ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ

ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΔΙΚΤΥΩΝ

Επιβλέπων Καθηγητής: Τριανταφύλλου Βασίλειος

Φοιτήτρια: Στυλιανή Μποντίκα ΑΜ: 152201760

ΠΑΤΡΑ, ΙΟΥΝΙΟΣ 2021

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Τις τελευταίες δεκαετίες, η εισαγωγή του διαδικτύου σε κάθε άξονα της επικοινωνίας και τομέα της βιομηχανίας είναι γεγονός. Στις πληροφορίες που διαχειρίζονται τα σύγχρονα υπολογιστικά συστήματα ανήκουν πλέον πολλών ειδών ευαίσθητα δεδομένα. Κάποια από αυτά αποτελούν προσωπικά δεδομένα, όπως κωδικοί και επικοινωνίες φυσικών και νομικών προσώπων και εταιριών, πληροφορίες για πατενταρισμένα προϊόντα κάθε τύπου αλλά και πληροφορίες απαραίτητες για τη διασφάλιση της ορθής λειτουργίας συστημάτων βλάβη στα οποία μπορεί να προκαλέσει καταστροφικές επιπτώσεις (τραπεζικά, αεροπορικά, νοσοκομειακά κ.α. συστήματα).

Κατά τη διάρκεια αυτής της μετάβασης διαχείρισης και αποθήκευσης ευαίσθητων δεδομένων από αναλογικό σε ψηφιακό τρόπο αναπτύχθηκαν και τακτικές υποκλοπής, μεταβολής και κακόβουλης επαναχρησιμοποίησης αυτών. Τέτοιες προσπάθειες ήταν εξαιρετικά επίφοβες και επιτυχής στο παρελθόν. Αυτό οφείλεται στο γεγονός ότι η τεχνολογία πληροφοριών αποτελεί ένα περίπλοκο επιστημονικό πεδίο, αποτελούμενο κάθε στιγμή ταυτόχρονα από τεχνολογίες του παρελθόντος και μια συνεχή αύξηση σε τεχνολογίες νέων συστημάτων, δικτύων, λογισμικού και πρωτοκόλλων. Παράλληλα, η χρήση των παραπάνω εργαλείων πρέπει να είναι επαρκής στην αντιμετώπιση της μεγάλης ποικιλίας των γνωστών αλλά και αγνώστων τεχνικών αντίστοιχων επιθέσεων που θα προκύψουν στο μέλλον, πριν αυτές αλλοιώσουν ή υποκλέψουν τους επίμαχους πόρους.

Συνεπώς, η διασφάλιση της μαζικής ανταλλαγής πληροφοριών στο σύγχρονο κόσμο κρίθηκε τόσο απαραίτητη όσο και σύνθετη και η ύπαρξη συστημάτων που αποσκοπούν στην επίτευξη αυτού του σκοπού τόσο επιτακτική όσο και ένας συνεχής αγώνας δρόμου. Υπάρχουν δύο στάδια που διαχωρίζουν τις τακτικές αντιμετώπισης τέτοιων επιθέσεων, ενώ κάθε ένα από

αυτά υλοποιείται μέσω αντίστοιχων συστημάτων και εργαλείων λογισμικού. Αυτά είναι η ανίχνευση εισβολών (intrusion detection) και η πρόληψη εισβολών (intrusion prevention) σε ένα δίκτυο.

Όπως προκύπτει από τα παραπάνω, τα συστήματα ανίχνευσης ή πρόληψης εισβολών (IDS/IPS) προσφέρουν πολλαπλά πλεονεκτήματα ως προς τη διασφάλιση των δικτυακών επικοινωνιών αλλά έχουν και πολλούς περιορισμούς. Συγκεκριμένα, η αποτελεσματικότητα τους είναι ανάλογη του τρόπου εφαρμογής τους σε ένα δίκτυο, του τρόπου εγκατάστασής τους, την δυνατότητα χρήσης τους από τους διαχειριστές του δικτύου κ.α..

Κεφάλαιο 1:

Ακεραιότητα και Ασφάλεια Δικτύων

1.1 Αρχιτεκτονική Δικτύων

Ο παγκόσμια ραγδαίος ρυθμός ανάπτυξης υπολογιστικών δικτύων για την ικανοποίηση των αναγκών εταιριών, οργανισμών, κρατικών και ιδιωτικών υπηρεσιών, πανεπιστημίων και ατόμων είναι γεγονός εδώ και αρκετά χρόνια και έχει δώσει το έναυσμα για την συνέχιση του συγκεκριμένου μοτίβου στο μέλλον. Αποτέλεσμα αυτής της ανάπτυξης είναι η ανάγκη μίας καθορισμένης αρχιτεκτονικά λύσης για την ασφάλεια και την ακεραιότητα δικτύων. Κατά την προσπάθεια εύρεσης μιας τέτοιας λύσης, τα κριτήρια είναι η ευκολία υλοποίησης και ανάπτυξης, η δυνατότητα αντιγραφής και κάλυψης πιθανών δικτυακών επεκτάσεων και η ευκινησία και αξιοπιστία των συστατικών που την αποτελούν.

Πλέον, μετά από χρόνια δοκιμών και σφαλμάτων, υπάρχουν αρχιτεκτονικές και τρόποι επίτευξης της ακεραιότητας και ασφάλειας δικτύων που έχουν δοκιμαστεί αρκετά και θεωρούνται κοινώς αποδεκτοί και άλλοι που λόγω της εξέλιξης των απειλών είναι κατά γενική ομολογία ανεπαρκείς ως προς αυτήν.

Η έννοια της αρχιτεκτονικής ασφάλειας και ακεραιότητας δικτύων τελικά εκφράζει ένα πολυσύνθετο τμήμα των δικτύων με συστατικά διάφορες πολιτικές και κανόνες ασφαλείας, ενέργειες, πρωτόκολλα αλλά και εξοπλισμό (Υλικό & Λογισμικό). Το πλαίσιο της ασφάλειας δικτύων περιλαμβάνει από μόνο του πληθώρα όρων, που καθένας από αυτούς αφορά δικούς του τρόπους υλοποίησης (και συχνά δικούς του κανόνες και πολιτικές ασφαλείας, ενέργειες, πρωτόκολλα και εξοπλισμό για την εφαρμογή του). Οι παρακάτω όροι είναι οι συχνότερα συσχετιζόμενοι με την ασφάλεια και ακεραιότητα δικτύων.

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Διαθεσιμότητα (Availability)

Πριν όμως εμβαθύνουμε σε αυτή την αρχιτεκτονική και τις έννοιες που την αποτελούν, πρέπει να κατανοήσουμε τα συστατικά των σύγχρονων δικτύων. Τα σημερινά δίκτυα αποτελούνται από πολλά σημεία, κάθε ένα από τα οποία είναι εν δυνάμει στόχος επιθέσεων και χρειάζεται διαφορετικές μεθόδους ασφάλισης. Οι μέθοδοι ασφάλισης των σημείων ακολουθούν συγκεκριμένες ροές και χρησιμοποιούν τόσο συσκευές IDS/IPS όσο και άλλα εργαλεία και συσκευές. Συγκεκριμένα, τα κύρια σημεία των δικτύων (places in network ή PINs) είναι τα παρακάτω:

1.1.1 Κέντρο Πληροφορίας (Data Center - DC)

Το data center (DC) είναι το πιο καίριο κομμάτι ενός οργανισμού. Τα κέντρα δεδομένων περιέχουν τα πιο κρίσιμα στοιχεία πληροφοριών και πνευματικό κεφάλαιο ενός οργανισμού και ως εκ τούτου είναι ο πρωταρχικός στόχος όλων των στοχευμένων απειλών.

Τα κέντρα δεδομένων συνήθως περιέχουν εκατοντάδες ή χιλιάδες διακομιστές (servers) , κάτι που καθιστά τη δημιουργία και διαχείριση κατάλληλων κανόνων ασφαλείας για τον έλεγχο της πρόσβασης στο δίκτυο του DC πολύ σύνθετη, χρονοβόρα και μεγάλο φόρτο εργασίας στους διαχειριστές του δικτύου (network administrators). Παράλληλα, τα data centers περιλαμβάνουν συνήθως τις δικτυακές συσκευές πυρήνα (δρομολογητές και μεταγωγείς πυρήνα ή core router & core switches), χειριστές ασύρματου δικτύου (wireless controllers) και τους εικονικούς μεταγωγείς (virtual switches) των εποπτών (Hypervisors).

Ένα ρήγμα στην ασφάλεια του δικτύου του κέντρου πληροφορίας συνεπάγεται άμεσα πιθανή αδυναμία χρήσης του δικτύου, των διακομιστών και των υπηρεσιών που αυτό προσφέρει και συχνά επηρεάζει άμεσα το χρόνο ζωής των φυσικών και ψηφιακών διακομιστών του οργανισμού.

Τυπικές απειλές που στοχεύουν στα κέντρα δεδομένων είναι η εξαγωγή δεδομένων (data extraction), η διάδοση κακόβουλου λογισμικού (malware propagation), η μη εξουσιοδοτημένη πρόσβαση στο δίκτυο και έκθεση εφαρμογών (unauthorized network access), προσβολή botnet και κλοπή δεδομένων και πόρων από μολυσμένη συσκευή (botnet scrumping), απώλεια δεδομένων (data loss), κλιμάκωση προνομίων (privilege escalation) και αναγνώριση (reconnaissance).

1.1.2 Ιδιωτικά Δίκτυα (Campus Networks)

Τα ιδιωτικά δίκτυα, συχνά αποκαλούμενα «πανεπιστημιακά» λόγω της μορφής τους, περιέχουν μεγάλο αριθμό χρηστών, συμπεριλαμβανομένων υπαλλήλων, εργολάβων, επισκεπτών και συνεργατών του οργανισμού. Τα ιδιωτικά δίκτυα τέτοιου τύπου είναι εύκολοι στόχοι για ηλεκτρονικό ψάρεμα (phising), εκμεταλλεύσεις μέσω διαδικτύου (web-based exploits), μη εξουσιοδοτημένη πρόσβαση στο δίκτυο , διάδοση κακόβουλου λογισμικού και παραβιάσεις τύπου botnet. Βάση των πιο διαδεδομένων δικτυακών αρχιτεκτονικών τα campus δίκτυα επικοινωνούν με τους υπολοίπους πόρους του οργανισμού με τη χρήση μεταγωγών πρόσβασης (access switches) και ασύρματων σημείων πρόσβασης (wireless access points).

Παράλληλα, επειδή το επίπεδο χρηστών είναι το πιο επιρρεπές σε επιθέσεις για κάθε οργανισμό, αυτό αφορούν και οι περισσότεροι τρόποι διασφάλισης της εύρυθμης λειτουργίας και της προστασίας ενός δικτύου. Μία επίθεση στο επίπεδο χρηστών επηρεάζει διαφορετικούς πόρους του οργανισμού, ανάλογα με τη δικτυακή θέση (VLAN,subnet) και προσβάσεις του χρήστη (σε διακομιστές και λοιπούς πόρους του οργανισμού) στον οποίο ανήκει η μολυσμένη συσκευή. Συνήθως είναι λιγότερο κρίσιμη από επιθέσεις σε άλλα σημεία του δικτύου (places in network – PINs) και στοχεύει περισσότερο πόρους που αφορούν το χρήστη και λιγότερο πόρους που αφορούν ολόκληρο τον οργανισμό. Εξαίρεση στον κανόνα αυτό αφορούν τμήματα του οργανισμού που συμπεριλαμβάνουν χρήστες – διαχειριστές των διακομιστών αλλά και των δικτυακών συσκευών. Πρέπει να δοθεί μεγάλη έμφαση από τον οργανισμό για τη διασφάλιση και προστασία από επιθέσεις στις συσκευές των χρηστών – διαχειριστών καίριων πόρων του οργανισμού.

1.1.3 Δίκτυα Υποκαταστημάτων (Branch Networks)

Τα παρακλάδια του κεντρικού δικτύου του οργανισμού, συχνά αποκαλούμενα ως υποκαταστήματα λόγω της δικτυακής διάταξής τους, είναι συνήθως λιγότερο ασφαλή από τα PINs «πανεπιστημιακών» δικτύων και κέντρων δεδομένων επειδή ο δυνητικά μεγάλος αριθμός καταστημάτων καθιστά απαγορευτικό βάση κόστους να εφαρμοστούν όλες οι τεχνικές και υποδομές ασφαλείας που βρίσκονται στα υπόλοιπα PINs.

Επομένως, οι τοποθεσίες «υποκαταστημάτων» αποτελούν πρωταρχικούς στόχους για παραβιάσεις ασφαλείας. Είναι σημαντικό όμως ο οργανισμός του οποίου είναι τμήματα να βρει τη σωστή ισορροπία προνοώντας να συμπεριληφθούν σε αυτές οι ζωτικής σημασίας δυνατότητες ασφαλείας, διατηρώντας παράλληλα το κόστος σε προσιτό επίπεδο. Οι κυριότερες απειλές που δέχονται τα παρακλάδια του κεντρικού δικτύου συμπεριλαμβάνουν κακόβουλο λογισμικό τελικού σημείου (point-of-sale ή POS malware), εκμεταλλεύσεις ασύρματης υποδομής όπως ξενιστές-σημεία πρόσβασης(rogue access-points ή rogue APs), επιθέσεις τύπου μεσάζοντα (man-in-the-middle ή MitM attacks), μη εξουσιοδοτημένη / κακόβουλη δραστηριότητα πελάτη (unauthorized/malicious client activity) και εκμετάλλευση εμπιστοσύνης (exploitation of trust).

Επιθέσεις που στοχοποιούν τα PINs υποκαταστημάτων συχνότερα επηρεάζουν μόνο τους πόρους του συγκεκριμένου υποκαταστήματος του οργανισμού, ενώ σπανιότερα μεταφέρονται και σε άλλα σημεία αυτού.

1.1.4 Δικτυακό Άκρο (Network Edge)

Το δικτυακό άκρο είναι το κύριο σημείο εισόδου και εξόδου της κυκλοφορίας από και προς το Διαδίκτυο, και αυτό αποτελεί το λόγο που είναι το δικτυακό σημείο του οργανισμού υψηλότερου κινδύνου. Ταυτόχρονα, είναι το σημείο με την υψηλότερη σημασία για την ηλεκτρονική ανταλλαγή πληροφοριών και εμπόριο του οργανισμού.

Οι τυπικές απειλές που εμφανίζονται στο δικτυακό άκρο περιλαμβάνουν ευπάθειες διακομιστή ιστού (web server vulnerabilities), κατανεμημένες επιθέσεις άρνησης υπηρεσίας (distributed denial of service ή DDOS attacks), απώλεια δεδομένων και επιθέσεις τύπου μεσάζοντα. Το αποτέλεσμα επιθέσεων στο δικτυακό άκρο μπορεί να αποβεί εξίσου καταστροφικό με μία επιτυχημένη επίθεση στο σημείο του κέντρου πληροφορίας, ανάλογα με τη φύση του οργανισμού και της επίθεσης.

Ιδιαίτερη προσοχή χρειάζεται να δώσουν στην ασφάλεια του δικτυακού άκρου οργανισμοί ηλεκτρονικού εμπορίου, παροχής ηλεκτρονικών υπηρεσιών και οργανισμοί που η εύρυθμη λειτουργία τους καθιστά απαραίτητη τη συνεχή πρόσβαση στο Internet. Στην τελευταία κατηγορία συμπεριλαμβάνονται οργανισμοί οι υπάλληλοι των οποίων χρησιμοποιούν για λόγους εργασίας το δημόσιο σύννεφο (public cloud). Τέτοιες περιπτώσεις συχνά αφορούν το Microsoft Azure και άλλες υπηρεσίες email, τη διαδικτυακή φιλοξενία εταιρικών διακομιστών (enterprise server web hosting) σε κάποιον πάροχο cloud και οργανισμοί που είναι σε συνεχή επαφή με εξωτερικούς συνεργάτες ή πελάτες.

Επιθέσεις στο δικτυακό άκρο μπορεί να επηρεάσουν τον οργανισμό, καθυστερώντας ή κατακερματίζοντας την εμπορική λειτουργία του.

1.1.5 Ιδιωτικό Σύννεφο (Private Cloud)

Στο ιδιωτικό σύννεφο συνήθως «στεγάζονται» πόροι του οργανισμού που είναι απαιτητικοί σε αποθηκευτικό χώρο, που απαιτούν συχνές ενημερώσεις και που λόγω αρχιτεκτονικής ή σχεδιασμού δεν μπορούσαν ή δεν έπρεπε να συστεγαστούν με τους υπολοίπους πόρους του οργανισμού στο δίκτυο αυτού.

Η ασφάλεια στο ιδιωτικό σύννεφο συνήθως υπαγορεύεται σε συμφωνίες επιπέδου υπηρεσίας μεταξύ του οργανισμού και του παρόχου δικτύου του και απαιτεί ανεξάρτητους ελέγχους πιστοποίησης και αξιολόγησης κινδύνων.

Οι κύριες απειλές που στοχοποιούν το ιδιωτικό σύννεφο είναι ευπάθειες του διακομιστή ιστού, απώλεια πρόσβασης (loss of access), απώλεια δεδομένων, κακόβουλο λογισμικό και επιθέσεις τύπου μεσάζοντα.

Επιθέσεις στο ιδιωτικό σύννεφο επηρεάζουν τον οργανισμό με τρόπο που μπορεί να χάσει την δικτυακή πρόσβαση σε αυτό ή να επηρεαστεί η εμπιστευτικότητα και ακεραιότητα των δεδομένων του από και προς το συγκεκριμένο PIN.

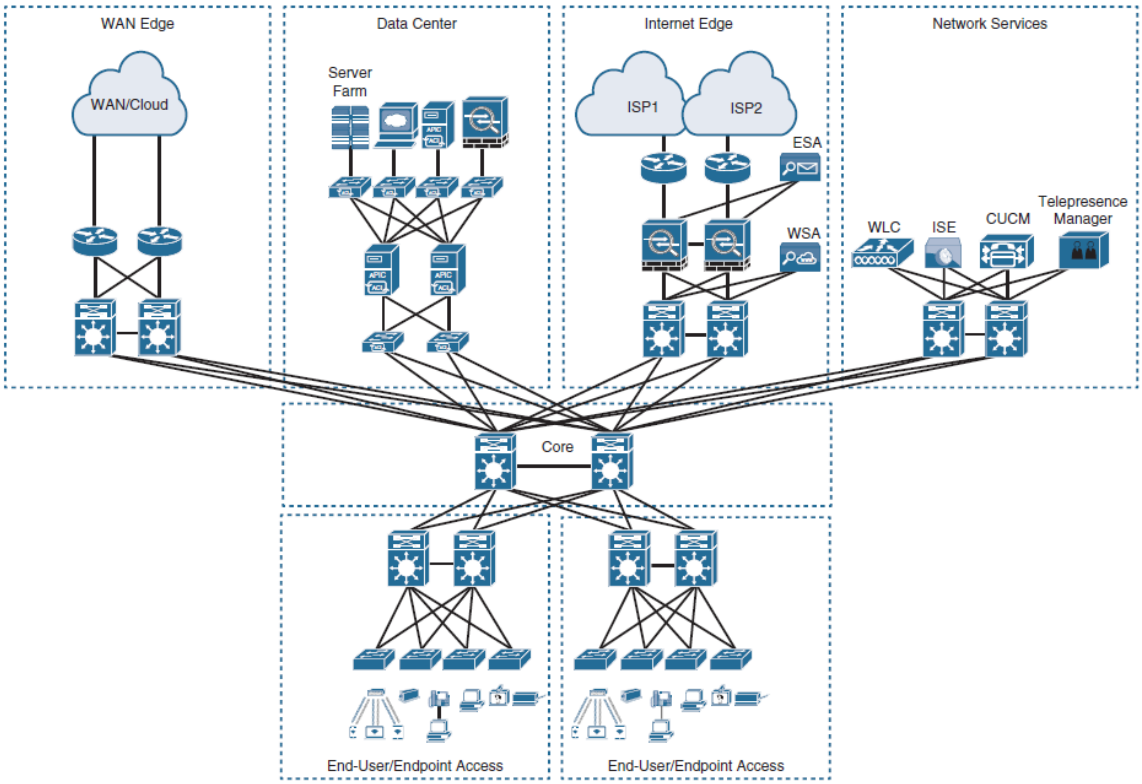
1.1.6 Δίκτυα Ευρείας Περιοχής (WAN)

Ένα δίκτυο ευρείας περιοχής (wide area network ή WAN) συνδέει τα υπόλοιπα δίκτυα υποκαταστημάτων ενός οργανισμού τόσο μεταξύ τους (αν υπάρχει ανάγκη) όσο και με το κεντρικό ιδιωτικό δίκτυο και με το κέντρο πληροφορίας. Σε έναν δικτυακά μεγάλο οργανισμό με εκατοντάδες δίκτυα υποκαταστημάτων, η διαχείριση της ασφάλειας στο δίκτυο ευρείας περιοχής είναι πολύ δύσκολη. Αυτό συμβαίνει διότι η φυσική υποδομή ανήκει στον πάροχο του δικτύου (Internet Service Provider ή ISP) και δεν έχουν πρόσβαση οι διαχειριστές δικτύου του οργανισμού.

Η ασφάλιση και ο έλεγχος των συγκεκριμένων υποδομών γίνονται από τον ISP και καλύπτονται από συμφωνίες επιπέδου υπηρεσίας (service level agreements ή SLAs). Τυπικές απειλές που εμφανίζονται στα WAN είναι η διάδοση κακόβουλου λογισμικού, η μη εξουσιοδοτημένη πρόσβαση στο δίκτυο, η υποκλοπή πακέτων (WAN sniffing) και οι επιθέσεις τύπου μεσάζοντα.

Επιθέσεις στο Δίκτυο Ευρείας περιοχής μπορούν να επηρεάσουν τις επικοινωνίες του οργανισμού από το κύριο ιδιωτικό δίκτυο (campus) και το κέντρο πληροφορίας (που συνήθως βρίσκονται στο ίδιο γεωγραφικό σημείο) προς οποιοδήποτε άλλο PIN, μειώνοντας την αποδοτικότητά τους ή επηρεάζοντας την εμπιστευτικότητα και ακεραιότητα των δεδομένων που μεταφέρονται από τις αντίστοιχες ζεύξεις (WAN links).

Εικόνα 1.1 Παράδειγμα σύγχρονης αρχιτεκτονικής δικτύου οργανισμού τριών επιπέδων (3-tier)



1.2 Ασφάλεια δικτύων

1.2.1 Αξιολόγηση Ασφαλείας

Πως μπορούμε όμως να κρίνουμε αν ένα δίκτυο είναι πραγματικά ασφαλές απέναντι στη συνεχή αύξηση αριθμού και πολυπλοκότητας πιθανών επιθέσεων του κυβερνοχώρου;

Για τη διευκόλυνση αξιολόγησης του επιπέδου ασφαλείας ενός δικτύου χρησιμοποιείται ως μέτρο ο βαθμός ικανότητας κάλυψης των παρακάτω τακτικών που εκφράζουν θεμιτές ενέργειες πριν, κατά τη διάρκεια αλλά και μετά την αντιμετώπιση κάποιας πιθανής επίθεσης στον οργανισμό.

