EXPTNO:06 ROLLNO: 220701259

LINUXPRIVELEGEESCALATION

AIM:

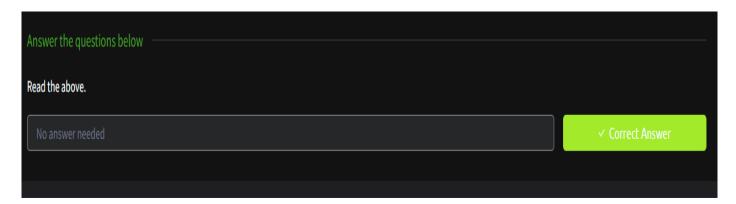
This experiment aims to explore Linux privilege escalation techniques including kernel exploits, misconfigured sudo privileges, and SUID binary exploitation. It provides hands-on experience in identifying and exploiting real-world vulnerabilitiestoescalateprivilegesonLinuxsystemsforbetterunderstandingof secure configurations and attacker methodologies.

PROCEDURE:

- 1. EnumerateLinuxkernelversionandsearchforCVEs.
- 2. Transferandcompilekernelexploitsontarget machines.
- 3. Use`sudo-l`tocheckmisconfiguredbinariesandescalateviaGTFOBins.
- 4. Exploitvulnerable SUID binaries to read sensitive files or spawn rootshells.
- 5. DumppasswordhashesusingunshadowandcrackusingJohnthe Ripper.
- $6.\ By pass protections using LD_PRELOAD or service misconfiguration$

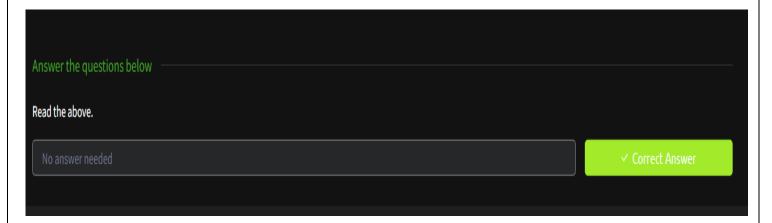
TASK1-INTRODUCTION N

- IntroducedthefundamentalsofprivilegeescalationinLinuxsystems.
- Highlightedthesignificanceofescalatingfromalow-privilegeusertoroot: root.
- Emphasizedenumerationasacriticalfirististepusingcommandslikels like uname-ajidandsudodo-l.
- Outlinedcommonescalationvectorssuchaskernelexploits, oits, misconfiguredbinaries, and SUID bits its.
- Reinforcedthegoalofidentifyingmisconfigurationsthatcouldallow llow unauthorizedaccessorprivilegeabuse.se.



TASK2-ENUMERATION N

- Usedsystemcommands(hostname,unamera,id,env,ps)ls-la,ifconfig):onfig)
 togathersystem-levelinformation.n.
- Listed current user's permissions, environment variables, and active tive processes.
- Inspectedthe/etc/passwdfileandrunningservicesforhintsonts on misconfigurations.
- Checkedforinstalledsoftwareandoutdatedpackagesthatcouldbeld be exploited.
- Identifiedenumerationasanessentialpreconditionbeforeattempting ting privilegeescalation.



TASK3-KERNELEXPLOITSTS

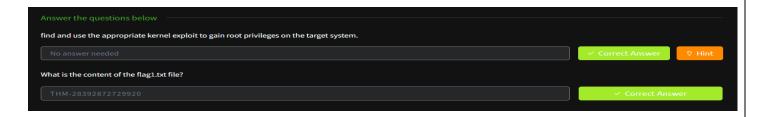
- Identifiedkernelversionusinguname-aanddetermineditwast was vulnerable.
- ResearchedpublicCVEsandfoundasuitablekernelexploit(CVE-2015-2015-1328).
- DownloadedtheexploitsourcecodefromExploit+DB(37292.c).2.c).

