



????????

??????????

????????

[illegible]

?????

[illegible]



[illegible]

?????? ? 1985 ??? (??? ?? ??????? RFC). Nmap ??????? ?? "???" ?? ??????????? ????? ? "?????????" <http://nmap.org>

????? URL ??????: имя пользователя:пароль@сервер:порт. ???? ?????? ???? ?????? ??????????, ??????? ???? ?? ??????

~~~~~ ? ~~~~~

המחברות נבחרו על ידי הוועדה המייעצת של **Nmap** (הוועדה המייעצת של **Nmap** היא הוועדה המייעצת של **Nmap**).

התחנות החדשות יבנו ב-2017, 2018 ו-2019. הרכיבים החדשים יבנו ב-2017, 2018 ו-2019. הרכיבים החדשים יבנו ב-2017, 2018 ו-2019.

**-PS (Ping SYN)** - *????, ??? ???? ping-????, ??? ???? ACK-???? TCP "ping" ?????? SYN-????, ????? ???? ???? ? ???? RST-???? (??? - SYN|ACK)*

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

[illegible]

-PP - mmmmmmm mmm ICMP "timestamp request (code 13)" mmm mmmmmmm mmmmm mmmmm

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

**-PB (Ping Both) -** ping-????? ?????. ?????? ?????????? ?????? ACK ? ICMP

האם ניתן להשתמש ב-`map-as-fingerprinting` כדי להבדיל בין שני קבצי `map` שונים? [הקישור](#)

[illegible]

**-A** ??? ???? ???? ???? additional advanced aggressive, ? ???? ???? -O, -sV, -T4 ? -v.

???????? UDP ?? ???? ?? ?????????, ????????? ???? <http://hmap6.sourceforge.net/> [3].

\*idmnd מזהה את כתובת ה-IP של המכשיר, ו-**st** מזהה את שם המכשיר. Nmap מזהה את כתובת ה-IP של המכשיר, ו-**st** מזהה את שם המכשיר.

-f (use fragmentation) -? ???? ????????????????????? SYN, FIN, Xmas ??? NULL-???????????????????? IP-???????????????????? TCP-???????????????????? "???" ?? "?????" ?? IP-???????????????????? TCP-????

[illegible]

**-V** (verbose output) - תוצאות מפורטות יותר של הפעולה. לדוגמה, במקום "Nmap" יציג את כל הפרטים הרלוונטיים.

```
-h (show help) - ?????? ?????? ?? ?????????? Nmap? ??????? ???? ? ?????? ?? ??????, ?? ?????? ??? ???????
```

```
-oN <имя_файла> (output Normal) - ?????????? ?????????? ?????????? ? ?????????? ??? ? ?????? ??? ?????????? ?????
```

????????? Nmap ? ?????? XML ?????? ?????: <http://www.insecure.org/hmap/hmap.dtd> [4]

XML: `????????????????????`

-oA <базовое\_имя\_файла> (output All) - ?????? ?????? ? ?? ?????? ?????? (??????, ??? ? XML). ?? ?????? ?????? ?? ?? ??, ? ?????? ??? ?????? ?????? base.nmap, base.gnmap ? base.xml







~~~~~ Nmap 2 ~~~~~

```
nmap -v target.example.com
```

```

##### 77 #####TCP-#### 77 #### target.example.com. ##### '-v' ##### 

```

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

[illegible]

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

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

[illegible]

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

החברה מפרסמת את כל המידע הרלוונטי לגביה באתר האינטרנט שלה www.gnil.co.il ובאתר האינטרנט של נאמן www.naman.com וכן באתר האינטרנט של רשות המיסים www.dns.gov.il.

[illegible]

~~~~~

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

~~~~~

Page 6 of 7



Page 7 of 7