ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Εντοπισμός κακόβουλων επιθέσεων παρεμβολής και αλλοίωσης δεδομένων σε συστήματα ιατρικών κλινικών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Εμμανουήλ Βογιατζή

Επιβλέπων : κ. Γεώργιος Στεργιόπουλος

Μέλη εξεταστικής επιτροπής: κα. Λήλιαν Μήτρου, κ. Σπύρος Κοκολάκης

Σάμος, Ιούνιος, 2024

Πρόλογος και ευχαριστίες

Σκοπός της διπλωματικής και του συγκεκριμένου συγγράμματος, όπως άλλωστε φανερώνει και ο τίτλος της, είναι η δημιουργία ενός συστήματος το οποίο περιέχει τους κατάλληλους κανόνες, για να εντοπίσει και να εμποδίσει κακόβουλες επιθέσεις παρεμβολής και αλλοίωσης δεδομένων σε συστήματα ιατρικών κλινικών. Προφανώς, για να πετύχουμε κάτι τέτοιο, είναι πολύ σημαντική η εγκαθίδρυση συνεργασίας με μία κλινική πραγματικών διαστάσεων, προκειμένου να μας τροφοδοτήσει με την απαραίτητη δικτυακή κίνηση. Αυτή την κίνηση, σε επόμενο χρόνο θα αναλύσουμε, και τέλος θα δημιουργήσουμε κατάλληλους κανόνες για την προστασία της. Κατά τη διάρκεια της εργασίας και για ευνόητους λόγους, θα διατηρηθεί η επωνυμία και οι ευαίσθητες πληροφορίες της κλινικής κρυφές. Για να γίνει αυτό εφικτό, θα εφαρμόσουμε τεχνικές ανωνυμοποίησης στα πακέτα που έχουμε στα χέρια μας.

Θα ήθελα πολύ να ευχαριστήσω την κλινική, έστω και ανώνυμα, για την πολύ σημαντική συνεισφορά της, και για την θετική της ανταπόκριση στην χρήση των δεδομένων. Επίσης, θα ήθελα να ευχαριστήσω, όλους όσους στάθηκαν δίπλα μου κατά την περίοδο εκπόνησης της διπλωματικής, και με τον τρόπο τους με βοήθησαν να ολοκληρώσω το έργο μου και όχι μόνο. Ένα μεγάλο ευχαριστώ επίσης στους καθηγητές μου, για τις γνώσεις που μου πρόσφεραν όλο αυτό το διάστημα. Τέλος, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου κ. Γιώργο Στεργιόπουλο, για τις κατευθύνσεις και τις συμβουλές που μου έδωσε πάνω στο θέμα, καθώς και για την γρήγορη ανταπόκρισή του. Ελπίζω να μπορέσουμε αργότερα να αναγάγουμε σε ερευνητικό επίπεδο όλη αυτή την προσπάθεια, προσφέροντας γνώση που μπορεί να βοηθήσει έστω και στο ελάχιστο, στην διασφάλιση ενός καλύτερου ιατρικού απορρήτου.

Εμμανουήλ Βογιατζή

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Πίνακας περιεχομένων

Λίστα Σχημάτων

Σε κάθε καταχώρηση εμφανίζεται η αρίθμηση, η λεζάντα, και η σελίδα.

Λίστα Πινάκων

Σε κάθε καταχώρηση εμφανίζεται η αρίθμηση, η λεζάντα, και η σελίδα.

Ακρωνύμια

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
PACS	Picture Archiving and Communication System
CVE	Common Vulnerabilities and Exposures
NAS	Network-attached Storage
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol

Περίληψη

Στην παρούσα διπλωματική εργασία θα κάνουμε χρήση του Snort, ενός εργαλείου ανίχνευσης (IDS) και αποτροπής (IPS) απειλών. Το συγκεκριμένο εργαλείο εφαρμόζεται σε δίκτυα, με σκοπό να ειδοποιήσει και να παρεμποδίσει την εξέλιξη κακόβουλων επιθέσεων σε χώρους που περιέχουν ευαίσθητα δεδομένα. Το σύστημα θα εστιάζει κυρίως σε χώρους κλινικών εγκαταστάσεων ασθενών, οι οποίοι κάνουν χρήση συστημάτων PACS. Για τον σκοπό αυτό, έχουμε συλλέξει δεδομένα από μία κλινική η οποία έχει στην κατοχή της ένα Synology το οποίο λειτουργεί ως server. Επίσης, κάνει χρήση της dcm4chee εφαρμογής, για μεταφορά, αποθήκευση και ανάκτηση των ιατρικών της δεδομένων.

Πάνω σε αυτό το παράδειγμα, θα προσπαθήσουμε και εμείς να αναπτύξουμε τη λογική εγκαθίδρυσης κανόνων, θα αναλύσουμε το περιβάλλον της κλινικής, την καθημερινή της κίνηση, καθώς και τις απειλές που δέχεται. Έπειτα, θα φτιάξουμε και θα εφαρμόσουμε τους κανόνες του συστήματος. Προτού γίνουν όμως όλα αυτά, και για να προστατέψουμε την ταυτότητα της κλινικής και των ασθενών της, θα δούμε τον τρόπο που ανωνυμοποιήσαμε τις ευαίσθητες πληροφορίες που περικλείουν τα πακέτα της κίνησης του δικτύου της.

Τέλος, θα καταθέσουμε τα συμπεράσματά μας, καθώς και θα δώσουμε ιδέες για μελλοντική ανάπτυξη του συστήματός μας. Όλα αυτά με σκοπό, να βοηθήσουν την ευρύτερη κοινότητα της ιατρικής και της διασφάλισης των πολύτιμων δεδομένων που αυτή διατηρεί στην κατοχή της.

Λέξεις Κλειδιά: *IDS, IPS, Snort, Rules, PACS, Synology, Ιατρικό απόρρητο, Κανόνες δικτύου, Κακόβουλες επιθέσεις, Anonymization*

Abstract

On the present thesis we are making use of Snort, a software tool for detection (IDS) and prevention (IPS) of malicious traffic, which is applied to networks in order to alert and prevent the ongoing activity of malicious attacks in places that sensitive information are of presence. The system mainly focuses on the environment of a clinical infrastructure, in which PACS systems are applied. For this reason, we gathered data from a clinic which has under its control a Synology Disk Station that is playing the role of a server, and is making use of a dcm4chee application for transport, storage and mining utilities of their medical data.

On this specific example, we will attempt to grow a system of rule setting, we will analyze the clinic's environment, its day to day traffic and the threats it is facing, and we will forge and apply the rules of the system. But before we dig deeper into our subject, and in order to protect the identity of the medical clinic and its' patients, we shall find a way to anonymize all the sensitive information that are included in the packet capture.

Finally, we will give our results on the subject and present ideas for future work. We hope that the work presented here and any future growth of the system will help the broader medical community into the protection of the medical data.

Keywords: *IDS, IPS, Snort, Rules, PACS, Synology, medical secret, network rules, malicious cyber attacks, anonymization*

1

Εισαγωγή

1.1 Συστήματα Εντοπισμού και Αποτροπής Διαδικτυακών Απειλών

Τα συστήματα εντοπισμού (**IDS**) και αποτροπής (**IPS**) απειλών, έχουν τη δυνατότητα να εφαρμοστούν σε δίκτυα τόσο μικρά όσο και μεγάλα. Αυτό συμβαίνει, καθώς διαθέτουν μεγάλο εύρος κινήσεων και είναι πολύ εύκολο να τα φέρει η οποιαδήποτε επιχείρηση ή οργανισμός στα μέτρα του. Μπορούν να είναι πολύπλοκα ή να εστιάζουν σε βασικές αδυναμίες, ανάλογα με τις ανάγκες και τις γνώσεις των ατόμων που τα διαχειρίζονται. Με ελάχιστους πόρους, μπορεί κάποιος να καλύψει μεγάλο εύρος κακόβουλων επιθέσεων και να διασφαλίσει τα δεδομένα του χώρου του από ανεπιθύμητες ενέργειες.

Σε ειδικότερη κλίμακα, τα συστήματα αυτά διαχωρίζονται σε **Host-based ή Network-based**. Το πρώτο, εστιάζει περισσότερο στην παρακολούθηση ενός μεμονωμένου μηχανήματος, και το σύστημα παρακολούθησης είναι εγκατεστημένο στον συγκεκριμένο μόνο host. Στην δεύτερη περίπτωση, το σύστημα παρακολουθεί γενικότερα τις κινήσεις του δικτύου και παίρνει αποφάσεις πριν τα πακέτα καταλήξουν στον στόχο τους. Και οι δύο περιπτώσεις, έχουν τα δυνατά και τρωτά τους σημεία. Ωστόσο, υπάρχουν και συστήματα που συνδυάζουν τα θετικά και των δύο καταστάσεων, δημιουργώντας έτσι υβρίδια συστήματα ανίχνευσης και πρόληψης.

Οποιαδήποτε προσέγγιση ωστόσο και να επιλέξουμε, είναι ιδιαίτερα σημαντικό να θυμόμαστε ότι τίποτα δεν μας παρέχει απόλυτη ασφάλεια. Αυτό καθιστά την ασφάλεια μια διαρκή διεργασία ανάλυσης των κινήσεων και ανάπτυξης των στρωμάτων άμυνας.

1.2 Αντικείμενο διπλωματικής

Συγκεκριμένα, το δικό μας σύστημα θα είναι Network-based. Σκοπός μας, είναι η χρήση των δεδομένων που έχουμε στα χέρια μας, προκειμένου να τα αναλύσουμε και να δημιουργήσουμε κανόνες. Αυτοί θα επιβλέπουν το δίκτυο, και θα αποτρέπουν καταστάσεις πριν αυτές ολοκληρωθούν και έρθουν σε επαφή με τον κάθε host. Για την επιτυχία του στόχου μας, θα δημιουργήσουμε κανόνες ανάλογα με τις ανάγκες μας.

Η δυσκολία της διπλωματικής έγκειται στο γεγονός, ότι πρέπει να αποτρέψουμε απειλές, διατηρώντας παράλληλα το δίκτυό μας λειτουργικό, χωρίς δηλαδή να κόβει τις κινήσεις που είναι θεμιτές. Πολλές φορές αυτό δεν είναι τόσο εύκολο, καθώς πόροι που χρησιμοποιεί ένας κακόβουλος χρήστης για να βρει αδυναμίες στο σύστημά μας, είναι οι ίδιοι πόροι που εμείς χρησιμοποιούμε για την διεκπεραίωση των καθημερινών μας αναγκών.

Όλα αυτά θα τα δούμε στην συνέχεια, προκειμένου να βρούμε την χρυσή τομή μεταξύ ενός ασφαλούς και λειτουργικού δικτύου.

1.3 Δομή της διπλωματικής

Στο **κεφάλαιο 2,** θα δούμε τον τρόπο σκέψης με τον οποίο θα αναζητήσουμε τις απειλές, και θα φτιάξουμε κανόνες γενικότερης φύσεως πέραν από αυτούς που θα προκύψουν κατά την ανάλυση των πακέτων μας. Στο **κεφάλαιο 3,** θα δούμε τον τρόπο και τα εργαλεία που χρησιμοποιήσαμε για να ανακτήσουμε και να ανωνυμοποιήσουμε την πληροφορία από το περιβάλλον της κλινικής, και θα κάνουμε την πρώτη μας ανάλυση. Η δημιουργία κανόνων που θα αναλυθεί στο **κεφάλαιο 4,** θα διαχωριστεί σε κανόνες που αναδύονται από την κακόβουλη και την καθημερινή κίνηση της κλινικής, καθώς και γενικούς κανόνες. Τέλος, θα διατυπωθούν τρόποι και σκέψεις διεξαγωγής μελλοντικής έρευνας στο **κεφάλαιο 5,** και τα συμπεράσματά μας στο **κεφάλαιο 6**.

2

Απειλές Περιβάλλοντος

Στο κεφάλαιο αυτό, θα κάνουμε μία ανασκόπηση των απειλών που δημιουργούνται στον χώρο της κλινικής από την ίδια της την υποδομή. Είναι γνωστό πως κάθε τεχνολογία και οποιοσδήποτε τρόπος επικοινωνίας μεταξύ των συσκευών, έχει τις δικές του αδυναμίες όσον αφορά την ασφάλεια. Για τον λόγο αυτό, θα κοιτάξουμε στις τεχνολογίες που χρησιμοποιεί η κλινική και θα βρούμε αναφορικά για αυτές CVE's με γνωστά exploit.

