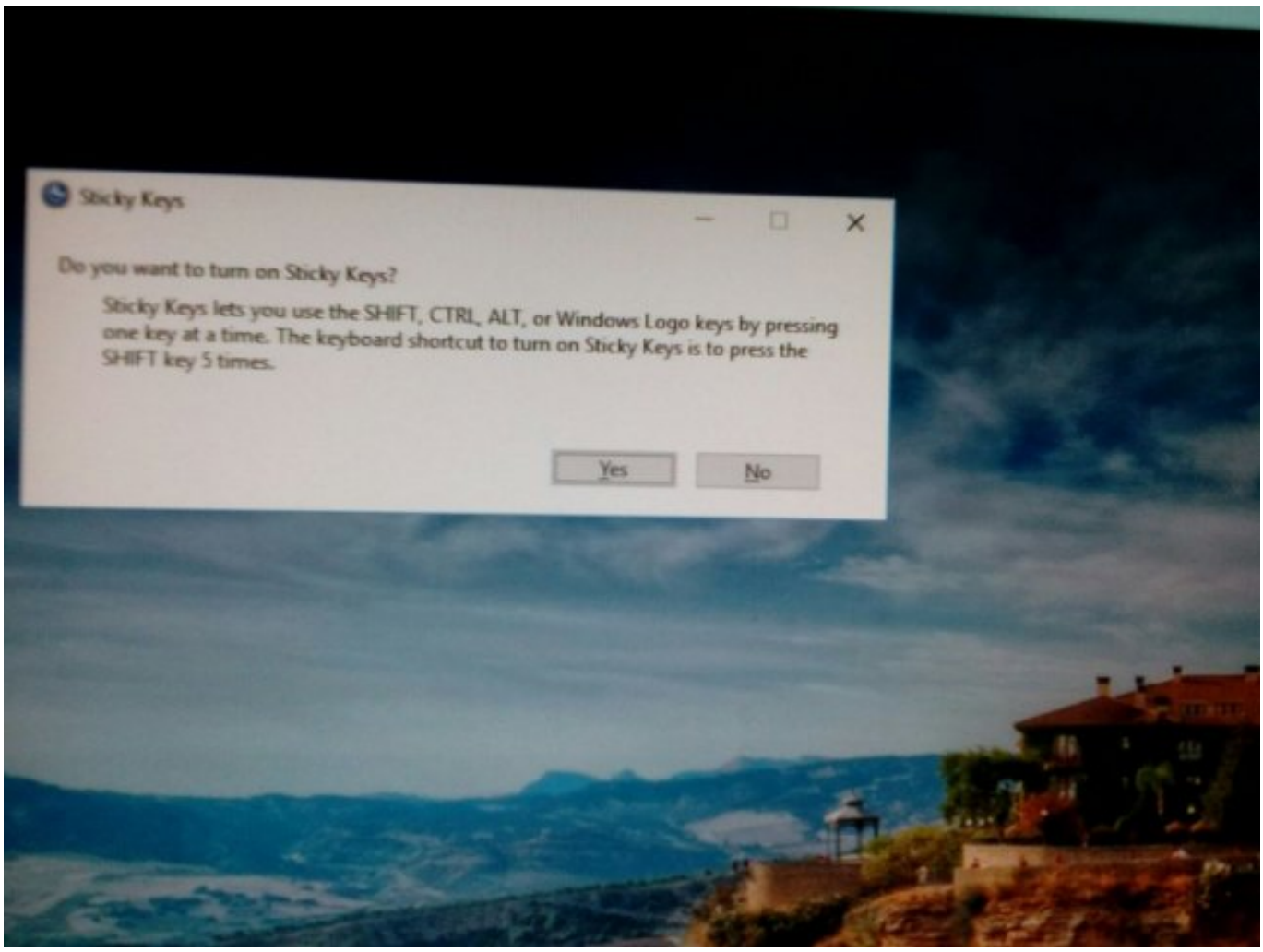
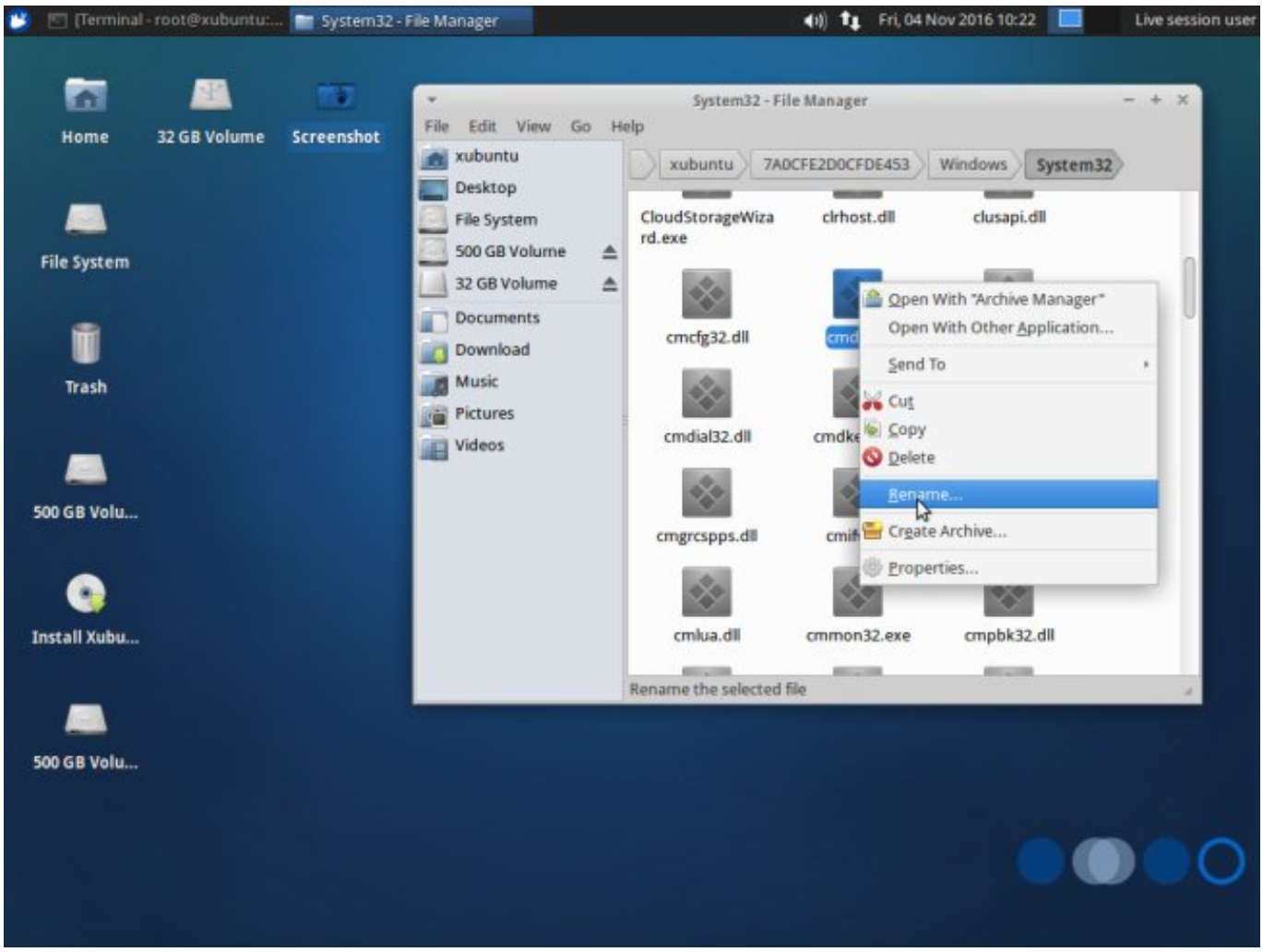
Zaboravljena administratorska lozinka na Windowsima 10

