply* πακέτο.

- Κατά τον έλεγχο του αρχικού πακέτου που περιέχεται στα data του το *Icmp Destination Unreachable Code 0/1*, βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό, στα *Εισερχόμενα Requests* από το προστατευόμενο δίκτυο.
  Το *spoofing* ανιχνεύτηκε από την ισχύ του Γενικού Κανόνα.

ΜΕΡΟΣ C

Έλεγχος του *Icmp Destination Unreachable – Administrative Prohibited* Πακέτου (*Type 3, Code 13*)

Στο σημείο αυτό παρουσιάζεται ξανά το **Σχήμα 2** έτσι ώστε να είναι πιο εύκολη η πρόσβαση σε αυτό, κατά την περιγραφή της διαδικασίας.



Σχήμα 2: Πιθανές Τοπολογίες

Ο `Sensor` εντοπίζει ένα *Icmp Destination Unreachable Code 13* πακέτο. Το πακέτο αυτό προέρχεται από το `Filter` και έχει προορισμό το προστατευόμενο δίκτυο.

Στην παρουσίαση του *Icmp* πρωτοκόλλου αναφέρθηκε ότι το *Icmp Error* μήνυμα έχει προορισμό τον αποστολέα του αρχικού πακέτου που οδήγησε στην δημιουργία του Error μηνύματος. Έτσι αν ένα τέτοιο πακέτο εντοπιστεί από τον `Sensor` αυτό δηλώνει ότι κάποιος από το προστατευόμενο δίκτυο έστειλε το αρχικό πακέτο που το δημιούργησε.

Το *Icmp Destination Unreachable Code 13* που στέλνει το `Filter` σε κάποιον host του προστατευόμενου δικτύου, δηλώνει ότι το κάποιο πακέτο που στάλθηκε από αυτόν τον host, δεν μπόρεσε να φτάσει στον προορισμό του, καθώς το `Filter` δεν επιτρέπει την διέλευση αυτών των πακέτων.
Το αρχικό πακέτο που στάλθηκε και το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος, θα περιέχεται στα data του *Icmp Destination Unreachable* πακέτου (μέρος του ή ολόκληρο).

Από τα *Icmp Destination Unreachable Code 13* πακέτα, αυτά που παρουσιάζουν ενδιαφέρον για την παρούσα μελέτη, είναι αυτά που περιέχουν ένα *Icmp Echo Request* ή ένα *Icmp Echo Reply* σαν το αρχικό πακέτο που δημιούργησε αυτό το *Icmp Error* μήνυμα.

Διαδικασία Ανίχνευσης

Ο `Sensor` εντοπίζει ένα *Icmp Destination Unreachable Code 13* το οποίο περιέχει στα data του ένα *Icmp Echo Request* ή ένα *Icmp Echo Reply* πακέτο (μέρος του ή ολόκληρο), το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος.
Το πακέτο αυτό προέρχεται από το `Filter` και έχει προορισμό το προστατευόμενο δίκτυο.
Η παρουσία του πακέτου αυτού, δηλώνει ότι προηγήθηκε μέσα από το προστατευόμενο δίκτυο, η αποστολή του αρχικού πακέτου που δημιούργησε το *Icmp Error* μήνυμα.

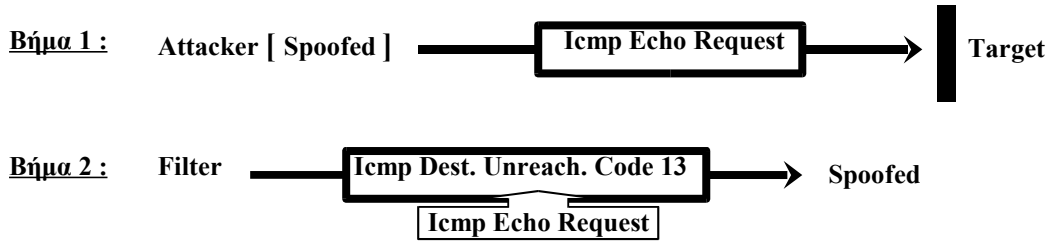
Έτσι αν το *Icmp Error* μήνυμα περιέχει ένα *Icmp Echo Request* πακέτο, το πακέτο αυτό θα πρέπει να έχει καταγραφεί και στα αποθηκευμένα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο.
Η επιτυχία ή η αποτυχία της αναζήτησης του πακέτου αυτού στα αποθηκευμένα *Εξερχόμενα Requests* θα οδηγήσει στην ανίχνευση του *spoofing*.

Αν το *Icmp Error* μήνυμα περιέχει ένα *Icmp Echo Reply* πακέτο, θα πρέπει να έχει καταγραφεί στα αποθηκευμένα *Εισερχόμενα Requests* προς το προστατευόμενο δίκτυο, το αντίστοιχο *Icmp Echo Request* πακέτο, που έχει ως αποστολέα τον παραλήπτη του *Reply* και ως παραλήπτη τον αποστολέα του *Reply* .
Η επιτυχία ή η αποτυχία της αναζήτησης του πακέτου αυτού στα αποθηκευμένα *Εισερχόμενα Requests* θα οδηγήσει στην ανίχνευση του *spoofing*.

C.1. Ανίχνευση του *spoofed Icmp Echo Request* πακέτου

C.1.1. Το *Icmp Destination Unreachable Code 13* περιέχει ένα *Icmp Echo Request*

Σενάριο



Αρχικά (Βήμα 1) ο `Attacker` στέλνει ένα *spoofed Icmp Echo Request* στον `Target`, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.

Στη συνέχεια (Βήμα 2) το `Filter` καθώς δεν επιτρέπει την διέλευση των *Icmp Echo Request* πακέτων, απαντάει στον `Spoofed` στέλνοντάς του ένα *Icmp Destination Unreachable Code 13*, το οποίο περιέχει το *Icmp Echo Request* πακέτο που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target`.