2.1 Τεχνολογίες στον Χώρο της Κλινικής

Ας κοιτάξουμε λοιπόν αναλυτικότερα τι έχει στην κατοχή της η κλινική:

- **Synology NAS DS423+**, το οποίο χρησιμοποιεί η κλινική ως **server** για να στήσει την εφαρμογή και να διαχειριστεί τα αρχεία της. Αυτό αναγνωρίζει ως μοναδικό χρήστη τον admin του συστήματος, ο οποίος μπορεί να βρει πρόσβαση σε αυτό με δύο τρόπους. Ο πρώτος είναι τοπικά, ενώ ο δεύτερος είναι μέσω του quickconnect. Το quickconnect, αποτελεί ένα διαχειριστικό portal της Synology για απομακρυσμένη διαχείριση του συστήματος.
- Εγκατεστημένη στον παραπάνω server, είναι η **εφαρμογή dcm4chee v5.30.0**. Όπως και στο Synology, έτσι και εδώ υπάρχει admin χρήστης ο οποίος την διαχειρίζεται. Επιπλέον, έχει δημιουργηθεί ένα group χρηστών, που ανήκει στους γιατρούς για την καθημερινή διεκπεραίωση των εργασιών τους. Η εφαρμογή είναι διαθέσιμη μόνο τοπικά.
- **LAN δίκτυο,** στο οποίο είναι συνδεδεμένες οι διάφορες συσκευές και μέσω αυτού επικοινωνούν μεταξύ τους.

- **Τερματικά,** που φέρουν **Windows 10** OS με περιορισμένα προνόμια για τους υπαλλήλους της κλινικής.

2.2 Exploit ανά Τεχνολογία

Όπως αναφέραμε, κάθε τι από τα παραπάνω, περιέχει τα δικά του τρωτά σημεία. Πολλά από αυτά μπορεί να μην έχουν ανακαλυφθεί ακόμα. Άλλα όμως, είναι γνωστά και έχουν δημοσιευμένα διανύσματα επίθεσης. Σε αυτά θα εστιάσουμε και εμείς σε πρώτη φάση, καθώς είναι πιο εύκολο για έναν επιτιθέμενο να τα βρει και να τα εκμεταλλευτεί. Για αυτόν τον λόγο, δημιουργήσαμε έναν πιθανό τρόπο σκέψης που θα μπορούσε να ακολουθήσει κάποιος τρίτος, προκειμένου να έχει πρόσβαση στις ευαίσθητες πληροφορίες μας.

2.2.1 Τρόποι προσέγγισης ευαίσθητης πληροφορίας

Για την αναζήτηση ευπαθειών, ψάχνουμε στα **attack surfaces** από τα οποία μπορεί κάποιος να έχει πρόσβαση στα αρχεία του PACS. Ιδανικά, κάποιος κακόβουλος θα ήθελε να βρίσκεται μέσα στο **τοπικό δίκτυο** της κλινικής. Αυτό θα του επέτρεπε να κάνει **pivoting** και να βρει την πληροφορία που θα αναζητούσε, αν είχε αρκετό χρόνο στην διάθεσή του. Ένας τρόπος που θα μπορούσε να επιτευχθεί η είσοδος του στο τοπικό δίκτυο, θα ήταν με την φυσική του παρουσία στο χώρο της κλινικής. Κάτι τέτοιο όμως, θα απαιτούσε φυσική ασφάλεια, την οποία δεν θα καλύψουμε σαν ενδεχόμενο στην παρούσα κατάσταση. Εναλλακτικά, θα μπορούσε να κάνει χρήση άλλων τεχνικών όπως **port forwarding.** Κατά την χρήση αυτών, ο επιτιθέμενος εκμεταλλεύεται ανοιχτές πόρτες στο δίκτυό μας, και κερδίζει μία θέση ανάμεσά μας. Στην συνέχεια, θα χρειαζόταν να βρει έναν τρόπο να ξεπεράσει την αυθεντικοποίηση είτε του Synology, είτε της εφαρμογής dcm4chee για να έρθει σε επαφή με τις ευαίσθητες πληροφορίες.

Ένας άλλος τρόπος, θα ήταν να έρθει απευθείας σε επαφή με το **quickconnect portal** του Synology - στην περίπτωση που αυτό είναι ενεργοποιημένο - και να εκμεταλλευτεί οποιαδήποτε μέσα για να ξεπεράσει την αυθεντικοποίησή του.

Τέλος, έστω ένας χρήστης (υπάλληλος ή μη σε τερματικό Windows 10), με προνόμια non-admin στο εσωτερικό δίκτυο. Κάνοντας χρήση μίας τεχνικής privilege escalation, θα μπορούσε να κατεβάσει λογισμικό που θα του επέτρεπε την παρακολούθηση του δικτύου και την εύρεση πιθανών credentials, τόσο για το dcm4chee, όσο και για το Synology. Οπότε, θα έπρεπε να δούμε και τα **privilege escalation vulnerabilities** που υπάρχουν στο λογισμικό των Windows 10.

2.2.2 Αδυναμίες για να προσέξουμε

Έχοντας υπόψη τα παραπάνω, πρέπει να αναλογιστούμε τι χρήζει προσοχής και σε ποιες γνωστές αδυναμίες μπορεί κάποιος να βρει το βήμα για να σπάσει τις γραμμές άμυνας. Έτσι, μετά από σκέψη και αναζήτηση, καταλήγουμε στα εξής σημεία:

- Για το LAN δίκτυο, πρέπει να κοιτάμε κυρίως **ποιες πόρτες είναι ανοιχτές** και να ορίζουμε ποιος θα έχει πρόσβαση μέσω αυτών. Επίσης, θα πρέπει να αναζητούμε πότε οι κινήσεις αυτές θα αρχίσουν να θεωρούνται ύποπτες και θα χρειαστεί να κόβονται.
- Για το quickconnect portal του Synology, καλό θα ήταν να χρησιμοποιήσουμε ένα **IP whitelist** και να κάνουμε drop όποιες IP δεν ανήκουν στην λίστα μας. Ένας λόγος που πρέπει να γίνει αυτό, είναι καθώς έχουν υπάρξει στο παρελθόν περιστατικά buffer overflow attack, μέσω των οποίων έχει διαρρεύσει ο κωδικός.
- Για το privilege escalation που μπορεί να έρθουμε αντιμέτωποι στα τερματικά των Windows, θα εστιάσουμε σε γνωστά exploits τα οποία είναι δημοσιευμένα και δεν έχουν γίνει patched από την Microsoft. Σε αυτά μετά από μια αναζήτηση για CVEs' που αφορούν επιθέσεις σε τοπικό δίκτυο καταλογίζουμε τα εξής:

  1)**Print Spooler Vulnerability**

  https://www.cvedetails.com/cve/CVE-2023-36874/

  2) **Service Tracing Privilege Elevation Vulnerability**

  https://www.cvedetails.com/cve/CVE-2020-0668/

  3) **MS16-016 mrxdav.sys WebDav Local Privilege Escalation**

  https://www.cvedetails.com/cve/CVE-2016-0051/

  4) **Office OLE Multiple DLL Side Loading Vulnerabilities**

  https://www.cvedetails.com/cve/CVE-2016-0041/

- Τέλος, όσον αφορά την εφαρμογή μας, δεν βρέθηκαν γνωστά exploits για το συγκεκριμένο version της. Οπότε, εκεί που θα πρέπει να εστιάσουμε, θα είναι σε περίεργα **μοτίβα που δεν ανήκουν στην καθημερινή κίνηση**. Κάτι που μπορούμε να ορίσουμε επίσης, είναι μία λίστα των IP που θα επιτρέπονται να έρθουν σε επαφή με την πόρτα εξυπηρέτησης της εφαρμογής.

3

Ανάκτηση, Ανωνυμοποίηση και Ανάλυση Κίνησης

Σε αυτό το κεφάλαιο, θα ασχοληθούμε κυρίως με την ανάλυση των πακέτων που έχουμε λάβει από το δίκτυο της κλινικής, προκειμένου να βρεθούμε στην θέση αργότερα να φτιάξουμε κανόνες κομμένους και ραμμένους στα μέτρα του οργανισμού. Αναφέρεται, ότι τα πακέτα της κακόβουλης κίνησης που θα αναλύσουμε είναι τεχνητά, με σκοπό να προσομοιάζουν πιθανές απειλές που θα μπορούσε να αντιμετωπίζει η κλινική. Προτού προχωρήσουμε όμως στην ανάλυση, θα σχολιάσουμε τον τρόπο και τα μέσα που χρησιμοποιήσαμε για να ανακτήσουμε την πληροφορία, και το χρονικό εύρος που καλύπτει η κίνηση. Επίσης, θα αναφέρουμε τα εργαλεία και τον τρόπο που παρέχουν ανωνυμία στα πακέτα μας, προκειμένου να προστατέψουμε τις πληροφορίες της κλινικής και του πελατολογίου της.

3.1 Ανάκτηση δεδομένων κίνησης

Για την ανάκτηση των δεδομένων, αποκτήσαμε φυσική παρουσία στον χώρο, έπειτα από συνεννόηση με τον υπεύθυνο της κλινικής, και κάναμε χρήση των εξής εργαλείων:

- Ένα **laptop** για ανάγνωση και αποθήκευση της πληροφορίας του δικτύου,
- ένα **managed switch TP-Link TL-SG105E** προκειμένου να κάνουμε mirror την κίνηση,
- δύο **καλώδια ethernet** και
- την εφαρμογή του **Wireshark,** για να μας βοηθήσει με την ανάγνωση της κίνησης.

Συγκεκριμένα, χρησιμοποιήσαμε τα δύο καλώδια με σκοπό να συνδέσουμε το ένα με το Synology NAS και το άλλο με το laptop μας πάνω στο managed switch. Έπειτα, τροποποιήσαμε τις λειτουργίες του switch για να κάνουμε mirror τα πακέτα του NAS στο προσωπικό μας laptop. Τέλος, κάναμε χρήση της εφαρμογής του Wireshark σε promiscuous mode, για ανάγνωση και αποθήκευση των πακέτων.

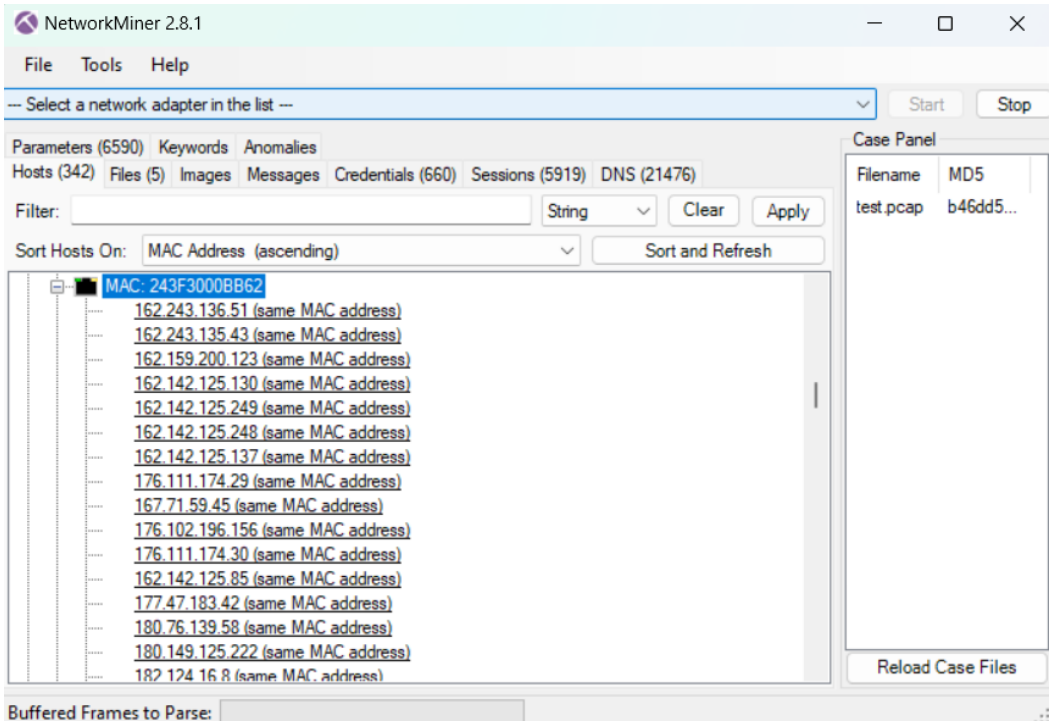
3.2 Ανωνυμοποίηση δεδομένων κίνησης

3.2.1 Διαχωρισμός Πακέτων

Πριν προβούμε σε ανωνυμοποίηση των πακέτων μας, καλό θα ήταν να **διαχωρίσουμε την κίνηση σε καθημερινή και κακόβουλη**. Ένας καλός λόγος για να το κάνουμε αυτό, είναι με σκοπό να σπάσουμε την πληροφορία σε μικρότερα κομμάτια, ώστε μεταγενέστερα να μας είναι πιο εύκολη η ανάλυσή της. Επίσης, στην κακόβουλη κίνηση υπάρχουν λιγότερα και διαφορετικά πράγματα που μας ενδιαφέρει να ανωνυμοποιήσουμε. Μας ενδιαφέρει να διατηρήσουμε τις πληροφορίες που μας παρέχουν οι επιθέσεις, προκειμένου να μπορέσουμε να προστατεύσουμε το σύστημά μας πιο αποδοτικά. Συνεπώς, στην κακόβουλη κίνηση θα ανωνυμοποιηθούν μόνο όσες πληροφορίες ανήκουν στο δίκτυό μας.

