STONESOFT

Network Security

Demo: Näin murtaudutaan webbikauppaan

Katri Riikonen, CISSP

Stonesoft lyhyesti

Secure Information Flow

Globaali yritys

- Globaali tietoturvayritys
- Perustettu 1990
- Listattu NASDAQ OMX
- Pääkonttori Helsingissä

Asiakaskeskeisyys

- Toimii Yhdysvalloissa, Euroopassa sekä Aasiassa
- Globaali 24/7 tuki
- Asiakkaita yli 90 maassa
- Keskitymme suuriin yrityksiin, jotka tarvitsevat korkeatasoista verkon tietoturvaa sekä katkeamattomia yhteyksiä

Innovaatio

- Integroidut verkon tietoturvan ja tietoliikenteen jatkuvuuden takaavat ratkaisut
- Tuotekehitys-yksiköt Suomessa ja Ranskassa
- Patentoidut tuotteet

STONESOFT
Network Security

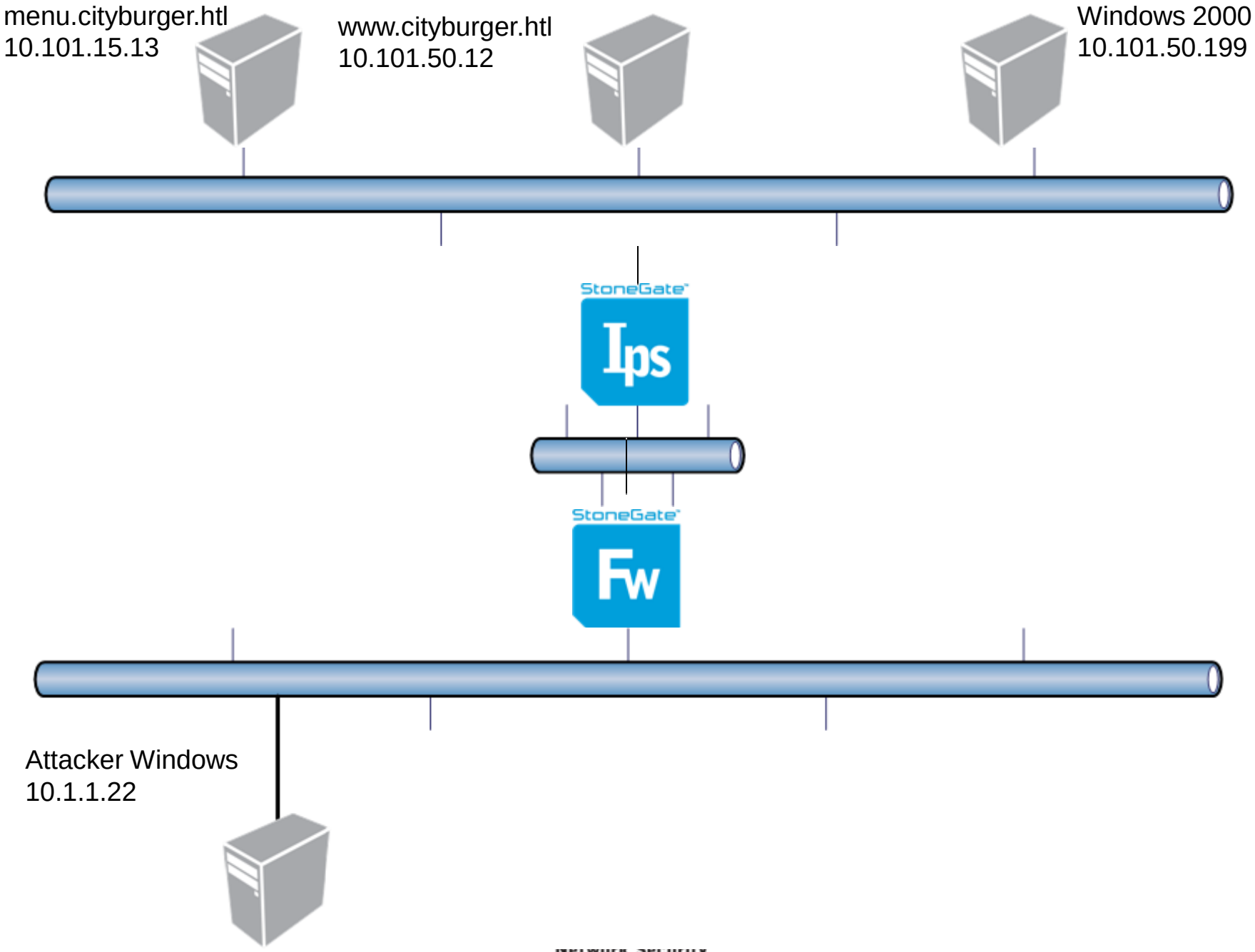
Hakkerin työskentelymenetelmät

- Kohteen identifiointi:
  - Domain-nimi, IP-osoite, tietokantapalvelin, etc.
- Tiedon kerääminen
  - Whois, DNS, Web-sivut, puhelinluettelot, etc.
  - Isäntäkone-/verkko-/porttiskannaus
  - Käyttöjärjestelmän määrittäminen
  - Palvelun identifiointi(Banner grabbing)

Exploiting Server Vulnerabilities

Tietojen kerääminen - nmap

STONESOFT
Network Security


menu.cityburger.htl
10.101.15.13
www.cityburger.htl
10.101.50.12
Windows 2000
10.101.50.199
StoneGate
Ips
StoneGate
Fw
Attacker Windows
10.1.1.22

Exploiting Server Vulnerabilities

Running the Exploit

STONESOFT
Network Security

Hacking Through the Web Site

Example target: www.cityburger.htl

STONESOFT
Network Security

How to Defend

What is seen in the network?

