Well, that escalated quickly! - A penetration tester's approach to privilege escalation
Escalating Privileges – Why?

• Usually, attackers gain low privileged access to a system

• High privileges are required to be fully operative

• Important but complex aspect of a pentest

• Little literature
Main Goals

• Learn different privilege escalation concepts and attacks

• Provide a practical and systematic privilege escalation approach
Registry

- Composed of keys and values
- Highest level keys are called root keys
- Keys included in other keys are called sub-keys
- Stores
  - systemwide software settings
  - security database
  - per-user configuration settings
- Protected by an ACL
Processes

- Contain:
  - process ID
  - executable program
  - security context
Jobs & Threads

- Jobs are groups of processes

- Threads are entities within a process
Services

- Used to start processes at system startup
- Consist of at least one executable file
- Run in the context of a user
  - Mostly non-interactive users
  - Usually in context of SYSTEM user
Privilege Escalation - Methods and Techniques
Overview

- Some techniques work for more than one Windows components
- Attack trees give an overview of different techniques
Insecure Services

- Weak Service Executable or Configuration File Permissions
  - Service Path contains whitespace(s)

- Unquoted Service Paths
  - Write permission in the directory are given

- Weak Service Permissions
  - Service tries to load a missing DLL

- DLL Hijacking
  - Service uses a relative file path to the DLL

- Weak Registry Key Permissions
  - Write permissions in one of the searched directories
Insecure Services

- Weak Service Executable or Configuration File Permissions
  - Service Path contains whitespace(s)
  - Write permission in the directory are given
- Unquoted Service Paths
- Weak Service Permissions
  - Service tries to load a missing DLL
- DLL Hijacking
  - Service uses a relative file path to the DLL
- Weak Registry Key Permissions
  - Write permissions in one of the searched directories
Insecure Services - Weak Executable File Permissions

• Service’s executable or configuration file with weak permissions

• Can be modified by a low privileged user

→ Exploit: Replace or modify file and trigger a restart of the service
Demo
Insecure Services

- Weak Service Executable or Configuration File Permissions
  - Service Path contains whitespace(s)
- Unquoted Service Paths
  - Write permission in the directory are given
- Weak Service Permissions
  - Service tries to load a missing DLL
- DLL Hijacking
  - Service uses a relative file path to the DLL
- Weak Registry Key Permissions
  - Write permissions in one of the searched directories
Insecure Services – DLL Hijacking

- Applications that:
  - try to load a missing DLL file
  - use relative file paths are possibly vulnerable

- Windows tries to find the DLL file in the following directories:
  - The directory from which the application is loaded
  - C:\Windows\System32
  - C:\Windows\System
  - C:\Windows
  - The current working directory
  - Directories in the system PATH environment variable
  - Directories in the user PATH environment variable

→ With write permissions to a folder above, an attacker can place a malicious DLL file
Demo
Outdated Software

- Companies can not always deploy patches in a timely manner

- Successful kernel exploits result in SYSTEM privileges

→ Exploiting high privileged processes
Outdated Software

- Recent Windows 10 Zero Days published by angry researcher:

SandboxEscape drops three more Windows 10 zero-day exploits

Security researcher makes good on her promise
Thursday, May 23, 2019

Uploaded the remaining bugs.

I like burning bridges. I just hate this world.

ps: that last windows error reporting bug was apparently patched this month. Other 4 bugs on github are still 0days. have fun.

Bye.
Weak Passwords

- Users may use weak passwords:
  - Wordlist
  - Brute force attacks

- Plaintext passwords in files:
  - C:\unattend.xml
  - C:\Windows\Panther\Unattend.xml
  - C:\Windows\Panther\Unattend\Unattend.xml
  - C:\Windows\system32\sysprep*
  - ...

- Plaintext passwords in registry:
  - HKLM\Software\Microsoft\Windows NT\WinLogon
  - ...

Insufficient Physical Access Protection

• An attacker with physical access to a system has more attack vectors:
  • Replacing Windows startup programs in an unencrypted disks
  • Extract decryption key from memory if pre-boot authentication is disabled (Cold Boot Attacks)
  • Direct Memory Access Attacks
  • TPM Sniffing
  • Attacks against CPU micro controller are possible
Insufficient Physical Access Protection

• Cold Boot Attack:

Cold Boot Attack | University of South Wales VeraCrypt Research Group
Direct Memory Access Attack
https://pulsesecurity.co.nz/articles/TPM-sniffing
Privilege Escalation Approach
Overview

Phase 1
General Information Gathering

Phase 2
Method and Technique Iteration

Phase 3
Reporting

Post-Exploitation
Information Gathering
Exploitation
Research and Development
Phase 1: General Information Gathering

• Systems have different:
  • Windows versions
  • service packs
  • CPU architectures
  • Purposes
  • network configurations
  • …

• Goal is to have a good overview of the system
Phase 2: Method and Technique Iteration

- Iterate through privilege escalation methods and techniques

- These can be ordered accordingly to the penetration test’s objective

- Every iteration consists of four steps
Steps of Phase 2

- [Step 1] Information Gathering:
  - Check whether system is vulnerable to method

- [Step 2] Research and Development:
  - Gather information about available exploits and customize to target system
  - Set-up a test environment
  - Consider possible security mechanisms
Steps of Phase 2

• [Step 3] Exploitation:
  ▪ Test exploit developed in step 2
  ▪ Previous steps have to be sometimes repeated

• [Step 4] Post-Exploitation
  ▪ Document steps and results
  ▪ Ask whether monitoring systems have detected the attacks
Conclusion
Conclusion

• This knowledge can also be used by system administrators and architects

• Windows systems:
  • great number of security mechanisms
  • granular configuration of privileges and access rights
  • patches published fast

• Learnt things about
  • Windows
  • Privilege escalation concepts
  • An approach for penetration testers
  • Tools that can be used
Escalating privileges is just a question of time
In many scenarios, you do not necessarily need to locally escalate your privileges.
Q&A Session
Any further questions?
Don't hesitate to contact me.

Khalil Bijjou
k.bijjou@sec-consult.com
+41 79 896 73 08
SEC Consult (Schweiz) AG
Turbinenstrasse 28
8005 Zürich, Schweiz
www.sec-consult.com