Dradis Framework
Importing information will get you root!

Theofanis Kasimis
CCNA, CCNA Security, OSCP
CEO Audax Cybersecurity
Email: fkasimis@audax.gr
Twitter: @_fkasimis_

AUDAX
CYBERSECURITY

The Dradis Project

Το Dradis είναι μια πλατφόρμα open-source και χρησιμοποιείτε από ερευνητές ασφάλειας & τμήματα IT για την υποβολή εκθέσεων – αναφορών και παρέχει μια κεντρική αποθήκη πληροφοριών για να παρακολουθούμε οτιδήποτε έχει γίνει μέχρι στιγμής, και τι είναι ακόμα μπροστά.

Γιατί Dradis Framework;;;;;;;;

AUDAX
CYBERSECURITY

Παράδειγμα Νο1

* Ερευνητές Ασφάλειας / Penetration Testers

AUDAX
CYBERSECURITY

silviu@silviu (10.10.0.153) - byobu

```
            printk(KERN_ERR "VBoxNetAdp: Can't
 register VBOXNETADP_CTL_DEV_NAME " device! rc=%
d\n", rc);
            return rc;
        }
        LogRel(("VBoxNetAdp: Successfully star
ted.\n"));
        return 0;
    }
    else
<nux.c" [readonly] 445L, 13961C 405,13        91%
```

```
A:  30,6 V:  30,6 A-V:  0,000 ct:  0,000   0/  0
```

```
ie hotel
India victor Oscar delta Echo delta Bravo oscar fo
xtrot EIGHT
echo kilo oscar charlie Uniform delta India papa
Lima alfa papa sierra hotel yankee golf RIGHT_BRAC
KET
Victor echo mike AMPERSAND Golf romeo alfa novembe
r
Oscar romeo charlie Oscar india delta sierra india
 delta
```

```
~ubuntu1) ...
rocessing triggers for man-db (2.7.0.2-2) ...
etting up libgmp10:i386 (2:6.0.0+dfsg-4build1) ...
etting up libnettle4:i386 (2.7.1-3) ...
etting up libhogweed2:i386 (2.7.1-3) ...
etting up libp11-kit0:i386 (0.20.2-5) ...
etting up libtasn1-6:i386 (4.0-2) ...
Setting up libgnutls-deb0-28:i386 (3.2.16-1ubuntu2.
) ...
etting up libsqlite3-0:i386 (3.8.6-1) ...
```

```
lo                                          bmon 3.2
Interfaces                  | RX bps       pps
>lo                         |      0         0
 eth0                       |   846B         6
   qdisc none (pfifo_fast)  |      0         0
 virbr0                     |      0         0
----------------------------+----------------

------ Press d to enable detailed statistics -----
---- Press i to enable additional information ----
Thu Dec 18 10:52:15 2014        Press ? for help
```

```
│   ├── runtime_active_time
│   ├── runtime_enabled
│   ├── runtime_status
│   ├── runtime_suspended_time
│   └── runtime_usage
├── subsystem -> ../../../../bus/workq
ueue
└── uevent

2622 directories, 11578 files
```

```
ENONET 64 Machine is not on the network
EADDRINUSE 98 Address already in use
ENODATA 61 No data available
ECHRNG 44 Channel number out of range
EADDRNOTAVAIL 99 Cannot assign requested address
ECHILD 10 No child processes
EL3HLT 46 Level 3 halted
ENOLCK 37 No locks available
ECONNABORTED 103 Software caused connection abort
EBADF 9 Bad file descriptor
```

```
  File: '/sys/module/llc/sections/.rodata.str1.8'
  Size: 4096          Blocks: 0          IO Bloc
k: 4096   regular file
Device: fh/15d  Inode: 22395       Links: 1
Access: (0444/-r--r--r--)  Uid: (    0/    root)
 Gid: (    0/    root)
Access: 2014-12-18 10:52:15.097065506 +0200
Modify: 2014-12-18 10:52:15.097065506 +0200
Change: 2014-12-18 10:52:15.097065506 +0200
 Birth: -
```

```
  1  [||||||   34.4%]    Tasks: 179, 449 thr; 3
  2  [||||||   40.9%]    Load average: 2.04 1.09
  3  [||||||   39.4%]    Uptime: 01:52:28
  4  [||||||| 47.1%]
  Mem[||||2528/7880MB]
  Swp[       0/8086MB]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% M
13824 silviu     20   0  596M 38908 26796 R 35.7
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7
```

```
00000980  ff 25 c2 16 20 00 68 06  00 00 00 e9 80 f
f ff ff  |.%.. .h.........|
00000990  ff 25 ba 16 20 00 68 07  00 00 00 e9 70 f
f ff ff  |.%.. .h.....p...|
000009a0  ff 25 b2 16 20 00 68 08  00 00 00 e9 60 f
f ff ff  |.%.. .h.....`...|
000009b0  ff 25 aa 16 20 00 68 09  00 00 00 e9 50 f
f ff ff  |.%.. .h.....P...|
000009c0  ff 25 a2 16 20 00 68 0a  00 00 00 e9 40 f
f ff ff  |.%.. .h.....@...|
```

```
ACPI_AVAILABLGeneral Commands MACPI_AVAILABLE(1)

NAME
       acpi_available  -  test whether ACPI sub-
       system is available

SYNOPSIS
       acpi_available

DESCRIPTION
       acpi_available checks  whether  the  ACPI
       ("Advanced Configuration and Power Inter-
ilable(1) line 1 (press h for help or q to quit)
```

```
u⁰  14.10  0:--  1:hollywood*
```

```
1h52m  2.04  4x3.3GHz  7.7G32%  2014-12-18 10:52:15
```

Παράδειγμα Νο2

* Τμήματα IT

Dradis Framework 3.0.0

dradisframework.dev/nodes/2

Dradis Framework

Upload output from tool | Export results | Configuration

All issues

Nodes

- scope
- Uploaded files
- hosts

Dradis Framework 3.0.0

Nodes / scope

+ Add subnode | Delete | Rename | Move

Notes

URLs and credentials

Evidence

(nothing yet)

Attachments

project-sow.pdf 36.08 KB

Drop zone

Content for this note

edit remove

Title

URLs and credentials

Details

Username	Password	Role
pentest1	Password!!	Admin
pentest2	Password!!	User

Target URLs

https://intranet.insecure.com
https://portal.insecure.com

Τεχνογνωσία

- Ruby
- Linux (Kali 2.0), Mac, Windows
- Συλλογή & αποθήκευση πληροφοριών
- Εύκολο στη χρήση & την προσαρμογή
- Παραμετροποιήσιμο
- Μικρό & φορητό
- Προγραμματισμένες εργασίες

AUDAX
CYBERSECURITY

Η τεχνολογία πίσω από την σκηνή

AUDAX
CYBERSECURITY

- Import XML Files
- Plugins of Dradis Framework
- Reporting Tools

AUDAX
CYBERSECURITY

…Plugins…

Nikto
Web Vulnerability Scanner
#ImAWhiteHat

Nmap

OpenVAS
Open Vulnerability Assessment System

BURPSUITE
PROFESSIONAL

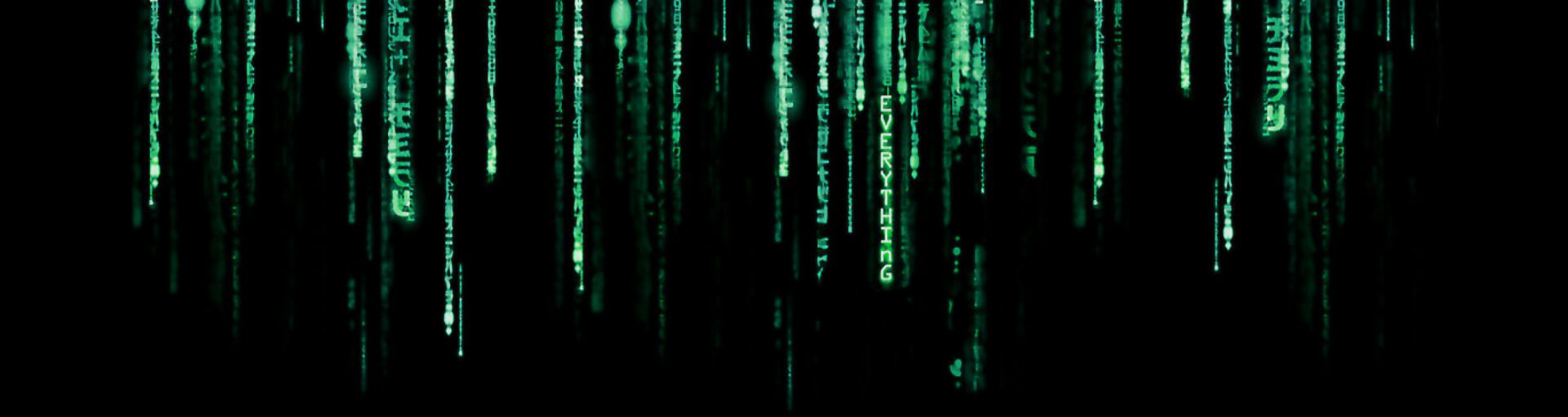
Import XML file….

```
module Plugins
  module Upload
    include NmapUpload
  end
end
```

