«ΠΡΟΓΡΑΜΜΑ ΑΝΑΠΤΥΞΗΣ ΤΗΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΕΡΕΥΝΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΣΕ ΝΕΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ (ΠΑΒΕΤ-ΝΕ-2004)»

ΕΣΤΙΑ: «Μία ολοκληρωμένη πλατφόρμα ελέγχου ασφάλειας υπολογιστών και παροχής προστασίας στο Διαδίκτυο»

Παραδοτέο Π1.1: «Ανάλυση Απαιτήσεων»

Κωδικός Έργου: 04BEN8

Σύντομη περιγραφή: Στο έγγραφο αυτό παρουσιάζουμε τις απαιτήσεις των χρηστών για το εργαλείο ελέγχου ελλείψεων ασφαλείας που θα κατασκευαστεί στα πλαίσια του έργου ΕΣΤΙΑ καθώς και τις απαιτήσεις που πρέπει αυτό να πληροί. Παρουσιάζουμε διάφορα υπάρχοντα εργαλεία ελέγχου ασφάλειας και αναλύουμε τις δυνατότητές τους με σκοπό, συγκρίνοντας τα αποτελέσματα της ανάλυσης αυτής, να επιλέξουμε το εργαλείο που θα χρησιμοποιήσουμε στην ανάπτυξη του ΕΣΤΙΑ.

Προβλεπόμενη Ημερομηνία Παράδοσης	**30/06/2005**
Ημερομηνία Παράδοσης	**07/07/2005**
Επίπεδο Ασφάλειας Εγγράφου	**Δημόσιο Έγγραφο**
Συντελεστές	**Virtual Trip, FORTH**

Στο έργο ΕΣΤΙΑ συμμετέχουν οι φορείς:

Virtual Trip	Συντονιστής	Ελλάδα
FORTH	Συνεργάτης	Ελλάδα

Πίνακας Περιεχομένων

1. Απαιτήσεις Χρηστών

Στις παραγράφους που ακολουθούν παρουσιάζονται οι απαιτήσεις των χρηστών όπως αυτές διαμορφώθηκαν από ερωτηματολόγια και αλλά και προσωπικές επαφές. Ο δειγματικός χώρος των χρηστών καλύπτει το ευρύτερο φάσμα των χρηστών του διαδικτύου: Διαχειριστές Συστημάτων και Δικτύων, Ιδιοκτήτες Μ.Μ.Ε., υπάλληλοι Μ.Μ.Ε., "home users", "advanced users", … Οι κύριες απαιτήσεις μπορούν να ομαδοποιηθούν στις κατηγορίες «Απλότητας», «Χρηστικότητας» και «Λειτουργικότητας». Την πρώτη κατηγορία την ζητούσαν κυρίως οι «απλοί χρήστες» ενώ οι πιο ειδικευμένοι ζητούσαν επιπλέον λειτουργικότητα.

1.1. Απλότητα

Το σύστημα θα πρέπει:

- να είναι απλό στη χρήση για να χρησιμοποιηθεί από μη έμπειρους χρήστες.
- να έχει web interface και να μην απαιτεί την εγκατάσταση λογισμικού στα υπό εξέταση συστήματα.
- να υποστηρίζει την ελληνική γλώσσα.
- να παρέχει ακριβείς και βοηθητικές μεταφράσεις για τους αγγλικούς όρους.
- να δίνει απλά παραδείγματα και επαρκή βοήθεια για τους τεχνικούς όρους.
- να δίνει στον απλό χρήστη αναλυτικές οδηγίες για την επιδιόρθωση του ρήγματος ή κενού ασφάλειας. Πάντα όμως θα παρέχονται και τεχνικές λεπτομέρειες που θα μπορούν να αξιοποιηθούν από τον διαχειριστή του συστήματος ή από την ομάδα υποστήριξης του έργου, σε περίπτωση που δεν υπάρχει διαχειριστής (για παράδειγμα σε κάποιον «home user»).

