Sovversione del sistema

alla ricerca di anomalie in un sistema compromesso

Italian Security Mailing List

SIKUREZZA.ORG

smau 2005

e-Academy

Gestione Incidenti Informatici

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

The Coroner ^H^H^H^H^H^H^H^H Attacker's Toolkit

- occultamento
- backdoor
- pulizia dei log
- sovversione del kernel
- canali di comunicazione "covert"
- data hiding

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Occultamento

- È la **prima** necessità di un attaccante
- Tale necessità è **imperativa**
- Risponde alla legge del "**Tutto o Nulla**"
- Può essere tanto banale e superficiale quanto **evoluto** e **radicato** nel sistema colpito

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Tecniche di Occultamento

- Un attaccante **esperto** o uno script kid **ben equipaggiato** non mostrano incautamente la loro presenza.

- Le tecniche di occultamento di un intruso che abbia ottenuto **accesso come super-utente** sono oggi raffinatissime rispetto a solo **10 anni fa**.

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Tecniche di Occultamento

- .../.evil.c
- if(strstr(name, secret) != NULL) continue;
- if(strstr((char *)&(dirptr->dname),
  (char *)SUBVISUS) != NULL) {...}
- ext2fs_read_bb_inode(fs, &bb);
- ext2fs_badblocks_list_add(bb, i);
- ext2fs_update_bb_inode(fs, bb);

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

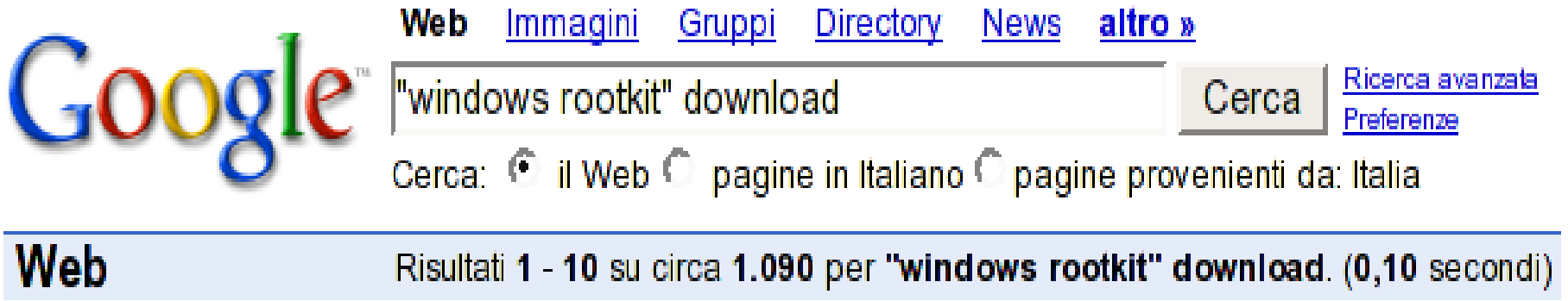
Backdoor

- È il "**canale di ritorno**" di un attaccante.
- Teoricamente:
- È **invisibile**
- Permette accesso come **super-utente**
- È **personale** (ovvero non è utilizzabile da altri attaccanti)

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Backdoor

- Sono disponibili centinaia di backdoor per i più (e meno) comuni sistemi operativi. Questo rende potenzialmente pericolosi anche gli attaccanti meno esperti dal punto di vista tecnico.



Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Pulizia dei Log

- **Case History - log binario: Linux /var/run/utmp**

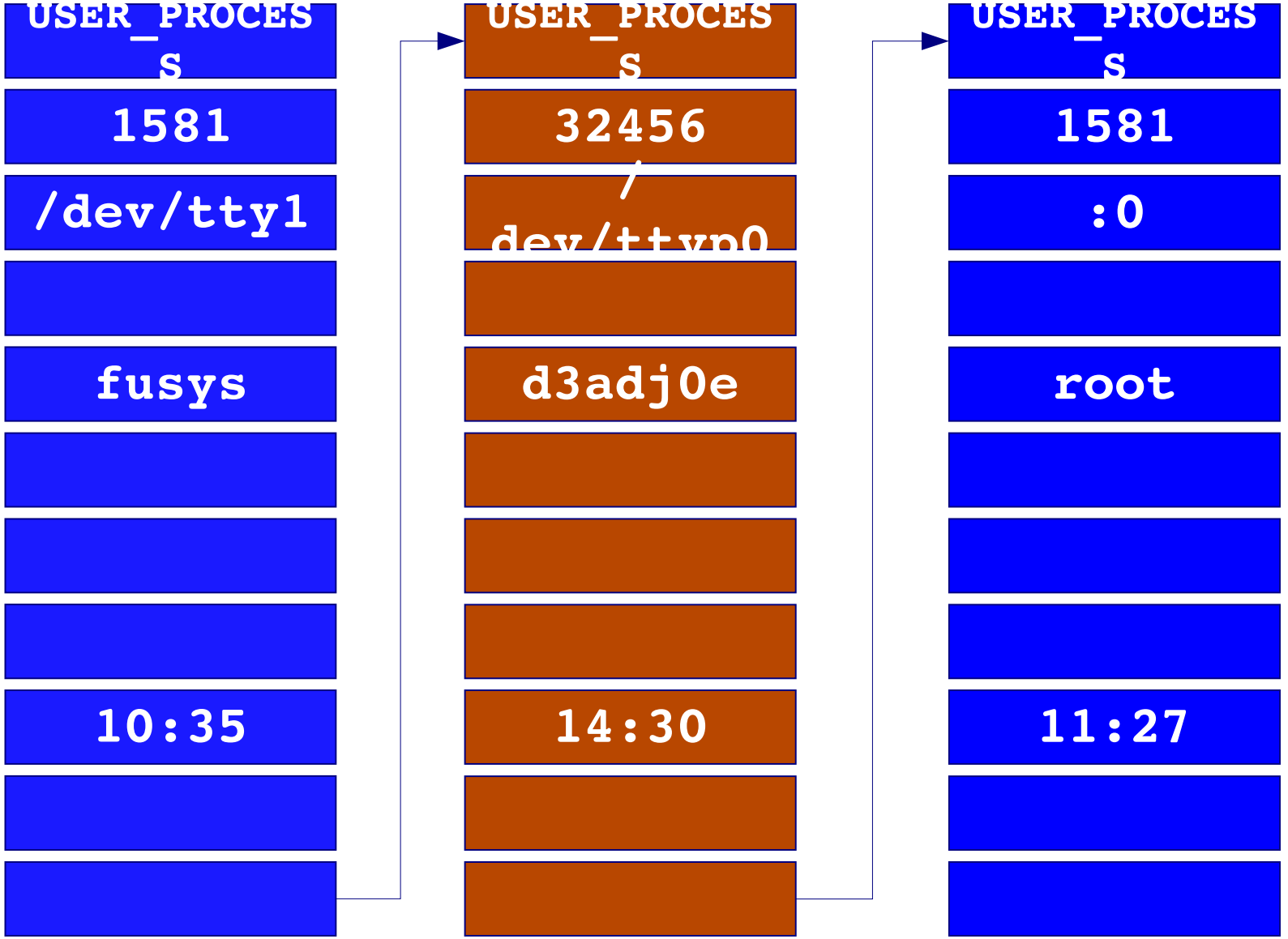
La pagina man di **w(1)** e **who(1)** mostra che il file di log utilizzato è **/var/run/utmp**.
Questo è un file binario, con una struttura specifica.

