ANTCOLONY

Фильтры Wireshark'а для обнаружения попыток сетевого сканирования

Подсказки для системных администраторов

ICMP-SCAN:

(ip.flags == 0x00) && (icmp.type == 8 && icmp.code == 0) && (icmp.seq == 0) && (not data)

(ip.flags == 0x00) && (tcp.flags == 0x0002) &&(tcp.dstport == 443)

(ip.flags == 0x00) && (tcp.flags == 0x0010) && (tcp.dstport == 80)

(ip.flags == 0x00) && (icmp.type == 13 && icmp.code == 0) && (icmp.seq == 0) && (icmp[8:4] == 00:00:00:00) && (not data)

(((ip.flags == 0x00) && (icmp.type == 8 && icmp.code == 0) && (icmp.seq == 0) && (not data)) || ((ip.flags == 0x00) && (tcp.flags == 0x0002) &&(tcp.dstport == 443)) || ((ip.flags == 0x00) && (tcp.flags == 0x0010) && (tcp.dstport == 80)) || ((ip.flags == 0x00) && (icmp.type == 13 && icmp.code == 0) && (icmp.seq == 0) && (icmp[8:4] == 00:00:00:00) && (not data)))

PROTOCOL SCAN:

icmp.type==3 && icmp.code==2

XMAS:

tcp.flags==0X029

NULL:

tcp.flags==0x000

SYN-STEALTH:

(ip.flags == 0x00) && (tcp.flags == 0x0002) && (tcp.option_kind == 2) && not (tcp.option_kind == 3 || tcp.option_kind ==4)

FULL:

(ip.flags == 0x02) && (tcp.flags == 0x00c2) && (tcp.option_kind == 2 && tcp.option_kind ==3 && tcp.option_kind ==4 && tcp.option_kind ==8)