1.2. Χρηστικότητα

Το σύστημα θα πρέπει:

- να παρέχει αναλυτικά reports, γραμμένα τόσο σε τεχνικό μέρος για τους διαχειριστές όσο και σε «απλά ελληνικά» για τους μη έμπειρους χρήστες.
- να εμφανίζει ένδειξη ολοκλήρωσης (progress bar).
- να παρέχει "wizards" για εφαρμογή τυπικών ελέγχων (παράδειγμα: έλεγχος για κενά ασφάλειας σε Windows® client, έλεγχος για κενά ασφάλειας σε Linux Server).

- να μπορεί να αποθηκεύσει τις ρυθμίσεις κάποιου χρήστη (sign in).

1.3. Λειτουργικότητα

Το σύστημα θα πρέπει:

- να μπορεί να ελέγξει ολόκληρα δίκτυα υπολογιστών.
- να *μην* επιτρέπει την «εξέταση» σε υπολογιστή όπου δεν έχουμε πρόσβαση.
- να μπορεί να ελέγξει υπολογιστές που βρίσκονται πίσω από εταιρικό firewall ή / και NAT.
- να αναγνωρίζει εάν ο υπολογιστής προς έλεγχο βρίσκεται πίσω από firewall ή / και NAT. Ένας χρήστης σπάνια γνωρίζει την τοπολογία του δικτύου του.
- να μπορεί να ελέγξει ένα ολόκληρο δίκτυο, παρέχοντας πληροφορίες για τυχόν κενά ασφάλειας στη σχεδίασή του (wireless access points, share points, share printers,κ.α.). Στην αναφορά που θα δίνει, θα πρέπει να μπορεί να προτείνει λύσεις (έστω τυποποιημένες) για την ασφαλή σχεδίαση ενός δικτύου.
- να μπορεί να ελέγξει οποιαδήποτε συσκευή «μιλάει» TCP/IP (ADSL routers, wireless access points, PC, servers).
- να δέχεται σαν είσοδο τα logs ενός server και να μπορεί να εξάγει χρήσιμα συμπεράσματα για τυχόν επιθέσεις. Το κομμάτι αυτό του συστήματος μπορεί να είναι ξεχωριστό λογισμικό και δεν χρειάζεται να καλύπτει τις απαιτήσεις των «τεσσάρων σημείων», της απλότητας και της χρήσης ελληνικών.

1.4. Άλλες απαιτήσεις

Το σύστημα θα πρέπει:

- να είναι διαρκώς και επαρκώς ενημερωμένο.
- να συνδυάζει την απαίτηση για ταχύτητα στην ολοκλήρωσή του αλλά και για ακριβή και αναλυτικό έλεγχο του υπό εξέταση υπολογιστή.
- να παρέχει τον source κώδικά του ώστε να μπορεί να ελεγχθεί για την «διακριτικότητά» του.
- να χρησιμοποιεί την βασική δομή των τεσσάρων σημείων (port scanner, service identifier, test generator, packet generator).

2. Απαιτήσεις Εργαλείων Διείσδυσης

Έχοντας συγκεντρώσει τις απαιτήσεις των χρηστών, έχουμε κάποιες κατευθύνσεις για τον καθορισμό των προδιαγραφών του προς ανάπτυξη συστήματος. Στις ακόλουθες παραγράφους αναλύουμε τις απαιτήσεις που επιθυμούμε να πληροί το εργαλείο διείσδυσης που θα επιλεγεί για την ανάπτυξη του ΕΣΤΙΑ. Θα παρουσιάσουμε διαφορετικά εργαλεία διείσδυσης και θα αναλύσουμε τις δυνατότητές τους. Συγκρίνοντας τις δυνατότητες αυτές θα παρουσιάσουμε αυτό που επιλέχθηκε ως καταλληλότερο για την ανάπτυξη του ΕΣΤΙΑ.