L'attaccante non deve far altro che accedere alla pagina man di **utmp(5)** per scoprire tale struttura.

Ogni utente è registrato in una struttura di cui sono **noti dimensioni e contenuti teorici**

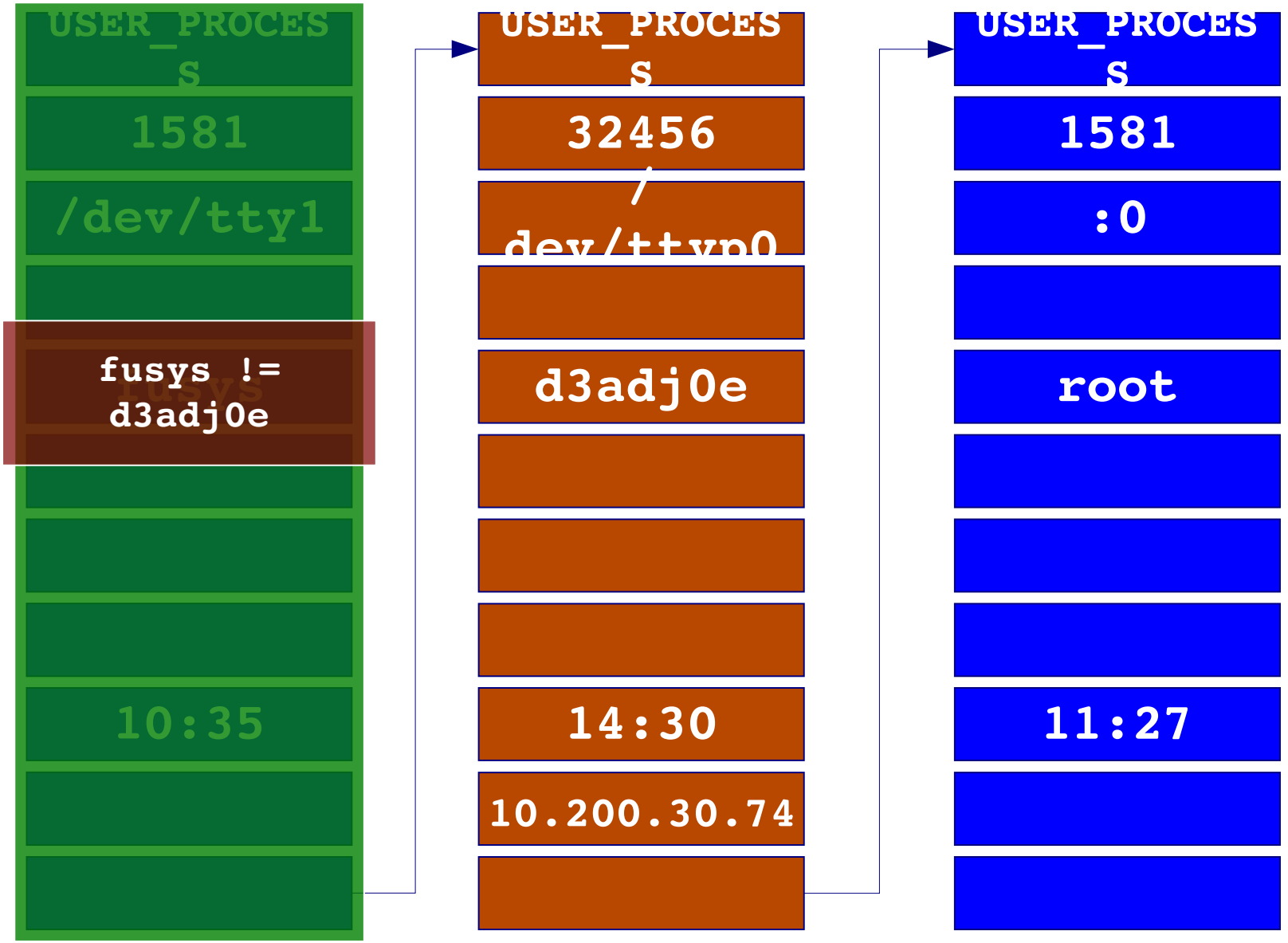
Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

/var/run/utmp (esemplificazione)