Στόχος με τον έλεγχο που θα γίνει στο *Icmp Destination Unreachable Code 13* πακέτο που εντοπίζεται από τον `Sensor`, είναι να ανιχνευτεί, αν το *Icmp Echo Request* που περιέχει το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και που υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο, είναι ένα *spoofed* πακέτο.

C.1.1.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

- Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target`, το `Filter` δεν θα επιτρέψει στο πακέτο να περάσει.

Στη συνέχεια (Βήμα 2) κατά την αποστολή του *Icmp Destination Unreachable Code 13* από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Request* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Request* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed`, θα αναζητήσει το πακέτο αυτό στα αποθηκευμένα *Εξερχόμενα Requests* από το NetC.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το *Icmp Echo Request* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 13*, με κάποιο από τα αποθηκευμένα *Εξερχόμενα Requests* το οποίο να έχει στείλει ο `Spoofed` στον `Target` και έτσι το *spoofing* θα ανιχνευτεί.

Τοπολογία B

Σε αυτή την τοπολογία το σενάριο δεν έχει εφαρμογή καθώς το *spoofed Icmp Echo Request* από τον `Attacker` στον `Target`, δεν πρόκειται να προκαλέσει την δημιουργία ενός *Icmp Destination Unreachable Code 13* που να περιέχει ένα *Icmp Echo Request* πακέτο.

Τοπολογία C

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου (Βήμα 1) από τον `Attacker` στον `Target` το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2, ο οποίος θα το αποθηκεύσει στα *Εξερχόμενα Requests* από το NetA, σαν αυτό να έχει προέλθει από τον `Spoofed`.

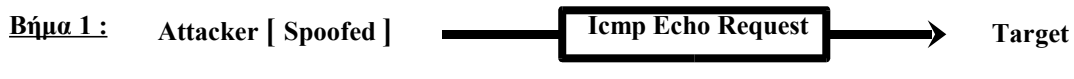
Στη συνέχεια το πακέτο θα φτάσει στο `Filter` το οποίο δεν θα επιτρέψει την διέλευσή του.

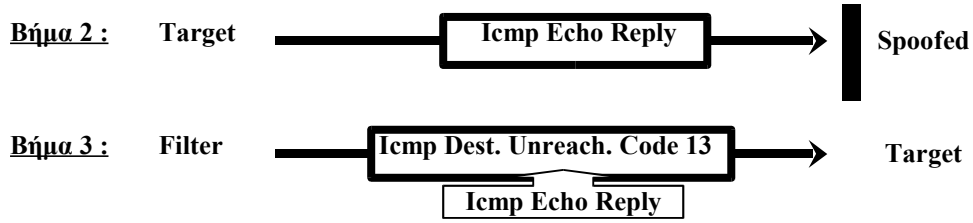
Κατά την αποστολή του *Icmp Destination Unreachable Code 13* (Βήμα 2) από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Request* πακέτο), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Request* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed`, θα αναζητήσει το πακέτο αυτό στα αποθηκευμένα *Εξερχόμενα Requests* από το NetA.

Ο `Sensor` στη θέση S2 θα καταφέρει να αντιστοιχήσει το *Icmp Echo Request* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 13*, με το πακέτο που αποθήκευσε προηγουμένως στα *Εξερχόμενα Requests* το οποίο υποτίθεται ότι έστειλε ο `Spoofed` στον `Target` και έτσι το *spoofing* δεν θα ανιχνευτεί.

C.1.2. Το *Icmp Destination Unreachable Code 13* περιέχει ένα *Icmp Echo Reply*

Σενάριο





Αρχικά (Βήμα 1) ο `Attacker` στέλνει ένα *spoofed Icmp Echo Request* στον `Target`, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.

Στη συνέχεια (Βήμα 2) ο `Target` απαντάει στον `Spoofed`, στέλνοντάς του ένα *Icmp Echo Reply*.
Το `Filter` όμως δεν επιτρέπει την διέλευση αυτών των πακέτων και το πακέτο δεν φτάνει σον προορισμό του.
Στη συνέχεια (Βήμα 3) το `Filter` καθώς δεν επέτρεψε την διέλευση του *Icmp Echo Reply*, απαντάει στον `Target`, στέλνοντάς του ένα *Icmp Destination Unreachable Code 13*, το οποίο περιέχει το *Icmp Echo Reply* πακέτο που έστειλε ο `Target` στον `Spoofed`.

Στόχος με τον έλεγχο που θα γίνει στο *Icmp Destination Unreachable Code 13* πακέτο που εντοπίζεται από τον `Sensor`, είναι να ανιχνευτεί αν το *Icmp Echo Reply* που περιέχει, το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και που υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο, έχει προέλθει από ένα *spoofed Icmp Echo Request* πακέτο.

C.1.2.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

- Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target`, το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1, ο οποίος θα το αποθηκεύσει στα *Εισερχόμενα Requests* προς το NetB, σαν αυτό να έχει προέλθει από τον `Spoofed`.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1 και θα φτάσει στο `Filter`.

> **Σημείωση**
>
> Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S1 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων. Από αυτόν τον έλεγχο το *spoofing* δεν θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 13* (Βήμα 3) από το `Filter` στον `Target` (ο οποίος έστειλε το *Icmp Echo Reply* πακέτο), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1.
Ο `Sensor` στη θέση S1 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Target` στον `Spoofed`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Spoofed` προς τον `Target`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetB.

Ο `Sensor` στη θέση S1 θα καταφέρει να αντιστοιχήσει το εξερχόμενο από το NetB *Icmp Echo Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 13*, με το *Εισερχόμενο Request* που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target` και το οποίο αποθήκευσε προηγουμένως και έτσι το *spoofing* δεν θα ανιχνευτεί.

Τοπολογία Β

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target` (Βήμα 1), οι οποίοι ανήκουν και οι δύο στο NetA, το πακέτο αυτό δεν θα γίνει αντιληπτό από τον `Sensor` στη θέση S1, καθώς ανήκει στο εσωτερικό traffic του δικτύου το οποίο ο `Sensor` στη θέση S1 δεν επεξεργάζεται.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1 και θα φτάσει στο `Filter`.