- Κριτήρια ασφαλείας πριν την επίθεση αποτελούν τα παρακάτω:

  - **Δυνατότητα τακτικού ελέγχου ασφαλείας:**

    Η τακτική αυτή πραγματοποιείται με τη βοήθεια συσκευών και συστημάτων. Παρ ’ότι είναι σημαντική για την άμυνα του οργανισμού, συχνά δεν υλοποιείται επαρκώς καθώς επιφέρει υλικό και διαχειριστικό κόστος.

- **Δυνατότητα άμεσης επιβολής κανόνων και πολιτικών ασφαλείας:**

Η δυνατότητα αυτή είναι απαραίτητη για το δίκτυο ενός οργανισμού, καθώς σε περίπτωση επίθεσης η ζημιά συχνά είναι αντιστρόφως ανάλογη με εκθετικό τρόπο του χρόνου ασφάλισης του δικτύου. Υλοποιείται με τη χρήση συσκευών ασφαλείας και εναλλακτικών ζεύξεων μεγάλων ταχυτήτων.

- **Δυνατότητα αύξησης αυστηρότητας μέτρων ασφαλείας του δικτύου (Device Hardening/Policy Hardening) :**

Η υλοποίηση της συγκεκριμένη τεχνικής απαιτεί συνεχή ενημέρωση από τους διαχειριστές δικτύου, ασφαλείας και διακομιστών του οργανισμού για τις επερχόμενες μεθόδους επιθέσεων και των βέλτιστων τρόπων αντιμετώπισής τους. Επιφέρει διαχειριστικό κόστος στον οργανισμό.

- Κριτήρια ασφαλείας κατά τη διάρκεια μίας επίθεσης:

- **Δυνατότητα ανίχνευσης μιας επίθεσης (Detection):**

Πολλές από τις πιο επιτυχημένες επιθέσεις στα σύγχρονα δίκτυα καταφέρνουν να είναι δυσδιάκριτες από τα συστήματα ασφαλείας, καθώς δεν συνεπάγονται καθυστερήσεις ή αδυναμία χρήσης δικτυακών πόρων. Είναι

σημαντικό να υπάρχουν κατάλληλα συστήματα και τεχνογνωσία στον οργανισμό για την έγκαιρη ανίχνευσή τους.

- **Δυνατότητα περιορισμού μιας επίθεσης (Block):**

Μετά την ανίχνευση μίας επίθεσης στο δίκτυο του οργανισμού, είναι σημαντικό να περιοριστεί η δικτυακή περιοχή στην οποία έχει επιρροή. Η δυνατότητα περιορισμού είναι ανάλογη με την αρχιτεκτονική του δικτύου του οργανισμού και λαμβάνει πολύ σημαντικό ρόλο το επίπεδο και η μέθοδος τμηματοποίησης που δικτύου του οργανισμού, όπως θα αναλύσουμε παρακάτω.

- **Δυνατότητα άμυνας απέναντι σε μία επίθεση (Defend):**

Η δυνατότητα άμυνας του οργανισμού εκφράζει το πόσο εύκολα μπορεί να αποβληθεί το κακόβουλο λογισμικό (ή σπανιότερα υλικό) από το εταιρικό δίκτυο, ιδεατά χωρίς να επηρεάσει τη λειτουργία του. Αποτελεί τον βασικό σκοπό των διαχειριστών του οργανισμού κατά τη διάρκεια μίας επίθεσης.

- Κριτήρια ασφαλείας μετά την αντιμετώπιση της επίθεσης:

  - **Δυνατότητα εκτίμησης συμπεριφοράς της επίθεσης (Scope):**

Μετά την αντιμετώπιση της επίθεσης στον οργανισμό, είναι σημαντικό να γνωστοποιηθεί στους διαχειριστές του ο τρόπος υλοποίησης της επίθεσης καθώς και να προσδιορισθεί όσο το δυνατόν καλύτερα το σύνολο των συστημάτων και συσκευών που επηρέασε.

  - **Δυνατότητα περιορισμού αντίστοιχων μελλοντικών επιθέσεων (Contain):**

Από την παραπάνω πληροφορία προκύπτουν οι ενέργειες που πρέπει να πραγματοποιηθούν από τους διαχειριστές, ώστε να αντιμετωπιστεί η ευπάθεια που εκμεταλλεύτηκε η επίθεση. Η αντιμετώπιση ευπαθειών γίνεται ευκολότερη μέσω της συμμόρφωσης συστημάτων που θα αναλύσουμε παρακάτω και συχνά συνεπάγεται διαχειριστικό ή και υλικό κόστος (στην περίπτωση που επιπλέον εξοπλισμός ασφαλείας κρίνεται απαραίτητος).

- **Δυνατότητα επιδιόρθωσης των επιβλαβών αποτελεσμάτων της επίθεσης (Remediate):**

Το πιο σύνηθες μετά από την αντιμετώπιση μίας επίθεσης στον οργανισμό είναι η αυτόματη επαναφορά της εύρυθμης λειτουργίας του. Παρ' όλα αυτά, μία μεγάλη γκάμα επιθέσεων αφήνει επιβλαβή αποτελέσματα στον οργανισμό (αλλάζοντας τις ρυθμίσεις συσκευών και συστημάτων, επηρεάζοντας αρχεία, κ.α.).

Οι διαχειριστές των συστημάτων του οργανισμού, με τη βοήθεια εξειδικευμένου εξοπλισμού πρέπει να μπορούν να επιδιορθώσουν αυτές τις βλάβες, διότι επηρεάζουν την εύρυθμη λειτουργία του οργανισμού αλλά και συχνά δημιουργούν περαιτέρω ευπάθειες, καλλιεργώντας το έδαφος για μελλοντικές επιθέσεις. Κάποιες σύγχρονες, έξυπνες επιθέσεις επηρεάζουν τα συστήματα και το δίκτυο του οργανισμού με τρόπο που «ανοίγουν τρύπες» στο πλέγμα ασφαλείας του προς διευκόλυνση μελλοντικών επιθέσεων πολλαπλών τύπων.

Εικόνα 1.2 Κριτήρια ασφαλείας ανάλογα το στάδιο της επίθεσης

1.2.2 Τακτικές επίτευξης Ασφαλείας

Οι παρακάτω βέλτιστες τακτικές (best practices) χρησιμοποιούνται για να παρέχουν τη δυνατότητα στους διαχειριστές των συστημάτων, δικτύου και διακομιστών του οργανισμού να υλοποιήσουν τις ενέργειες που ενδείκνυνται για την επαρκή κάλυψη των παραπάνω κριτηρίων αξιολόγησης.

- **Διαχείριση (Management):**

  Η μέθοδος διαχείρισης συσκευών και συστημάτων είναι σημαντικός παράγοντας για την συνεπή ανάπτυξη πολιτικών ασφαλείας και λειτουργίας στον οργανισμό και τη διαχείριση αλλαγών ροής εργασίας των συστημάτων αυτού. Συστήματα κεντρικής διαχείρισης (central/unified management) μπορούν να χρησιμοποιηθούν για να διευκολύνουν αισθητά το συντονισμό των παραπάνω πολιτικών και διάφορων μεθόδων ειδοποίησης (alerting).

- **Πληροφόρηση και συγχρονισμός ασφαλείας (Security Intelligence):**

Η μέθοδος της πληροφόρησης και συγχρονισμού ασφαλείας εκφράζει την δυνατότητα επικοινωνίας των συστημάτων του οργανισμού με εξωτερικές βάσεις δεδομένων και ομάδες οργανισμών ασφαλείας, που αποσκοπούν στον εντοπισμό αναδυόμενου κακόβουλου λογισμικού και απειλών στον κυβερνοχώρο.

Με την επικοινωνία αυτή, επιτρέπεται σε μια δικτυακή υποδομή να εφαρμόζει πολιτικές δυναμικά, λαμβάνοντας υπ'όψην της το συνεχώς αυξανόμενο πλαίσιο των νέων απειλών. Μέσω της συγκεκριμένης μεθόδου γίνεται κατορθωτή η ακριβής και έγκαιρη προστασία ασφαλείας του δικτύου του οργανισμού.

- **Συμμόρφωση (Compliance):**

Πολύ συχνά οι αναβαθμίσεις σε οποιουδήποτε τύπου λογισμικό αποσκοπούν στην κάλυψη ή επιδιόρθωση προβλημάτων ασφαλείας που έχουν αναδυθεί. Συνεπώς, αποτελεί μεγάλο ρίσκο η χρήση διακομιστών και λοιπών συσκευών που δεν έχουν στη διάθεσή τους τις τελευταίες ενημερώσεις λογισμικού.

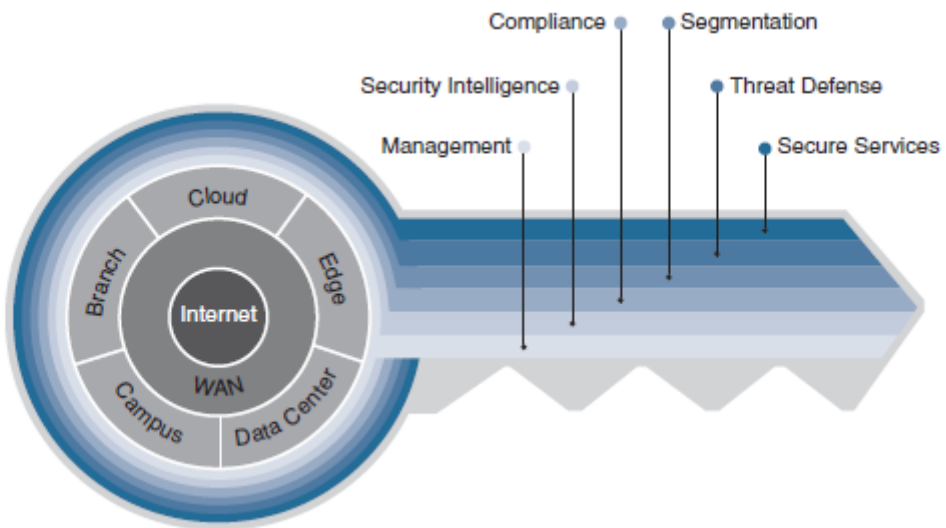
Το υλικό και λογισμικό που χρησιμοποιούνται για την βεβαίωση συμμόρφωσης προσφέρει μία μέθοδο επιβεβαίωσης και διατήρησης της επικαιροποίησης (updating) και επιδιόρθωσης (patching) των συστημάτων του οργανισμού.

- **Τμηματοποίηση (Segmentation):**

Η τμηματοποίηση περιλαμβάνει τον καθορισμό δικτυακών ορίων τόσο για τα δεδομένα όσο και για τους χρήστες. Η παραδοσιακή μη αυτόματη τμηματοποίηση χρησιμοποιεί έναν συνδυασμό διευθύνσεων δικτύου και VLAN για επιβολή πολιτικής.

Η προηγμένη τμηματοποίηση μειώνει τις προκλήσεις υλοποίησης με την αξιοποίηση της υποδομής με γνώμονα την ταυτότητα για την επιβολή πολιτικών με ένα αυτοματοποιημένο και επεκτάσιμο τρόπο (Security Group Tags ή SGTs, Dynamic Access Lists, Dynamic VLANs, κ.α.).

Εικόνα 1.3 Τεχνικές ασφάλισης των PIN του δικτύου του οργανισμού



1.3 Τύποι Δικτυακών Επιθέσεων

Με την εξέλιξη της τεχνολογίας αυξάνεται και ο αριθμός της ήδη πληθώρας εργαλείων και πόρων που έχουν ενσωματωθεί στην καθημερινότητα κάθε οργανισμού. Όμως, κάθε καινούρια εφαρμογή και τεχνολογία που εισάγεται στο δίκτυο του οργανισμού συνοδεύεται από πιθανούς κινδύνους και παρουσιάζει έναν εν δυνάμει στόχο επιθέσεων. Συνεπώς, οι πιθανές μορφές επιθέσεων που μπορεί να δεχθεί το δίκτυο ενός οργανισμού είναι ανάλογες του αριθμού των εργαλείων που έχει στη διάθεσή του και τον τρόπο χρήσης αυτών από το προσωπικό που τον αποτελεί.

Όπως αναφέραμε παραπάνω, κάθε σημείο του δικτύου του οργανισμού φέρει τα δικά του εργαλεία, τεχνικές και αρχιτεκτονική προστασίας του αλλά και τους δικούς του πιθανούς κινδύνους και ευπάθειες. Παρακάτω αναφέρονται συνοπτικά οι πιο διαδεδομένοι τύποι επιθέσεων, ο τρόπος λειτουργίας τους αλλά και τα αποτελέσματα που επιφέρουν στο δίκτυο του οργανισμού.

- **Κακόβουλο Λογισμικό (Malware):**

Ο όρος malware χρησιμοποιείται για την περιγραφή κακόβουλου λογισμικού, συμπεριλαμβανομένων λογισμικό κατασκοπείας συστημάτων (spyware), λογισμικό εξαγοράς

πληροφοριών (ransomware), ιών και σκουλικιών (worms). Το κακόβουλο λογισμικό παραβιάζει ένα δίκτυο μέσω μιας ευπάθειας, συνήθως όταν ένας χρήστης κάνει κλικ σε έναν επικίνδυνο σύνδεσμο ή ένα συνημμένο email που στη συνέχεια εγκαθιστά επικίνδυνο λογισμικό. Μόλις βρει πρόσβαση στο σύστημα, το κακόβουλο λογισμικό μπορεί να κάνει τα εξής:

- Να αποκλείσει την πρόσβαση σε βασικά στοιχεία της συσκευής (ransomware).
- Να εγκαταστήσει κακόβουλο λογισμικό ή πρόσθετο επιβλαβές λογισμικό.
- Να λάβει κρυφά πληροφορίες διαβιβάζοντας δεδομένα από τον σκληρό δίσκο (spyware).
- Να διασπάσει ορισμένα στοιχεία καθιστώντας το σύστημα μη λειτουργικό.

- **Ηλεκτρονικό Ψάρεμα (Phishing):**

Το ηλεκτρονικό ψάρεμα (phishing) είναι η πρακτική αποστολής δόλιων επικοινωνιών που φαίνεται να προέρχονται από αξιόπιστη πηγή, συνήθως μέσω email. Ο στόχος της επίθεσης είναι να κλέψει ευαίσθητα δεδομένα, όπως δεδομένα και κωδικούς πιστωτικών καρτών και στοιχεία σύνδεσης (credentials) σε συστήματα και ιστοσελίδες, ή να εγκαταστήσει κακόβουλο λογισμικό στο μηχάνημα του θύματος.

Το ηλεκτρονικό ψάρεμα είναι μια όλο και πιο κοινή απειλή στον κυβερνοχώρο. Οι προσπάθειες ηλεκτρονικού ψαρέματος που αποστέλλονται είναι πλαστές επικοινωνίες που φαίνεται να προέρχονται από κάποια αξιόπιστη πηγή, αλλά που μπορούν να θέσουν σε κίνδυνο όλους τους τύπους δεδομένων των χρηστών. Οι επιθέσεις αυτές μπορούν να διευκολύνουν την πρόσβαση στους διαδικτυακούς λογαριασμούς και τα προσωπικά δεδομένα των χρηστών, να λάβουν δικαιώματα για τροποποίηση και συμβιβασμό συνδεδεμένων συστημάτων (όπως τερματικά σημείων πώλησης και συστήματα επεξεργασίας παραγγελιών) και σε ορισμένες περιπτώσεις εισβάλλουν σε ολόκληρα δίκτυα υπολογιστών έως ότου παραδοθεί χρέωση λύτρων. Μερικές φορές οι επίδοξοι εισβολείς είναι ικανοποιημένοι με τη λήψη προσωπικών δεδομένων, όπως τα στοιχεία της πιστωτικής κάρτας για οικονομικό κέρδος.

Σε άλλες περιπτώσεις, τα μηνύματα ηλεκτρονικού "ψαρέματος" αποστέλλονται για τη συλλογή πληροφοριών σύνδεσης υπαλλήλων ή άλλων λεπτομερειών για χρήση σε άλλες κακόβουλες επιθέσεις εναντίον μερικών ατόμων ή ολόκληρου του οργανισμού. Το ηλεκτρονικό ψάρεμα (phishing) είναι ένας τύπος επίθεσης στον κυβερνοχώρο τον οποίο όλοι οι χρήστες του οργανισμού πρέπει να γνωρίζουν για να μπορούν να προστατευτούν επαρκώς και να διασφαλίσουν την ασφάλεια του ηλεκτρονικού ταχυδρομείου σε ολόκληρο τον οργανισμό.

- **Επιθέσεις τύπου διαμεσολαβητή:**

Οι επιθέσεις Man-in-the-middle (MitM), επίσης γνωστές ως επιθέσεις υποκλοπής, εμφανίζονται όταν οι εισβολείς εισάγονται σε μια συναλλαγή δύο μερών.

Μόλις οι εισβολείς διακόψουν την κίνηση, μπορούν να φιλτράρουν και να κλέψουν δεδομένα. Τα κοινά σημεία εισόδου για επιθέσεις MitM είναι τα παρακάτω:

- Σε μη ασφαλές δημόσιο ασύρματο δίκτυο Wi-Fi, οι εισβολείς μπορούν να τοποθετηθούν μεταξύ της συσκευής ενός επισκέπτη και του δικτύου. Με αυτό τον τρόπο, ο επισκέπτης χωρίς να το γνωρίζει διαβιβάζει όλες τις πληροφορίες μέσω της συσκευής του εισβολέα.

- Σε ενσύρματο δίκτυο, όταν ο επιτιθέμενος παριστάνει την προκαθορισμένη πύλη (default gateway) της συσκευής, ανακόπτοντας τα μηνύματα ARP (Address Resolution Protocol) που προορίζονται προς αυτήν και μεταβιβάζοντας τα αυτός στο υπόλοιπο δίκτυο. Οι δικτυακές συσκευές μπορούν να αμυνθούν στις επιθέσεις τύπου διαμεσολαβητή σε ενσύρματο δίκτυο με τη χρήση τεχνικών DHCP snooping, dynamic ARP inspection κ.α..

Οι πιο διαδεδομένες μέθοδοι υλοποίησης μιας επίθεσης τύπου διαμεσολαβητή είναι οι παρακάτω:

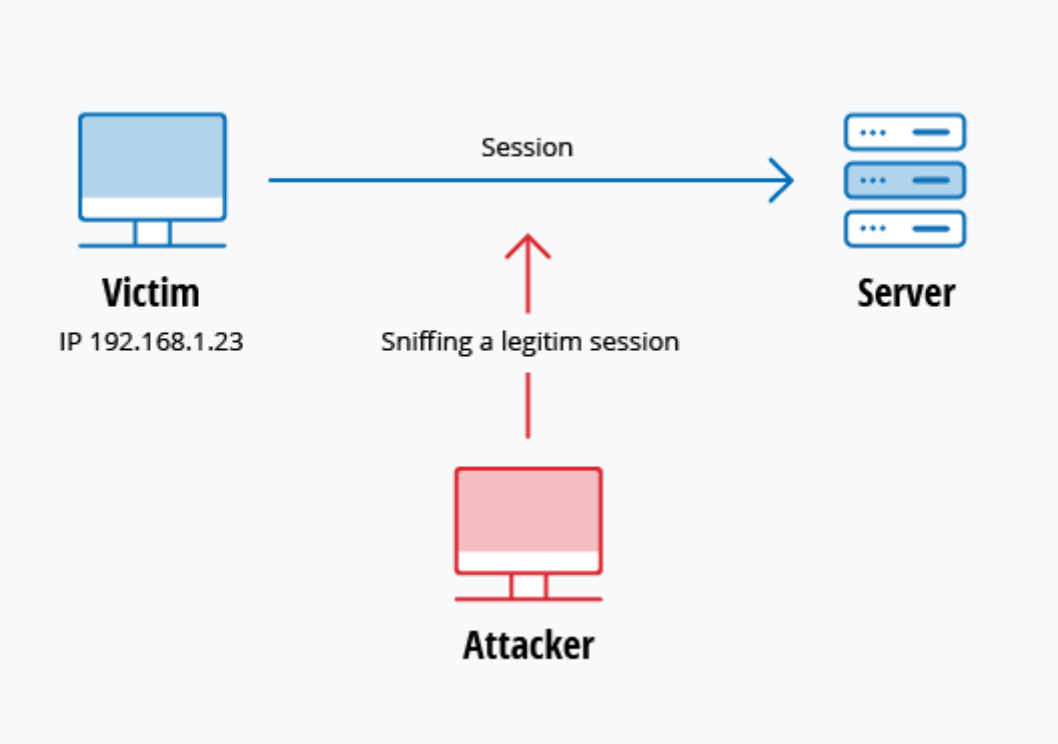
- Παραβίαση συνεδρίας (Session highjacking)

Σε αυτή την υλοποίηση επίθεσης τύπου MitM, ένας εισβολέας εισβάλλει σε μια περίοδο σύνδεσης μεταξύ ενός αξιόπιστου πελάτη και ενός διακομιστή δικτύου. Ο επιτιθέμενος υπολογιστής αντικαθιστά τη διεύθυνση IP του για τον αξιόπιστο πελάτη, ενώ ο διακομιστής συνεχίζει τη συνεδρία, πιστεύοντας ότι επικοινωνεί με τον πελάτη. Για παράδειγμα, η επίθεση μπορεί να ξεδιπλωθεί ως εξής:

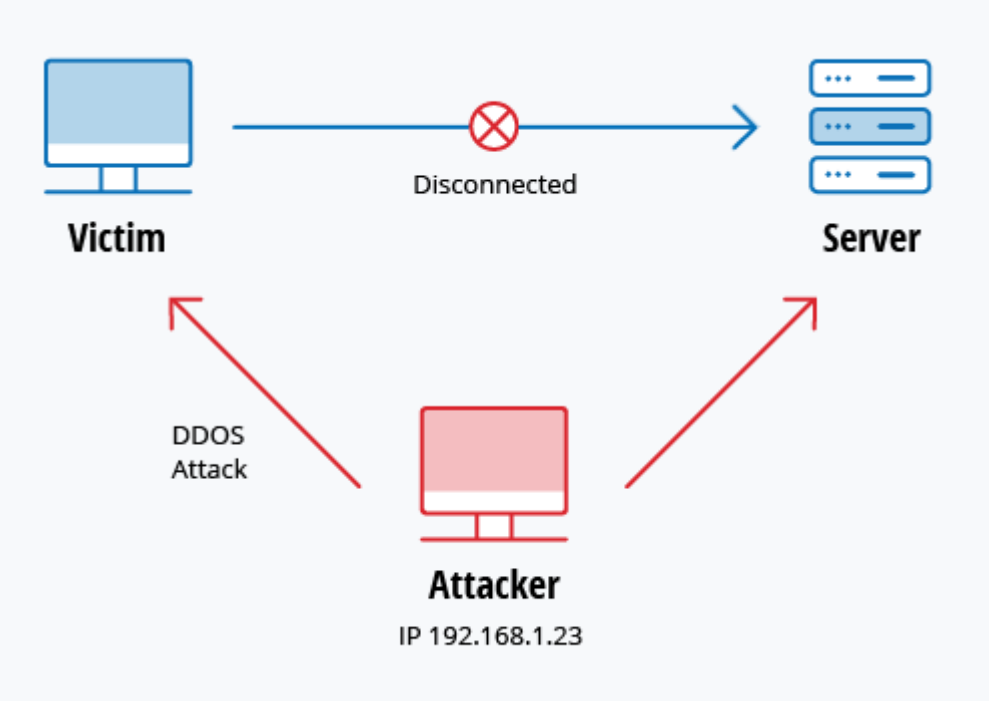
1. Ένας πελάτης συνδέεται με έναν διακομιστή.

