EXPTNO:07 ROLLNO: 220701259

WINDOWSPRIVELEGEESCALATION

AIM:

- Understandthetechniquesusedtoescalateprivilegesonwindowssystems.

- Explorecommonmisconfigurationsandvulnerabilitiesinreal-worldandCTF scenarios.

- Usecommand-linetoolsandscriptstoextractcredentials,accessrestrictedfiles, and gain elevated privileges.

- Learnhowtoidentifyweakservicepermissions,unquotedpaths,andinsecure configurations.

- Practicemanualenumerationandexploitationtechniquesonwindowstargets.

PROCEDURE:

1. AnalyzePowerShellhistoryandconfigurationfilesforstored passwords.

2. Use`cmdkey`,`runas`,andPuTTYsavedsessionstoaccessotherusers' contexts.

3. Exploitvulnerablescheduledtasksandserviceswithweakpermissions.

4. Leveragemisconfiguredservicestoreplacebinariesorabusequotedpaths.

5. DumpSAMandSYSTEMhashesusingSeBackup/SeRestoreprivileges.

6. UsetoolslikeImpacketandPsExectoreusecredentialsandaccessAdmin accounts.

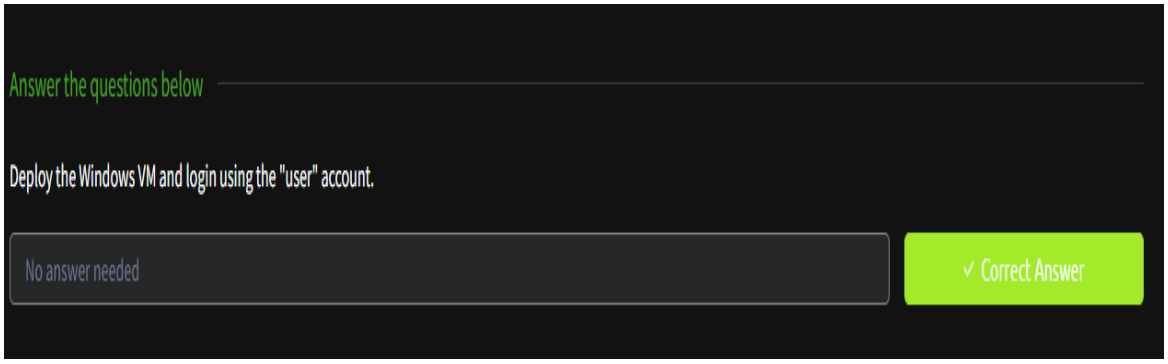
7. ExploitDLLhijackinginvulnerablesoftwaretoescalateto SYSTEM.

TASK1– INTRODUCTION

- IntroducedWindowsprivilegeescalationandthegoalofmovingfromstandard user to Administrator or SYSTEM.

- Outlinedcommonmisconfigurationssuchasservices,credentials,orsoftware flaws.

- Emphasizedsafeenumeration,logreview,andprivilegeabusemethods.

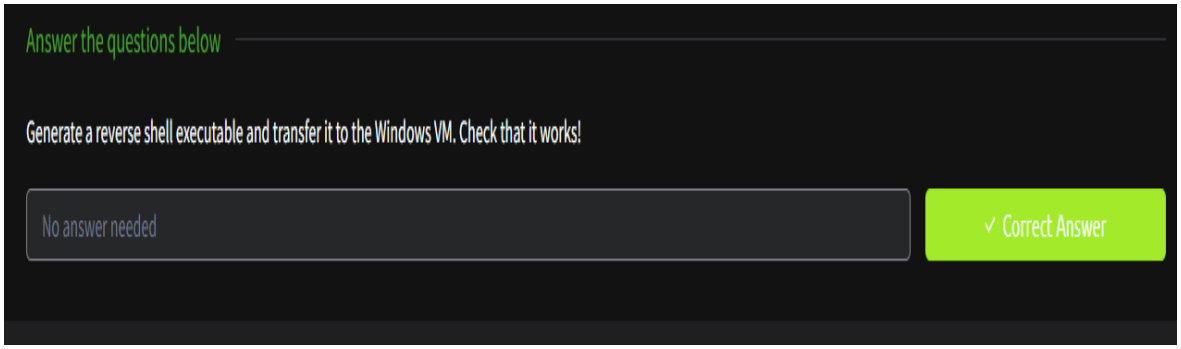


TASK2– ENUMERATION

- Used`whoami`, `systeminfo`,and`netuser`toenumeratethesystem.

