

VirtualBox virtuális gépeinek titkosítása

PCLinuxOS Magazine – 2017. június

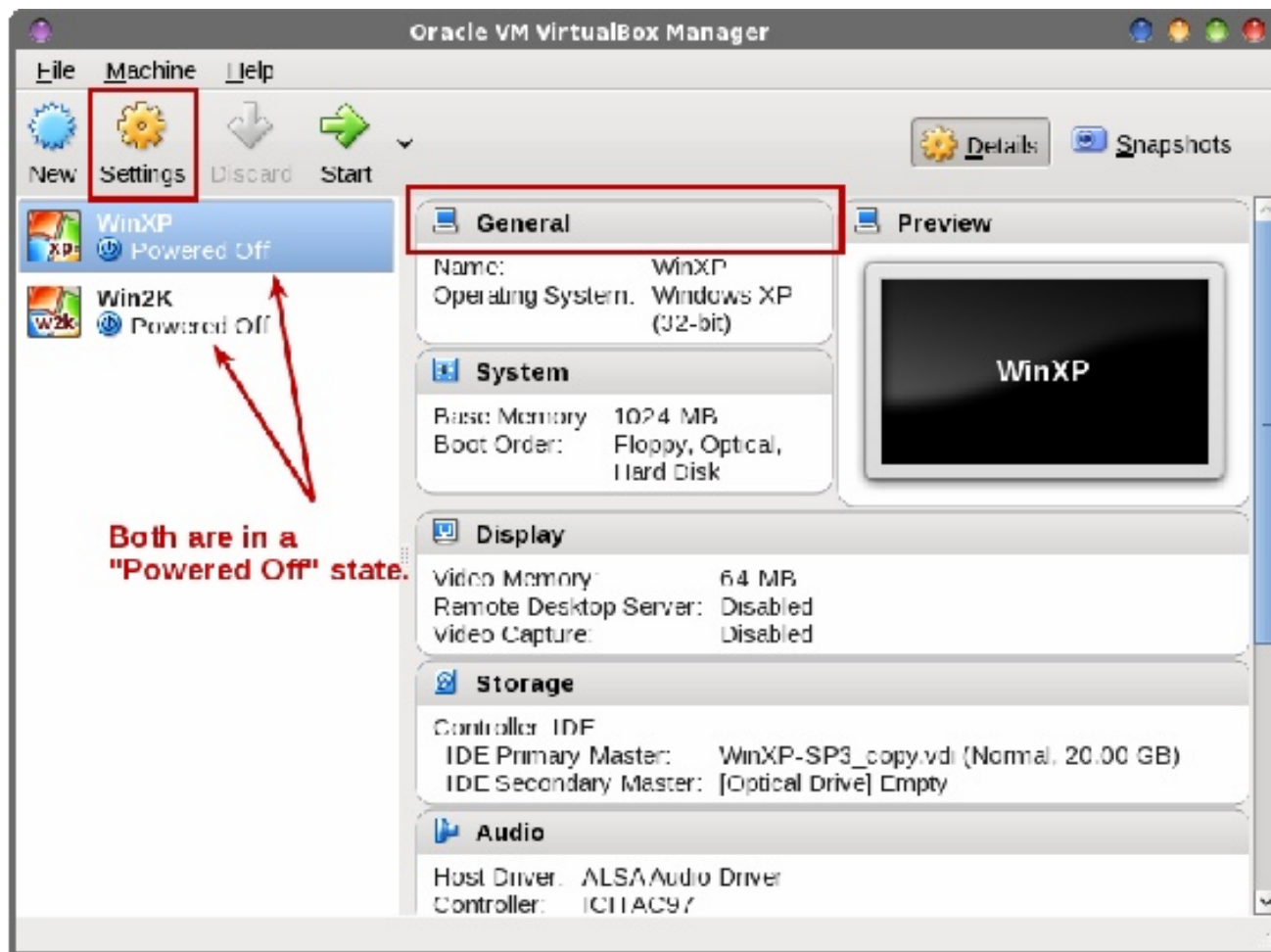
Írta: Paul Arnote (parnote)

A Virtual Box egyik újdonsága (5.x-től kezdődően), hogy lehetővé teszi a virtuális gépeken a virtuális merevlemez titkosítását. Napjaink számítástechnikai környezetében, amikor a privát szférád minden oldalról folyamatos támadásnak van kitéve, szükségét érezheted a Virtual Box-os VM-ed titkosításának.

