Siťová bezpečnost a firewall

Oleksandr Petronyuk

ubuntu

Obsah

- Prvky ideálního firewallů
- Co firewall nevyřeší
- Základní služby a jejích slabiny
- Profily útoku
- Detekce průníku do sitě
- Typický postup pro vniknuti do sitě a protiopatření
- Jak ochránit středně malou firmu

ubuntu

Prvky ideálního firewallu

- Filtrování paketu
- Překlad síťových adres(NAT)
- Služby proxy

Co firewall nevyřeší

- Na světě existuje tolik různých způsobu napadení sítě, že úplně bezpečná není žádná metoda
- Dalším problémem je ochrana proti protokolům, které se se rozhodnete propouštět
- Skryté hraniční přechody
- Nepoučení zaměstnanci

Služby a jejích slabiny

- **Bežné internetové služby**
- -DNS(53 udp)
- -FTP(20 a 21 tcp)
- -HTTP(80 tcp)
- -IMAP(143 tcp)
- -NTP(123 udp)
- -POP(110 tcp)
- -SMTP(25 tcp)

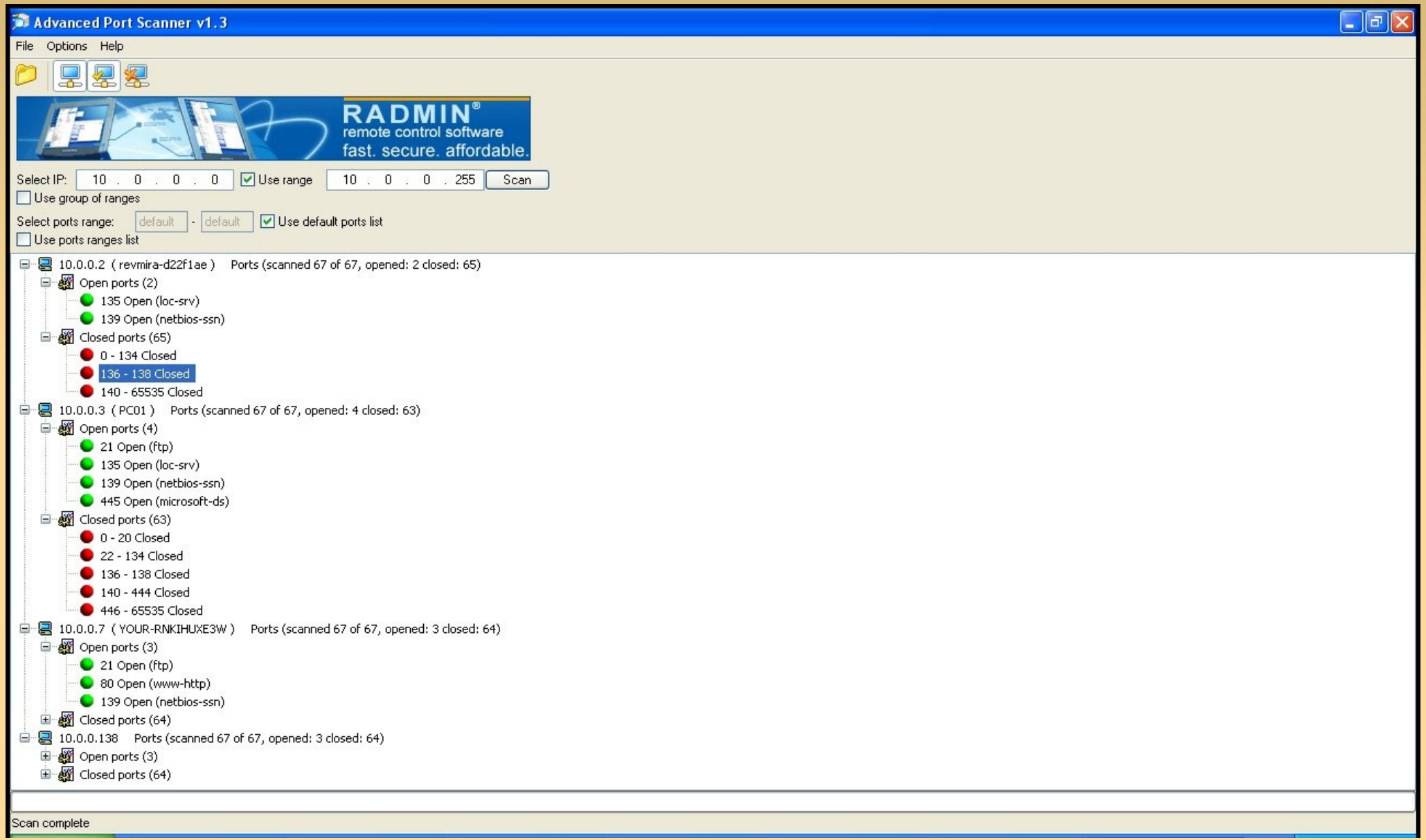
Profily utoku

- Ping of Death
- Teardrop
- UDP floods
- SYN floods
- Smurf
- Fraggle
- Chybně formatováné zprávy