> **Σημείωση**
>
> Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S1 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων. Από αυτόν τον έλεγχο το *spoofing* θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 13* (Βήμα 3) από το `Filter` στον `Target` (ο οποίος έστειλε το *Icmp Echo Reply* πακέτο), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1.
Ο `Sensor` στη θέση S1 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Target` στον `Spoofed`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Spoofed` προς τον `Target`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetA.

Ο `Sensor` στη θέση S1 δεν θα καταφέρει να αντιστοιχήσει το *Icmp Echo Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 13*, με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests* το οποίο να έχει στείλει ο `Spoofed` στον `Target` και έτσι το *spoofing* θα ανιχνευτεί.

Τοπολογία C

➲ Λειτουργία του **Sensor στη θέση S1**

Κατά την αποστολή του *spoofed Icmp Echo Request* πακέτου από τον `Attacker` στον `Target` (Βήμα 1), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1, ο οποίος θα το αποθηκεύσει στα *Εισερχόμενα Requests* προς το NetB, σαν αυτό να έχει προέλθει από τον `Spoofed`.

Στη συνέχεια κατά την αποστολή του *Icmp Echo Reply* από τον `Target` στον `Spoofed` (Βήμα 2), το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1 και θα φτάσει στο `Filter`.

> **Σημείωση**
>
> Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S1 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων. Από αυτόν τον έλεγχο το *spoofing* δεν θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 13* (Βήμα 3) από το `Filter` στον `Target` (ο οποίος έστειλε το *Icmp Echo Reply* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S1.
Ο `Sensor` στη θέση S1 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Target` στον `Spoofed`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο, που πρέπει να έχει προηγηθεί από τον `Spoofed` προς τον `Target`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetB.

Ο `Sensor` στη θέση S1 θα καταφέρει να αντιστοιχήσει το εξερχόμενο από το NetB *Icmp Echo Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 13*, με το *Εισερχόμενο Request* που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target` και το οποίο αποθήκευσε προηγουμένως και έτσι το *spoofing* δεν θα ανιχνευτεί.

C.1.3. Εξαγόμενα Συμπεράσματα

Όταν εξετάζεται ένα *Icmp Destination Unreachable Code 13* πακέτο για την ανίχνευση πιθανών *spoofed Icmp Echo Request* πακέτων, σημαντικό ρόλο παίζει το πακέτο που περιέχεται στα data του, και το οποίο είναι αυτό που δημιούργησε το *Icmp Error* μήνυμα.
Το εσωτερικό πακέτο μπορεί να είναι ένα *Icmp Echo Request* ή ένα *Icmp Echo Reply* και υποτίθεται ότι στάλθηκε από το προστατευόμενο δίκτυο.
Σε κάθε περίπτωση, εφόσον το *spoofing* ανιχνευτεί, τα συμπεράσματα που εξάγονται είναι διαφορετικά και η πληροφορία που παράγεται βοηθάει στην κατανόηση του τρόπου με τον οποίο το *spoofing* υλοποιήθηκε.
Έτσι εάν το *Icmp Destination Unreachable Code 13* πακέτο που εντοπίστηκε περιέχει ένα :

- ***Icmp Echo Request***

  - Το *Icmp Error* μήνυμα δημιουργήθηκε γιατί το *Icmp Echo Request* που περιέχει, δεν έφτασε στον προορισμό του, καθώς το `Filter` δεν επιτρέπει την διέλευση των *Icmp Echo Request* πακέτων.

  - Το *Icmp Echo Request* υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο και πρέπει να γίνει έλεγχος των αποθηκευμένων *Εξερχόμενων Requests*, προς αναζήτηση του πακέτου αυτού στο εξερχόμενο traffic του δικτύου που προηγήθηκε.

  - Σε περίπτωση που ανιχνευτεί το *spoofing*, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Spoofed`, του οποίου την διεύθυνση, χρησιμοποιεί ο `Attacker` ως διεύθυνση αποστολέα σε *spoofed Icmp Echo Request* πακέτα, που στέλνει.

  - Το *spoofing* θα ανιχνευτεί στην περίπτωση που ο `Attacker` (αυτός που στέλνει τα *spoofed* πακέτα), δεν ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Spoofed`, του οποίου την διεύθυνση χρησιμοποιεί ως διεύθυνση αποστολέα στα *spoofed* πακέτα που στέλνει.

ⓘ Έτσι όταν το *spoofing* ανιχνευτεί (Τοπολογία A) το συμπέρασμα που εξάγεται είναι :

Alert c1

*Κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Request** πακέτο*
*σε κάποιον άλλο Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
*προσποιούμενος ότι είναι κάποιος Host **που ανήκει** στο προστατευόμενο δίκτυο.*

Συμβολισμός

➢ ***Icmp Echo Reply***

☞ Το *Icmp Error* μήνυμα δημιουργήθηκε γιατί το *Icmp Echo Reply* που περιέχει δεν έφτασε στον προορισμό του καθώς, το `Filter` δεν επιτρέπει την διέλευση των *Icmp Echo Reply* πακέτων.

☞ Το *Icmp Echo Reply* υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο και πρέπει να γίνει έλεγχος των αποθηκευμένων *Εισερχόμενων Requests*, προς αναζήτηση του αντίστοιχου εισερχόμενου προς το προστατευόμενο δίκτυο *Icmp Echo Request* πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και ως παραλήπτη τον αποστολέα του *Reply*.

☞ Σε περίπτωση που ανιχνευτεί το spoofing, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Target`, στον οποίο στέλνει ο `Attacker` *spoofed Icmp Echo Request* πακέτα, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.

☞ Το *spoofing* θα ανιχνευτεί στην περίπτωση που ο `Attacker` ανήκει επίσης στο προστατευόμενο δίκτυο μαζί με τον `Target`, στον οποίο στέλνει τα *spoofed* πακέτα.