- Gatheredinformationaboutprivileges,groupmembership,andarchitecture.

- Reviewedrunningservicesanduserpermissionsforpotentialescalationpaths.



TASK3–PASSWORDRECOVERYTECHNIQUES

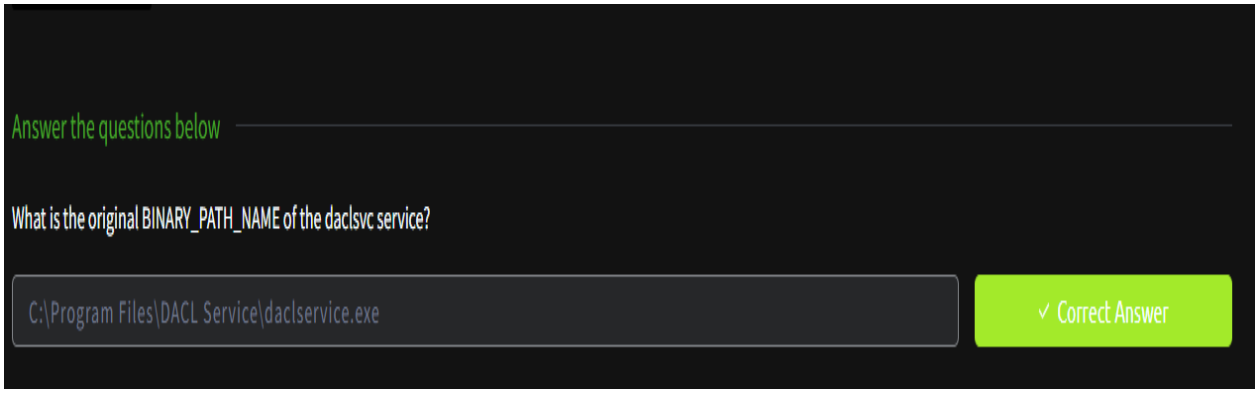
- ExtractedpasswordfromPowerShellhistory:`ZuperCkretPa5z`(julia.jones).

- FoundplaintextDBpasswordinIISweb.config:`098n0x35skjD3`(db_admin).

- Used`cmdkey`and`runas`toaccessmike.katzdesktopandretrieve flag.

- RetrievedPuTTYpasswordforthom.smithfromsavedsession: `CoolPass2021`.

- Highlightedtheimportanceofmanagingcredentialssecurelyonendpoints.



TASK4–SCHEDULEDTASKABUSE

- Exploitedscheduledtaskwithwriteaccesstoinjectareverseshell script.

- Used`nc64.exe`tosetupabackdoorconnectionwithlistener.

- Triggeredtasktogainaccessastaskusr1andretrievedtheflag.

- Demonstratedthedangerofinsecuretaskpermissions.

- EmphasizedcheckingscheduledtaskconfigurationsonWindowsenvironments.

TASK5–WEAKSERVICEPERMISSIONS

- Used`icacls`tofindmodifiableserviceexecutables.

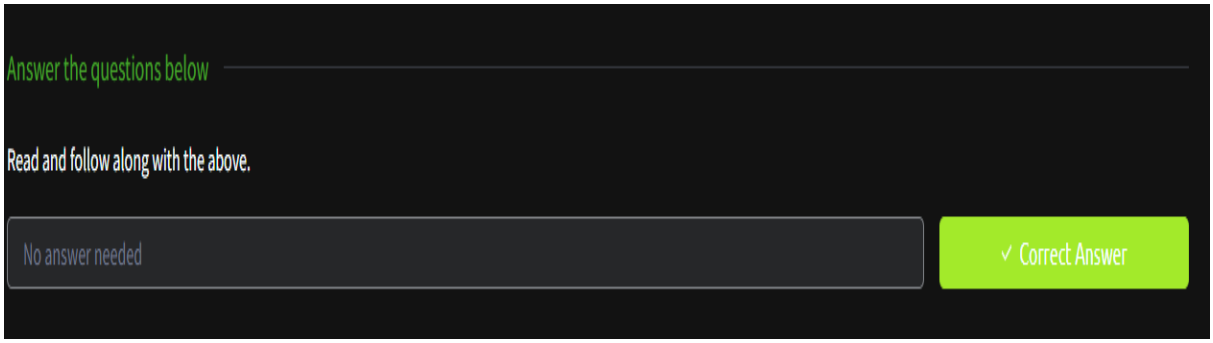
- Createdreverseshellwith`msfvenom`,downloadedviaPythonHTTPserver.

