anti-sniffers

NEPED

- http://www.apostols.org/projectz/neped/

Anti-Sniff

- http://www.l0pht.com/antisniff/index.html

Sentinel

- http://www.packetfactory.net/Projects/Sentinel/

tecniche

- DNS test
- Etherping Test
- ARP Test
- ICMP Ping Latency Test

DNS test

- sul segmento della macchina da testare, creo false connessioni tcp verso hosts inesistenti
- uno sniffer rozzo mandera` richieste al DNS per risolvere i nomi degli host
- intercetto le richieste e quindi rivelo lo sniffer

Etherping Test

- si basa su imperfezioni nel kernel di alcuni sistemi (alcuni Linux, NetBSD, NT)
- mando alla macchina da testare un ping echo con destination IP corretto e falso MAC address
- se la macchina mi risponde, so che la sua interfaccia e` in modo promiscuo

ARP Test

- si basa su imperfezioni nel kernel di alcuni sistemi (alcuni Linux, NetBSD, NT)
- mando in rete una arp request riguardante l'IP della macchina da testare.
- la richiesta e` corretta in tutto tranne che non e` un broadcast, ma e` inviata ad un MAC address inesistente
- se ottengo risposta, la macchina e` in modo promiscuo

ICMP Ping Latency Test

- misuro il tempo di risposta al ping (RTT) della macchina in test
- creo numerose false connessioni tcp sul segmento della macchina
- se la macchina ha l’interfaccia in modo promiscuo deve processare queste richieste
- mi aspetto che RTT cresca

Ad un primo esame

- non sono affidabili
- alcuni test possono sovraccaricare la rete
- ci sono problemi sulle switched LAN
- i test non hanno validita` universale (rivelano solo alcuni sniffer o funzionano solo con alcuni OS o solo in certe condizioni di traffico)
- e` possibile predere delle precauzioni in modo da eludere tutti i test

Rilevazione remota di sniffer

- per ora non e` noto un efficiente sistema di rilevazione remota delle interfacce di rete in modo promiscuo
- Possiamo conoscere con certezza solo lo stato dell’interfaccia locale

ifstatus

- e` un semplice script in C che legge lo stato dell'interfaccia locale (in molti sistemi ifconfig fa lo stesso)
- se l'interfaccia e` in modo promiscuo ifstatus scrive un messaggio su stdout
- installando ifstatus su tutte le macchine posso monitorare automaticamente lo stato di tutte le interfacce di rete
- e` bene nascondere il programma

ifstatus: dove trovarlo

- ftp://coast.cs.purdue.edu/pub/tools/unix/ifstatus/
- http://security.fi.infn.it/tools/ifstatus/
- http://www.ja.net/CERT/Software/ifstatus/

Autore:

David A. Curry - Purdue University