Το εργαλείο διείσδυσης (vulnerability scanner) είναι αυτό που θα εκτελεί την εικονική επίθεση στα προς εξέταση υπολογιστικά συστήματα με σκοπό την εύρεση και καταγραφή αδυναμιών ασφαλείας. Τα βασικά υποσυστήματα από τα οποία αποτελείται συνήθως ένα εργαλείο διείσδυσης είναι τα ακόλουθα:

- **Port scanner**: Ο port scanner είναι το τμήμα το οποίο ελέγχει «ποια ports είναι ανοιχτά», δηλαδή σε ποια ports «ακούνε» εφαρμογές.
- **Service Identifier**: Αυτό το τμήμα προσπαθεί να ανακαλύψει ποιες εφαρμογές τρέχουν σε κάθε ένα από τα ανοιχτά ports.
- **Test generator**: Αφού αναγνωρίσει ποια εφαρμογή τρέχει σε κάθε ανοιχτό port, το σύστημα αναθέτει στον test generator να δημιουργήσει επιθέσεις διείσδυσης κατάλληλες για την συγκεκριμένη εφαρμογή.
- **Packet generator**: Αυτό το τμήμα είναι υπεύθυνο για την δημιουργία και αποστολή των κατάλληλων πακέτων IP τα οποία περιέχουν μία συγκεκριμένη επίθεση (η οποία δίνεται ως παράμετρος από τον test generator).

Οπότε θέλουμε το κάθε προς εξέταση εργαλείο να περιλαμβάνει τουλάχιστον τα παραπάνω υποσυστήματα. Επιπλέον, θέλουμε το εργαλείο να παρέχει κάποιου είδους πληροφορία για τη πρόοδο του ελέγχου κάθε στιγμή. Επίσης, θέλουμε το εργαλείο να μας παρέχει αναλυτικά αποτελέσματα για τα «ρήγματα» ασφάλειας τα οποία βρήκε - ακόμα και για τα λιγότερο σημαντικά από αυτά. Παρέχοντας αυτές τις πληροφορίες, θα μπορεί ο διαχειριστής του συστήματος να διορθώσει το πρόβλημα ασφάλειας στο σύστημά του και να το κάνει του περισσότερο ανθεκτικό σε μελλοντικές επιθέσεις.

Στην περίπτωση που ο «διαχειριστής» είναι ένας απλός χρήστης, θα δίνονται σαφής οδηγίες ώστε να διορθώσει μόνος του τα κενά στην ασφάλεια του μηχανήματός του. Επιθυμητό θα ήταν το σύστημα διείσδυσης να μπορεί να ελέγχει περισσότερες από μία IP διευθύνσεις χωρίς να χρειάζεται ο χρήστης να ξεκίνα καινούργιο έλεγχο για κάθε νέα, αλλά αρχικά να ορίζει ποιες θέλει να ελέγξει και το σύστημα να του επιστρέφει τα αποτελέσματα από όλους τους ελέγχους. Αυτό θα είναι χρήσιμο σε διαχειριστές δικτύων.

Το σύστημα διείσδυσης θα πρέπει να είναι γενικού σκοπού έτσι ώστε να μπορεί να αναγνωρίζει ελλείψεις ασφαλείας σε πολλά διαφορετικά λειτουργικά συστήματα και σε διαφορετικές υπηρεσίες αυτών. Ως συνέπεια του προηγούμενου, θα θέλαμε το εργαλείο που θα χρησιμοποιήσουμε να είναι εύκολα επεκτάσιμο, δηλαδή όταν βγαίνει μια καινούργια υπηρεσία ή - σπανιότερα - ένα νέο λειτουργικό σύστημα, να μπορούμε εύκολα να δημιουργούμε νέους έλεγχους ασφάλειας ή - ακόμα καλύτερα - η ανανέωση αυτή να γίνεται αυτόματα μέσω κάποιας υπηρεσίας χρησιμοποιώντας την υπάρχουσα σύνδεση με το διαδίκτυο. Ως αποτέλεσμα του προηγούμενου θα θέλαμε το εργαλείο να είναι όσο το δυνατόν διαδεδομένο και να υποστηρίζεται από μια όσο το δυνατόν μεγαλύτερη ομάδα προγραμματιστών και χρηστών. Μια άλλη επιθυμητή δυνατότητα του εργαλείου διείσδυσης είναι η δημιουργία διαφορετικών προφίλ ελέγχου για τις περισσότερο κοινές επιθέσεις έτσι ώστε να μπορούμε να δίνουμε στο χρήστη κάποια έτοιμα προφίλ για να ελέγχει τα συστήματα που τον ενδιαφέρει χωρίς να χρειάζεται να ορίσει τη κάθε λεπτομέρεια του έλεγχου κάθε φορά. Τέλος θέλουμε το εργαλείο που θα χρησιμοποιήσουμε να είναι ανοιχτού λογισμικού ώστε να μπορούμε να κάνουμε τις απαραίτητες αλλαγές / προσθήκες σε αυτό για να μπορούμε να το χρησιμοποιήσουμε όπως απαιτείται στο πρόγραμμα ΕΣΤΙΑ.

