Detekce NATů na lokální síti

- MOTIVACE
- JAK NA TO?
- SOFTWARE
- DETEKCE NA SÍTI POD-O-LEE
- NÁPADY PRO DALŠÍ GENERACI

Proč detekovat NATy

- Kradení konektivity
- Snížení bezpečnosti
- Legislativní důvody

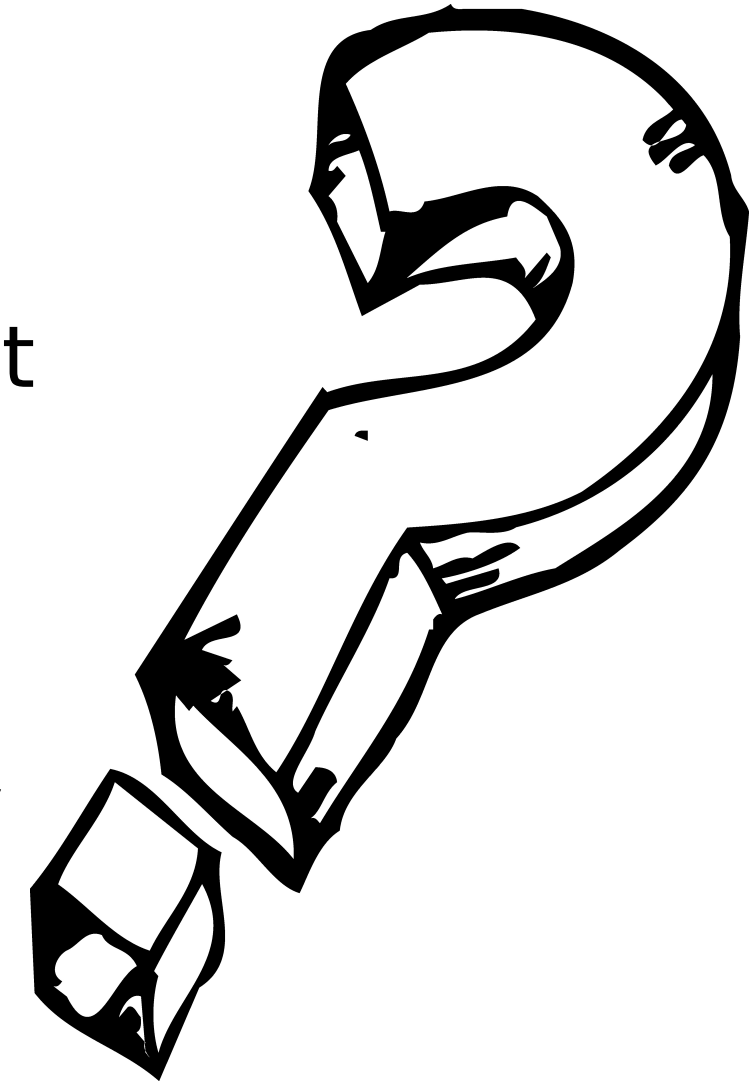
Jak zjistit NAT?