Ne kapkodd el a titkosítás elutasítását. Például itt, az USA-ban sokan használunk (és veszünk) jövedelemadó számító programot, hogy kitöltsük és bevalljuk a jövedelemadónkat. Azok között a fájlok között van néhány NAGYON kényes és személyes adat, amik végzetes romboláshoz vezethetnek, ha rossz kezekbe kerülnek.

Ha nem online szolgáltatást használsz a jövedelemadó-bevallás kitöltésre és beadására (ami egy teljesen más biztonsági problémakör), az összes adó-szoftver sajnos csak Windows, iOS, vagy Android alatt fut. Nincs olyan, ami alaptól Linuxon menne. Ilyetén módon, Linux alatt alaptól futó adó-szoftver hiányában a Linux-felhasználók arra kényszerülnek, hogy virtuális gépen, általában VirtualBox-ban, futtassák a kiválasztott szoftvert.

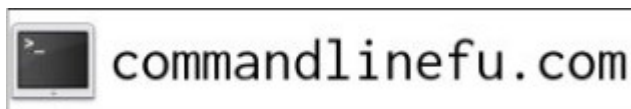
Ez csak egy példa azokra a magán, személyes, kényes adatokra, amiket nem akarsz gátlástalan kezekbe adni. Biztosan eszedbe jutnak olyan adatfajták, amik a te esetedben relevánsak lehetnek. A a VirtualBox virtuális gépeinek titkosítási lehetősége segíthet abban, hogy biztosítsd, a kényes adataid ne kerülhessenek rossz kezekbe.



Hogyan csináljuk

Induljunk ki abból, hogy már van telepített VM-ed. A VM legyen kikapcsolva. A VM titkosítását nem végezheted el, ha az felfüggesztett, vagy „felvétel” állásban van.

Ezután, ki kell választanod a titkosítandó Vm-et. Ellenőrizd, hogy a VM „Kikapcsolt”-at jelezzen a VM állapotát illetően. Ha nem az, akkor indítsd el a VM-et és megfelelően kapcsolj ki. Ezután kattints akár a „Beállítások” ikonra az eszközsávon, akár az „Általános” feliratra az ablak közepe felé (a fenti képen pirossal kiemelve).





Most helyezze jelölést a „Titkosítás bekapcsolása” elé és válassza ki a használni kívánt titkosítási szintet. A lehetőségek akár AES-XTS256-PLAIN64 (mutatom), vagy AES-XTS128-PLAIN64. A különbség az, hogy 128, vagy 256 bites titkosítást használ. A harmadik lehetőség (az alapbeállítás), „hagyj változatlanul”, nem tűnik értelmes választásnak. Így írás közben el nem tudom képzelni, hogy miért akarná valaki is ezt a lehetőséget alkalmazni.

Ahogy az az összes jelszónál szokott lenni, válassz egy erős jelszót, keverve a kis- és nagybetűket, számokat, szimbólumokat és írásjeleket. Előre figyelmeztetek, valaki már készített [eszközt](#), amivel a gyenge jelszavakat használó VirtualBox VM-ek titkosítása feltörhető. Az eszköz „brute force” módszert alkalmaz, amitől a gyenge jelszó úgy omlik

össze mint Jerikó falai, hasztalanná téve a titkosítást – és potenciálisan kitéve az adataidat fűrkésző szemeknek ... vagy rosszabbnak.

Erre gondolva írd be egy BIZTONSÁGOS jelszót az első jelszó beviteli négyzetbe. Majd, írd be újra a jelszavadat a második jelszó beviteli négyzetbe megerősítésül. Most csak kattints az OK-ra.

Amikor leütötte az OK gombot, menj és foglald el magad. Készíts szendvicset, vagy csipeget valamit. A VirtualBox az egész virtuális merevlemezdet titkosítja, ami eltarthat egy darabig. Unalmas lehet nézni és várni, ahogy a előrehaladás-jelző halad a 100%-os készenlét felé.



