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

????????

Nmap - the Network Mapper. ??????? ??? ??????????? ? ??????????? ??????????? ????.

?????????????

nmap [?????(?) ???????????] [?????] <???? ??? ???? #1,[#N]>

????????

????????? Nmap ??????????? ??? ??????????? ????? ? ????? ??????????? ????????, ??????????? ????????? ???????? ??????????? ??? ? ???? ?????? ? ??????????? ?? ?????. ??? ????? Nmap ??????????? ????? ????????? ??????? ???????????, ?????, ??? UDP, TCP connect(), TCP SYN (???????????), FTP proxy (?????? ????? ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree,

SYN ? NULL-???????????. ????? ????????? ?? ???????? ????????? ? ??????? "????? ?????? ?????? ???????????".

Nmap ????? ??????????? ??????? ????? ??????????? ??????????, ? ??????: ??????????? ??????????? ??????? (????? - ??) ????????? ????? ? ??????????? ????????? ????? TCP/IP, "????????" ???????????, ??????????? ??????????? ??????? ???????? ? ?????? ???????? ???????, ??????????? ???????????, ??????????? ????????? ?????? ??????? ????????????

ping-??????, ??????????? ? ??????????? ?????? ??????, ??????????? ??????? ???????? ????????, ?????? (??? ??????????? portmapper) RPC-???????????, ??????????? ? ???????????? IP-??????????? ? ????? ??????????? ??????? IP-??????? ? ??????? ?????? ??????????? ?????.

??????????? ?????? Nmap ???????? ?????? ?????????????? ?????? ????????? ?????? ? ???????? ?????? ? ????????? ?????, ???? ??????????? ????????? ? ????? ???????? ??????, ??????????? ?? ???? ??????. ???? ??????????? ????? ????????? ??????????: "??????", "???????????" ? "????????????". ????????? "??????" ????????, ??? ????????? ?????? ??????????? ?????? ???. ????????? "???????????" ????????, ??? ????????, ???????? ?????? ??? ?????? ??????????? ???????? ?????? ? ????? ????? ? Nmap ?? ???? ?????????? ??? ????????. "????????????" ????????, ??? ?? ??????????? ??????????? Nmap ????????? ?????? ???? ??? ????????, ??? ???? ???????? ?????? ?? ???????? Nmap ?????????? ??? ????????. ??? ???????? Nmap ?????????? ?

????? ?????? (???? ???? ??????????? ??????????? ?????? ????? ??????????).

? ??????????? ?? ????????? ?????, Nmap ????? ????? ?????????? ???????? ??????????????? ??????????????? ?????: ????? ????????? TCP ISN, ??? ??????????? (*username*) ???????? ????????, ??????????????????? ??????????? ????, ?????????? ?????, ??????????????? ??????????? IP-??????? ? ?.?.

_____

??????????? ????? ????? ?????????????? ???? ? ??????. ???? ????? ??????????? ??? ?????? ??????????? ?????? ??????????, ?????? ???????? ?? ??????????? ??????????? ??????????? ??? ?????? ??? ????????? ???????? ????????? ???????????. Nmap ??????????? ??????????? ? ??????????? ???????? ???????? ?? ????. ??, ??? ????? ????????? ?????

????? ? ??????????, ????? ????????? ???? ?????? ? ??????? ? ???????? ???????? ?????? Nmap ? ????? ??????? ??????????. ?? ????? ????? ???????? ???????? Nmap ? ?????? **'-h'** ??? ???????? ??????? ??????? ?? ???? ??????.

????? ?????? ?????? ???????????

-sT (scan TCP) - ??????????? ????? TCP connect(). ???????? ????? ????? ??????????? TCP-??????. ??????? connect(), ??????????? ? ????? ??, ???????? ??????? ??????????? ? ????? ?????? ???????? ??????. ???? ???????? ? ???????? ???????? ???? ?????? ? ??????????? ??????????? ??????, ?? ???????? ??????????? connect() ????? ???????? (?.?. ??????????? ?????

??????????), ? ????????? ?????? ???????? ???? ???????? ????????, ???? ?????? ? ???? ??????????? ??????????? ??????.

??? ????, ????? ??????????? ?????? ?????, ??????????? ????? ?? ????? ??????? ????????? ?? ??????????? ?????. ???? ????? ??????????? ????? ??????????? ??????? (?.?. ??????????) ??????, ???????? ??? log-???? ????? ???????? ?????????????????? ??????????? ??????? ??????????? ? ?????? ??????????? ?????? ????????. ??????, ??????????????? ??????????,
???????? ??????????? ?????? ??????, ??????????? ??? ??????.

-sS (scan SYN) - ??????????? ????? TCP SYN. ???? ????? ????? ???????? "???????????" ???????????, ???????? ??? ???? ?????? TCP-????????? ? ?????? ??????????? ?????? ?? ?????????????. Nmap ??????? SYN-?????, ??? ?? ??????????? ??????? ???????? ??????????, ? ??????? ?????. ??????? ?????? SYN/ACK ? ?????? ???????? ?? ??, ??? ???? ???????? ?????? ??????

? ????????????. ???? **RST** ? ?????? ???????? ????????. ???? Nmap ?????? ????? SYN/ACK, ?? ? ????? ??????????? ????????? **RST**-????? ??? ?????? ??? ?? ???????????? ????????? (??????? ??? ???????? ???????? ???? ??), ????? ??????? ????? ???????? ??????????? ????? ??????????. ??????????? ?????? ????? ?????? root ??? ??????????? ??????????? SYN-??????.

??? ????????? ???????? ?????? ?????? ??? ??????????? ??????? ????? ???????? ? ?????? **-sS** ?? ?????? ??????????? ?????, ??????????? ???????? ?????-???? ???? ?? ???? ???????? ???????? ??????????? ???? ???? **??????? ???????**, ??? ??? ???????????? ????? ????? **-p**. ??? ????? ??????? ? ??????? ?????? **-PS <порт>**. ????????, ???? ????? ??????????? ????? ?????????? ? sendmail, ??? ????? ????????????

?? ???????? ????? ??????????, ?? ????? ??????? sendmail ??????????. ??????? ??????? Nmap ????? ????????? ????????? ??????? (??????):

nmap -n **-sS** -p25 **-PS25** 24.0.0.0/8

-sF,-sX,-sN (scan **F**IN, scan **X**mas, scan **N**ULL) - "?????????" FIN, Xmas Tree ? NULL-???????????. ??? ?????? ??????????? ? ??????, ???? SYN-???????????? ?? ?????-???? ???????? ????????? ????????????????. ???, ????????? ????????? ? ???????? ??????? "????????" ?????????? SYN-?????? ?? ?????????? ??? ?????, ? ????????? ???? Synlogger ??? Courtney ???????? ????????