Για τον σκοπό αυτό, κάναμε χρήση του **Network Miner**, ενός εργαλείου ανάλυσης PCAP αρχείων. Έτσι, θα διαχωρίσουμε τις IP που προκύπτουν από το εξωγενές περιβάλλον του οργανισμού, με αυτές από το εσωτερικό του. Σύντομα, καταλήγουμε σε ένα συμπέρασμα που θα μας λύσει τα χέρια και θα μας βοηθήσει στον διαχωρισμό της κίνησης σε μηδαμινό χρόνο.

Αυτό λοιπόν που ανακαλύψαμε φαίνεται στην παρακάτω εικόνα:



Εικόνα 3.1.2.1

Βλέπουμε ότι υπάρχουν πολλές IP οι οποίες φέρουν την ίδια MAC. Το μυαλό μας πάει απευθείας σε **τεχνικές IP Spoofing.** Παρατηρώντας ορισμένες ακόμα μεταβλητές, γρήγορα βγάζουμε το συμπέρασμα ότι το μεγαλύτερο αν όχι **όλο το ποσοστό της εξωτερικής κίνησης, προέρχεται από μία και μόνο MAC**, την 24:3f:30:00:bb:62. Για να επαληθεύσουμε την θεωρία μας, αναζητήσαμε αν μας επιστρέφονται πακέτα εκτός δικτύου πέραν από αυτά που προέρχονται από την συγκεκριμένη MAC. Προς διευκόλυνσή μας, το αποτέλεσμα ήταν μηδενικό. Έτσι, με αυτό το σκεπτικό, διαχωρίσαμε την κίνηση σε καθημερινή και κακόβουλη, με μόνο παράγοντα δηλαδή αυτόν της MAC.

3.2.2 Ανωνυμοποίηση Πακέτων

Σε συνέχεια, προχωράμε στην ανωνυμοποίηση των πακέτων η οποία έγινε με την χρήση του **tracewrangler**. Το συγκεκριμένο εργαλείο, παρέχει δυνατότητες **ανωνυμοποίησης μέχρι επιπέδου 4, στα TCP** πακέτα. Για τις υπόλοιπες ευαίσθητες πληροφορίες, έγινε **εύρεση και αντικατάσταση** με ψευδή στοιχεία, ωστόσο ακριβώς ίδιου μήκους, προκειμένου να επηρεαστεί όσο λιγότερο η δομή των πακέτων. Το subnet άλλαξε σε **10.51.1.0/24,** ενώ **αφαιρέθηκε το payload από τα ICMP** πακέτα. Οι **MAC** από όλες τις συσκευές, αλλάξαν σε **τυχαίες**. Οι διευθύνσεις **IPv6 αντικαταστάθηκαν** και αυτές με άλλες **τυχαίες,** ωστόσο με **συγχρονισμένα prefix**. Τέλος, όλες οι **TCP και UDP πόρτες στο διάστημα 1-1024 παρέμειναν οι ίδιες,** ενώ κάποιες ευαίσθητες -όπως αυτή της επικοινωνίας με τον PACS- αλλάξαν.

Στην κακόβουλη κίνηση από την άλλη πλευρά, αλλάξαμε μόνο τα στοιχεία της κλινικής, όπως πόρτες, IP και MAC. Δεν αποκρύψαμε τίποτα από την πλευρά του επιτιθέμενου, ώστε να διατηρήσουμε και όσο το δυνατόν καλύτερες τις ικανότητες ανάλυσης των επιθέσεων.

3.3 Ανάλυση δεδομένων κίνησης

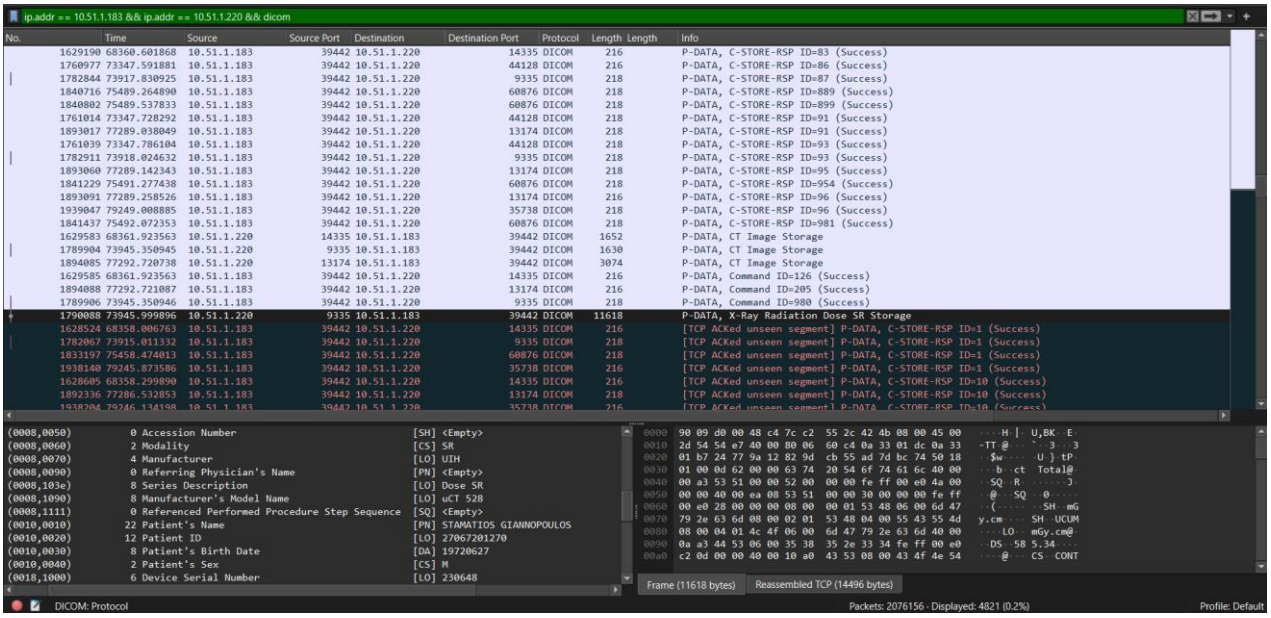
Με σκοπό να πετύχουμε μια καλύτερη ανάλυση, προγραμματίσαμε την διαδικασία ανάκτησης, ώστε να καλύψει το βελησνεκές μίας ολόκληρης εργάσιμης ημέρας. Με τον τρόπο αυτό, μπορούμε να δημιουργήσουμε μια πιο ολοκληρωμένη άποψη όσον αφορά τις διεργασίες που τρέχουν για το διάστημα που ο **οργανισμός παραμένει λειτουργικός**, για τις **διαδικασίες που τρέχουν στο παρασκήνιο σε νυχτερινές ώρες**, καθώς και **για κινήσεις κακόβουλες που διαδραματίζονται ανεξάρτητα του ωραρίου της κλινικής**.

3.3.1 Παρατηρήσεις Καθημερινής Κίνησης

Με όλα τα στοιχεία πλέον στα χέρια μας, θα παρουσιάσουμε μια αναφορά που έχει ως σκοπό, την αναγνώριση των συσκευών του δικτύου, και πως αυτές, επικοινωνούν μεταξύ τους. Επίσης, προσπαθούμε να δούμε αν, και πόσες IP εκτός του δικτύου μας, έρχονται σε επαφή με αυτό, καθώς και για ποιον σκοπό.

Για αυτόν το λόγο, αναλύσαμε την χρονική περίοδο με την μεγαλύτερη κίνηση στο δίκτυο της κλινικής και καταλήξαμε σε κάποια γενικά συμπεράσματα. Τα δύο υψίστης σημασίας μηχανήματα στο δίκτυο και σε αυτά που θα δοθεί και το μεγαλύτερο βάρος, είναι κυρίως το **Synology NAS,** που βρίσκεται κάτω από την διεύθυνση **10.51.1.183,** και ο **αξονικός,** στην διεύθυνση **10.51.1.220**. Ειδικά ο αξονικός, επικοινωνεί κυρίως με το Synology NAS και ελάχιστα με το υπόλοιπο δίκτυο, αφού μόλις τα 159 από τα δύο εκατομμύρια περίπου πακέτα, απευθύνονται σε άλλες επικοινωνίες πέρα από την μεταξύ τους. Ακόμα και αυτά τα 159 πακέτα όμως, αφορούν responses σε multicast requests.

Συγκεκριμένα, παρακάτω βλέπουμε μια επιτυχή μεταφορά αρχείων από το αξονικό μας στο Synology:



Εικόνα 3.1.3.1

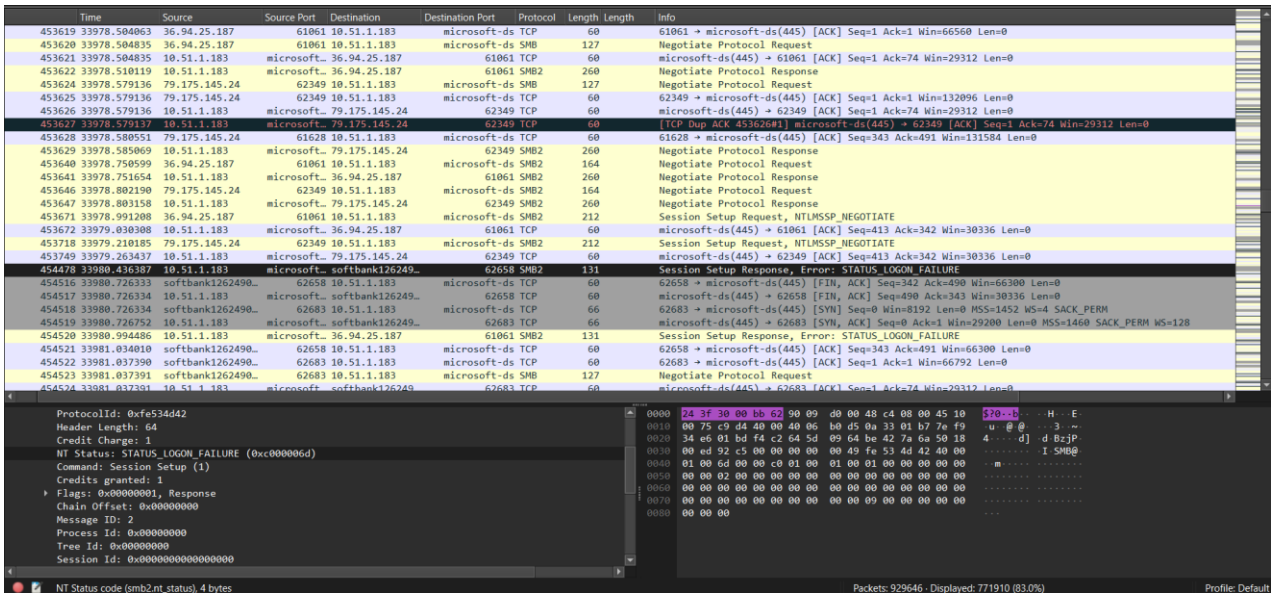
Όπως φαίνεται και στα packet details, μπορούμε να δούμε το φύλο, την ηλικία, το όνομα και όλα τα υπόλοιπα χαρακτηριστικά του ασθενή, τα οποία προς αποφυγή παρεξηγήσεως, είναι όπως ενημερώσαμε ανωνυμοποιημένα. Επίσης, στην λίστα με τα πακέτα, μπορούμε να διαπιστώσουμε ότι γίνεται και μεταφορά εικόνων με χρήση πρωτοκόλλου dicom, οι οποίες φυσικά, προέρχονται από τον αξονικό.

