Security First Principles

**LEAST PRIVILEGE – Assessment**

Learning Outcome 1

Understanding Windows horizontal and vertical privilege escalation vulnerabilities

* Step 4 folder: C:\Users\DSU\Desktop\Step 4
* Step 6 folder: C:\System32\Step 6
* Question 2 command:

wmic service get name,displayname,pathname,startmode |findstr /I “Auto” |findstr /I /v “C:\Windows\\” |findstr /I /v “””

* Question 3 path: C:\Program Files\Runnable Service
  + Exploited as C:\Program Files\Runnable Service\Service.exe
* Question 5 command: sc create [ServiceName] binPath= "[C:\Path\To\New\Shell.exe]" start= auto

Rubric for **Lab Exercise 1: Windows Unquoted Service Paths**

|  |  |  |  |
| --- | --- | --- | --- |
| **Content Criteria** | **Correct (4 points)** | **Partially correct (2 points)** | **Incorrect (0 points)** |
| **Step 4** | A file titled “(student name).txt” appears in the “Step 4” folder. | Something other than a .txt file is named “(student name)”, the student’s name is not discernable, or the student edited or deleted other files in the folder. | No text file exists in the folder. |
| **Step 6** | A file titled “(student name).txt” appears in the “Step 6” folder. | Something other than a .txt file is named “(student name)”, the student’s name is not discernable, or the student edited or deleted other files in the folder. | No text file exists in the folder. |
| **Question 1** | The student states that the vulnerability is an unquoted service path. | The student states that the vulnerability is related to a Windows service or filesystem privilege configuration. | The student states that the vulnerability is related to any other issue. |
| **Question 2** | The student states the correct (or equivalent) cmd command which returns only the unquoted service path used in the exercise. | The student states a cmd command that is similar to the correct command, but it returns more files than necessary. | The student does not state a cmd command or the command stated does not identify the unquoted service path. |
| **Question 3** | The student states the correct vulnerable path. | The student states a more general or specific path than the correct vulnerable path. | The student states a path that is not relevant to the exercise. |
| **Question 4** | The student clearly explains how they crafted and ran their exploit. Evidence is provided. | The student attempts to explain, but some aspects are unclear. Evidence is missing or not relevant. | The student’s explanation is missing or incomprehensible. Evidence is not provided. |
| **Question 5** | The student states the correct command and arguments to create the new SYSTEM-level service. | The student states the correct command, but the arguments are incorrect. | The student states an incorrect command. |

Learning Outcome 2

Understanding Linux horizontal privilege escalation vulnerabilities

* Question 3 file: /usr/bin/shell
* Question 2 command:  
  find / -perm -u=s -type f 2>/dev/null
* Step 4 folder: /home/kali/Desktop/Step 4

Rubric for Lab Exercise 2: Linux SUID

|  |  |  |  |
| --- | --- | --- | --- |
| **Content Criteria** | **Correct (4 points)** | **Partially correct (2 points)** | **Incorrect (0 points)** |
| **Step 4** | A text file titled “(student name)” appears in the “Step 4” folder on the kali user’s desktop. | Something other than a .txt file is named “(student name)”, the student name is not discernable, or the student edited or deleted other files in the folder. | No text file exists in the folder. |
| **Question 1** | The student correctly identifies that the SUID bit is the permission causing the vulnerability in this exercise. | The student identifies that SGID, sticky bit, or a similar permission or attribute is causing the vulnerability in this exercise. | The student identifies that any other configuration is causing the vulnerability in this exercise. |
| **Question 2** | The student states the correct (or equivalent) Bash command which returns the SUID file used in the exercise along with the default SUID files. | The student states a Bash command that is similar to the correct command, but it returns more files than necessary. | The student does not state a Bash command or the command stated does not identify the SUID file. |
| **Question 3** | The student states the correct path, identifies it as Bash, and recognizes that the ‘privileged’ flag is enabled. Evidence is provided. | The student states a similar path to the correct file, identifies it as a shell, that it was modified from source, or the | The student states an irrelevant path, identifies it as any other application, or does not identify the modification. |

Learning Outcome 3

Understanding Linux vertical privilege escalation vulnerabilities

* Step 5 folder: /root/Step 5
* Question 3 text to append: “,/usr/bin/su”

Rubric for Lab Exercise 3: Linux visudo

|  |  |  |  |
| --- | --- | --- | --- |
| **Content Criteria** | **Correct (4 points)** | **Partially correct (2 points)** | **Incorrect (0 points)** |
| **Step 5** | A text file titled “(student name)” appears in the “Step 5” folder in the root user’s home directory. | Something other than a .txt file is named “(student name)”, the student name is not discernable, or the student edited or deleted other files in the folder. | No text file exists in the folder. |
| **Question 1** | The student correctly identifies that the student user’s ability to run visudo is the permission causing the vulnerability in this exercise. | The student identifies some other error related to sudo configuration. | The student identifies an error with a command other than sudo. |
| **Question 2** | The student correctly verifies the Question 1 results by running sudo -l as the student user and has 3 or fewer failed sudo attempts in the log file for this exercise. | The student runs the sudo command with a different flag or has between 4 and 5 failed sudo attempts in the log file for this exercise. | The student runs a command other than sudo or has more than 5 failed sudo attempts in the log file for this exercise. |
| **Question 3** | The student appends the correct text to the sudoers file, enabling su command access for the student user. | The student appends text to the sudoers file, but it gives more permissions than necessary to the student user or gives permissions to other users. | The student does not edit the sudoers file or edits it in a way that makes sudo unusable. |

Learning Outcome 4 (Optional)

DevOps for PrivEsc Vulnerability Management

Rubric for Puzzler: PrivEsc Scanning Script

|  |  |  |  |
| --- | --- | --- | --- |
| **Content Criteria** | **Correct (4 points)** | **Partially correct (2 points)** | **Incorrect (0 points)** |
| **Scanning** | The script(s) scan for and successfully identify all of the privilege escalation vulnerabilities in the lab as well as at least one more of the student’s choice. | The script(s) scan for and successfully identify some, but not all, of the vulnerabilities in the lab. | The script(s) do not scan for or identify the vulnerabilities in the lab. |
| **Reporting** | The script(s) print out useful information that would allow a security analyst or system administrator to identify and correct the vulnerabilities. | The script(s) print out some information concerning the vulnerability, but important identifying aspects are missing or incomplete. | The script(s) do not print out a report. |
| **Correcting** | The script(s) successfully correct the identified vulnerabilities that can be corrected automatically. System stability is not impacted. | The script(s) successfully correct some of the vulnerabilities that can be corrected automatically, or the corrections cause some system components to fail. | The script(s) do not correct vulnerabilities that can be corrected automatically, or the corrections crash the system. |
| **User Interface Design** | The script(s) are easy to run, handle errors without crashing, and display useful messages to the user. | The script(s) have a learning curve, don’t handle some errors experienced during runtime, or don’t communicate well with the user. | The script(s) are not understandable, frequently crash, or don’t communicate with the user. |
| **Documentation** | The script(s) are well-documented throughout. | The script(s) have some documentation, but it is hard to understand or incomplete. | The script(s) have no documentation. |