Τεχνολογικό Πανεπιστήμιο Κύπρου
Σχολή Μηχανικής και Τεχνολογίας

Πτυχιακή εργασία

Penetration Testing on the Infrastructure of a Federated Identity and Authentication Provider

Ευάγγελος Φωτίου

Λεμεσός, Μάϊος 2022

ΤΕΧΝΟΛΟΓΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή εργασία

Penetration Testing on the Infrastructure of a Federated Identity and Authentication Provider

του

Ευάγγελου Φωτίου

Επιβλέπων Καθηγητής

Δρ. Μιχάλης Σιριβιανός

Λεμεσός, Μάϊος 2022

Πνευματικά δικαιώματα

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής του Τεχνολογικού Πανεπιστημίου Κύπρου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέπων καθηγητή μου Δρ. Μιχάλη Σιριβιανό και βοηθούς Δρ. Νίκο Σαλαμάνο, Δρ. Κωνσταντίνο Παπαδάμου, για την βοήθεια και την καθοδήγηση τους καθ΄ όλη τη διάρκεια της διπλωματικής μου εργασίας.

ΠΕΡΙΛΗΨΗ

Ο σκοπός της δοκιμής διείσδυσης που γίνεται στον διαδικτυακό διακομιστή ιστού που φιλοξενεί υπηρεσίες που παρέχουν ταυτότητα και πιστοποίηση και εφαρμογές του INCOGNITO είναι για την αξιολόγηση της ασφάλειας του και κατά πόσο αυτή είναι επαρκής έτσι ώστε να τον προστατέψει από οποιαδήποτε είδους επίθεση στον κυβερνοχώρο από κάποιο κακόβουλο χρήστη. Επίσης γίνεται για να εξεταστεί εάν οι αμυντικές μέθοδοι όπως και οι πολιτικές ασφαλείας που χρησιμοποιεί είναι αρκετές. Παράλληλα όμως γίνεται και η αξιολόγηση των δυνατοτήτων των εργαλείων που χρησιμοποιήθηκαν τα οποία αποτελούν τα πιο σύγχρονα ανοικτού κώδικα εργαλεία τα οποία ο οποιοσδήποτε μπορεί να έχει πρόσβαση. Πιο συγκεκριμένα η έρευνα αυτή αποσκοπεί στο να βρεθούν τυχόν ευπάθειες που μπορεί να υπάρχουν στο σύστημα τις οποίες οι διαχειριστές δεν γνωρίζουν και οι οποίες θα μπορούσαν να επιτρέψουν σε ένα κακόβουλο χρήστη να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα είτε σε κάποιο μέρος δεδομένων ή ευαίσθητων πληροφοριών που δεν θα έπρεπε. Παρουσιάζεται μια ολοκληρωμένη επίδειξη ενός Penetration Testing κατά την οποία δοκιμάζονται διαφόρων ειδών επιθέσεις και τεχνικές οι οποίες θα μπορούσαν να πραγματοποιηθούν από ένα κακόβουλο χρήστη που προσπαθεί να εισβάλει στο σύστημα μαζί με τα εργαλεία τα οποία χρησιμοποιήθηκαν και γιατί. Τα αποτελέσματα της δοκιμής αυτής μπορεί να αποτελέσουν οδηγό για τους διαχειριστές του συστήματος για την κάλυψη και επιδιόρθωση τυχόν κενών ασφαλείας που μπορεί να υπάρχουν έτσι ώστε να αποφευχθεί μελλοντική επίθεση από οποιοσδήποτε κυβερνοεγκληματία, η οποία μπορεί να επιφέρει σοβαρές συνέπειες τόσο στα δεδομένα που διαφυλάσσονται αλλά και στα άτομα που αφορά το συγκεκριμένο σύστημα.

Λέξεις κλειδιά: Penetration Testing, INCOGNITO, ευπάθειες

ABSTRACT

This thesis journal aims to perform a Penetration Testing to the online identity and authentication provider web server that holds services and applications of INCOGNITO to assess its security and protection level against any type of cyber-attack from a malicious user. Also, another goal of this assessment is to check the defense mechanisms and safety policies that utilizes are adequate for its protection. At the same time, we evaluate the performance of the tools used in the process which are state of the art open-source tools that are widely used and accessible to anyone. More specifically, the research aims to find any possible vulnerabilities or misconfigurations that may exist in the system that the system administrators might be unaware of as this is a development server, that could allow a user with malicious intentions to gain unauthorized access to the system itself or to a part of information that shouldn't have. This thesis presents the entire procedure of Penetration Testing during which are attempted a different kinds of attacks and techniques that a malicious user could perform along with the tools used and for what purpose. The results of this Penetration Testing can be a useful guide for the system administrators to learn about any possible vulnerabilities and release the appropriate security patches to fix those security flaws and prevent a future attack of any cybercriminal that could cause severe consequences not only for the data that are kept but also for the people responsible for the server.

Keywords: Penetration Testing, INCOGNITO, vulnerabilities