Detekce vniknutí

- Skenování IP adres
- Skenování portů
- Průzkum služeb
- Výber cíle a průzkumy slabých mist
- Automatizované útoky na hesla
- Útoky na specifické služby

Detekce vniknuti



ubuntu

Možné řešení

- V praxi existuje malo spolehlivých systému detekce vniknuti
- Většinou se zavádějí firewally s funkcemi protokolování a varování.
- Většina nedokáže reagovat na útok automaticky
- **Možné řešení**
- Kvalitní loggy
- Dohledové systémy(Nagios) atd...

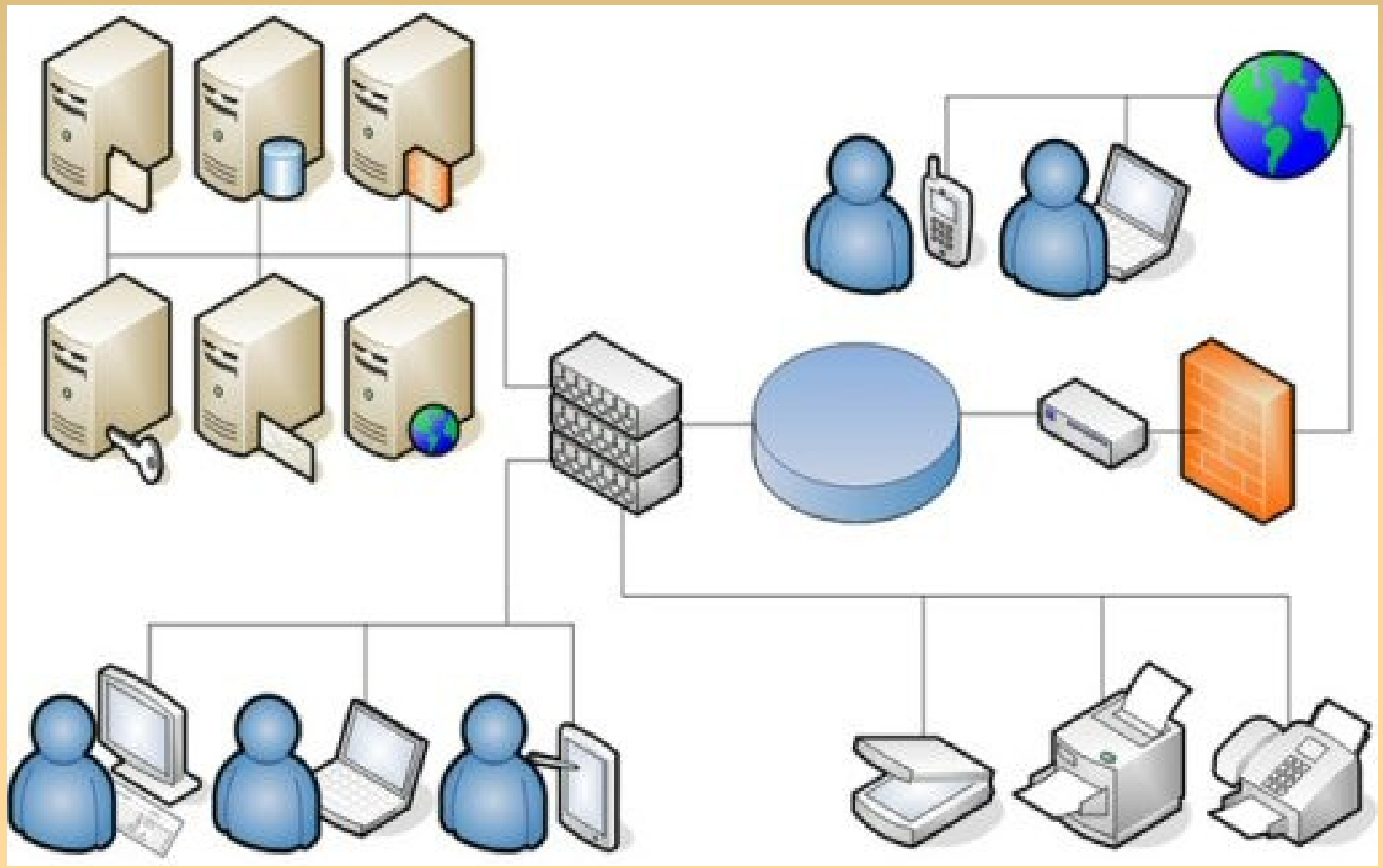
Analýza středně malých podniků

- Většinou 10-20 počítaců
- Vyhrazený jeden počítač pro služby souborů a tiskáren
- Menšina těchto podniků používá firewall
- Nejeví zájem o zabezpečení dokud nedojde ke ztratě důležitých dat