ⓘ Έτσι στην περίπτωση που το *spoofing* ανιχνευτεί (Τοπολογία B), το συμπέρασμα που εξάγεται είναι:

Alert c2

*Κάποιος Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Request** πακέτο*
*σε κάποιον άλλο Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*προσποιούμενος ότι είναι κάποιος Host **πουδεν ανήκει** στο προστατευόμενο*

Συμβολισμός

Στον επόμενο πίνακα παρουσιάζονται συγκεντρωμένα τα αποτελέσματα από την μελέτη που έγινε προηγουμένως, όσο αναφορά την ανίχνευση των *spoofed Icmp Echo Request* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 13* πακέτα που εισέρχονται στο προστατευόμενο δίκτυο.

Στην 1η στήλη του πίνακα αναφέρεται το περιεχόμενο του πακέτου (αν περιέχει ένα *Icmp Echo Request* ή *Reply*). Επίσης αναφέρεται ο αποστολέας και ο παραλήπτης του πακέτου αυτού.

Στη συνέχεια αναφέρεται η θέση του κάθε συστήματος που παίρνει μέρος στην διαδικασία σε σχέση με το προστατευόμενο δίκτυο, δηλαδή εάν βρίσκεται εντός ή εκτός από αυτό.

Η επόμενη στήλη δηλώνει την τοπολογία του σχήματος 2, που αντιστοιχεί στην συγκεκριμένη διάταξη.

Στην επόμενη στήλη δηλώνεται για ποιον host ανιχνεύεται (εάν ανιχνεύεται) το *spoofing* από τον `Sensor`.

Στην προτελευταία στήλη αναφέρεται εάν το *spoofing* είναι δυνατόν να ανιχνευτεί σε κάθε περίπτωση.

Στην τελευταία στήλη αναγράφεται το alert που παράγεται σε κάθε περίπτωση που ανιχνεύεται το *spoofing,* όπως προέκυψε από την παραπάνω μελέτη.

Το ■ σε κάποια πεδία του πίνακα δηλώνει ότι το *Icmp Destination Unreachable Code 13* πακέτο δημιουργήθηκε, γιατί δεν επιτράπηκε πρωτύτερα από το `Filter`, η διέλευση του αρχικού πακέτου που περιέχει (1η στήλη του πίνακα), όταν αυτό κατευθυνόταν προς τον Host που αναγράφεται σε αυτό το πεδίο του πίνακα.

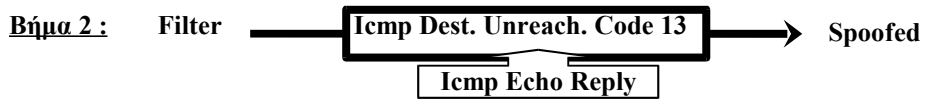
Ανίχνευση των ***spoofed Icmp Echo Request*** πακέτων, εξετάζοντας τα ***Icmp Destination Unreachable Code 13*** πακέτα.								
Περιεχόμενο , Κατεύθυνση του *Icmp Dest. Unreach. Code 13* Πακέτου	**Θέση του κάθε Host σε σχέση με το Προστατευόμενο Δίκτυο**				**Τοπολογία**	**Ανίχνευση για τον**	**Ανίχνευση**	**Alert**
	Attacker	**Spoofed**	**Target**	**Sensor**				
Icmp Echo Request (Filter → Spoofed)	Out	**In**	Out	S2	A	Spoofed	**NAI**	**c1**
	Out	**In**	Out	S2	B	Spoofed	**Δεν Ισχύει**	--
	In	**In**	Out	S2	C	Spoofed	**OXI**	--
Icmp Echo Reply (Filter → Target)	Out	Out	**In**	S1	A	Target	**OXI**	--
	In	Out	**In**	S1	B	Target	**NAI**	**c.2**
	Out	Out	**In**	S1	C	Target	**OXI**	--

Πίνακας C-1 : Συμπεράσματα για την Ανίχνευση των *spoofed Icmp Echo Request* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 13* πακέτα.

C.2. Ανίχνευση του *spoofed Icmp Echo Reply* πακέτου

Σενάριο

Βήμα 1 : **Attacker [Spoofed]** → **Icmp Echo Reply** → **Target**



Αρχικά (Βήμα 1) ο `Attacker` στέλνει ένα *spoofed Icmp Echo Reply* στον `Target`, χρησιμοποιώντας ως διεύθυνση αποστολέα αυτή του `Spoofed`.
Στη συνέχεια (Βήμα 2) το `Filter` καθώς δεν επιτρέπει την διέλευση των *Icmp Echo Reply* πακέτων, απαντάει στον `Spoofed` στέλνοντάς του ένα *Icmp Destination Unreachable Code 13*, το οποίο περιέχει το *Icmp Echo Reply* πακέτο που υποτίθεται ότι έστειλε ο `Spoofed` στον `Target`.

Στόχος με τον έλεγχο που θα γίνει στο *Icmp Destination Unreachable Code 13* πακέτο που εντοπίζεται από τον `Sensor`, είναι να ανιχνευτεί αν το *Icmp Echo Reply* που περιέχει το οποίο οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και που υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο, είναι ένα *spoofed* πακέτο.

C.2.1. Εφαρμογή Ανίχνευσης στις Διάφορες Τοπολογίες

Τοπολογία Α

- Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Reply* πακέτου από τον `Attacker` στον `Target`, το `Filter` δεν θα επιτρέψει στο πακέτο να περάσει.

Στη συνέχεια (Βήμα 2) κατά την αποστολή του *Icmp Destination Unreachable Code 13* από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Reply* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed` στον `Target`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Target` προς τον `Spoofed`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetC.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το *Icmp Echo Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 13*, με κάποιο από τα αποθηκευμένα *Εισερχόμενα Requests* το οποίο να έχει στείλει ο `Target` στον `Spoofed` και έτσι το *spoofing* θα ανιχνευτεί

Τοπολογία B

Σε αυτή την τοπολογία το σενάριο δεν έχει εφαρμογή καθώς το *spoofed Icmp Echo Reply* από τον `Attacker` στον ανύπαρκτο `Target`, δεν θα φτάσει ποτέ στο `Filter` αλλά ούτε και στον `Sensor`.
Το πακέτο αυτό καθώς ανήκει στο εσωτερικό traffic του NetA, ο `Sensor` δεν θα το επεξεργαστεί.

