Betörés megrendelésre,

avagy etikus hackerek munka közben

Bemutatkozás

Buherátor

Silent Signal

IT biztonsági szakértő

OSCP

buherator@silentsignal.hu

Pánczél Zoltán

Silent Signal

IT biztonsági szakértő

CISSP, OSCP, OSCE,
OSWP, GPEN

panczel.zoltan@silentsignal.hu

Feladat ismertetése

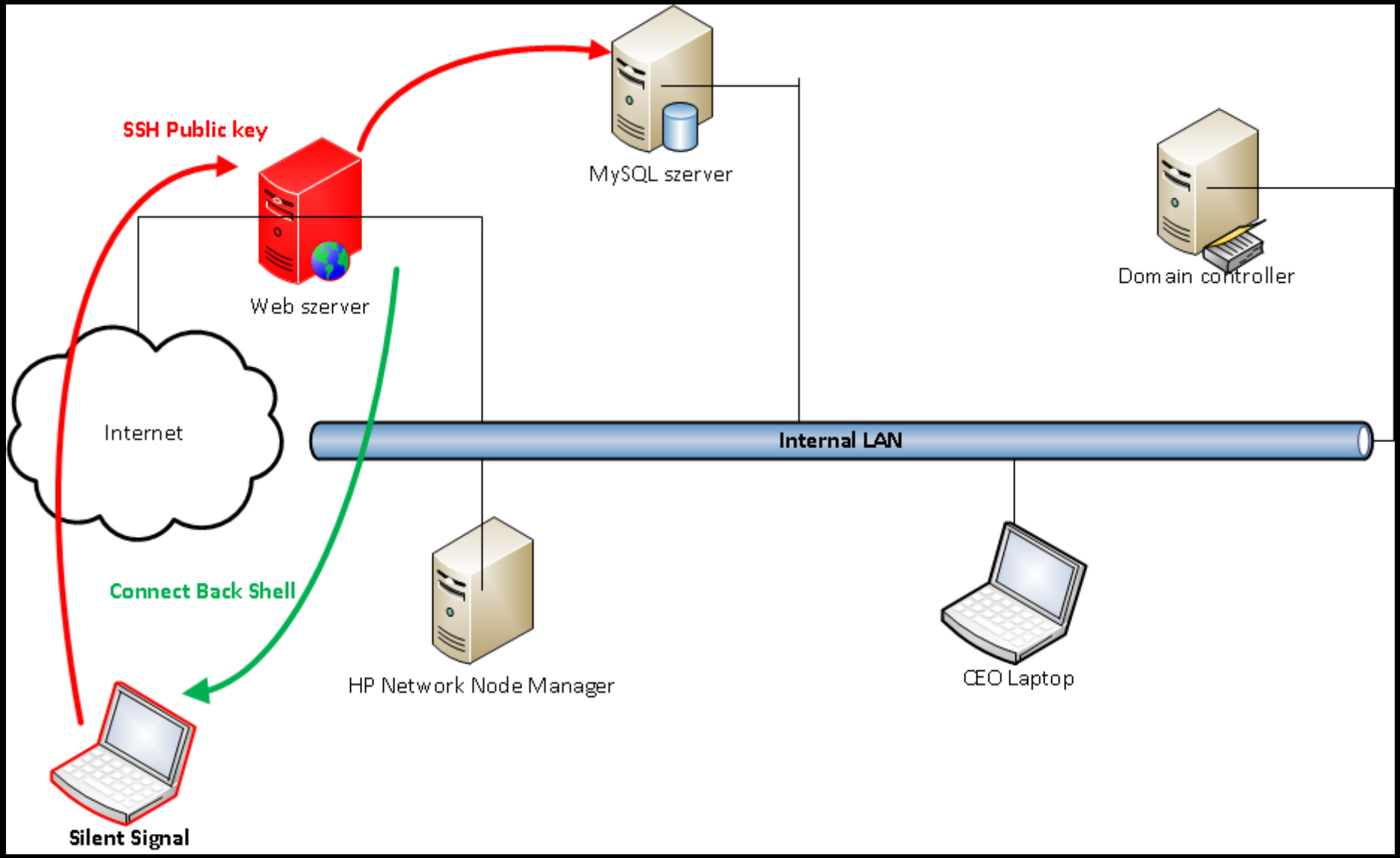
- Blackbox penetration testing
- Külső hálózat irányából
- Kliens oldali támadás NEM engedélyezett
- Hálózat támadása NEM engedélyezett
- Social Engineering NEM engedélyezett
- CEO laptopjáról egy fájl megszerzése a cél