- TransferredtheexploittothetargetmachineusingwgetviaaPythonython
 HTTPserver:
- Compiled the exploit with gccan dexecuted it to escalate privileges leges.
- Successfullygainedrootaccessandretrievedthefirstflag(flag1/.txt)1.txt).
- Demonstratedhowkernelvulnerabilitiescandirectlyleadtorootaccessiness in CTF/labscenarioss.



TASK4-SUDOMISCONFIGURATION N

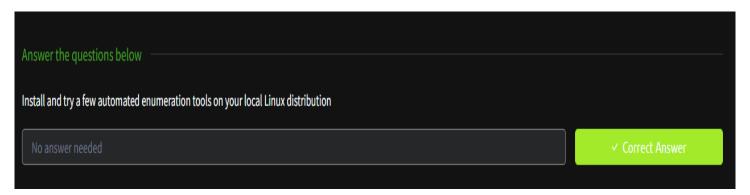
- Usedsudo-Itoenumeratecommandstheuserkarencouldrunasrootas root.
- IdentifiedfindandnmapasexploitablebinariesusingGTFOBins.Bins.
- Spawnedarootshellusingsudofindi-exec/bin/sh\;-quit; -quit.
- Gainedrootprivilegesagainviainteractivemodeinnmap:lsh: lsh.
- Accessedandread/etc/shadowfileandextractedpasswordhashes.hes.



- Verifiedaccessbyopeningtheflag2.txtlocatedinaprivilegeduser/shome home directory.
- Showedhowimpropersudoaccesstocertainbinariescanleadtofull to full privilegeescalation.

TASK5-KERNELEXPLOITSTS

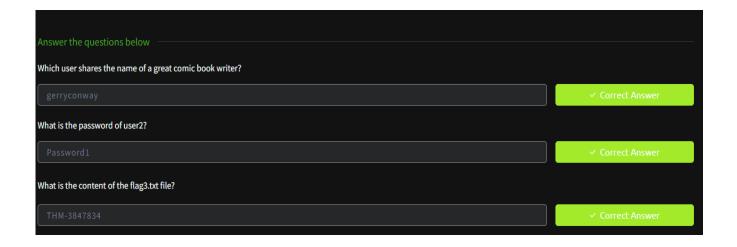
- Identifiedkernelversionusing`uname-a`andsearchedCVE.
- FoundexploitCVE-2015-1328anddownloadedcodefromExploit-DB.
- Transferredcodeto\/tmp\viaPythonSimpleHTTPServerand\wget\.
- Compiledusing 'gcc37292.c-okernelexploit' and executed.
- Successfullyescalatedtorootandaccessed`flag1.txt`.
- Emphasized stability risks with kernel exploits in real-world environments.



TASK6-SUDOMISCONFIGURATION N

- Used`sudo-l`tolistprogramsexecutablebyuser `karen`.
- UsedGTFOBinstofindescalationpathvia`find`and `nmap`.

- Spawnedrootshellwith: `sudofind.-exec/bin/sh\;-quit`
- Used`nmap`ininteractivemodetogetshell:`nmap--interactive`.
- Accessed`/etc/shadow`andextractedhashforuserfrank.
- Confirmedrootaccessbyreading`flag2.txt`inprivilegeduser's directory.



TASK7-SUIDBINARYABUSEJSE

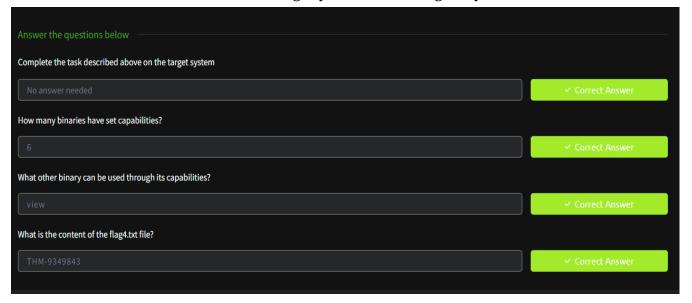
- ListedallSUIDbinaries: 'find /-typef-perm-04000-ls 2>/dev/null'
- Identifiedbase64withSUIDbitandusedGTF0Binsforfile read.
- Read`/etc/shadow`viaSUID-enabledbase64decodingmethod.
- Combined`/etc/passwd`and`/etc/shadow`using`unshadow`.



