

KAIP TAPTI HAKERIU: JUOKAIS IR RIMTAI

Of.lt 0x06





Control Panel

Settings Help

„hakeris“ yra:

- Kažkas gaminantis baldus kirviu?
- Kietas programmeris?
- Kažkokio vieno dalyko ekspertas (kernel hacker)?
- Kažkas mėgstantis intelektualius išbandymus?
- Žmogus randantis nestandartinius sprendimus?
- Informacijos saugumo ekspertas?
- Asmuo vykdantis nusikaltimus naudodamas IT?

Tikslaus apibrėžimo gal ir nėra, bet manau visi „viduje“ suprantame apie ką eina kalba

OK :)

Hacker cat



Lovez hacking



I DON'T GET IT. IT'S JUST A GUY STARING AT A COMPUTER FOR TWENTY SECONDS.

MY... GOD...

THAT'S A TIME-LAPSE VIDEO OF TWO WEEKS.



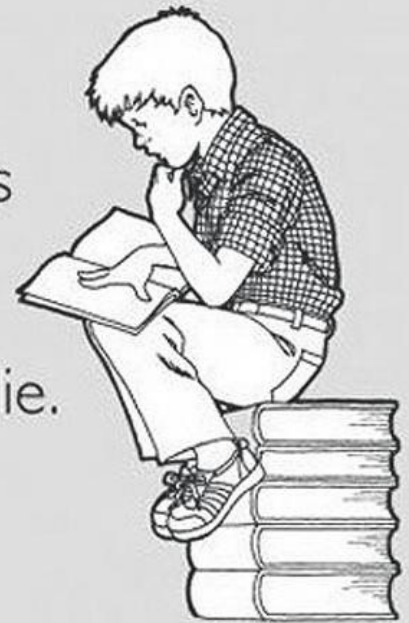
There is a reason movies never portray hacking realistically.



MOTYVACIJA

- „Hakeriu“ tampama:
 - Geriau pradėti anksčiau, bet tai ne auksinė taisyklė
 - Lytis, išsilavinimas, akių spalva didelės įtakos neturi
- Reikalavimai:
 - Tai ką ketini daryti turi būti natūraliai įdomu
 - Iš dalies pamiršti tai ko mokė mokykloje, universitete ar „hakingo kursuose“ ir žinias pasiimti PAČIAM
 - „Hakeriškas mąstymas / logika“
 - DAUG laiko, noro ir energijos
 - ...

When work feels overwhelming, remember that you're going to die.



- Forensics
- Hardware hacking
- Reverse engineering
- Vulnerability research
- Exploit development
- Cryptography
- Social engineering
- WEB hacking**
- Malware analysis
- Software development
- Log Off Thurrott...
- Shut Down...

- Server security
- Network security
- Database security
- Application security**
- Cryptography
- OS Security
- etc etc etc...

- SQL injection
- Cross site scripting**
- Code execution
- Buffer overflows
- Logic errors
- etc etc etc

A problem has been detected and windows has been shut down to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this stop error screen, restart your computer, If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any new hardware or software. Disable BIOS memory options such as cache or parity. If you need to use safe Mode to remove or disable components, your computer, press F8 to select Advanced Boot Options, and then select Safe Mode.

NUO KO PRADĚTI?!?

*** STOP: 0x000000D1 (0x00000000)

*** gv3.sys -

Beginning dump of physical memory
Physical memory dump complete
Contact your system administrator for assistance.

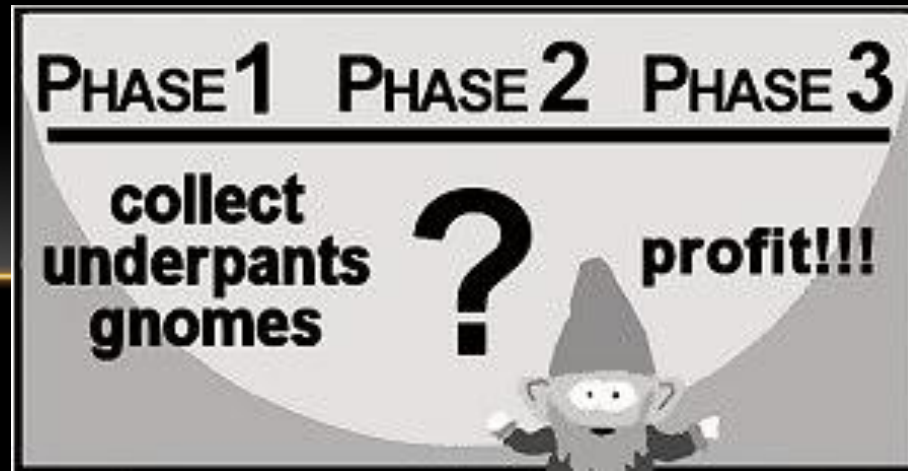


Norint kažką nuveikti reikia žinoti ką ir kaip galima nuveikti

Reikalingos žinios:

1. Informacija yra Internete
2. Ją reikia surasti
3. Ją reikia suprasti
4. Ją reikia pritaikyti

P.S. Norint imtis sudėtingų dalykų reikia suvokti paprastus



Pasiūlymas pradžiai: WEB saugumas

- Pažeidžiamumų klasės yra gerai žinomos ir gerai dokumentuotos
- Nesudėtinga eksperimentuoti
- Tereikia naršyklės :)

Naudingi šaltiniai:

- OWASP testing guide:
https://www.owasp.org/index.php/Category:OWASP_Testing_Project
- OWASP Broken WebApp security project:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project#tab=Main
- Dar ~20 panašių projektų: <http://punter-infosec.com/tag/vulnerable-web-applications>

METASPLOITABLE

Tinka išbandyti metasploit funkcionalumą

- Ubuntu 8.04
- Tomcat 5.5
- Distcc, tikiwiki ir pasenęs MySQL

<http://blog.metasploit.com/2010/05/introducing-metasploitable.html>

Youtube:

http://www.youtube.com/results?search_query=metasploitable&aq=f



NAUDINGI RESURSAI

- Išmanote kompiuterių architektūrą ir norite „ką nors pareversinti“? <http://tuts4you.com/download.php>
- Papildomai kažko naudingo (pvz. demonstracijų) galima paieškoti ir www.securitytube.net
- Norite turėti įrankius „po ranka“? <http://www.backtrack-linux.org/>
- Nepamirškime ir „wargame'ų“ <http://www.overthewire.org/wargames/>
-

Tolimesni patarimai

- Susiraskite jums tinkančių ir patinkančių informacijos šaltinių.
- Nepamirškite ir knygų – informacija ten gal ir ne naujausia, bet gerai sistematizuota
- Nedarykite klaidų – nepažeiskite įstatymų, laikykitės atokiau nuo kreditinių kortelių, realių svetainių laužimo, DDoS ir kenksmingos programinės įrangos kūrimo/platinimo. Tai nėra „kieta“ bei neprideda jums taškų, tačiau gali nuvesti į vietą kur jums galimai pakeis orientaciją.

