

(Ne)poznati napadi i zaštita

Robert Petrunić
Algebra

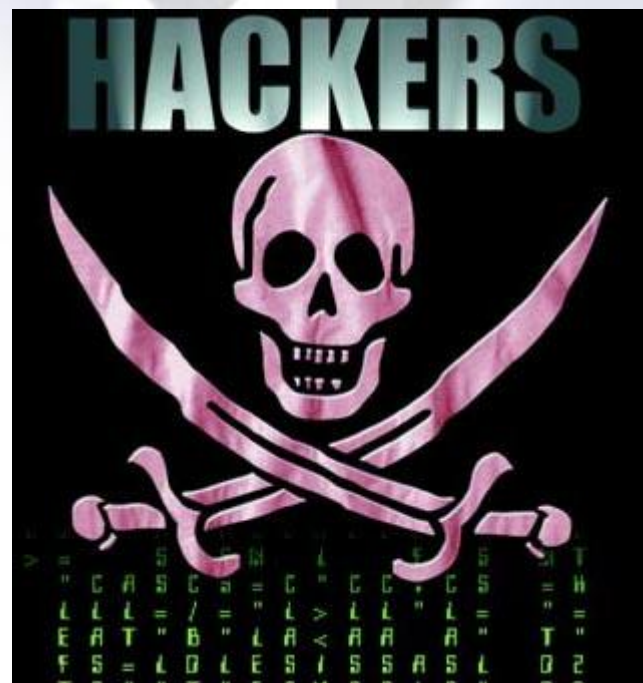
Sadržaj

- RDP MitM napad (DEMO)
- Defense in depth (sveobuhvatna zaštita)
- Tehnologije Windows Servera 2008 koje podižu sigurnost na mreži
- Trojanski konj (DEMO)

IZVOLITE MOJU LOZINKU

ZADATAK – ADMIN PASS

- Pokrenuti ARP poisoning
 - Izvesti RDP MitM napad
 - Pronaći admin password
- ### TREBAMO LI IĆI DALJE?
- Upasti na sistem



DEMO/HACKER

NE DAM SVOJU LOZINKU

ZADATAK – ONEMOGUĆITI RDP MitM NAPAD

- Server 2003 + SP1
uključiti RDP preko SSL-a
- Server 2008
- TREBAMO LI IĆI DALJE?
- IPSec na žici



DEMO / ADMIN



Defense in Depth (Sveobuhvatna zaštita)

Defense in depth

Upravljanje zakrpama

Windows update
Microsoft update
WSUS 3
SMS (System center)