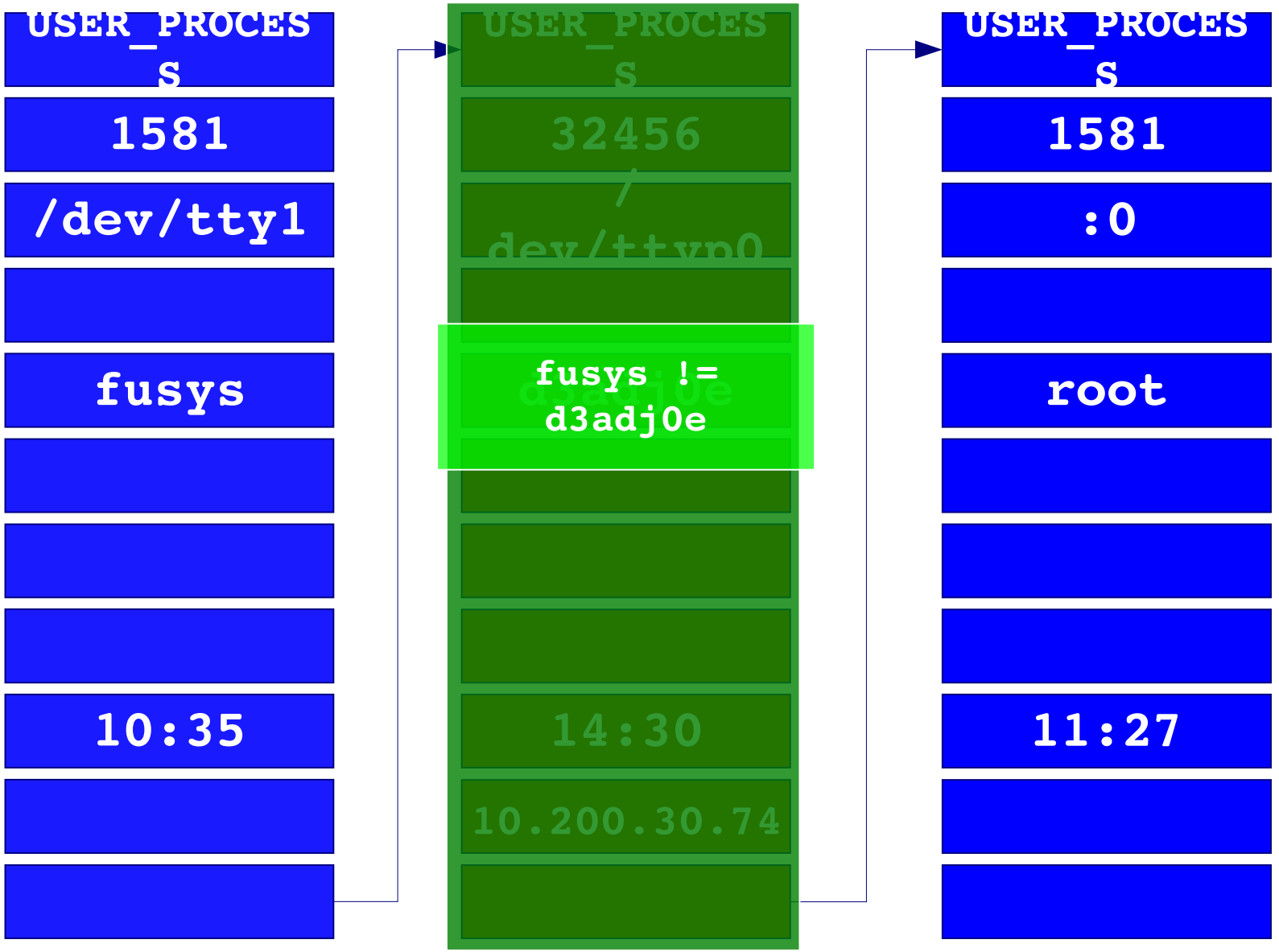
Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

HideMe d3adj0e



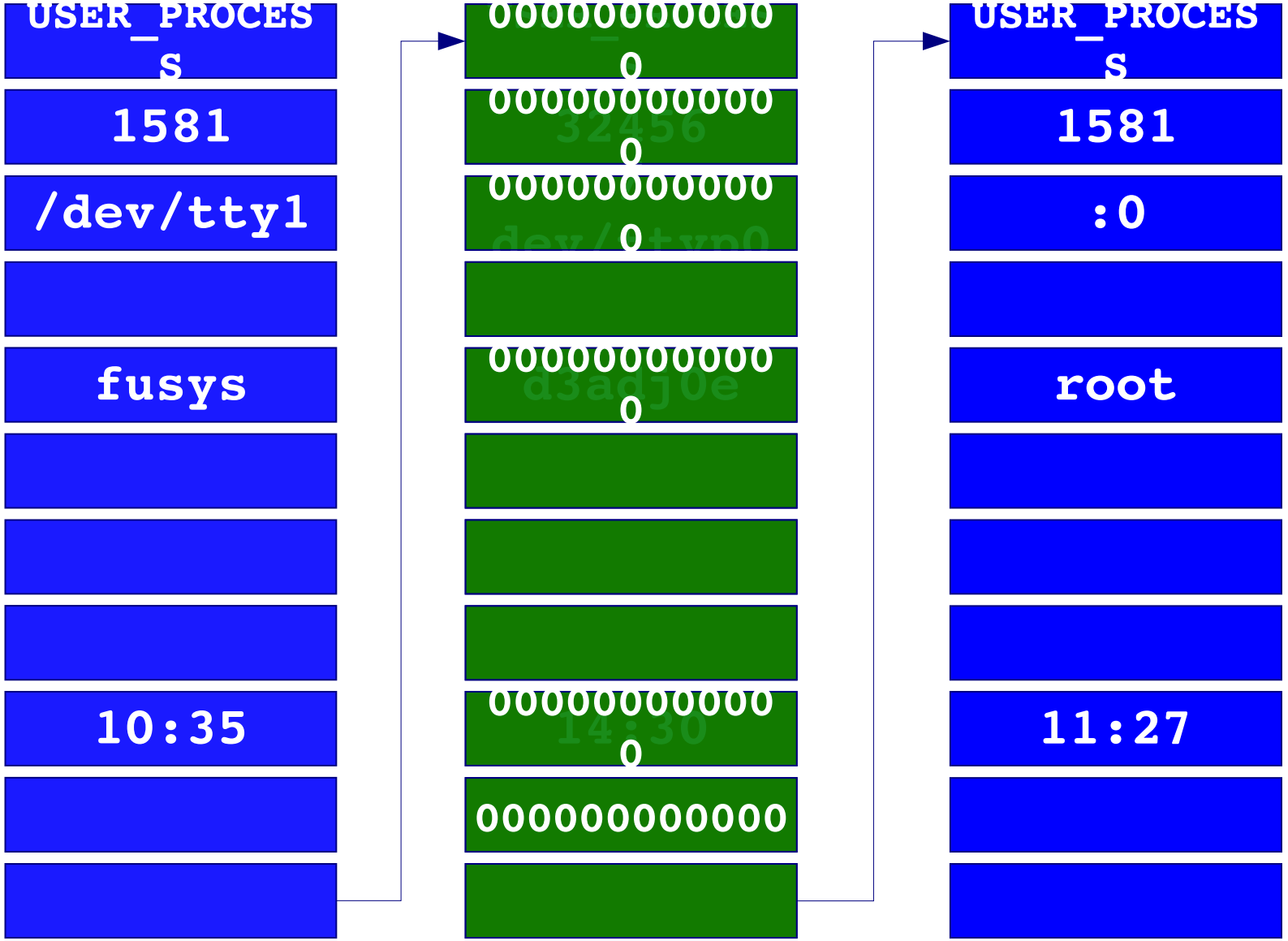
Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

HideMe d3adj0e

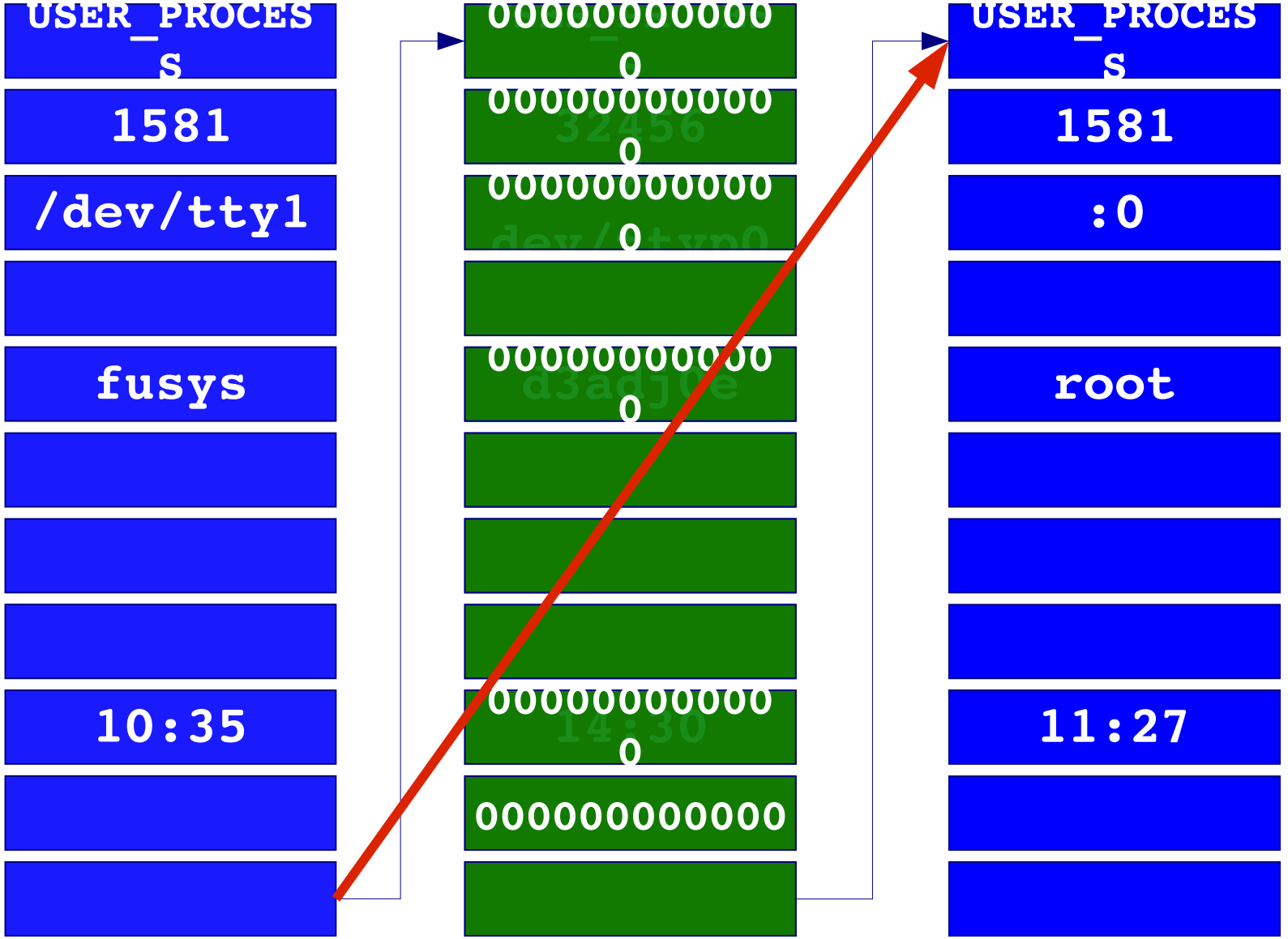


Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

HideMe d3adj0e



HideMe d3adj0e



Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Pulizia dei Log

utmp e wtmp contemplano un uso **legittimo** dei campi NULL

è necessaria **non solo** una correlazione con il numero dei processi attivi e con le eventuali cwd, ma una analisi "**statistica**" delle dimensioni del file in rapporto all'ora di sistema (utmp)

o una **correlazione** (non sempre possibile) tra gli **UID** presenti nel sistema e la presenza di **record** nel log (wtmp)

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Pulizia dei Log

- **Case History - log ASCII: IIS 5.1 W3SVC1**

Essendo in semplice **ASCII**, possono essere modificati a mano con **qualunque editor di testo**

Tool automatizzati permettono **flessibilità** e **velocità** di esecuzione

Tutto ciò che occorre all'attaccante è la conoscenza del **formato delle stringhe** che compongono il log

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Pulizia dei Log

- Case History - log ASCII: **IIS 5.1 W3SVC1**

```
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET
/SQL/login.asp 200 0 10806 HTTP/1.1 192.168.1.10
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET
/searchform.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:53:42 10.20.30.40 192.168.1.10 80 GET
/cgi-bin/evil.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:53:42 10.20.30.40 192.168.1.10 80 GET
/SQL/login.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:53:42 10.20.30.40 192.168.1.10 80 GET
/SQL/oldtest.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET
/Default.htm 200 0 10806 HTTP/1.1 192.168.1.10
```


Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Pulizia dei Log

```
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET/SQL/login.asp 200 0 10806 HTTP/1.1 192.168.1.10
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET /searchform.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:53:42 10.20.30.40 192.168.1.10 80 GET /cgi-bin/evil.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:53:42 10.20.30.40 192.168.1.10 80 GET /SQL/login.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:53:42 10.20.30.40 192.168.1.10 80 GET /SQL/oldtest.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET /Default.htm 200 0 10806 HTTP/1.1 192.168.1.10
```

```
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET /SQL/login.asp 200 0 10806 HTTP/1.1 192.168.1.10
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET /searchform.asp 200 0 0 HTTP/1.1 192.168.1.10
2003-11-26 14:47:40 192.168.1.185 192.168.1.10 80 GET /Default.htm 200 0 10806 HTTP/1.1 192.168.1.10
```


Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Sovversione del Kernel

- Negli ultimi **7 anni** notevole impulso hanno avuto le tecniche di manipolazione in "**zona kernel**"

- L'articolo di Halflife sulla e-zine **Phrack** (http://www.phrack.com) ha svelato al mondo degli attaccanti il concetto di "**kernel rootkit**"

