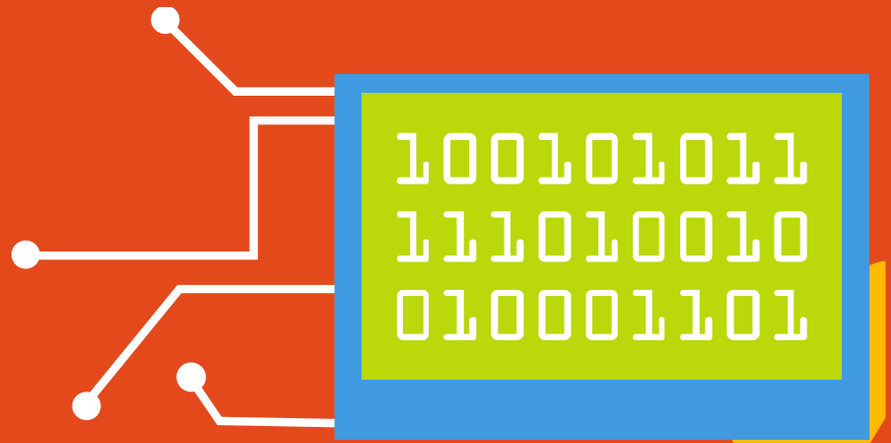
KONFERENCA

Microsoft

# Cybersecurity v letu 2017

Halis Tabaković, FMC




TEHNOLOGIJA

# Predavatelj: Halis Tabaković, FMC d.o.o.

- 10 let izkušenj v IT
- MCT, MCSE,…
- Security
- PowerShell
- Domain Services
- Hyper-V
- Office 365 & Azure
- …

# Agenda

1. Uvod
2. Primeri napadov (PtH)
3. DEMO: Primer napada
4. Novosti in izboljšave v zadnjih OS
5. DEMO: LAPS
6. DEMO: Credential Guard
7. Sysinternals Utilities
8. Najpogostejše napake administratorjev
9. Najboljše prakse in zaključek
10. Vprašanja in odgovori

# Uvod

## Trenutno stanje:

- Napadi na organizacije so v velikem porastu
  (večji porast pri internih napadih)
- 201 dan – povprečje dni, da se odkrije napad/vdor v organizacijo
- 70 dni  - povprečje dni, da se odpravijo posledice napada
- 60% majhnih podjetij (do 100 zaposlenih) preneha s poslovanjem v manj kot pol leta po napadu
- WannaCry (WanaCrypt0r 2.0) ransomware

Viri: http://www.milpond.com/60-small-businesses-close-within-six-months-cyber-attack/
http://www.eweek.com/security/breaches-from-malicious-or-criminal-attacks-more-costly-than-average
https://www.ekransystem.com/en/blog/cyber-security-statistics-2016

# Primeri napadov (AD)

- Pass the Hash (PtH)

- Kerberoast (Offline cracking)

- Forged Kerberos Ticket (Silver & Golden Ticket)