SIGURNOST RAČUNALA

Defense in depth

Upravljanje zakrpama

Zaštita od virusa

SIGURNOST RAČUNALA

Anti Virus
Anti Spyware
Anti RootKit
Anti Spam
ANTI MALWARE

Defense in depth

Upravljanje zakrpama

Zaštita od virusa

Vatrozid

SIGURNOST RAČUNALA

Na granici mreže
Na svakom serveru
Na svakom računalu

Defense in depth

Upravljanje zakrpama

Zaštita od virusa

Vatrozid

IDS, IPS, Honeynet

SIGURNOST RAČUNALA



Detekcija
Prevenција
Zamka

Defense in depth

Upravljanje zakrpama

Zaštita od virusa

Vatrozid

IDS, IPS, Honeynet

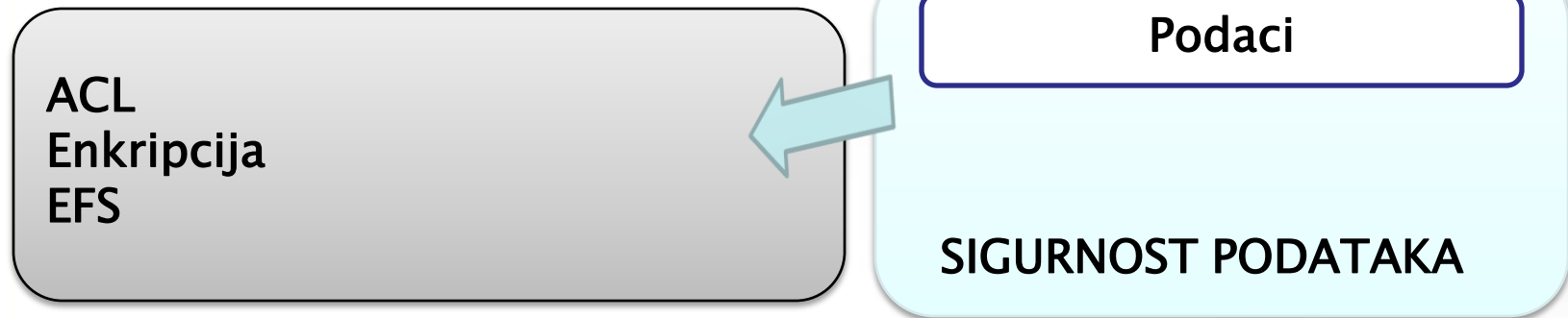
Hardening servera

SIGURNOST RAČUNALA

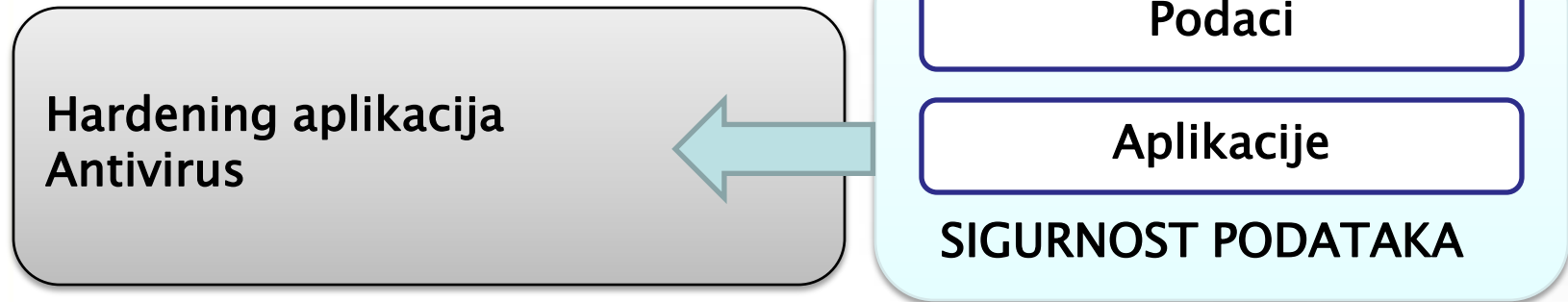
Registry

...