- Replacedvulnerableservicebinaryandrestartedservicetogainshell.

- Retrievedflagsfromsvcusr1andsvcusr2usingmodifiedservices.

- Demonstratedexploitationofunquotedservicepaths.

- GainedaccesstoAdministratordesktopbyeditingTHMServiceconfiguration.



TASK6–SeBackup/SeRestorePRIVILEGEESCALATION

- Verified`SeBackupPrivilege`using`whoami/priv`.

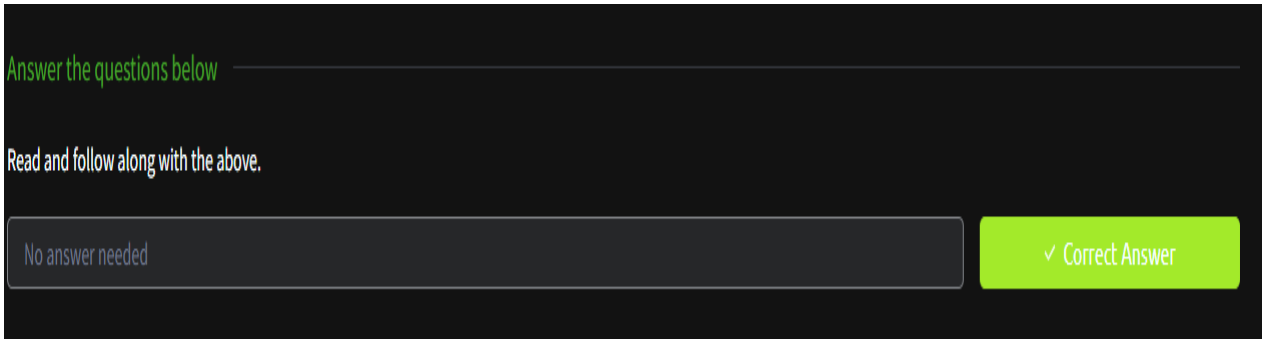
- BackedupSAMandSYSTEMfilesandsharedthemviaSMB server.

- Used`secretsdump.py`toextractpasswordhashesfrombackups.

- Used`psexec.py`andthedumpedhashtogainAdministrator shell.

- RetrievedfinalflagfromAdministrator's desktop.

- Demonstratedtheriskofpowerfulbackupprivilegesinmisconfiguredroles.



TASK7–VULNERABLESOFTWAREEXPLOITATION

- IdentifiedvulnerablesoftwarewithDLLsearchorderhijackingissues.

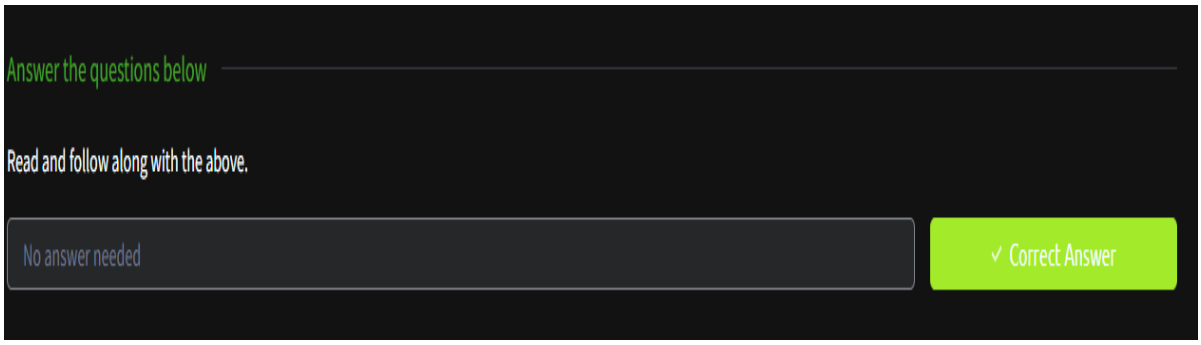
- ModifiedpublicexploitscripttoaddnewusertoAdministrators group.