Τοπολογία C

➲ Λειτουργία του **Sensor στη θέση S2**

Κατά την αποστολή (Βήμα 1) του *spoofed Icmp Echo Reply* πακέτου από τον `Attacker` στον `Target`, το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2 και θα φτάσει στο `Filter`.

> **Σημείωση**
>
> Όταν το *Icmp Echo Reply* περάσει από τον Sensor στη θέση S2 τότε θα εκτελεστεί η διαδικασία ανίχνευσης του *spoofing* όπως περιγράφηκε στον έλεγχο των *Icmp Echo Reply* πακέτων. Από αυτόν τον έλεγχο το *spoofing* θα ανιχνευτεί.

Κατά την αποστολή του *Icmp Destination Unreachable Code 13* (Βήμα 3) από το `Filter` στον `Spoofed` (ο οποίος υποτίθεται ότι έστειλε το *Icmp Echo Reply* πακέτο) το πακέτο αυτό θα περάσει από τον `Sensor` στη θέση S2.
Ο `Sensor` στη θέση S2 εντοπίζοντας ότι στα data του πακέτου υπάρχει ένα *Icmp Echo Reply* το οποίο υποτίθεται ότι έχει στείλει ο `Spoofed` στον `Target`, θα αναζητήσει το αντίστοιχο *Icmp Echo Request* πακέτο που πρέπει να έχει προηγηθεί από τον `Target` προς τον `Spoofed`, στα αποθηκευμένα *Εισερχόμενα Requests* προς το NetA.

Ο `Sensor` στη θέση S2 δεν θα καταφέρει να αντιστοιχήσει το *Icmp Echo Reply* πακέτο που περιέχεται στο *Icmp Destination Unreachable Code 13*, με κάποιο από τα αποθηκευμένα

Εισερχόμενα Requests το οποίο να έχει στείλει ο `Target` στον `Spoofed` και έτσι το *spoofing* θα ανιχνευτεί.

C.2.2. Εξαγόμενα Συμπεράσματα

Όταν εξετάζεται ένα *Icmp Destination Unreachable Code 13* πακέτο για την ανίχνευση πιθανών *spoofed Icmp Echo Reply* πακέτων, το πακέτο αυτό προέρχεται από το `Filter` και περιέχει στα data του το *spoofed Icmp Echo Reply*.
Σε κάθε περίπτωση, εφόσον το *spoofing* ανιχνευτεί, τα συμπεράσματα που εξάγονται είναι τα παρακάτω :

- Το *Icmp Error* μήνυμα δημιουργήθηκε γιατί το *Icmp Echo Reply* που περιέχει δεν έφτασε στον προορισμό του καθώς το `Filter` δεν επιτρέπει την διέλευση αυτών των πακέτων.

- Το *Icmp Echo Reply* υποτίθεται ότι προήλθε από το προστατευόμενο δίκτυο και πρέπει να γίνει έλεγχος των αποθηκευμένων *Εισερχόμενων Requests*, προς αναζήτηση του αντίστοιχου εισερχόμενου προς το προστατευόμενο δίκτυο *Icmp Echo Request* πακέτου, που έχει ως αποστολέα τον παραλήπτη του *Reply* και παραλήπτη τον αποστολέα του *Reply*.

- Το *spoofed Icmp Echo Reply* είναι το πακέτο που περιέχεται στα data του *Icmp Error* μηνύματος που στέλνει το `Filter` στο προστατευόμενο δίκτυο.

- Σε περίπτωση που ανιχνευτεί το *spoofing*, τότε αυτό θα γίνει από την πλευρά του δικτύου στο οποίο ανήκει ο `Spoofed`, του οποίου την διεύθυνση, χρησιμοποιεί ο `Attacker` ως διεύθυνση αποστολέα σε *spoofed Icmp Echo Request* πακέτα, που στέλνει.

- Αν ανιχνευτεί το *spoofing*, τότε αν ο `Attacker` ανήκει επίσης στο προστατευόμενο δίκτυο με τον `Spoofed`, το *spoofing* θα έχει ανιχνευτεί και σε προηγούμενο στάδιο κατά τον έλεγχο του *Icmp Echo Reply* όταν αυτό εξέρχεται από το προστατευόμενο δίκτυο.

ⓘ Αν μετά από τον έλεγχο του *Icmp Destination Unreachable Code 13* που περιέχει ένα *Icmp Echo Reply*, αποδειχτεί ότι το *Icmp Echo Reply* είναι *spoofed* και αν αυτό το πακέτο δεν έχει επισημανθεί και νωρίτερα ως *spoofed* από προηγούμενο έλεγχο (Τοπολογία Α), τότε το συμπέρασμα που εξάγεται είναι :

Alert c3

> *Κάποιος Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
> *στέλνει ένα **spoofed Icmp Echo Reply** πακέτο*
> *σε κάποιον άλλο Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
> *προσποιούμενος ότι είναι κάποιος Host **που ανήκει** στο προστατευόμενο δίκτυο.*

Συμβολισμός

ⓘ Αν μετά από τον έλεγχο του *Icmp Destination Unreachable Code 13* που περιέχει ένα *Icmp Echo Reply*, αποδειχτεί ότι το *Icmp Echo Reply* είναι *spoofed* και αν αυτό το πακέτο έχει επισημανθεί και νωρίτερα ως *spoofed* από προηγούμενο έλεγχο (Τοπολογία C), τότε το συμπέρασμα που εξάγεται είναι :

Alert c4

*Κάποιος Host που **ανήκει** στο προστατευόμενο δίκτυο,*
*στέλνει ένα **spoofed Icmp Echo Reply** πακέτο*
*σε κάποιον Host που **δεν ανήκει** στο προστατευόμενο δίκτυο,*
*προσποιούμενος ότι είναι κάποιος άλλος Host **που ανήκει** στο προστατευόμενο δίκτυο.*

Συμβολισμός

Στον επόμενο πίνακα παρουσιάζονται συγκεντρωμένα τα αποτελέσματα από την μελέτη που έγινε προηγουμένως, όσο αναφορά την ανίχνευση των *spoofed Icmp Echo Reply* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 13* πακέτα που εισέρχονται στο προστατευόμενο δίκτυο.