SYN-????????????.

???? ??????????? ? ????????. ? FIN-??????????? ? ???????? ??????? ??????????? FIN-?????. ? Xmas Tree ??????????? ????? ? ??????? ?????? FIN|URG|PSH, ? NULL-??????????? ?????????? ????? ??? ??????. ???????? ???????????? RFC 973 ?. 64, ?? ??????????? ????? ?????? ???????? ?? ????? ?????, ????????? ?? ???????? ????, ??????? RST, ? ?? ????? ??? ???????? ???? ?????? ??????????? ??? ??????.

??????????? Microsoft Windows, ??? ??????, ?????? ????????? ??????????? ??? ??????????? ???????? ? ????? ????? ?????. ??????? ????? ?? ????????? Windows ?? ???????? ? ????? RST-?????, ? ?????? ?????? ?? ????? ???????? ? ????? ??. ?????? ?? ???? ???? ???? ????? ?????, ? ? Nmap ???? ??????? ???????? ???????? ??? ??????????? ??????????? ??????, ?????????? ????? ?????????.

???? ? ?????????? FIN-???????????? ?? ???????? ?????? ???????? ??????, ?? ??? ?? Windows. ???? ?? ??? ??? ?????? ?????? ????????, ??? ??? ????? ???????, ? SYN-??????????? ?????????? ???????? ?????, ?? ?? ?????? ????? ?????? ???? ? ?? Windows. ? ????????, Windows ?? ???????????? ??, ?????????? ???? ??????????. ? ????? ?? ????????? ????? Cisco, BSDI, IRIX, HP/UX ? MVS. ??? ??? ?? ?? ?????????? RST-??????.

-sP (scan **P**ing) - ping-"????????????". ?????? ??? ?????????? ???? ?????? ?????? ???????? ?????? ? ??????????? ????. Nmap ????? ??????? ???, ?????? ICMP-????????? "??????? ???" ?? ?????? IP-?????, ????????? ????. ????, ??????????? ????? ?? ???, ???????? ????????.

????????? ????? (??????? microsoft.com) ????????? ???-??????. ?? ???? ??????? Nmap ????? ???????? TCP ACK-????? ?? 80-? ???? ??????????? ????? (?? ????????). ???? ? ????? ?? ???????? RST-?????, ???? ???????. ?????? ????? ?????????? SYN-???? ? ??????? ? ???? RST ??? SYN|ACK. ??? ????????????, ?? ?????????? ???????? root, ??????????? ????? connect().

??? root-???????????? Nmap ?? ???????? ?????????? ??????????? ??? ????? - ICMP ? ACK. ?? ?????? ???????? ???, ????????? ????? **'-P'**, ???????? ????. ???????, ??? ping-??????????? ?? ????????? ??????????? ? ????? ?????? ? ?????? ???????? ????? ??????????? ??????????. ??????????? ??? ????? ?????? ? ??????, ???? ?? ?????? ????????? ????? ping-?????, ?? ????????

??????????? ??????.

-sV (scan Version) - ????????? ?????? ??????????? ?????? ?????, ?? ???????? ?????????? ??????????? ?????. ????? ????????? ??????????? ????? ??????? ?????? ???????? TCP ?/??? UDP-??????. ??? ???? ????? ? ?????? ???????? ??????? ????? ????? ??????? ??????, ??????? ?????? ??????????? ?????? ???? (??? ??????????? ??????? ?? ???? ?????? "????????????" ??????, ???? nmap-services). ??? ??????????? ????? ????? ???????? ??????????? ??????????? ?????? ?????, ??????? ???????? ???????????????? ??????????? ???? ?????? ? ????? ??????????? ????? ? ?????? ?????, ?? ????????? ??????????? ??????????? ?????. ????, ????????? nmap-service-probes ??????????? ??? ??????????? ??????????? ??????, ? ??????? ??????? ????? ???????? ??????????? ?????? ??????????? ? ?????? ????????. Nmap ???????? ??????????? ???????? ?????? (ftp, ssh, telnet, http), ??? ??????????? (ISC Bind, Apache httpd, Solaris telnetd), ????? ?????? ? ?????????????? ??????????? (?????? ????????? SSH). ???? Nmap ???????????? ? ?????????? OpenSSL, ?? ?????????? ??????????? ? SSL-??????? ? ??????????? ??????????, ????? ?????? ???????? "?3" ??????????. ???? ??????????? ??????? RPC, Nmap ???????????? ????? ?? RPC ?? ?????? "?????? ????" ??? ??????????? ?????? ???????? RPC ? ?????? ??????. ????????, ??? ????? -A ????? ???????? ???? ?????. ??? ????????? ?????

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

-sU (scan **U**DP) - ??????????? UDP-????. ???? ????? ??????????? ??? ??????????, ????? UDP-????? (RFC 768) ?? ??????????? ????? ???????? ????????. ?? ?????? ???? ??????????? ?????? ??????????? UDP-????? ??? ??????. ???? ? ????? ???? ??????? ICMP-????????? "???? ??????????", ??? ????????, ??? ???? ??????. ? ????????? ?????? ?????????????, ??? ?????????? ????

??????.

???????? ??????? ??????????? UDP-?????? ??????????? ????????. ?? ? ???? ?????? ?????????? ? ???????? "????" ? ?????? **rpcbind** ?? Solaris. ?? ????? ???? ????????? ?? ????? ?? ?????????????????? UDP-?????? ? ???????, ?????? 32770. ???? ?? ?????????? ???, ?? ????? ??? ?? ?????, ??????????? ?? 111-? ???? ?????????? ??? ???.

? ?????????, ??????????? UDP-?????? ???????? ????? ????????, ???????? ??????????? ??? ?? ??????? ???????????? RFC 1812 (?????? 4.3.2.8) ?? ??????????? ???????? ???????????? ICMP-???????? "???? ??????????". ????????, ???? Linux (??????? net/ipv4/icmp.h) ??????????? ???????????? ????? ????????? ?? 80 ?? 4 ??????? ? ???????? 0,25 ???????, ???? ??? ??????????? ???? ????????. ? ?? Solaris ??? ????? ??????? ??????????? (2 ???????? ? ???????), ? ??????? ??????????? Solaris ??????? ??? ????? ????????.