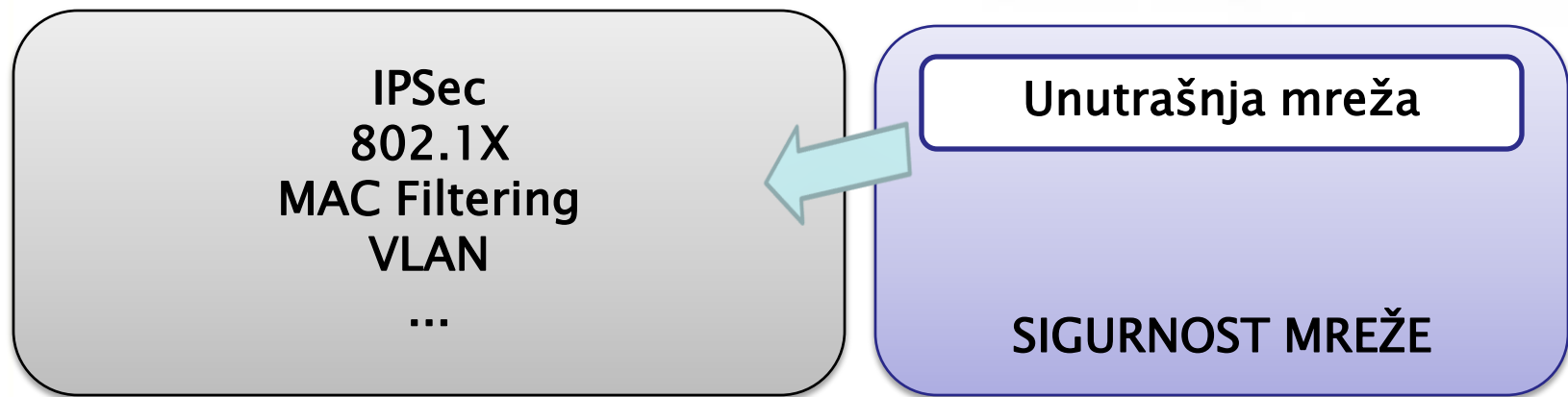
Defense in depth



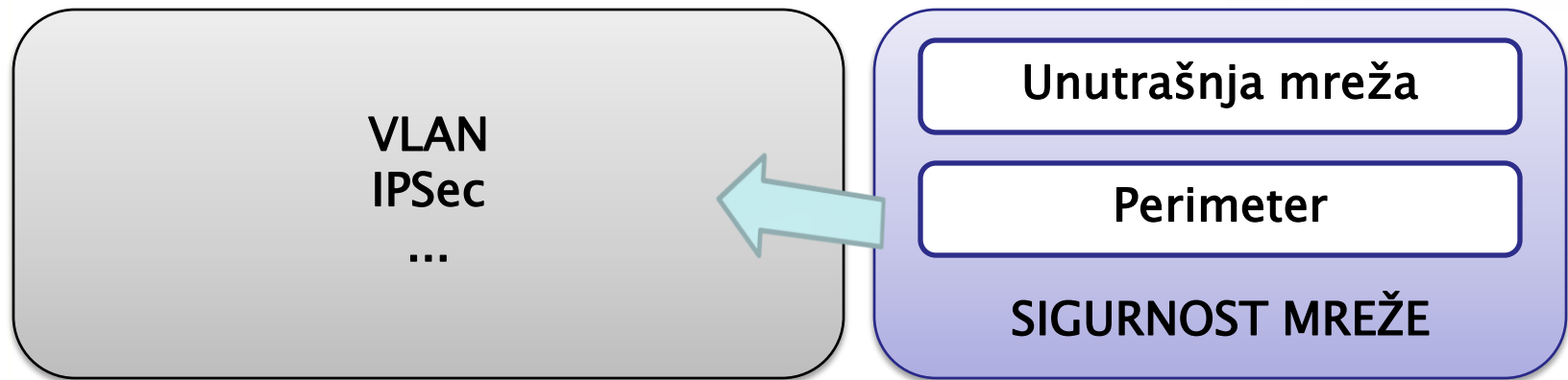
Defense in depth



Defense in depth



Defense in depth



Defense in depth

Upravljanje zakrpama

Zaštita od virusa

Vatrozid

IDS, IPS, Honeynet

Hardening servera