Sigurno ste se u svom poslu sistemca mnogo puta našli u situaciji da trebate resetirati administratorsku lozinku na *Windows* sistemu. Uputa u čarobnom svijet Interneta ima dovoljno, neke su više, neke manje uspješne. Otkako su izašli *Windows 10* neminovno je da se zaboravljaju lozinke i na tom sustavu. Ovaj slučaj se desio na privatnom laptopu korisnika koji su postavili administratorsku lozinku i ubrzo je zaboravili. Laptop su donijeli jednom kolegi koji je pokušao sa nekoliko "starih" načina resetiranja, ali bez uspjeha, pa je zatražio pomoć. *O*dmah je proradila profesionalna znatiželja koja "čuči" u svakom "pravom" sistemcu. Nakon pretraživanja Interneta i eliminacije "sumnjivih" metoda, uočavamo jednu koja koristi *Linux Live CD*, s kojom smo uspješno odradili zadatak. Vjerojatno se može iskoristiti i na drugim verzijama *Windows* sustava.

Zapravo metoda koristi jedan "prljavi trik" koji nam dozvoljava da zaobiđemo *GUI* prijavu na Windows i dobijemo administratorske ovlasti pomoću *Ubuntu* instalacijskog CD medija. Zapravo iskorištavamo *defaultno* uključen mehanizam zvan "Sticky Keys", dio *Windows Ease of Access* mogućnosti koja omogućava da za neke prečice tipkovice ili velika slova ne morate držati više tipaka pritisnutih u isto vrijeme. Kad uključite "Sticky Keys" mehanizam pozivom, *Windowsi* interpertiraju vaš pojedinačni stisak *Ctrl - Alt - Del*, kao da su pritisnute istovremeno. Kome uopće koristi ovakva funkcija prečica? Po informacijama jedan od razloga su hendikepirane osobe s fizičkim nedostatkom. Čemu sada ova priča a članak je o resetiranju administratorske lozinke? Evo zašto. Nakon što smo došli do prijave na *Windows 10* sustav, stisnimo 5-6 puta *Shift* tipku. Pojavi se "Sticky keys" dijalog.



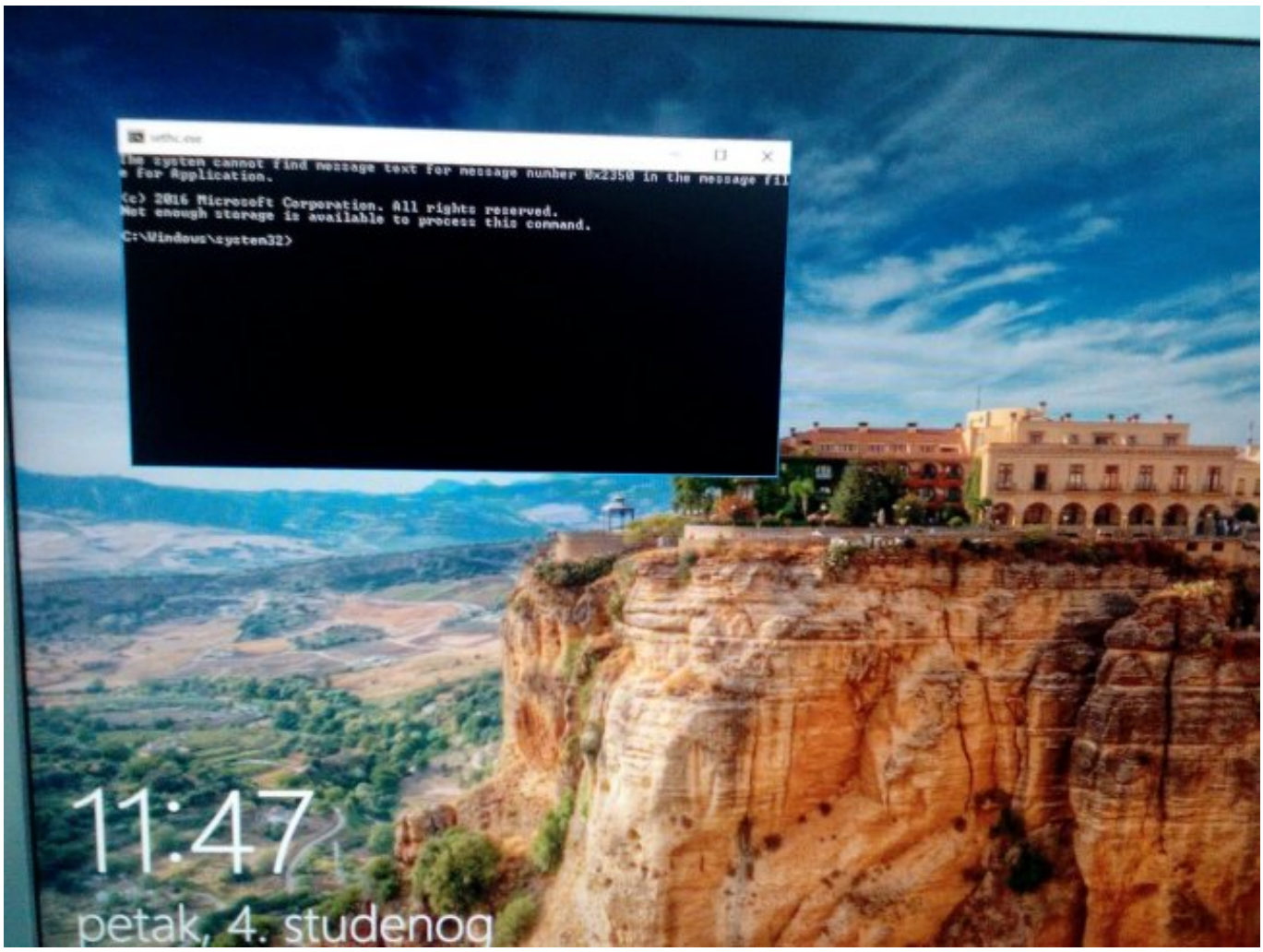
Ok. Što s tim napraviti ? Želimo doći do administratorskih ovlasti na sistemu. Da li se može napraviti da 5 puta pritisnemo *Shift* i dobijemo *command prompt?* Po ovoj uputi može :) Ubacimo *Ubuntu* instalacijski medij i podignemo *live* sistem bez instalacije na disk. Pomoću postojećeg *File Managera* okrijemo u našem slučaju putanju, */media/xubuntu/7A0CFE2D0CFDE453/Windows/System32*. U njemu se nalazi *cmd.exe* kojeg se želimo "dokopati".



