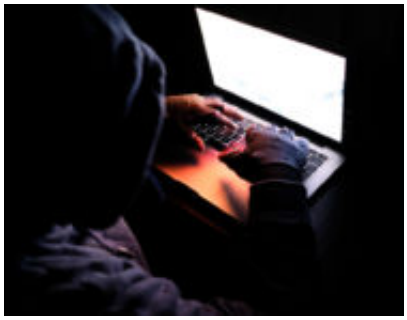
Rischi dell'accesso fisico non autorizzato

Author : Daniele Rigitano

Date : 23 maggio 2018



Prefazione

Come reagireste se affermassi che i tre maggiori Sistemi Operativi (SO) in commercio - Windows, Linux e MacOSX - contengono al loro interno una falla che permette, in pochi e semplici passi, il pieno accesso ai dati archiviati nei vostri Personal Computer (PC)?

Se aggiungessi che non importa quanto è complessa la vostra *passphrase* di accesso, poiché chiunque abbia la possibilità di “mettere le mani” sul vostro PC può bypassarla, o resettarla, a proprio piacimento?

Infine, ultimo ma non meno importante, se affermassi che i suddetti produttori di SO sono da lungo tempo a conoscenza di queste falle. Anzi, che alcune di esse non fossero considerate “falle”, ma vere e proprie “**feature**” dei loro SO?

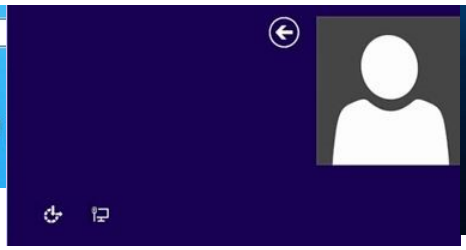
Seguitemi e vi illustrerò alcuni metodi con i quali un’utente malevolo, sfruttando tali *feature*, può prendere il pieno controllo del dispositivo reimpostando le password utente e/o creando account di tipo amministratore.

Microsoft Windows

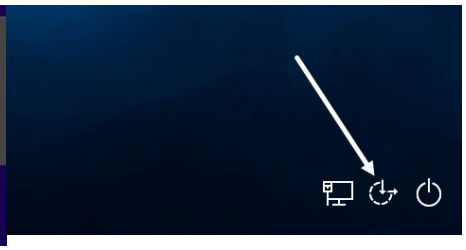
Il SO di casa Redmond, da Windows XP in poi, mette a disposizione nella schermata di Logon un utility per l’“accessibilità”. Questa dovrebbe consentire di facilitare l’uso del computer ad ipovedenti e non udenti, tramite le funzionalità: *assistente vocale*, *lente di ingrandimento* e *contrasto elevato*. Ma la cosa, come vedremo, nasconde anche alcune insidie.

La procedura per reimpostare la password, infatti, si basa proprio su questa utility e fa capo all’eseguibile **utilman.exe**.