SIGURNOST RAČUNALA

Podaci

Aplikacije

SIGURNOST PODATAKA

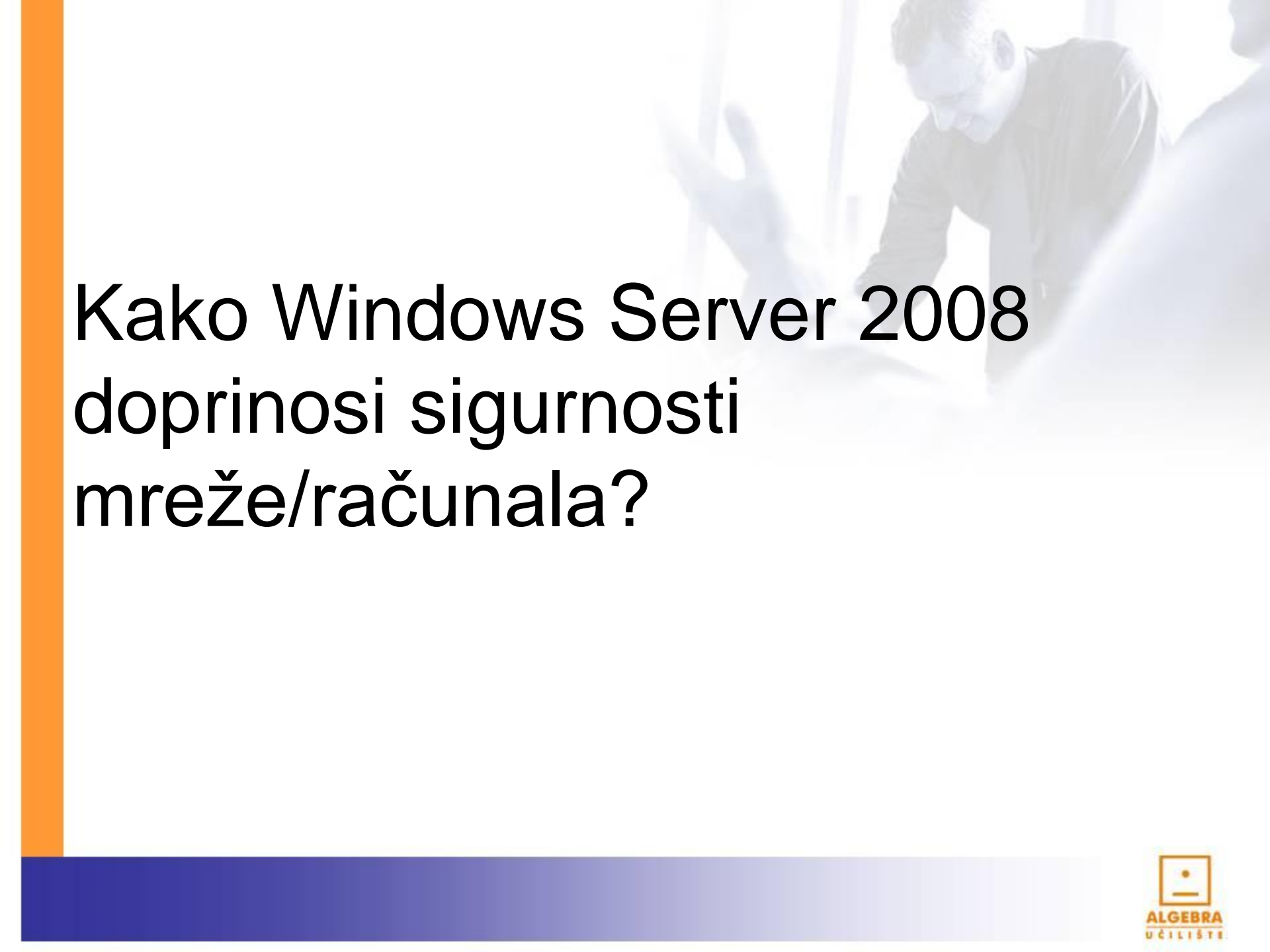
Unutrašnja mreža

Perimeter

SIGURNOST MREŽE

FIZIČKA SIGURNOST

POLICY, PROCEDURE i OSVJEŠĆENOST KORISNIKA !!!



Kako Windows Server 2008 doprinosi sigurnosti mreže/računala?

