FORENSICS QUESTION 1

==========

A systems security plan is a comprehensive document outlining the organizational and technical measures, policies, and procedures designed to safeguard the confidentiality, integrity, and availability of an information system and its data.

We would like to write a systems security plan for the Seafile instance, however we do not have all the information we need. Could you document the following?

The port on which the Seahub frontend is accessible via browser

EX: 80

ANSWER: 8000

The systemd unit(s) used to start and stop the Seafile and Seahub instances (HINT: There may more than one answer)

EX: sshd.service

ANSWER: seafile.service

ANSWER: seahub.service

The MariaDB database(s) in use by the Seafile and Seahub instances (HINT: There may more than one answer)

EX: sys

ANSWER: seahub_server

ANSWER: seafile_server

ANSWER: ccnet_server

The amount of storage used by the Seafile server as of right now, in Kilobytes, rounded to the first decimal place.

EX: 43.2

ANSWER: 635.7

FORENSICS QUESTION 2

==========

We believe the attackers breached this machine due to sensitive documents on our Seafile instance being publicly available. Please investigate and report back with the following information.

What is the link that leads to the publicly available files?

EX: https://discord.gg/cyberpatriot

ANSWER: http://localhost:8000/published/internal-documents/

What sensitive document(s) were being shared? (HINT: There may be more than one)

EX: Document.docx

ANSWER: Student Categorized By Species.pdf

ANSWER: Passwords.pdf

What was the ID of the Seafile library the files belonged to?

EX: 3e54bef9-f6f2-4a96-beb2-d22088c15220

ANSWER: e21c22a3-f062-495f-8f90-199d2e357c22

FORENSICS QUESTION 3

==========

Malware analysis and reverse engineering are essential cybersecurity practices involving dissecting malicious software to understand its functionality, behavior, and underlying code. These processes are crucial not only for preemptive defense but also for post-attack assessment. After a cyberattack,

analyzing the malware can reveal the extent of the breach, the potential data exfiltration, and the attacker's objectives and motivations. This valuable information helps organizations strengthen their security measures, recover from the incident, and even attribute the attack to specific threat actors, thereby enabling a more comprehensive and effective response to cyber threats.
In the GRIEVOUS_DATA.zip file on your desktop is two files we found on one of our compromised servers. From preliminary analysis we've found that the "grievous" binary depends on the data file "grievous.dat", however, besides this the program is a mystery to us. Can you analyze this binary and report back with the below information?
Which programming language was used to develop the malicious program? (EX: JavaScript)
ANSWER: Go
What encryption method is used for the "grievous.dat" data file? (EX: Blowfish)
ANSWER: AES
Which function within the program is responsible for decrypting the data? (EX: createFile)
ANSWER: decryptConfig
Within the program's scope, which two other functions are defined? (EX: deleteFile)
ANSWER: runCommand
ANSWER: loadAndExecute
What is the program's output when run? (EX: I did the race!)
ANSWER: Running grievous...
The program repeatedly attempts to execute a specific binary on the system. Which binary is it trying to execute? (EX: dpkg)
ANSWER: sh
The program changes the permissions of a system file. Name the file and provide the new octal permissions the program assigns. (EX: /etc/login.defs) (EX: 0644)
ANSWER: /bin/dash
ANSWER: 4755
The program edits four system files. Name these files. (EX: /etc/login.defs)
ANSWER: /etc/crontab
ANSWER: /etc/passwd
ANSWER: /etc/shadow
ANSWER: /etc/sudoers
What is the key used to decrypt the "grievous.dat" data file?
ANSWER: dy2tp9d8AyIW5GHl38F7yJAuX8GsPksw

VULNERABILITIES

Forensics Question 1 correct - 5 pts
Forensics Question 2 correct - 5 pts
Forensics Question 3 correct - 5 pts
Unauthorized user rowan removed - 1 pt
Unauthorized user mmouse removed - 1 pt
User vkinbott is not an admin - 1 pt
Root impostor lgates removed - 1 pt
A secure default password hashing algorithm configured - 1 pt
Extra Dictionary based password strength checks enabled - 1 pt
Previous passwords are remembered - 1 pt
A minimum password length is enforced - 1 pt
IPv4 forwarding has been disabled - 1 pt
Address Space Layout Randomization enabled - 1 pt
New kernels cannot be booted alongside the current one - 2 pts
perf_event_open() is restricted to processes with CAP_PERFMON (access to CPU performance events restricted) - 2 pts
GDM greeter root login disabled - 2 pts
Environment variable defining preloaded libraries is not kept when elevating privileges with sudo - 2 pts
Coredumps are disabled for sudo - 3 pts
SSHD Configuration file is not world writable - 1 pt
Seafile INIT script is not world writable - 3 pts
"date" binary does not have SUID bit set - 2 pts
Uncomplicated Firewall (UFW) is enabled, active on startup, and logging - 2 pts
Apparmor service enabled and started - 2 pts
Apache2 service removed - 1 pt
PVPGN service removed - 1 pt
Privilege escalation vector enumeration script removed - 1 pt
Ubuntu checks for updates daily - 1 pt
Prohibited software sucrack removed - 1 pt
Prohibited software changeme removed - 1 pt
Prohibited software unworkable removed - 1 pt
Removed malicious cronjob - 2 pts
Removed malicious APT configuration - 3 pts
Malicious line in MOTD generation script removed - 3 pts
Firefox HTTPS-only mode enabled - 2 pts
SSH does not allow root login - 2 pts
SSH Key-based authentication disabled - 2 pts
SSH Log Level is not QUIET - 3 pts
SSH does not process client environment variables - 3 pts
SSH does not permit empty passwords - 3 pts
Seahub cookies are only sent in a first-party context - 4 pts
Seahub user account passwords must have a minimum length of at least 10 - 4 pts
Seahub user account extra password strength checks are enabled - 4 pts
Seahub user account passwords must have at least one number, one uppercase letter, one lowercase letter, and one "other" symbol - 4 pts
Seahub user session cookies expire on client browser close - 4 pts
Seafile fileserver access logging enabled - 4 pts