Γνωρίζουμε βέβαια ότι μπορεί να μην υπάρχει ένα σύστημα διείσδυσης που να μας παρέχει όλα τα παραπάνω. Στην περίπτωση αυτή θα επιλέξουμε αυτό που ταιριάζει καλύτερα στις απαιτήσεις που θέσαμε.

Στην επόμενη ενότητα περιγράφουμε μερικά από τα περισσότερο γνωστά εργαλεία για έλεγχο διείσδυσης και τις ιδιότητες τους.

2.1.Γνωστά Συστήματα Διείσδυσης

Στην παράγραφο αυτή θα παρουσιάσουμε μερικά από τα πιο γνωστά συστήματα διείσδυσης. Τα στοιχεία για τα συστήματα αυτά συλλέχθηκαν κυρίως από το διαδίκτυο.

2.1.1. GFI LANGuard

Το πρώτο εργαλείο που παρουσιάζουμε είναι το LANGuard της GFI. Πρόκειται για ένα εμπορικό σύστημα που επιτρέπει στον χρήστη του να ελέγχει μια ή περισσότερες IPs μέσα στον οργανισμό του ανάλογα με την αδεία που έχει αγοράσει από την εταιρία. Παρέχει αυτόματη αναγνώριση ελαττωμάτων ασφάλειας στο προς εξέταση δίκτυο αναλύοντας τα λειτουργικά συστήματα και τις υπηρεσίες που τρέχουν σε αυτά. Επίσης, επιτρέπει γρήγορο και έγκυρο «port scanning» και έτσι μπορεί να ανακαλύψει ποιο λειτουργικό σύστημα και ποιες υπηρεσίες υπάρχουν σε κάθε μηχάνημα του δικτύου που εξετάζουμε.

Παρέχει και άλλες περισσότερο εξειδικευμένες λειτουργίες όπως η αυτόματη διαχείριση των «service packs» και «patches» για τις διαφορετικές εφαρμογές και τα διαφορετικά λειτουργικά συστήματα, η εύρεση κοινόχρηστων χώρων στο υπό εξέταση δίκτυο, εύρεση ασύρματων κόμβων και άλλες. Αυτό το σύστημα είναι αρκετά καλό και χρησιμοποιείται από οργανισμούς που τους ενδιαφέρει η ασφάλεια μέσα στα όρια του δικτύου τους. Όμως δεν μπορεί να χρησιμοποιηθεί σε ένα πρόγραμμα γενικού σκοπού όπως είναι το ΕΣΤΙΑ για δύο λόγους. Πρώτον, δεν παρέχεται άδεια που να σου επιτρέπει να ελέγχεις όλες τις πιθανές IP διευθύνσεις και, δεύτερον, δεν είναι ανοιχτού κώδικα όπως θα επιθυμούσαμε.

2.1.2. SAINT®

Το δεύτερο εργαλείο που παρουσιάζουμε είναι το SAINT της SAINT corporation. Πρόκειται για ένα εμπορικό σύστημα κλειστού κώδικα. Το SAINT παρέχει την δυνατότητα εύρεσης κάποιου ελαττώματος ασφαλείας στο δίκτυο ενός οργανισμού ή κάποιας εταιρίας. Επίσης, παρέχει στους διαχειριστές του δικτύου ένα εξειδικευμένο λογισμικό ώστε να μπορούν να δημιουργούν και να σχεδιάζουν αναλύσεις για την ασφάλεια του δικτύου τους. Επιπλέον, παρέχει αυτόματο μηχανισμό για την ενημέρωση για νέου είδους επιθέσεις.