Külső felderítés

- Linux webszerver azonosítása
- Fájl feltöltés probléma (nem triviális)
- Apache php fájl kezelési “feature” kihasználása
- Root jogosultság megszerzése
- Dual homed szerver

DEMO

Stage 2

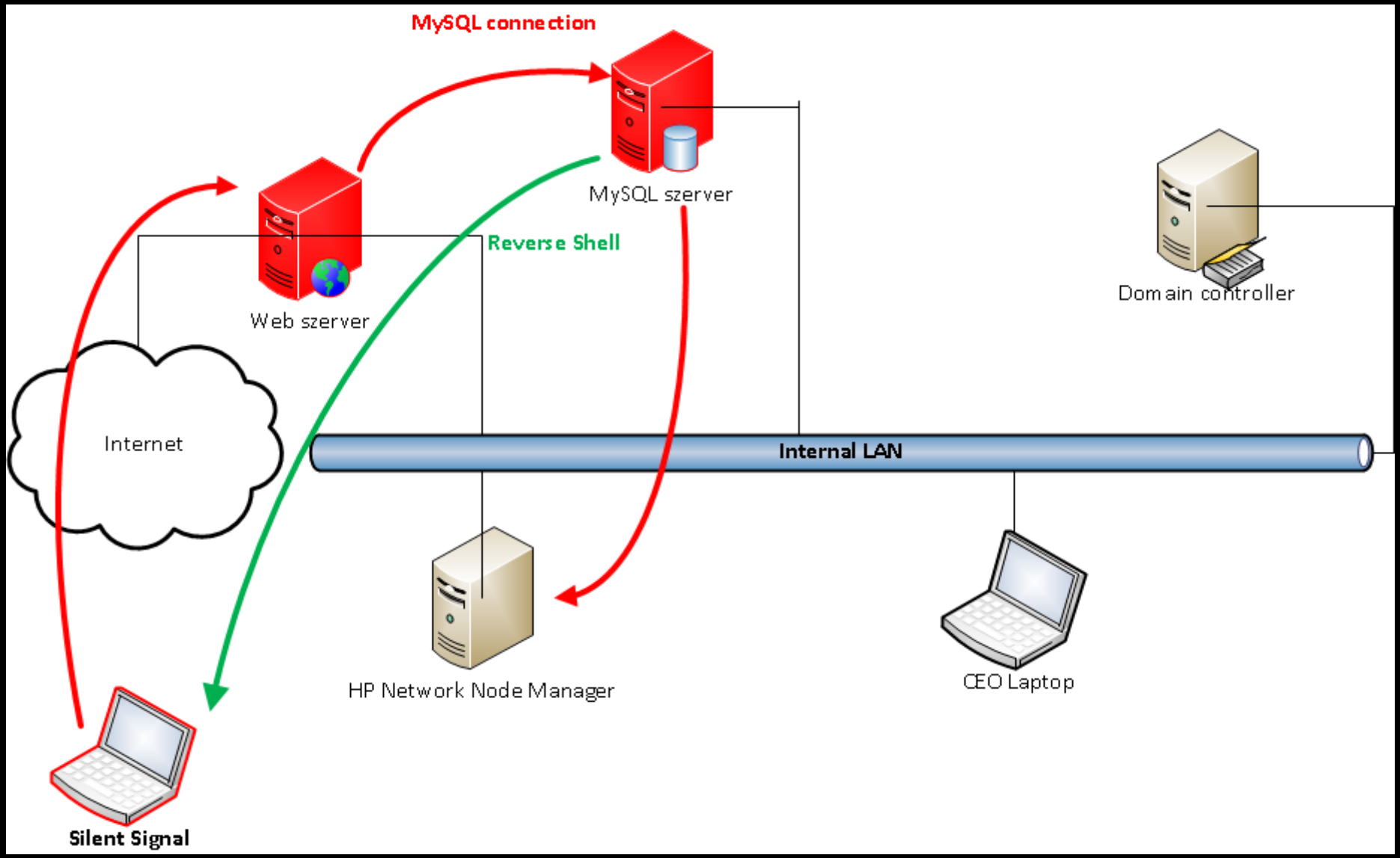

SSH Public key
MySQL szerver
Web szerver
Domain controller
Internet
Internal LAN
Connect Back Shell
HP Network Node Manager
CEO Laptop
Silent Signal

Belső hálózat felderítése 1.