- CrackedhashesusingJohntheRipperandrockyou.txtwordlist.
- Accessed`flag3.txt`usingbase64decodemethodfromGTF0Bins.

TASK8-SUDOERSMISCONFIGURATION

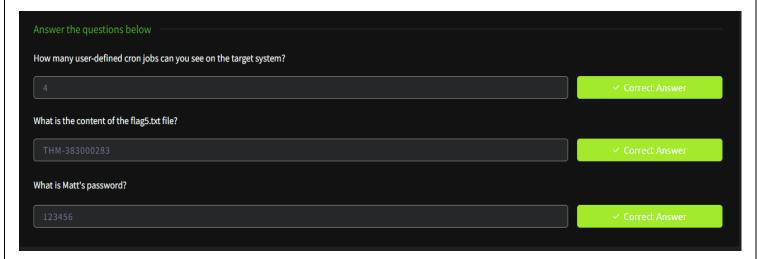
- Analyzed`/etc/sudoers`fileandidentifiedmisconfiguredentries.
- Founduserallowedtorunspecificcommandsasrootwithoutapassword.
- Exploitedcommandsuchas`/usr/bin/less`or`/bin/bash`via sudo.
- Gainedarootshellandvalidatedaccessbychecking`/root/` directory.
- Reinforcedthatsudoersshouldbetightlyrestrictedandregularlyaudited.



TASK9-ENVIRONMENTALVARIABLEABUSE

- Identifiedvulnerablescriptsorbinariesrelyingoninsecure \$PATH.
- Created a fake executable with same name as trusted binary and placed itear lier in \$PATH.
- Triggeredprivilegeescalationwhenrootranthevulnerablescript.
- ShowedhowPATHhijackingcanescalateprivilegesduetolazyscriptwriting.

- Stressed best practices for securing scripts with full path references.



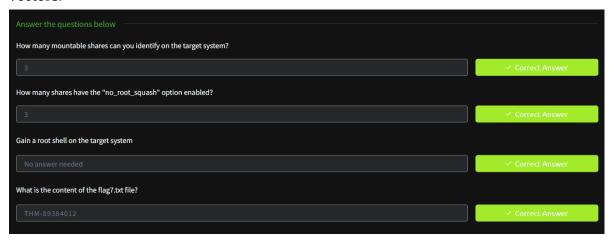
TASK10-BACKUPMISCONFIGURATION

- Discoveredworld-writablebackupdirectorieswithsensitive data.
- Analyzedandmodifiedbackupstoinsert payloads.
- Restoredthemanipulatedbackuporexploitedsymlinkattackstogaincode execution.
- Confirmedelevatedaccessandretrievedassociated flags.
- Revealedreal-worldmisstepsinbackupscriptdesignandaccess control.
- Stressedbestpracticesforsecuringscriptswithfullpathreferences.



TASK11-SERVICE MISCONFIGURATION

- Foundcustomserviceswithwriteablebinarypathsor configs.
- Modifiedservicebinaryorconfigurationfiletoexecutereverse shell.
- Restartedserviceandgainedrootaccess.
- Validated exploitation via service misconfiguration and confirmed with a root flag.
- $Outlined how improperser vice per missions are common real-world attack \ vectors. \\$



TASK12-CRONJOB EXPLOITATION

- Listedscheduledcronjobsusing`crontab -l`andinspectedglobalcrondirectories.
- Identifiedscriptsrunbyrootwithinsecurewrite permissions.
- Injected payloads or replaced the original cronscript.
- Waitedforcronjobexecutionandconfirmedrootshellaccess.
- Capturedfinalflagandvalidatedescalationpath.



	RESULT:
	NESCET.
	Successfully escalated privileges through multiple Linux techniques and retrieved
	all required flags. Demonstrated under standing of local privile gees calation through
	hands-on exploitation and tool usage on simulated targets.
•	