PATRON-IT

https://martinhaller.cz

Barcamp HK 2018

Nebezpečí přichází skrze USB

MARTIN HALLER

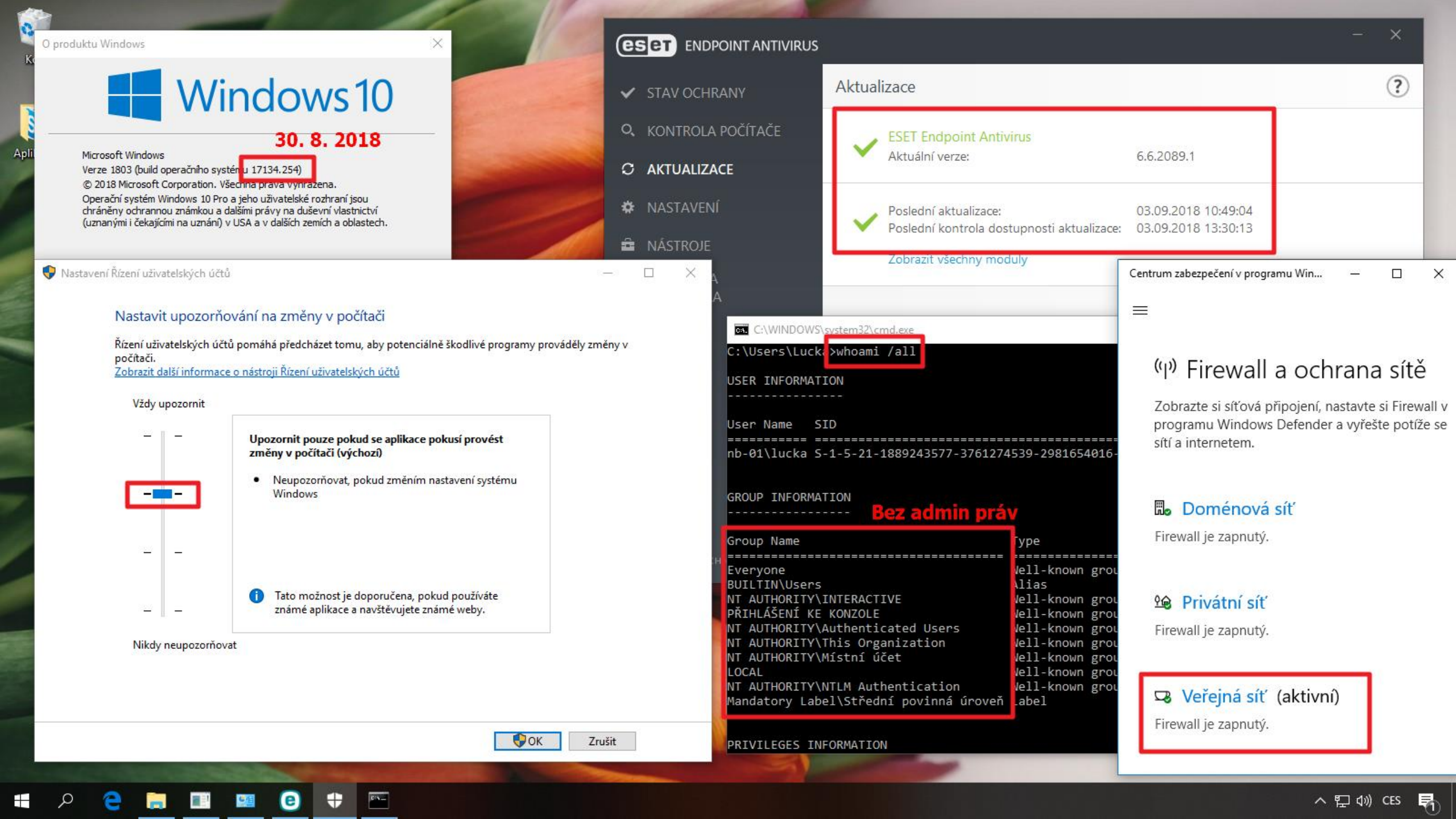
MCSE, CCNP, ECSA


14:46
úterý 4. září
EliteBook 8460p
intel
CORE i5
Windows 7

Bash Bunny

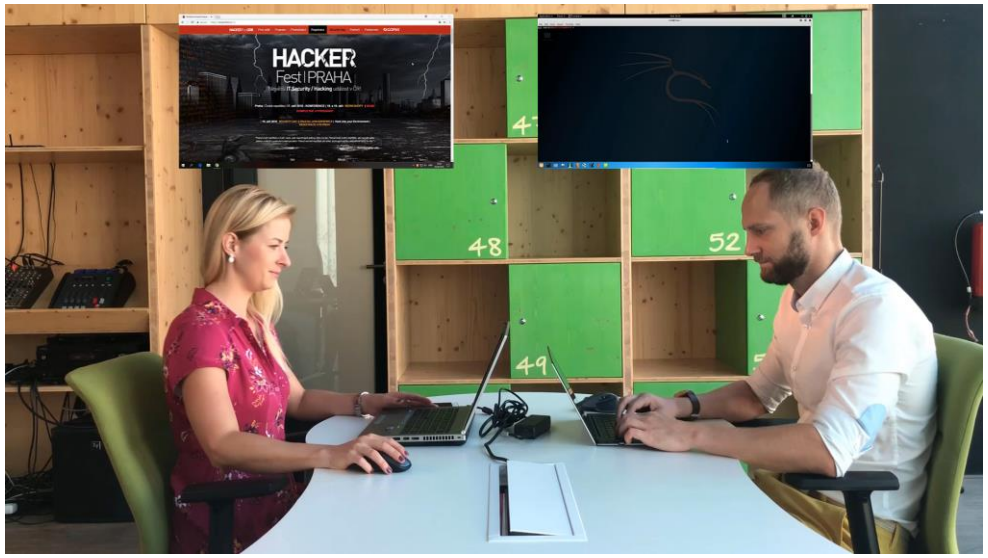
„PC on stick“

- Quad-core ARM Cortex A7, 512 MB DDR3, 8 GB storage
- RGB dioda
- Přepínač „payloadů“
- Režimy: síť, klávesnice, storage
- Komunita (cca 89 payloadů)
- Cena cca 4500 Kč