Στο γενικότερο πλαίσιο των επικοινωνιών του intranet, παρατηρούμε πολλά **MDNS πακέτα** για την αναγνώριση των συσκευών του δικτύου μεταξύ τους. Βλέπουμε επίσης, ότι υπάρχουν αρκετοί **σταθεροί υπολογιστές και εκτυπωτές**, καθώς και παρατηρείται η καθημερινή φυσιολογική κίνηση της κλινικής.

3.3.2 Παρατηρήσεις Κακόβουλης Κίνησης

Από την άλλη μεριά αντιλαμβανόμαστε σύντομα, ότι υπάρχει ένα σημείο στο οποίο στηρίζεται ο επιτιθέμενος, προκειμένου να εκτελέσει όλες του τις ενέργειές. Εύλογα, το σημείο αυτό απευθύνεται στο Synology NAS με IP 10.51.1.183. Όπως αναφέραμε και νωρίτερα, το NAS είναι διαθέσιμο από το extranet μέσω του quickconnect portal. Προχωρώντας περαιτέρω στην ανάλυσή μας, διαπιστώνουμε τις εξής προσπάθειες από τον επιτιθέμενο:

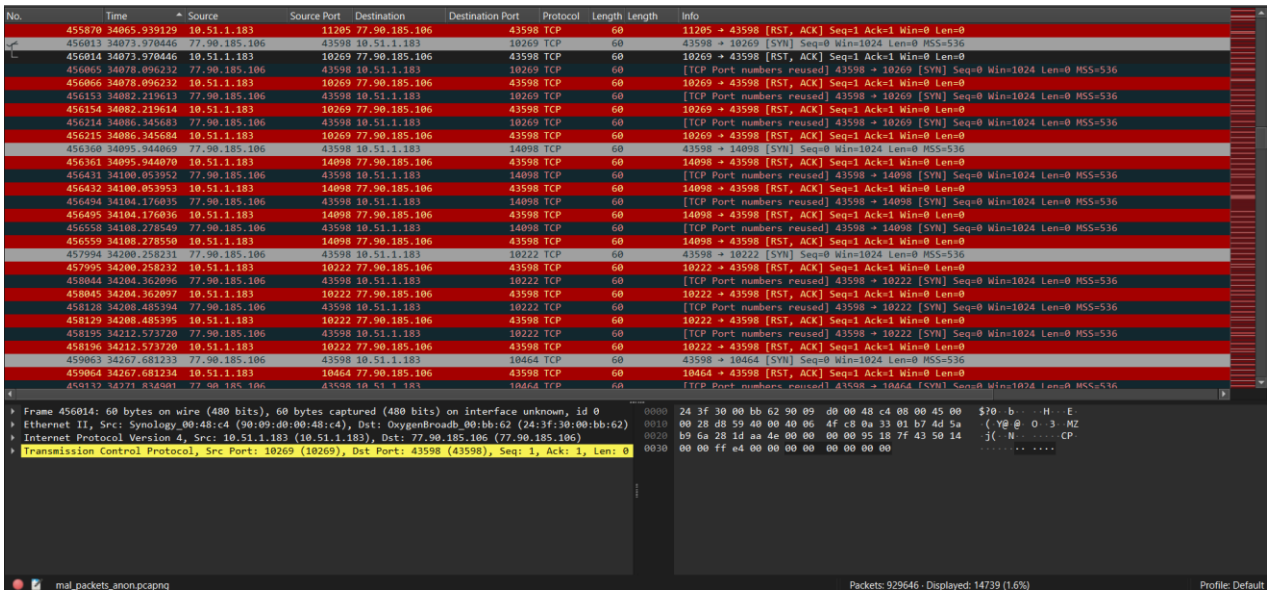
1. Περίπου 7/10 πακέτα στοχεύουν στην **πόρτα 445** του Synology και όχι αδικαιολόγητα, αφού υπάρχουν γνωστοί τρόποι εκμετάλλευσής της. Ενδεικτικά παρατίθενται ένα στιγμιότυπο:



Εικόνα 3.1.3.2

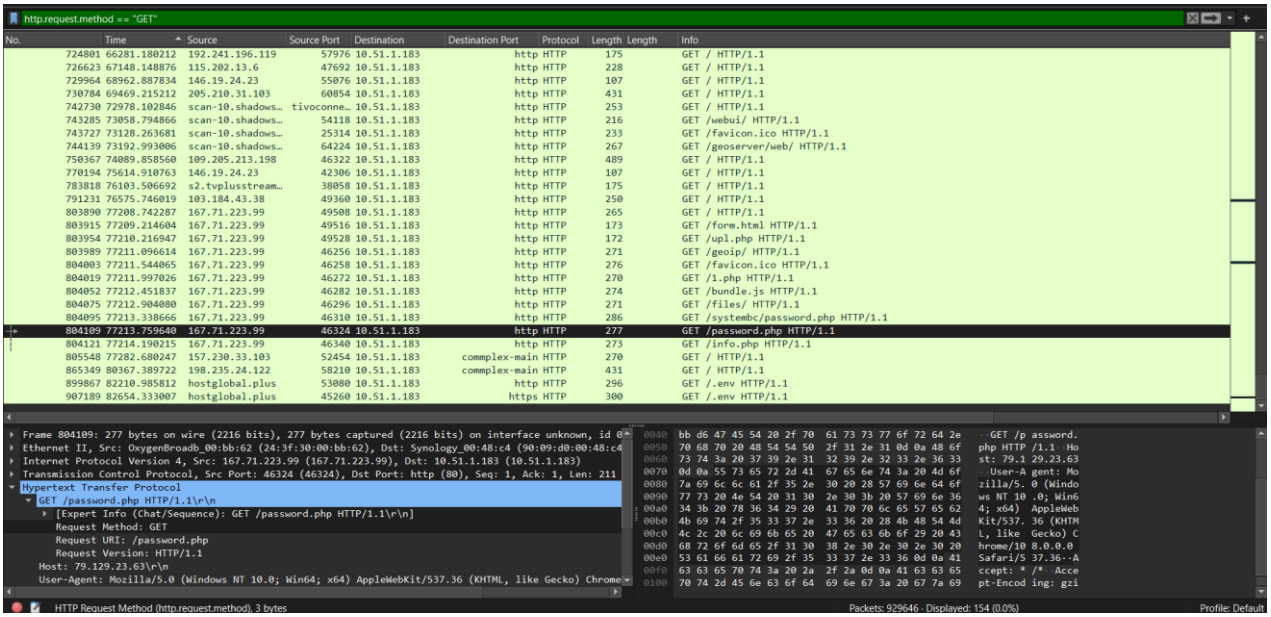
Αν προσέξουμε τα μηνύματα, καταλαβαίνουμε ότι πρόκειται για μια συνεχή απόπειρα απόκτησης πρόσβασης στο σύστημα της κλινικής.

2. Από μόνη της η κίνηση όμως, αν και ανεπιτυχής, παραμένει αρκετά επιβραδυντική, αφού ένα στα τρία πακέτα της ολικής κίνησης προέρχονται από κακόβουλες προσπάθειες. Μία τέτοια κατάσταση φορτώνει το δίκτυό μας καταλήγοντας και σε πιθανά σενάρια **DDoS**. Κινήσεις που δεν στοχεύουν κάπου συγκεκριμένα και το επιβεβαιώνουν, φαίνονται και παρακάτω:



Εικόνα 3.1.3.3

3. Τέλος, ένα ακόμα σενάριο που παρατηρείται, είναι αυτό ενός **File Inclusion Attack**. Η τεχνική αυτή, στοχεύει στην εύρεση αρχείων που περιέχουν ευαίσθητη πληροφορία με απλές μεθόδους GET πάνω από HTTP πρωτόκολλα όπως στο παρακάτω παράδειγμα:



Εικόνα 3.1.3.4

Πολύ σύντομα, έχουμε στα χέρια μας αρκετά σενάρια τα οποία πρέπει να καλύψουμε και αρκετούς κανόνες που πρέπει να δημιουργήσουμε, ώστε να εξασφαλίσουμε πως αυτές οι απόπειρες δεν θα συνεχιστούν. Για αυτό, στο επόμενο κεφάλαιο θα ξεκινήσουμε να δημιουργούμε κανόνες και να καλύπτουμε γενικά πλαίσια συμμόρφωσης. Στην συνέχεια, θα καταλήξουμε σε πιο

ειδικά πλαίσια, μετά από προσεκτικότερη ανάλυση των πληροφοριών των πακέτων. Επίσης, θα φτιάξουμε ξεχωριστούς κανόνες για την καθημερινή και κακόβουλη κίνηση, οι οποίοι όμως θα συνεργάζονται, προκειμένου το σύστημα να παραμείνει λειτουργικό και ταυτόχρονα ασφαλές.

4

Δημιουργία κανόνων

Για την δημιουργία κανόνων, γνωστοποιήσαμε πως θα κάνουμε χρήση του Snort, το οποίο, θα χρησιμοποιήσουμε τόσο ως IDS όσο και ως IPS. Βασισμένοι σε αυτό, μπορούμε να πούμε πως το Snort έχει δύο κύριες λειτουργίες, μία εκ των οποίων είναι αυτή των ειδοποιήσεων (**alerts**), και η άλλη αυτή της απόρριψης πακέτων (**drop**) αντίστοιχα. Θα χρησιμοποιήσουμε την πρώτη λειτουργία, για καταστάσεις οι οποίες ανήκουν σε μια γκρίζα ζώνη και χρήζουν ανθρώπινου ελέγχου. Την δεύτερη λειτουργία από την άλλη, για καταστάσεις στις οποίες πρέπει να ληφθούν άμεσα μέτρα και να τερματιστεί η επικοινωνία μεταξύ δύο μερών.

4.1 Ρυθμίσεις Snort

Προκειμένου το Snort να χρησιμοποιηθεί σε inline mode, δηλαδή για να μπορεί να ελέγχει το ποια κίνηση θα επιτραπεί να εισχωρήσει στο δίκτυο και ποια όχι, πρέπει πρώτα να προχωρήσουμε σε κάποιες βασικές ρυθμίσεις. Αρχικά, θα χρειαστούμε ένα έξτρα **ethernet adapter,** ώστε το ένα να διαβάζει την κίνηση και το άλλο να την 'ρίχνει' αν είναι απαραίτητο. Δεύτερον, πρέπει να ρυθμιστεί το **configuration file** του Snort, ώστε να ξέρει ποια λειτουργία θα ακολουθήσει.