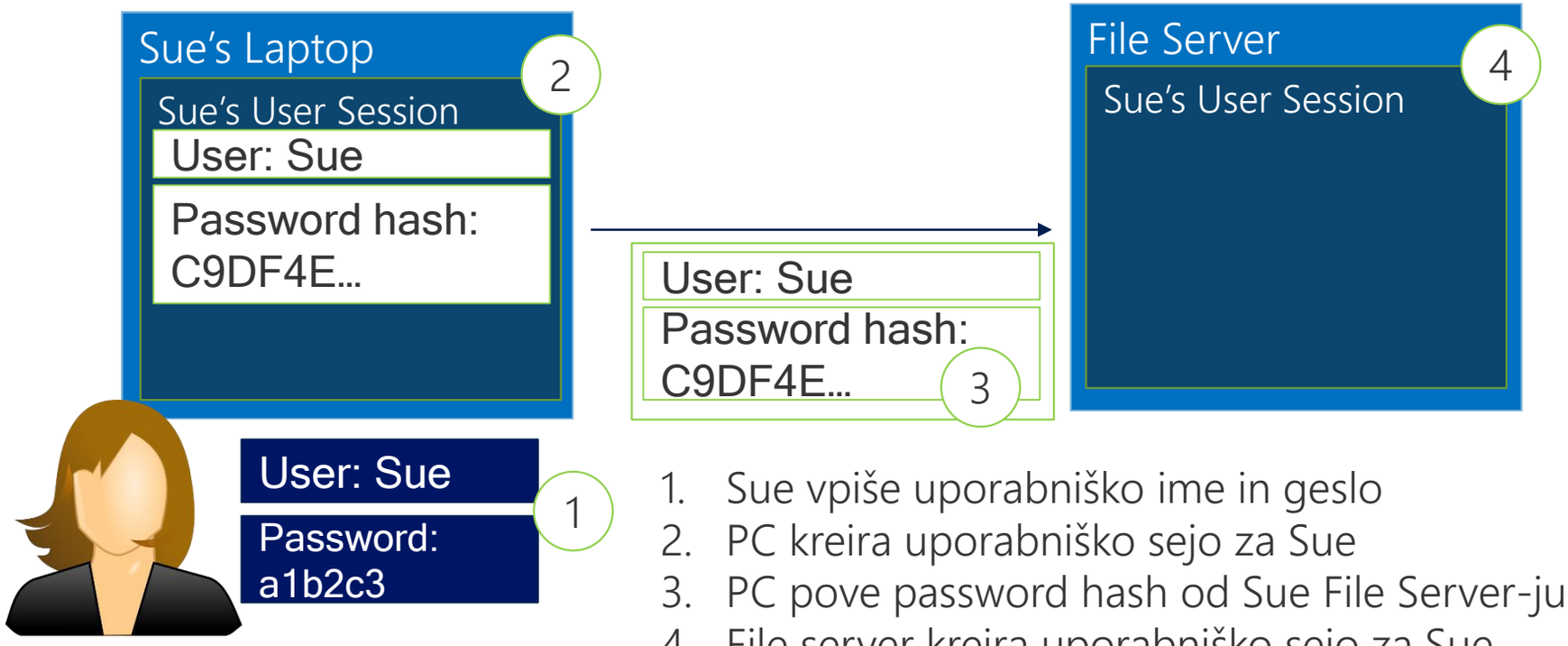
https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

- Izkoriščanja ranljivosti zaradi neposodobljenih DC in/ali delovnih postaj (npr. MS14-068, MS16-032,…)

# Pass the Hash (PtH)

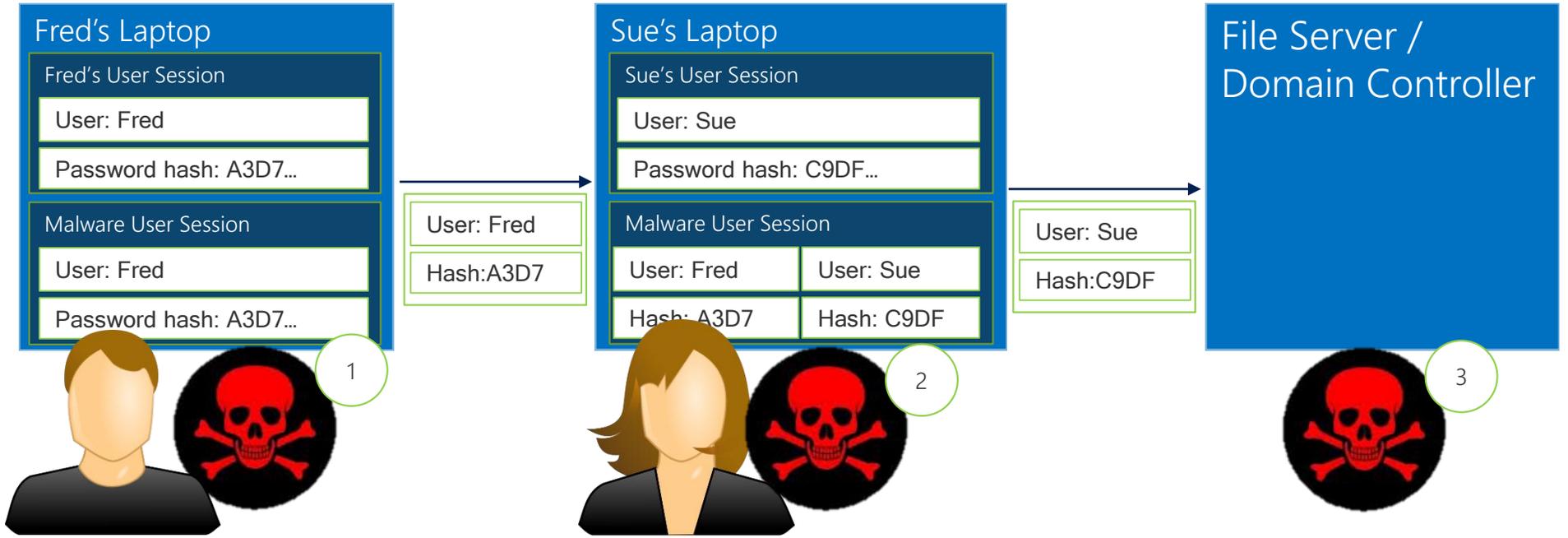
- Najbolj pogost napad
- Obstaja tam, kjer je možen single-sign on (SSO)
- V kolikor želimo SSO, smo izpostavljeni napadu PtH
- Če imamo SSO, ne moremo popolnoma preprečiti PtH napad – lahko ga samo otežimo…

# Single-Sign On




1. Sue vpiše uporabniško ime in geslo
2. PC kreira uporabniško sejo za Sue
3. PC pove password hash od Sue File Server-ju
4. File server kreira uporabniško sejo za Sue

# Pass-the-Hash




1. Fred zažene malware
2. Malware okuži računalnik od Sue in Freda
3. Malware okuži File Server ali DC

# Demo: Primer napada

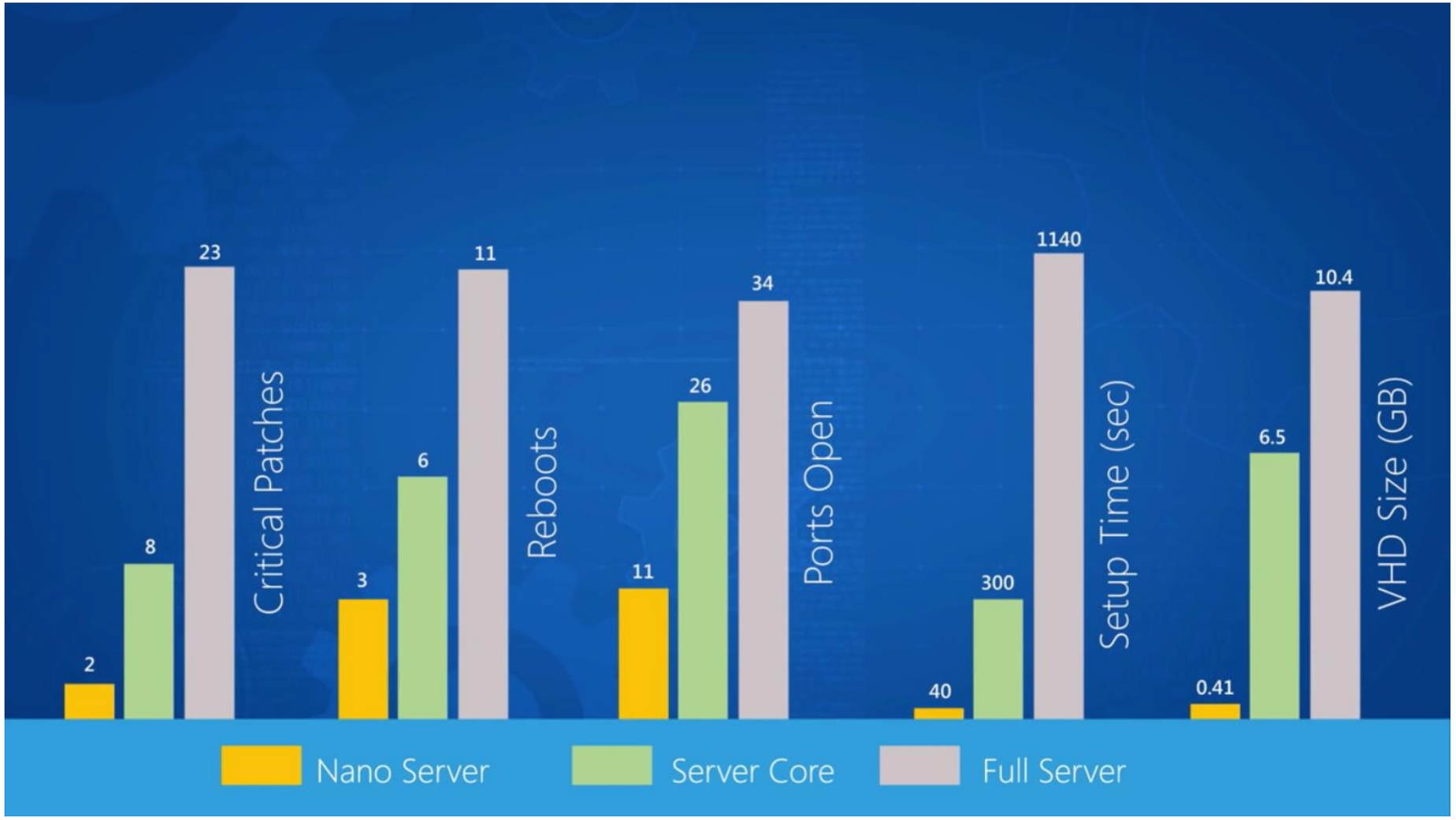
Microsoft

KONFERENCA

# Novosti in izboljšave

- Nano Server (rabimo Software Assurance)
- Containers
- Secure Boot, Trusted Boot, ELAM
- Guarded fabric and shielded VMs
- JEA / JIT Administration
- ATA (Advanced Threat Analytics)
- OMS (Microsoft Operations Management Suite)
- Device Guard
- Credential Guard
- LAPS
- …

# Nano Server


Critical Patches
2
8
23
Reboots
3
6
11
Ports Open
11
26
34
Setup Time (sec)
40
300
1140
VHD Size (GB)
0.41
6.5
10.4
Nano Server
Server Core
Full Server

# LAPS

Local Administrator Password Solution:

- Centraliziran management
- Gesla se periodično spreminjajo
- Gesla so kompleksna (sami lahko določamo nivo)
- Support preko Microsoft Premier Support Services

https://technet.microsoft.com/en-us/mt227395.aspx

# Demo: LAPS

Microsoft

KONFERENCA

# Credential Guard

- Ena izmed najpomembnejših varnostnih novosti v Windows 10