- UsedPowerShellISEtoexecuteexploitpayload.

- HandledDefenderblockingandscripterrorsvia debugging.

- GainedAdministratorprivilegesbyreplacingDLLinpath.

- RetrievedfinalflagfromAdministrator’s desktop.



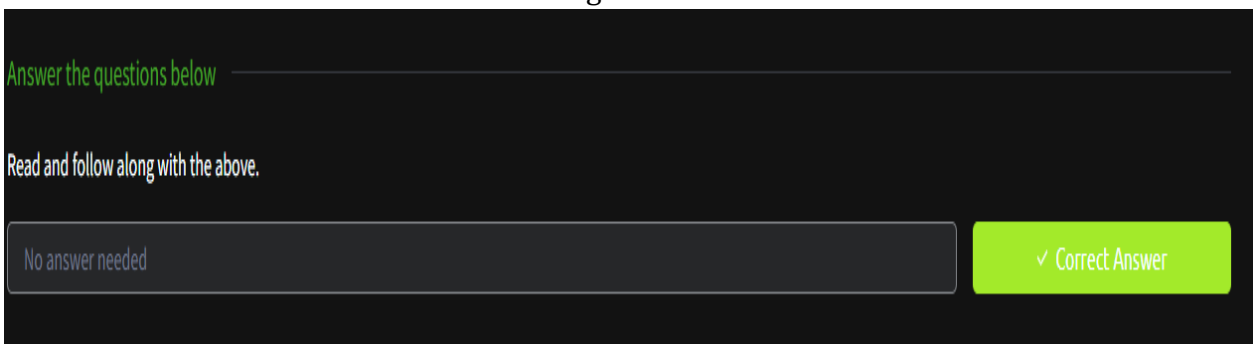
TASK8–UNQUOTEDSERVICEPATHEXPLOIT

- Analyzedserviceexecutablepathslackingquotes.

- Placedmaliciousreverseshellatexpectedpathsegment(e.g.,`C:\Program.exe`).

- Restartedtheservicetotriggerunintendedbinaryexecution.

- Gainedadminshellandextractedthefinalflag.



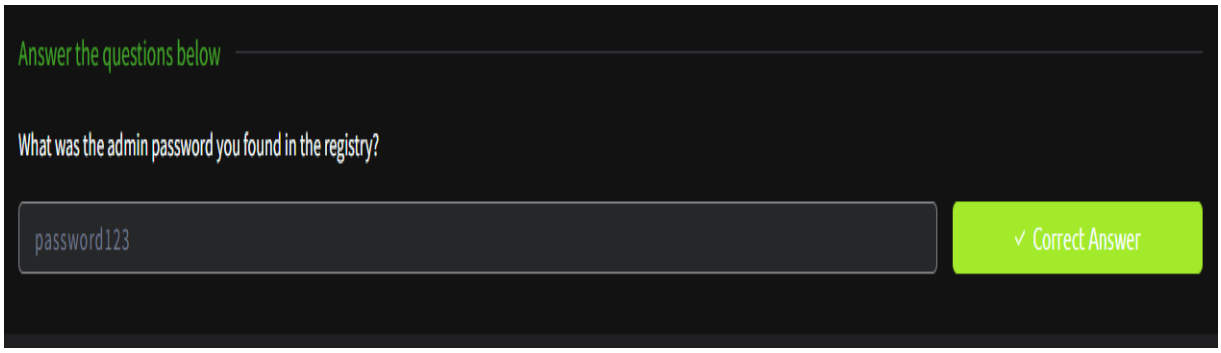
TASK9–SERVICEBINARYREPLACEMENT

- Identifiedservicebinarieswithwritepermissions.

- Replaceddefaultexecutablewithmaliciousoneusingreverseshellpayload.

- Restartedservicetorunmaliciousbinaryandelevateaccess.

- ConfirmedaccessbyretrievingtheAdministrator’sdesktop flag.

