Privilege Escalation

Strathmore
UNIVERSITY

Topics

Privilege Escalation

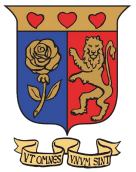
Objectives

- Understand Privilege Escalation Concepts
- Correlate Privilege Escalation with other steps of the Hacking Methodology, i.e Gaining Access
- Combine Information Gathering, as a prerequisite in performing a Privilege Escalation attack scenario

- Linux Privilege Escalation
  - Permissions
  - Techniques
  - Tools
  - Defenses
  - Lab
- Windows Privilege Escalation
  - Permission structure
  - Techniques
  - Tools
  - Defenses
  - Lab

Linux Privilege Escalation

Techniques



Strathmore UNIVERSITY

Linux Privilege Escalation can be:

- Privilege Escalation by kernel exploit
  - Dirty Cow Exploit - Linux Kernel 2.6.22 < 3.9 (x86/x64)
  - Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation
  - Linux 5.3 - Privilege Escalation via io_uring Offload of sendmsg()
  - Use of ExploitDB, searchsploit on Linux
- Privilege Escalation by Password Mining
  - By looking at bash history of user on home directory

Privilege Escalation by Sudo

Strathmore UNIVERSITY

*Applies to a user who turns of passwd for sudo

1. Start with taking the ssh instance of the victim machine by using the command ssh
2. In command prompt type: sudo -l
3. Elevate privilege using sudo find . -exec /bin/sh \; -quit

•

Other Techniques

Strathmore UNIVERSITY

- Privilege Escalation by File Permissions
  - Attempting to access and read shadow file, obtain hashed password of sudo user. Requires read access through check :

    ls -al /etc/shadow
- Privilege Escalation by Crontab

Linux Lab

[Vulnerable Machine]

Windows Privilege Escalation

Techniques

Strathmore UNIVERSITY

- Using DLL Hijacking
  - DLL Search Order Hijacking
- Bypass User Account Control
  - if UAC protection is not at the highest level, some Windows programs can escalate privileges, or execute COM objects with administrative privileges.
- Access Token Manipulation

DLL Hijacking

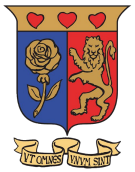
Strathmore UNIVERSITY

- Also known as DLL search order hijacking, takes advantage of search order to reach legitimate DLLs
- DLL preloading.
    - This involves planting a malicious DLL with the same name as a legitimate DLL, in a location which is searched by the system before the legitimate DLL.

Mitigation

- Disallow loading of remote DLLs
- Enable Safe DLL Search Mode to force search for system DLLs in directories with greater restrictions
- Use auditing tools such as PowerSploit to detect DLL search order hijacking vulnerabilities and correct them

Access Token Manipulation



Strathmore UNIVERSITY

- Windows uses access tokens to determine the owners of running processes
- Access token manipulation involves fooling the system into believing that the running process belongs to someone other than the user who started the process

Three ways of achieving it:

- Duplicating an access token
- Creating a new process with an impersonated token
- Leveraging username and password to create a token

Windows Lab

Windows Vulnerable Machine