Ασφάλεια Συστημάτων Υπολογιστών

ΕΡΓΑΣΤΗΡΙΑΚΗ ΆΣΚΗΣΗ (PROJECT)

Διδάσκων: Dr Μάριος Αναγνωστόπουλος

Ξάνθη, 05 Δεκεμβρίου 2024

ΥΓ1: Κάθε ομάδα πρέπει να επιλέξει ένα από τα ακόλουθα θέματα. Κάθε ομάδα μπορεί να αποτελείται από έως και 3 φοιτητές/τριες.
ΥΓ2: Οι εργασίες θα γίνουν παρουσίαση στο τελευταίο μάθημα του εξαμήνου.

1ο Θέμα Υλοποίηση TLS, IPSEC, Tor

Εισαγωγή

Σκοπός της εργασίας είναι να εφαρμοστούν τεχνολογίες που παρέχουν ασφάλεια στο επίπεδο δικτύου (IPSec) και στο επίπεδο μεταφοράς (SSL/TLS), να δημιουργηθούν και πραγματοποιηθεί διαχείριση ψηφιακών πιστοποιητικών, και θα αξιοποιηθούν υπηρεσίες που παρέχουν ανωνυμοποίηση όπως είναι το δίκτυο Tor.

Περιγραφή σεναρίου

Στα πλαίσια της εργασίας θα υλοποιήσετε μια δικτυακή εφαρμογή για ανταλλαγή μηνυμάτων που θα προστατεύει την εμπιστευτικότητα και ακεραιότητα των δεδομένων, και θα επιτρέπει την ανωνυμοποιημένη πρόσβαση από τους χρήστες. Συγκεκριμένα, οι χρήστες θα ανταλλάσσουν μηνύματα μέσω sockets και θα εφαρμόσουν τα πρωτόκολλα TLS, IPSEC και Tor, για την προστασία της εμπιστευτικότητας, ακεραιότητας των μηνυμάτων, και ανωνυμίας των χρηστών.

Φάση 1: Δημιουργία (μη ασφαλούς) καναλιού επικοινωνίας

Αρχικά, θα υλοποιηθεί η επικοινωνία των χρηστών. Συγκεκριμένα, θα υλοποιήσετε μια εφαρμογή σε ότι γλώσσα προγραμματισμού επιθυμείτε που θα επιτρέπει την δικτυακή επικοινωνία μεταξύ των χρηστών σε επίπεδο εφαρμογής με την χρήση sockets.

Φάση 2: Προστασία της επικοινωνίας με TLS/SSL

Το κανάλι επικοινωνίας που υλοποιήθηκε στην προηγούμενη φάση είναι ευάλωτο σε επιθέσεις eavesdropping. Συνεπώς, ένας επιτιθέμενος μπορεί να το παρακολουθεί (sniffing) και να υποκλέψει ή να τροποποιήσει τα μεταδιδόμενα δεδομένα. Επιπροσθέτως, ένας επιτιθέμενος θα μπορούσε να υποδυθεί (masquerade) κάποιον χρήστη. Για το σκοπό αυτό θα πρέπει το κανάλι επικοινωνίας να προστατευτεί με την χρήση της τεχνολογίας TLS, προκειμένου να επιτευχθεί αυθεντικοποίηση των χρηστών μεταξύ τους και κρυπτογραφημένη μετάδοση των δεδομένων. Προκειμένου να δημιουργήσετε TLS σύνδεση, θα πρέπει να δημιουργήσετε ψηφιακά πιστοποιητικά (X.509) για όλες τις οντότητες του συστήματος (συνδιαλλαγμένους χρήστες). Η έκδοση των πιστοποιητικών πραγματοποιείται από μια αρχή πιστοποίησης (Certification Authority - CA). Η CA, η οποία διαθέτει ένα self-signed πιστοποιητικό, θα αναλάβει την έκδοση και υπογραφή των πιστοποιητικών των χρηστών. Οι οντότητες θα λάβουν τα πιστοποιητικά από την CA αφού δημιουργήσουν ένα ζεύγος δημοσίου-ιδιωτικού κλειδιού και υποβάλλουν στην CA ένα CSR (certificate signing request). Για τη δημιουργία και τη διαχείριση των ψηφιακών πιστοποιητικών θα πρέπει να χρησιμοποιηθεί η κρυπτοβιβλιοθήκη *OpenSSL*. Δεν απαιτείται στα πλαίσια της εργασίας, η χρήση μηχανισμών ανάκλησης πιστοποιητικών (π.χ. CRLs). Στα πεδία που απαιτείται να συμπληρώσετε κατά την δημιουργία των ψηφιακών πιστοποιητικών θα πρέπει να χρησιμοποιήσετε τα στοιχεία των μελών της ομάδας σας (Ονοματεπώνυμο και Αριθμό Μητρώου).