Για τον λόγο αυτό χρησιμοποιήσαμε:

1) Ένα DIGITUS DN-70440 WIRELESS 150N USB2.0 ANTENNA ADAPTER.
2) Στο config αρχείο μας κάνουμε τις εξής τροποποιήσεις:

i. Θέτουμε το HOME_NET ως το intranet της κλινικής 10.51.1.0/24 και ως εξωτερικό θεωρούμε το οτιδήποτε άλλο.

```
ipvar HOME_NET  10.51.1.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

Εικόνα 4.1.1

ii. Για την λειτουργία του inline mode, πρέπει να προσθέσουμε τις παρακάτω γραμμές στο αρχείο μας:

```
# Configure DAQ related options for inline operation. For more inf
#
 config daq: afpacket
 config daq_dir: /usr/lib/x86_64-linux-gnu/daq
 config daq_mode: inline
 config daq_var: buffer_size_mb=128
#
# <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
```

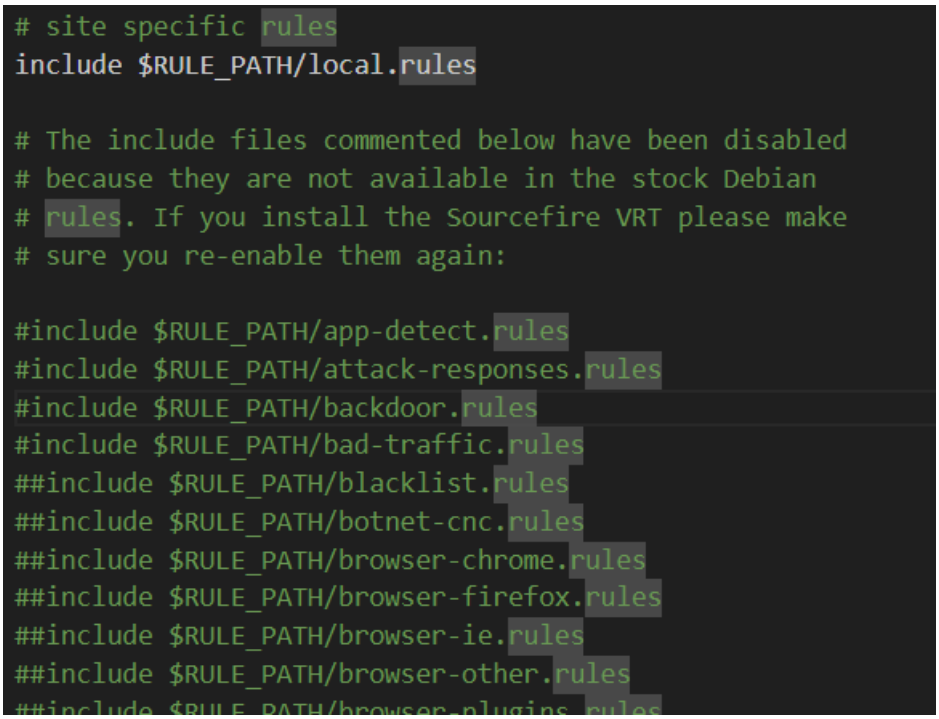
Εικόνα 4.1.2

```
# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6
```

Εικόνα 4.1.3

Οι παραπάνω γραμμές θα δηλώσουν στο Snort, πώς θέλουμε να διαχειριστεί τα πακέτα μας, που θα βρει τις βιβλιοθήκες που χρειάζεται, και τέλος, αν πρόκειται για ζωντανή λήψη των αρχείων, ή για κάποιο dump που θα του δώσουμε προς εξέταση.

iii. Το Snort από μόνο του, διαθέτει επίσης πολλούς κανόνες που έχουν δημιουργηθεί από την κοινότητά του. Επειδή εμείς όμως θα φτιάξουμε τους δικούς μας, πρέπει να αποκλείσουμε αυτούς που δεν χρειαζόμαστε, προκειμένου να μην εμποδίσουν το έργο μας. Ωστόσο, θα εφαρμόσουμε κάποιους από αυτούς για πιο κοινές αδυναμίες που ενδιαφέρουν και το δικό μας δίκτυο. Έτσι, στο config file, αφαιρούμε όλα τα αρχεία, των οποίων οι κανόνες δεν μας ενδιαφέρουν, και κρατάμε μόνο το **local.rules** στο οποίο θα συνθέσουμε τους δικούς μας.



Εικόνα 4.1.4

iv. Τέλος, διατηρούμε τις υπόλοιπες ρυθμίσεις ίδιες όπως ήταν προκαθορισμένες.

4.2 Κανόνες αντιμετώπισης κακόβουλης κίνησης

Πλέον είμαστε έτοιμοι να αναλύσουμε και να δημιουργήσουμε τους κανόνες μας. Για αρχή όπως αναφέραμε, θα εστιάσουμε στην παραγωγή κανόνων που αντιμετωπίζουν άμεσες απειλές που δεχόμαστε. Για αυτό, έχουμε προβεί στην δημιουργία μιας σειράς κανόνων, οι οποίοι βασίστηκαν στην αρχική μας ανάλυση. Κατά το πέρας όμως της διαδικασίας, τους εξειδικεύσαμε, προκειμένου να αντιμετωπίζουν καταστάσεις που χρήζουν μεγαλύτερης προσοχής.

4.2.1 Σύνθεσης Κανόνων Κακόβουλης Κίνησης

Παρακάτω, θα παραχωρηθεί ένας πίνακας με το σύνολο των κανόνων και το μοναδικό τους αναγνωριστικό, για χρήση γρήγορης αναφοράς.

Sid: 2000001	alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Ping"; sid:2000001;)
Sid: 2000002	drop tcp any any -> 10.51.1.183 445 (msg:"Potential Synology Samba Vulnerability attack"; sid:2000002;)
Sid: 2000003	alert tcp any any -> 10.51.1.183 80 (msg:"Potential File Inclusion Attack Attempt"; \ content:"GET"; http_method ;sid:2000003;)
Sid: 2000004	alert tcp 10.51.1.183 any -> any any (msg:"SMB Login Failure Attempt"; \ content:"|6d 00 00 c0|"; rawbytes; depth:250; \ sid:2000004; gid:201;)
	rate_filter gen_id 201, sig_id 2000004, track by_dst, \ count 5, seconds 120, new_action drop, timeout 60
Sid: 2000005	alert tcp any any -> any any (msg:"Admin Credentials"; \ content: "|61 00 64 00 6d 00 69 00 6e|"; rawbytes; depth:250; \ sid:2000005;)
Sid: 2000006	alert tcp 10.51.1.183 any -> any any (msg:"HTTP Restricted area access"; \ content: "|4e 6f 74 20 41 6c 6c 6f 77 65 64|"; rawbytes; depth:250; \ sid:2000006;)
Sid: 2000007	alert tcp 10.51.1.183 any -> any any (msg:"HTTP Bad request"; \ content:"|42 61 64 20 52 65 71 75 65 73 74|"; rawbytes; \ depth:250; sid:2000007;)
Sid: 2000008	alert icmp $EXTERNAL_NET any -> any any (msg:"ICMP packet deformed!"; \ dsize:!32; dsize:!64; sid:2000008;)
Sid: 2000009	drop icmp $EXTERNAL_NET any -> any any (msg:"Big ICMP payload!"; \ dsize:>64; sid:2000009;)

Πίνακας 4.2.1

4.2.2 Επεξήγηση Κανόνων Κακόβουλης Κίνησης

Για τον κάθε κανόνα στον παραπάνω πίνακα, θα εξηγήσουμε i) το τι λειτουργία εκτελεί, ii) τον λόγο που δημιουργήθηκε, iii) καθώς και θα φέρουμε ένα αντίστοιχο παράδειγμα απειλής που αντιμετωπίζουμε στο pcap της κακόβουλης κίνησης που αναλύουμε, αν αυτό υπάρχει.

a) alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Ping"; sid:2000001;)

i. Ο συγκεκριμένος κανόνας, μας ενημερώνει για οποιοδήποτε Ping έρχεται στο εσωτερικό μας δίκτυο από εξωτερική πηγή. Το **alert,** σημαίνει πως ο κανόνας αποτελεί απλή προειδοποίηση. Το **icmp,** αποτελεί το πρωτόκολλο που θα παρακολουθεί το Snort, ενώ στην συνέχεια δηλώνουμε τις **IP** και τις **πόρτες** για τις οποίες θα ισχύει ο παραπάνω κανόνας. Για παράδειγμα, θεωρούμε ότι προσέχουμε για pings, που προέρχονται από μια εξωτερική πηγή, και οποιαδήποτε πόρτα της (any), και καταλήγουν σε οποιαδήποτε συσκευή του εσωτερικού μας δικτύου και σε οποιαδήποτε πόρτα της. Τέλος, δηλώνουμε ένα μήνυμα που θα εμφανίζεται κάθε φορά που αντιμετωπίζουμε τέτοια συμπεριφορά, και δίνουμε στον κανόνα μας μια μοναδική ταυτότητα (2000001).

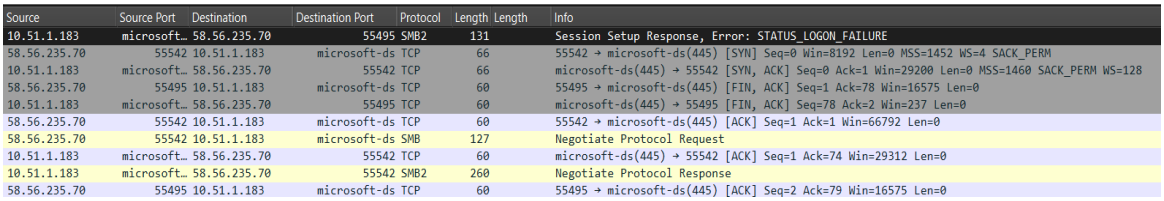
ii. Το συγκεκριμένο alert, μας ενδιαφέρει, καθώς παρακολουθεί τα pings που προέρχονται από το εξωτερικό του δικτύου και συχνά αποτελούν το πρώτο δείγμα επίθεσης από κακόβουλες μηχανές. Οπότε, η ύπαρξη του κανόνα είναι σημαντική ανεξάρτητα της κίνησης που δεχόμαστε.

b) drop tcp any any -> 10.51.1.183 445 (msg:"Potential Synology Samba Vulnerability attack"; sid:2000002;)

i. Σε αντίθεση με τον προηγούμενο κανόνα, αυτός ρίχνει (drop) τα πακέτα αν αυτά πληρούν τους όρους που έχουμε θέσει. Εδώ, αν βρεθεί κάποιο tcp statement που στοχεύει στην πόρτα **445 (SMB)** του server μας, το σύστημα ρίχνει την επικοινωνία, με μήνυμα “Potential Synology Samba Vulnerability Attack”.

ii. Καθώς παρατηρήθηκαν πολλά πακέτα κακόβουλης κίνησης να στοχεύουν στην πόρτα 445 του Synology της κλινικής, προσπαθώντας να εκμεταλλευτούν μια αδυναμία του συστήματος, θεωρήθηκε αναγκαία η καθιέρωση αυτού του κανόνα. Επίσης, μετά από ανάλυση της καθημερινής κίνησης, η συγκεκριμένη πόρτα δεν χρησιμοποιείται από το ενδοδίκτυο. Προφανώς, η πόρτα θα μπορούσε να ήταν κλειστή και από τις εσωτερικές ρυθμίσεις του Synology, αλλά αφού η περίπτωση δεν έχει καλυφθεί, την καλύπτουμε εμείς.

iii. Μια από τις πολλές περιπτώσεις που βρίσκουμε τέτοιες κινήσεις κατά την διάρκεια της ανάλυσης, είναι η ακόλουθη :



Source	Source Port	Destination	Destination Port	Protocol	Length	Length	Info
10.51.1.183	microsoft…	58.56.235.70	55495	SMB2	131		Session Setup Response, Error: STATUS_LOGON_FAILURE
58.56.235.70	55542	10.51.1.183	microsoft-ds	TCP	66		55542 → microsoft-ds(445) [SYN] Seq=0 Win=8192 Len=0 MSS=1452 WS=4 SACK_PERM
10.51.1.183	microsoft…	58.56.235.70	55542	TCP	66		microsoft-ds(445) → 55542 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
58.56.235.70	55495	10.51.1.183	microsoft-ds	TCP	60		55495 → microsoft-ds(445) [FIN, ACK] Seq=1 Ack=78 Win=16575 Len=0
10.51.1.183	microsoft…	58.56.235.70	55495	TCP	60		microsoft-ds(445) → 55495 [FIN, ACK] Seq=78 Ack=2 Win=237 Len=0
58.56.235.70	55542	10.51.1.183	microsoft-ds	TCP	60		55542 → microsoft-ds(445) [ACK] Seq=1 Ack=1 Win=66792 Len=0
58.56.235.70	55542	10.51.1.183	microsoft-ds	SMB	127		Negotiate Protocol Request
10.51.1.183	microsoft…	58.56.235.70	55542	TCP	60		microsoft-ds(445) → 55542 [ACK] Seq=1 Ack=74 Win=29312 Len=0
10.51.1.183	microsoft…	58.56.235.70	55542	SMB2	260		Negotiate Protocol Response
58.56.235.70	55495	10.51.1.183	microsoft-ds	TCP	60		55495 → microsoft-ds(445) [ACK] Seq=2 Ack=79 Win=16575 Len=0

Εικόνα 4.2.1

c) alert tcp any any -> 10.51.1.183 80 (msg:"Potential File Inclusion Attack Attempt"; \ content:"GET"; http_method ;sid:2000003;)

i. Εδώ δεχόμαστε μια ενημέρωση από το σύστημα για πακέτα που κατευθύνονται στην πόρτα **80 (https)** και κάνουν χρήση της **μεθόδου GET**. Ο λόγος που δεν πραγματοποιούμε drop στα πακέτα, είναι καθώς η ίδια μέθοδος χρησιμοποιείται και για γνήσια requests μεταξύ client-server.

ii. Είχαμε πολλές περιπτώσεις που έγινε χρήση της μεθόδου GET για εύρεση άλλων σελίδων στο directory, οι οποίες πιθανότατα να περιέχουν και ευαίσθητες πληροφορίες. Οι προσπάθειες αυτές, αποτελούν έναν τύπο File Inclusion Attack. Οι επιθέσεις στοχεύουν σε αδυναμίες, που επιτρέπουν σε έναν μη αυθεντικοποιημένο πρόσωπο, να έχει πρόσβαση σε αρχεία και σελίδες που δεν θα έπρεπε να έχει. Γίνεται κατανοητό λοιπόν, ότι αυτές οι κινήσεις πρέπει να παρακολουθούνται στενά και να παίρνονται μεμονωμένες αποφάσεις για την κάθε σύνδεση.

iii. Παράδειγμα αποτελεί :