Jak ochránit středně velkou firmu

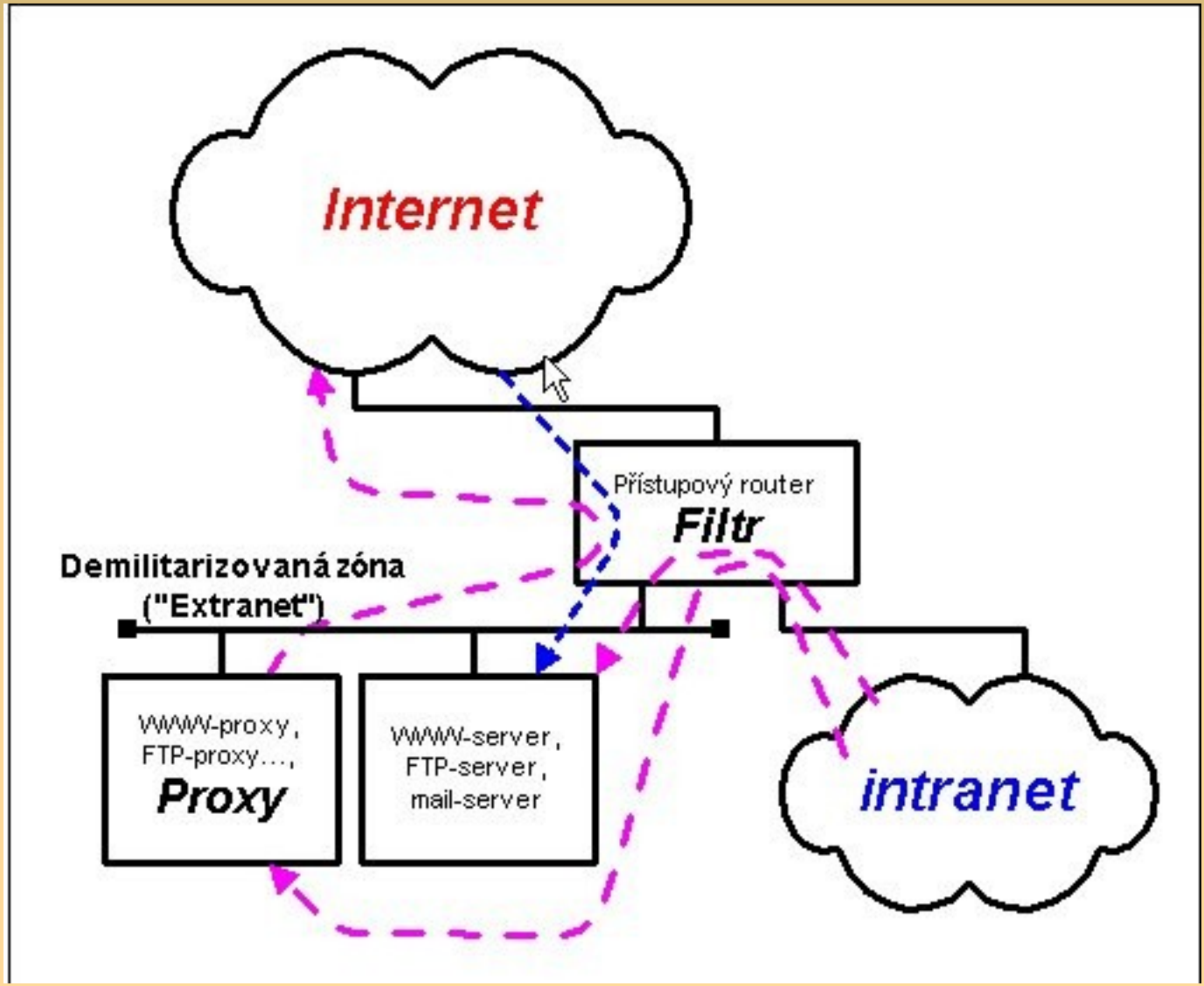
- U středně malých podniků není třeba při zabezpečování sítě jít do extrému
- Analyza nákladů a vynosů prozradí, že postačí méně přísné zabezpečení
- Tyto firmy nemají tolik důležitých informaci, které by zajímali náhodého hackera nebo konkurenci
- Výstavba firewalu za switchem

Jak ochránit středně malou firmu



ubuntu

Jak ochránit středně malou firmu



ubuntu

Použitá literatura

Siťová bezpečnost a firewall Oleksandr Petronyuk

ubuntu

Děkuji za pozornost

ubuntu