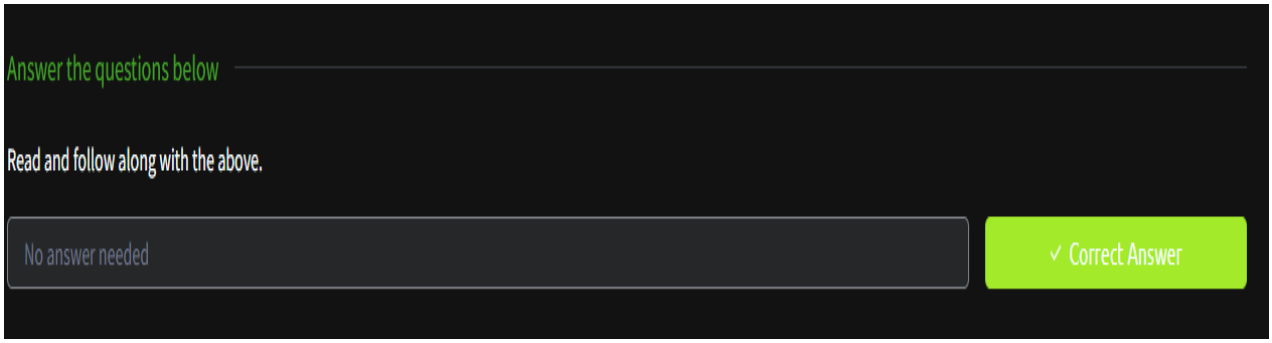


TASK10–RDPACCESSTOADMIN ACCOUNT

- EstablishedRDPconnectionusingcrackedorinjectedadmincredentials.

- UsedGUIorcommand-linetoolstoenumerateservicesand extract flags.

- Navigatedto`C:\Users\Administrator\Desktop`forfinalflagretrieval.

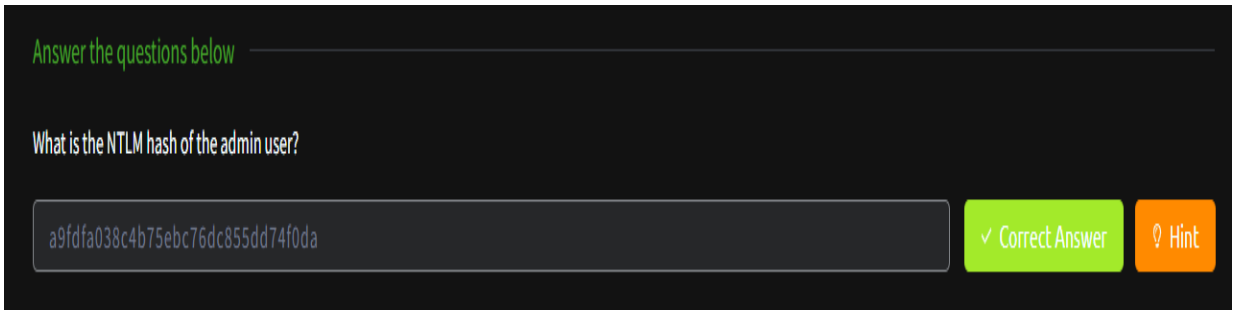


TASK11– PASSWORDHASH REPLAY

- Dumpedpasswordhashesusing`secretsdump.py`.

- Replayedadministratorhashusing`psexec.py`forshellaccess.

- BypassedpasswordauthenticationusingNTLMreplaytechniques.



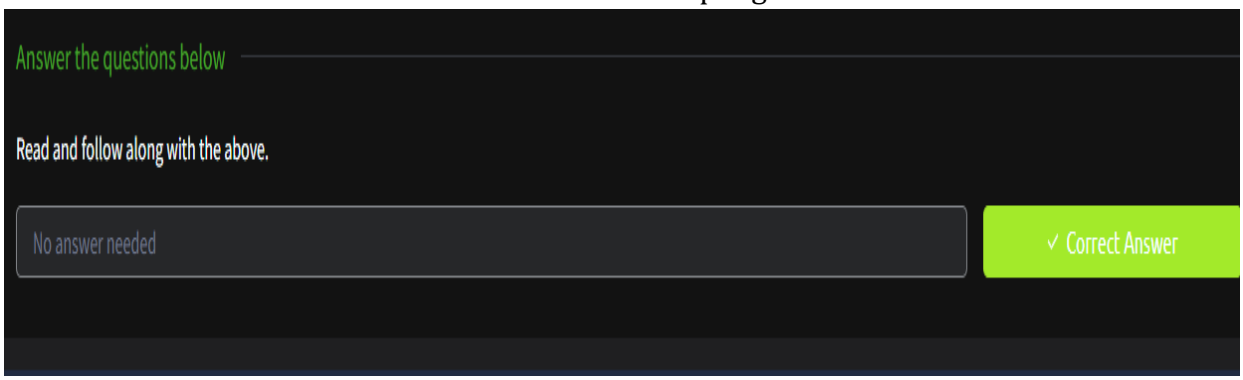
TASK12–SOFTWAREESCALATIONVIALOGICFLAW

- Discoveredvulnerablesoftwarewithpost-installlogicflaw.