2. Ο υπολογιστής του εισβολέα αποκτά τον έλεγχο του πελάτη.
3. Ο υπολογιστής του εισβολέα αποσυνδέει τον πελάτη από το διακομιστή.
4. Ο υπολογιστής του εισβολέα αντικαθιστά τη διεύθυνση IP του πελάτη με τη δική του διεύθυνση IP και πλαστογραφεί τους αριθμούς ακολουθίας του πελάτη.
5. Ο υπολογιστής του εισβολέα συνεχίζει το διάλογο με τον διακομιστή και ο διακομιστής πιστεύει ότι εξακολουθεί να επικοινωνεί με τον πελάτη.

Εικόνα 1.4 Επίθεση Παραβίασης Συνεδρίας 1/2



Εικόνα 1.4 Επίθεση Παραβίασης Συνεδρίας 2/2



- Πλαστογράφηση διεύθυνσης IP (IP spoofing)

Η πλαστογράφηση διεύθυνσης IP χρησιμοποιείται από έναν εισβολέα για να εξαπατήσει ένα σύστημα ότι επικοινωνεί με μια γνωστή, αξιόπιστη οντότητα πείθοντάς το έτσι να παρέχει στον εισβολέα πρόσβαση στο σύστημα. Ο εισβολέας στέλνει ένα πακέτο με τη διεύθυνση προέλευσης IP ενός γνωστού, αξιόπιστου κεντρικού υπολογιστή (υπολογιστή του οργανισμού) αντί της δικής του διεύθυνσης προέλευσης IP σε έναν κεντρικό υπολογιστή προορισμού. Ο κεντρικός υπολογιστής στόχος μπορεί να αποδεχτεί το πακέτο και να πραγματοποιήσει ενέργειες σε αυτό.

- Επίθεση επανάληψης

Μια επίθεση επανάληψης εμφανίζεται όταν ένας εισβολέας παρεμποδίζει και αποθηκεύει παλιά μηνύματα και στη συνέχεια προσπαθεί να τα στείλει αργότερα, πλαστοπροσωπώντας έναν από τους συμμετέχοντες. Αυτός ο τύπος επίθεσης μπορεί να αντιμετωπιστεί εύκολα με χρονικές σημάνσεις περιόδου λειτουργίας ή nonce (ένας τυχαίος αριθμός ή μια συμβολοσειρά που αλλάζει με την ώρα).

- Επίθεση υποκλοπής (eavesdropping attack)

Επιθέσεις υποκλοπής συμβαίνουν μέσω της παρακολούθησης της κυκλοφορίας του δικτύου. Παρακολουθώντας, ένας εισβολέας μπορεί να αποκτήσει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών και άλλες εμπιστευτικές πληροφορίες που μπορεί να στέλνει ένας χρήστης μέσω του δικτύου. Η υποκλοπή μπορεί να είναι παθητική ή ενεργή:

- Παθητική υποκλοπή: Ένας εισβολέας εντοπίζει τις πληροφορίες "ακούγοντας" τη μετάδοση μηνυμάτων στο δίκτυο.

- Ενεργή υποκλοπή: Ένας εισβολέας λαμβάνει ενεργά τις πληροφορίες μεταμφιεσμένος ως φιλική μονάδα και στέλνοντας πακέτα αίτησης

πληροφοριών (requests/queries) σε άλλα συστήματα του δικτύου του οργανισμού (πομπούς). Αυτό ονομάζεται ανίχνευση, σάρωση ή παραβίαση.

Ο εντοπισμός παθητικών επιθέσεων υποκλοπής είναι συχνά πιο σημαντικός από τον εντοπισμό ενεργών επιθέσεων, καθώς οι ενεργές επιθέσεις απαιτούν από τον εισβολέα να αποκτήσει γνώση των φιλικών μονάδων πραγματοποιώντας παθητική υποκλοπή.

Προς το παρόν, δεν υπάρχει μεμονωμένη τεχνολογία ή διαμόρφωση για την αποτροπή όλων των επιθέσεων MitM. Γενικά, η κρυπτογράφηση και τα ψηφιακά πιστοποιητικά παρέχουν μια αποτελεσματική προστασία έναντι επιθέσεων MitM, διασφαλίζοντας τόσο την εμπιστευτικότητα όσο και την ακεραιότητα των επικοινωνιών. Αλλά μια επίθεση του συγκεκριμένου τύπου μπορεί να εγχυθεί στη μέση των επικοινωνιών με τέτοιο τρόπο ώστε η κρυπτογράφηση να μην βοηθήσει.

- **Επίθεση άρνησης υπηρεσίας (Denial of Service ή DoS attack):**

Μία επίθεση άρνησης εξυπηρέτησης "πλημμυρίζει" συστήματα, διακομιστές ή δίκτυα με κίνηση προς εξάντληση πόρων και εύρους ζώνης. Ως αποτέλεσμα, τα συστήματα δεν μπορούν να εκπληρώσουν νόμιμα/αυθεντικά αιτήματα.

Οι εισβολείς μπορούν επίσης να χρησιμοποιήσουν πολλές παραβιασμένες συσκευές για να ξεκινήσουν αυτήν την επίθεση. Επίθεση με χρήση πολλαπλών πηγών για τη δημιουργία της κίνησης είναι γνωστές ως επιθέσεις κατανεμημένης διανομής άρνησης υπηρεσίας (DDoS).

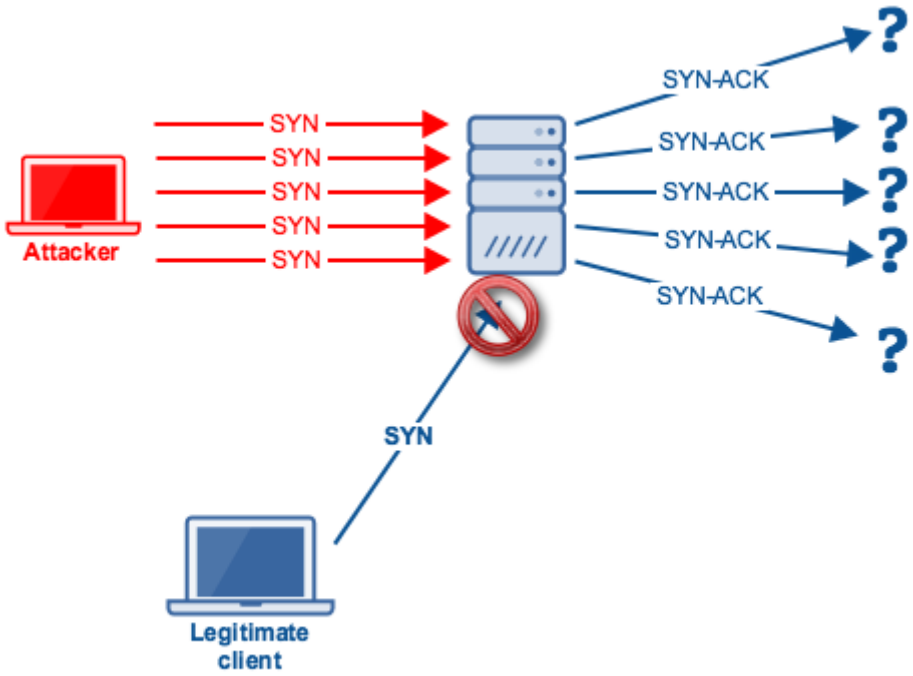
Τέτοιες επιθέσεις μπορεί να είναι σύντομες (π.χ. Ping of Death) ή να χρειάζονται περισσότερο χρόνο να αναπτυχθούν (π.χ. Slowloris). Σύμφωνα με έκθεση της Radware, το 33% των επιθέσεων DDoS διαρκεί περίπου μια ώρα. Το 60% διαρκεί λιγότερο από μια ολόκληρη μέρα. Τέλος, 15% διαρκούν έως και ένα μήνα.

Οι μέθοδοι υλοποίησης επιθέσεων τύπου DDoS είναι πολλοί, με πιο γνωστούς τους παρακάτω:

- Επίθεση πλημμύρας TCP SYN (TCP SYN flood attack)

Σε αυτήν την επίθεση, ένας εισβολέας εκμεταλλεύεται τη χρήση του χώρου αποθήκευσης κατά τη διάρκεια μιας χειραψίας προετοιμασίας περιόδου σύνδεσης Transmission Control Protocol (TCP). Η συσκευή του εισβολέα πλημμυρίζει τη μικρή ουρά του συστήματος στόχου με αιτήματα σύνδεσης, αλλά δεν αποκρίνεται όταν το σύστημα στόχος απαντά σε αυτά τα αιτήματα. Αυτό προκαλεί το χρονικό όριο λήξης αναμονής απόκρισης του συστήματος-στόχου, περιμένοντας την απόκριση από τη συσκευή του εισβολέα, γεγονός που κάνει το σύστημα να "καταρρέει" καθιστώντας το μη ανταποκρίσημο. Αυτός ο τύπος επίθεσης εκμεταλλεύεται το μηχανισμό τριπλής χειραψίας TCP, που αποσκοπεί στη δημιουργία αξιόπιστου καναλιού επικοινωνίας.

Εικόνα 1.5 Επίθεση τύπου πλημμύρας TCP SYN



- Επίθεση δακρύου (teardrop attack)

Αυτή η επίθεση προκαλεί τα πεδία αντιστάθμισης μήκους και κατακερματισμού σε διαδοχικά πακέτα πρωτοκόλλου TCP να αλληλεπικαλύπτονται στο σύστημα ή διακομιστή δέκτη της επίθεσης δακρύου. Το αμυνόμενο σύστημα προσπαθεί να ανακατασκευάσει πακέτα κατά τη διάρκεια της διαδικασίας, αλλά αποτυγχάνει. Στη συνέχεια συγχέεται και καταρρέει.

- Επίθεση τύπου Ping of Death

Σε αυτό τον τύπο επίθεσης χρησιμοποιούνται πακέτα IP για να κάνουν "ping" (χρησιμοποιώντας πρωτόκολλο ICMP) ένα σύστημα στόχου με μέγεθος πακέτου πάνω από το μέγιστο των 65.535 byte. Δεν επιτρέπονται πακέτα IP αυτού του μεγέθους, οπότε το αμυνόμενο σύστημα κατακερματίζει το πακέτο IP. Μόλις το σύστημα προορισμού επανασυναρμολογήσει το πακέτο, μπορεί να αντιμετωπίσει υπερχείλιση buffer και άλλα σφάλματα.

- Επίθεση με χρήση Botnet

Τα botnets είναι τα συστήματα (πολλές φορές χιλιάδες ή εκατομμύρια) που έχουν μολυνθεί από κακόβουλο λογισμικό υπό έλεγχο χάκερ προκειμένου να πραγματοποιήσουν επιθέσεις τύπου DDoS. Αυτά τα bots ή συστήματα "ζόμπι" χρησιμοποιούνται για τη διεξαγωγή επιθέσεων εναντίον των συστημάτων στόχου, συχνά κατακλύζοντας το εύρος ζώνης και τις δυνατότητες επεξεργασίας του συστήματος αυτού. Οι επιθέσεις DDoS με χρήση botnet είναι δύσκολο να εντοπιστούν επειδή οι μολυσμένες συσκευές συνήθως βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες.

- **Έγχυση βάσης δεδομένων SQL (SQL injection):**

Η έγχυση SQL (SQL Injection) χρησιμοποιείται στο πλαίσιο μιας επίθεσης σε εφαρμογές που αποθηκεύουν και διαχειρίζονται τα δεδομένα τους μέσω ενός Συστήματος Διαχείρισης Βάσης Δεδομένων. Χρησιμοποιώντας αυτή την τεχνική ο επιτιθέμενος εκμεταλλεύεται μια ευπάθεια της εφαρμογής και εισάγει κακόβουλο SQL κώδικα σε σημεία όπου η εφαρμογή περιμένει θεμιτά δεδομένα από τον χρήστη.

Μια τέτοια ευπάθεια προκύπτει στην περίπτωση που η εφαρμογή δεν διαθέτει έναν μηχανισμό σωστού φιλτραρίσματος των δεδομένων εισόδου του χρήστη. Λ.χ. δεν ψάχνει για τυχόν χαρακτήρες διαφυγής εμφωλευμένους μέσα στο αίτημα ενός χρήστη ή δεν υπάρχει αυστηρός έλεγχος των τύπων των δεδομένων που εισάγει ο χρήστης.

Οι επιθέσεις έγχυσης SQL επιτρέπουν σε έναν επιτιθέμενο να έχει πρόσβαση σε απόρρητα δεδομένα, να μπορεί να επεξεργαστεί διαβαθμισμένα δεδομένα, να διαγράψει δεδομένα, να γίνει διαχειριστής του εξυπηρετητή της βάσης δεδομένων αλλά και να αποκτήσει πρόσβαση σε υπολογιστικούς πόρους με προνόμια διαχειριστή.

- **Εκμετάλλευση ευπαθειών πρώτης ημέρας (Zero-day Exploit):**

Μία τέτοια επίθεση χτυπά μετά την ανακοίνωση μιας ευπάθειας δικτύου, αλλά πριν από την εφαρμογή μιας ενημέρωσης κώδικα ή μιας λύσης.

Οι επιτιθέμενοι στοχεύουν την ευπάθεια που αποκαλύφθηκε κατά τη διάρκεια αυτού του χρονικού διαστήματος. Η ανίχνευση απειλών ευπάθειας μηδενικής ημέρας απαιτεί συνεχή ενημέρωση των διακομιστών και συστημάτων.

- **Σήραγγα Συστήματος Ονοματοδοσίας Διαδικτύου (Domain Name Server tunneling ή DNS tunneling):**

Μία επίθεση τύπου σήραγγας συστήματος ονοματοδοσίας διαδικτύου χρησιμοποιεί το πρωτόκολλο DNS για την επικοινωνία διαφορετικού τύπου κίνησης (εκτός DNS) μέσω της θύρας 53 (UDP). Στέλνει HTTP και άλλη κίνηση πρωτοκόλλου μέσω DNS. Υπάρχουν διάφοροι, νόμιμοι λόγοι για τη χρήση του DNS tunneling, ωστόσο, υπάρχουν επίσης κακόβουλες χρήσεις για τη χρήση υπηρεσιών σήραγγας ψηφιακού ιδιωτικού δικτύου (Virtual Private Network ή VPN Tunneling).

Τέτοιου τύπου επιθέσεις μπορούν να χρησιμοποιηθούν για τη μεταμφίεση της εξερχόμενης κίνησης ως DNS, αποκρύπτοντας δεδομένα που συνήθως κοινοποιούνται μέσω σύνδεσης στο Διαδίκτυο. Για κακόβουλη χρήση, τα αιτήματα DNS υποβάλλονται σε επεξεργασία για την αποβολή δεδομένων από ένα παραβιασμένο σύστημα στην υποδομή του εισβολέα. Μπορεί επίσης να χρησιμοποιηθεί για εντολές και έλεγχο επιστροφών κλήσεων από την υποδομή του εισβολέα σε ένα παραβιασμένο σύστημα.

- **Επίθεση κωδικού πρόσβασης (Password Attack):**

Καθώς οι κωδικοί πρόσβασης είναι ο πιο συχνά χρησιμοποιούμενος μηχανισμός για τον έλεγχο ταυτότητας των χρηστών σε ένα σύστημα πληροφοριών, η απόκτηση κωδικών πρόσβασης είναι μια κοινή και αποτελεσματική προσέγγιση επίθεσης. Η ανίχνευση του κωδικού πρόσβασης ενός ατόμου μπορεί να επιτευχθεί ψηφιακά με «εισπνοή» (sniffing) της σύνδεσής του με το δίκτυο για την απόκτηση μη κρυπτογραφημένων κωδικών πρόσβασης, τη χρήση κοινωνικής μηχανικής (social engineering), την απόκτηση πρόσβασης σε μια βάση δεδομένων κωδικών πρόσβασης ή την "τυχαία" εικασία.

Η τελευταία προσέγγιση μπορεί να γίνει είτε με τυχαίο είτε με συστηματικό τρόπο:

- Εκτίμηση κωδικού πρόσβασης με τρόπο brute force, δηλαδή με χρήση της μεθόδου τυχαίας προσέγγισης μέσω πληθώρας δοκιμών διαφορετικών κωδικών πρόσβασης και ελπίζοντας σε επιτυχία. Κάποια λογική μπορεί να εφαρμοστεί στην μέθοδο brute force δοκιμάζοντας κωδικούς πρόσβασης που σχετίζονται με το όνομα του ατόμου, τον τίτλο εργασίας, τα χόμπι ή παρόμοια αντικείμενα.

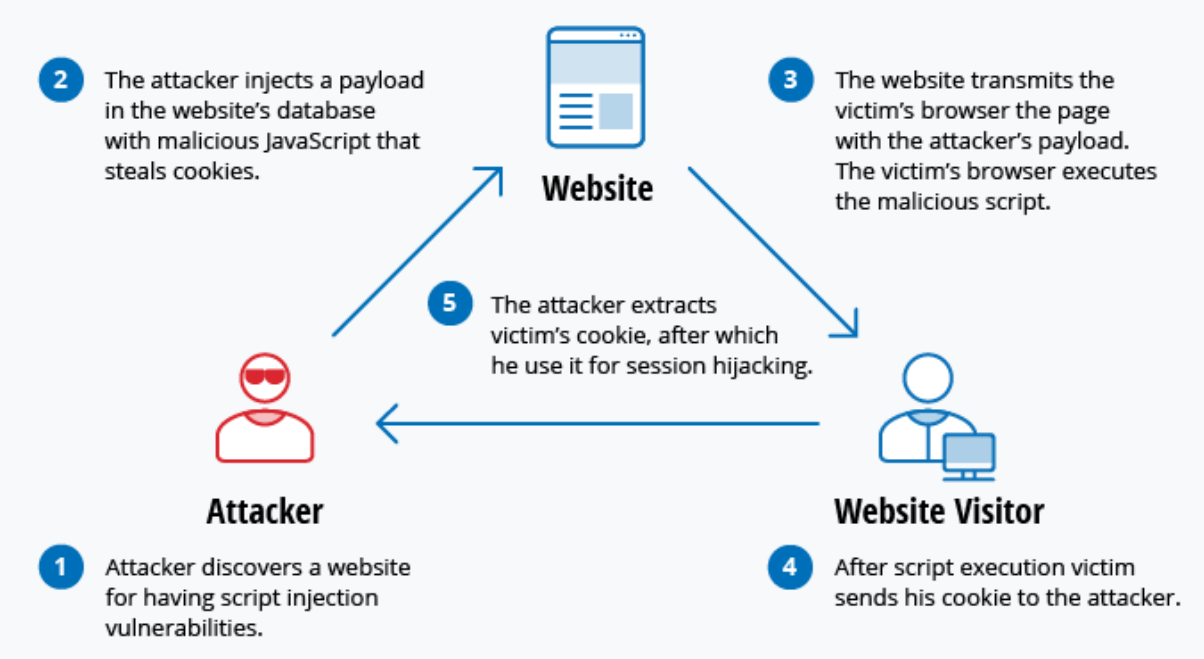
- Εκτίμηση κωδικού πρόσβασης με τρόπο επίθεσης λεξικού, όπου χρησιμοποιείται ένα λεξικό κοινών κωδικών πρόσβασης για την απόπειρα πρόσβασης στον υπολογιστή και στο δίκτυο ενός χρήστη. Μια προσέγγιση είναι η αντιγραφή ενός κρυπτογραφημένου αρχείου που περιέχει κωδικούς πρόσβασης και η εφαρμογή της ίδιας κρυπτογράφησης σε ένα λεξικό των κοινώς χρησιμοποιούμενων κωδικών πρόσβασης συγκρίνοντας μετά τα αποτελέσματα.

- **Επίθεση σεναρίων μεταξύ ιστοτόπων (Cross-site Scripting ή XSS attack):**

Οι επιθέσεις XSS χρησιμοποιούν πόρους ιστού τρίτων για την εκτέλεση σεναρίων (scripts) στο πρόγραμμα περιήγησης ιστού του θύματος ή σε εφαρμογή με δυνατότητα δέσμης ενεργειών (scriptable application). Συγκεκριμένα, ο εισβολέας εισάγει ωφέλιμο φορτίο πακέτου δεδομένων (ή αλλιώς payload, δηλαδή το πεδίο που μαζί με τους headers των επιπέδων δικτύου συνιστά το πακέτο) με κακόβουλη χρήση γλώσσας JavaScript στη βάση δεδομένων ενός ιστότοπου. Όταν το θύμα ζητά μια σελίδα από τον ιστότοπο, ο ιστότοπος μεταδίδει τη σελίδα, με το ωφέλιμο φορτίο του εισβολέα ως μέρος του σώματος γλώσσας HTML (HTML body), στο πρόγραμμα περιήγησης του θύματος, το οποίο εκτελεί το κακόβουλο σενάριο. Για παράδειγμα, ενδέχεται να στείλει κάποιο πρόσθετο (cookie) του θύματος στον διακομιστή του εισβολέα έτσι ώστε ο εισβολέας με τη σειρά του να το εξαγάγει και να το χρησιμοποιήσει για παραβίαση συνεδρίας.

Οι πιο επικίνδυνες συνέπειες συμβαίνουν όταν το XSS χρησιμοποιείται για την εκμετάλλευση πρόσθετων τρωτών σημείων. Αυτές οι ευπάθειες μπορούν να επιτρέψουν σε έναν εισβολέα να κλέψει όχι μόνο πρόσθετα (cookies), αλλά και να καταγράψει κτυπήματα πλήκτρων, να τραβήξει στιγμιότυπα οθόνης, να ανακαλύψει και να συλλέξει πληροφορίες δικτύου και να αποκτήσει πρόσβαση και να ελέγξει από απόσταση τη συσκευή του θύματος.

