

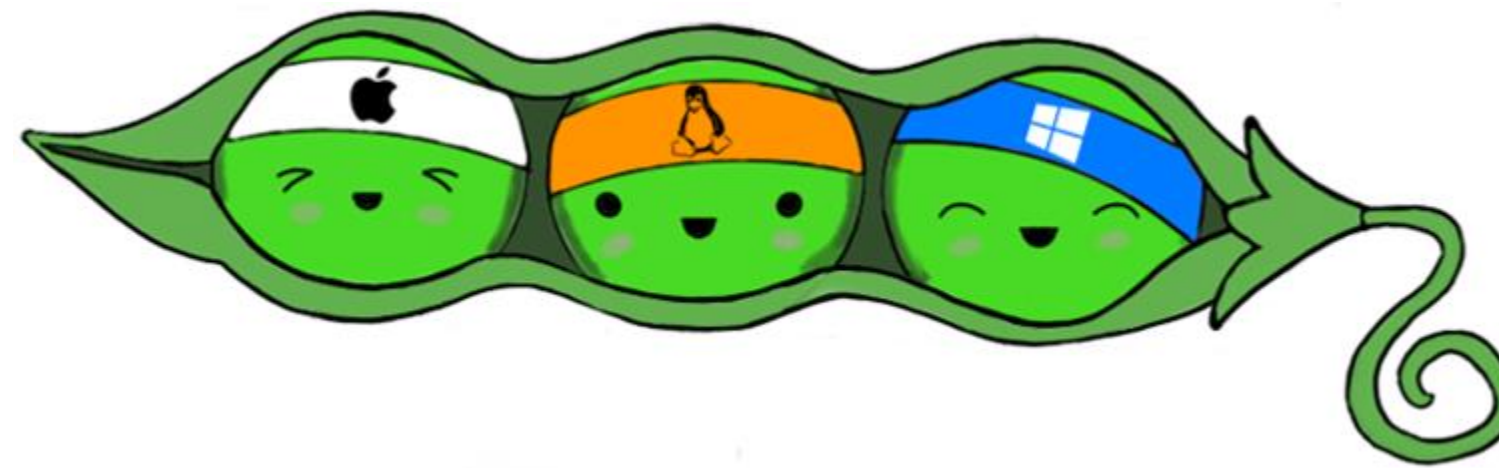
Privilege Escalation with PEASS-NG



Rishalin Pillay

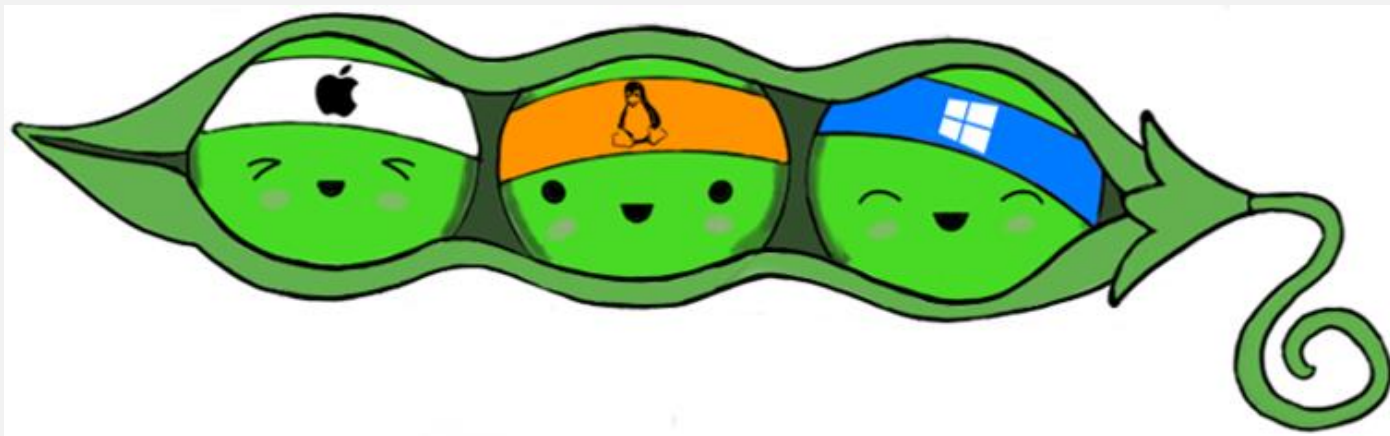
OFFENSIVE SECURITY AUTHOR & SPECIALIST

@r1shal1n



Creator: Carlos Polop

PEASS-NG consists of tools which search for possible privilege escalation paths that one could exploit, printing them to the console with nice colors so you can recognize misconfigurations easily.