Το σύστημα αυτό, αν και έχει αρκετές δυνατότητες από αυτές που έχουμε θέσει ως απαιτήσεις, έχει τα ίδια μειονεκτήματα με το προηγούμενο σύστημα που παρουσιάσαμε. Δεν είναι ανοιχτού κώδικα και δεν μας επιτρέπει, με καμία από τις άδειες που παρέχονται, να ελέγχουμε οποιαδήποτε IP διεύθυνση.

2.1.3. N-stealth

Το N-stealth έχει δημιουργηθεί από την N-stalker. Είναι ένα εμπορικό σύστημα το οποίο μπορεί να κάνει ελέγχους ασφαλείας σε υπολογιστές που λειτουργούν ως "web servers" είτε άλλες συσκευές δικτύου όπως "routers" και "firewalls" που τρέχουν υπηρεσίες δικτύου. Οπότε η συλλογή των ελέγχων επιθέσεων που μπορεί να παράγει δεν απευθύνεται σε οποιοδήποτε μηχάνημα.

Επιπλέον χρησιμοποιεί κάποια βάση δεδομένων για να αποθηκεύει τη συλλογή των ελέγχων ασφαλείας η οποία ανανεώνεται εβδομαδιαία ή και συχνότερα, ανάλογα με τις απαιτήσεις του χρήστη. Υποστηρίζει επίσης ιδεατά μηχανήματα "virtual hosts", "buffer overflow engine", "log analyzer" ο οποίος εξετάζει τα "logs" ενός "web server" για να εντοπίσει τυχόν επιθέσεις. Τέλος υπάρχει μία αδεία χρήσης του N-stealth που σου επιτρέπει να ελέγξεις οποιοδήποτε "web server". Το σύστημα τρέχει από ένα "dedicated" μηχάνημα, συνήθως μέσα σε ένα οργανισμό.

2.1.4. Retina®

Το Retina® είναι ένας "network security scanner" που έχει δημιουργηθεί από την eEye Digital Security. Το Retina® είναι ένα βραβευμένο σύστημα διείσδυσης το οποίο είναι γνωστό για την ακρίβεια, ταχύτητα και "non-intrusiveness"[1]. Παρέχει μηχανισμούς για τη μορφοποίηση του προγράμματος ανάλογα με τις απαιτήσεις του κάθε οργανισμού.

Παρέχει προηγμένη μηχανή για "scanning" καθώς και μια κατανοητή βάση δεδομένων η οποία αποθηκεύει τις γνώστες αδυναμίες ασφαλείας και η οποία ανανεώνεται αυτόματα με νέες απειλές. Επίσης μπορεί να αναγνωρίσει διάφορες συσκευές δικτύου καθώς και μη-εξουσιοδοτημένα προγράμματα όπως P2P, malware,

[1] Δηλαδή, ελέγχει αν είναι ευάλωτο κάνοντας επιθέσεις που δεν προκαλούν βλάβη στο σύστημα. Για παράδειγμα, ελέγχει εάν υποφέρει από DoS attacks χωρίς όμως να εκτελεί ένα DoS attack.

spyware etc. Τέλος το Retina® υποστηρίζει ελέγχους ασφάλειας σε διαφορετικά λειτουργικά συστήματα, παρέχει δυνατότητες για τη δημιουργία προσωπικών ελέγχων ασφαλείας καθώς και προσαρμοσμένες αναφορές ασφάλειας. Το Retina® είναι ένα σύστημα ελέγχου ασφαλείας το οποίο προορίζεται κυρίως για οργανισμούς και δεν παρέχει τη δυνατότητα ελέγχου οποιασδήποτε IP διεύθυνσης.