Στη 1η στήλη του πίνακα αναφέρεται στο περιεχόμενο το πακέτου (αν περιέχει ένα *Icmp Echo Request* ή *Reply*) και στην κατεύθυνση του σχετικά με το προστατευόμενο δίκτυο.

Στη συνέχεια αναφέρεται η θέση του κάθε συστήματος που παίρνει μέρος στην διαδικασία σε σχέση με το προστατευόμενο δίκτυο, δηλαδή εάν βρίσκεται εντός ή εκτός από αυτό.

Η επόμενη στήλη δηλώνει την τοπολογία του σχήματος 2, που αντιστοιχεί στην συγκεκριμένη διάταξη.

Στην επόμενη στήλη δηλώνεται για ποιον host ανιχνεύεται (εάν ανιχνεύεται) το *spoofing* από τον `Sensor`.

Στην προτελευταία στήλη αναφέρεται εάν το *spoofing* είναι δυνατόν να ανιχνευτεί σε κάθε περίπτωση.

Στην τελευταία στήλη αναγράφεται το alert που παράγεται σε κάθε περίπτωση που ανιχνευτεί το *spoofing* όπως προέκυψε από την παραπάνω μελέτη.

Το ■ σε κάποια πεδία του πίνακα δηλώνει ότι το *Icmp Destination Unreachable Code 13* πακέτο δημιουργήθηκε, γιατί δεν επιτράπηκε πρωτύτερα από το `Filter`, η διέλευση του αρχικού πακέτου που περιέχει (1η στήλη του πίνακα), όταν αυτό κατευθυνόταν προς τον Host που αναγράφεται σε αυτό το πεδίο του πίνακα.

Ανίχνευση των ***spoofed Icmp Echo Reply*** πακέτων, εξετάζοντας τα ***Icmp Destination Unreachable Code 13*** πακέτα.								
Περιεχόμενο, Κατεύθυνση του *Icmp Dest. Unreach. Code 13* Πακέτου	**Θέση του κάθε Host σε σχέση με το Προστατευόμενο Δίκτυο**				**Τοπολογία**	**Ανίχνευση για τον**	**Ανίχνευση**	**Alert**
	Attacker	**Spoofed**	**Target**	**Sensor**				
Icmp Echo Request (Filter → Spoofed)	Out	**In**	Out	S2	A	Spoofed	**NAI**	**c.3**
	Out	**In**	Out	S2	B	Spoofed	**Δεν Ισχύει**	--
	In	**In**	Out	S2	C	Spoofed	**NAI**	**c.4**

Πίνακας C-2 : Συμπεράσματα για την Ανίχνευση των spoofed *Icmp Echo Reply* πακέτων, εξετάζοντας τα *Icmp Destination Unreachable Code 13* πακέτα.

C.3. Επίλογος Για τον Έλεγχο των *Icmp Destination Unreachable Code 13* Πακέτων.

Όταν εντοπιστεί ένα *Icmp Destination Unreachable Code 13* πακέτο, το πακέτο αυτό ελέγχεται για να ανιχνευτεί αν αυτό έχει προέλθει από κάποια διαδικασία *spoofing*, δηλαδή αν αυτό το πακέτο είναι απάντηση σε ένα *spoofed Icmp Echo Request* ή *Icmp Echo Reply* πακέτο.

Η τεχνική της ανίχνευσης του *spoofing* με την εξέταση ενός *Icmp Destination Unreachable Code 13* πακέτου, ελέγχει το πακέτο που περιέχεται στα data του, το οποίο είναι το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος.

Στη συνέχεια γίνεται προσπάθεια συσχέτισης του αρχικού πακέτου, το οποίο μπορεί να είναι ένα *Icmp Echo Reply* ή ένα *Icmp Echo Request*, με κάποιο από τα *Εισερχόμενα* ή τα *Εξερχόμενα Requests* που αποθηκεύονται για το προστατευόμενο δίκτυο.

Αν το αρχικό πακέτο είναι ένα *Icmp Echo Request*, τότε αυτό θα πρέπει να αντιστοιχηθεί με κάποιο από τα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο και αν αυτό δεν συμβεί τότε προκύπτει ότι το *Icmp Error* μήνυμα έχει δημιουργηθεί ως απάντηση σε ένα *spoofed Icmp Echo Request* πακέτο.
Στην περίπτωση που βρεθεί το αντίστοιχο αποθηκευμένο *Request*, η παρουσία του *Icmp Error* μηνύματος θα θεωρηθεί φυσιολογική και το *spoofing* (εάν υφίσταται) δεν θα ανιχνευτεί.

Αν το αρχικό πακέτο είναι ένα *Icmp Echo Reply*, τότε αυτό θα πρέπει να αντιστοιχηθεί με κάποιο από τα *Εισερχόμενα Requests* προς το προστατευόμενο δίκτυο και αν αυτό δεν συμβεί τότε προκύπτει ότι το *Icmp Error* μήνυμα έχει δημιουργηθεί ως απάντηση σε ένα *spoofed Icmp Echo Request* ή ένα *spoofed Icmp Echo Reply* πακέτο.

Στην περίπτωση που το *spoofing* ανιχνευτεί, όπως αποδείχτηκε από την παραπάνω μελέτη ανάλογα με το αρχικό πακέτο που περιέχεται στα data του *Icmp Error* μηνύματος τα συμπεράσματα που εξάγονται, εκτός από την επισήμανση για την ύπαρξη του *spoofing*, δίνουν επίσης σημαντική πληροφορία για το πως αυτό υλοποιήθηκε, όσο αναφορά την θέση του κάθε host που πήρε μέρος στην διαδικασία, σε σχέση με το προστατευόμενο δίκτυο.