- Injectedadmincreationorshellcommandsintoconfigfiles.

- Triggeredsoftwaretoexecutelogicandescalateprivileges.

- Verifiedaccessvianewuserandconfirmedviadesktopflag.

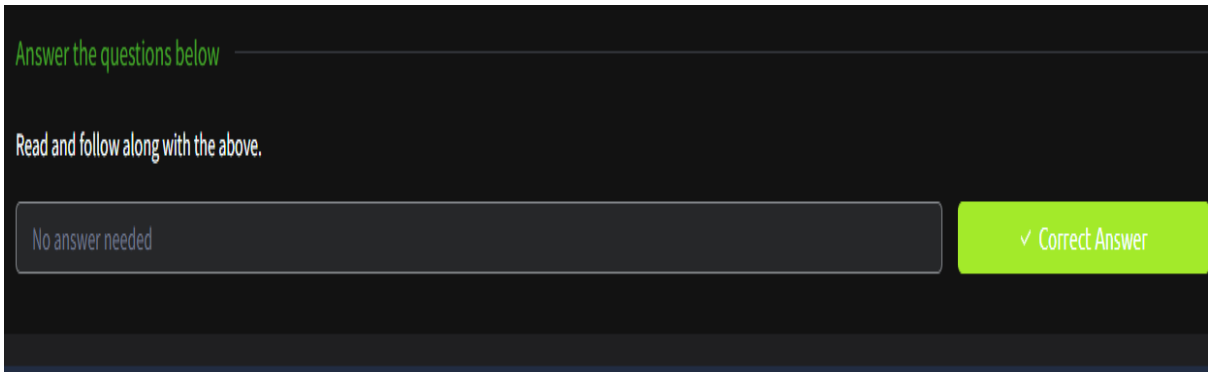


TASK13–MIMIKATZCREDENTIALDUMP

- UsedMimikatztodumpplaintextpasswordsand tickethashesfrom memory.

- Extracteddomainorlocaladmincredentialsfrom LSASS.

- Usedcredentialstoswitchusersoraccessprotected files.

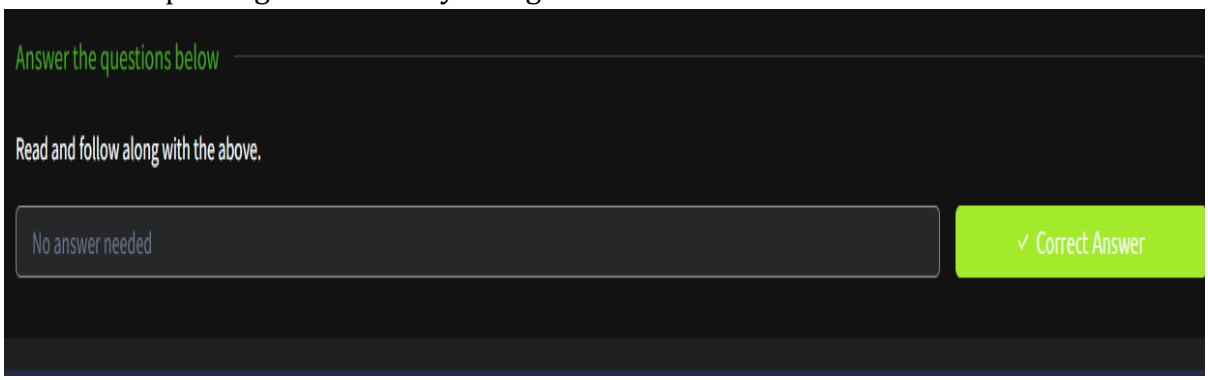


TASK14– DLLINJECTIONINADMINPROCESS

- InjectedmaliciousDLLintoaprocessrunningasAdministrator.