U istom direktoriju nalazi se izvršna datoteka *sethc.exe,* naš "Sticky Keys" sa početka priče. Ako zamjenimo uloge ovim dvjema datotekama, dobivamo mogućnost da 5X pritisnuti *Shift* na *Windowsima* pokrene *command prompt*, umjesto "Sticky Keys" funkcije. Na *Ubuntu live* distribuciji to možemo napraviti preko *GUI Rename..* ali i pomoću komandne linije. Prijavljeni kao admin iskoristimo naredbu *cp* da napravimo "zamjene uloga".

```
root@xubuntu:/media/xubuntu/7A0CFE2D0CFDE453/Windows/System32#
root@xubuntu:/media/xubuntu/7A0CFE2D0CFDE453/Windows/System32# cp cmd.exe cmdX.exe
root@xubuntu:/media/xubuntu/7A0CFE2D0CFDE453/Windows/System32# cp sethc.exe cmd.exe
root@xubuntu:/media/xubuntu/7A0CFE2D0CFDE453/Windows/System32# cp cmdX.exe sethc.exe
```

Napavimo *restart*, izbacimo *Ubuntu* medij i na prijavnom "prozoru" stisnimo *Shift* 5X. Pojavljuje se "na prozor" popularni *cmd*.



Za našeg fiktivnog administratora imena "user" koji je zaboravio lozinku zatražimo novu lozinku pomoću naredbe.

```
C:\Windows\system32>net user user *

Type a password for the user:
Retype the password to confirm:
The command complete successfully.
```

To je to. Uspjeli smo postojećem adminu postaviti novu lozinku i poništiti staru zaboravljenu.