Έτσι τα πιθανά Alerts που μπορούν να δημιουργηθούν αν το *spoofing* ανιχνευτεί μετά τον έλεγχο ενός *Icmp Destination Unreachable Code 13* πακέτου, είναι τα παρακάτω :

Σημείωση

Ο host που φαίνεται μαρκαρισμένος στο κάθε alert είναι αυτός που ανήκει στο προστατευόμενο δίκτυο και για τον οποίο ανιχνεύεται το *spoofing* από τον Sensor. Ο host αυτός μπορεί να παίζει τον ρόλο είτε του Spoofed (η δικιά του διεύθυνση χρησιμοποιείται σε *spoofed* πακέτα που στέλνονται από κάποιον άλλον), είτε του Target (σε αυτόν στέλνονται τα *spoofed* πακέτα).

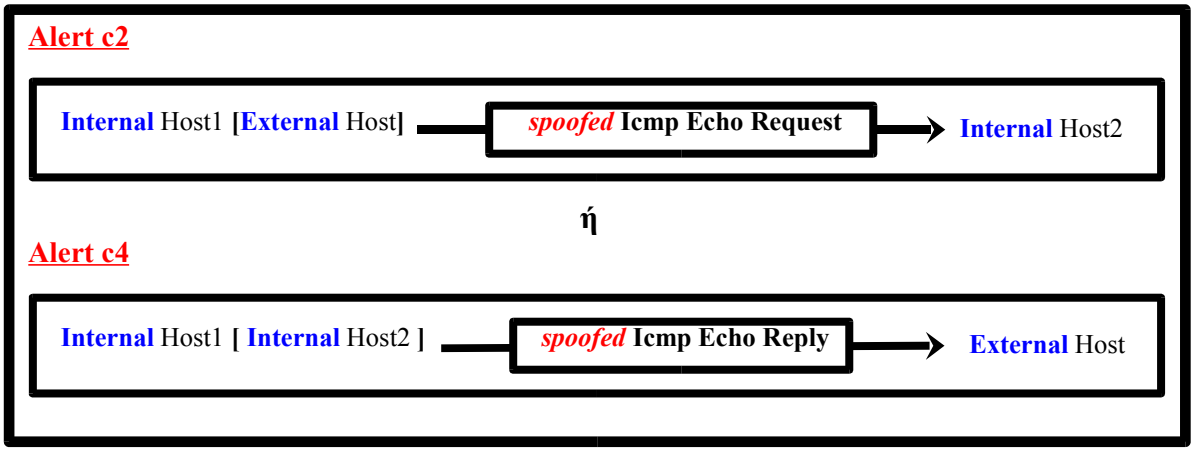
Alert C1

Το Alert C1 είναι το Alert c1 όπως παρουσιάστηκε στην παραπάνω μελέτη. Το Alert C1 δημιουργήθηκε μετά από τον έλεγχο του *Icmp Destination Unreachable Code 13* πακέτου, καθώς ικανοποιήθηκαν οι παρακάτω συνθήκες :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Destination Unreachable Code 13* πακέτο.
- Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και το οποίο περιέχεται στα data του *Icmp Destination Unreachable Code 13* πακέτου, είναι ένα *Icmp Echo Request* πακέτο.

- Κατά τον έλεγχο του αρχικού πακέτου που περιέχει στα data του το *Icmp Destination Unreachable Code 13*, δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό, στα αποθηκευμένα *Εξερχόμενα Requests* από το προστατευόμενο δίκτυο.

Alert C2



Το Alert C2 αποτελείται από δύο σκέλη, τα οποία είναι τα δύο πιθανά σενάρια που μπορεί να ισχύουν ώστε να δημιουργηθεί το Alert C2.
Και τα δύο αυτά alerts κατά τον έλεγχο, ικανοποιούν τις ίδιες συνθήκες και γι' αυτό δεν είναι δυνατόν να γίνει ένας πιο συγκεκριμένος διαχωρισμός μεταξύ τους.
Οι συνθήκες που ικανοποιούνται κατά τον έλεγχο και δημιουργείται το Alert C2 είναι οι παρακάτω :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Destination Unreachable Code 13* πακέτο.
- Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και το οποίο περιέχεται στα data του *Icmp Destination Unreachable Code 13* πακέτου, είναι ένα *Icmp Echo Reply* πακέτο.
- Κατά τον έλεγχο του αρχικού πακέτου που περιέχεται στα data του το *Icmp Destination Unreachable Code 13*, δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό, στα *Εισερχόμενα Requests* από το προστατευόμενο δίκτυο.
- Το *spoofing* έχει ανιχνευτεί σε προηγούμενο στάδιο, με ξεχωριστό έλεγχο που έχει γίνει στο *Icmp Echo Reply* πακέτο, που περιέχεται στα data του *Icmp Error* μηνύματος.

Alert C3

Το Alert C3 είναι το Alert c3 όπως παρουσιάστηκε στην παραπάνω μελέτη. Το alert αυτό δημιουργήθηκε μετά από τον έλεγχο του *Icmp Destination Unreachable Code 13* πακέτου, καθώς ικανοποιήθηκαν οι παρακάτω συνθήκες :

- Το πακέτο που ελέγχεται, είναι ένα *Icmp Destination Unreachable Code 13* πακέτο.
- Το αρχικό πακέτο που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και το οποίο περιέχεται στα data του *Icmp Destination Unreachable Code 13* πακέτου, είναι ένα *Icmp Echo Reply* πακέτο.
- Κατά τον έλεγχο του αρχικού πακέτου, που περιέχεται στα data του το *Icmp Destination Unreachable Code 13*, δεν βρέθηκε το αντίστοιχο *Icmp Echo Request* πακέτο με αυτό, στα *Εισερχόμενα Requests* από το προστατευόμενο δίκτυο.
- Το *spoofing* δεν έχει ανιχνευτεί σε προηγούμενο στάδιο, με ξεχωριστό έλεγχο που έχει γίνει στο *Icmp Echo Reply* πακέτο, που περιέχεται στα data του *Icmp Error* μηνύματος.