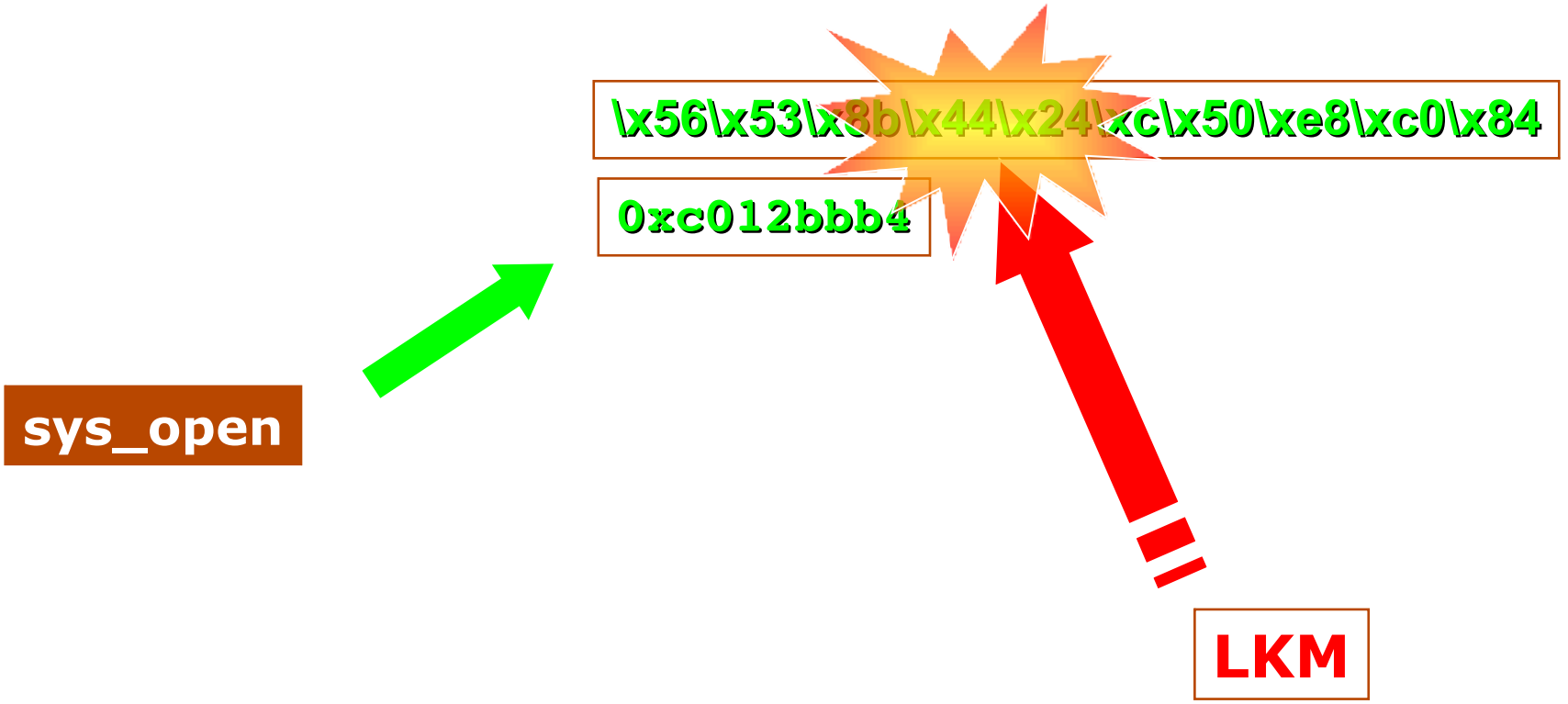
- Un rootkit inserito nel kernel di un sistema operativo **non** modifica i binari o le librerie di sistema e **compromette** il funzionamento di ogni operazione richiesta dall'amministratore. **Non** è possibile fidarsi di nulla, neanche delle operazioni di lettura di un floppy disk !

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: Linux fake sys_call

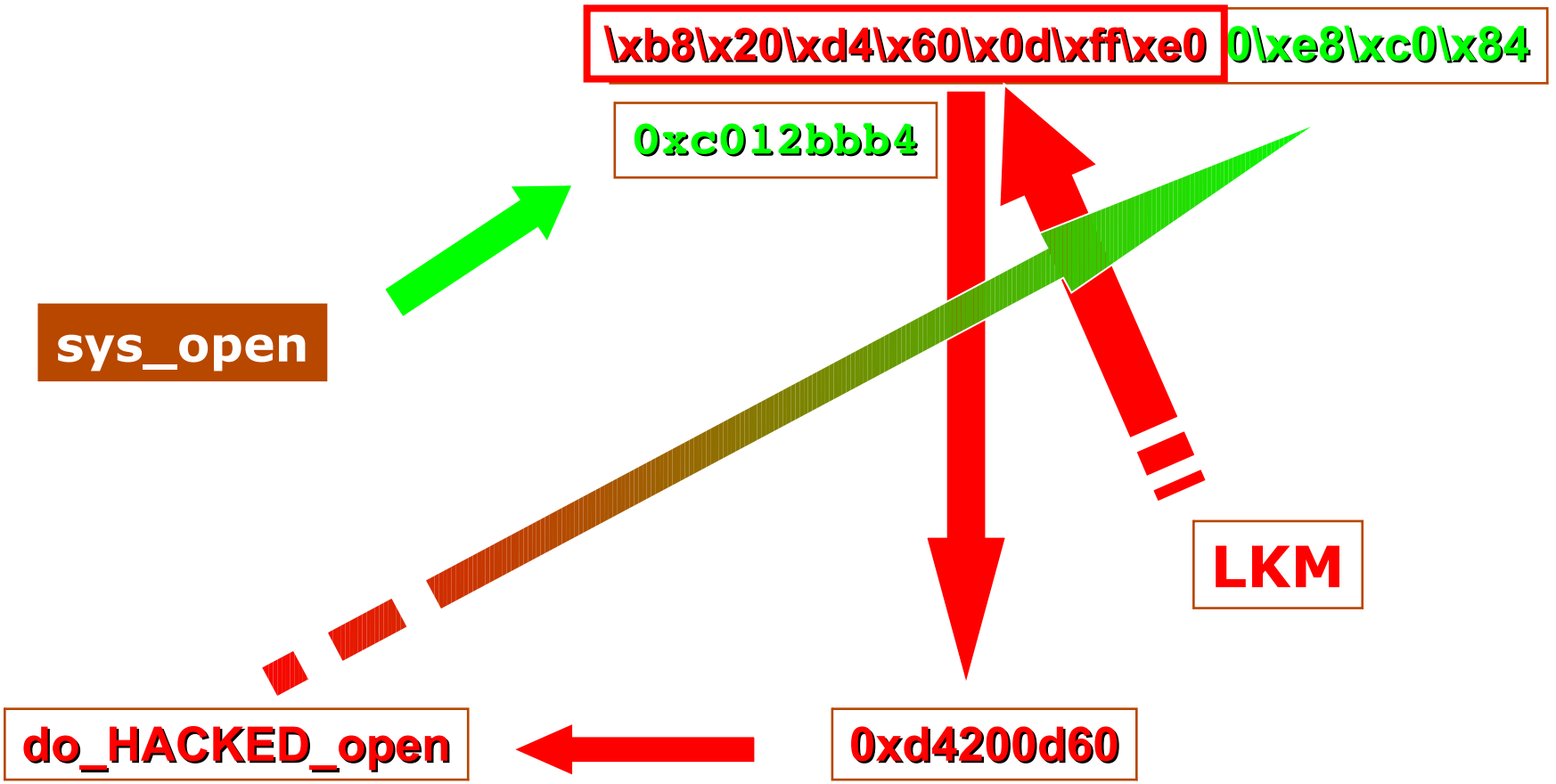
Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: Linux sys_call jump



Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: Linux sys_call jump



Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

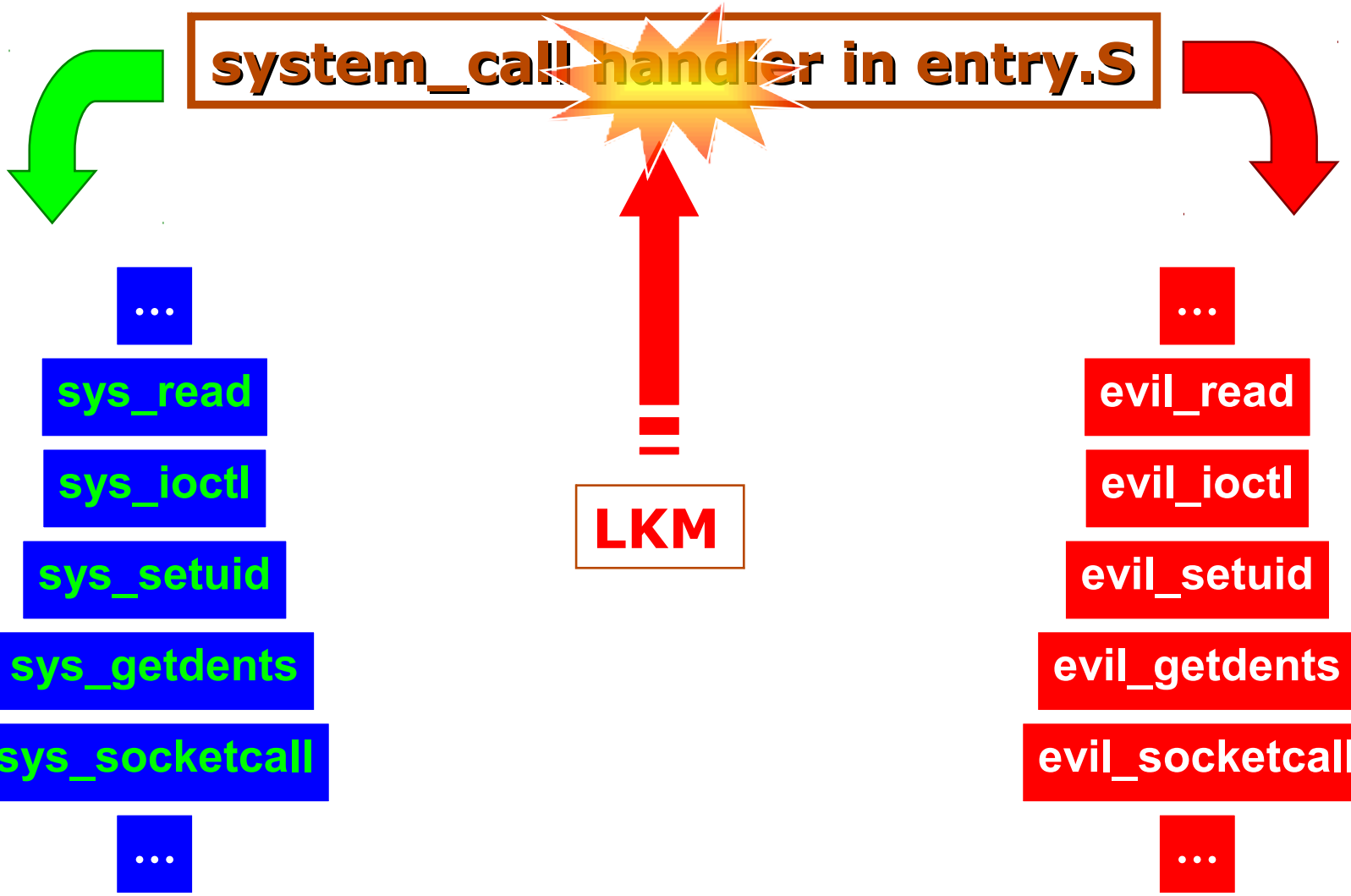
Case History: Linux IDT manipulation

```
unsigned sys_call_off,
sct;
char sc_asm[100], *p;
```

```
asm ("sidt %0" : "=m" (idtr));
readkmem (&idt, idtr.base + 8*0x80, sizeof(idt));
sys_call_off = (idt.off2 << 16) | idt.off1;
readkmem (sc_asm, sys_call_off, 100);
p = (char*)memmem (sc_asm, 100, "\xff\x14\x85",
3);
sct = *(unsigned*)(p+3);
```