- Windows 2003 szerver
- MySQL adatbázis kezelő
- MySQL UDF feature kihasználása
  - Egyéb lehetőség parancs végrehajtásra?
- SYSTEM jogosultság megszerzése

DEMO

Stage 3

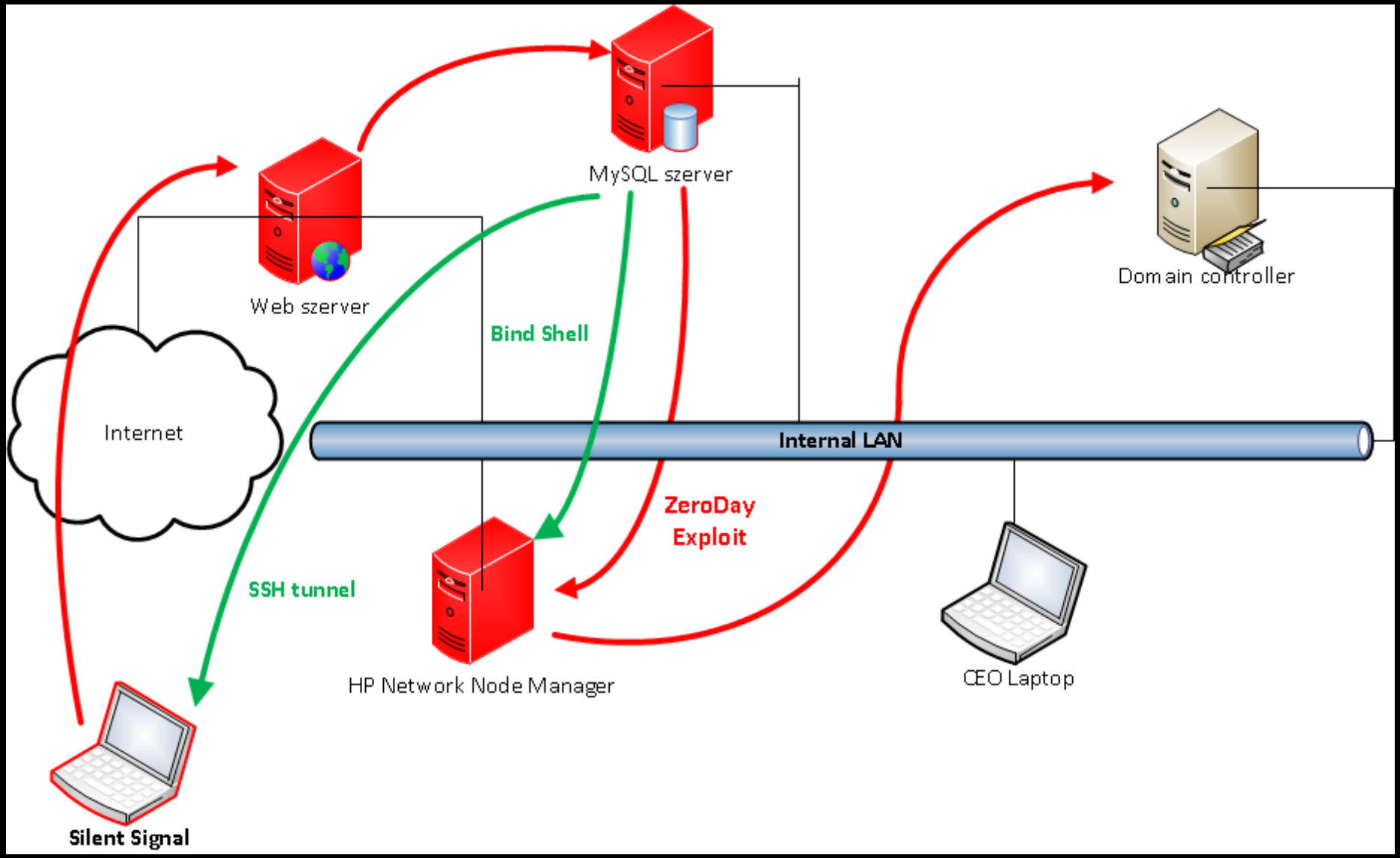

MySQL connection
MySQL szerver
Reverse Shell
Web szerver
Domain controller
Internet
Internal LAN
HP Network Node Manager
CEO Laptop
Silent Signal

Belső hálózat felderítése 2.