Φάση 3: Προστασία της επικοινωνίας με IPSec

Μια ενναλακτική μέθοδος για την προστασία του καναλιού επικοινωνίας είναι η χρήση IPSec μηχανισμού. Στα πλαίσια αυτά, θα ενεργοποιήσετε τον μηχανισμό IPSec στο λειτουργικό σύστημα του υπολογιστής σας. Θα πρέπει να χρησιμοποιήσετε την υποδομή της Φάσης 1, και τα πιστοποιητικά που δημιουργήσατε στην Φάση 2.

Φάση 4: Παροχή ανωνυμοποίησης με την χρήση Tor (Bonus)

Προκειμένου να παρέχεται ανωνυμοποίηση της επικοινωνίας και προστασία της ταυτότητας των χρηστών χωρίς να φαίνεται η πραγματική IP διεύθυνση τους, απαιτείται η χρήση τεχνολογίας ανωνυμοποίησης. Μια τέτοια μέθοδος είναι η χρήση του δικτύου ανωνυμίας Tor. Συνεπώς, σε αυτή την φάση θα πρέπει να τροποποιήσετε την υποδομή της Φάσης 1, προκειμένου οι χρήστες να λειτουργούν και ως Hidden Service (HS). Θεωρείστε ότι οι υπόλοιποι χρήστες γνωρίζουν εκ των προτέρων την .onion διεύθυνση των HS.

Σύγκριση

Σε κάθε Φάση της υλοποίησης (Φάση 1-4), θα παρακολουθήσετε τα μεταδιδόμενα πακέτα με την χρήση εργαλείου σύλληψης πακέτων (Wireshark, tcpdump, κλπ) και θα συγκρίνετε την ασφάλεια του καναλιού με την χρήση των διαφορετικών τεχνολογιών. Χρησιμοποιήστε/περιορίστε την εμφανιζόμενη κίνηση με κατάλληλα φίλτρα προκειμένου να εμφανίζεται η δικτυακή κίνηση που σας ενδιαφέρει. Τέλος, συγκρίνετε τα πρωτόκολλα TLS και IPv6/IPsec ως προς τον τρόπο και την ευκολία χρήσης τους, το επίπεδο της παρεχόμενης ασφάλειας κλπ. Συμπεράνετε πότε είναι προτιμότερη η μια τεχνολογία έναντι της άλλης.

Παραδοτέα

Κατά την τελική παράδοση της εργασίας, όλος ο πηγαίος κώδικας θα πρέπει να αναρτηθεί στο eclass του μαθήματος. Επιπλέον θα συγγράψετε και θα παραδώσετε μια αναφορά που θα περιέχει την τεκμηρίωση των ζητούμενων της εκάστοτε φάσης:

1. Τεκμηρίωση προγραμμάτων και επεξήγηση τυχόν δικών σας παραδοχών.
2. Πηγαίο κώδικα και εκτελέσιμα προγράμματα.
3. Στιγμιότυπα εκτέλεσης προγράμματος με σύντομο σχολιασμό (screenshots).
4. Περιγραφή και τρόπος δημιουργίας δημοσίου-ιδιωτικού κλειδιού, ψηφιακών πιστοποιητικών, κλπ. Εντολές και screenshot του OpenSSL.
5. Ανάλυση των αποτελεσμάτων χρήσης του εργαλείου σύλληψης πακέτων (sniffer) και ενδεικτικά στιγμιότυπα εκτέλεσης (screenshots). Επεξήγηση των φίλτρων που χρησιμοποιήθηκαν.
6. Περιγραφή των τροποποιήσεων των συστημάτων για τη χρήση του πρωτοκόλλου IPsec.
7. Περιγραφή της χρήσης της βιβλιοθήκης και των τροποποιήσεων των συστημάτων για την χρήση του Tor.
8. Σύγκριση μεταξύ των τεχνολογιών TLS και IPsec.
9. Περιγραφή και τρόπος δημιουργίας των HS και της υλοποίησης του δικτύου Tor

Η εργασία πρέπει να παραδοθεί μέσω της πλατφόρμας ηλεκτρονικής μάθησης e-class εντός της προκαθορισμένης προθεσμίας. Το τελικό παραδοτέο πρέπει να είναι αρχείο .zip/rar.

2ο Θέμα Υλοποίηση ενός IDS

Εισαγωγή

Σκοπός της εργασίας είναι να εγκατασταθούν εργαλεία για τον εντοπισμό εισβολών (IDS).

Περιγραφή σεναρίου

Στα πλαίσια της εργασίας θα εγκαταστήσετε και παραμετροποιήσετε ένα Intrusion Detection System (IDS) και θα πραγματοποιήσετε επιθέσεις για τον έλεγχο του. Συγκεκριμένα θα πραγματοποιήσετε τουλάχιστον **5 επιθέσεις χειροκίνητα** (πχ. Δημιουργία κακόβουλων πακέτων) και χρήση τουλάχιστον **3 αυτοματοποιημένων εργαλείων** (πχ. NMap). Παράλλληλα θα βλέπετε τα alerts που θα δημιουργούνται. Για την περίπτωση τις δικής σας κακόβουλης κίνησης να δημιουργήσετε τους κανόνες (signature) που θα τις εντοπίζουν. Αναλύστε και σχολιάστε τα alerts που δημιουργούνται.

Bonus

Εγκαταστήστε τα κατάλληλα εργαλεία για την οπτικοποίηση των alerts.

ΥΓ: Κάθε ομάδα που θα αναλάβει την υλοποίηση IDS θα πρέπει να επιλέξει διαφορετικό εργαλείο για εγκατάσταση (Snort, Suricata, Zeek, etc)

Παραδοτέα

Κατά την τελική παράδοση της εργασίας, θα πρέπει να αναρτηθεί στο eclass του μαθήματος μια αναφορά που θα περιέχει την τεκμηρίωση των ζητούμενων της υλοποίησης:

1. Διαδικασία εγκατάστασης και παραμετροποίησης των εργαλείων συνοδευόμενα με απαιτούμενα screenshot. Επεξήγηση τυχόν δικών σας παραδοχών
2. Περιγραφή και τρόπος λειτουργίας των κανόνων που υλοποιήσατε/παραμετροποιήσατε.
3. Στιγμιότυπα εκτέλεσης προγράμματος με σύντομο σχολιασμό (screenshots).
4. Ανάλυση των αποτελεσμάτων χρήσης του IDS και ενδεικτικά στιγμιότυπα εκτέλεσης (screenshots) με τα alerts. Επεξήγηση των κανόνων που εκτελέστηκαν.
5. Διαδικασία εγκατάστασης και παραμετροποίησης του εργαλείου για την οπτικοποίηση των alerts.

Η εργασία πρέπει να παραδοθεί μέσω της πλατφόρμας ηλεκτρονικής μάθησης e-class εντός της προκαθορισμένης προθεσμίας. Το τελικό παραδοτέο πρέπει να είναι αρχείο .zip/rar.

3ο Θέμα Υλοποίηση ενός Sandbox για την ανάλυση malware

Εισαγωγή

Σκοπός της εργασίας είναι να εγκατασταθούν εργαλεία για την δυναμική ανάλυση malware (sandbox).