```
167.71.223.99    46282 10.51.1.183    http HTTP    274    GET /bundle.js HTTP/1.1
167.71.223.99    46296 10.51.1.183    http HTTP    271    GET /files/ HTTP/1.1
167.71.223.99    46310 10.51.1.183    http HTTP    286    GET /systembc/password.php HTTP/1.1
167.71.223.99    46324 10.51.1.183    http HTTP    277    GET /password.php HTTP/1.1
167.71.223.99    46340 10.51.1.183    http HTTP    273    GET /info.php HTTP/1.1
```

Εικόνα 4.2.2

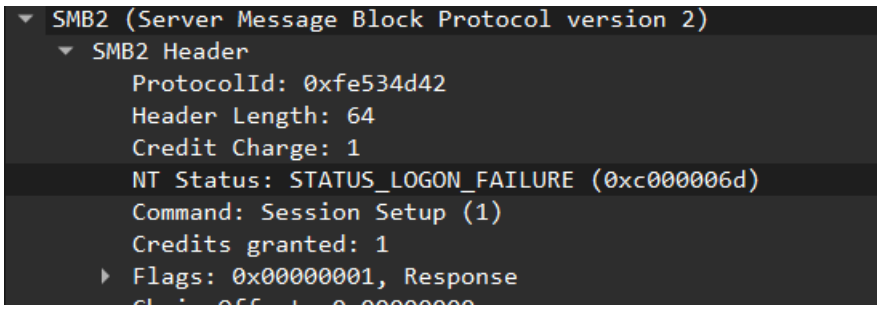
d) alert tcp 10.51.1.183 any -> any any (msg:"SMB Login Failure Attempt"; \ content:"|6d 00 00 c0|"; rawbytes; depth:250; \ sid:2000004; gid:201;)

i. Στον κανόνα παραπάνω, ψάχνουμε αν μέσα στο πακέτο μας, συμπεριλαμβάνεται η πληροφορία που σημάνει ότι υπάρχει **Login Failure,** προκειμένου να μας ενημερώσει αν γίνεται κάποια αποτυχημένη προσπάθεια σύνδεσης στο Synology Server. Αυτή σε **raw bytes** μεταφράζεται σε 6d 00 00 c0. Για αυτόν τον λόγο, χρησιμοποιούμε και τα παραπάνω κριτήρια. Το **depth,** δηλώνει σε τι βάθος θα ψάξει το Snort μέσα στο payload σε bytes, προκειμένου να βρει την πληροφορία. Το depth, είναι δηλωμένο στα 250 bytes, αφού συνήθως αυτή η πληροφορία δίνεται από τις πρώτες στο πακέτο και δεν θεωρούμε ότι πρέπει να ψάξουμε περαιτέρω, γλιτώνοντας έτσι και

πόρους. Τέλος, το gid, αποτελεί ένα id παραγωγής γεγονότος, το οποίο θα χρησιμοποιήσουμε στον επόμενο κανόνα.

ii. Όπως φάνηκε και στον κανόνα 2000002, ο επιτιθέμενος προσπαθεί να εκμεταλλευτεί μια αδυναμία του συστήματος, η οποία όμως συχνά του επιστρέφει ένα μήνυμα "**STATUS_LOGON_FAILURE**" από το SMB. Έτσι, μπορούμε να κάνουμε πιο συγκεκριμένο τον κανόνα για την σύνδεση στην πόρτα 445, ώστε αν χρειαστεί να χρησιμοποιηθεί από το εσωτερικό δίκτυο, να μην παρουσιάζει περιορισμό σε γνήσιους χρήστες. Παρά το γεγονός ότι αποτελεί alert, ο επόμενος κανόνας θα μας βοηθήσει να τον χρησιμοποιούμε με υβρίδιο τρόπο.

iii. Παρατηρούμε πολλά STATUS_LOGON_FAILURE στα packet details του response, ένα από τα οποία φαίνεται παρακάτω :



Εικόνα 4.2.3

e) rate_filter gen_id 201, sig_id 2000004, track by_dst, \
count 5, seconds 120, new_action drop, timeout 60

i. Το **rate_filter**, αποτελεί μια εντολή η οποία δημιουργεί ένα γεγονός κάτω υπό συγκεκριμένες προϋποθέσεις. Όπως αναφέραμε, θέλουμε να χρησιμοποιήσουμε τον κανόνα με sid = 2000004 με υβρίδιο τρόπο. Για αυτό, χρησιμοποιούμε το rate_filter με ορίσματα το gid και το sid του κανόνα αυτού. Το **track by_dst** όρισμα, μετράει πόσες φορές έχει πυροδοτηθεί ο κανόνας 2000004, από την IP στην οποία προορίζεται το STATUS_LOGON_FAILURE μήνυμα, δηλαδή του client. Αν επαναληφθεί για 5 συνεχόμενες φορές μέσα σε διάστημα 120 δευτερολέπτων, τότε δημιουργείται ένα action drop, που αποτρέπει περαιτέρω προσπάθειες για διάστημα 60 δευτερολέπτων.

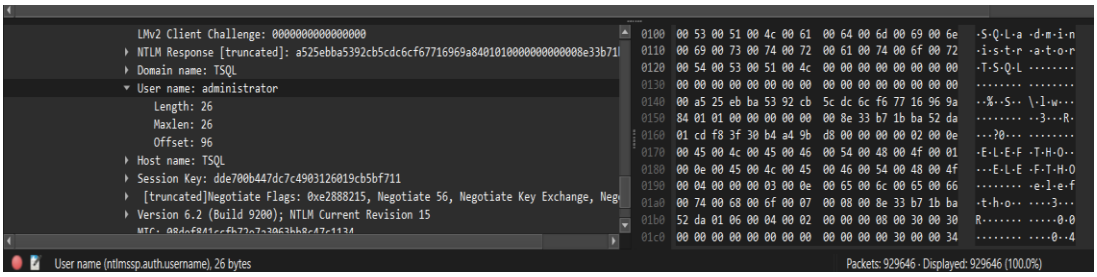
ii. Η ανάγκη λοιπόν μίας πιο ευέλικτης λύσης στην περίπτωση που αποφασίσουμε ότι χρειαζόμαστε το SMB για γνήσιες κινήσεις, μας προτρέπει στην δημιουργία αυτού του συνδυασμού κανόνων.

f) alert tcp any any -> any any (msg:"Admin Credentials"; \
content: "|61 00 64 00 6d 00 69 00 6e|"; rawbytes; depth:250; \
sid:2000005;)

i. Αντίστοιχα με τον 2000004, αναζητούμε για προσπάθειες εισόδου με **στοιχεία admin** και ειδοποιούμε. Σε τέτοιες περιπτώσεις, δημιουργείται ένα byte sequence 61 00 64 00 6d 00 69 00 6e.

ii. Στις ίδιες απόπειρες εισόδου, γίνεται χρήση admin credentials για την ολοκλήρωση του **privilege escalation**. Για τον λόγο αυτό, είναι σημαντικό να παρατηρούμε και αυτήν την μεταβλητή και να παρακολουθούμε αν η πηγή από όπου προέρχεται η κίνηση είναι αποδεκτή ή όχι. Ωστόσο, το ζήτημα που προκύπτει, μπορεί στις περισσότερες περιπτώσεις να αντιμετωπισθεί με ένα IP whitelist που θα εφαρμόσουμε στην συνέχεια.

iii. Μια τέτοια περίπτωση φαίνεται και στο επόμενο στιγμιότυπο:



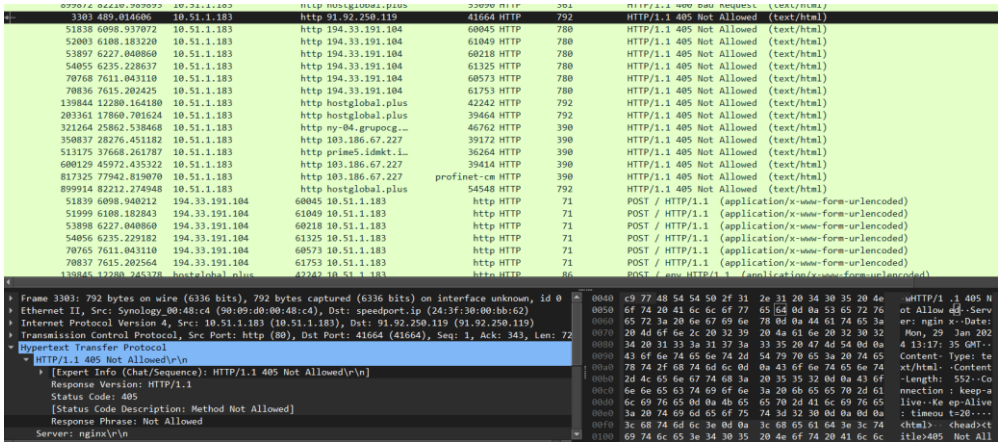
Εικόνα 4.2.4

g) alert tcp 10.51.1.183 any -> any any (msg:"HTTP Restricted area access"; \
content: "|4e 6f 74 20 41 6c 6c 6f 77 65 64|"; rawbytes; depth:250; \
sid:2000006;)

i. Σε συνέχεια του sid = 2000003, παρατηρούμε και αν υπάρχει προσπάθεια εισόδου σε **restricted areas** του http πρωτόκολλου. Αυτό γίνεται με ένα **response** από τον server, με byte sequence 4e 6f 74 20 41 6c 6c 6f 77 65 64.

ii. Αφού έχουμε File Inclusion τύπου επιθέσεις, είναι λογικό πολλές σελίδες που φέρουν ευαίσθητης πληροφορίας, να μην είναι διαθέσιμες στο ευρύ κοινό και να επιστρέφουν τέτοια μηνύματα. Για αυτό, ειδοποιούμε όταν κάτι τέτοιο συμβεί.

iii. Τα πακέτα που πληρούν τέτοιες προϋποθέσεις στην κίνησή μας, φαίνονται παρακάτω:



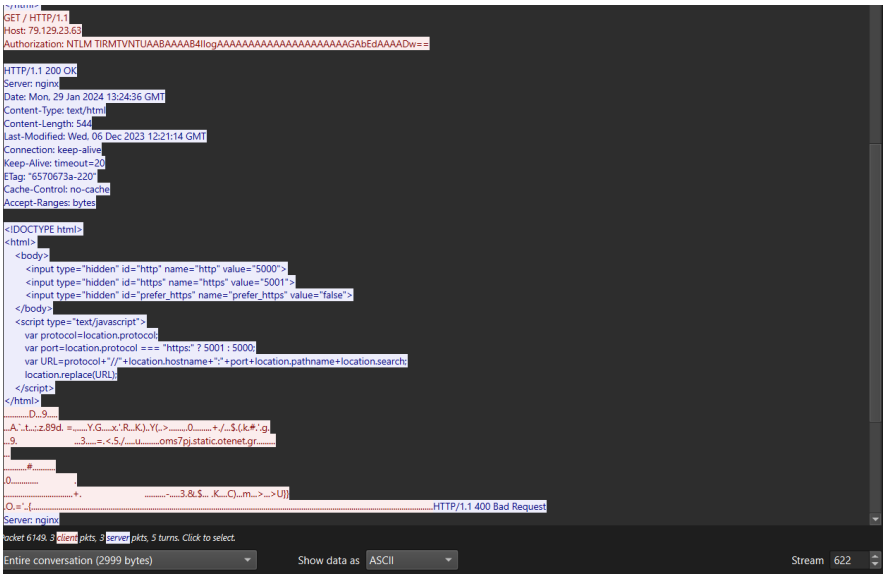
Εικόνα 4.2.5

h) alert tcp 10.51.1.183 any -> any any (msg:"HTTP Bad request"; \
content:"|42 61 64 20 52 65 71 75 65 73 74|"; rawbytes; \
depth:250; sid:2000007;)

i. Ένα byte sequence 42 61 64 20 52 65 71 75 65 73 74, δηλώνει κάποιο **http bad request**. Με τον παραπάνω κανόνα, αναλύουμε και προειδοποιούμε για τέτοια πακέτα.

ii. Πολλές φορές αυτά τα πακέτα δηλώνουν περιπτώσεις που κάποιος κακόβουλος χρήστης προσπαθεί να **τροποποιήσει** πληροφορία στα http request. Με αυτόν τον τρόπο, προσπαθεί να πετύχει αδυναμίες στο σύστημα, ή στα πρωτόκολλα επικοινωνίας, κάτι που δικαιολογεί την ύπαρξη τέτοιων κανόνων.

iii. Παράδειγμα αποτελεί το tcp stream 622, όπου γίνεται η απόπειρα απόκτησης πληροφορίας, με χρήση ψευδών credits και επιστρέφεται ένα Bad Request μήνυμα:



Εικόνα 4.2.6

i) alert icmp $EXTERNAL_NET any -> any any (msg:"ICMP packet deformed!"; \
dsize:!32; dsize:!64; sid:2000008;)

i. Ο κανόνας αυτός εστιάζει στα ping που προέρχονται από το εξωτερικό δίκτυο όπως και ο 2000001, με την διαφορά ότι προσέχουμε αν το payload του ping είναι **διαφορετικό από 32 ή 64 bytes**.

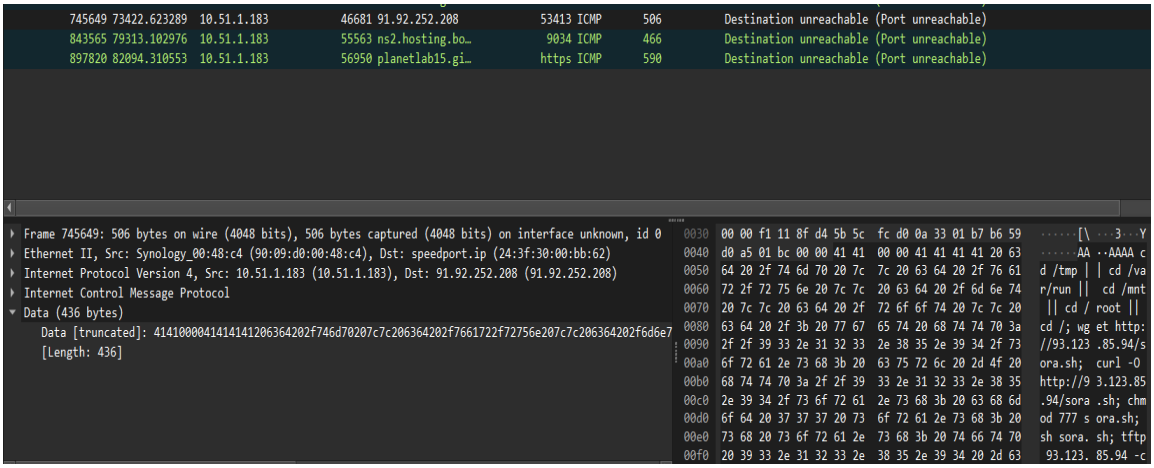
ii. Ο λόγος που μας ενδιαφέρει αυτή η περίπτωση, είναι καθώς το προκαθορισμένο payload των Windows και των UNIX συστημάτων είναι 32 και 64 bytes αντίστοιχα. Έτσι, αν το payload είναι διαφορετικό, σημαίνει ότι η πληροφορία που κουβαλάει το ICMP πακέτο έχει σίγουρα **τροποποιηθεί**. Στον επόμενο κανόνα εξηγούμε γιατί κάτι τέτοιο είναι σημαντικό.

j) drop icmp $EXTERNAL_NET any -> any any (msg:"Big ICMP payload!"; \
dsize:>64; sid:2000009;)

i. Ο κανόνας αυτός εστιάζει στα ping που προέρχονται από το εξωτερικό δίκτυο όπως ο 2000008 και ο 2000001. Η διαφορά έγκειται στο ότι προσέχουμε αν το payload του ping είναι **μεγαλύτερο από 64 bytes**. Σε τέτοιες περιπτώσεις τα πακέτα γίνονται **drop**.