Nmap ?????????? ???????? ????? ??????????, ? ?????????????? ???????? ?????????? ??????????? ????????, ??????????? ??? ????? ?????????? ???? ????????? ????????, ??????? ??????????? ??????? ???????. ??? ??????, Microsofs ????? ??? ?????????????, ? ?? ?????????? ? ????? ?? ??????? ??????????. ??????? ?? ????? ?????? ?????? ??????????? ??? 65535 UDP-?????? ?????, ?????????? ??? ?????????? ?? Windows.

-sO (scan **O**pen protocol) - ??????????? ?????????? IP. ?????? ????? ??????????? ??? ?????????? IP-??????????, ??????????? ??????????? ?????. ????? ?????????? ? ???????? ????? IP-??????? ??? ??????-???? ????????? ??? ??????? ???????? ??????????? ?????. ???? ???????? ????????? "???????? ??????????", ?? ?????? ???????? ?????? ?? ???????????. ? ????????

?????? Nmap ???????????, ??? ???????? ??????????????? ??????.

???????? ?? (AIX, HP-UX, Digital UNIX) ? ???????? ????? ??????????? ???????? ???????? "???????? ??????????". ?? ???? ??????? ??? ??????????? ???????? ????? "???????" (?.?. ?????????????).

???????? ???????? ??????? ????? ? ??????? ??????????? UDP-??????, ??????????? ??????? ????????? ICMP-???????? ????? ????? ????? ????? ?????. ?????? ???? "??? ????????" IP-???????? ??????? ????? ???? ?? 8 ???, ??????? 256 ??????????? ????? ??????????? ?? ??????????? ?????.

-sI <zombie_хост[:порт]> (scan **I**dle) - ???????? ?????????? ???????? ?????????? ??????????? ??????. ?????????? ????? ??????????????? ????, ?? ??????? ??? ???? ??????? ?? ?????? IP-??????. ?????? ????? ??????????? ????? IdleScan, ??????????? ?????????????? ?????? ????? ??? ??????????? ????-"?????". ????? ??????????? ??????????, ???? ??? ??????????? ????????? ????????? ??????? ??????? ????? ???????? ?? ?????? ????????? IP. ??????? ??????????? ?????????? ???????? ????? ?? ???????? ?????-"?????". ????? ??????, ????? ??????????????? ???? ? ?????????????? ?????????? "?????", ?????? ???? ????? "????????", ? ????? ?????????? ? ???????? ????????. ?????? ???? ?????????? ????? ???? ????? ?????? ??? ?????? ????? "??????? ?????". ??

??????????? ?????? ? ???????? ????? ??????, ?? ?????? ??????????? ? ???.<u>здесь</u> [2]. ?? ?????? ??????? ?????????? ???? ?? ???????? ????????? IPID ?? ?????-"?????". ? ????????? ????? Nmap ????? ??????????? ????? ????? ?? ????????? ??? "tcp ping".

-sA (scan **A**CK) - ??????????? ACK-???????????. ???? ??????????????? ????? ??????????? ??? ?????????? ?????? ?????? (ruleset) ????????. ? ????????, ?? ???????? ????????, ??????? ?? ??????????? ???? ????????? ??? ?????? ???????? ???????, ??????????? ??????? SYN-??????.

? ???? ?????? ?? ??????????? ???? ????? ??????????? ACK-????? (?? ????????? ?????????? ????? *acknowledgement number* ? *sequence number*). ???? ? ????? ?????? RST-?????, ???? ??????????????? ??? "???????????". ???? ?????? ?? ??????????? (??? ?????? ICMP-???????? ? ?????????????? ?????), ???? ??????????????? ??? "??????????".

???????, ??? Nmap ?? ?????? "???????????" ????? ? ??????????, ??????? ???? ?? ?? ????????? ?? ?????? ???????? ????? ??? ??????????? ????? ???? ??????????, ??? ????? ????????, ??? ??? ????? ??????????????? ? ???????? ?????????????. ???????? ???? ????????, ??? ??? ????? ??????? ?? ??????? ????????? ????? "??????" ? ??????????? ???????????.

-sW (scan **W**indow) - ??????????????? ????? TCP Window. ???? ????? ????? ?? ACK-???????????, ?? ??????????? ????, ??? ?????? ? ??? ??????? ????? ?????????? ???????? ????? ????? ??? ?? ,??? ? ??????????/??????????????. ??? ????? ???????, ???????? ???????? ???? Initial Window TCP-??????, ?????????????? ?????? ? ????? ?? ????????? ??? ??????, ????? ??????? ???????????????

??????????????? ????????? ??????? ???? ? ????????? ??.

????? ???????? ??????????????? ?????? ???????? ? ???? ?? ??????? ???? ???????? ?????? AIX, Amiga, BeOS, BSDI, Cray, 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-hackers.

-sR (**s**can **R**PC) - ??????????? **R**PC-???????????. ??? ????? ??????????? ????????? ? ??????? ???????? ??????????? ? ????????? ????????? ????????, ??????? ??????????? RPC-.????, ? ????? ?? ??????. ??? ????? ??? ???????? TCP/UDP-????? ????? ??????????? NULL-????????? ???????? SunRPC, ????? ???? ??????????? **R**PC-????? ? ??????????? ?? ???? ????????. ?????

???????, ?? ???? ????????? ??????????, ??????? ????? ?? ???????? ? ??????? ??????? '**rpcinfo -p**'. ??? ???? portmapper ??????????? ????? ?????? ?????????? ??? TCP-wrapper??.

-sL (**s**can **L**ist) - ???????? ?????? ??????????? ???????. ??? ????? ????????? ??? ???????? ?????? ??????? ??????, ??????? **?????** ??????????? Nmap, ?? ?????? ???????? ???????????. ?? ????????? ??????????? ????? ??????, ?????? ??? ????? ??????????, ????????? ????? **-n**. ????? ????? ?????????????? ? ??????, ????? ??? ?????????? ?????????? ????? ???????? ?????????? ?????? ?? ?? ??????? ? ?.?.

-b <ftp_relay хост> (**b**ounche scan) - ??????????? ????? "??????? ????? **F**TP". ?????????? "???????????" ???????? FTP (RFC 959) ???????? ????????? "??????????" (proxy) ftp-??????????. ??????? ???????, ? ??????????? ????? source.com ????? ??????????? ? ftp-???????? target.com ? ????????? ????, ??????????? ?? ???, ?? ????? ????? Internet! ???????, ??? ?????? ??????????

