Kako pomoću nmap-a pronaći crva Conficker

Mrežni crv poznat pod nazivima **Conficker** ili **Downadup** ostat će zabilježen kao jedan od najznačajnijih događaja u IT području. Počeo se širiti krajem prošle godine, da bi na kraju zarazio preko 10 miliona **Windows** računala. Isprva je koristio grešku u **RPC** funkciji da bi se bez autentikacije ulogirao na računala koja nisu imala instaliranu zakrpu **MS08-067**.

Nakon što bi bio uklonjen, opet bi se vratio na isto računalo iako je spomenuta zakrpa već instalirana, što ukazuje da je koristio i druge ranjivosti. Osvajao bi i računala koja nemaju instaliran **SP3** za **XP**. Kao jednu od metoda širenja istraživači su naveli i pogađanje trivijalnih zaporki.

Najnovija inačica sigurnosnog alata nmap u stanju je prepoznati računala zaražena tim virusom. Naredbi treba dati slijedeće parametre:

```
nmap -PN -T4 -p139,445 -n -v --script=smb-check-vulns --script-
args safe=1 [targetnetworks]
```

Umjesto targetnetworks stavite IP adresu vaše mreže, na pr 192.168.10.0/24. Ako se nakon IP adrese skeniranog računala pojavi poruka:

```
Conficker: Likely INFECTED
```

požurite do tog računala s CD-om na kojem je program za uklanjanje tog crva. USB stick koristite samo ako se može zaključati, da se na njega ne može pisati, jer se ovaj crv voli nastaniti na USB memorije.

Da bi to radilo, potrebna je verzija **nmapa 4.85 BETA6**. Evo linka s kojeg možete skinuti nmap za Windowse:

http://nmap.ucsd.edu/nmap/dist/nmap-4.85BETA6-setup.exe

Požurite, jer najnovija inačica Downadup-C prijeti da će se prvog aprila spojiti u netbot i prepustiti zaražena računala na milost i nemilost napadačima, koji ih onda mogu koristiti na pr. za slanje spama ili masovni napad na određene sajtove.

uto, 2009-03-31 15:17 - Aco Dmitrović**Vijesti:** Sigurnost [1]
Kategorije: Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Source URL: https://sysportal.carnet.hr./node/549

Links
[1] https://sysportal.carnet.hr./taxonomy/term/13
[2] https://sysportal.carnet.hr./taxonomy/term/30

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr