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

What is Privilege Escalation?

Privilege Escalation

- Privileges mean what a user is permitted to do. Common privileges include viewing and editing files, or modifying system files.
- Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected by an application or user.

Privilege Escalation(Cont)

- What precedes Priv Esc?
  - Based on hacking methodology

- What types of attacks can achieve the steps above?
  - i.e DoS

Ama

Types of Privilege Escalation

Vertical

- Accesses to functions that are reserved for higher privilege users or applications.
  - Gaining administrative privileges
  - Jailbreaking Devices
  - Lock Screen Bypass

Horizontal

- The attacker is a normal, low-end user who accesses the information of other normal users.
  - Accessing accounts on the same user level
  - Stealing usernames/passwords

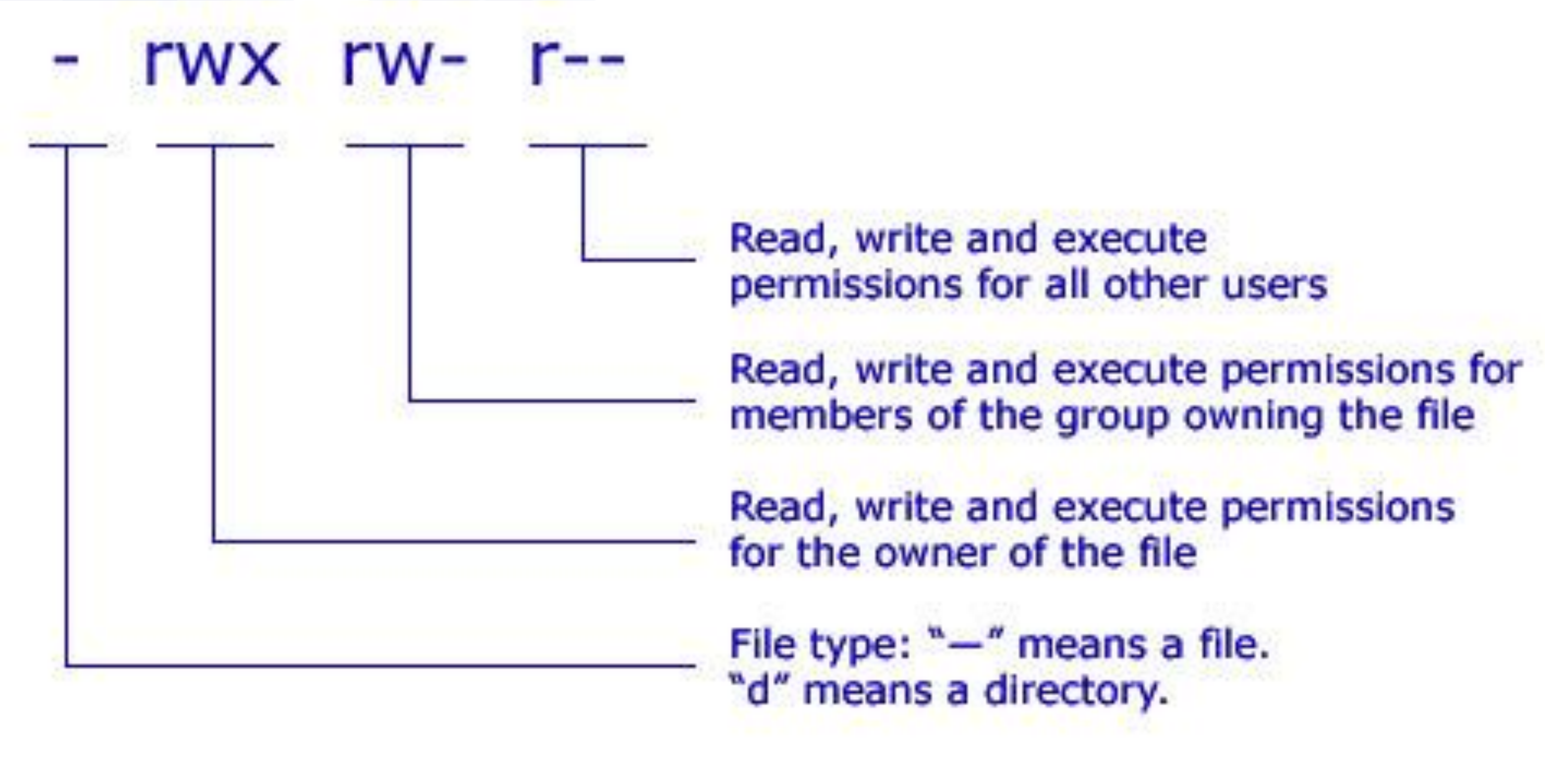
Privilege Escalation Platforms

- Linux Privilege Escalation
- Windows Privilege Escalation
- Hardware?

Linux Privilege Escalation

Linux Permission Structure

r - 4 , w - 2, x -1



Read, write and execute permissions for all other users

Read, write and execute permissions for members of the group owning the file

Read, write and execute permissions for the owner of the file

File type: "—" means a file. "d" means a directory.

Privilege Escalation by Sudo

Exercise - *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

-

Techniques

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

Other Techniques

- 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

Mitigation/Defense

1. Keep all the important information on the server side and send only Session ID's to the client side. For this kind of setup the session state of HTTP should be set to persistent.
2. Encoding and Encryption is an essential step in protecting any information from an attacker. This technique adds another step as the data needs to be encrypted and decrypted again and again.
3. Ensure that strong password policies are setup so that there are less chances of brute forcing the password and escalating the privileges.

Defenses (Cont)

4. All the unused ports should be closed by default and all the files should have read only access enabled to them and giving write permissions to only users and groups

who need them.

5. Sanitizing all the user inputs treating them as malicious. A whitelist of characters should be created and only those characters should be allowed.

6. Last but not the least, all the applications and systems should be patched and updated to the latest security version WAF

Windows Privilege Escalation

Windows Permission Structure

- root is “Local System” Account
- Windows UAC (User Account Control)
- disabled admin account, instead uses UAC
- “sudo” is “runas” to run with privileges

Types of Accounts:

- Local User
- Domain User
- The LocalSystem

User Access Control

- All users run as an unprivileged user by default, even when logged on as an Administrator
- Once running, the privilege of an application cannot be changed.
- Users are prompted to provide explicit consent before using elevated privilege, which then lasts for the life of the process.

Techniques

- 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

- 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

- 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

Defense Against Priv ESc

1. Run users and apps with lowest privileges
2. Implement multi-factor authentication and authorization
3. Regularly patch and update kernel
4. Use encryption techniques to protect sensitive data
5. Test for coding errors and bugs thoroughly
6. Implement a privilege separation methodology
7. Change UAC settings to Always Notify
8. Use whitelisting tools to identify and block malicious software
9. Use fully qualified paths in all windows applications

Privilege Escalation Tools

- BeRoot
- PowerSploit
- Linux Exploit Suggester
- Windows Exploit Suggester
- MimiKatz