???????? ? 1985 ???? (????? ??? ??????? ???? RFC). Nmap ????????? ??? "????" ??? ??????????? ?????? ? "???????????" ftp-???????.

????, ?? ?????? ??????????? ? ftp-??????? "???" ??????????? ? ????? ??????????? ?????????????? ?? ????? (???????? 139-?). ???? ftp-?????? ????????? ?????? ? ??????????? ?????? ? ?????-???? ??????? (???????? /incoming), ?? ????? ?????? ????????? ????? ?????? ?? ??? ????. ????????, ??????????? ????? '**-b**', ??????????? ????? URL ??????? ftp, ???????????? ? ???????? "???????????".

?????? URL ?????????: **имя_пользователя:пароль@сервер:порт**. ????? ??????? ????? ??????? ???????????, ????????? ????? ?? ?????????.

????? ????????? ? ?????? ????????????? ???????????

??? ????? ?? ??????????? (?.?. ???????? ????????? ?????? Nmap ? ??? ?? ????????), ?????? ??? ??? ???????? ?????? ?????????.

-P0 (**P**ing **0**) - ?? ??????????? ping-????? ?????? ????? ?? ?????????????????? ???????????. ??? ????? ????????? ??????????????? ????, ??????????? ????????? ICMP-??? ? ??????? ??????????. ???????? ????? ???? ???????? microsoft.com, ? ?? ?????? ?????? ??????????? ????? '**-P0**'???'**-PT80**'(??. ????), ????? ??????????? ????? ????.

-PT (**P**ing **T**CP) - ??????????? TCP "ping". ?????? ??????? ??????? ICMP-???, Nmap ????????? TCP ACK-????? ?? ??????????? ???? ? ??????? ?????. ???? ???? ???????, ?? ? ????? ?????? ?????? RST-?????. ??? ??-root ??????????? ??????????? ??????? connect(). ??? ????? ????????? ??? ?????????? ????????? ??????????? ?????, ???? ???? ????????? ICMP-??? ????????

??????????. ??? ????????? ?????? ????? ??????????? ??????, ?? ??????? ????? ??????????? ACK-????, ??????????? ????? '**-PT <номер_порта>**'. ?? ????????? ??????????? 80-? ????, ????????? ?? ??????????? ??????? ?? ??????????.

-PS (**P**ing **S**YN) - ?????, ????? ??????????? ??? ping-??????. ??? ???? ????? ACK-?????? TCP "ping" ??????????? SYN-?????. ???????? ????? ???????? ? ????? RST-?????? (???? - SYN|ACK).

-PU [portlist] (**P**ing **U**DP) - ??????????? UDP Ping. Nmap ?????????? UDP-?????? ?? ????????? ???? ? ??????? ? ????? ICMP "port unreachable" (??? ?????? ?? ???????? ?????? UDP) ???? ???? ???????. ????????? ??????????? ?????, ??????????? UDP, ?? ???????? ?? ???????, ??? ????? ??????????? ?????, ??????? ???????? ???????.

-PE (Ping ICMP) - ??? ????? ??????????? ? ???????? ping-??????? ?????????? ping-????? (?????? ICMP-???). ????? ??????????? ??? ?????? ???????? ?????? ? ????? ??????? ????? ? ??????????? ???????????. ????? ???? ??????????? ????????? ICMP-????? ???? ????? ????????. ??? ???????, ????? ???? ??????????? ????? "????? ??????" ??? ??????.

-PP - ?????????? ????? ICMP "timestamp request (code 13)" ??? ??????????? ???????? ??????.

-PM - ????? ? ???????**-PE** ?**-PP** ?? ??????????? ????, ??? ??????????? ????? "netmask request" (ICMP code 17).

-PB (**P**ing **B**oth) - ????? ping-?????? ?? ????????. ?????????? ??????????? ??????? ???? ACK ? ICMP.

-O (**O**perating system detection) - ??? ????? ?????????? ?????????? ??????????? ??????? ??????????? ????? ? ??????? ?????? ??????????? ????? TCP/IP. ??????? ??????, Nmap ??????????? ?????? ????????, ??????????????? ?? ?????? ??????? ??????? ???????? ??????????? ?????????? ??????????? ?? ??? ??. ? ?????????? ??????????? ?????????? ??????????????? "??????????",

????????? ?? ??????????? ???????? ???????? ? "????????" ????? ?? ???. ????? ?????????? ????????? ??????????? ? ?????????? ????? ??????????? ??????? ????????? ??, ?????????? ? ????? nmap-os-fingerprinting, ? ?? ????????? ????? ??????????? ??????? ? ???? ? ?????? ?? ??????????? ?????.

???? ????? ??????? ??????? ???? ?? ?????? ????????? ? ?????? ????????? ????? ?? ??????? ????. ???? ?? ?????????? ??????, ? ??????? ??? ??????? ??????????, ?? Nmap ?? ???? ??????????? ?????? ?? - ??????? ??? ????? ???? ??????. ???? ??, ?? ?????-???? ???????? ??????? ????? ?? ??????????????? ????????, ????????? Nmap ? ?????? '**-d**' ? ??????? ??????????? ????????.

-A ??? ????? ???????? ????? **a**dditional **a**dvanced **a**ggressive, ? ????????? ????? -O, -sV, -T4 ? -v.

-6 - ????? ????????? ???????????? ????????? IPv6. ??? ???? ????? ??????????? IPv6 ??? ???????????? ???? ?????, ? ????? ???? ??????? ????? ??????????? ????? DNS (?????? AAAA) ??? ??????????? IP-???????, ???????? 3ffe:501:4819:2000:210:f3ff:fe03:4d0. ?? ?????? ??????, ??????????????? ?????? ?????? TCP connect()-???????????? ? TCP connect() Ping-???????????. ???? ???

????????? UDP ??? ?????? ??? ???????????, ??????????? ????? http://nmap6.sourceforge.net/ [3].

-I (**I**dent scan) - ??????????? reverse-ident ???????????. ???????? Ident (RFC 1413) ???????????? ??????? ??? ??????????? (*username*) ????????, ?????????????? TCP, ???? ???? ???? ??????? ?? ??????????????? ??????????. ???, ????????, ?? ?????? ??????????? ? ? ????? http ? ????? ??????????? identd ??? ??????? ?? ??????? ??????????? root. ??? ????? ???? ??????? ?????? ??? ????????????