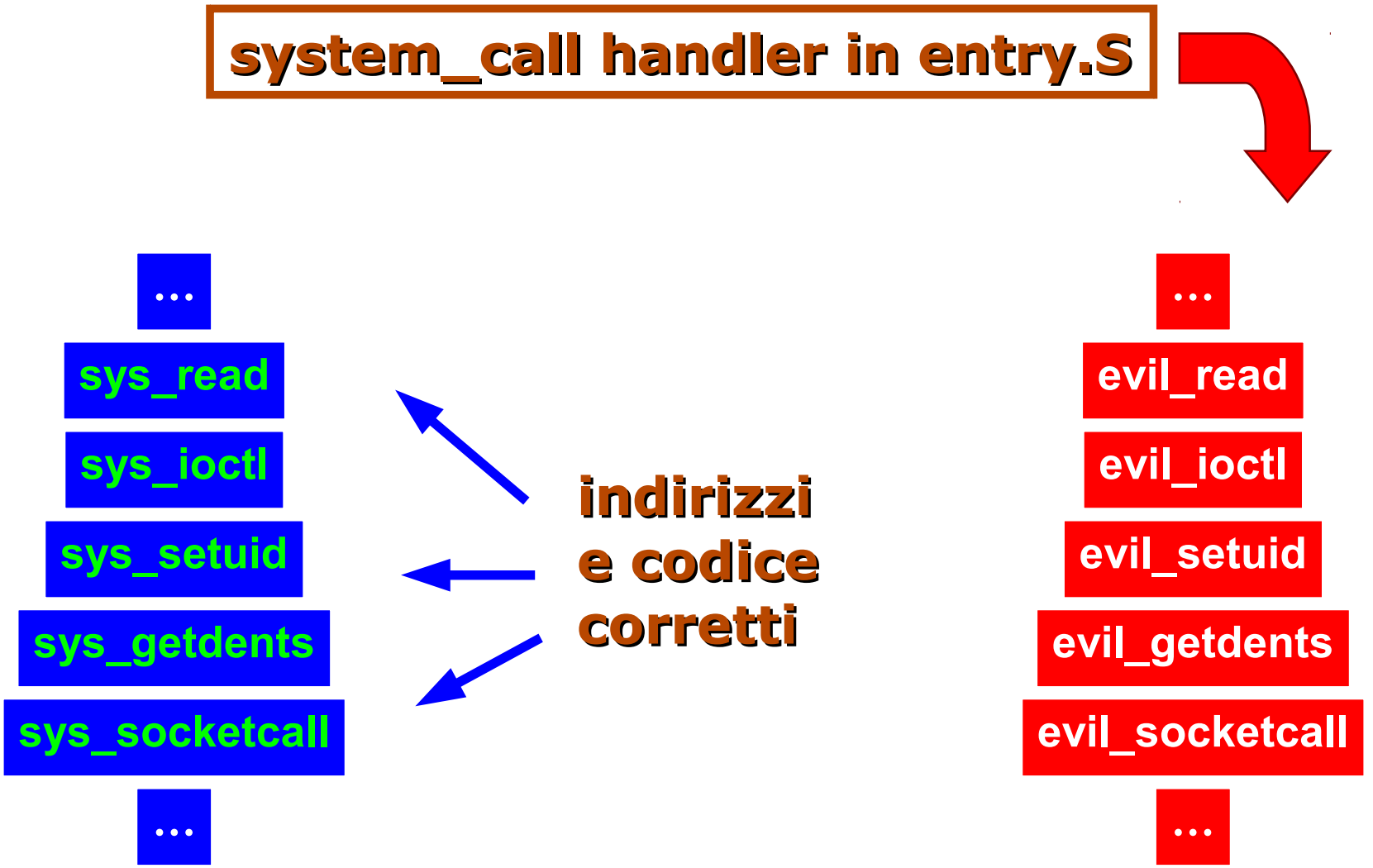

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: Linux IDT manipulation



Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: Linux IDT manipulation



Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Sovversione del Kernel

- Esistono molti strumenti che si basano sulle "**impronte**" lasciate da un kernel rootkit
- Purtroppo, come ogni signature-based, tali HIDS soffrono di **falsi negativi** per rootkit creati ad-hoc o modificati all'uopo (**0-day**)
- L'analisi della memoria virtuale e fisica del sistema si rende **necessaria** per valutare le possibili **discrepanze** presenti nei vari sotto-sistemi del kernel
- Purtroppo è necessario sapere cosa capiti "**dietro le quinte**" del sistema, per poterne identificare le anomalie

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Canali "Covert"

- Rappresentano una delle forme più **avanzate** di **backdoor**
- Permettono una comunicazione affidabile con il sistema compromesso, ma di "**basso profilo**" in termini di protocolli e flussi di comunicazione
- Spesso è molto **complesso** accorgersene

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: ICMP Tunneling

- **Semplice** esempio di comunicazione "covert"
- **Conosciuto** ed **ampiamente** documentato
- Indicativo del **reale pericolo** di questo tipo di strumenti (difficile da scoprire e da analizzare)

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: ICMP Tunneling

- 007Shell è una backdoor per Linux e Win32
- Offre una shell remota (bash, cmd.exe) **senza aprire porte TCP o UDP**
- Il flusso trasmissivo di I/O è incapsulato all'interno di messaggi ICMP di tipo **ECHO_REPLY**
- I dati possono essere o meno "**offuscati**"

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: ICMP Tunneling

```
13:44:53.686762 xxx.xxx.xxx.xxx > xxx.xxx.xxx.xxx: icmp: echo request
(ttl 2, id 2819, len 92)
0x0000   4500 005c 0b03 0000 0201 5a09 xxxx xxxx      E..\......Z.@|..
0x0010   xxxx xxxx 0800 a1fe 4100 1501 0000 0000      .{......A.......
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
```

Legenda

- IP Header
- ICMP Protocol Identifier
- ICMP Type
- ICMP Code
- ICMP Data

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: ICMP Tunneling

```
[root@SMAU 007Shell]# ./007Shell -c -h 10.0.0.14
007Shell v.1.0 - Let's Dig Covert !
[covert@007Shell]# pwd
 tmp
[covert@007Shell]# uname -a
Linux escort 2.4.7-10 #1 Thu Sep 6 17:27:27 EDT 2001
i686 unknown
[covert@007Shell]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/bin/nologin
gmorris:x:506:506::/home/gmorris:/bin/bash
[covert@007Shell]# snafuz!
See ya Covert, James ...
[root@SMAU 007Shell]#
```


Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: ICMP Tunneling

```
16:46:47.624065 10.0.0.14 > 10.0.0.62: icmp: echo reply (DF)
(ttl 64, id 0, len 71)
0x0000   4500 0047 0000 4000 4001 266b 0a00 000e    E..G..@.@.&k....
0x0010   0a00 003e 0000 2b88 0000 0000 0000 0000    ...>..+.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   7077 64                                    pwd.............
0x0040   0000 0000 0000 00                          .......
16:46:47.628191 10.0.0.62 > 10.0.0.14: icmp: echo reply (DF)
(ttl 64, id 0, len 73)
0x0000   4500 0049 0000 4000 4001 2669 0a00 003e    E..I..@.@.&i...>
0x0010   0a00 000e 0000 591b 0000 01f0 0000 0000    ......Y.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   2f74 6d70                                  /tmp............
0x0040   0000 0000 0000 0000 00                     .........
16:46:47.628450 10.0.0.62 > 10.0.0.14: icmp: echo reply (DF)
(ttl 64, id 0, len 68)
0x0000   4500 0044 0000 4000 4001 266e 0a00 003e    E..D..@.@.&n...>
0x0010   0a00 000e 0000 ffff 0000 02f0 0000 0000    ................
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0040   0000 0000                                  ....
```


Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: ICMP Tunneling

```
16:46:47.624065 10.0.0.14 > 10.0.0.62: icmp: echo reply (DF)
(ttl 64, id 0, len 71)
0x0000   4500 0047 0000 4000 4001 266b 0a00 000e    E..G..@.@.&k....
0x0010   0a00 003e 0000 2b88 0000 0000 0000 0000    ...>..+.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   7077 64                                    pwd.............
0x0040   0000 0000 0000 00                          .......
16:46:47.628191 10.0.0.62 > 10.0.0.14: icmp: echo reply (DF)
(ttl 64, id 0, len 73)
0x0000   4500 0049 0000 4000 4001 2669 0a00 003e    E..I..@.@.&i...>
0x0010   0a00 000e 0000 591b 0000 01f0 0000 0000    ......Y.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   2f74 6d70                                  /tmp............
0x0040   0000 0000 0000 0000 00                     .........
16:46:47.628450 10.0.0.62 > 10.0.0.14: icmp: echo reply (DF)
(ttl 64, id 0, len 68)
0x0000   4500 0044 0000 4000 4001 266e 0a00 003e    E..D..@.@.&n...>
0x0010   0a00 000e 0000 ffff 0000 02f0 0000 0000    ................
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0040   0000 0000                                  ....
```


Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: ICMP Tunneling

```
16:46:47.624065 10.0.0.14 > 10.0.0.62: icmp: echo reply (DF)
(ttl 64, id 0, len 71)
0x0000   4500 0047 0000 4000 4001 266b 0a00 000e    E..G..@.@.&k....
0x0010   0a00 003e 0000 2b88 0000 0800 0000 0000    ...>..+.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   3b71 e4 0000 0000 0000 0000 0000 0000      pwd............
0x0040   0000 0000 0000 00                          .......
16:46:47.628191 10.0.0.62 > 10.0.0.14: icmp: echo reply (DF)
(ttl 64, id 0, len 73)
0x0000   4500 0049 0000 4000 4001 2669 0a00 003e    E..I..@.@.&i...>
0x0010   0a00 000e 0000 591b 0000 0800 0000 0000    ......Y.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000    ................
0x0030   2526 6d70 0a                               %&mp............
0x0040   0000 0000 0000 0000 00                     .........
16:46:47.628450 10.0.0.62 > 10.0.0.14: icmp: echo reply (DF)
(ttl 64, id 0, len 68)
0x0000   4500 0044 0000 4000 4001 266e 0a00 003e    E..D..@.@.&n...>
0x0010   0a00 000e 0000 ffff 0000 0800 6162 6364    ............abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374    efghijklmnopqrst
0x0030   7576 7778 797a 6162 6364 6566 6768 696a    uvwxyzabcdefghij
0x0040   6b6c 6d6e 6f70 7172 73                     klmnopqrs
```


Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Data Hiding

- Le directory nascoste **non** rappresentano "**l'ultima frontiera**"
- **Ogni filesystem** cui l'attaccante abbia accesso può diventare un repository più o meno stealth (stampanti, appliance, telecamere IP, ...)
- Conosciute a livello teorico ma ancora non sfruttate "**in the wild**" sono le **manipolazioni a basso livello** dei filesystem (inode, metadata, journal, swap, ...)

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: BigBoo

- Questo semplice tool crea delle aree riservate su disco in un filesystem ext2 o in uno swapfile Linux
- I blocchi utilizzati saranno marcati come **BAD** all'interno dell'inode 1 (ext2) o come **BAD_PAGE** (swap)
- Esistono altri codici di questo tipo (quasi tutti sotto forma di proof of concept), ma il loro numero è ancora esiguo

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: BigBoo

- # ./BigBoo -h
- Uso: ./BigBoo -i -s|-b -l -f [-e] [-c file] [-x file] -v [-h|-?]
- -i modalita' interattiva (pseudoshell)
- -s crea BAD_PAGES nello swapfile
- -b utilizza BAD_BLOCK
- -l mostra i file nascosti
- -f elimina l'area di storage
- -e utilizza la crittografia per proteggere i dati
- -c copia il file nell'area di storage
- -x estrai il file dall'area di storage
- -v chiedi a BigBoo di essere prolisso
- -h questo noioso messaggio

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: BigBoo

- # ./BigBoo -i -v
- Welcome to the Ghost House.
- boo> swcp /boot/vmlinuz-2.6.7-new
- Tento di allocare 516 pagine nello swapfile /dev/hda2...
- Numero totale di pagine marcate bad = 516
- Creo boo_sb in /dev/hda13
- boo> swls
- file presenti: 1
- sB/boot/vmlinuz-2.6.7-new 2108877 bytes
PAGINA 1280
- boo>

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: BigBoo

- **Non tutti** i tool forensi analizzano i bad block o le pagine degli swapfile
- In ogni caso il contenuto dei blocchi interessati è stato **cifrato** e le operazioni di copia potrebbero essere interfacciate ad un **socket**
- Questo software mantiene, **senza cifrarli**, i metadata relativi ai file nascosti all'interno del superblock della partizione scelta dall'attaccante
- Il superblock contiene **coppie di valori numerici** che mostrano una **forte correlazione** con i risultati di dumpe2fs(8) per quanto riguarda i blocchi marcati come bad

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Case History: BigBoo

- L'anomalia più evidente si palesa qualora l'attaccante decida di **cancellare un file dall'area nascosta**
- Se può essere strano che un hard disk mostri da un giorno all'altro un certo numero di bad block, cosa potrebbe causare un aumento ed una diminuzione del numero totale di blocchi **nell'unità di tempo**, soprattutto quando sono sempre gli stessi ?
- Ma quanti sistemisti analizzano l'output di dumpe2fs(8) nonostante tengano sott'occhio i valori SMART ?

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Dubbi

- La maggior parte dei tool forensi **non** è **flessibile**: la staticità delle procedure può portare ad un senso di falsa sicurezza o falsa comprensione ?
- I tool migliori sono flessibili quanto il loro utilizzatore **umano**. Ma al di fuori degli usuali exploit e script pre-confezionati, l'avversario è un essere umano spesso **molto** flessibile
- L'analisi di un **sistema compromesso** è ben **differente** dall'analisi del **computer di un indiziato**

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it

Domande ?

smau 2005

e-Academy

Gestione Incidenti Informatici

enforcer

Matteo Falsetti
mfalsetti@enforcer.it

Sovversione del sistema – SMAU Milano 22/10/2005 – mfalsetti@enforcer.it