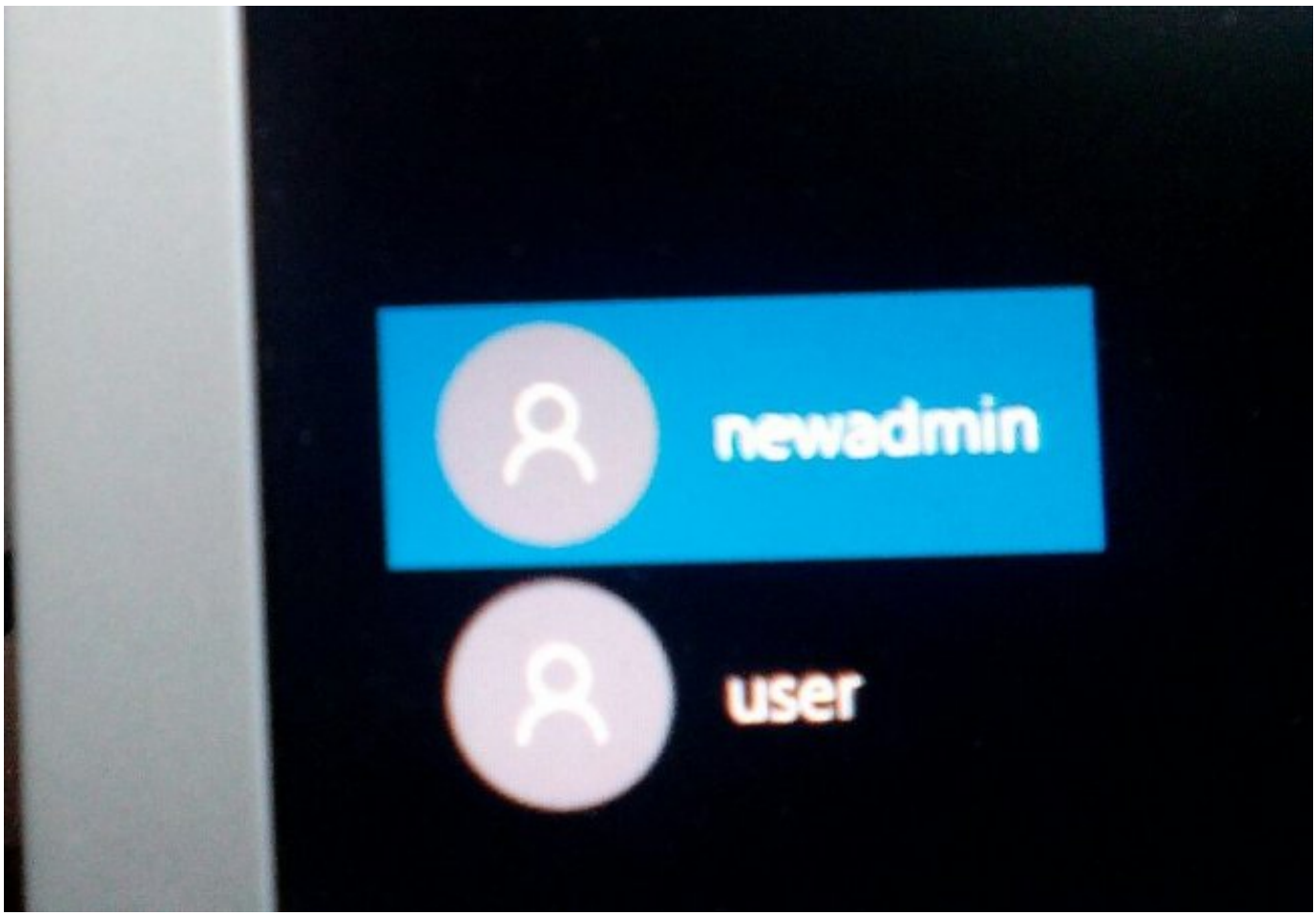
Također postoji mogućnost da otvorite "novog administratora" imena *newadmin* putem naredbe.

```
C:\Windows\system32>net user /add newadmin lozinka
The command completed successfully.
```