Περιγραφή σεναρίου

Στα πλαίσια της εργασίας θα εγκαταστήσετε και παραμετροποιήσετε ένα sandbox και θα αναλύσετε τουλάχιστον **10 διαφορετικά malware** για τον έλεγχο του. Μπορείτε να κατεβάσετε malware samples από Online repositories όπως είναι το **MalwareBazaar, VX Underground,** κλπ. Ακολούθως να αναλύσετε και να σχολιάσετε τα logs που δημιουργήθηκαν. Επιπλέον αναλύστε τα ίδια malware σε **3 διαφορετικά Online sandbox** (πχ. app.any.run, www.joesandbox.com, κλπ) και συγκρίνετε τα αποτελέσματα. Ποιο θεωρείτε παρέχει την καλύτερη ανάλυση και για ποιο λόγο. Δώστε έμφαση στην καταγραφόμενη δικτυακή κίνηση (pcap files).

Bonus (Εναλλακτικά ένα από τα δύο)

i) Προσπαθήστε να κάνετε hardening (όσο το δυνατόν καλύτερα) στην υποδομή σας και να δημιουργείστε ένα simulated network (Πχ. Με το inetsim) και αναλύστε διαφορές στα logs πριν και μετά το hardening. Εκτελέστε κατάλληλα εργαλεία για να εντοπίσετε artifacts που προδίδουν την παρουσία του sandbox.

ii) Μελετήστε τα YARA rules και προσαρμόστε την υλοποίηση σας για να τα υποστηρίζει. Τι επιπλέον προσφέρουν?

ΥΓ: Κάθε ομάδα που θα αναλάβει την υλοποίηση sandbox θα πρέπει να επιλέξει διαφορετικό sandbox για εγκατάσταση (CAPE, drakvuf, Cuckoo, etc) και διαφορετική κατηγορία malware (virus, trojan, worms, etc)

ΠΡΟΣΟΧΗ: Για την προστασία του υπολογιστή σας και του δικτύου σας, το κατέβασμα των malware samples θα γίνει ΜΟΝΟ από virtual machines. Επιπλέον το sandbox θα είναι απομονωμένο χωρίς σύνδεση στο Internet!

Παραδοτέα

Κατά την τελική παράδοση της εργασίας, θα πρέπει να αναρτηθεί στο eclass του μαθήματος μια αναφορά που θα περιέχει την τεκμηρίωση των ζητούμενων της υλοποίησης:

1. Διαδικασία εγκατάστασης και παραμετροποίησης των εργαλείων συνοδευόμενα με απαιτούμενα screenshot. Επεξήγηση τυχόν δικών σας παραδοχών.
2. Περιγραφή και τρόπος λειτουργίας του εργαλείου και της αρχιτεκτονικής (τοπολογίας) που δημιουργήσατε.
3. Στιγμιότυπα εκτέλεσης προγράμματος με σύντομο σχολιασμό (screenshots).
4. Ανάλυση των αποτελεσμάτων χρήσης του sandbox και ενδεικτικά στιγμιότυπα εκτέλεσης (screenshots) με τα logs. Επεξήγηση των logs που δημιουργήθηκαν.
5. Επεξηγήστε τα χαρακτηριστικά της κατηγορίας του malware που επιλέξατε και σχολιάστε κοινές ή διαφορετικές συμπεριφορές.

6. Συγκρίνετε τις διαφορές μεταξύ της δική σας υλοποίησης και των Online εργαλείων. Ποιο θεωρείτε παρέχει την καλύτερη ανάλυση και για ποιο λόγο. Δικαιολογήστε και δώστε screenshots.
7. Διαδικασία hardening και έλεγχος των artifact που προδίδουν την παρουσία sandbox.

Η εργασία πρέπει να παραδοθεί μέσω της πλατφόρμας ηλεκτρονικής μάθησης e-class εντός της προκαθορισμένης προθεσμίας. Το τελικό παραδοτέο πρέπει να είναι αρχείο .zip/rar.