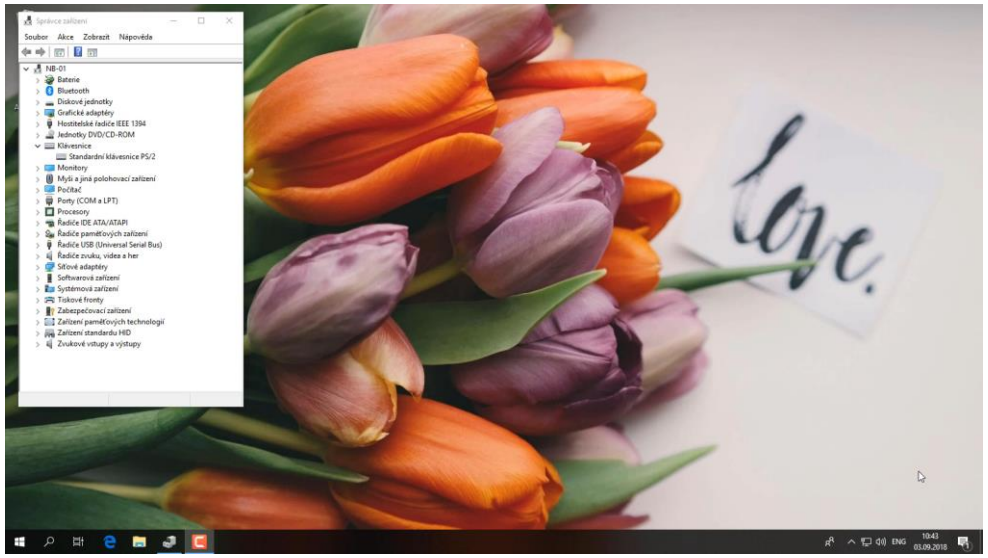

O produktu Windows
Windows 10
30. 8. 2018
Microsoft Windows
Verze 1803 (build operačního systému 17134.254)
© 2018 Microsoft Corporation. Všechna práva vyhrazena.
Operační systém Windows 10 Pro a jeho uživatelské rozhraní jsou chráněny ochrannou známkou a dalšími právy na duševní vlastnictví (uznanými i čekajícími na uznání) v USA a v dalších zemích a oblastech.
ESET ENDPOINT ANTIVIRUS
STAV OCHRANY
KONTROLA POČÍTAČE
AKTUALIZACE
NASTAVENÍ
NÁSTROJE
Aktualizace
ESET Endpoint Antivirus
Aktuální verze: 6.6.2089.1
Poslední aktualizace: 03.09.2018 10:49:04
Poslední kontrola dostupnosti aktualizace: 03.09.2018 13:30:13
Zobrazit všechny moduly
Nastavení Řízení uživatelských účtů
Nastavit upozorňování na změny v počítači
Řízení uživatelských účtů pomáhá předcházet tomu, aby potenciálně škodlivé programy prováděly změny v počítači.
Zobrazit další informace o nástroji Řízení uživatelských účtů
Vždy upozornit
Upozornit pouze pokud se aplikace pokusí provést změny v počítači (výchozí)
Neupozorňovat, pokud změním nastavení systému Windows
Tato možnost je doporučena, pokud používáte známé aplikace a navštěvujete známé weby.