Windows Server 2008

- Terminalni servisi
 - Udaljene aplikacije
 - TS Gateway
 - TS Web pristup
 - RDC 6.0 (6.1)
- **Network Access Protection**
- TCP/IP promjene
- **Internet Information Services 7**

Windows Server 2008 (2)

- **Read Only Domain Controller**
- BitLocker drive enkripcija
- Core verzija Windows Servera 2008
- **Address Space Layout Randomization**
- **Windows Service Hardening**
- Local system account – manje servisa
- **Cryptography Next Generation**

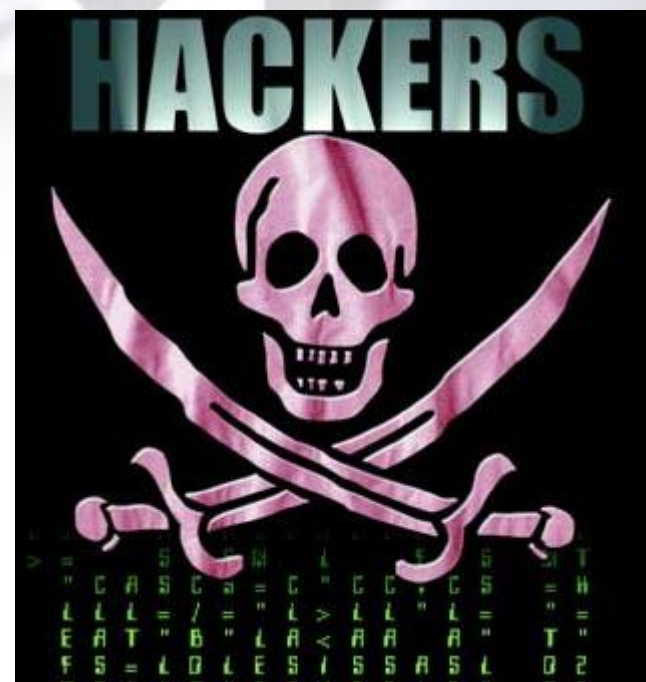
MOLIM TE POKRENI ME

ZADATAK – PRISTUP RAČUNALU

- Kreirati trojanskog konja
- Navesti žrtvu da ga pokrene
- Spojiti se na žrtvino računalo

TREBAMO LI IĆI DALJE?

- Potpuna kontrola žrtve ...

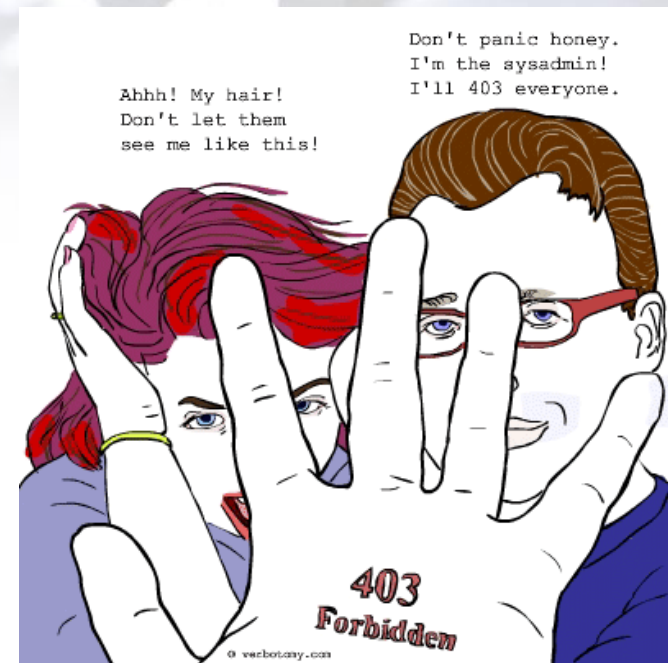


DEMO/HACKER

NE trojanskim konjima

ZADATAK – ONEMOGUĆITI NAPAD TROJANSKIM KONJIMA

- Edukacija korisnika
- Osvješćenost
- Ne biti admin na računalu
- Izbjegavati softver iz nepouzdatih izvora



DEMO / ADMIN

Linkovi

- [CEH službene stranice](#)
- [Algebra](#)
- [Robert Petrunić – blog](#)
- [Tekst koji opisuje ranjivost TS-a](#)
- [Home of Server 2008](#)
- [Top 10 novih stvari u Serveru 2008](#)



robert.petrunic@algebra.hr



Hvala