Εικόνα 1.5 Επίθεση τύπου Cross-Site Scripting



Κεφάλαιο 2:

Συστήματα Ανίχνευσης Εισβολών

2.1 Ορισμός και Ιστορικότητα Συστημάτων Ανίχνευσης Εισβολών

Το πλήθος των επιθέσεων που αναφέραμε σε προηγούμενο κεφάλαιο αποσκοπούν στο να καταπατήσουν την εμπιστευτικότητα, την ακεραιότητα ή την διαθεσιμότητα κάποιου συστήματος του οργανισμού ώστε να: α) αποκτήσουν πρόσβαση σε πληροφορίες, β) μεταχειριστούν πληροφορίες ή γ) καταστήσουν ένα σύστημα μη-αξιόπιστο ή άχρηστο.

Ανίχνευση επιθέσεων είναι η διαδικασία παρακολούθησης γεγονότων-συμβάντων που συμβαίνουν σε ένα σύστημα ή δίκτυο και η ανάλυσή τους για πιθανές απειλές. Το λογισμικό/σύστημα που υλοποιεί αυτή την διαδικασία ονομάζεται *Σύστημα Ανίχνευσης Εισβολών* (IDS).

Στα πρώιμα στάδια της ανάπτυξής τους, ο Fred Cohen το 1984 εξέφρασε τις αμφιβολίες του για την δυνατότητα των συστημάτων αυτών να ανιχνεύουν μία εισβολή κατά

οποιαδήποτε συγκυρία και πως οι απαιτούμενοι πόροι για την ανίχνευση αυξάνονταν δυσανάλογα με το επίπεδο της κίνησης δεδομένων του δικτύου[1].

Το 1986, μία άλλη επιστήμονας, η Dorothy E. Denning, επικουρούμενη από τον Peter G. Neumann, δημοσίευσε το μοντέλο αρχιτεκτονικής ενός συστήματος ανίχνευσης εισβολών που χρησιμοποιήθηκε αποτελώντας το σκαλοπάτι για την εξέλιξή τους[2]. Το μοντέλο αυτό λάμβανε υπ'όψην του στατιστικές για να ανιχνεύσει παρεκτροπές από το μοτίβο της δικτυακής κίνησης δεδομένων, στατιστικές με βάση τα δικτυακά προφίλ των χρηστών του δικτύου του οργανισμού, των συστημάτων υποδοχής και των συστημάτων στόχων, καθώς και ένα κανόνα με βάση το έμπειρο σύστημα για την ανίχνευση γνωστών τύπων εισβολών σε συστήματα. Στο ινστιτούτο έρευνας SRI International της Καλιφόρνια, του δόθηκε η ονομασία Intrusion Detection Expert System (IDES). Το μοντέλο αυτό χρησιμοποιήθηκε σε σταθμούς εργασίας του οργανισμού Sun Microsystems, όπου θα μπορούσε να εξετάζει τόσο το χρήστη όσο και τα δεδομένα σε επίπεδο δικτύου. Η Teresa F. Lunt, σχεδίασε και παρουσίασε την ενδεχόμενη προσθήκη τεχνικού νευρωνικού δικτύου ως ένα τρίτο εργαλείο[3].

---

1 Cohen, F., 1987. "Computer Viruses Theory and Experiments," Computers and Security, vol. 6, pp. 22--35.

2 Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131.

3 Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121.

Έτσι, αρκετά αργότερα και αφού προηγήθηκαν πολλές υλοποιήσεις συστημάτων παρομοίου σκοπού και λειτουργίας, η SRI προχώρησε το 1993 στην υλοποίηση της επόμενης γενιάς IDES, τα Next-generation Intrusion Detection Expert System (NIDES)[4].

Λίγο νωρίτερα, το 1988 δημιουργήθηκε το Multics Intrusion Detection and Alerting System (MIDAS), ένα έμπειρο σύστημα που έκανε χρήση P-Best και Lisp, και άλλων στατιστικών για την μείωση διαδρομών ελέγχου[5].

Το Wisdom & Sense (W&S) ήταν και αυτό ένα σύστημα όπου δημιουργώντας κανόνες με βάση τις στατιστικές ανάλυσης, τους χρησιμοποίησε για την ανίχνευση ανωμαλιών. Αναπτύχθηκε το 1989 στο Los Alamos National Laboratory[6] των Η.Π.Α.

Τον ίδιο χρόνο έγινε μία έκρηξη από απόπειρες βελτιστοποίησης της αρχιτεκτονικής και λειτουργίας των συστημάτων ανίχνευσης. Αποτέλεσμα της μίας από αυτές είναι και το Information Security Officer's Assistant (ISOA), σύστημα πρωτότυπο για το 1990, καθώς είχε τη δυνατότητα να κάνει χρήση πολλών στρατηγικών ανίχνευσης, όπως στατιστικές, ένα προφίλ χρήστη και ένα έμπειρο σύστημα[7].

---

4 Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International.

5 Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988.

6 Vaccaro, H.S., and Liepins, G.E., "Detection of Anomalous Computer Session Activity," The 1989 IEEE Symposium on Security and Privacy, May, 1989.

7 Winkeler, J.R., "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks," The Thirteenth National Computer Security Conference, Washington, DC., pages 115–124, 1990.

Το ίδιο ίσχυε για το σύστημα ComputerWatch, που αναπτύχθηκε στο AT&T Bell Labs και χρησιμοποιούσε στατιστικές και κανόνες για την μείωση του όγκου των δεδομένων που χρήζουν ανάγκης ελέγχου για την επαρκή ανίχνευση εισβολών[8].

Στη συνέχεια, το 1991, οι ερευνητές του Davis πανεπιστημίου της Καλιφόρνια, δημιούργησαν ένα πρωτότυπο πρότυπο κατανεμημένου συστήματος ανίχνευσης εισβολών (DIDS), το οποίο ήταν επίσης ένα έμπειρο σύστημα[9].

Την ίδια χρονιά, εν συνεχεία της έρευνας που απέδωσε το W&S, το εργαστήριο Los Alamos National Laboratory των Η.Π.Α. ανέπτυξε το υπάρχων σύστημά της, δημιουργώντας ένα πρωτότυπο σύστημα ανίχνευσης εισβολών, επονομαζόμενο ως Network Anomaly Detection and Intrusion Reporter (NADIR). Ήταν βασισμένο σε μεγάλο βαθμό στο έργο των Dennnig και Lunt[10].

---

8 Dowell, Cheri, and Ramstedt, Paul, "The ComputerWatch Data Reduction Tool," Proceedings of the 13th National Computer Security Conference, Washington, D.C., 1990.

9 Snapp, Steven R, Brentano, James, Dias, Gihan V., Goan, Terrance L., Heberlein, L. Todd, Ho, Che-Lin, Levitt, Karl N., Mukherjee, Biswanath, Smaha, Stephen E., Grance, Tim, Teal,Daniel M. and Mansur, Doug,

"DIDS (Distributed Intrusion Detection System) -- Motivation, Architecture, and An Early Prototype," The 14th National Computer Security Conference, October, 1991, pages 167–176.

10 Jackson, Kathleen, DuBois, David H., and Stallings, Cathy A., "A Phased Approach to Network Intrusion Detection," 14th National Computing Security Conference, 1991.

Το Lawrence Berkeley National Laboratory της Καλιφόρνια, το 1998, ανακοίνωσε το λογισμικό Bro. Αυτό χρησιμοποιούσε την δική του γλώσσα κανόνων για την ανάλυση των πακέτων από την βιβλιοθήκη συλλογής Libpcap δεδομένων[11].

Αργότερα την ίδια χρονιά, αναπτύχθηκε ένας αναλυτής κίνησης πακέτων δικτύου (sniffer), κάνοντας χρήση της παραπάνω βιβλιοθήκης. Ονομάστηκε Snort και είχε ως σήμερα εκρηκτική ανοδική πορεία, καταλήγοντας πλέον ως το μεγαλύτερο στον κόσμο σύστημα με λειτουργίες ανίχνευσης και αντιμετώπισης εισβολών[12].

Το 2001 το σύστημα Audit Data Analysis and Mining (ADAM) χρησιμοποιεί το εργαλείο ανάλυσης κίνησης πακέτων δικτύου tcpdump για την δημιουργία προφίλ των κανόνων για την ταξινόμησή τους[13].

Τέλος, το 2003 από τους Δρ. Yongguang Zhang και Δρ. Wenke Lee υποστηρίζεται η τεράστια σημασία των συστημάτων ανίχνευσης εισβολών[14] σε υπολογιστικά συστήματα δικτύων και πιο συγκεκριμένα σε δίκτυα με κινούμενους κόμβους.

---

11 Paxson, Vern, "Bro: A System for Detecting Network Intruders in Real-Time," Proceedings of The 7th USENIX Security Symposium, San Antonio, TX, 1998.

12 Kohlenberg, Toby (Ed.), Alder, Raven, Carter, Dr. Everett F. (Skip), Jr., Esler, Joel., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, "Snort IDS and IPS Toolkit," Syngress, 2007, ISBN 978-1-59749-099-3.

13 Barbara, Daniel, Couto, Julia, Jajodia, Sushil, Popyack, Leonard, and Wu, Ningning, "ADAM: Detecting Intrusions by Data Mining," Proceedings of the IEEE Workshop on Information Assurance and Security, West Point, NY, June 5–6, 2001.

14 Yongguang Zhang and Wenke Lee, "Intrusion detection in wireless adhoc networks", MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking, pp 275-28, 2000.

2.2 Πεδία δράσης συστημάτων ανίχνευσης εισβολών

Όπως έχουμε αναφέρει συνοπτικά σε προηγούμενο κεφάλαιο οι έννοιες που σχετίζονται με την ασφάλεια των πληροφοριών που «διασχίζουν» ένα δίκτυο είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Πέρα από αυτές τις βασικές αρχές, σε δεύτερο επίπεδο υπάρχουν οι έννοιες τις αυθεντικοποίησης και μη-απάρνησης. Μια σύντομη περιγραφή αυτών των εννοιών θα ήταν η παρακάτω:

Εμπιστευτικότητα (Confidentiality): Πρόληψη μη-εξουσιοδοτημένης αποκάλυψης πληροφοριών και προστασία προσωπικών δεδομένων. Αναφέρεται κυρίως στην ανάγνωση πληροφοριών και σημαίνει ότι τα δεδομένα που μεταφέρονται θα αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα και συστήματα.

Ακεραιότητα (Integrity): Πρόληψη μη-εξουσιοδοτημένης μεταβολής πληροφοριών. Αναφέρεται στη δημιουργία και στη διαγραφή πληροφοριών και σημαίνει ότι η μεταδιδόμενη πληροφορία παραμένει ως έχει.

Διαθεσιμότητα (Availability): Η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα.

Αυθεντικοποίηση (Authentication): Η γνώση με βεβαιότητα ότι η οντότητα που αξιώνει ότι έστειλε τις πληροφορίες είναι όντως αυτή και όχι κάποια άλλη.

Μη-απάρνηση (Non-repudiation): Η γνώση με βεβαιότητα ότι η οντότητα στην οποία στέλνουμε πληροφορίες τις έχει πάρει ή όχι, έτσι ώστε να μη μπορεί να απαρνηθεί την παραλαβή τους.

2.3 Κατηγορίες και στόχος συστημάτων IDS

2.3.1 Τύποι συστημάτων ανίχνευσης εισβολών

Σύστημα ανίχνευσης εισβολής δικτύου (Network Intrusion Detection System ή NIDS) :

Το σύστημα ανίχνευσης εισβολής δικτύου τοποθετείται στην υποδομή του δικτύου σε συγκεκριμένα στρατηγικά σημεία, όπως π.χ. τα υποδίκτυα (PINs) που είναι πιο ευάλωτα σε

εκμετάλλευση ή επίθεση. Ένα NIDS που τοποθετείται σε αυτά τα PINs παρακολουθεί ολόκληρη την εισερχόμενη και εξερχόμενη κίνηση που ρέει προς και από τις συσκευές δικτύου του συγκεκριμένου τμήματος του οργανισμού.

Σύστημα ανίχνευσης εισβολής τερματικού (Host Intrusion Detection System ή HIDS):

Ένας άλλος τρόπος προσέγγισης είναι αυτός που χρησιμοποιεί το σύστημα ανίχνευσης εισβολής τερματικού. Το HIDS ρυθμίζεται σε όλους τους υπολογιστές του οργανισμού (τερματικά) που είναι συνδεδεμένοι στο δικτυακό περιβάλλον του οργανισμού.

Παρακολουθεί τις συσκευές με πρόσβαση τόσο στο εσωτερικό δίκτυο όσο και στο Διαδίκτυο. Καθώς είναι εγκατεστημένο σε υπολογιστές δικτύου, μπορεί να εντοπίσει κακόβουλα πακέτα δικτύου που μεταδίδονται εντός του οργανισμού (εσωτερικά), συμπεριλαμβανομένων τυχόν μολυσμένων συσκευών που επιχειρούν να εισβάλουν σε άλλους συστήματα. Το NIDS συνήθως δεν το κάνει αυτό.

Σύστημα ανίχνευσης εισβολής με βάση δικτυακές ανωμαλίες (Anomaly-Based Intrusion Detection System ή AIDS) :

Αυτός ο τύπος IDS βασίζεται σε μια μέθοδο ή μια προσέγγιση όπου το πρόγραμμα παρακολουθεί την τρέχουσα κυκλοφορία του δικτύου του οργανισμού και αναλύει το μοτίβο του έναντι προκαθορισμένων κανόνων ή βασικών τιμών.

Στη συνέχεια, αναγνωρίζει και ειδοποιεί τους διαχειριστές για οποιαδήποτε ασυνήθιστη συμπεριφορά παρατηρείται στο εύρος ζώνης δικτύου, συσκευές, θύρες (δικτύου και όχι φυσικές θύρες συσκευών) , πρωτόκολλα κ.λπ.

Σύστημα ανίχνευσης εισβολών βάσει υπογραφής (Signature-Based Intrusion Detection System ή SIDS) :

Αυτά τα συστήματα διαθέτουν μια ολοκληρωμένη βάση δεδομένων ή βιβλιοθήκη υπογραφών και ιδιοτήτων που παρουσιάζονται από γνωστές επιθέσεις εισβολής ή κακόβουλες απειλές. Το συστήματα ανίχνευσης εισβολών βάσει υπογραφής παρακολουθούν όλα τα πακέτα δικτύου και εντοπίζουν πιθανό κακόβουλο λογισμικό, αναλύοντας εάν αυτές οι υπογραφές ταιριάζουν με τις ύποπτες δραστηριότητες που συμβαίνουν.

2.3.2 Τύποι ελέγχου που χρησιμοποιούν τα συστήματα ανίχνευσης εισβολών

Ένα σύστημα ανίχνευσης εισβολών είναι λογισμικό ή συνδυασμός λογισμικού και υλικού το οποίο εξ ορισμού λειτουργεί παθητικά. Αυτό σημαίνει πως δεν εφαρμόζει τεχνικές

για να περιορίσει την εξάπλωση μίας επίθεσης, αλλά μένει μόνο στην αναγνώριση και την υπόδειξη επιθέσεων στον διαχειριστή ασφάλειας του δικτύου.

Τα συστήματα ανίχνευσης επιθέσεων χρησιμοποιούν για την ανίχνευση είτε τον τρόπο στατιστικής διαταραχών είτε την παρατήρηση κακόβουλης συμπεριφοράς.

- Η ανίχνευση με βάση στατιστική διαταραχών (statistical anomaly), καθιερώνει ένα «συνηθισμένο προφίλ δραστηριότητας» με στατιστικό τρόπο. Κατά την καθιέρωση του προφίλ αυτού, πρέπει να γίνει έλεγχος από τους διαχειριστές του δικτύου, ώστε να βεβαιωθεί πως εκφράζει το δίκτυο υπό συνθήκες φυσιολογικής συμπεριφοράς. Αλλαγές στα δικτυακά συστήματα και συσκευές, στις δικτυακές ζεύξεις ή στην λογική κίνησης του δικτύου (switching, routing) μπορούν να αποτελέσουν σημάδι επίθεσης για το σύστημα αντιμετώπισης εισβολών. Αυτό συμβαίνει διότι ο τρόπος αυτός ανίχνευσης βασίζεται στο γεγονός ότι, όλες οι επιθετικές δραστηριότητες θεωρούνται ανωμαλίες και, πως, οποιαδήποτε παρέκκλιση από το σύνηθες προφίλ συνεπάγεται επίθεση.

- Η ανίχνευση κακόβουλης συμπεριφοράς (Misuse detection), από την άλλη, βασίζεται στο ότι υπάρχουν κάποια προκαθορισμένα σχέδια επίθεσης (όπως έχουμε αναφέρει νωρίτερα στις κατηγορίες επιθέσεων), ονομαζόμενα πρότυπα ή υπογραφές (signatures). Αν το σύστημα ανιχνεύσει κάποιο από τα πρότυπα μίας πιθανής προσπάθειας παράβασης, τότε συμπεραίνει ότι δέχεται επίθεση

και προσπαθεί να κάνει ταυτοποιήσεις. Ο τρόπος αυτός είναι ο πιο σύνηθες στα περισσότερα IDS.

2.3.3 Στόχοι συστημάτων ανίχνευσης εισβολών

Ανεξάρτητα από το αν ένα σύστημα ανίχνευσης εισβολών χρησιμοποιεί στατιστικά διαταραχών ή παρατήρηση κακόβουλης συμπεριφοράς, οι στόχοι του είναι κοινοί με τα υπόλοιπα συστήματα της ίδιας κατηγορίας. Οι λίγες διαφοροποιήσεις προκύπτουν, ανάλογα με το πόσο εξελιγμένο είναι το σύστημα, όπως θα δούμε σε επόμενο κεφάλαιο και στον τρόπο υλοποίησης (λόγω δυνατοτήτων) των στόχων αυτών. Παρακάτω υπάρχουν οι στόχοι ενός τέτοιου συστήματος:

- **Αναγνώριση αποκλίνουσας συμπεριφοράς του δικτύου του οργανισμού.**

Πρωταρχικός στόχος του IDS είναι να παρακολουθεί τις δραστηριότητες των συστημάτων του οργανισμού στο δίκτυο αλλά και την κίνηση των χρηστών του δικτύου του PIN στο οποίο έχει εγκατασταθεί. Βάσει αυτής της δυνατότητας

παρακολούθησης, πραγματοποιεί την άμεση ανίχνευση αποκλίνουσας συμπεριφοράς κίνησης δικτυακών πακέτων.

- **Ταυτοποίηση αποκλίνουσας συμπεριφοράς του δικτύου του οργανισμού.**

Έπειτα από την αναγνώριση, στόχος του IDS είναι να ταυτοποιήσει πιθανές προσπάθειες επίθεσης. Για την ταυτοποίηση, κάνει χρήση των δεδομένων που έχει στη διάθεσή του μέσω της βάσης δεδομένων του. Η βάση δεδομένων ενός IDS είτε είναι αποκλειστικά τοπική , δίνοντάς της έτσι στατική υπόσταση, είτε δυναμική.

Στατική βάση δεδομένων για ένα IDS σημαίνει πως το σύστημα ελέγχει τοπικά την κάθε παρεκκλίνουσα δικτυακή συμπεριφορά, ψάχνοντας για κάποιο ταιριαστό γνωστό μοτίβο σε αυτήν προς αντιστοίχιση. Είναι εξαιρετικά σημαντικό τα συστήματα με στατική βάση δεδομένων να παραμένουν ενημερωμένα, καθώς εναλλακτικά υπάρχει αυξημένο ρίσκο αδυναμίας αναγνώρισης της επίθεσης.

Αντίστοιχα, συστήματα ανίχνευσης εισβολών με δυναμική βάση συμπεριφέρονται διαφορετικά ως προς τη διαδικασία ταυτοποίησης της επίθεσης. Τα συστήματα αυτά εμφανίστηκαν μόλις τα τελευταία χρόνια στα δίκτυα οργανισμών και είναι εξελιγμένα προϊόντα που ονομάζονται συστήματα ανίχνευσης εισβολών επόμενης γενιάς. Συνήθως κρατούν λιγότερα στοιχεία στην τοπική τους βάση, αλλά βασίζονται αρχιτεκτονικά στην συνεχή επικοινωνία τους με τον οργανισμό ασφαλείας που έχει ορίσει ο κατασκευαστής (συχνά τμήμα του ιδίου).

Σε περίπτωση επίθεσης, ανεβάζουν πακέτα που περιέχουν πληροφορίες για το μοτίβο της επίθεσης, μέσω του διαδικτύου, στους διακομιστές του οργανισμού ασφαλείας. Ο οργανισμός ασφαλείας με τη σειρά του, απαντά με τα απαραίτητα στοιχεία για την ταυτοποίηση της επίθεσης αλλά και προτάσεις επαναφοράς του δικτύου και των πόρων (συστήματα/εφαρμογές) που έχουν πληγεί στη φυσιολογική τους κατάσταση.

Τα παραπάνω συστήματα απαιτούν για την εύρυθμη λειτουργία τους πρόσβαση στο διαδίκτυο (προς επικοινωνία με τον οργανισμό ασφαλείας) και σε περίπτωση απώλειας αυτής (ίσως λόγω μίας επίθεσης) η αποδοτικότητά τους μειώνεται καθιστώντας τα πλήρως εξαρτόμενα από την τοπική τους βάση δεδομένων. Περισσότερες λεπτομέρειες για τα συστήματα αυτά θα αναφέρουμε και αναλύσουμε σε επόμενο κεφάλαιο.

- **Καταγραφή του συμβάντος και ενημέρωση των διαχειριστών του συστήματος.**

Για την επαναφορά του δικτύου του οργανισμού σε φυσιολογική συμπεριφορά μετά από μία επίθεση, είναι απαραίτητη η παρέμβαση των διαχειριστών του. Το IDS, ως παθητικό σύστημα, δεν λαμβάνει ενέργειες επιδιόρθωσης, πρέπει όμως να μπορεί να καταγράψει τη παρατηρούμενη συμπεριφορά και να ενημερώσει τους διαχειριστές για να το κάνουν οι ίδιοι. Η έγκαιρη ενημέρωση είναι πρωτίστης σημασίας, καθώς από ο χρόνος ενημέρωσης είναι άμεσα συσχετιζόμενος με το χρόνο επιδιόρθωσης του προβλήματος. Παράλληλα, όπως αναφέραμε σε προηγούμενο κεφάλαιο, το μέγεθος του προβλήματος που προκαλούν στο

δίκτυο πολλοί τύποι επιθέσεων μεγαλώνει εκθετικά με την αύξηση του χρόνου επαναφοράς του.

