Legal information

This book and the software fragments included present techniques thanks to which both IT environment can be protected by its user as well as other systems can be attacked.

That's why we would like to draw your attention to the fact that this handbook, live training videos and software included can be used only to protect your IT environment. Conducting an attack on other IT system without the permission of its respective owner is penalized by the federal Computer Fraud and Abuse Act (if you live outside the United States, please refer to your local law).

"(a) Whoever--

- having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
- intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

  information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency

on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

information from any department or agency of the United States; or

information from any protected computer if the conduct involved an interstate or foreign communication;

- intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
- knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

- knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(a)trafficking affects interstate or foreign commerce; or such computer is used by or for the Government of the United States; with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal

entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section. (b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section. (c) The punishment for an offense under subsection (a) or (b) of this section is--

a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

the offense was committed for purposes of commercial advantage or private financial gain;

the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

the value of the information obtained exceeds $5,000;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if--

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and [former paragraph (4) stricken effective Oct. 11, 1996].

The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General."

While being an administrator and using the tools described in the handbook in order to protect your own IT environment, or gettin to know the hacking techniques presented, you always have to be sure that your actions are fully legal. The points below should be treated as examples, not as a full and complete list.

- The handbook, live training videos and the training operating system should be kept in a place unavailable for any third person.
- If you discover any new problem or lack of security in the tested environment, you have to inform the administrator.
- You have to be really careful during the testing, any third person cannot be harmed by your actions. If you accidentally enter any other IT system during your tests, you have to cease them and inform the administrator.
- All tests should have a complete documentation: the test, its aim, plan, people taking part in it.
- The results of the tests should be kept away from any third person.
- Tests conducted for any third person should be carried out only after obtaining a written permission.
- Only testing environment should be used to conduct the tests.

Additional legal info can be found in the full text of the federal Computer Fraud and Abuse Act.