Windows 7



Windows 8/8.1



Windows 10

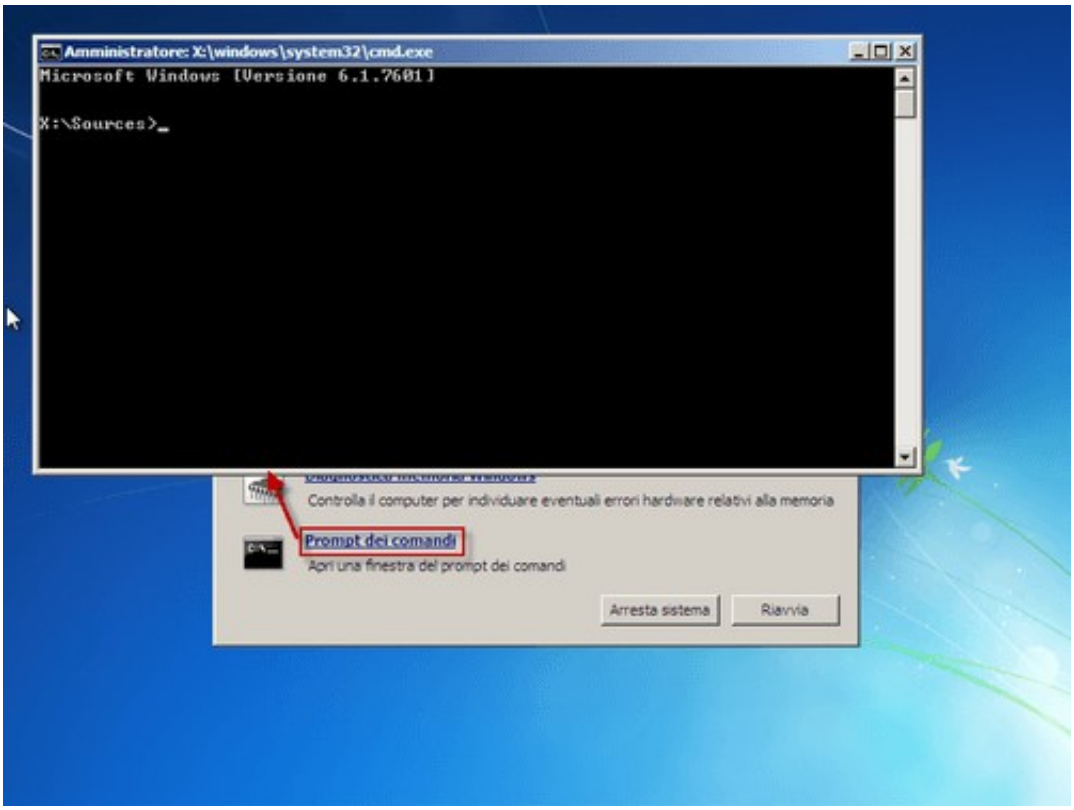
Per effettuare un cambio password o la creazione di un'utenza amministrativa, pertanto, abbiamo la necessità di poter accedere al *Prompt dei Comandi*, quindi all'eseguibile cmd.exe.

L'idea è quella di sovrascrivere utilman.exe con cmd.exe, in modo da poter avviare il *prompt*, invece di utilman. In questo modo si avrebbe la possibilità di eseguire i comandi necessari per ottenere quanto detto in precedenza dalla schermata di Logon.

Ma per far questo dobbiamo modificare i rispettivi file eseguibili, dal momento che sono entrambi file di sistema, senza però avere alcun tipo di utenza sul dispositivo.

L'operazione, proposta in tre semplici passi, è tanto semplice quanto disarmante; occorre:

1. munirsi di un disco/pendrive di avvio di Windows;
2. avviare la modalità di "Ripristino del Computer" dal disco di avvio;
3. selezionare l'opzione di ripristino tramite *Prompt dei Comandi*, per ottenere una shell con privilegi amministrativi sulla macchina vittima.



Successivamente basta eseguire la sequenza di comandi di seguito elencata per sostituire utilman.exe con cmd.exe.

```
move

copy C:\Windows\System32\cmd.exe c:\Windows\System32\Utilman.exe
```

Fatto ciò, non rimane che riavviare e, appena possibile, selezionare l’icona di accessibilità per ottenere un prompt dei comandi in modalità amministratore.

A questo punto è possibile digitare quanto segue per creare un’utenza amministrativa.

```
net user  /add  net localgroup administrators  /add
```

Infine, per non lasciare tracce di quanto effettuato, ripristiniamo l’utility utilman originale.

```
del
 C:\Windows\System32\Utilman.exe  ren
 C:\Windows\System32\Utilman.exe.bak Utilman.exe
```