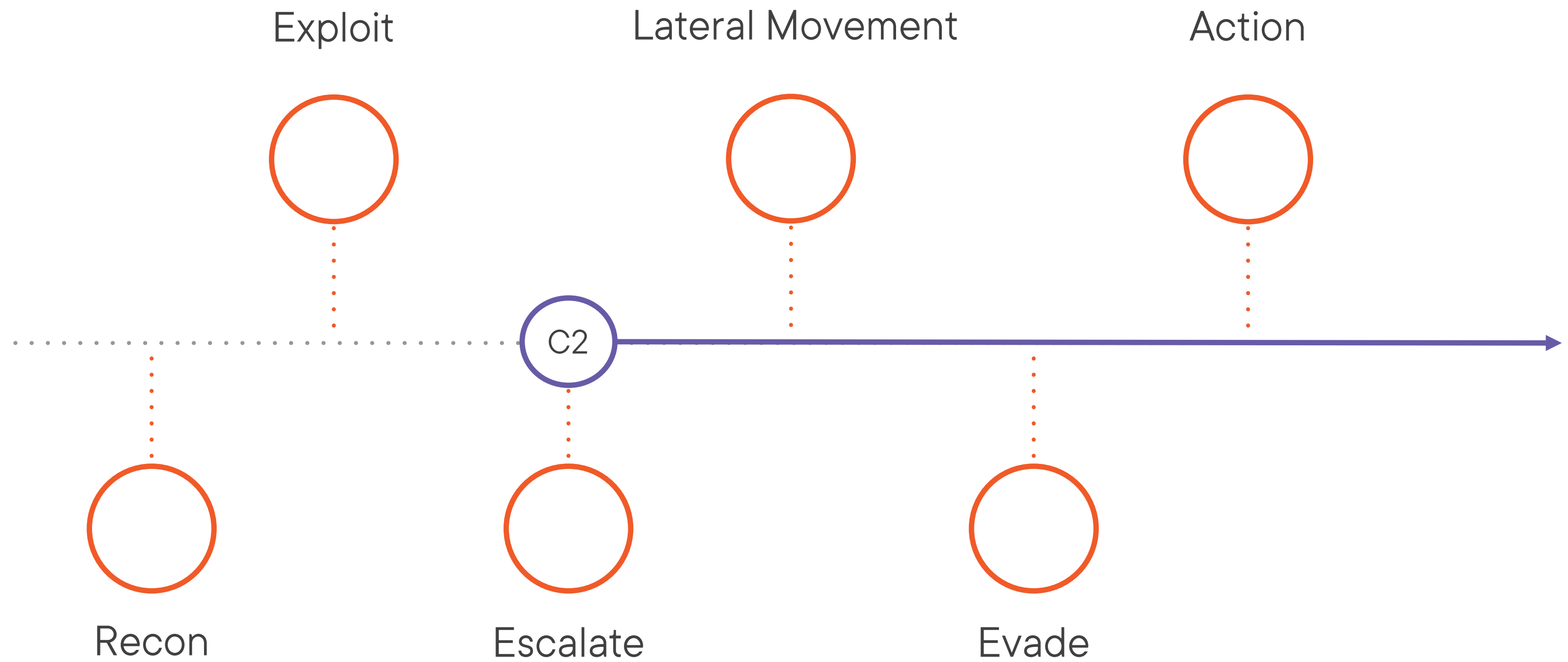


Privilege Escalation Script Suite

GitHub - <https://github.com/carlospolop/PEASS-ng>


What makes it special; why use this one?

