БДЗ

Большое домашнее задание

WHOAMI

- Igor Ivanov

- Background: *nix/Win Sysadmin / Development

- ~3y Infosec Engineer

Security CTFs, Pentests, various cool stuff

Skills needed

- shell scripting (bash)

- python scripting

- SSH (keys, options, forwarding)

- hash identification

- some web (LFI, SQLi, RCE…)

- patience)

- privilege escalation

- persistence

- fuzzing

- gdb debugging

- version control systems

- curl, nc, awk, sed etc.

- more patience ;)

About the box

- Import ovf image into VirtualBox

- Check port forwarding

- Start with http://127.0.0.1:8080

- SSH available at 127.0.0.1:2222

- 9 tasks

- no kernel vulnerabilities

- get to root)

I'm stuck

- What you can do?

- What you got?

- How you can apply this knowledge?

- Try harder

- Ask:

  - Google group (https://groups.google.com/forum/#!forum/mifibox)

  - telegram: @lctrcl (personal)

  - email: evanowe@gmail.com

  - No spoilers for others

Documentation

- No Word please

- Ideally: writeup in Markdown

- Tools: sublime text, keepnote, cherrytree, LaTEX

Useful info

- Basic linux privilege escalation (https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/)

- CTF Field guide (https://trailofbits.github.io/ctf/)

Questions

- get started: https://github.com/lctrcl/mifibox