"???????" TCP-??????????? ? ?????? ??????????? ?????? (?.?. ??????????? ??????????????? ????? '**-sT**'). Nmap ????????? identd ??????????? ????? ??????????? ? ?????? ???????? ??????. ??????????, ???? ????? ?? ????? ????????, ???? ?? ??????? ????? ?? ??????? identd.

-f (use **f**ragmentation) - ??? ????? ??????????? ???????????? ? SYN, FIN, Xmas ??? NULL-??????????? ? ????????? ?? ??????????? ??????????????? IP-??????????? ? ????? ???????? ??????????. ???? ??????????? ? ???, ????? ??????? TCP-???????? ?????? ?? ???????????? ??????????? (?????? ???) ?? ??????? ????????. ??????????? ???? "????????" ??? IP-???????? ? ???? TCP-?????.

??? ??????????? ????????? ??????????? ???????, ?????? ?????? ??????????? ? ?????? ???????? ??????? ??????, ? ????????? Nmap ?????? ???? ????????. ?????? ?????????, ???????? ??? ?????? ????????? ????????? "????????" ??? ??????? ??????? ????? ????????? ????????. ???, ????????, ?????? ???????? "????????" ????? ????? ?? ?? ????????? ??????? 36-???????? ????????. ?
?????? ?? ??? ?????? 24-??????? ????????.

-v (verbose output) - ??????????? ????? "??????????? ??????". ??? ????? ??????????????? ??????????????? ? ????? ???????, ????????? ??? ???? Nmap ???????? ???????? ? ???? ?????????? ??????? ????????. ??? ????????? ??????? ??????? ????? ??????? ?? ??????. ?? ? ???? ?? ??????? ??? ????? '**-d**', ?? ?? ??????????? ?????? ? ??? ????? ??????????? ??????.

-h (show **h**elp) - ???????? ??????? ?? ???????????? Nmap ? ????????? ????? ? ???????? ?? ????????, ?? ???????? ???? ????????.

-oN <имя_файла> (**o**utput **N**ormal) - ??????????? ?????????? ??????????? ? ?????????? ???? ? ??????? ??? ??????????? ?????.

-oX <имя_файла> (**o**utput **X**ML) - ??????????? ?????????? ??????????? ? ????, ????????? ? ???????? ????????, ? ??????? **XML**.??? ????????? ?????????? ????? ???????????????? ????? Nmap?. ?? ?????? ??????????? ???????? '-' (??? ???????) ??? ?????? ?? stdout. ??????????? ????? ? ???? ?????? ????? ????????. Document Type Definition (DTD) ?????????????????? ????????

??????????? Nmap ? ??????? XML ??????? ?????: http://www.insecure.org/nmap/nmap.dtd [4].

-oG <имя_файла> (**o**utput **G**repable) - ??????????? ?????????? ??????????? ? ????, ????????? ? ???????? ?????????, ? ???????,??????? ??? ?????? ???? **grep**. ??? ???????? ??????, ??? ??????? ??? ?????? ??????????? ? ???? ??????. ?????? ?????? ?? ????? ????? -oM (??. ?????? ??????) ? ??????????? ??? ??????????????? ? ??????? ??????????. ?????? ?? ??????????? ???????????

XML. ????? ???????? ??????????????? ????????? '-'.

-oA <базовое_имя_файла> (**o**utput **A**ll) - ??????????? ?????????? ?? ???? ??????? ???????? (??????????, grep ? XML). ??? ??????????? ??????? ???? ?????, ? ???????? ????? ????? ?????????? base.nmap, base.gnmap ? base.xml.

-oS <имя_файла> (**o**utput **S**cript kiddie) - ??? ??????????? ?? ???????????? ??? ????????? ????? s|<ipT kiDdi3: thls l0gz th3 r3suLtS of YouR ScanZ iN a **s|<ipT kiDd|3** f0rM iNto THe fiL3 U sPecfy 4s an arGuMEnT! U kAn glv3 the 4rgument r'-r' (wltHOUt qUOteZ) to sh00t output iNT0 stDouT!@!!

--resume <имя_файла> - ???? ?? ???????? ??????????? ???? ???????? ????????? <Ctrl C>, ?? ?? ?????? ????????? ???, ????????? ??? ?????, ???? ????????? ??????????? ??????????? ? ???-???? ? ??????? ????? '**-oG**' ??? '**-oN**'. ? ???? ?????? ???????? Nmap ? ????????? ???? ???? ? ????? ?????, ? ??????? ??????????? ?????? ??????????? ??????. ??? ???? ??????? ?????? ?????

???????? ?? ?????, ???????? ??? ??????????? ??????????? ????? ???????????? ?????, ???????? ? ????????? ??????. Nmap ???????? ??????????? ? ??????, ????????? ?? ???????? "??????????".

--append_output ??????????, ? ?? ??????? ???-????.

-iL <имя_файла> (**i**nput **L**ist) - ????????? ???????? ??????? ?????? ?? ????????? ?????. ???? ?????? ????????? ?????? ???? ?????? ??? **IP**-???????, ??????????? ????????, ??????? ????????? ??? ??????????? <CR><LF> (?????? ???? - ? ????? ??????). ???? ?? ?????? ??????????? Stdin ? ???????? ????????? ??????????? ? ??????, ??????? ?????? ????? ????? ?????? '**-**'. ????? ????????? ?????????? ? ????????

????????? ????????? ? ??????? "???????? ??????? ???????? ?????".

-iR (**i**nput **R**andom) - ???? ?? ??????? ??? ?????, Nmap ????? ??????????? ???????? ????????? ?? ?????, ?????? ??????? ???????? ? ??????? ?????????? ???????? ??????. ???? ?????? ????? ??????, ??? ?? ??? ?? ????????. ??????? ????? ??????????? ??? ?????????????? ??????????? Internet.

-p <диапазон(ы)_портов> (**p**orts) - ??? ????? ????????? Nmap, ????? ????? ????????? ???????????????. ????????, '**-p23**' ???????? ???????????? 23 ????? ?? ??????? ??????. ???? ??????? ????????? ???? '**-p 20-30,139,60000-**', Nmap ????? ??????????? ????? ? ???????? ? 20 ?? 30 ???????????, 139 ? ?? 60000 ? ???? (?? 65535). ?? ????????? Nmap ????????? ??? ????? ? ????????? 1-1024,

????????? ??? ??? ?????????? ? ????? services.