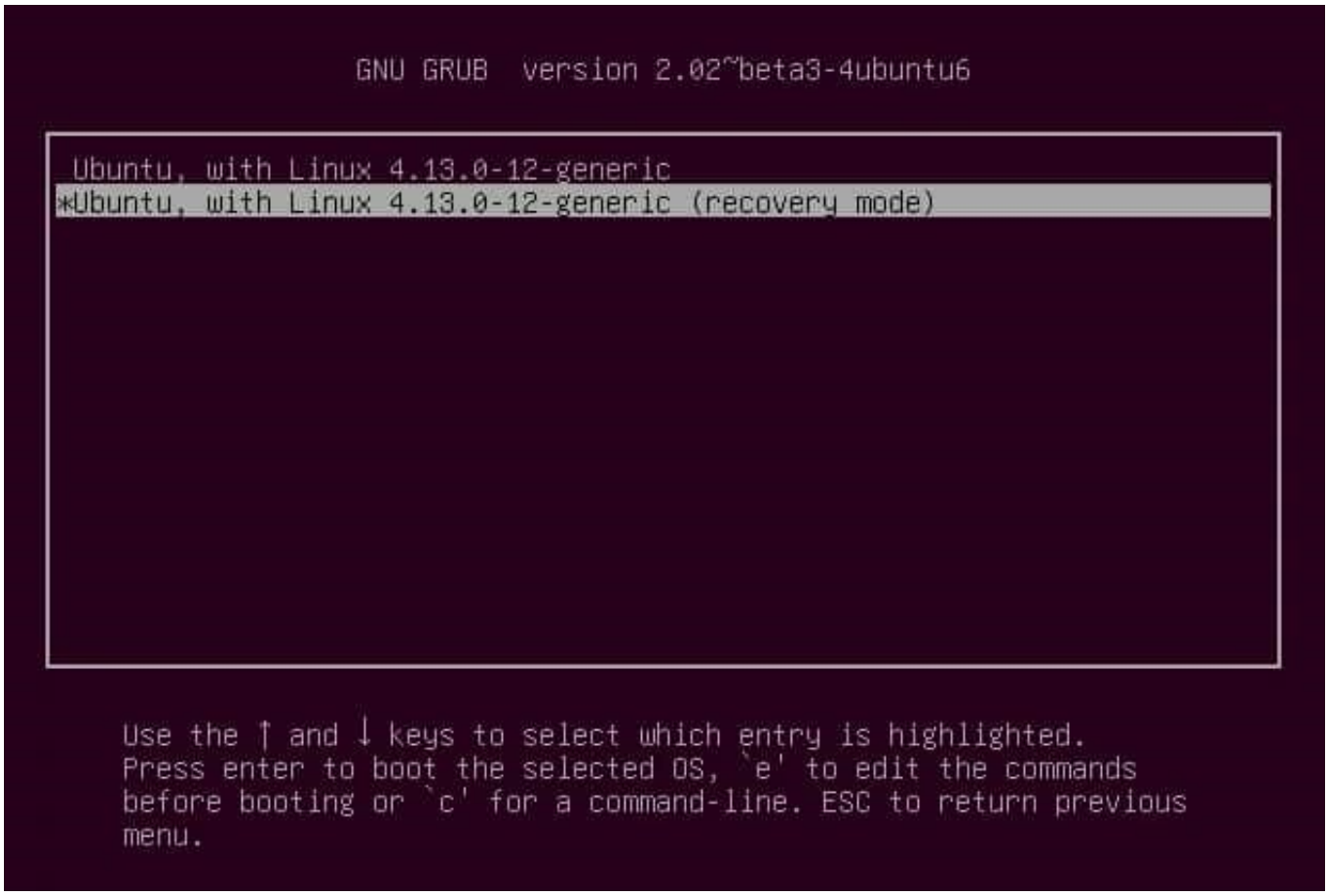
Al termine dell’azione “malevola” si può inoltre, ove possibile, riportare il sistema ad un punto di ripristino precedente, in modo da non destare alcun sospetto verso gli utilizzatori della macchina.