-
-

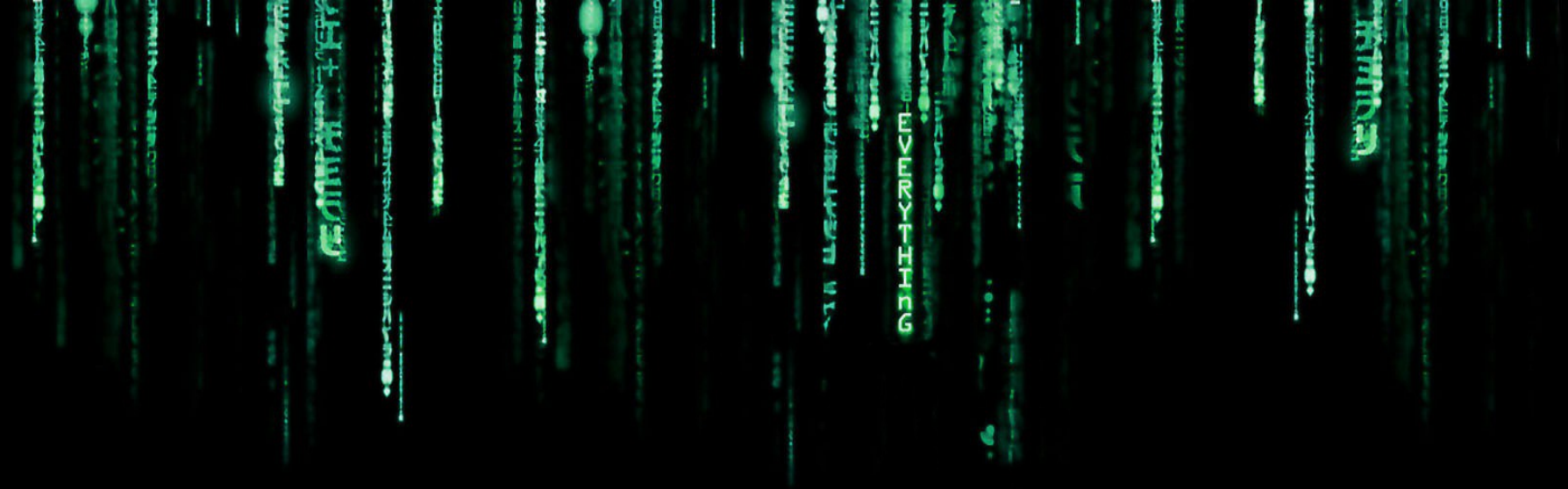
Τι πετύχαμε….;

AUDAX
CYBERSECURITY



- Συγκέντρωση πληροφοριών ανα τερματικό
- Κατηγοριοποίηση Κενών ασφάλειας ανα τερματικό
- Κατηγοριοποίηση βαθμού επικινδυνότητας (green, orange, red)
- Αποθήκευση αποτελεσμάτων για έλεγχο αργότερα ανα ημέρα/τερματικό
- Προγραμματισμένες εργασίες ανα τερματικό

AUDAX
CYBERSECURITY



* DEMOOO

AUDAX
CYBERSECURITY

ΤΕΛΟΣ ΠΑΡΟΥΣΙΑΣΗΣ

ΣΑΣ ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ

2ΗΜΕΡΟ ΣΥΝΕΔΡΙΟ
ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ & ΤΙΣ ΨΗΦΙΑΚΕΣ ΑΠΕΙΛΕΣ

6° infocom SECURITY

Upgrade your Knowledge
Protect your Business

ethical hacking

AUDAX
CYBERSECURITY