Kill Chain



MITRE ATT&CK

Tactics



- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

MITRE ATT&CK

Tactics

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1548.001

SETUID/SETGID

T1055.001

DLL Injection

T1547.001

Registry Keys

More Information

WinPeas

Checklist – Local Windows Privilege Escalation

<https://book.hacktricks.xyz/windows-hardening/checklist-windows-privilege-escalation>

LinPeas

Checklist – Linux Privilege Escalation

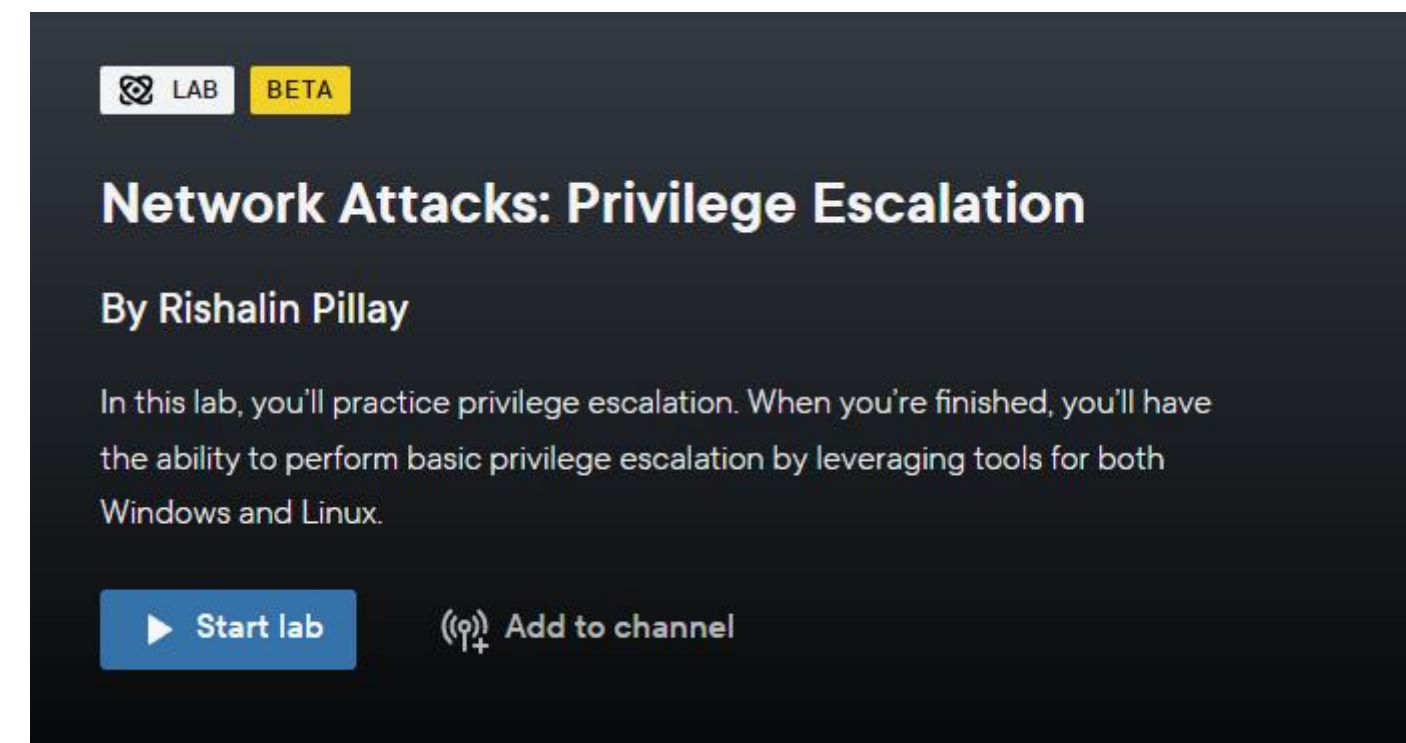
<https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>

More Information

LAB

Network Attacks: Privilege Escalation

<https://app.pluralsight.com/labs/detail/14831c12-b0ca-48c3-9b14-f31030dbd597/toc>



The screenshot shows a dark-themed interface for a Pluralsight lab. At the top left, there is a 'LAB' icon and a 'BETA' badge. The main title 'Network Attacks: Privilege Escalation' is displayed in a large, bold font. Below the title, it says 'By Rishalin Pillay'. A descriptive paragraph follows: 'In this lab, you'll practice privilege escalation. When you're finished, you'll have the ability to perform basic privilege escalation by leveraging tools for both Windows and Linux.' At the bottom, there are two buttons: a blue 'Start lab' button with a play icon, and a 'Add to channel' button with a plus icon inside a circle.

LAB BETA

Network Attacks: Privilege Escalation

By Rishalin Pillay

In this lab, you'll practice privilege escalation. When you're finished, you'll have the ability to perform basic privilege escalation by leveraging tools for both Windows and Linux.

▶ Start lab

⛶ Add to channel