-F (**F**ast scan) - ??????? ???????????. ????????? Nmap ?? ??????????? ??????????? ?????? ?????? ??? ????, ??????? ??????????? ? ????? services. ??????????? ???????? ??????? ??????, ??? ???? ?? Nmap ????????? ??? 65535 ??????.

-D <ложный_хост1,[ложный_хост2],[,ME],...> (use **D**ecoy hosts). - ? ???? ?????? Nmap "???????" ?????? ?????, ?????? ??????? ???????? ??????????? ? ??????????? ? ???????? ??????????. ??? ???? ?? ??????? ??????????? ????? ????????? ????????, ??? ??????????? ??????????????? ??????????? ? ????????? ?????? (?????????? ??????? **I**P-????????), ??? ?????

????????? ??????????? ?????? ????????? **I**P-??????.

?????? ??????????? ???????. ?? ????? ????? ??????? ???? **I**P-????? (???????? '**ME**') ? ???????? ?????? ?? ?????. ?????? ???? ?? ????????? ???????? '**ME**' ?? ????? ??????? ? ????, ????????? ????-????????? (???????? Solar Designer's Excellent Scanlogd) ??????? ??? **I**P-????? ??? ???????? ?????????????. ???? ?? ???? ?? ??????? ???????? '**ME**', Nmap ???????? ??? ?? ????????? ???????. ????? ?? ?????? ???????

????? ?????? ?????? ?? **I**P-???????. ???????, ??? ?????, ???????? ???? ? ???????? ??????, ?????? ??????? ??????????? ? ?????????????, ? ????????? ?????? ?? ?????? "????????" ?????????? ???? **S**YN-????????. ??? ????? ????? ?????????????? ??????????? ?????? ?????, ?????? ??? ???? ?????? ????? ?? ???????????, ?? ??????????????? ????????? ?????? ???????? ???.

????? ????????, ??? ????????? ????-???????? ???????? ?????? ?????, ??????????????? ??????? ??????????. ??????? ?????? ???? ????? ???????? ????????? ?? ??????????? ??????. ??? ???????? ????? ????????? ???? ? ??? ??????, ???? ?? ??????? ? ???????? ??????? ????? ????? ????? ??? 'localhost'. ??????? ????????? ??????????? ??? ?????.

?????? ????? ????? ??????????????? ? ????? ??????? ??????????, ? ????? ??? ??????????? ??????????? ??????. ???? ?? ??????? ????? ?????? ??????, ??? ???????? ??????? ??????????? ? ??????? ??? ????? ??????. ????????? ?????????? ????? ??????????????? ???? ?????? (?? ??? ????? ?? ?? ??????????), ? ? ???? ?????? ??????????????? ?????? ?????? ?? ???? ??? ??????????
??????????.

-S <IP-адрес> (set **S**ource) - ???? Nmap ?? ???? ??????????????? ?????????? **I**P-????? ?????? ????? (??? ?? ???????? ??????????????? ????????), ??? ?????????? ??????????????? ??????? **I**P-?????, ????????? ??? ? ???????? ???????? ?????? ????? (.?.? ????? ??????????, ??????? ?? ?????? ???????????). ?????? ?????????? ?????? ????? - ??? ???????? ????????? ???????????

???????? ????? ???-?? ??????. ? ???? ?????? ?? ?? ??????? ???????? ????????, ?????? ?? ??????? ??????????? ????? ???????? ???????? ??????????? ? ?????????? ???? ?????. ??? ????? ????????? ? **'-S'**????????? ??????????? ????? **'-e'**.

-e <интерфейс> (**i**nterface) - ????????? Nmap, ????? ????????? ????? ??????????????? ??? ??????/???????? ???????. ??? ?????????? ??????????? ? ???????? ???????? ?????. Nmap ?????? ??? ?????????? ????????, ????? ?????? ??? ??????????????? ????????, ???? ?? ?????-???? ???????? ?? ?? ???? ????? ???????.

-g <номер_порта> - ????????? ????? ????? ?? ????? ??????????, ??????? ????? ???????????????? Nmap ??? ??????????????? ???????????. ?????? ????????? ? ???????? ??????? ????????? ???????? ??????? DNS (???? 53) ? FTP-DATA (???? 20) ? ??????????? ??? ????? ? ??????????? ??????????. ???? ?????? ???????? ??????? "?????" ? ??????????????? ??????????, ??????? ??????????

?????? ?? ????? ?????????? ?????? ??? ?????? ????? 53-? ??? 20-? ????.

??? ??????????? UDP-?????? Nmap ??????? ??????? 53-? ????, ? ????? 20-?. ??? TCP-?????? - ????????. ???????, ??? ??? ?????? ?? ???? "???? ?????????" ? ??????? ? ??????? ?? ?????? ????????. ????????, ?? ?? ??????? ?????????? ???????? ????????? ISN. ?????? ? ??? Nmap ?????????????? ?????? ????? ????? ??? ???? ????, ???? ???? ?? ??????????? ????? ? **'-g'**.

--data_length <число> - ?????? Nmap ???????? ?????, ?????????? ????? ????????. ????? ???????, TCP-????? ????? ????? 40 ???, ? ICMP "echo requests" - 28. ??? ????? ????????? ? ??????????? ??????? (????? ??????? ??? ??????????? ??) ????????? ????? ??????? ????. ????????? ??????????.

-n ??????? ?? ???????????????? ?????? ??????????? ?????? ? DNS-?????. ??????????? ??????? ??????????.

-R ?????? ?????????????? ?????? ??????????? ?????? ? DNS-?????.

-r ?? ??????????? ?????? ??????????? ?????? ????????? ???????.

-ttl <значение> ?????????? ? ???? TTL ??????????? ??????? IPv4 ???????? ????????.

--randomize_hosts - ????????? Nmap ?? ??????????? ???????? ??????????? ?????? ?????? ?? 2048 ????? ????? ?????????????? ?? ???????????. ??? ????? ?????? ??????????? ????? ???????? ??? ???????? ?????? ???????? ??????????, ???????? ??? ?? ??????????? ?? ???????? ? ?????? ????????? ??????, ??????????????? ????? ????????? ??????????.