Linux

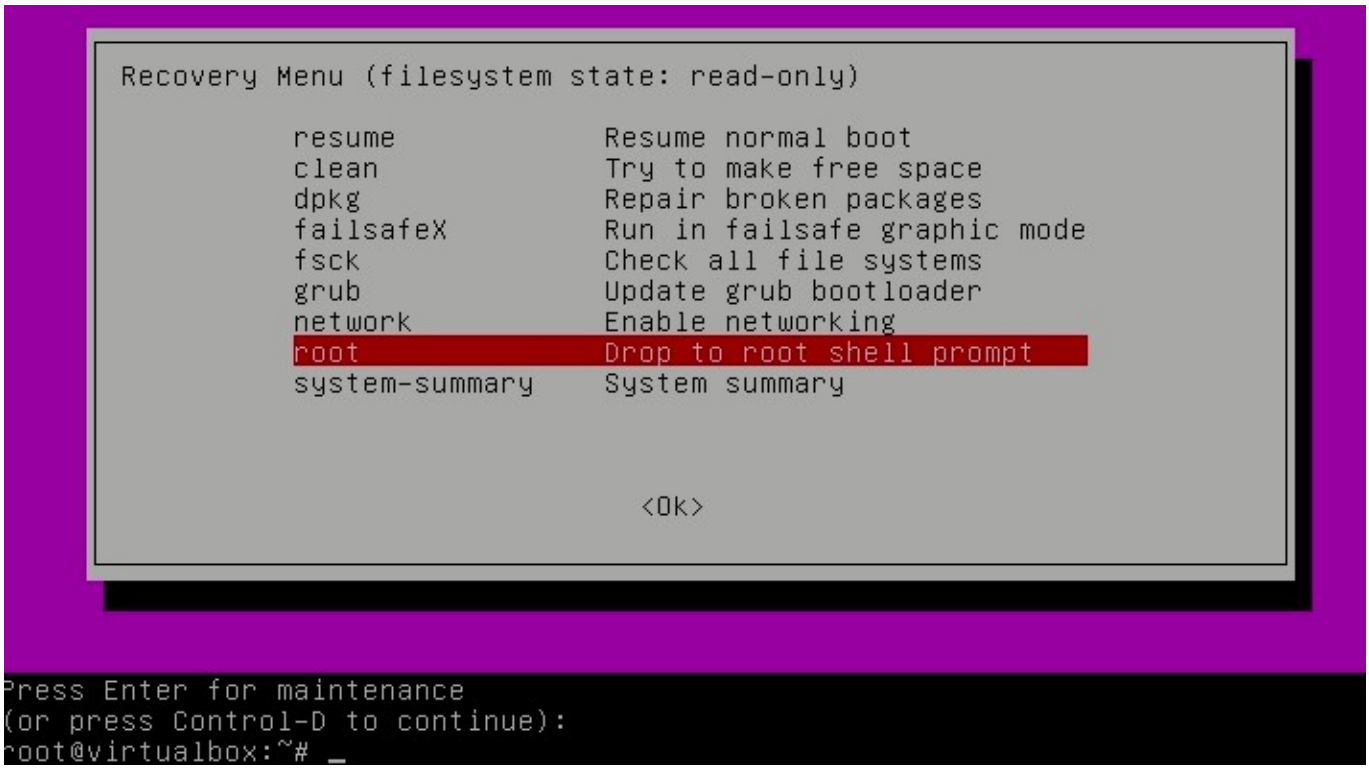
Anche il SO targato Torvalds & Stallman prevede semplici metodologie di recupero password.