Innentől kezdve, bármikor indítod el a virtuális gépedet, kérni fogja a VM-jelszavadat.

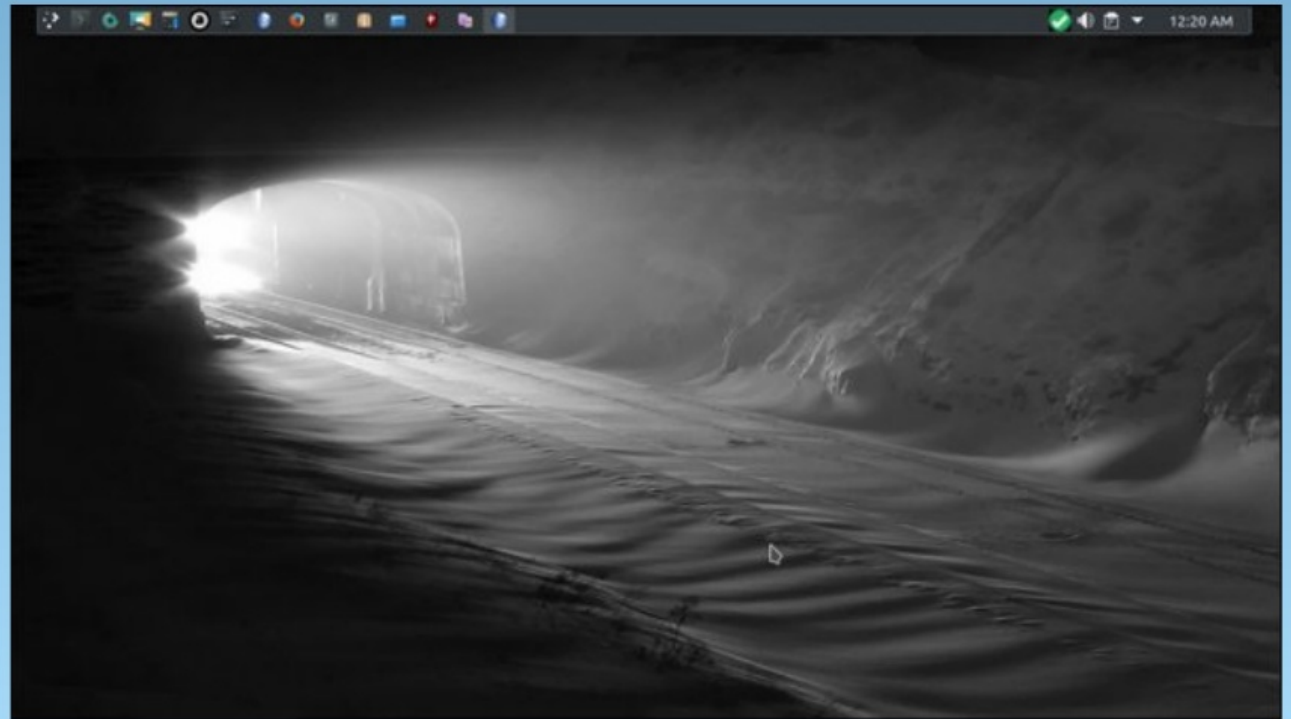
Összegzés

Napjainkban a személyes tered és adataid többirányú támadásnak vannak kitéve, nem lehetsz elég óvatos az adataiddal. Egy csepp megelőzés többet ér mint egy hektónyi kezelés. Ám ha az adataid egyszer rossz kezekbe kerültek, nincs ellenszer. Ez alkalommal a megelőzés a gyógyszer maga. Védj az adataidat, mindenképp óvd meg azokat a nyilvánosságra kerüléstől.

Köszönd meg, hogy a VirtualBox eszközöket ad a kezébe az adataid védelméhez. Ha nem használod az eszközöket, akkor csak magadat hibáztathatod bármilyen biztonsági rés esetén.



Screenshot Showcase



Posted by pirate, May 18, 2017, running KDE.