-M <максимум_сокетов> (**M**ax sockets) - ??????????????? ??????????? ?????????? ??????, ??????????? ??????????? ? ?????? TCP connect() ???????????. ????????? ???????? ???????? ??????? ????????? ??????? ???????????, ?? ???????????? "?????" ??????????? ?????. ??? ????????? ???? ????? ????? ??????????? ????? '**-sS**', ??? ??? SYN-??????????? ??????? ????? "???????????" ?????????????

?????????.

--packet_trace ????????? ??? ??????????? ? ??????????? ?????? ? ??????? TCPDump.

--datadir [каталог] ??? ??????? Nmap ????????? ?????? ?? ?????? nmap-services, nmap-protocols, nmap-rpc, ? nmap-os-fingerprints. ?? ?????????????? Nmap ????? ?? ????????? --nmapdir. ????? ??????????? ????????? ????????? NMAPDIR, ????? ???? --/nmap, ? ????? ???? ????????? /usr/share/nmap . ? ????? Nmap ??? ?? ? ??????? ????????. ???? ?????? ????? ???? ??????

????????? ???? ??????.

????? ????????? ????????? ??????????

?????? Nmap ??????????? ??????????? ????????? ????????? ? ??????????? ? ??????????????? ??????????? ????. ????????? ??????????????, ??-??????, ??? ????????? ??????????? ???????? ???????????????, ? ??-??????, ??? ????????? ??????????? ????????? ??????. ???? ??? ?? ????????? ??????????????? ????????? ????????? ??????????, ?? ?????? ????????? ?? ??????????????,
????????? ??? ?????.

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> (**T**iming options) - ??? ????? ??????????????? ???????? ????? ??????????. ????????? ????? ??????????? ? ???????? ????????. ????? **Paranoid** ??????????? ? ??????, ????? ????? ?????? ??????????? ??????????????? ????-????????. ? ???? ?????? ??????????? ???????? ????? ????????. ??????????? ??????????? ??

~~??????????, ????? ???? Nmap ??????? ??????????? ??????????????, ? ??????????? ?? ??????? ??? 5 ???? ???? ??????? ??????.~~

????? **Sneaky** ????? ?? ????? Paranoid. ??????? ??????????? ? ???, ??? ???????? ????? ???????? ???? ??????? ??????????? 15 ??????.

????? **Polite** ??????????? ? ??????, ????? ??????????? ?????????????? ???????? ?? ???? ? ???????? ??????????? "??????" ??????????? ?????. ? ???? ?????? ????? ???????? ?????????????? ? ?????????? ??????? 0,4 ???????.

????? **Normal** ??????????? Nmap ?? ????????. ? ???? ?????? ??????????? ??????????? ? ??????????? ???????? ????????, ? ?? ??????????? ??? ??????????? ???? ? ?????????????? ??????.

? ?????? **Aggressive** ?????????????? ??????????? ?? ??????????? ?????? ?????, ?????? 5 ???????, ?, ????? ????, ????? ???????? ?????? ?? ?????? ?? ???????? 1,25 ???????.

????? **Insane** ??????????? ?????? ??? ??????????? ????? ??????? ?????. ????? ??????????? ?????? ????? ????????? 75 ??????, ? ???????? ?????? ?? ?????? - 0,3 ???????.

??????? ?????? ???????? ?????????????? ????, ? ?? ?????? ??????? ??? ?????? ??????? ???????? ??????. ???, ????? **'-T0'** ???????? ????? **Paranoid**. ? **'-T5'** - **Insane**. ???????? ?????????????? ???????, ? ??????? ??? ???? ??????????? ????. ???????, ??? ????? **'-T'** ??????????? ???????? Nmap ?? ??????? ??????, ? ?? ?????? ?????????????? ? ???????, ??????????? ???? (??? ??????????? ???????????? ????????).

--host_timeout <миллисекунд> - ??????????? ?????, ???????? Nmap ?? ??????? ??????????? ?????? ?????, ?????? ??? ?? ???????? ? ?????????? IP-??????. ?? ???????? ???? ???????? ??????????, ?.?. Nmap ?? ????????? ? ?????????? ?????? ?? ????????? ??????????? ????????.

--max_rtt_timeout <миллисекунд> (maximal round-trip time **timeout**) - ??????????? ??????? ??????? ?????????? ?????????, ? ??????? ???????? Nmap ??????? ????? ?? ????????? ??????, ?????? ??? ????????? ?????? ???? ??????? ?????. ?? ????????? ??? ???????? ??????????? ?????? 5000 ??????????.

--min_rtt_timeout <миллисекунд> - ???? ??????????? ???? ????????? ???????? ?? ???????? ??????, Nmap ????? ?? ???????? ????????, ????????? ??? ????? ????? ????? ???????. ??? ???????? ???????????, ?? ????? ???????? ? ?????? ??????? ? ????????, ?????????? ???????? ?????, ??? ??????. ??? ????? ??????????? ?????? ??????? ??????? ???????? ??????, ?.?. Nmap ? ????? ?????? ????? ????? ? ??????? ?????????? ???? ??????? ?? ???????? ?? ????, ?????? ????? ?? ???.

--initial_rtt_timeout <миллисекунд> - ??????????? ?????, ???????? ?? ????????? ????. ??? ????? ??????????? ? ???????? ??? ??????????? ??????, ?????????? ??????????, ???????? ? ?????? **'-P0'**. ?????? Nmap ??????????? ???????? ??????????? ???????? ????? ????????. ???????? ?? ????????? ????????? 6000 ??????????.

--max_parallelism <количество> - ??????????? ??????????? ?????????? ??????????? ???????? ???????????, ??????????? Nmap. ????????? ????? ???????? ?????? 1 ????????, ??? Nmap ??????? ?? ????? ??????????? ????? ?????? ????? ? ???? ?????? ???????.

--min_parallelism <количество> - ??????????? ??????????? ?????????? ??????????? ???????? ???????????, ??????????? Nmap. ??????????? ???????? ??????????? ??????? ????? ????????.

--scan_delay <миллисекунд> - ??????????? ?????????? ????? ???????? ????? ???????. ??? ????? ????? ??????????? ??? ???????? ???????? ?? ???? ? ?????????? ??????????? ??????????? ???????????.

??????? ??????? ???????? ?????