2.1.5. NESSUS

Το nessus είναι το πιο γνωστό εργαλείο διείσδυσης το οποίο παρέχεται υπό το καθεστώς του ανοικτού λογισμικού. Επίσης είναι ολοκληρωμένο εργαλείο διείσδυσης παρέχοντας όλες τις απαραίτητες λειτουργίες καλύπτοντας ταυτόχρονα όλες τις απαιτήσεις που θέσαμε σαν προαπαιτούμενες σε προηγούμενη παράγραφο.
Χαρακτηριστικά, το nessus παρέχει μια ολοκληρωμένη μηχανή για «port scanning» και αναγνώριση υπηρεσιών, ημιαυτοματοποιημένο μηχανισμό για την ενημέρωση για νέου είδους επιθέσεις, δημιουργία εύκολων και ευανάγνωστων αναφορών για την κατάσταση των υπό εξέταση μηχανημάτων και τέλος μια εξειδικευμένη γλώσσα για τη συγγραφή «σεναρίων» επίθεσης. Τέλος επιτρέπει τον έλεγχο οποιασδήποτε IP διεύθυνσης χωρίς την ανάγκη κάποιας ειδικής αδείας χρήσης, αφού παρέχεται κάτω από την GNU GPL.

Το nessus ήδη χρησιμοποιείται από περισσότερους από 75,000 οργανισμούς και υποστηρίζεται από μια μεγάλη κοινότητα προγραμματιστών και χρηστών που συνεχώς δημιουργούν νέους ελέγχους ασφαλείας. Στην επόμενη παράγραφο γίνεται σαφές ότι το nessus είναι το καταλληλότερο σύστημα διείσδυσης με βάση τις απαιτήσεις που θέλουμε να πληρούνται για να μπορεί να χρησιμοποιηθεί στα πλαίσια του προγράμματος ΕΣΤΙΑ.

2.2. Αξιολόγηση των Εργαλείων Διείσδυσης

Σε αυτή τη παράγραφο θα δούμε μια συγκριτική αξιολόγηση με βάση τις απαιτήσεις που θέσαμε στη παράγραφο §2. Στο παρακάτω πίνακα φαίνονται τα διαφορετικά συστήματα διείσδυσης που έχουμε ήδη παρουσιάσει καθώς και τι μας προσφέρει το καθένα από τις δυνατότητες που θέλουμε να έχει για να μπορεί να χρησιμοποιηθεί στο ΕΣΤΙΑ.

Κάθε σύστημα βέβαια παρέχει και άλλες ίσως περισσότερο εξειδικευμένες δυνατότητες μερικές από τις οποίες έχουμε αναλύσει παραπάνω. Εμάς όμως, για να μας είναι χρήσιμο θέλουμε να πληροί όσο το δυνατόν περισσότερες από τις απαιτήσεις που δίνουμε στον πίνακα.

Στην οριζόντια στήλη βλέπουμε το κάθε σύστημα που έχουμε παρουσιάσει και στην κάθετη τις απαιτήσεις που πληροί. Οπότε μπορούμε εύκολα να εξάγουμε τις δυνατότητες του καθενός συστήματος διείσδυσης κοιτώντας τη κάθετη στήλη κάτω από το αντίστοιχο σύστημα.

Basic Subsystem είναι το βασικό υποσύστημα πίσω από ένα εργαλείο διείσδυσης και αποτελείται από τα εξής άλλα: Port Scanner, Service Identifier, Test Generator και Packet Generator. Το Unlimited IP Scan Range αναφέρεται στην ύπαρξη άδειας με την οποία το σύστημα να μπορεί να ελέγξει οποιαδήποτε IP διεύθυνση. Το General Purpose Scans αναφέρεται στην δυνατότητα του συστήματος να μπορεί να ελέγξει για ρήγματα ασφάλειας σε περισσότερα από ένα λειτουργικά συστήματα και διαφορετικές υπηρεσίες που παρέχουν αυτά. Τέλος το System Support αναφέρεται στην ύπαρξη ή μη ομάδας υποστήριξης είτε από την εταιρία που το δημιούργησε είτε από τρίτους.