Τα συστήματα ανίχνευσης εισβολών χρησιμοποιούν ένα σύνολο εργαλείων με σκοπό να διευκολύνουν τους διαχειριστές στον έλεγχο του δικτύου και των συστημάτων, όπως τα αρχεία καταγραφής πρόσβασης χρήστη (user access logs), τα αρχεία καταγραφής πρόσβασης σε αρχεία (file access logs) και τα αρχεία καταγραφής συμβάντων του συστήματος (system event logs).

Πέρα από την απλή καταγραφή, τα συστήματα ανίχνευσης εισβολών μπορούν να δημιουργούν ίχνη παρακολούθησης, τα οποία γίνονται εμφανή αφού επιτευχθεί η επίθεση. Ενώ τα παθητικά συστήματα δεν σχεδιάστηκαν με κύριο σκοπό την αποτροπή επιθέσεων, υπάρχουν αρκετές ενδείξεις αναπτυγμένων, σύνθετων επιθέσεων, οι οποίες γίνονται εμφανείς μόνο μετά την ολοκλήρωση μιας εισβολής.

- **Αναγνώριση ενεργειών που προηγούνται μιας επίθεσης.**

Τα IDS ανιχνεύουν αναγνωριστικές ενέργειες που προηγούνται μίας επίθεσης. Για την πραγματοποίηση μίας επίθεσης, συνήθως υπάρχουν κάποια στάδια που προηγούνται αυτής. Ο επιτιθέμενος πρώτα εξετάζει τον υποψήφιο στόχο του, ώστε να συγκεντρώσει πληροφορίες για αυτόν και να εντοπίσει ένα σημείο εισόδου, το οποίο θα του επιτρέψει να πραγματοποιήσει την επίθεση με επιτυχία. Συχνές μέθοδοι επίτευξης του παραπάνω είναι η προσπάθεια αναγνώρισης συσκευών (ip/device scanning ακολουθούμενη από mac-address lookup) και πόρων αυτών που είναι ανοιχτοί προς χρήση (port scanning).

Δίχως την ύπαρξη ενός IDS, ο επιτιθέμενος είναι πολύ πιθανόν να πραγματοποιήσει τις αναγνωριστικές του κινήσεις ανενόχλητος και χωρίς να γίνει αντιληπτός.

- **Αποθήκευση πληροφοριών μοτίβου επίθεσης.**

Ακόμα, με την χρήση των IDS συλλέγονται πληροφορίες και παρατηρούνται μοτίβα (patterns) που αφορούν επιθέσεις που πραγματοποιούνται καθημερινά εναντίον ενός δικτύου και των συστημάτων του, οι οποίες θα βοηθήσουν στην αποκατάσταση των συστημάτων που παραβιάστηκαν και την διόρθωση αδυναμιών και παραλήψεων στα ήδη υπάρχοντα μέτρα ασφάλειας.

Οι πληροφορίες και στοιχεία που μπορεί να συλλέξει το σύστημα ανίχνευσης εισβολών μπορούν επίσης να βοηθήσουν στην ευκολότερη αναγνώριση (και κατά συνέπεια αντιμετώπιση) αντίστοιχων μελλοντικών επιθέσεων αλλά και για τον εντοπισμό του επιτιθέμενου με σκοπό την ποινική δίωξη του. Το τελευταίο είναι συχνός συντελεστής για το δισταγμό του υποψήφιου επιτιθέμενου.

Η συγκεκριμένη διαδικασία είναι σημαντική για την εξασφάλιση της μακροπρόθεσμης προστασίας του δικτύου και των συστημάτων του οργανισμού και την αποτελεσματικότερη προστασία τους από συνθετότερες επιθέσεις που ίσως ακολουθήσουν στο μέλλον.

- **Παροχή πλασματικών δικτύων (honeypot)**

Τα συστήματα IDS χρησιμοποιούνται για δημιουργία πλασματικών δικτύων, που προσομοιώνουν τη μορφή πόρων ενός συστήματος. Τα πλασματικά δίκτυα αυτά χρησιμοποιούνται για να προσελκύσουν τους επιδόξους εισβολείς και να αποσπάσουν την προσοχή τους από το πραγματικό δίκτυο, ενώ οι ενέργειες τους παρακολουθούνται.

Στόχος της παραπάνω ενέργειας του συστήματος ανίχνευσης εισβολών είναι ο εντοπισμός ενδείξεων για πιθανές προσπάθειες επίθεσης, κατά τις οποίες συχνά εντοπίζονται ίχνη παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών πόρων.

2.4 Λειτουργία συστημάτων ανίχνευσης εισβολών

Έχοντας αναφέρει τις κατηγορίες και τους σκοπούς των IDS είναι κατάλληλη στιγμή να εμβαθύνουμε στον τρόπο λειτουργίας τους.

Ξεκινώντας, πρέπει να αναφέρουμε ότι ανεξαρτήτως τον τύπο του συστήματος ανίχνευσης εισβολών, ο τρόπος με τον οποίο συλλέγει και διαχειρίζεται δεδομένα για την κίνηση του δικτύου του οργανισμού επιτυγχάνεται κάνοντας χρήση όμοιων ενεργειών και τελικά εργαλείων και πρωτοκόλλων. Ο τρόπος συλλογής και διαχείρισης συνοψίζεται σε τρεις ενέργειες.

Η πρώτη ενέργεια, απαραίτητη στη λειτουργία κάθε IDS είναι ο έλεγχος των πακέτων δικτυακής κίνησης. Ο έλεγχος αυτός ιδεατά αφορά την εισερχόμενη (inbound ή ingress) αλλά και εξερχόμενη (outbound ή egress) κίνηση του δικτύου του PIN στο οποίο είναι εγκατεστημένο το IDS. Η κίνηση που είναι ικανό ένα τέτοιο σύστημα να επιθεωρήσει είναι αυτή των παρακάτω κατηγοριών:

- Κίνηση πρωτοκόλλου TCP: Τα πακέτα TCP (segments) έχουν στο πεδίο protocol την τιμή 6. Αφορά την κίνηση κάθε τύπου εφαρμογών, από και προς πολλών τύπων διακομιστές εντός και εκτός του οργανισμού, αλλά και κίνηση διαχείρισης. Κάποια από τα πρωτόκολλα που λειτουργούν μέσω TCP χρησιμοποιούνται καθημερινά από τους χρήστες του δικτύου του οργανισμού (http-https, sftp-ftp, smtp, κ.α.) αλλά και από τους διαχειριστές αυτού (ssh, tacacs, κ.α.) .

- Κίνηση πρωτοκόλλου UDP: Τα πακέτα UDP (segments) έχουν στο πεδίο protocol την τιμή 17. Αφορά την κίνηση περιορισμένων λειτουργιών των χρηστών του οργανισμού και των τερματικών τους (dhcp, dns, radius, εφαρμογές VoIP, εφαρμογές streaming κ.α.), αλλά και των συσκευών δικτύου (snmp - snmp traps, syslog, κ.α.).

- Κίνηση πρωτοκόλλου ICMP: Τα πακέτα του (segments) έχουν στο πεδίο protocol την τιμή 1 (ή 58 για ICMPv6). Αφορά την κίνηση περιορισμένων λειτουργιών των τερματικών του οργανισμού (keepalives εφαρμογών, secure network access control μέσω radius για συσκευές VoIP και τερματικών, κ.α.) αλλά αποτελεί και εργαλείο για

τους διαχειριστές του δικτύου (ping, traceroute). Κίνηση τέτοιου τύπου πολύ συχνά χρησιμοποιείται από επίδοξους εισβολείς αφού βρουν πρόσβαση σε ένα δίκτυο για να «ανακαλύψουν» τους πόρους που το αποτελούν και πιθανές αδυναμίες ασφαλείας αυτών (device scanning, port scanning μέσω Nmap και αντιστοίχων εργαλείων και στη συνέχεια mac-address lookup).

- Κίνηση δικτύου διαχειριστικής φύσης: Πολλά πρωτόκολλα είναι αόρατα για τις συσκευές των χρηστών και χρησιμοποιούνται από τις συσκευές δικτύου, τους διακομιστές και επόπτες. Συχνά, τα συστήματα ανίχνευσης εισβολών δεν ρυθμίζονται να ανιχνεύουν τέτοια κίνηση αλλά πολλά από αυτά παρέχουν αυτή τη δυνατότητα στους διαχειριστές του οργανισμού. Κάποιες από τις κατηγορίες διαχειριστικής κίνησης είναι αυτή των δυναμικών πρωτοκόλλων δρομολόγησης (EIGRP – protocol number 88, OSPF – protocol number 89), πρωτοκόλλων δημιουργίας δικτύων επικάλυψης ή overlay networks (Vxlan, LISP) και πρωτοκόλλων ασφαλείας και κρυπτογράφησης (GRE – protocol number 47, ESP – protocol number 50, AH – protocol number 51, κ.α.).

Η δεύτερη ενέργεια είναι η επιθεώρηση των παραπάνω τύπων δικτυακής κίνησης και ανάλυσή του μοτίβου της. Ένα σύστημα ανίχνευσης εισβολών έχει αρκετούς τρόπους στη διάθεσή του για την επίτευξη της επιθεώρησης αυτής. Ο κάθε τρόπος βασίζεται σε κάποιο πρωτόκολλο σχεδιασμένο για την διευκόλυνση του ελέγχου του δικτύου από τους διαχειριστές του. Συνεπώς, τα παρακάτω πρωτόκολλα έχουν τον ίδιο σκοπό, που όμως υλοποιούν με αρκετά διαφορετικό τρόπο.

- **Πρωτόκολλα τύπου Netflow:**

Το NetFlow είναι ένα πρωτόκολλο που σχεδιάστηκε από την Cisco και παρουσιάστηκε πρώτη φόρα στους δρομολογητές Cisco το 1996. Παρέχει τη δυνατότητα συλλογής κίνησης δικτύου IP καθώς εισέρχεται ή εξέρχεται (inbound/outbound) από μια διεπαφή (physical port, virtual interface, vlan interface, κ.α.) μιας συσκευής . Αναλύοντας τα δεδομένα που παρέχονται από το NetFlow, ένας διαχειριστής δικτύου μπορεί να καθορίσει πράγματα όπως την πηγή και τον προορισμό της κυκλοφορίας, την κατηγορία υπηρεσίας και τις αιτίες της συμφόρησης. Μια τυπική ρύθμιση παρακολούθησης ροής χρησιμοποιώντας NetFlow αποτελείται από τρία κύρια στοιχεία.

- Εξαγωγέας ροής (flow exporter): συγκεντρώνει πακέτα σε ροές και εξάγει αρχεία ροής προς έναν ή περισσότερους συλλέκτες ροής.

- Συλλέκτης ροής (flow collector): υπεύθυνος για τη λήψη, αποθήκευση και προεπεξεργασία δεδομένων ροής που λαμβάνονται από έναν εξαγωγέα ροής.

- Εφαρμογή ανάλυσης (flow monitor): αναλύει δεδομένα ροής που λαμβάνονται στο πλαίσιο της ανίχνευσης εισβολής ή του προφίλ κυκλοφορίας.

Οι δικτυακές συσκευές που υποστηρίζουν το πρωτόκολλο NetFlow (routers, switches κ.α.) μπορούν να συλλέγουν στατιστικά κίνησης IP σε όλες τις διεπαφές όπου είναι ενεργοποιημένο το NetFlow και αργότερα να εξάγουν αυτά τα στατιστικά στοιχεία ως εγγραφές NetFlow προς τουλάχιστον έναν συλλέκτη NetFlow — συνήθως έναν διακομιστή που κάνει την πραγματική ανάλυση κίνησης, συχνά το ίδιο το σύστημα ανίχνευσης εισβολών.

Στην αρχή ήταν ιδιόκτητο πρωτόκολλο της Cisco αλλά γρήγορα έγινε ανοιχτό πρότυπο (open standard) και χρησιμοποιείται από δικτυακές συσκευές πολλών κατασκευαστών. Παρόμοιας λειτουργίας πρωτόκολλα με το netflow είναι το flexible netflow, netstream, sflow, ipfix, κ.α.

- **Πρωτόκολλο SNMP:**

Το Simple Network Management Protocol (SNMP) είναι ένα πρωτόκολλο για τη συλλογή και οργάνωση πληροφοριών σχετικά με τις διαχειριζόμενες συσκευές σε δίκτυα IP και για την αποστολή αντίστοιχων πληροφοριών με σκοπό την αλλαγή συμπεριφοράς αυτών. Στις συσκευές που υποστηρίζουν SNMP περιλαμβάνονται καλωδιακά μόντεμ, δρομολογητές, μεταγωγείς, διακομιστές, σταθμοί εργασίας, εκτυπωτές και άλλα. Το SNMP χρησιμοποιείται ευρέως στη διαχείριση δικτύου για εργαλείο παρακολούθησής του.

Λειτουργεί λαμβάνοντας δεδομένα διαχείρισης από τα διαχειριζόμενα συστήματα με τη μορφή μεταβλητών, που οργανώνονται σε μια βάση

πληροφοριών διαχείρισης (Management Information Base ή MIB) και περιγράφουν την κατάσταση και τη διαμόρφωση του συστήματος. Αυτές οι μεταβλητές μπορούν στη συνέχεια να εξεταστούν εξ αποστάσεως. Παράλληλα, είναι εφικτό να ρυθμιστούν μέσω SNMP οι διαχειριζόμενες συσκευές από τη συσκευή-διαχειριστή.

Σε τυπικές χρήσεις του SNMP, ένας ή περισσότεροι υπολογιστές διαχείρισης έχουν το καθήκον να παρακολουθούν ή να διαχειρίζονται μια ομάδα κεντρικών υπολογιστών ή συσκευών σε ένα δίκτυο υπολογιστών. Κάθε διαχειριζόμενο σύστημα εκτελεί ένα στοιχείο λογισμικού που ονομάζεται agent και αναφέρει πληροφορίες μέσω SNMP στον διαχειριστή (SNMP manager).

Ένα δίκτυο διαχειριζόμενο μέσω SNMP αποτελείται από τρία βασικά στοιχεία:

- Διαχειριζόμενες συσκευές.
- Λογισμικό που λειτουργεί σε διαχειριζόμενες συσκευές.
- Σταθμός διαχείρισης δικτύου (Network Management System ή NMS) - λογισμικό που λειτουργεί στον διαχειριστή.

Έχουν αναπτυχθεί και καθιερωθεί τρεις σημαντικές εκδόσεις του SNMP. Το SNMPv1 είναι η αρχική έκδοση του πρωτοκόλλου. Οι πιο πρόσφατες εκδόσεις, SNMPv2c και SNMPv3, διαθέτουν βελτιώσεις στην απόδοση, την ευελιξία και κυρίως την ασφάλεια στη μετάβαση των πληροφοριών.

Το SNMP είναι ένα συστατικό στοιχείο του Internet Protocol Suite όπως ορίζεται από την Ομάδα Μηχανικής Διαδικτύου (IETF). Αποτελείται από ένα σύνολο προτύπων για τη διαχείριση του δικτύου, συμπεριλαμβανομένου ενός πρωτοκόλλου επιπέδου εφαρμογής, ενός σχήματος βάσης δεδομένων και ενός συνόλου αντικειμένων δεδομένων.

- **Πρωτόκολλα Κατόπτρισης Θύρας:**

Η τεχνική κατόπτρισης θύρας ρυθμίζεται σε έναν μεταγωγέα (ή δρομολογητή) δικτύου για να στείλει ένα αντίγραφο κάθε πακέτου που εμφανίζονται σε μια ή περισσότερες θύρες του (ή σε ένα ολόκληρο VLAN) σε μια σύνδεση παρακολούθησης δικτύου που έχει οριστεί σε μια άλλη ή άλλες θύρες του.

Η τεχνική αυτή χρησιμοποιείται συνήθως για συσκευές δικτύου που απαιτούν παρακολούθηση της κυκλοφορίας δικτύου, όπως ένα σύστημα ανίχνευσης εισβολής ή τεχνολογία παρακολούθησης πραγματικών χρηστών (Real User Monitoring ή RUM) που χρησιμοποιείται για την υποστήριξη της διαχείρισης απόδοσης εφαρμογών (Application Performance Management ή APM).

Οι μηχανικοί ή οι διαχειριστές δικτύου χρησιμοποιούν κατοπτρισμό θύρας για την ανάλυση και τον εντοπισμό σφαλμάτων δεδομένων ή τη διάγνωση σφαλμάτων σε ένα δίκτυο. Ταυτόχρονα, βοηθά τους διαχειριστές να παρακολουθούν στενά την απόδοση του δικτύου και να τους ειδοποιεί όταν προκύπτουν προβλήματα. Μπορεί να χρησιμοποιηθεί

για να αντικατοπτρίζει είτε εισερχόμενη είτε εξερχόμενη κίνηση (ή και τα δύο) σε μονές ή πολλαπλές διεπαφές.

Η κατοπτρική θύρα σε μεταγωγέα Cisco αναφέρεται γενικά ως Switched Port Analyzer (SPAN), Remote Switched Port Analyzer (RSPAN) ή Encapsulated Remote Switched Port Analyzer (ERSPAN). Κάποιοι προμηθευτές έχουν διαφορετικά ονόματα για αυτό, όπως το Roving Analysis Port (RAP) σε μεταγωγείς 3Com, Port-aggregation TAP σε περιβάλλοντα KVM κ.α.

Η συνεχής ανάλυση της κίνησης που συλλέγει το σύστημα ανίχνευσης εισβολών κάνοντας χρήση των παραπάνω εργαλείων γίνεται εξετάζοντας συγκεκριμένα πεδία των πακέτων του δικτύου. Η βαθύτερη αυτή εξέταση αφορά κυρίως το πεδίο θύρας προορισμού (destination port) το οποίο υπάρχει τόσο στα πακέτα TCP όσο και UDP και χρησιμοποιείται για την πολυπλεξία κίνησης εφαρμογών. Από την τιμή του πεδίου αυτού φαίνεται η εφαρμογή για την οποία προορίζονται τα δεδομένα.

Άλλα πεδία που εξετάζουν τα συστήματα ανίχνευσης εισβολών είναι το πεδίο θύρας πηγής (source port), σημαίας (flag), τα πεδία που χρησιμοποιούνται για εφαρμογή ελέγχου υπηρεσίας (QoS group, CoS, IPP, DSCP) καθώς και τα δεδομένα του χρήστη ή payload.

Για την εξέταση των πακέτων με τέτοιο τρόπο χρησιμοποιούνται διάφορα εργαλεία, με γνωστότερο αυτών το NBAR (Network Based Application Recognition). Το NBAR αποτελεί τον μηχανισμό που χρησιμοποιείται από ορισμένους δρομολογητές και μεταγωγείς Cisco για την αναγνώριση μιας ροής δεδομένων ελέγχοντας ορισμένα πακέτα που αποστέλλονται. Ο εξοπλισμός δικτύωσης που χρησιμοποιεί αντίστοιχα εργαλεία κάνει βαθιά επιθεώρηση πακέτων σε ορισμένα από τα πακέτα σε μια ροή δεδομένων, για να προσδιορίσει σε ποια κατηγορία κυκλοφορίας ανήκει η ροή. Χρησιμοποιείται σε συνδυασμό με άλλες δυνατότητες και μπορεί στη συνέχεια να προγραμματίσει τα ολοκληρωμένα κυκλώματα

εσωτερικής εφαρμογής (ASIC) για τον κατάλληλο χειρισμό αυτής της ροής. Το NBAR και τα εργαλεία ιδίου τύπου θεωρούνται πρωτόκολλα επιπέδου εφαρμογής (OSI Layer 7).

Η τρίτη ενέργεια συλλογής και διαχείρισης είναι η άμεση ενημέρωση των διαχειριστών του δικτύου σε περίπτωση ανίχνευσης προβλημάτων ή ανωμαλιών στο δίκτυο, διαδικασία γνωστή ως alerting. Για την υλοποίηση του alerting τα συστήματα ανίχνευσης εισβολών κάνουν χρήση των παρακάτω πρωτοκόλλων που θα αναφέρουμε συνοπτικά.

- Το πρωτόκολλο Syslog, το οποίο δέχεται ειδοποιήσεις από συσκευές δικτύου και διακομιστές και τις κατηγοριοποιεί σε επίπεδα σοβαρότητας.

- Το πρωτόκολλο SMTP (και άλλα πρωτόκολλα email) τα οποία μεταφέρουν μηνύματα Syslog, SNMP και άλλα ενημερώνοντας μέσω email τους διαχειριστές του δικτύου του οργανισμού.

Κεφάλαιο 3:

Συστήματα Πρόληψης Εισβολών

3.1 Ορισμός και Ιστορικότητα Συστημάτων Πρόληψης Εισβολών

Τα συστήματα πρόληψης εισβολών (γνωστά και ως intrusion prevention systems ή IPS) είναι συστήματα-μέλη της οικογένειας των συσκευών ασφάλισης δικτυακών πόρων που λειτουργούν τόσο ανιχνεύοντας όσο και αντιμετωπίζοντας αναγνωρισμένες απειλές.

Ενώ οι πρώιμες μορφές IPS άρχισαν να εμφανίζονται στην αγορά στα μέσα της δεκαετίας του 1990 η υιοθέτηση του IPS άρχισε να αυξάνεται στο τελευταίο μέρος του 2005, όταν και άρχισαν να το υποστηρίζουν οι περισσότεροι προμηθευτές. Η μειωμένη ανταπόκριση της αγοράς ως τότε οφείλεται σε 2 διαφορετικούς παράγοντες.

1) Οι απειλές ως τότε ήταν αρκετά λιγότερες, καθώς υπήρχαν λιγότεροι επίδοξοι εισβολείς που είχαν στη διάθεσή τους τους απαιτούμενους πόρους για την

πραγματοποίηση μίας επίθεσης. Το κόστος αγοράς των απαραίτητων πόρων για την υλοποίηση των σύνθετων επιθέσεων ήταν απαγορευτικό για την πλειοψηφία των ατόμων που ανήκουν στην παραπάνω κατηγορία, ενώ η απαραίτητη τεχνογνωσία για την αναγνώριση αλλά και εκμετάλλευση αδυναμιών του δικτύου ενός οργανισμού σπάνιζε.

2) Τα συστήματα πρόληψης εισβολών, όπως και τα συστήματα ανίχνευσης εισβολών χρησιμοποιούν τεχνικές βαθιάς επιθεώρησης των πακέτων που διασχίζουν το δίκτυο (ως το επίπεδο εφαρμογής ή 7ο του OSI αλλά και τα δεδομένα του χρήστη ή payload), κάτι που επέφερε καθυστερήσεις στη ροή της κίνησης.

Ως τότε, πολλοί οργανισμοί χρησιμοποιούσαν αρχιτεκτονικές ασφαλείας δικτύου που αποτελούνταν από συστήματα ανίχνευσης εισβολών και φυσικές συσκευές τειχών προστασίας (firewalls), όπου τα δεύτερα εξέταζαν το πακέτο ως προς το περιεχόμενό του μέχρι τις επικεφαλίδες επιπέδου μεταφοράς (Layer 4 headers). Η καθυστέρηση οφείλεται στο ότι τα IPS βρίσκονται στην πορεία της κίνησης ώστε να μπορούν να παρέμβουν, αντί για παράπλευρα αυτής (IDS), σε συνδυασμό με το γεγονός πως θα έπρεπε να συγκρίνουν το κάθε πακέτο με όλες τις υπογραφές επιθέσεων της βάσης δεδομένων τους (συχνά χιλιάδες).

Το 2004, οι προμηθευτές IPS άρχισαν να δημιουργούν προφίλ ασφαλείας με σκοπό να χαρακτηρίσουν με μόνο μία υπογραφή την κάθε τύπου ευπάθεια, ανεξάρτητα με το πόσα είδη επιθέσεων σχετίζονταν με αυτήν.

Τα συστήματα πρόληψης εισβολών αποτελούν, σύμφωνα με τον ανεπίσημο ορισμό που τους έχει δοθεί, την εξελιγμένη μορφή των συστημάτων ανίχνευσης

εισβολών. Βασίζονται στις ίδιες αρχές με τα προηγηθέντα IDS έχοντας όμως επιπλέον σκοπούς, δυνατότητες και εργαλεία στη διάθεσή τους.

Εξελίχθηκαν σταδιακά από τα IDS, παράλληλα με την αύξηση σημείων εισόδου στα σύγχρονα δίκτυα, φτάνοντας τελικά την σημερινή τους «μορφή». Η αύξηση των σημείων εισόδου στο δίκτυο ενός οργανισμού αποτελεί άμεσο επακόλουθο της πολυπλοκότητας και του αριθμού των PIN που επιβάλλει η μοντερνοποίηση των σύγχρονων δικτύων οργανισμών.

Παρ' όλο που τα IPS αποτελούν πιο ολοκληρωμένες λύσεις ασφαλείας δεν καθιστούν απαρχαιωμένα τα συστήματα ανίχνευσης εισβολών και ούτε μάταιη τη χρήση τους για τα σύγχρονα δίκτυα. Πολλοί οργανισμοί σήμερα έχουν ενσωματώσει και τα δύο είδη των συστημάτων αυτών στο δίκτυο τους, ειδικά στα PINs του campus και data center.

Συχνά όμως, όταν ο οργανισμός δεν δρα βάσει πολύ αυστηρών κανόνων λειτουργίας στον τομέα της δικτυακής ασφαλείας (ίσως λόγω του ότι δεν διαχειρίζεται μεγάλο όγκο από ευαίσθητες πληροφορίες ή προσωπικά δεδομένα) βασίζεται σε συστήματα πρόληψης και όχι ανίχνευσης εισβολών για την άμυνα του έναντι πιθανών επιθέσεων.

Παράλληλα όμως, υπάρχουν περιπτώσεις οργανισμών όπου η χρήση ενός IPS δεν θα ήταν αποδοτική λόγω ιδιαιτεροτήτων της αρχιτεκτονικής του δικτύου του.

Τέλος, κάποιες φορές ένας οργανισμός καλύπτει αποδοτικά της ανάγκες του με τη χρήση ενός συστήματος ανίχνευσης εισβολών, έχοντας άλλα εργαλεία ή συστήματα και την απαραίτητη διαχειριστική τεχνογνωσία για να παρακάμψει της ελλείψεις αυτού.

Στις παρακάτω ενότητες θα αναλύσουμε ποιες είναι αυτές οι ελλείψεις των συστημάτων ανίχνευσης εισβολών και πως κάποιες από αυτές καλύπτονται από τα συστήματα πρόληψης εισβολών, ποιες οι διαφορές τους στους σκοπούς, την εγκατάσταση, τη χρήση και τη λειτουργία τους.

3.2 Σκοπός και λειτουργία συστημάτων πρόληψης εισβολών

Τα IPS είναι συστήματα αντιδραστικής φύσης, δηλαδή έχουν τη δυνατότητα να αντιδράσουν σε ερεθίσματα (π.χ. επιθέσεις) επιφέροντας αλλαγές στην κατάσταση του δικτύου του οργανισμού. Το γεγονός ότι έχουν τη δυνατότητα να επεξεργαστούν δεδομένα ώστε να αντιληφθούν τη δράση μίας επίθεσης αλλά και να εφαρμόσουν μέτρα βάσει αυτής της επεξεργασίας τα κάνει να θεωρούνται «έξυπνα» συστήματα.

Τα IPS εκτελούν έλεγχο πακέτων σε πραγματικό χρόνο, επιθεωρώντας σε βάθος κάθε πακέτο που ταξιδεύει μέσω του δικτύου. Εάν εντοπιστούν κακόβουλα ή ύποπτα πακέτα, το IPS θα πραγματοποιήσει μία ή παραπάνω από τις ακόλουθες ενέργειες:

- **Θα σταματήσει την προώθηση της κίνησης των πακέτων**.

Ένα IPS τοποθετημένο σωστά στο δίκτυο του οργανισμού βρίσκεται ενδιάμεσα της πορείας που ακολουθούν τα πακέτα του δικτύου που χρειάζεται να ασφαλιστούν. Αν κάποιο από αυτά τα πακέτα θεωρηθεί ανασφαλές, τότε το IPS «πετάει» το πακέτο ώστε να μην επηρεάσει περισσότερους πόρους του δικτύου.

- **Θα ενημερώσει του διαχειριστές του δικτύου.**

Η ενημέρωση των διαχειριστών είναι η διαδικασία που εξετάσαμε νωρίτερα για τα συστήματα ανίχνευσης εισβολών, και υλοποιείται με τους ίδιους τρόπους. Τα συστήματα πρόληψης εισβολών νέας γενιάς, που θα εξετάσουμε σε επόμενο κεφάλαιο, δίνουν νέες δυνατότητες ενημέρωσης, όπως ειδοποίηση σε τηλεφωνική συσκευή με τη μορφή μηνύματος ή ειδοποίηση μέσω κάποιου αισθητήρα ή ενεργοποιητή (actuator) στην περίπτωση ενσωμάτωσης με δίκτυα και συσκευές διαδικτύου των πραγμάτων (Internet Of Things ή IOT).

- **Θα τερματίσει την καθιερωμένη σύνδεση TCP μεταξύ πηγής και προορισμού.**

Στην περίπτωση που η κίνηση είναι πρωτοκόλλου TCP και όχι UDP, μία ασφαλής σύνδεση χρειάζεται να καθιερωθεί μεταξύ δύο συσκευών για την ανταλλαγή πακέτων μεταξύ τους. Η σύνδεση αυτή χρησιμοποιείται για όσο οι συσκευές ανταλλάσσουν πακέτα, ενώ παράμετροί της αλλάζουν ανάλογα τις συνθήκες (π.χ. window size). Τα συστήματα πρόληψης εισβολών καταρρίπτουν τη σύνδεση TCP σταματώντας έτσι την προώθηση κίνησης μεταξύ των δύο συσκευών αν ανιχνεύσουν ύποπτη κίνηση.

- **Θα σταματήσει τη συσκευή-πομπό από την προώθηση μηνυμάτων.**

Το IPS μπορεί να θεωρήσει τη συσκευή που έστειλε την ύποπτη κίνηση ως «μολυσμένη», αποκόπτοντας την από το υπόλοιπο δίκτυο του PIN, μη προωθώντας τα πακέτα που προέρχονται από αυτήν. Αυτή η ενέργεια μπορεί να ρυθμιστεί από το διαχειριστή όσον αφορά το χρόνο που το IPS θα καθιστά την συσκευή «μολυσμένη».

Με αυτόν τον τρόπο ο διαχειριστής ελέγχει την προώθηση της κίνησής της είτε μετά από συγκεκριμένο χρονικό διάστημα είτε μόνο μετά την δική του παρέμβαση στη συσκευή πρόληψης εισβολών. Στην περίπτωση των συσκευών IPS επόμενης γενιάς η κίνηση μπορεί να μπλοκαριστεί όχι μόνο βάσει διεύθυνσης συσκευής, αλλά και βάση ταυτότητας χρήστη. Απαραίτητη για την υλοποίηση αυτής της δυνατότητας είναι η επικοινωνία του IPS με του διακομιστές ελέγχου τομέα του οργανισμού (Domain Controllers) συνήθως μέσω Microsoft Active

Directory ή με του διακομιστές πρόσβασης δικτύου (NAC Servers) μέσω της χρήσης του πρωτοκόλλου Radius.

- **Θα αφαιρέσει τυχόν κακόβουλο περιεχόμενο που παραμένει στο δίκτυο μετά από μια επίθεση.**

Η διαδικασία αυτή υλοποιείται ανασυσκευάζοντας τις πληροφορίες χρήστη (payload) στα πακέτα του δικτύου, αφαιρώντας πληροφορίες κεφαλίδας (header information) και τυχόν μολυσμένα συνημμένα από διακομιστές αρχείων ή email.

- **Θα ενημερώσει το τείχος προστασίας.**

Τα συστήματα IPS συχνά είναι σε συνεχή επικοινωνία με το τείχος προστασίας του PIN του οργανισμού και μπορούν να ανταλλάξουν πακέτα με αυτό αλλά και να το επαναπρογραμματίσουν ή διαμορφώσουν αντίστοιχα (π.χ. προσθέτοντας πολιτικές λειτουργίας) για να αποτρέψουν αντίστοιχη επίθεση στο μέλλον.

3.3 Διαφορές συστημάτων πρόληψης με συστήματα ανίχνευσης εισβολών

3.3.1 Διαφορά στον τρόπο δράσης

Όπως αναφέραμε παραπάνω, τα συστήματα πρόληψης εισβολών «κληρονόμησαν» τις λειτουργίες των συστημάτων ανίχνευσης εισβολών. Αυτό σημαίνει πως τα IPS έχουν ως βάση τα ίδια πεδία λειτουργίας, στόχους και εργαλεία των IDS στη διάθεσή τους.

Παράλληλα όμως, τα συστήματα πρόληψης εισβολών είναι σαφώς πιο ολοκληρωμένα συστήματα καθώς έχουν τη δυνατότητα να επηρεάσουν την κίνηση του δικτύου, πέρα από να την αναγνωρίσουν. Για να αποκτήσουν αυτή τη δυνατότητα, κάνουν χρήση επιπλέον λογισμικού και συχνά υλικού (π.χ. περισσότερους ή δυνατότερους επεξεργαστές για ταχύτερη επεξεργασία πακέτων, περισσότερες κάρτες δικτύου για δυνατότητα περισσότερων ζεύξεων κ.α.).

Συνήθως τα IPS χρησιμοποιούν παρόμοιο λογισμικό με τα IDS ή αποτελούνται από δύο σχεδόν αυτοτελή τμήματα, την «μηχανή» (engine) IDS και το λογισμικό που τους δίνει τη δυνατότητα να φιλτράρουν την κίνηση συλλέγοντας πρώτα στοιχεία και στατιστικά για αυτήν. Συνεπώς, τα IPS έχουν εν δυνάμει ενεργό ρόλο στην ασφάλιση του δικτύου του οργανισμού, ενώ τα IDS αποτελούν ένα παθητικό μηχανισμό παρακολούθησης, που απαραίτητη για τη χρηστικότητά του είναι η δυνατότητα ανθρώπινης παρέμβασης.

Εν κατακλείδι, η βασικότερη διαφορά μεταξύ των δύο ειδών συστημάτων είναι πως ένα IDS είναι στατικό στη φύση του. Παρακολουθεί την κίνηση του δικτύου και σε περίπτωση ύποπτης δραστηριότητας μπορεί μόνο να στείλει ειδοποιήσεις στους διαχειριστές. Αντίθετα, ένα IPS όχι μόνο ειδοποιεί, αλλά μπορεί επίσης να λάβει μέτρα για τον μετριασμό του προβλήματος.

Επομένως, η απάντηση στο πότε απαιτείται η ενσωμάτωση ενός IPS για τη λήψη διορθωτικών ενεργειών στο δίκτυο του οργανισμού πηγάζει από το εκτιμητέο επίπεδο του πιθανού κινδύνου. Μια λύση IPS παρέχει τη δυνατότητα λήψης διορθωτικών ενεργειών προτού ο διαχειριστής συστήματος έχει την ευκαιρία να ανταποκριθεί, κάτι που μπορεί να είναι επιθυμητό κατά τη διάρκεια μιας ενεργής επίθεσης εναντίον συστημάτων.

Αξίζει να σημειωθεί πως κανένα σύστημα δεν είναι αλάθητο και η λειτουργία ενός IPS στο δίκτυο ενός οργανισμού χωρίς ανθρώπινη παρέμβαση, είναι δυνατόν να προκαλέσει σφάλμα τύπου I (ή ψευδώς θετικό) και να αποκλείσει τη «νόμιμη» κίνηση από χρήστες του δικτύου PIN του οργανισμού. Ταυτόχρονα όμως, πολλοί τύποι επίθεσης είναι σαφώς ορισμένοι και αφήνουν συγκεκριμένο δικτυακό αποτύπωμα, συνεπώς μπορούν εύκολα να αποκλειστούν αποτελεσματικά με τη χρήση ενός IPS.

3.3.2 Διαφορά στη θέση στο δίκτυο

Μία ακόμη βασική διαφορά μεταξύ των αρχιτεκτονικών δικτύων που η ασφάλειά τους βασίζεται σε συστήματα ανίχνευσης εισβολών με αυτών που η ασφάλειά τους βασίζεται

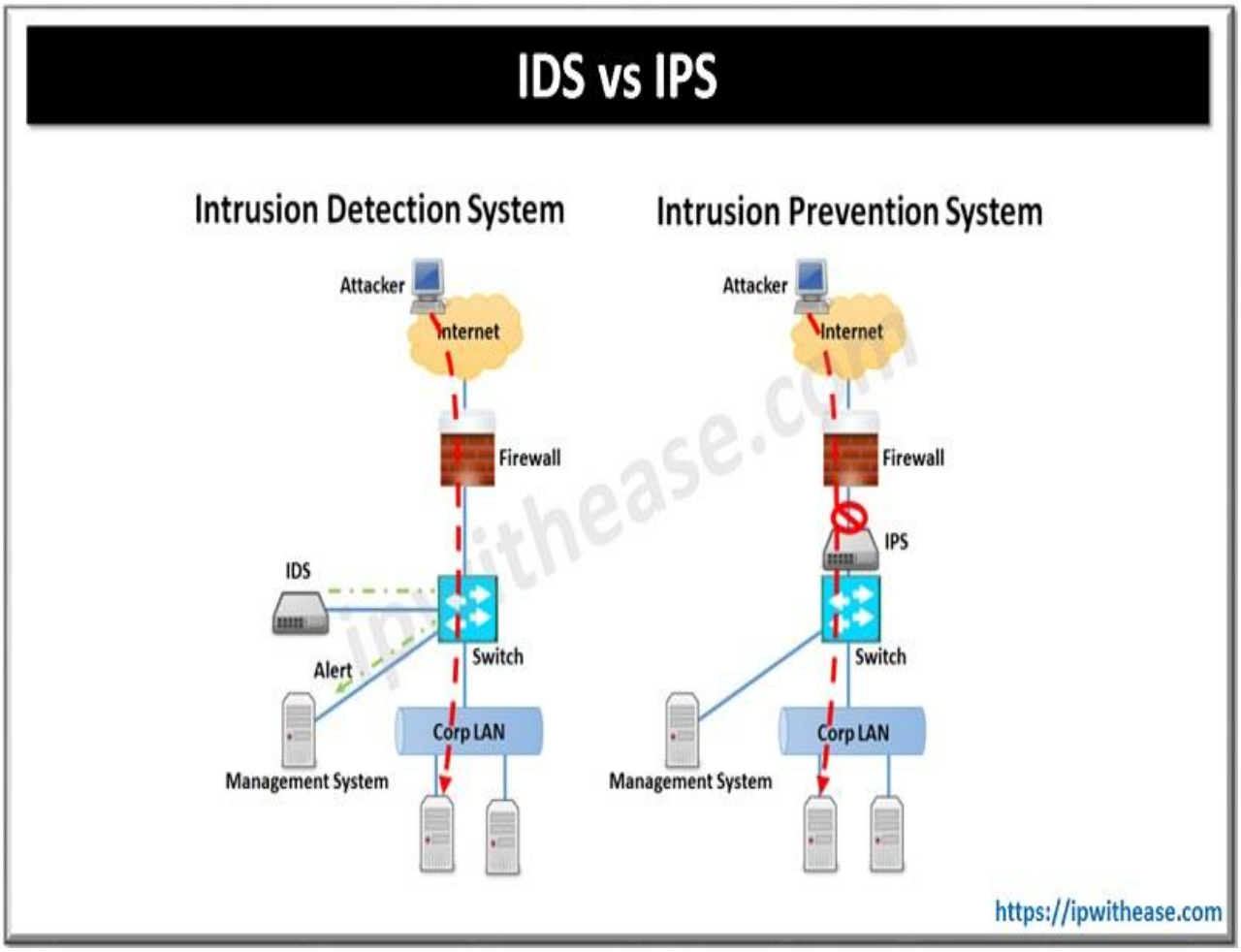
σε συστήματα πρόληψης εισβολών είναι η θέση των επίμαχων συσκευών. Όπως αναφέραμε αρκετές φορές ήδη, τα IDS δεν μπορούν να λειτουργήσουν ενεργά για να προστατέψουν το δίκτυο και συνεπώς τοποθετούνται παράλληλα στις ζεύξεις που υποστηρίζουν τον όγκο της δικτυακής κίνησης του PIN που χρήζει προστασίας. Αυτό συμβαίνει διότι αν βρίσκονταν στην πορεία της (Inline) θα την καθυστερούσαν περαιτέρω χωρίς να έχουν δυνατότητα επέμβασης.

Από την άλλη μεριά, τα IPS για να λειτουργήσουν ιδεατά, προσφέροντας δυνατότητα αυτόματης επέμβασης στην ασφάλεια του δικτύου του οργανισμού, πρέπει να τοποθετηθούν στην πορεία της κίνησης αυτής. Η καθυστέρηση που αναφέραμε νωρίτερα ως λόγο αργής ενσωμάτωσης των συσκευών πρόληψης εισβολών στα σύγχρονα δίκτυα οφείλεται σε αυτή τη διαφορά αρχιτεκτονικής.

Η καθυστέρηση που επιφέρουν συσκευές IPS στην κίνηση των πακέτων στο δίκτυο είναι όλο και λιγότερο αισθητή. Αυτό συμβαίνει διότι υπάρχουν συνεχείς βελτιώσεις στα συστήματα (π.χ. ταχύτητας επεξεργαστή, μνήμης και καρτών δικτύου) των IPS αλλά και στις ταχύτητες των δικτυακών ζεύξεων (καλώδια ethernet, οπτικές ίνες, υποδοχείς sfp). Καθώς το IPS θα πρέπει να βρίσκεται στην πορεία του μεγαλύτερου όγκου της κίνησης του PIN ώστε να την εξετάζει επαρκώς, είναι σημαντικό να είναι συνδεδεμένο με ζεύξεις μεγάλης ταχύτητας με τους υπολοίπους πόρους του δικτύου, συχνά πολλαπλές, με χρήση τεχνολογιών συγκέντρωσης ζεύξεων (link aggregation).

Στην παρακάτω εικόνα φαίνεται η διαφορά αυτή, επισημαίνοντας τη δυνατότητα του IPS να απορρίπτει ύποπτη κίνηση.

Εικόνα 3.1 Τυπική θέση IDS και IPS.



3.3.3 Διαφορά στους τρόπους ανίχνευσης ύποπτης κίνησης

Τα IPS, έχοντας κατά κόρον κοινές λειτουργίες με τα IDS, χρησιμοποιούν παρόμοιους τρόπους ανίχνευσης ύποπτης κίνησης με αυτούς που εξετάσαμε σε προηγούμενο κεφάλαιο. Οι τρόποι αυτοί είναι οι παρακάτω:

1. **Τρόπος ανίχνευσης βάσει υπογραφής (Signature-Based).**

Η προσέγγιση βάσει υπογραφής χρησιμοποιεί προκαθορισμένες υπογραφές γνωστών απειλών δικτύου. Οι υπογραφές αυτές υπάρχουν στη βάση δεδομένων του συστήματος πρόληψης εισβολών, η οποία ενημερώνεται από διακομιστές στο διαδίκτυο τόσο του κατασκευαστή όσο και άλλων οργανισμών. Όταν ξεκινά μια επίθεση, το IPS προσπαθεί να καταλάβει αν ταιριάζει με μία από αυτές τις υπογραφές ή μοτίβα, και στη συνέχεια το σύστημα λαμβάνει τα απαραίτητα μέτρα.

Είναι σημαντικό να σημειωθεί πως τεχνικές επίθεσης οι οποίες έχουν εξελιχθεί ή διαμορφωθεί πρόσφατα, με υπογραφή άγνωστη ως προς το σύστημα πρόληψης εισβολών συχνά παρακάμπτουν τις άμυνές του, καθώς δεν μπορεί να τις ταιριάξει με τις παλαιότερες υπογραφές που αναγνωρίζει μέσω της βάσης δεδομένων που χρησιμοποιεί. Συνεπώς, ένα σύστημα πρόληψης εισβολών που χρησιμοποιεί αποκλειστικά τρόπο ανίχνευσης βάσει υπογραφής καθιστά δύσκολη την ανίχνευση προηγουμένως άγνωστων απειλών και δεν προστατεύει πάντα επαρκώς από αυτές.

2. Τρόπος ανίχνευσης βάσει ανωμαλίας (Anomaly-Based).

Η προσέγγιση βάσει ανωμαλίας χρησιμοποιεί προκαθορισμένες μορφές δικτυακής κίνησης που προκύπτουν από συγκεκριμένες επιθέσεις στο δίκτυο. Όπως και στην ανίχνευση βάσει υπογραφής, στοιχεία για την ταυτοποίηση αυτών των μορφών υπάρχουν τόσο στη βάση δεδομένων του τοπικού συστήματος όσο και σε εξωτερικές βάσεις.

Πολλά IPS, στην περίπτωση που δεν μπορούν να βρουν τα απαραίτητα στοιχεία στην τοπική τους βάση δεδομένων συμβουλεύονται σε πραγματικό χρόνο τους παραπάνω διακομιστές και άλλες προκαθορισμένες από τον κατασκευαστή ομάδες ασφαλείας (π.χ. Advanced Malware Protection Community, Advanced Microsoft and Industry disclosures, Cisco Talos, κ.α.). Σε τέτοια περίπτωση, τα IPS απορρίπτουν την ύποπτη κίνηση περιμένοντας την ετυμηγορία των εξωτερικών πηγών που συμβουλεύεται.