Nikdy neupozorňovat
OK
Zrušit
C:\WINDOWS\system32\cmd.exe
C:\Users\Lucka>whoami /all
USER INFORMATION
User Name SID
nb-01\lucka S-1-5-21-1889243577-3761274539-2981654016-
GROUP INFORMATION
Bez admin práv
Group Name
Everyone
BUILTIN\Users
NT AUTHORITY\INTERACTIVE
PŘIHLÁŠENÍ KE KONZOLE
NT AUTHORITY\Authenticated Users
NT AUTHORITY\This Organization
NT AUTHORITY\Místní účet
LOCAL
NT AUTHORITY\NTLM Authentication
Mandatory Label\Střední povinná úroveň
PRIVILEGES INFORMATION
Centrum zabezpečení v programu Win...
Firewall a ochrana sítě
Zobrazte si síťová připojení, nastavte si Firewall v programu Windows Defender a vyřešte potíže se sítí a internetem.
Doménová síť
Firewall je zapnutý.
Privátní síť
Firewall je zapnutý.
Veřejná síť (aktivní)
Firewall je zapnutý.
CES

Ukázka č. 1 – počítač bez dozoru

Prezentace



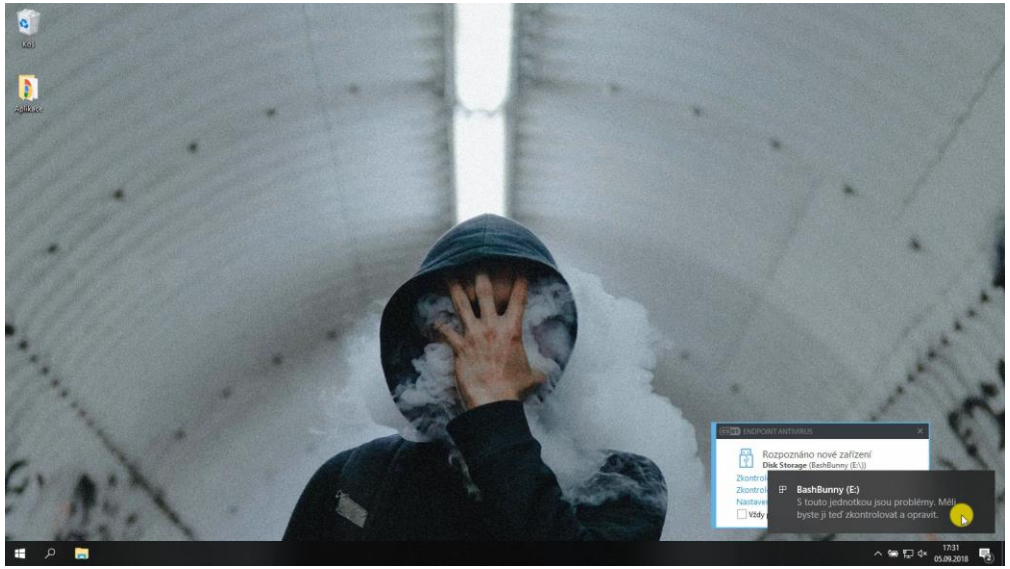
Co se stalo



Ukázka č. 2 – prosba o pomoc

Prezentace

Co jsme získali



Děkuji za pozornost

https://martinhaller.cz

PATRON-IT

Alternativní zařízení

USB Armory – 3.500 Kč

USB Rubber ducky – 2.300 Kč

Raspberry Pi Zero W – 500 Kč

Digispark – 30 Kč