Codul Hackerului - Codul onoarei

Hackerii sînt utilizatori de computere, care pătrund în sisteme informatice protejate. Cu cît un **hacker** este mai bun, el poate pătrunde în programe foarte securizate, cum ar fi cele de la Pentagon, CIA, FBI, NATO sau NASA.

Crackerii sînt . Termenul a apărut în SUA la începutul anilor **'80**, în replică la folosirea abuzivă de către mass-media a termenului de **hacker**, cu intenţia de a delimita cele două noţiuni diferite.

Hackerii forţează un sistem doar pentru palmares. El nu foloseşte intrarea în reţeaua securizată pentru interese financiare proprii, pentru sustragerea de documente secrete şi pentru publicarea lor. Etica **hackerilor** se bazează pe două principii **:**

1) Datoria morală de a răspîndi cunoştinţe, prin distribuirea de **"Free software"** (programe gratuite), uşurînd astfel accesul la informaţie.

2) Condamnarea vandalismului şi a atentatelor la confidenţialitate.

Există **crackeri** cu un statut legal – oficial. **"Tiger teams-urile"** sînt echipe de crackeri profesionişti care testează sistemele de securitate de la distanţă, folosin reţele şi canale de tip **"x.com", "x.org",** sau **"x.gov"**, considerate impenetrabile. Dacă nu ar fi ţinute în mare secret, s-ar putea admira cu siguranţă, în programele acestor echipe de "Tigri", cele mai ingenioase artificii software, care s-au imaginat vreodată. Se pare că aceşti crackeri profesionişti provin din rîndul hackerilor care şi-au înfrînat dorinţa de a comite infracţiuni spărgînd sisteme, dorinţă care în noua ipostază şi-o pot satisface pe cale legală. Aceşti hackeri îşi iau angajamentul că nu vor divulga niciodată secretele reţelelor, dar nu trebuie să ne bazăm pe asta referitor la siguranţa vieţii lor după aceea. Pentru a ajunge **hacker** sau **cracker** trebuie să cunoşti extrem de bine informatică şi să-ţi dedici mult timp acestei ocupaţii.

Codul hackerului

1. **Nu ataca** niciodată, cu răutate, un sistem. Nu şterge şi nu modifica fişierele. Nu provoca prăbuşirea sau încetinirea unui sistem. Excepţie fac procedurile de accesare şi de ascundere a urmelor.
2. **Nu furniza** niciodată şi nimănui numele tău real, numărul de telefon sau adresa. Mulţi dintre hackerii renumiţi, după ce au fost prinşi, i-au denunţat pe toţi cei pe care îi cunoşteau, pentru a li se mai îndulci pedepsele.
3. **Fereşte-te** de computerele guvernului. O să descoperi foarte repede că încercarea de a pătrunde o instalaţie **MilTac** se află la graniţa imposibilului şi s-ar putea să fii arestat înainte de a spune "peşte". **"Fratele cel mare"** are o

grămadă de resurse disponibile şi tot timpul de care are nevoie, pentru a te vîna. Guvernul poate petrece ani întregi pentru a te urmări. Aşa că cel mai bine nu te arunca cu capul înainte într-o asemenea treabă. În cele din urmă îţi va părea rău.

4. **Sub nici o formă** nu trebuie să foloseşti codurile de acasă. Este cea mai nesăbuită operaţiune. Folosirea abuzivă a codurilor a dus la prăbuşirea multor oameni, care la început păreau foarte inteligenţi şi promiteau mult. Cele mai multe coduride tip **PBX/950/800s (Private Branch Exchange)** posedă **ANI (Automatic Number Identification – Număr automat de identificare)**. În cazul în care le foloseşti, vei fi prins fără nici o îndoială. Şi mai grav este să foloseşti o cartelă de apelare **"And calling cards are an even worse idea"**
5. **Nu-i** incrimina pe alţii, indiferent de cît de mult îi urăşti. Generarea de dispute între oameni, este un lucru îngrozitor şi de cele mai multe ori nu rezolvă problemele.
6. **Fii atent** la ce foloseşti. Nu lansa coduri în reţele deschise. Vor dispărea în cîteva zile şi îţi vei pierde noua comoară. Trebuie să ştii că folosirea unor numere de cărţi de credit este considerată o infracţiune gravă.
7. **Dacă**, din anumite motive, chiar trebuie să foloseşti unele coduri, foloseşte-le pe cele proprii. Nu folosi coduri găsite pe INTERNET, pentru că sînt şanse foarte mari ca ele să fie puse special şi să fie monitorizate pentru a-i prinde pe fraieri.
8. **Eşti liber** să pui cît mai multe întrebări, dar fă-o în aşa fel încît cel care îţi va răspunde să nu îşi de-a seama la ce îţi folosesc lămuririle respective. Oamenii nu sînt prea săritori cînd e vorba să împărtăşească şi altora cunoştinţe rare. Este necesar să înveţi din propria experienţă.
9. **Fii puţin** paranoic. Foloseşte cît mai multe programe pentru a-ţi încripta fişierele, păstrează-ţi materialele scrise în locuri secrete.
10. **Dacă** eşti prins, nu spune nimic autorităţilor. Refuză să vorbeşti şi cere să fii asistat de un avocat.
11. **Dacă** Poliţia îţi bate la uşă şi îţi prezintă un mandat de percheziţie, cercetează-l cu atenţie, pentru că este dreptul tău. Află ce au voie şi ce nu au voie să facă pe baza acelui mandat, iar dacă au voie să facă ceva, împiedică-i.
12. **Dacă** este posibil nu folosi propria linie telefonică, în timp ce penetrezi anumite sisteme. Piratează linia telefonică a vecinului sau foloseşte un telefon clonat sau orice altceva. Dacă stai prea mult timp în reţea, sînt mari şanse ca într-o zi să fii prins pe baza ANI. Să nu fii niciodată prea sigur că eşti invincibil, pentru că, indiferent dacă va dura ceva vreme, poţi fi detectat.
13. **Fă** tot posibilul pentru ca operaţiunile de urmărire să devină foarte complicate şi costisitaore, pentru cei care se ocupă cu acest lucru. Pentru asta trebuie să foloseşti serviciile mai multor companii telefonice, să nu stai în reţea prea mult şi să alternezi orele şi datele.
14. **Nu** păstra notiţe scrise. Păstrează toate informaţiile în computer, încriptate cu programe cît mai bune. Notiţele scrise pot fi folosite la tribunal de către acuzatori.

vornicescu_angelica@yahoo.com