Είναι σημαντικό να σημειωθεί πως τα IPS που βασίζονται αποκλειστικά στον τρόπο ανίχνευσης βάσει ανωμαλίας έχουν μη βέλτιστη λειτουργία όταν αντιμετωπίζουν άγνωστη συμπεριφορά. Οι μεγάλες αλλαγές στη δικτυακή ροή συχνά αναγνωρίζονται ως ανωμαλία ανεξάρτητα με το αν είναι προϊόντα επίθεσης ή όχι. Συνεπώς, οποιαδήποτε αλλαγή στην αρχιτεκτονική του δικτύου, είτε αυτή αφορά προσθήκη ή αφαίρεση φυσικού εξοπλισμού, είτε προσθήκη, αφαίρεση ή παραμετροποίηση λογισμικού διακομιστών ή συσκευών δικτύου, γίνεται ακόμη πιο σύνθετη λόγω της συσκευής πρόληψης εισβολών.

3. Τρόπος ανίχνευσης βάσει πολιτικής (Policy-Based):

Για τα IPS υπάρχει και ένας τρίτος τρόπος ανίχνευσης απειλών στο δίκτυο, υλοποιούμενος είτε σε συνεργασία με άλλα συστήματα είτε ανεξάρτητα από αυτά. Ο τρόπος αυτός είναι η ανίχνευση εισβολών βάσει πολιτικής και είναι ο μόνος που διαφέρει αισθητά ως προς την υλοποίηση του από οργανισμό σε οργανισμό.

Αυτή η προσέγγιση τυπικά δεν υποστηρίζεται από τα συστήματα ανίχνευσης εισβολών και θεωρείται η πιο εκλεπτυσμένη και προσαρμόσιμη στα μέτρα του οργανισμού. Απαιτεί από τους διαχειριστές του οργανισμού να διαμορφώσουν πολιτικές ασφαλείας σύμφωνα με την οργάνωση και την υποδομή του δικτύου και να αποθηκευτούν είτε στο IPS είτε σε αντίστοιχο σύστημα, όπως το τείχος προστασίας (ανάλογα με τη λύση του κάθε κατασκευαστή). Κατά τη συγκεκριμένη υλοποίηση το IPS με τη βοήθεια των διαχειριστών αποκτά ολοκληρωμένη εικόνα του PIN του δικτύου του οργανισμού στο οποίο βρίσκεται και βαθιά κατανόηση των δικτυακών ροών πακέτων. Συλλέγει στατιστικά για τα πρωτόκολλα που χρησιμοποιούνται στο δίκτυο και χρησιμοποιώντας έξυπνους μηχανισμούς ορίζει περιθώρια απόκλισης φυσιολογικής λειτουργίας που θεωρεί ανεκτά, προβλέποντας εξαιρετικές περιπτώσεις που μπορεί να προκύψουν.

Τα IPS επόμενης γενιάς μπορούν ακόμη να συνδυάσουν συγκεκριμένου τύπου κίνηση με κάποιο χρήστη του οργανισμού αλλά και να δημιουργήσουν αντιστοιχήσεις συσκευών-χρηστών, αποθηκεύοντας όλες τις συσκευές που χρησιμοποιούνται ή ανήκουν σε συγκεκριμένο χρήστη στο ίδιο προφίλ (εξαιρετικά χρήσιμο σε οργανισμούς που κάνουν χρήση πολιτικών «bring your own device»).

Ο τρόπος ανίχνευσης βάσει πολιτικής επιφέρει σημαντικό φόρτο εργασίας στους διαχειριστές κατά την εγκατάσταση του συστήματος πρόληψης εισβολών στο δίκτυο του οργανισμού αλλά και με κάθε αλλαγή στην αρχιτεκτονική του, καθώς πρέπει ξανά να οριστεί το προφίλ του PIN του δικτύου του οργανισμού και να υπάρξει ενημέρωση στο IPS για τις αντίστοιχες πολιτικές ασφαλείας που ακολούθησαν την αλλαγή. Παράλληλα όμως, είναι ο πιο αποδοτικός τρόπος ανίχνευσης απειλής σε περίπτωση που αυτή είναι άγνωστη προς το σύστημα πρόληψης εισβολών, διότι δεν βασίζεται στην αναγνώρισή της μέσω μίας βάσης δεδομένων αλλά και ούτε στο ότι αυτή θα επιφέρει ανωμαλίες στο προφίλ της κίνησης του PIN του δικτύου του οργανισμού.

Τα σύγχρονα συστήματα πρόληψης εισβολών χρησιμοποιούν πάνω από μία από τις παραπάνω μεθόδους για την ανίχνευση απειλών, και σε αυτά συχνά αναφερόμαστε ως υβριδικά συστήματα. Τα υβριδικά συστήματα λειτουργούν ανιχνεύοντας ανωμαλίες στο σύστημα και δημιουργώντας δυναμικά υπογραφές που αντιστοιχούν σε κάθε μία από αυτές. Με αυτό τον τρόπο, συμπληρώνουν τη βάση δεδομένων τους, διατηρώντας ιστορικότητα και έχοντας τη δυνατότητα να αναγνωρίσουν επαναλαμβανόμενα άγνωστα μοτίβα ανωμαλιών, χωρίς να τα αντιμετωπίζουν σαν αποτελέσματα επιθέσεων δημιουργώντας ψευδώς θετικά σφάλματα.

3.4 Εξέλιξη Συστημάτων Πρόληψης Εισβολών

Τα τελευταία χρόνια, καθώς οι τεχνολογίες που χρησιμοποιούν τα παραδοσιακά IPS έχουν παγιωθεί και γίνει γνωστές από τους επίδοξους χάκερ, αναδύονται όλο και πιο σύνθετες και εκλεπτυσμένες μορφές απειλών και επιθέσεων που απειλούν τα σύγχρονα δίκτυα. Καθώς τα παραδοσιακά συστήματα πρόληψης εισβολών χρησιμοποιούσαν τακτικές στατικής χρονικά ανίχνευσης (static point-in-time detection) στην ουσία πάντα «κυνηγούσαν» τους επιτιθέμενους προσπαθώντας να ενημερώνονται για τις επιτυχείς επιθέσεις και να προστατεύονται από αυτές πριν στοχοποιηθούν τα PIN του δικτύου του οργανισμού στα οποία ανήκουν. Στην πραγματικότητα, αυτή η διαδικασία βασίζεται σε μεγάλο βαθμό στην ενημέρωση των συστημάτων από τους κατασκευαστές τους, μόνο λαμβάνοντας δεδομένα και βρίσκοντας τις αδυναμίες αυτών μετά από επιτυχείς επιθέσεις.

Ο παράγοντας της τύχης στην εξίσωση είναι σημαντικός, καθώς η όλη λογική ασφαλείας που πρόσφεραν τα συστήματα πρόληψης εισβολών στο δίκτυο του οργανισμού βασιζόταν στο να είναι άλλοι οργανισμοί οι πρώτοι στόχοι μιας καινοτόμας επίθεσης. Έτσι, αναλύονταν οι αδυναμίες που αποδείχθηκαν εκμεταλλεύσιμες και το σύστημα οχυρωνόταν, μέχρι να προκύψει η επόμενη καινοτόμα απειλή.

Η λογική αυτή δεν ικανοποιούσε την αγορά, καθώς σήμαινε πως τα IPS δεν μπορούν πάντα να παρέχουν αξιόπιστη προστασία στο δίκτυο του οργανισμού, και κάθε φορά που οι επίδοξοι χάκερ εφεύρισκαν μία καινούρια τεχνική επίθεσης μεσολαβούσε χρόνος μέχρι να φτάσει η αντίστοιχη ενημέρωση ασφαλείας στο σύστημα.

Παράλληλα, το λογισμικό αλλά και υλικό που χρησιμοποιούσαν τα παραδοσιακά IPS ήταν είτε εκμεταλλεύσιμο και επιρρεπές σε τεχνικές εξαπάτησης είτε ανίκανο να εφαρμόσει πλήρως τις σύνθετες και απαιτητικές σε πόρους λύσεις που έχρηζε απαραίτητη η προσπάθεια αποδοτικής άμυνας στις όλο και πιο έξυπνες και ραφιναρισμένες απειλές προς το δίκτυο.

Οι πιο διαδεδομένες λύσεις που εφαρμόστηκαν για να αντιμετωπίσουν τα παραπάνω προβλήματα είναι δύο.

- Ενσωμάτωση λειτουργιών πρόληψης εισβολών σε δικτυακές συσκευές διαφορετικού τύπου, δημιουργώντας πιο πολλά σημεία ελέγχου της δικτυακής κίνησης (πλέγματα ασφαλείας).

- Διαρκής εξέλιξη των εργαλείων και δυνατοτήτων των συστημάτων πρόληψης εισβολών με αποτέλεσμα την δημιουργία συσκευών της κατηγορίας IPS επόμενης γενιάς.

3.5 Συσκευές δικτύου με δυνατότητες πρόληψης εισβολών

Σύμφωνα με την παραδοσιακή αρχιτεκτονική δικτύων που χρησιμοποιούν IPS για την κάλυψη των αναγκών ασφαλείας τους, η θέση αυτών είναι κοντά στην «άκρη»

του δικτύου του PIN, και συνήθως είναι άμεσα συνδεδεμένο με το τείχος προστασίας. Η αρχιτεκτονική αυτή είναι αποδοτική, καθώς ελέγχεται όλη η κίνηση που εισέρχεται και εξέρχεται από το δίκτυο, όμως δεν καλύπτει επαρκώς όλα τα πιθανά ευάλωτα σημεία στο δίκτυο του PIN του οργανισμού.

Αυτό γίνεται προφανές αν συλλογιστούμε πως η κίνηση μέσα στο δίκτυο, και ειδικότερα μέσα στο ίδιο VLAN (layer 2 traffic με βάση την αρχιτεκτονική OSI), δεν «περνάει» από το τείχος προστασίας, το οποίο αποτελεί το όριο επιπέδου δικτύου (layer 3 boundary). Συνεπώς, οποιαδήποτε επιβλαβής κίνηση για το δίκτυο μεταφέρεται τοπικά, δεν ανιχνεύεται από το σύστημα πρόληψης εισβολών. Έτσι εκείνο αδυνατεί να αντιδράσει σε αυτήν. Παρόμοιες περιστάσεις συναντάμε στην περίπτωση διάδοσης πακέτων μέσα στο ασύρματο δίκτυο (wireless) ή και από το ενσύρματο στο ασύρματο και ανάποδα.

Επιπλέον, συνήθως το δίκτυο ενός οργανισμού αποτελείται από πολλά VLANS, με το Firewall να αποτελεί το κομβικό σημείο σύνδεσης αυτών, ώστε να μπορεί να πραγματοποιεί έλεγχο πακέτων. Σε αυτή την περίπτωση είναι αδύνατο να ασφαλιστούν όλα αυτά τα υποδίκτυα με τη χρήση μίας μοναδικής συσκευής πρόληψης εισβολών, ενώ το κόστος (τόσο φυσικό όσο και διαχειριστικό) ενσωμάτωσης μίας σε κάθε VLAN καθιστά αυτή την τεχνική απαγορευτική, ειδικά για τους οργανισμούς που χρησιμοποιούν εκατοντάδες ή χιλιάδες VLAN στα μεγαλύτερα PIN τους.

Όλα αυτά τα πολύ σύνθετα ερωτήματα απαντήθηκαν με την ενσωμάτωση λειτουργιών πρόληψης εισβολών σε συσκευές σημείων πρόσβασης (Access Points), χειριστές ασύρματου δικτύου (Wireless Controllers ή WLCs), τείχη προστασίας επόμενης γενιάς (next generation firewalls ή NGFWs), σταθμούς διαχείρισης δικτύου

(Network Management System ή NMS) και χειριστές δικτύωσης καθοριζόμενης από λογισμικό (Software Defined Network ή SDN Controllers).

- **Δυνατότητες πρόληψης εισβολών σε Access Points (APs):**

Τα Access Points αποτελούν τις συσκευές επιπέδου πρόσβασης (access layer) για τους ασύρματους χρήστες στο δίκτυο του οργανισμού. Το ασύρματο τμήμα του δικτύου ενός οργανισμού συχνά συνδέει τόσο συσκευές του οργανισμού (laptops, sensors, actuators, κ.α.) όσο και προσωπικές συσκευές του προσωπικού του (laptops, smartphones, tablets, κ.α.) με το υπόλοιπο δίκτυο.

Παρέχοντας στα APs τη δυνατότητα να δρουν σαν συστήματα πρόληψης εισβολών ασφαλίζεται το ασύρματο δίκτυο και οι απειλές που μπορεί να το επηρεάσουν είτε μέσω επιθέσεων είτε μέσω σύνδεσης μολυσμένων συσκευών σε αυτό αντιμετωπίζονται πριν επηρεάσουν το υπόλοιπο δίκτυο του PIN του οργανισμού. Τα Access Points λειτουργούν είτε σε ελαφριά λειτουργία (lightweight mode) με μειωμένη δυνατότητα λήψης αποφάσεων και με τη βοήθεια του Wireless Controller, είτε αυτόνομα (autonomous APs), όμως και οι δύο τρόποι λειτουργίας σύγχρονων APs υποστηρίζουν δυνατότητες πρόληψης εισβολών.

- **Δυνατότητες πρόληψης εισβολών σε Χειριστές Ασύρματου Δικτύου (WLCs):**

Οι χειριστές ασύρματου δικτύου αποτελούν τα σημεία συνάντησης του ασύρματου με το ενσύρματο τμήμα του δικτύου του οργανισμού. Οι βασικές λειτουργίες τους είναι να προωθούν την ασύρματη κίνηση στο ενσύρματο δίκτυο, αλλά και να αποτελούν σημείο ελέγχου και διαχείρισης των APs και των συσκευών που συνδέονται ασύρματα στο δίκτυο του οργανισμού.

Συνήθως οι Wireless Controllers τοποθετούνται στα PINs campus και data center λόγω του ότι τείνουν να είναι τα σημεία με τα περισσότερα APs που πρέπει να υποστηριχθούν. Η παρουσία τους στα υπόλοιπα PINs συνήθως καθίσταται απαγορευτική λόγω κόστους, και η λειτουργία των APs των υπολοίπων PINS συνίσταται να είναι αυτόνομη (ή flex-connect) λόγω επιπλέον καθυστέρησης στην περίπτωση που πρέπει να προωθεί όλη την κίνηση μέσω ζεύξεων WAN με προορισμό τον WLC (που ανήκει σε άλλο PIN).

Παρέχοντας στους χειριστές ασύρματου δικτύου τη δυνατότητα να δρουν σαν συστήματα πρόληψης εισβολών, κάθε πιθανή απειλή που εμφανίζεται στο ασύρματο τμήμα του δικτύου του οργανισμού αντιμετωπίζεται πριν «περάσει» στο ενσύρματο τμήμα ή μολύνει ολόκληρο το ασύρματο υποδίκτυο (WLAN).

- **Δυνατότητες πρόληψης εισβολών σε τείχη προστασίας επόμενης γενιάς (NGFWs):**

Τα τείχη προστασίας επόμενης γενιάς αποτελούν εξελιγμένες συσκευές προστασίας του δικτύου του οργανισμού, που μπορούν να εξετάσουν τη δικτυακή κίνηση αρκετά πιο λεπτομερώς από τα παραδοσιακά τείχη προστασίας. Τα NGFWs μπορούν να ελέγξουν τα πακέτα όχι μόνο προς τις επικεφαλίδες (headers) αλλά και προς το ωφέλιμο φορτίο (payload) και να λάβουν σύνθετες αποφάσεις που δεν περιορίζονται στην αποδοχή ή απόρριψη του πακέτου.

Τα NGFWs έχουν περαιτέρω λειτουργίες όπως επίγνωση, ενημερότητα και έλεγχο κίνησης εφαρμογών στο δίκτυο, ενσωματωμένο σύστημα πρόληψης εισβολών και πρόσβαση σε πόρους του σύννεφου για απόκτηση πληροφοριών απειλών. Τέλος, παρέχουν περιβάλλοντα τύπου «sandbox» για τον έλεγχο απειλών σε πραγματικό χρόνο με τη χρήση ενός ασφαλούς, απομονωμένου περιβάλλοντος.

Βάσει των πιο διαδεδομένων αρχιτεκτονικών δικτύου των σύγχρονων οργανισμών, το τείχος προστασίας αποτελεί κομβικό σημείο ένωσης των υποδικτύων ενός PIN του οργανισμού. Αυτό συμβαίνει διότι έχοντας τέτοια θέση (κεντρική) το Firewall μπορεί να ελέγξει την κίνηση από και προς κάθε υποδίκτυο (εκτός από τις demilitarized ζώνες, σε περίπτωση που αυτές υπάρχουν). Η ενσωμάτωση συστημάτων πρόληψης εισβολών στο Firewall αποτελεί αποτελεσματικό τρόπο αύξησης του επιπέδου ασφαλείας του δικτύου,

καθώς συνεπάγεται την ύπαρξη IPS σε κάθε ζώνη του δικτύου του οργανισμού, κάτι που παλαιότερα λόγω κόστους ήταν συχνά αδύνατο.

- **Δυνατότητες πρόληψης εισβολών σε σταθμούς διαχείρισης δικτύου (NMS):**

Οι σταθμοί διαχείρισης δικτύου συνήθως αποτελούν είτε αφοσιωμένους διακομιστές (dedicated servers) είτε λογισμικό εγκατεστημένο σε αυτούς. Η τυπική τους χρήση αφορά την λήψη δικτυακών πληροφοριών από τις συσκευές δικτύου του οργανισμού (switches, routers, APs κ.α.) για την έγκαιρη ανίχνευση βλαβών.

Παράλληλα όμως, στην περίπτωση που ένα σύστημα NMS έχει δυνατότητες IPS, μπορεί να συλλέξει στοιχεία από τις παραπάνω συσκευές αλλά και το τείχος προστασίας του οργανισμού και να εκτελέσει διορθωτικές ενέργειες. Ο τρόπος που υλοποιείται αυτή η διαδικασία είναι σε συνεργασία με τις υπόλοιπες συσκευές, τις οποίες ρυθμίζει με τρόπο που απορρίπτει την ύποπτη κίνηση.

Ένα κοινό παράδειγμα τέτοιας ενέργειας αποτελεί την απόρριψη ύποπτης κίνηση ICMP (traceroute) για σκοπούς port-scanning από κάποια συσκευή στο δίκτυο. Όταν ο σταθμός διαχείρισης δικτύου αναγνωρίσει μεγάλα επίπεδα κίνησης ICMP σε πολλά διαδοχικά ports από μία συσκευή, μπορεί να

στείλει μία λίστα πρόσβασης στον άμεσα συνδεδεμένο μεταγωγέα κάνοντας τον να απορρίψει την κίνηση της μολυσμένης συσκευής.

- **Δυνατότητες πρόληψης εισβολών σε χειριστές δικτύωσης καθοριζόμενης από λογισμικό (SDN Controllers):**

Οι χειριστές δικτύωσης καθοριζόμενης από λογισμικό αποτελούν καινούρια τεχνολογία που λειτουργεί σε συνδυασμό με συγκεκριμένους μεταγωγείς δικτύου, αντίστοιχου τύπου. Οι μεταγωγείς αυτοί (SDN Switches) έχουν μειωμένη «νοημοσύνη» και δυνατότητα αυτόνομης δράσης, μπορούν όμως να κάνουν χρήση των δυνατοτήτων που τους προσφέρει ο SDN Controller, όντας σε συνεχή επικοινωνία μαζί του.

Ένας καλός τρόπος να αντιληφθούμε καλύτερα την παραπάνω αρχιτεκτονική είναι να την συγκρίνουμε με αυτή των Lightweight Access Points (LAPs) και του Wireless Controller. Τα SDN switches, μπορούν να δεχθούν εντολές και ρυθμίσεις από τον SDN Controller, με χρήση του οποίου μπορούμε να τα επηρεάσουμε κατά δεκάδες ή εκατοντάδες κάθε φορά. Πολλοί οργανισμοί, που το δίκτυο τους αποτελεί μεγάλος αριθμός δικτυακών συσκευών, βασίζονται στην χρήση των SDN Controllers για την γρήγορη και αξιόπιστη ρύθμισή του μειώνοντας την πιθανότητα ανθρώπινου λάθους.

Στην περίπτωση που ο SDN Controller έχει δυνατότητες IPS, αφού αναγνωρίσει ύποπτη συμπεριφορά από τις ροές δεδομένων που διαχειρίζεται

μέσω επικοινωνίας με τα SDN Switches μπορεί να ενημερώσει τους διαχειριστές, να ρυθμίσει πολιτικές στο Firewall αλλά και να ρυθμίσει τους μεταγωγείς να απορρίπτουν την ύποπτη κίνηση, ή και όλη την κίνηση από τις πιθανώς μολυσμένες συσκευές.

3.6 Συσκευές πρόληψης εισβολών επόμενης γενιάς (NGIPS):

Πλέον τα σύγχρονα δίκτυα των οργανισμών είναι όλο και μεγαλύτερα, αποτελούμενα από μεγάλο αριθμό δικτυακών συσκευών και πόρων πολλών διαφορετικών τύπων. Παρ' όλο που τα συστήματα ελέγχου και ορατότητας λειτουργιών και κατάστασης δικτύου είναι πλέον αρκετά διαδεδομένα και προσιτά σε σύγκριση με τα προηγούμενα χρόνια, η τακτική υλοποίηση ελέγχων ασφαλείας καθίσταται αδύνατη λόγω του διαχειριστικού βάρους που επιβάλλει σε τόσο μεγάλο όγκο συσκευών. Παράλληλα, όσο μεγαλύτερο είναι ένα δίκτυο, τόσο περισσότερα είναι και τα πιθανά ευάλωτα σημεία του.

Το παραπάνω, σε συνδυασμό με το ότι πολλοί τύποι επιθέσεων δημιουργούνται και εξελίσσονται συνεχώς ανάγκασε τους κατασκευαστές να κάνουν το επόμενο μεγάλο βήμα στην άμυνα των σύγχρονων δικτύων από επίδοξους εισβολείς, δηλαδή την δημιουργία έξυπνων, αυτόνομων συστημάτων που μπορούν να

διαχειριστούν και να σταματήσουν τη ζημία ακόμη και των πιο εξελιγμένων γνωστών και άγνωστων επιθέσεων. Τα συστήματα αυτά ονομάζονται συσκευές πρόληψης εισβολών επόμενης γενιάς.