- Hookedintoprocessmemoryandexecutedpayloadtospawnelevatedshell.

- Confirmedprivilegeescalationbylistingusertokens.

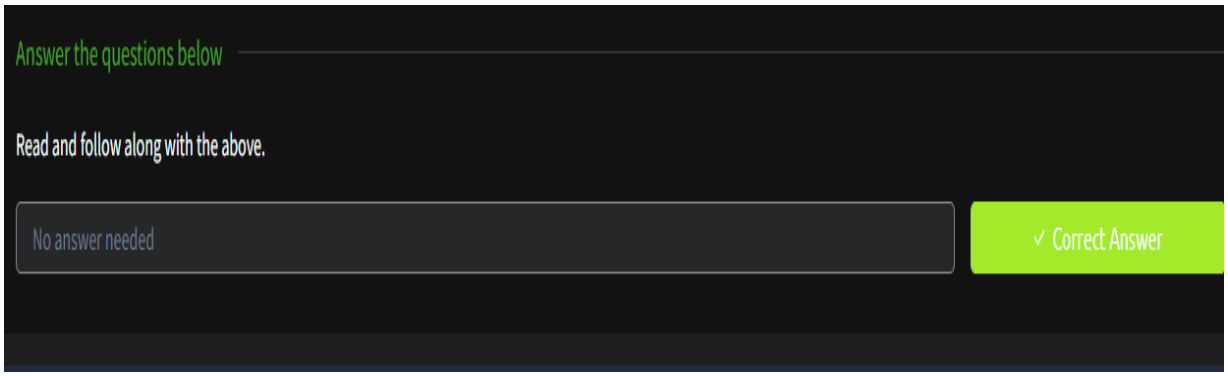


TASK15–HIJACKEDAUTO-RUNENTRY

- Detectedauto-runregistrykeyspointingtowritablepaths.

- Modifiedtheexecutablepathtoareverseshell payload.

- Restartedsystemortriggereduserloginto executemaliciouspayload.

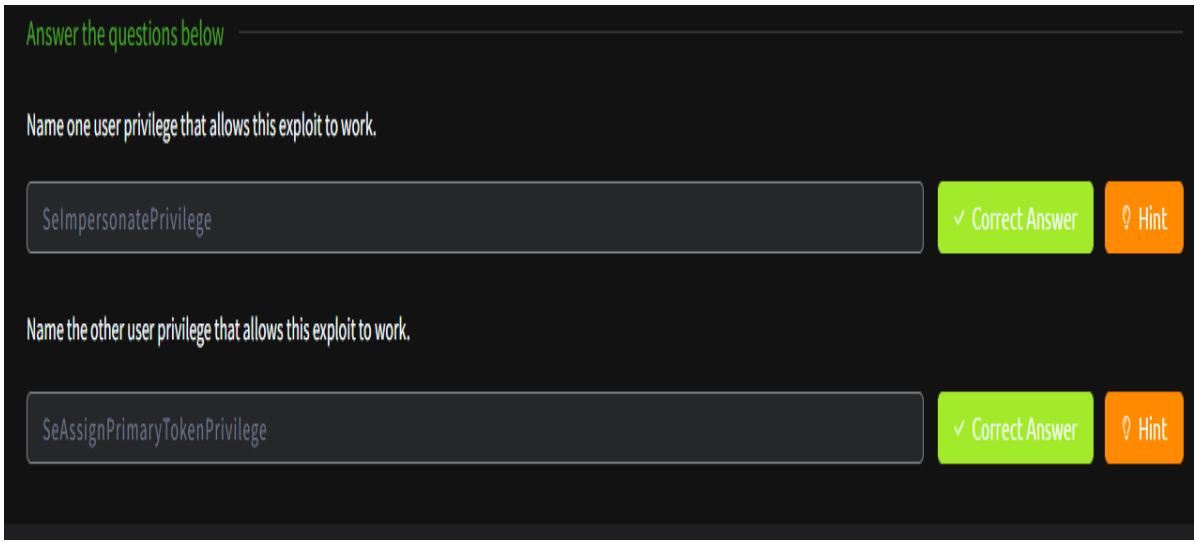


TASK16– VULNERABLEDRIVER EXPLOIT

- Identifiedkernel-modedriverwithlocalprivilegeescalationflaw.