???, ??? ?? ???????? ?????? ??? ?? ??????????, Nmap ??????????? ??? ????? ??? ?? ???????? ????? (?.?. ?????, ??????????? ???????????). ??????????? ????? ?????? ??????????? ???? - ??????? ??? ??? ??? ????? ? ????????? ?????? ????? ???????? ????? ? ??????????. ???? ?? ?????? ??????????????? ??????? IP-???????, ??? ??????????? ??????? ??????? **'/<mask>'** ("??????") ????? ????? ??? IP-?????? ??????????? ?????. ????? ????? ????????? ????????? ????????:

'/0' - ??????????? ???? ????????;

'/16' - ??????????? ?????? ?????? B;

'/24' - ??????????? ?????? ?????? ?;

'/32' - ??????????? ?????? ????????? ????.

Nmap ????????? ????? ????? ??????? ??????? IP-??????, ???????? ?????? ? ????????? ??? ??????? ?? ????????. ????????, ??????????? ??????????????? ??????? ?????? B ? ??????? 128.210.*.*. ?????? ??? ???? ????? ????? ?? ???????? ????????:

128.210.*.*

128.210.0-255.0-255

128.210.1-50,51-255.1,2,3,4,5-255

128.210.0.0/16

??? ??? ????? ???????????. ???????, ??? ???? ?? ??????????? "????????" ("*"), ?? ? ??????????? ???????? ??? ??????????? ???????? ?? ???????? "????? ??????" ???? ??????????. ???????? ??? ???? ??????. ???? ?? ??????? ? ???????? ???????? IP-?????? ?????? '*.*.5,6-7', Nmap ??????????? ??? IP-??????, ?????????????? ?? 5,6 ???? 5,7. ????? ???????? ??????? ?????? ????????
Nmap ????????? ????.

???????

??????? ????????? ??????? ???????????? Nmap ? ????????????? ??????? ??????? ????????? ? ????????? ????????? ? ????????? ?????.

nmap -v target.example.com

??????????? ??? ???????????????? TCP-????? ?? ????? target.example.com. ????? '**-v**' ???????? ????????? ?????? ?????????? ?????? ? ???? ???????? ???????????.

nmap -sS -O target.example.com/24

????????? SYN-??????????? ???? 255 ????? ? ???????? ?????? C, ????? ?? ??????? ???????? target.example.com. ????? ????, ????????????? ?????????? ?? ??????? ?? ??????????? ??????. ??? ????? ??? ????????? ?????? root.

nmap -sX -p 22,53,110,143,4564 128.210.*.1-127

??????????? Xmas-??????????? ?????? ???????? ??????? (0-127) ?????? ?? 255 ???????? ?????? B ????????? ??????????? 128.210.*.*. ?? ???? ?????? ?????????? ?????????? sshd (22 ????), DNS (53), pop3d (110), imapd (143) ? ????????? ????? 4564. ???????? ????????, ??? Xmas-??????????? ?? ????? ???????? ? ?? Windows, CISCO, IRIX, HP/UX ? BSDI.

nmap -v --randomize_hosts -p80 *.*.2.3-5

Nmap ????? ?????? ??? ??????, IP-???? ??????? ??????????? ?? .2.3, .2.4 ? .2.5. ???? ??? ?????? root, ?? ????? ?????? ???????????? ????? ??????????? ??????, ????? ????? '**-sS**'. ?? ??????? ????? ?????????? ?????, ?????? ??????? ?????????? ?? 127. ??????? ?? ?????????? ?????? ?????? ????????? ??????? '127-222'. ??????????? ???????????!

host -l company.com |cut '-d' -f 4| ./nmap -v -iL

????????????? ??????? DNS ???? ? ????? ????? ? ?????? company.com, ??????? ????? ? Nmap ?? ??????. ??? ???????? ??????? ??? GNU/Linux. ??? ?????? ?? ??? ????? ????????? ????????? ?????.

????????? ??????

???? ?? ?????????? ????-???? ????????, ???????? ? ???????? ????? ????????, ??? ????? ???? ? ????, ????????? ? ?????? ??????? - ?????????? ???????? ??? ??? ??????????. ?? ????????? ????? ?????????? ??? ????????? ??, ????? ????????? ???? ????? Nmap. ????????? ?????? ??? ??????????????? ????????? ? URL, ??? ??? ????????? ????? ????????.

??????

??????? ??????:

fyodor [at] insecure [dot] org (fyodor [at] insecure [dot] org)

http://www.insecure.org/ [5]

??????? ??????:

alex [at] cherepovets-city [dot] ru (alex [at] cherepovets-city [dot] ru)

http://www.cherepovets-city.ru/insecure [6]

????????????????

???????? ?????? Nmap ? RuNmap ?? ?????? ???????? ?? ???????

http://www.cherepovets-city.ru/insecure [6]

http://www.insecure.org/ [5]

nmap (??????? ??????) (c) 1997-2003 Fyodor

runmap (??????? ??????) (c) 1999-2003 ??????? ??????

????????? **libcap** ?????????????? ???????? ? Nmap. ???????? ????????? ?????: Van Jacobson, Craig Leres ? Steven McCanne, ??????????? ??????????? Lawrence Berkley ????????????? ??????????, ??????, ??????????. ??????, ??????????????? ? Nmap, ????? ???? ????????????. ??????? ??? ????????? ????? ??????? ?? ?????.ftp://ftp.ee.lbl.gov/libcap.tar.gz. [7]

??? ???????? ??????? ????????? ????????? ??????????. ?? ?????? ??????? ???????????? ?/??? ??????????? ?? ? ??????????? ? ??????????? GNU General Public License, ???????????? Free Software Foundation, ?????? 2. ???? ??? ?? ?????????? ?????? ????????, ?? (Insecure.Org) ?????? ??????????? ???? ??????????.

???????? ??????????? ??? ???????????? ?????-???? ????????. ??????? ? ?????????? ?????????? ?? ??????:

alex [at] cherepovets-city [dot] ru (alex [at] cherepovets-city [dot] ru)

Источник (получено *2026-06-02 20:56*):
http://muff.kiev.ua/content/nmap-network-mapper-utilita-dlya-skanirovaniya-i-issledovaniya-bezopasnosti-seti

Ссылки:
[1] http://www.cherepovets-city.ru/insecure/runmap/runmap-versionscan.htm
[2] http://www.cherepovets-city.ru/insecure/runmap/runmap-idlescan.htm
[3] http://nmap6.sourceforge.net/
[4] http://www.insecure.org/nmap/nmap.dtd
[5] http://www.insecure.org/
[6] http://www.cherepovets-city.ru/insecure
[7] ftp://ftp.ee.lbl.gov/libcap.tar.gz.