ii. Αυτό που προσπαθούμε να αποτρέψουμε με τον 2000009, είναι να μην πετυχαίνεται επικοινωνία δύο μερών με την χρήση pings μέσω του δικτύου μας. Η συγκεκριμένη επίθεση βασίζεται στην τεχνική **ICMP Tunneling,** όπου ένα αθώο ping μπορεί να κρύψει πληροφορία μέσα του και να κάνει χρήση ενός server, ώστε αυτός να το μεταδώσει αντί του αποστολέα. Έτσι, κόβουμε το οτιδήποτε περιέχει πληροφορία μεγαλύτερη των 64 bytes.

iii. Στην κίνηση μας παρατηρούμε και τέτοιες καταστάσεις, όπως η παρακάτω:



Εικόνα 4.2.7

4.3 Κανόνες εστιασμένοι στην καθημερινή κίνηση

Στην παραπάνω παράγραφο, διατυπώθηκαν οι κανόνες που χρειαζόμασταν, προκειμένου να αντιμετωπίσουμε την κακόβουλη κίνηση. Τώρα, χρειάζεται να κάνουμε την ίδια δουλειά για τις εσωτερικές κινήσεις. Η διαφορά με την προηγούμενη διαδικασία, είναι ότι αυτήν την φορά θα παρατηρήσουμε τις κινήσεις του εσωτερικού δικτύου, προκειμένου να δημιουργήσουμε **εξαιρέσεις** ως προς το ποιες IP είναι φυσιολογικό να χρησιμοποιούν υπηρεσίες και να επικοινωνούν με άλλες συσκευές, και ποιες όχι. Για τον σκοπό αυτό, κάναμε χρήση του Wireshark και φτιάξαμε φίλτρα, προκειμένου να μεταβούμε στα εξής συμπεράσματα:

1. Η συσκευή με IP 10.51.1.220 που ανήκει στον αξονικό της κλινικής, επικοινωνεί μόνο με την 10.51.1.183 στο δίκτυο, που ανήκει στο Synology. Πέραν αυτού, απαντάει μόνο σε multicast μηνύματα.
2. Αντίστροφα, ο server μας (10.51.1.183), δέχεται πακέτα μόνο μέσω της dicom πόρτας 39442 από τον αξονικό (10.51.1.220).
3. Ο server (10.51.1.183), εξυπηρετεί την συσκευή με IP 10.51.1.30 μόνο μέσω της 15393 και της 60616.
4. Ο server (10.51.1.183), εξυπηρετεί τις υπόλοιπες συσκευές του δικτύου μέσω των 14865 και 46151.
5. Τέλος, παρατηρούνται πολλά πακέτα discovery μεταξύ των συσκευών του δικτύου, με χρήση κυρίως της UDP πόρτας 8791.

4.3.1 Σύνθεση Κανόνων Καθημερινής Κίνησης

Αυτές οι επικοινωνίες αποτελούν την βασική μορφή κίνησης που παρατηρείται στο intranet της κλινικής. Είναι εύλογο λοιπόν, πάνω σε αυτά τα δεδομένα, να επιτρέπουμε και να αποτρέπουμε παραπάνω ενέργειες. Προφανώς, υπάρχουν και αρκετά multicast μηνύματα που αφορούν εκτυπωτές και άλλες βασικές διαδικασίες, οπότε πρέπει να είμαστε προσεκτικοί ως προς το τι κόβουμε, προκειμένου να διατηρηθεί η λειτουργικότητα του οργανισμού. Συμπερασματικά, δημιουργούνται οι κανόνες που παρουσιάζονται στον παρακάτω πίνακα:

sid : 3000001	drop tcp any any -> 10.51.1.220 any (msg:"Illegal communication attempted at 10.51.1.220"; sid : 3000001;)
sid : 3000002	pass tcp 10.51.1.183 39442 -> 10.51.1.220 any (sid : 3000002;)
sid : 3000003	drop tcp any any -> 10.51.1.183 any (msg:"Illegal communication attempted at 10.51.1.183"; sid 3000003;)
sid : 3000004	pass tcp 10.51.1.220 any -> 10.51.1.183 39442 (sid : 3000004;)
sid : 3000005	pass tcp 10.51.1.30 any -> 10.51.1.183 [15393, 60616] (sid : 3000005;)
sid : 3000006	pass tcp $HOME_NET any -> 10.51.183 [14865, 46151] (sid : 3000006;)

sid : 3000007	pass udp $HOME_NET any -> $HOME_NET 8791 (sid : 3000007;)

Πίνακας 4.3.1

Διαχωρίζουμε τους κανόνες της καθημερινής κίνησης από αυτούς της κακόβουλης, με μία διαφορά στο αναγνωριστικό τους. Για τους κανόνες της κακόβουλης κίνησης, χρησιμοποιούμε sid που ξεκινάει από **δύο εκατομμύρια και ένα**, ενώ για αυτούς της καθημερινής, από **τρία εκατομμύρια και ένα.** Ο διαχωρισμός αυτός γίνεται, ώστε να μας είναι πιο εύκολο να αναλύσουμε την κίνηση σε περίπτωση περιστατικού. Έχοντας αναφέρει και αυτό, ας δούμε αναλυτικά τον ρόλο του κάθε κανόνα.

4.3.2 Επεξήγηση Κανόνων Καθημερινής Κίνησης

Είναι σημαντικό να σημειώσουμε ότι στην παρούσα φάση, εστιάζουμε στην προστασία του αξονικού και του server μας, καθώς αυτά είναι τα δύο μηχανήματα που φέρουν την ευαίσθητη πληροφορία. Για τον λόγο αυτό, σκεφτόμαστε πως για αρχή δεν θα θέλαμε **καμία συσκευή**, χωρίς την έγκρισή μας, **να έχει πρόσβαση σε αυτά τα μηχανήματα**. Έτσι, θα ξεκινήσουμε από το μηδέν, και θα χτίσουμε εξαιρέσεις στην συνέχεια, για το πώς μπορεί να αποκτηθεί πρόσβαση σε αυτές. Αυτό μπορεί να αποτελεί μια ελαφρώς πιο αργή διαδικασία, ωστόσο προσφέρει γενικότερα μεγαλύτερη ασφάλεια. Οι κανόνες με sid **3000001** και **3000003** πραγματοποιούν ακριβώς αυτήν την λειτουργία, αποκόπτουν δηλαδή οποιαδήποτε επικοινωνία προς τον αξονικό και τον server.

Όπως δηλώσαμε στις πέντε παρατηρήσεις που παρουσιάσαμε παραπάνω, η μόνη συσκευή που έρχεται σε άμεση επαφή με τον αξονικό είναι ο server. Το πρωτόκολλο που χρησιμοποιείται για την μεταξύ τους επικοινωνία είναι το **dicom** και η πόρτα **39442** από πλευράς του server. Για αυτό, δημιουργούμε δύο κανόνες που επιτρέπουν αυτήν την επικοινωνία, τόσο όταν ο server λειτουργεί ως πομπός (sid : **3000002**), αλλά και όταν λειτουργεί ως παραλήπτης (sid : **3000004**).

Αφού λοιπόν ολοκληρώσαμε με τις επικοινωνίες του αξονικού, προχωράμε στις επικοινωνίες του server. Ο κανόνας sid : **3000005,** επιτρέπει στην συσκευή 10.51.1.30 να επικοινωνεί με τον server μέσω των θυρών 15393 και 60616, που αποτελούν **πόρτες διαχείρισης** κιόλας της εφαρμογής. Αυτό δηλώνει επίσης, πως η συγκεκριμένη IP χρησιμοποιείται από τον διαχειριστή του συστήματος (**admin**). Στην συνέχεια ο sid : **3000006,** επιτρέπει σε όλες τις IP του intranet, να επικοινωνούν με την εφαρμογή μέσω πρωτοκόλλου HTTP στις πόρτες 14865 και 46151. Τέλος, προκειμένου να αποφύγουμε την υποβίβαση της λειτουργίας του οργανισμού, δημιουργούμε τον κανόνα με sid : **3000007**. Αυτός επιτρέπει την εύρεση των συσκευών μεταξύ τους με χρήση πρωτοκόλλου UDP, στην πόρτα 8791.

4.4 Κανόνες γενικής φύσεως

Στην ενότητα 2.2.2, αναφέραμε κάποιες περιπτώσεις στις οποίες εκ φύσεως παρουσιάζονται θέματα ασφαλείας στα λογισμικά των Windows 10 που κάνει χρήση ο οργανισμός. Για να αντιμετωπίσουμε αυτό το κενό ασφαλείας, βρήκαμε τέσσερις κανόνες των οποίων ο δημιουργός αποτελεί η κοινότητα του Snort. Αναλυτικά, προσθέσαμε στο σύστημά μας τους εξής κανόνες:

Print Spooler Vulnerability	CVE 2022-29104	sid:59730, rev:1
Print Spooler Vulnerability	CVE 2021-34527	sid:57877, rev:2
WebDAV mini redirector driver Vulnerability	CVE 2016-0051	sid:37587, rev:2
Windows Error Reporting Service Vulnerability	CVE 2023-36874	sid:62035, rev:1

Πίνακας 4.4.1