- Omogoča shranjevanje naših gesel v izoliranem, virtualnem containerju do katerega napadalci nimajo dostopa (napadalec ne vidi hash gesla)
- LSA process je povsem izoliran od operacijskega sistema
- https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage

# Demo: Credential Guard

Microsoft

KONFERENCA

# Sysinternals Suite

Top 5 orodij za security:

- Sysmon
- AccessChk
- Autoruns
- LogonSessions
- Process Explorer & Process Monitor

# Najpogostejše napake administratorjev

- Prijava na delovno postajo kot domenski administrator
- Preveč domenskih administratorjev
- Preveč pravic servisnih računov
- Domenski kontrolerji imajo nameščene tudi druge vloge
- Domenski kontrolerji (in delovne postaje) niso posodobljeni
- Domenski kontrolerji ne uporabljajo zadnjih OS
- Lokalni administratorji imajo ista gesla
- Uporabljamo nekompleksna gesla, ki ne potečejo
- Ne brišemo starih računov (user/computer)

# Najboljše prakse

- Dokumentirano okolje
- Zagotavljamo revizijske sledi – Auditing
- JEA/JIT Administration
- Redno posodabljanje sistemov
- Če je le možno, uporabljamo zadnje verzije OS
- Ne nameščamo drugih vlog na DC
- Čim manjše število uporabnikov v priviligiranih skupinah
- Urejene skupinske politike (brez gesel, jasno dokumentirane)

# Kontakt:


Moj blog: http://halis.eu

FMC stran: http://fmc.si/

Moj email: halis@halis.eu
halis.tabakovic@fmc.si

# Q & A