- Nmap and exploit 

- SQL Injection 

STONESOFT
Network Security

Evaasiotekniikat

- Stonesoft herätteli IPS-valmistajia vuoden 2010 aikana havahtumaan evaasioiden tuomaan ongelmaan
- Evaasiot nousivat kansainväliseen medianäkyvyyteen ja valmistajat riensivät parantamaan tuotteitaan
- Tutkimus jatkuu ja uusia löytöjä odotetaan runsaasti vuodelle 2011

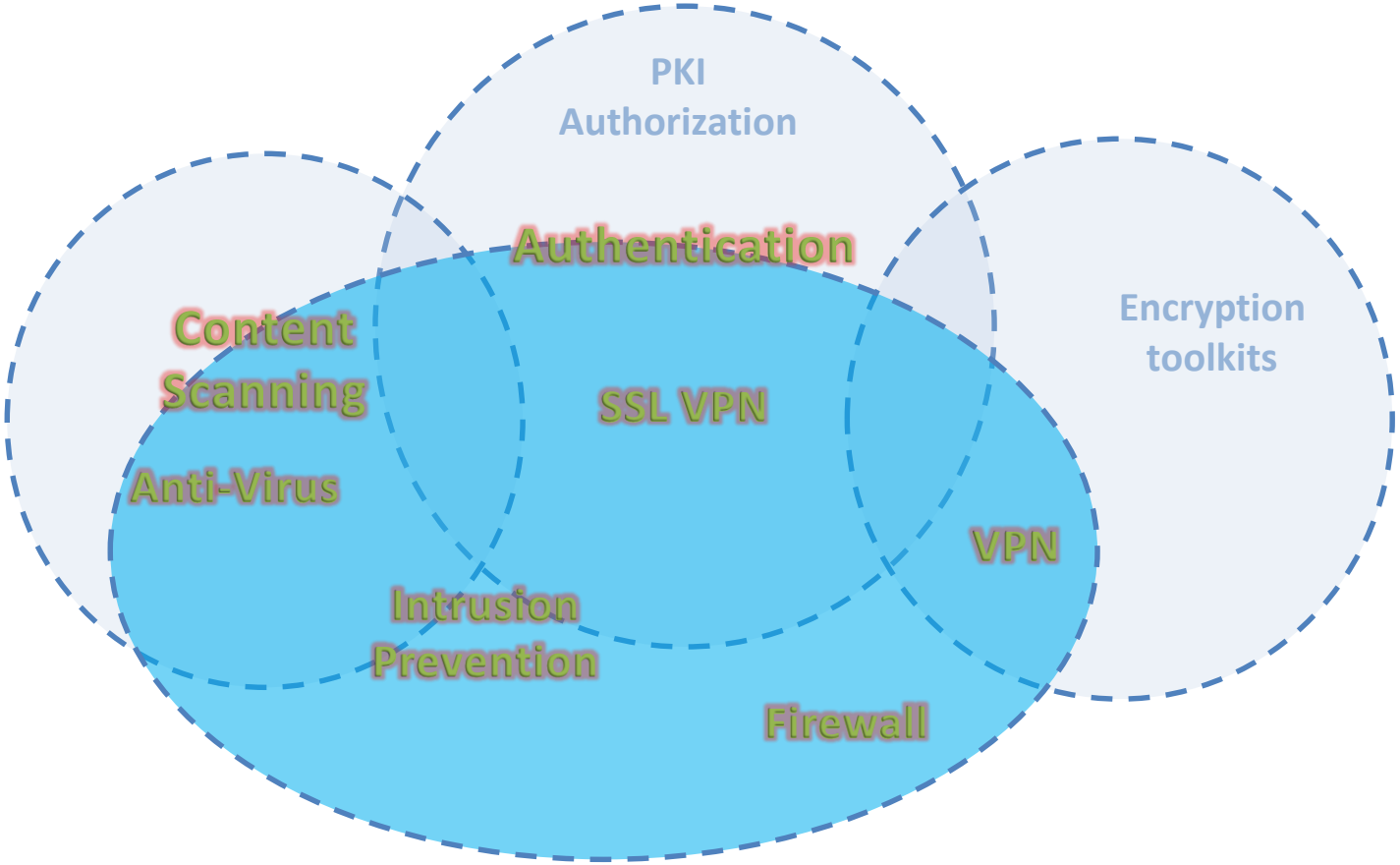
STONESOFT
Network Security

Tietoturva on Prosessi…

Kuvien lähde: http://www.gettyimages.fi/detail/98196428/Fuse

STONESOFT
Network Security

Toiminta-alue



STONESOFT
Network Security