- Windows 2003 R2 szerver
- HP NNM 7.53
- Up to date rendszer
- 0-day biztonsági hiba kihasználása
- SYSTEM jogosultság

DEMO

Stage 4

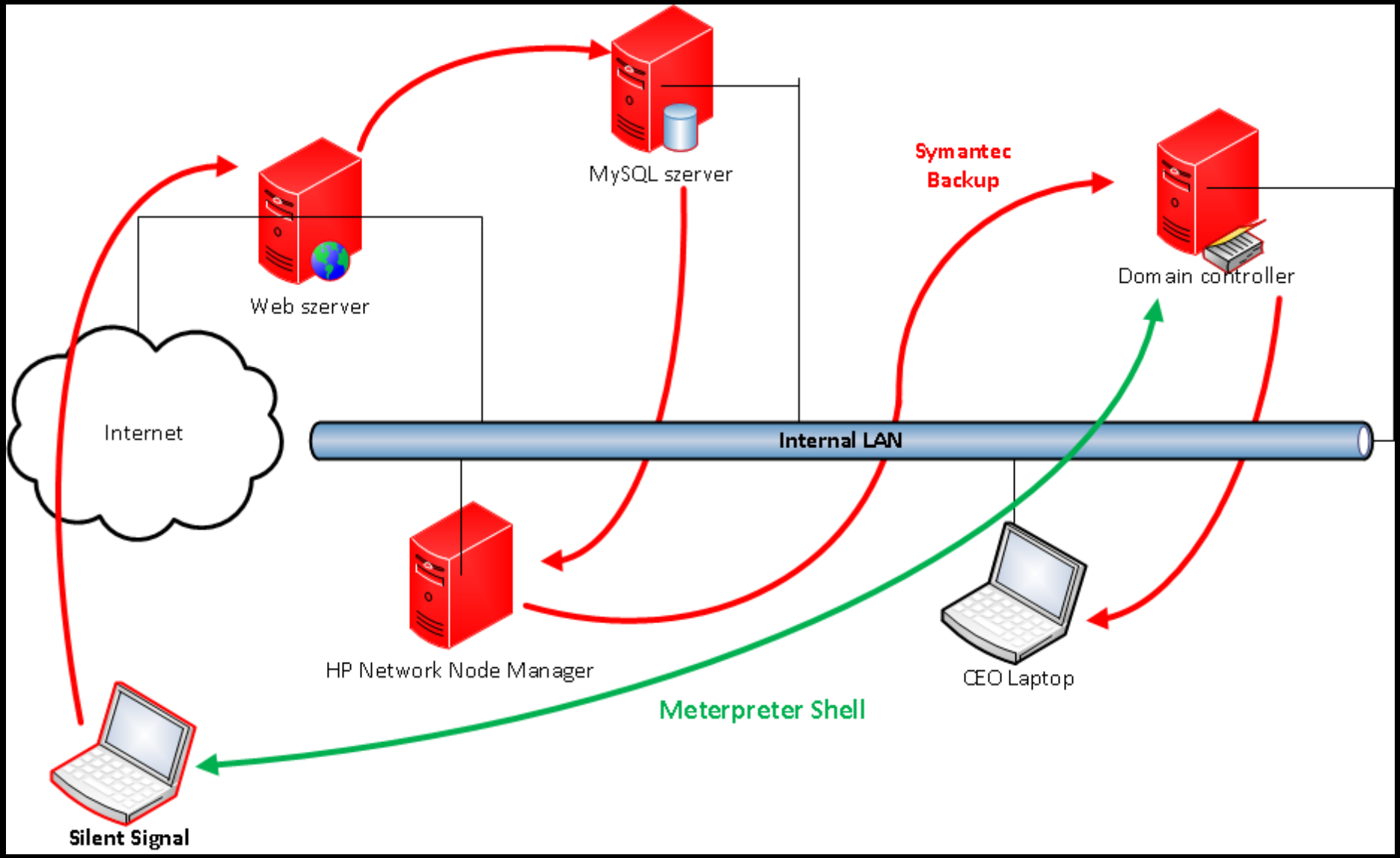

MySQL szerver
Web szerver
Domain controller
Bind Shell
Internet
Internal LAN
ZeroDay
Exploit
SSH tunnel
HP Network Node Manager
CEO Laptop
Silent Signal

DC hackelés

- Windows 2003 szerver
- Backupból system
- Symantec Backup Exec BoF
- Domain admin létrehozása
- CEO owned ☺

DEMO

Stage 5


MySQL szerver
Symantec
Backup
Web szerver
Domain controller
Internet
Internal LAN
HP Network Node Manager
CEO Laptop
Meterpreter Shell
Silent Signal

Javaslatok

- Feltöltő script konfigurációjának vizsgálata
- Dual homed környezet felülvizsgálata
- SQL
  - Korlátozott SQL felhasználó létrehozása
  - MySQL szerver csökkentett jogkörrel való futtatása
- WAF bevezetésének lehetősége
- Szoftver frissítések telepítése

ESET Smart Security kérdés

Melyik az a payload típus, amelyik lefutáskor kapcsolatot kezdeményez a támadó gépe felé?

A: Reverse shell

B: Bind shell

C: Root shell

D: Bourne-Again shell

Köszönjük a figyelmet!