Generátor topológie siete pomocou ping, traceroute a nmap

Marcel Hlopko

Cieľ

- Scan celej siete
- Zistiť hierarchickú štruktúru
- Pre všetky stanice zistiť ip adresu a fully qualified domain name (ak existuje)
- Pre všetky stanice zistiť bežiace služby

Prostriedky

- Ping
- Traceroute
- SNMP
- DNS (nslookup ls, dig axfr)

Čo využijeme

- Ping pre zoznam živých hostov
- Traceroute pre zistenie hierarchickej štruktúry
- Nmap pre scan portov

Algorytmus

- Príklad: ČVUT
- Najprv scan 147.32.*.1 (24)
  - Ak nič potom 147.32.*.129 (25)
    - Ak nič potom 147.32.*.65 (26)
    - a 147.32.*.193 (26)

Výsledky testu

- Sobota 10 hodín ráno
- 3913 hostov alive
- Doba trvania: 37 minút :(
- Cca 150kb textových súborov

- A mail od kolejneho správcu siete:

System IDS v hodinovem mericim intervalu detekoval opakovane pokusy o pripojeni na IP adresy site CVUT, ktere nejsou a nebyly v provozu, tento provoz byl navic navazovan napric ruznymi IP segmenty, tj. nejedna se o lokalni broadcasty v ramci LAN. Je tak velmi pravdepodobne, ze nize uvedeny stroj je napaden virem ci ovladan hackerem, pripadne muze jeste jit o chybnou konfiguraci stroje ci opakovane omylyuzivatele.

- IP adresa podezreleho stroje: 147.32.89.82
- DNS jmeno tohoto stroje: ozembuch.pod.cvut.cz
- Cilove porty TCP spojeni: 80,636,113,23,0
- Nove navazanych spojeni: 1014000 :))

Ďakujem a odpovedám na otázky