Ο ορισμός των συσκευών πρόληψης εισβολών επόμενης γενιάς προκύπτει από τις λειτουργίες και δυνατότητες που πρέπει να έχει ένα σύστημα πρόληψης εισβολών για να θεωρηθεί μέλος της παραπάνω κατηγορίας. Σύμφωνα με τον ορισμό που δίνει η Garter Inc., τα NGIPS πρέπει να συμπεριλαμβάνουν λειτουργικότητα IPS, αλλά και να παρέχουν τις παρακάτω λειτουργίες:

- **Ενημερότητα κατάστασης δικτύου σε πραγματικό χρόνο:**

  Το σύστημα πρόληψης εισβολών επόμενης γενιάς πρέπει να είναι σε θέση να ανακαλύψει και να παρέχει ένα γενικό πλαίσιο πληροφοριών για τις εφαρμογές, χρήστες, συσκευές χρηστών και δικτύου, λειτουργικά συστήματα, ευπάθειες, υπηρεσίες, διαδικασίες, συμπεριφορές δικτύου, αρχεία και απειλές.

- **Προηγμένη προστασία και αποκατάσταση απειλών:**

  Το NGIPS πρέπει να εντοπίζει γρήγορα, μπλοκάρει, περιορίζει και αποκαθιστά προηγμένες απειλές μέσω ενσωματωμένου συστήματος

προηγμένης προστασίας από κακόβουλο λογισμικό (Advanced Malware Protection System ή AMPS) για δίκτυα και λύσεις sandboxing.

- **Έξυπνος αυτοματισμός ασφάλειας:**

Το NGIPS συσχετίζει αυτόματα ενδείξεις απειλών, πληροφορίες με βάση γενικό πλαίσιο και δεδομένα ευπάθειας δικτύου για να εκτελεί τα εξής:

  - Βελτιστοποίηση άμυνας με αυτοματοποίηση ενημερώσεων πολιτικών προστασίας (automated protection policy updates).

  - Γρήγορος εντοπισμός χρηστών που επηρεάζονται από μια επίθεση από την πλευρά χρηστών του οργανισμού (client-side attack).

  - Λήψη ειδοποιήσεων όταν ένας κεντρικός υπολογιστής παραβιάζει μια πολιτική διαμόρφωσης (configuration policy).

  - Ανίχνευση της εξάπλωσης κακόβουλου λογισμικού, δημιουργώντας μία βάση κανονικής κίνησης του δικτύου και εντοπίζοντας ανωμαλίες που προκύπτουν σε αυτό.

- Εντοπισμός και προσθήκη ετικετών (marking) σε συσκευές χρηστών και διακομιστές που ενδέχεται να παραβιαστούν από κακόβουλα μέσα (exploit kits, malware, command-and-control) με δείκτη συμβιβασμού (Indicator Of Compromise ή IoC).

- **Απαράμιλλη απόδοση και επεκτασιμότητα:**

Οι συσκευές NGIPS ενσωματώνουν ένα μονοφασικό (single-pass) σχέδιο χαμηλού χρόνου απόκρισης (low-latency), για πρωτοφανή απόδοση και επεκτασιμότητα.

- **Ορατότητα και έλεγχος εφαρμογών:**

Τα NGIPS μειώνουν τις απειλές μέσω της ανίχνευσης εφαρμογών. Τα περισσότερα NGIPS αναγνωρίζουν πάνω από 4000 εμπορικές εφαρμογές, με υποστήριξη για προσαρμοσμένες εφαρμογές. Ταυτόχρονα, μπορούν να περιορίσουν η να αποκόψουν τελείως τη δυνατότητα πιθανώς μολυσμένων συσκευών να τις χρησιμοποιήσουν, χωρίς να επηρεάσουν τη χρήση άλλων εφαρμογών.

- **Φιλτράρισμα διευθύνσεων URL:**

Οι συσκευές NGIPS πρέπει να παρέχουν έλεγχο πρόσβασης ιστότοπων και να καλύπτουν πολλαπλές κατηγορίες αυτών. Τα NGIPS πολλών κατασκευαστών παρέχουν έλεγχο για περισσότερες από 80 κατηγορίες διευθύνσεων και περισσότερες από 280 εκατομμύρια μεμονωμένες διευθύνσεις URL.

Επιπλέον, τα NGIPS πολλών κατασκευαστών ξεπερνούν τις παραπάνω δυνατότητες, έχοντας αυξημένες λειτουργίες και εργαλεία στην διάθεσή τους προς διευκόλυνση διαχείρισης, ενημέρωσης και εγκατάστασης, αποδοτικότερη προστασία από απειλές αλλά και αξιοπιστία και μείωσης της πιθανότητας χρόνου αργίας (downtime). Οι παρακάτω δυνατότητες χαρακτηρίζουν αυτά τα προτερήματα συστημάτων πρόληψης εισβολών επόμενης γενιάς πολλών κατασκευαστών:

- **Κεντρική διαχείριση:**

Ορισμένα NGIPS ελέγχονται κεντρικά από διαχειριστικά κέντρα, τα οποία παρέχουν ένα μονό παράθυρο επίβλεψης (single pane of glass architecture) για συλλογή πληροφοριών γεγονότων και διαχείριση πολιτικής.

- **Νοημοσύνη απειλών μέσω ενημέρωσης από το σύννεφο:**

Τα NGIPS που υποστηρίζουν αυτή τη δυνατότητα ενημερώνονται από ομάδες και οργανισμούς πληροφοριών απειλής. Έτσι, λαμβάνουν επικαιροποιημένες ενημερώσεις υπογραφών στη βάση δεδομένων τους, καθώς και πληροφορίες φιλτραρίσματος διευθύνσεων URL προς απόρριψη συνδέσεων προς ή από διευθύνσεις IP, διευθύνσεις ή και ονόματα τομέα (domain names).

- **Υψηλή διαθεσιμότητα (High Availability) και ομαδοποίηση (Clustering):**

Τα NGIPS συχνά μπορούν να χρησιμοποιηθούν ως ενεργά / σε κατάσταση αναμονής (μοντέλο active/standby) ή ομαδοποιημένα εντός πλαισίου (σε λειτουργία cluster). Και οι δύο αυτές τεχνικές χρησιμοποιούν πάνω από μία συσκευές NGIPS, η πρώτη για αξιοπιστία (συνέχιση λειτουργίας του δεύτερου NGIPS σε περίπτωση βλάβης του πρώτου) και η δεύτερη για αύξηση δυνατοτήτων επεξεργασίας δεδομένων (τεχνική resource pooling).

- **Υποστήριξη οικοσυστήματος δικτύου με λογισμικό πολλών κατασκευαστών αλλά και λογισμικό ανοιχτού κώδικα**:

Τα NGIPS συχνά διαθέτουν ανοιχτές διεπαφές προγραμμάτων εφαρμογής (API) για ενσωμάτωση με τα αντίστοιχα προϊόντα.

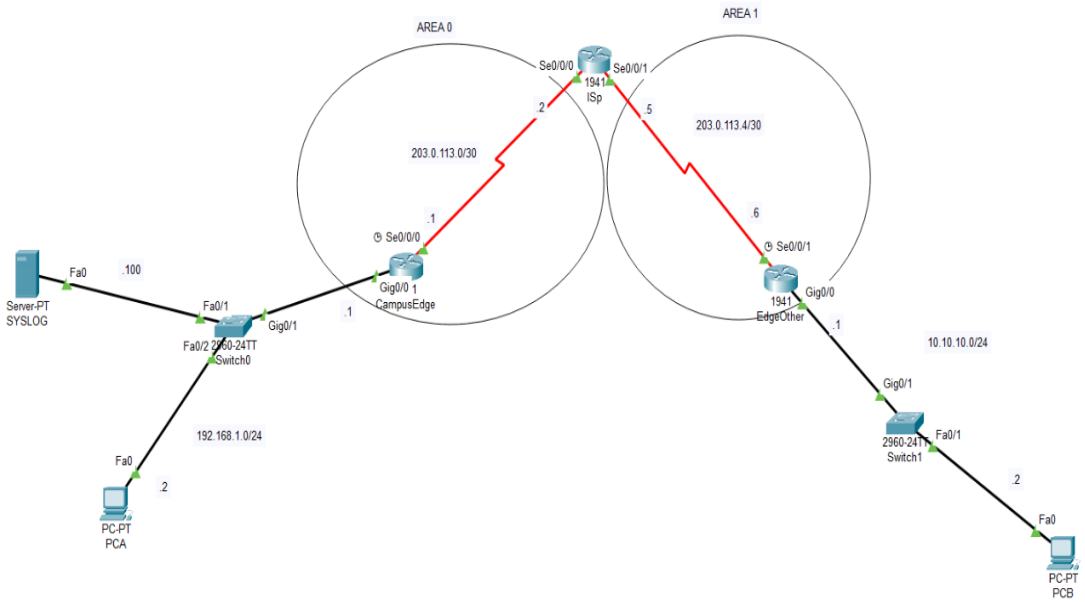
3.7 Προσομοίωση λειτουργίας συστήματος πρόληψης εισβολών:

Παρακάτω υπάρχει προσομοίωση λειτουργίας ενός συστήματος πρόληψης εισβολών με χρήση του λογισμικού προσομοίωσης δικτύων Cisco Packet Tracer. Κατά την υλοποίηση του σεναρίου που ακολουθεί, χρησιμοποιούνται δρομολογητές «Cisco 1941», μεταγωγείς «Cisco Catalyst 2960», προσομοιωμένα τερματικά υπολογιστών και προσομοιωμένος διακομιστής Syslog. Για την ολοκλήρωση του εργαστηρίου χρησιμοποιήθηκαν περαιτέρω εργαλεία και μονάδες που δεν συμπεριλαμβάνονται στην προκαθορισμένη μορφή του λογισμικού προσομοιωμένων συσκευών.

Το σενάριο που θα παρουσιάσουμε αφορά το PIN του campus του δικτύου ενός οργανισμού, το οποίο χρησιμοποιεί το δρομολογητή που ονομάσαμε «Campus Edge» για να συνδεθεί στο Internet (κάνοντας χρήση δημόσιας ή public IP). Ο δρομολογητής αυτός, έχει δυνατότητες IDS/IPS με χρήση υπογραφής.

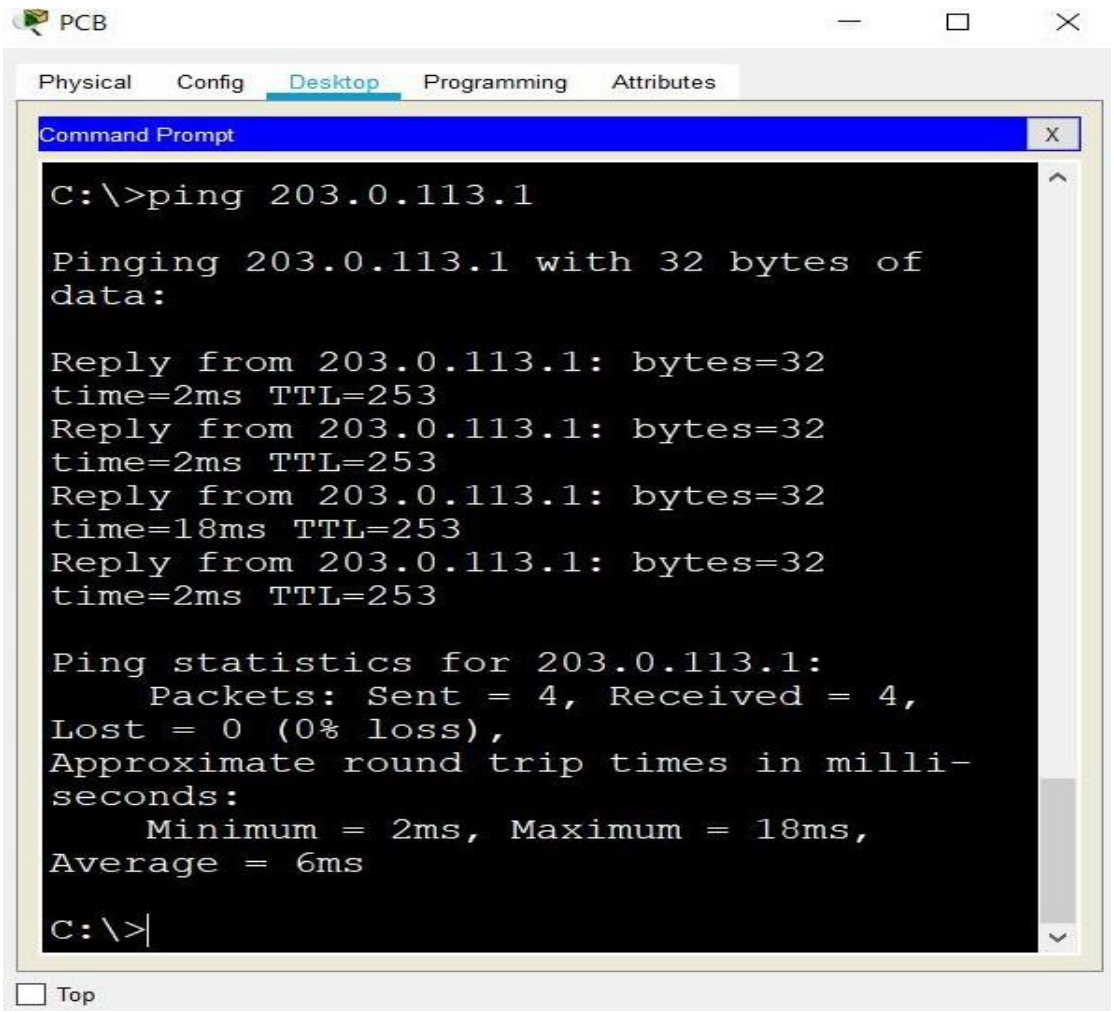
Ο επίδοξος εισβολέας χρησιμοποιεί τη συσκευή PCB και επιχειρεί ip scanning με χρήση ICMP (ping), για να εντοπίσει δρομολογητές οργανισμών που συνδέονται στο Internet, ώστε να πραγματοποιήσει password attack και να αποκτήσει πρόσβαση σε αυτούς. Μια τέτοια επίθεση είναι κοινότυπη, και «κάθε» δρομολογητής που έχει πρόσβαση στο Internet ίσως δέχεται δεκάδες από αυτές καθημερινά. Στην ουσία, όπως εξετάσαμε στο κεφάλαιο των PINS, αυτή είναι μία επίθεση στο PIN του δικτυακού άκρου.

Εικόνα 3.2 Τοπολογία Προσομοίωσης Σεναρίου



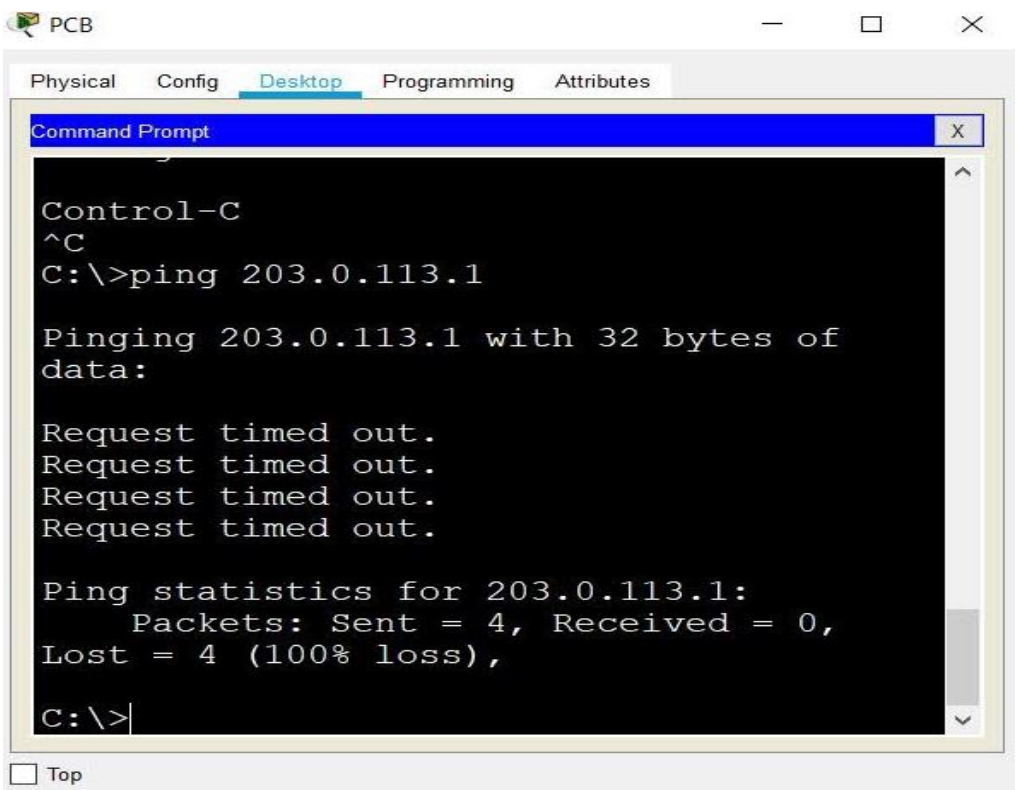
Κατά τη διαδικασία του scanning, ο επιτιθέμενος στέλνει πακέτο ICMP echo request στην δημόσια διεύθυνση του δρομολογητή CampusEdge. Στην περίπτωση που ο δρομολογητής δεν έχει κάποιο σύστημα ασφαλείας να τον προστατεύσει, απαντάει στα παραπάνω μηνύματα με πακέτα τύπου ICMP echo reply που αποδεικνύουν επιτυχή επικοινωνία και δείχνουν την διεύθυνσή του, όπως φαίνεται στην παρακάτω εικόνα.

Εικόνα 3.3 Μηνύματα ICMP Echo Reply στη συσκευή του επιτιθέμενου.



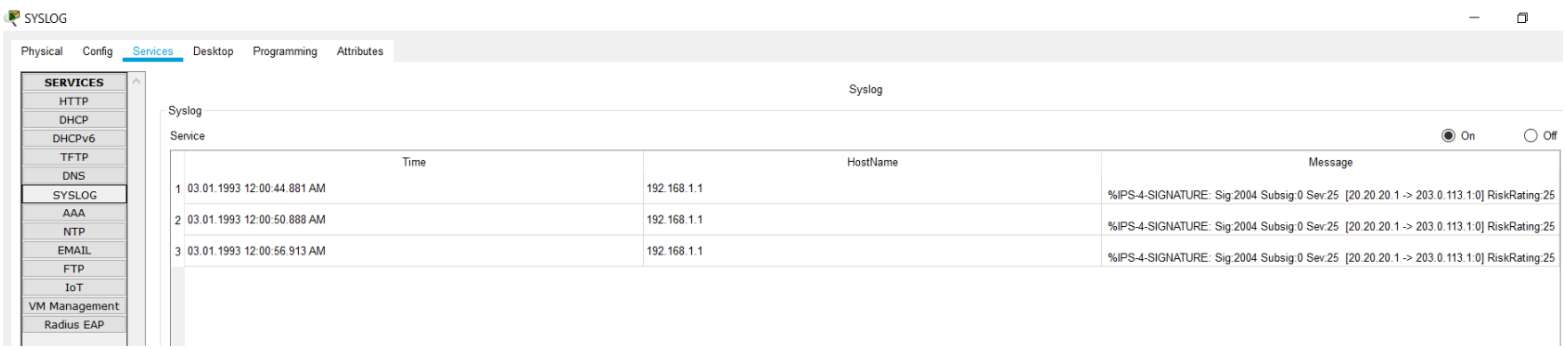
Με την ενίσχυση του δρομολογητή με δυνατότητες συστήματος πρόληψης εισβολών, ο δρομολογητής αγνοεί τα μηνύματα ICMP Echo Request του επιτιθέμενου και έτσι δεν του δίνει πληροφορίες για τη δημόσια διεύθυνσή του (η οποία δείχνει και την σχετική του θέση στο παγκόσμιο δίκτυο). Με αυτόν τον τρόπο, ο επιτιθέμενος, δεν αναγνωρίζει πως η διεύθυνση αυτή χρησιμοποιείται από κάποια συσκευή και δεν μπορεί να προετοιμάσει το έδαφος για κάποιο password attack σε αυτήν.

Εικόνα 3.4 Άρνηση αποστολής μηνυμάτων ICMP Echo Reply στη συσκευή του επιτιθέμενου από το δρομολογητή του οργανισμού.



Παράλληλα, ο δρομολογητής πρέπει να είναι ρυθμισμένος ώστε να ειδοποιεί το διακομιστή αποθήκευσης μηνυμάτων τύπου Syslog, και εν συνεχεία να γίνεται γνωστή στους διαχειριστές η προσπάθεια ύποπτης επικοινωνίας από εξωτερικές πηγές στο διαδίκτυο.

Εικόνα 3.5 Εγγραφές αναγνωρισμένων υπογραφών στο διακομιστή Syslog του οργανισμού



Όπως φαίνεται παραπάνω, ο διακομιστής Syslog (με διεύθυνση 192.168.1.100) έλαβε ενημέρωση από την εσωτερική διεύθυνση του δρομολογητή CampusEdge (192.168.1.1), πως δέχθηκε επίθεση στην δημόσια διεύθυνσή του (203.0.113.1), η οποία ταιριάζει με υπογραφή της βάσης δεδομένων του (2004:0), από τη δημόσια διεύθυνση 20.20.20.1. Η διεύθυνση αυτή είναι διαφορετική από τη δημόσια διεύθυνση του δρομολογητή του επιτιθέμενου (203.0.113.6) και χρησιμοποιείται για να δείξει πως οι επίδοξοι εισβολείς πραγματοποιούν τις επιθέσεις τους χρησιμοποιώντας ενδιάμεσους σταθμούς, συνήθως διακομιστές που υπάρχουν σε διεθνή ύδατα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία

CCNP and CCIE Enterprise Core ENCOR 350-401Official Cert Guide ISBN-13: 978-1-58714-523-0

CCNP and CCIE Security Core SCOR 350-701 Official Study Guide ISBN-13: 978-0135971970

Guide to Intrusion Detection and Prevention Systems (IDPS) ISBN-13 978-1494758813

Intrusion Detection and Prevention for Mobile Ecosystems ISBN-13 978-1-138-03357-3

Ιστοσελίδες

https://www.oreilly.com/library/view/defensive-security-handbook/9781491960370/ch19.html

https://blogs.arista.com/blog/evolution-from-pins-to-pics-cloud-networking

https://www.varonis.com/blog/ids-vs-ips/?fbclid=IwAR0ejWPA4wFxoKS6hG8R_Mt5vzI9RPNPZJUicGluQRy5lsEW13xmWrPmigg

https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

https://www.ciscopress.com/articles/article.asp?p=1336425

https://support.huawei.com/enterprise/en/doc/EDOC1100034077/cc2c0fe2/ips-configuration

https://www.juniper.net/documentation/en_US/jsa7.3.3/jsa-risk-manager-adapter-configuration-guide/topics/concept/concept-jsa-rm-cisco-ngips.html