- Compiledandexecutedexploittowritearbitrarydatato memory.

- ElevatedfromusertoSYSTEMusingcraftedexploit.



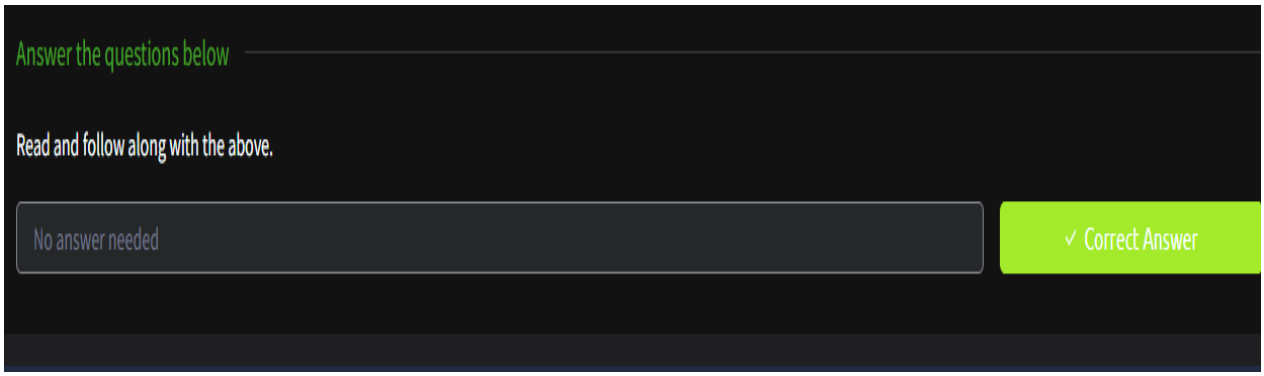
TASK17–ABUSINGINSTALLER PACKAGES

- FoundMSIorinstallerscriptsrunwithelevatedprivileges.

- Modifiedinstallertospawnshelloradduser.

- Raninstallertoachieveprivilege escalation.

- CapturedAdministratorflagonsuccess.



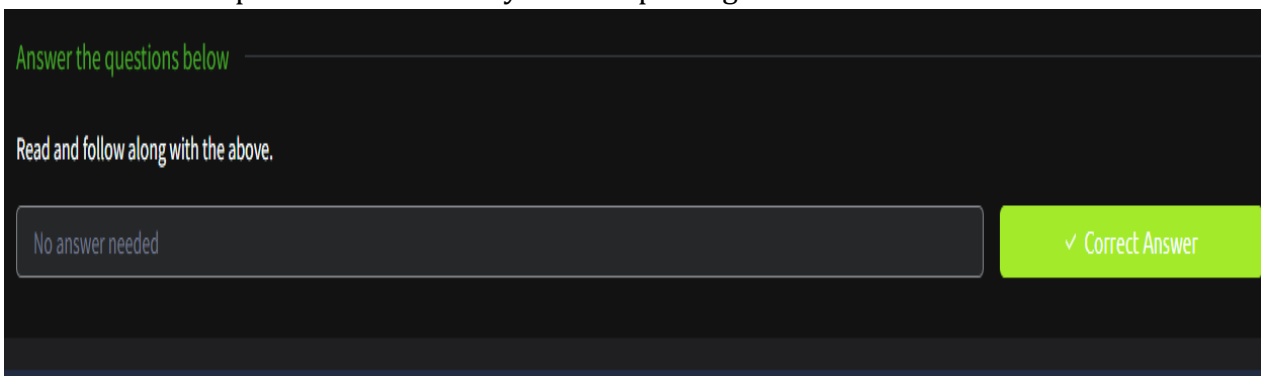
TASK18–CLEANUPAND PERSISTENCE

- Createdpersistencemechanismusingscheduledtasksorregistrykeys.

- Deletedevidencesuchasshells,tempfiles,and logs.

- Removedaddedusersandrestoredbinariestocover tracks.

- Documentedstepstakenforlateranalysisandreporting.



RESULT:

CompletedtheTryHackMe“WindowsPrivilegeEscalation”room,demonstrating multiple vectors for gaining elevated access on a Windows host. Learnt how to identify and exploit weak configurations, extract sensitive data, and manipulate services to gain control. Skills acquired are directly applicable to real-world penetration testing and red-team simulations.