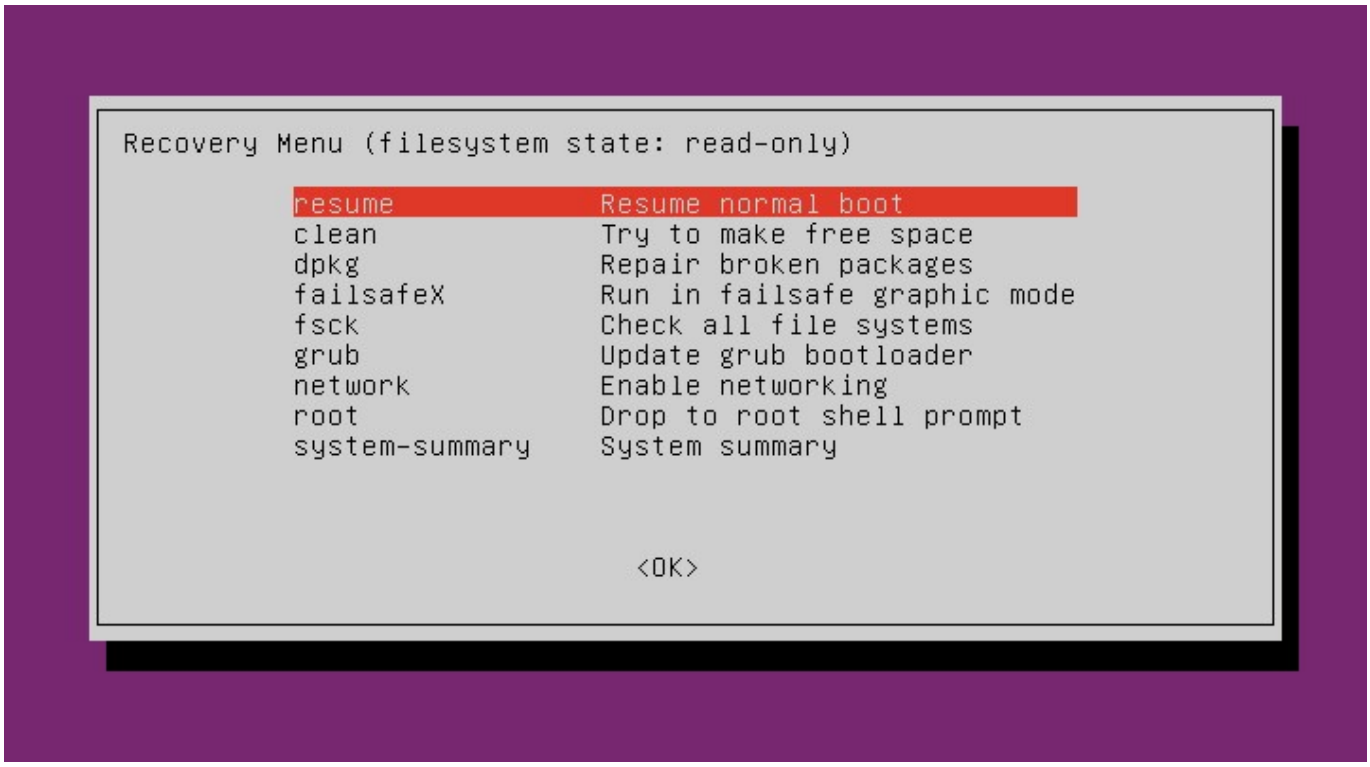
Prendiamo in esame una delle distribuzioni più usata dagli utenti Linux: Ubuntu.

Durante la fase di boot tenendo premuto il tasto “shift”, si accede alla schermata del bootloader grub 2 che permette di selezionare la modalità di ripristino del SO tramite l’opzione “*Advanced options for Ubuntu”.*



Dalla console di ripristino è possibile selezionare l’opzione che consente l’avvio di una shell di root:





A questo punto, resettare una qualsiasi password utente diventa molto semplice.

Per prima cosa è necessario garantirsi i permessi di accesso sulla partizione di root:

```
mount -rw -o remount /
```

Questa operazione abilita la possibilità di resettare la password di un qualsivoglia utente:

```
passwd   exit
```

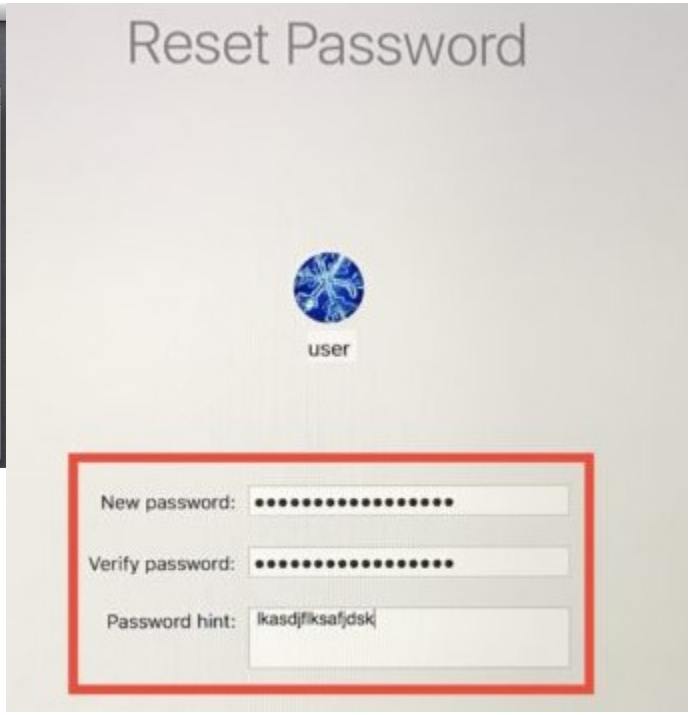
Infine, a seguito del comando exit, si torna al menu della modalità di ripristino, dalla quale è possibile selezionare l'opzione per riprendere il normale avvio del SO.

MacOsX

Anche la casa di Cupertino permette di ripristinare una password utente tramite console di ripristino.

Per fare ciò, occorre avviare il Macintosh facendo pressione contemporaneamente sui tasti *accensione* + *Command* + *R*.

Dopo qualche minuto si accederà alla console di ripristino: dalla barra del menù occorre selezionare
Utilità à *Terminale*.



Il comando da digitare è *resetpassword*: dopo qualche attimo comparirà la schermata che consente di selezionare l'utente per il quale si intende resettare la password.

A questo punto non ci resta che digitare semplicemente i caratteri della nuova *passphrase* negli appositi campi, cliccare su avanti ed infine riavviare.

Conclusioni

Quanto esposto nei paragrafi precedenti, a primo impatto, potrebbe essere giudicato inammissibile. In realtà per quanto riguarda Linux e MacOsX, tali funzionalità sono perfettamente previste dalle procedure di ripristino dei propri SO.

Più delicato è l'ambito Microsoft. In questo caso la procedura che sfrutta il componente utilman.exe è stata inizialmente considerata un possibile bug di sviluppo tant'è che qualcuno, tra gli altri anche lo scrivente, ha deciso di contattare il supporto Microsoft per chiedere lumi e sciogliere le riserve a riguardo.

In risposta, il supporto Microsoft ha giudicato la propria schermata di Logon totalmente sicura. Aggiungendo che, a loro avviso, la *reale* vulnerabilità insiste nella possibilità di accedere fisicamente al sistema. In parole povere secondo Microsoft, se un utente malevolo ha la possibilità di "mettere le mani" fisicamente su un dispositivo, quest'ultimo è da considerarsi intrinsecamente vulnerabile e, pertanto, assoggettabile a qualsiasi tipo di manomissione e/o compromissione.

A questo punto, almeno due domande nascono spontanee:

1. a cosa servono le certificazioni dei SO che, secondo l'Orange Book, sono valutabili in base a quattro classi di "fiducia": da D (meno sicuro) ad A (più sicuro)?
    1. Nello specifico poiché Windows è certificato EAL4+, posizionabile tra TCSEC B1 e B2, come si giustifica questa carenza in sicurezza fisica rispetto a quanto richiesto da tale livello di sicurezza?

TCSEC	ITSEC	CC
D	E0	No equivalent
No equivalent	No equivalent	EAL1
C1	E1	EAL2
C2	E2	EAL3
B1	E3	EAL4
B2	E4	EAL5
B3	E5	EAL6
A1	E6	EAL7

2. cosa dovrebbe quindi fare uno sventurato utente che vede la sicurezza fisica del suo dispositivo compromessa?

Non si possono di certo inibire le periferiche CD/DVD/USB tramite BIOS, sarebbe una grave

perdita di usabilità, né tantomeno eliminare le funzionalità previste dalle procedure di ripristino.

Ed allora, cosa fare? Di seguito qualche consiglio:

Tralasciando soluzioni esotiche quali mettere sotto chiave il proprio PC o installare costosissimi impianti di sicurezza audio/video, la soluzione è molto semplice: la **crittografia**.

Abilitando rispettivamente *Bitlocker*, *Ubuntu Encrypted Custom Install* e *FileVault*, quanto esposto nei paragrafi precedenti risulta non attuabile a meno che non si conosca l'apposita chiave di cifratura, poiché il sistema cifra l'intera partizione di avvio.

A cura di: **Daniele Rigitano**