	LANGuard	SAINT®	N-stealth	Retina®	NESSUS
Basic Subsystem	✓	✓	✓	✓	✓
Progress Indication	✗	✗	✓	✓	✓
Analytical Reports	✓	✓	✓	✓	✓
Unlimited IP Scan Range	✗	✗	✓	✗	✓
General Purpose Scans	✓	✓	✗	✓	✓
Automated or Semi-automated updates	✓	✓	✓	✓	✓
Support for Manually Created Attack Scripts	✓	✓	✗	✓	✓
Open Source License	✗	✗	✗	✗	✓
Support for Creation of Common Attack Profiles	✓	✗	✗	✓	✓
System Support	✓	✓	✓	✓	✓
Fine-Grain Authorization	✓	✓	✓	✓	✓
NAT Bypassing	✗	✗	✗	✗	✗
Firewall Bypassing	✗	✗	✗	✗	✗
User Friendly	✓	✓	✓	✓	✓

Έκτος από τις απαιτήσεις που θέσαμε στη πρώτη παράγραφο και που θέλουμε να έχει το εργαλείο διείσδυσης, ελέγχουμε προς τέσσερις ακόμα κατευθύνσεις οι οποίες θα μας βοηθήσουν στην ορθότερη και ευκολότερη υλοποίηση του εργαλείου μας. Αυτές οι κατευθύνσεις είναι οι:

- Fine-Grain Authorization

  είναι η δυνατότητα να μπορούμε να ελέγξουμε μόνο συγκεκριμένες IP διευθύνσεις για τις οποίες έχουμε άδεια. Στο nessus μπορούμε να ελέγχουμε οποιαδήποτε IP διεύθυνση άλλα μπορούμε να περιορίσουμε τους χρηστές τους nessus να μπορούν να ελέγχουν μόνο ένα περιορισμένο αριθμό από IPs.

Στα υπόλοιπα εργαλεία ανάλογα με την αδεία χρήσης που αγοράζεται μπορούμε να ελέγξουμε και ένα περιορισμένο αριθμό από IP διευθύνσεις π.χ. στα όρια ενός οργανισμού. Το πρόβλημα είναι ότι το εργαλείο ΕΣΤΙΑ δεν πρέπει να χρησιμοποιηθεί από κακόβουλους χρήστες ώστε να επιτίθονται σε συστήματα που δεν έχουν νόμιμη πρόσβαση (DoS attacks)

- NAT/Firewall Bypassing
  είναι η δυνατότητα να ελέγχουμε μηχανήματα που βρίσκονται πίσω από κάποιο NAT ή Firewall. Κανένα από τα συστήματα αυτά δεν το έχει προβλέψει αυτό γιατί προορίζονται για χρήση στο εσωτερικό ενός οργανισμού και όχι για inter-organizational scanning.
- Web interface
  Όλα παρέχουν μία γραφική διεπαφή χρήστη (GUI) για τη χρήση τους σαν out-standing εργαλεία. Εμείς θα θέλαμε να παρείχαν ένα web interface για να μπορούσαμε να το χρησιμοποιήσουμε αυτούσιο.

2.3. Επιλογή Εργαλείου Διείσδυσης

Όπως βλέπουμε από τον παραπάνω πίνακα το μόνο εργαλείο που ικανοποιεί όλες μας τις απαιτήσεις είναι το nessus. Τα κυριότερα πλεονεκτήματα του nessus είναι:

- είναι λογισμικό ανοιχτού κώδικα, το οποίο σημαίνει ότι μπορούμε να επέμβουμε στο κώδικα του για να τον προσαρμόσουμε με βάση τις ανάγκες μας
- μπορούμε να ελέγξουμε οποιαδήποτε IP διεύθυνση
- υπάρχει μια πολύ μεγάλη κοινότητα που υποστηρίζει το nessus και παράγει συνέχεια νέες επιθέσεις και νέες αναβαθμίσεις για το ίδιο το σύστημα.

Τα υπόλοιπα συστήματα που εξετάσαμε είναι αρκετά καλά συστήματα τα οποία όμως προορίζονται για χρήση μέσα σε κάποιο οργανισμό και όχι για τον έλεγχο οποιαδήποτε IP διεύθυνσης.

3. Παραπομπές

[1] GFI LANGuard

"http://www.gfi.com/lannetscan"

[2] SAINT®

"http://www.saintcorporation.com"

[3] NESSUS

"http://www.nessus.org"

[4] N-stealth

"http://www.nstalker.com/eng/products/nstealth/"

[5] Retina

"http://www.eeye.com/html/products/retina/index.html"