
OMU
HACKERS

/dmuhackers

@dmuhackers

Privilege Escalation

Disclaimer

Don't do illegal shit

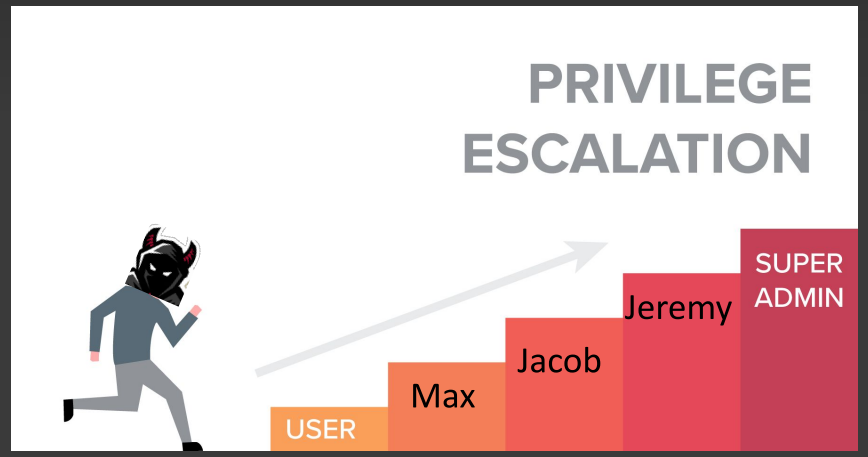
OMU HACKERS

Overview

- What is Privilege Escalation?
- Priv Esc tools
- Challenges

What is Privilege Escalation?

- Priv Esc is gaining unauthorised access to more or higher permissions, restricted to the current user
- Useful when an initial remote foothold has little or unuseful access
- Achieved through exploiting software bugs, poor user access control, designs flaws, etc



Priv Esc tools

- LinEnum – Local enumeration and privesc checker (linux)
- pspy – Monitor processes running, cron jobs etc. (linux)
- GTFOBins – Searchable database of binaries useful in privesc (linux)
- SUDO_KILLER - A tool to identify and exploit sudo rules' misconfigurations and vulnerabilities within sudo (linux)
- PrivEsc Workshop – Practical slides and exercises for practicing privesc. (windows and linux)
- PEASS – PrivEsc Awesome Script Suite. Local enumeration/privesc checking scripts (windows and linux)
- Windows Exploit Suggester – automated tool that checks windows version with known CVEs, Metasploit modules etc.
- Windows Kernel exploits – Selection of kernel exploits for known CVEs

Challenges

http://bit.ly/wk11_PrivEsc