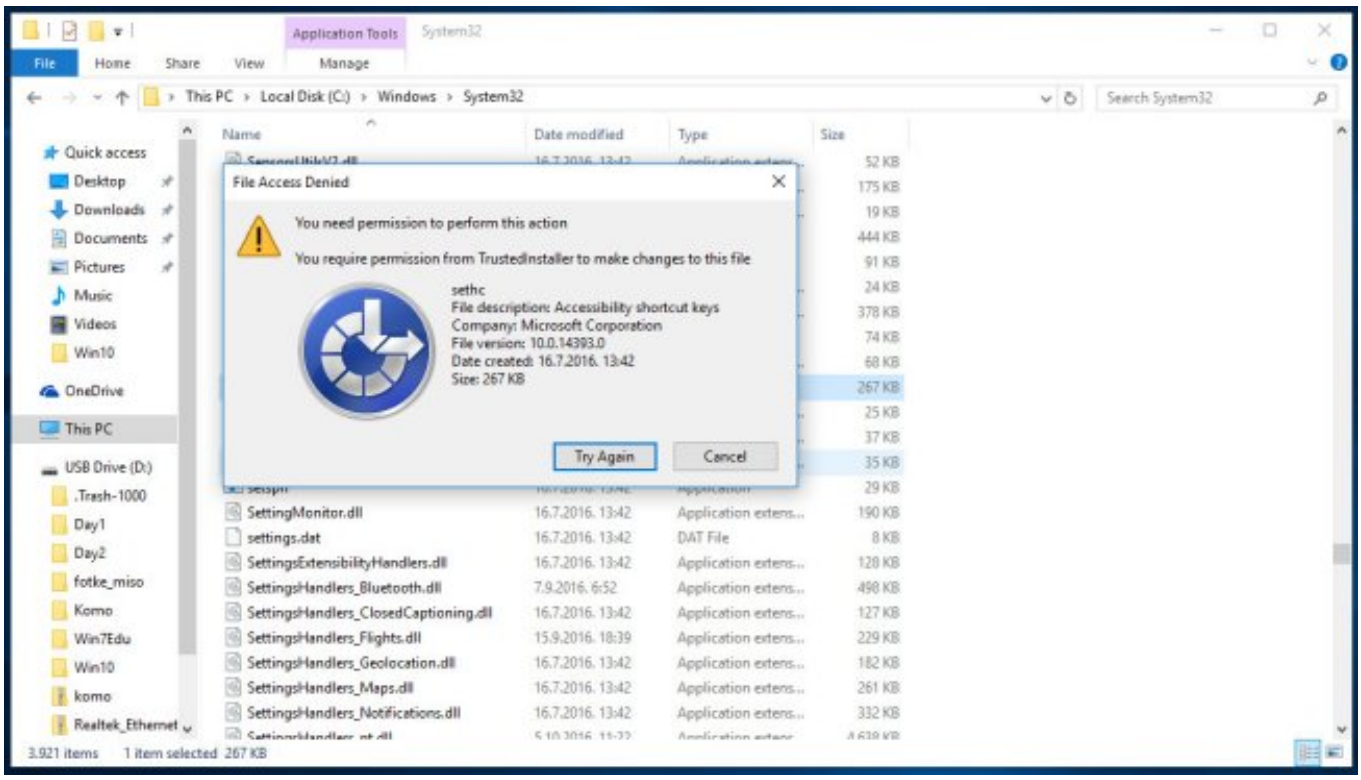
Dodamo ga u ulogu administratora.

```
C:\Windows\system32>net localgroup administrators newadmin /add
The command completed successfully.
```

Na prijavi sada postoje 2 administratorska korisnika.



Birajte kojeg želite :) Naravno ne zaboravite ponovo na sistemu vratiti stvari na svoje mjesto. Da vam sustav ne ostane sa zamjenjenim *sethc.exe* i *cmd.exe*. Pokušaj preimenovanja datoteka nakon prijave na *Windows 10* sustav ne uspijeva.



Po *defaultu* nemate dopuštenje za promjenu na sistemskim datotekama koji su u vlasništvu sistemskog korisnika zvanog "TrustedInstaller", iz sigurnosnih razloga. Dozvolu korisniku *newadmin* možemo dati kroz *Advanced Security Settings for Data*, koju naravno uklonite nakon preimenovanja *sethc.exe* i *cmd.exe* izričito na korisnika "TrustedInstaller". Mi nismo željeli narušavati *Windows 10* sistem dozvola i odlučili smo se za *Linux Way*.

Ponovno smo pokrenuli *Ubuntu live session*. Pokrenuli naredbe.

```
root@xubuntu:/media/xubuntu/7A0CFE2D0CFDE453/Windows/System32# cp cmd.exe sethc.exe
root@xubuntu:/media/xubuntu/7A0CFE2D0CFDE453/Windows/System32# cp cmdX.exe cmd.exe
```

I ponovo pokrenuli *Windows 10*. Sada vam cmd.exe opet normalno funkcionira kao i prije. "Sticky Keys" ponovo "hvata" 5x *Shift*.

pon, 2016-11-28 13:47 - Goran Šljivić**Kuharice:** Windows [1]
Kategorije: Operacijski sustavi [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1700

Links
[1] https://sysportal.carnet.hr/taxonomy/term/18
[2] https://sysportal.carnet.hr/taxonomy/term/26