





# Nmap - the Network Mapper. Утилита для сканирования и исследования безопасности

Опубликовано muff.kiev.ua (<http://muff.kiev.ua>)

```
##### -sS #####
##### -p ##### -PS <порт> ##### scndmail #####
##### scndmail ##### Nmap #####

nmap -i -sS -p25 -PS25 24.0.0.0/8

-sF, -sX, -sN (scan FN, scan Xmas, scan NULL) - "##### FN, Xmas Tree ? NULL, ##### SYN, ##### RST, ##### SYN, ##### SYN, ##### Sylogger ??? Courtesy ##### SYN, #####

##### FN, ##### FN, ##### FN/URGFSH ? NULL, ##### RFC 973 3, 64, ##### RST, 1 ##### RST, 1 #####
#####

##### Microsoft Windows, ##### Windows ? ##### RST, ##### Nmap #####
#####

##### FN, ##### Windows, ##### SYN, ##### Windows, ##### Windows ? ##### Cisco, BSD, IRIX, HP/UX ?
MVS, ##### RST, #####

-sP (scan Ping) - ping - "##### ICMP, ##### IP, #####
##### (##### microsoft.com) ##### Nmap ##### TCP ACK, ##### RST, ##### SYN, ##### RST ? SYNACK, ##### root, ##### connect(),
##### Nmap ? ##### -ICMP ? ACK, ##### -P, ##### ping - "#####
#####

-sV (scan Version) - "##### TCP, ##### UDP, #####
##### - "#####
##### Nmap, ##### (ftp, ssh, telnet, http, ##### (ISC Bind, Apache httpd, Solaris scheld), ##### SSH, ##### OpenSSL, ##### SSL, #####
##### RPC, Nmap, ##### RFC, ##### -A, #####

##### http://www.cherepovets-city.ru/insecure/runmap/runmap-versionscan.htm [1] - "##### Nmap ?
#####

-sU (scan UDP) - "##### UDP, ##### RFC 768, ##### ICMP, ##### UDP, #####
#####
##### rpbind ? Solaris, ##### UDP, ##### 32768, ##### 111-3 #####
#####
##### RFC 1812 (##### 4.3.2.8) ##### ICMP, ##### Linux (##### net(ipv4-kmp.h) ##### 80 74 ##### 0.25 #####
##### 2) Solaris ##### Solaris #####

Nmap ##### Microsoft ##### 65535
UDP, ##### Windows.

-sO (scan Open protocols) - "##### IP, ##### IP, #####
##### Nmap #####
##### (AIX, HP-UX, Digital UNIX) - "##### (1.2) #####
#####
##### ICMP, ##### IP, ##### 256 #####
#####

-sI <zombie_xorc[nopt]> (scan IRI) - "##### IP, ##### IRI, #####
#####
##### здесь [2] - "##### ping"

-sA (scan ACK) - "##### ACK, ##### (ackseq) ##### SYN, #####
##### ACK, ##### RST, ##### ICMP, #####
##### Nmap ? #####
##### -sW (scan Window) - "##### TCP Window, ##### ACK, #####
##### initial Window TCP, #####
#####
#####
##### AIX, Amiga, BeOS, BSD, Cay, Tru64 UNIX, DG-UX, OpenVMS, Digital UNIX, FreeBSD, HP-UX, OS/2, IRIX, MacOS, NetBSD, OpenBSD, OpenStep, QNX, Rhapsody, SunOS 4.x, Ultrix, VAX ? VxWorks, ##### nmap-backers.
```