Spolehlivé metody

- rozdíl v TTL
- rozdíl v OS fingerprint

Doplňkové metody

- rozdíl v TimeStamp
- vysoké odchozí porty
- velikosti oken



Detekční programy

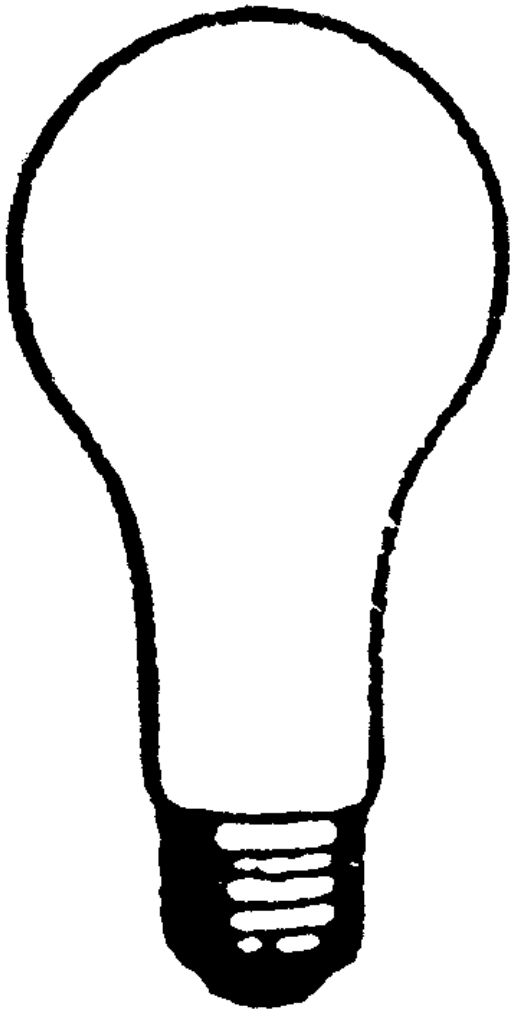
- NATDET (http://elceef.itsec.pl/natdet/)
- MASQDET (http://toxygen.net/misc/)

NATy na Pod-O-Lee

- IP6/2004, hlava III., bod 3.
- mirror trafiku
- bash, bash, bash

Nápady pro další generace

- pozor na zbytečné pakety
- pozor na false-positive
- třídění logů podle počítačů
- automatické odpojování
- statistiky
- ...



Děkuji za pozornost

DOTAZY?

mail: mr@MikyMaus.org
jabber: mr.MikyMaus@jabber.org

Detekce NATů na lokální síti

- MOTIVACE
- JAK NA TO?
- SOFTWARE
- DETEKCE NA SÍTI POD-O-LEE
- NÁPADY PRO DALŠÍ GENERACI

Jakub Fišer mr@MikyMaus.org mr.MikyMaus@jabber.cz

Proč detekovat NATy

- Kradení konektivity
- Snížení bezpečnosti
- Legislativní důvody

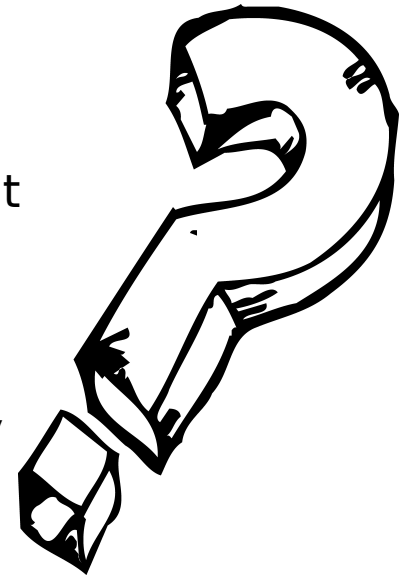
Jak zjistit NAT?

Spolehlivé metody

- rozdíl v TTL
- rozdíl v OS fingerprint

Doplňkové metody

- rozdíl v TimeStamp
- vysoké odchozí porty
- velikosti oken



Detekční programy

- NATDET (http://elceef.itsec.pl/natdet/)
- MASQDET (http://toxygen.net/misc/)

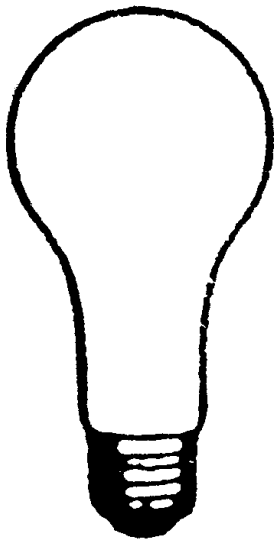
NATy na Pod-O-Lee

- IP6/2004, hlava III., bod 3.
- mirror trafiku
- bash, bash, bash

5

Nápady pro další generace

- pozor na zbytečné pakety
- pozor na false-positive
- třídění logů podle počítačů
- automatické odpojování
- statistiky
- ...



Děkuji za pozornost

DOTAZY?

mail: mr@MikyMaus.org
jabber: mr.MikyMaus@jabber.org