Στην πρώτη στήλη, δίνουμε αναφορά για την αδυναμία από την οποία προστατεύει ο συγκεκριμένος κανόνας, καθώς παραδίδουμε και το αντίστοιχο CVE στην στήλη δύο. Το μοναδικό χαρακτηριστικό που εμφανίζεται στην στήλη τρία, αναφέρεται στον κανόνα της κοινότητας. Με μία απλή αναζήτηση στο διαδίκτυο, είναι εύκολο να βρούμε παραπάνω λεπτομέρειες για τον καθένα. Είναι σημαντικό να πούμε πως όλοι οι κανόνες εστιάζουν σε συγκεκριμένα bytes των πακέτων που εισέρχονται. Χρήση παρόμοιας λογικής έχουμε κάνει και κατά την σύνθεση των δικών μας κανόνων.

5

Μελλοντική Εργασία

Συνοψίζοντας το έργο μας, έχουμε κάνει μια αρκετά δυναμική πρώτη γραμμή άμυνας. Αυτή μας προστατεύει τόσο ενάντια σε ζωντανές επιθέσεις, όσο και σε δυνητικά νέες. Έτσι, δεν μας μένει παρά να εμβαθύνουμε στο να κατανοήσουμε παραπάνω σε αυτό που αποσκοπεί ο κακόβουλος χρήστης, κατά την περίοδο των επιθέσεών του. Μια βαθύτερη ανάλυση των κινήσεών του, θα μας βοηθήσει στο να εστιάσουμε με περισσότερη λεπτομέρεια στα σημεία που χρήζουν προστασίας. Ταυτόχρονα, θα πετύχουμε ένα πιο ευέλικτο δίκτυο για το εσωτερικό του οργανισμού. Η ευελιξία του δικτύου είναι σημαντική, καθώς όσο πιο γενικοί είναι οι κανόνες, τόσο πιο εύκολα μπορούν να βλάψουν και την λειτουργικότητά μας.

Οπότε σε επόμενο βήμα, θέλουμε ιδανικά να αναλύσουμε συγκεκριμένα τμήματα των πακέτων της κακόβουλης κίνησης, να δούμε τι έχει τροποποιήσει σε αυτά ο επιτιθέμενος, και τι κερδίζει – αν κερδίζει – από αυτές τις απόπειρες. Επίσης, θέλουμε να κοιτάξουμε στα TCP flags και να δούμε, αν με κάποιο τρόπο, διαφορετικά TCP statements απειλούν άμεσα την ακεραιότητά μας.

Ένα άλλο σημείο που είχε αρκετό ενδιαφέρον, είναι η χρήση τεχνικών IP tunneling κατά τις οποίες ο server μας δέχεται ICMP πακέτα μεγάλης πληροφορίας. Θέλουμε να εντρυφήσουμε σε αυτό, και να δούμε αν και πως διαχειρίζεται το δίκτυό μας αυτές τις καταστάσεις, και αν όντως ολοκληρώνεται κάποια επικοινωνία όπως την έχει προγραμματίσει ο επιτιθέμενος.

Τέλος, μας ενδιαφέρει να κοιτάξουμε και τις τεχνικές File Inclusion που έχουν διαδραματιστεί. Αυτό που μας νοιάζει περισσότερο, είναι να επιβεβαιώσουμε αν έχουν αποκτηθεί αρχεία και ποια είναι αυτά. Μας ενδιαφέρει η πληροφορία που έχουν, το πως αυτή μπορεί να χρησιμοποιηθεί, καθώς και αν είναι κρυπτογραφημένη ή όχι. Όλα αυτά αποτελούν σημεία καμπής, τα οποία μπορούν να παίξουν καθοριστικό ρόλο στη διασφάλιση του ιατρικού απορρήτου. Τέλος, πρέπει να αναζητήσουμε, αν έχει αποκτηθεί τελικά κάποια ευαίσθητη

πληροφορία που έχει διαφύγει από την αρχική μας ανάλυση. Σε πρώτη φάση δεν φαίνεται να είναι αυτό το ενδεχόμενο, ωστόσο δεν γνωρίζουμε αν, και πόσα περιστατικά έχουν λάβει μέρος στο παρελθόν.

6

Συμπεράσματα

Συμπερασματικά, παρατηρούμε ότι ακόμα και οργανισμοί που έχουν και διαχειρίζονται δεδομένα υψίστης σημασίας, έχουν πολλές φορές άγνοια των κινδύνων που περικυκλώνουν την κάθε τεχνολογία. Είναι πολλές οι περιπτώσεις που δεν υπάρχει η κατάλληλη εκπαίδευση, ενώ πολλές φορές η ίδια η τεχνική κατεύθυνση είναι απούσα. Καταλαβαίνουμε λοιπόν, πως είναι πολύ σημαντικό κάθε φορά που προστίθεται μια καινούργια τεχνολογία σε έναν οργανισμό, να ενημερωνόμαστε για τα πλεονεκτήματα και μειονεκτήματά της, καθώς και να αναζητούμε τους κινδύνους που υποβόσκουν.

Αυτό προσπαθεί και η συγκεκριμένη εργασία να καλύψει, αλλά και να αποδείξει. Με αυτό το σκεπτικό σαν κίνητρο και με την παρούσα ευκαιρία που μας δόθηκε, καταφέραμε να φέρουμε εις πέρας τον στόχο μας. Είδαμε πολλές περιπτώσεις επιθέσεων σε ζωντανό χρόνο και δημιουργήσαμε κανόνες τόσο για αυτές, όσο και κανόνες που εστιάζουν στο να παραμείνει το σύστημα λειτουργικό. Συμπεράναμε επίσης, πως η ανάλυση και η προετοιμασία είναι αυτές που χτίζουν το αποτέλεσμα, και αποτελούν τεχνικές που θα μας βοηθήσουν στην ενδυνάμωση του συστήματος σε μελλοντικό στάδιο.

Ολοκληρώνοντας, αξίζει να σημειώσουμε πως η συμβολή της κάθε κοινότητας είναι πάντα σημαντική. Ενδεικτικά, στην συγκεκριμένη περίσταση υπήρχαν κανόνες του Snort που χρησιμοποιήσαμε και βρήκαμε από την κοινότητά του, τους οποίους σε άλλη περίπτωση θα έπρεπε να αφιερώσουμε χρόνο στην ανάλυση και δημιουργία τους.

Βιβλιογραφία

https://en.wikipedia.org/wiki/ICMP_tunnel , ICMP tunneling basics

https://excellium-services.com/2022/09/28/how-does-icmp-tunneling-work-how-can-it-be-used-malicious-purposes/ , ICMP tunneling for malicious purposes

http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html , manual for Snort rule generation

https://www.wireshark.org/docs/wsug_html_chunked/ChapterWork.html , manual for working with Wireshark filters

https://www.tracewrangler.com/documentation/TraceWrangler.html , documentation for tracewrangler anonymization tool

https://www.cvedetails.com/vulnerability-search.php?f=1&vendor=Microsoft%2C+&product=Windows+10%2C+&cweid=&cvssscoremin=&cvssscoremax=&hasexp=1&publishdatestart=&publishdateend=&updatedatestart=&updatedateend=&cisaaddstart=&cisaaddend=&cisaduestart=&cisadueend=&opt_av%5B%5D=Local&opt_ac%5B%5D=Low&opt_pr%5B%5D=None&opt_pr%5B%5D=Low&opt_c%5B%5D=High&opt_i%5B%5D=High&opt_a%5B%5D=High&page=1 , CVE list for Windows 10 exploits

https://www.netresec.com/docs/NetworkMiner_Manual.pdf , NetworkMiner manual

https://www.sumologic.com/glossary/file-inclusion/#:~:text=File%20inclusion%20attack%20types,-There%20are%20two&text=When%20website%20or%20web%20application,sensitive%20files%20in%20other%20directories.

Παράρτημα Ι - Scripts για δοκιμή και εφαρμογή κανόνων Snort

Στο παράρτημα αυτό παρατίθενται τα scripts για την δοκιμή και την εφαρμογή των κανόνων που έχουμε δημιουργήσει. Αφού λοιπόν έχουμε δημιουργήσει τους κανόνες μας, τους δοκιμάζουμε σε πρώτη μοίρα στα δικά μας δεδομένα, ώστε να δούμε αν λειτουργούν ορθά. Αν περάσουμε το συγκεκριμένο στάδιο με επιτυχία, το Snort εφαρμόζεται σε live δίκτυα. Προκειμένου να το πετύχουμε αυτό, τρέχουμε δύο διαφορετικά σενάρια για την κάθε περίπτωση στο UNIX περιβάλλον μας, με την χρήση των παρακάτω scripts.

1. Για την δοκιμασία στα δεδομένα μας:

sudo snort -c /etc/snort/snort.conf --enable-inline-test -i <eth0> -q -A console -r <file>.pcap

2. Για παρατήρηση και παρεμβολή σε πραγματικό χρόνο:

sudo snort -c /etc/snort/snort.conf -Q -A console -q -I <eth0>:<eth1> -l <log_file>

Όπου <eth0> και <eth1>, συμπληρώνουμε την ονομασία από τους προσαρμογείς δικτύου του συστήματός μας. Αντίστοιχα, όπου <file>, συμπληρώνουμε το όνομα του αρχείου της κίνησης που θέλουμε να δοκιμάσουμε με κατάληξη pcap. Τέλος, όπου <log_file>, συμπληρώνουμε με το όνομα του αρχείου που θέλουμε να αποθηκευτεί το αρχείο καταγραφών μας αν επιλέξουμε με την παράμετρο -l.