ΕΠΙΛΟΓΟΣ ΚΕΦΑΛΑΙΟΥ

Στο Κεφάλαιο αυτό παρουσιάστηκε μία μέθοδος με την οποία είναι δυνατόν να ανιχνευτεί το *Icmp Echo spoofing* όταν αυτό υφίσταται. Η τεχνική που περιγράφηκε όταν εφαρμόζεται σε ένα δίκτυο, επισημαίνει *spoofed Icmp Echo* πακέτα που μπορεί να στέλνονται σε αυτό, καθώς και το γεγονός ότι στέλνονται *spoofed* πακέτα που έχουν σαν διεύθυνση αποστολέα την διεύθυνση κάποιου συστήματος του προστατευόμενου δικτύου. Σε κάθε περίπτωση εκτός από την επισήμανση του *spoofing* υπάρχει δυνατότητα να περιγραφεί και ο τρόπος με τον οποίο υλοποιήθηκε, όσο αναφορά την θέση του κάθε συστήματος που πήρε μέρος στην διαδικασία σε σχέση με το προστατευόμενο δίκτυο.

Στην μελέτη που έγινε σε αυτό το Κεφάλαιο θεωρήθηκε ότι η εφαρμογή των τεχνικών του *ingress* και *egress filtering* είναι δεδομένη, και έγινε προσπάθεια να καλυφθούν κάποιες από τις περιπτώσεις για τις οποίες οι δύο παραπάνω τεχνικές δεν επαρκούν.

Η τεχνική της ανίχνευσης που περιγράφηκε έχει δύο κύριες λειτουργίες :

- Να αποθηκεύει τα *Icmp Echo Request* πακέτα που εισέρχονται και εξέρχονται από το προστατευόμενο δίκτυο, έτσι ώστε με αυτόν τον τρόπο να κρατάει κάποιο είδος ιστορικού για αυτά.

- Να ελέγχει τα *Icmp Echo Reply* και *Icmp Destination Unreachable (Code 0/1,13)* πακέτα που εξέρχονται και εισέρχονται στο προστατευόμενο δίκτυο, για το αν έχουν λόγο ύπαρξης, με την έννοια ότι υπήρξε ένα *Icmp Echo Request* πακέτο που μπορεί να οδήγησε στην δημιουργία τους.

Ο έλεγχος των *Icmp Echo Reply* πακέτων, έχει άμεση σχέση με την φορά αυτών των πακέτων σε σχέση με το προστατευόμενο δίκτυο, δηλαδή αν εισέρχονται ή εξέρχονται από αυτό, καθώς από αυτό θα βγουν σημαντικά συμπεράσματα για τον τρόπο με τον οποίο το *spoofing* υλοποιήθηκε.

Για τα *Icmp Destination Unreachable* πακέτα που ελέγχονται, σημαντικό ρόλο παίζει το πακέτο που περιέχουν στα data τους, καθώς αυτό είναι που οδήγησε στην δημιουργία του *Icmp Error* μηνύματος και θα πρέπει να βρεθεί το αντίστοιχο αποθηκευμένο *Icmp Echo Request* που έχει σχέση με αυτό.

Επίσης στην περιγραφή που έγινε για τον έλεγχο των *Icmp Destination Unreachable* πακέτων θεωρήθηκε δεδομένο ότι αυτά τα πακέτα μπορούν να εισέρχονται μόνο στο προστατευόμενο δίκτυο, δηλώνοντας ότι κάποιο πακέτο που στάλθηκε από αυτό δημιούργησε το *Icmp Error* μήνυμα. Στις συγκεκριμένες τοπολογίες που εξετάστηκαν, έγινε η παραδοχή ότι ο Sensor που εξετάζει τα πακέτα βρίσκεται ανάμεσα στο προστατευόμενο δίκτυο και στο `Filter` το οποίο δημιουργεί τα *Icmp Error* μηνύματα. Δεν εξετάστηκε η περίπτωση που ένα `Filter` μπορεί να υπάρχει και ανάμεσα από τον `Sensor` και το προστατευόμενο δίκτυο, καθώς τότε θα υπήρχαν και *Icmp Destination Unreachable* πακέτα με την αντίθετη φορά, δηλαδή από το προστατευόμενο δίκτυο προς τα έξω. Η διαδικασία της ανίχνευσης σε αυτήν την περίπτωση θα έπρεπε να πραγματοποιεί περισσότερους ελέγχους που να εξετάζουν και την φορά που έχει το πακέτο που περιέχεται στο *Icmp Error* μήνυμα.
Επίσης σημαντική προϋπόθεση για την λειτουργία του `Sensor`, είναι ότι δεν πρέπει να επεξεργάζεται τα πακέτα που ανταλλάζουν τα συστήματα του προστατευόμενου δικτύου μεταξύ τους. Αν αυτό συμβαίνει τότε κάποιες από τις περιπτώσεις του *spoofing* που ο `Attacker` ανήκει στο ίδιο δίκτυο με τον `Target` δεν θα είναι δυνατόν να ανιχνευτούν.

Η προτεινόμενη θέση του `Sensor` που εκτελεί την διαδικασία της ανίχνευσης, είναι αμέσως μετά τα συστήματα του προστατευόμενου δικτύου, -τα οποία μπορεί να διασυνδέονται μεταξύ τους με ένα Hub ή ένα Switch- και πριν τον border Router ή το Firewall του δικτύου.

Η Τεχνική της ανίχνευσης που περιγράφηκε σε αυτό το Κεφάλαιο έχει υλοποιηθεί με κώδικα που αναπτύχθηκε στα πλαίσια αυτής της εργασίας και παρουσιάζεται στο Κεφάλαιο 6. Ο κώδικας αυτός ενσωματώθηκε σαν plug-in στο IDS *Snort* το οποίο παρουσιάζεται στο επόμενο Κεφάλαιο, το οποίο αποτελεί έναν νοηματικό σύνδεσμο ανάμεσα στο παρόν Κεφάλαιο και το Κεφάλαιο 6.