eCitadel Practice Round

Alma Linux 9

Answer Key

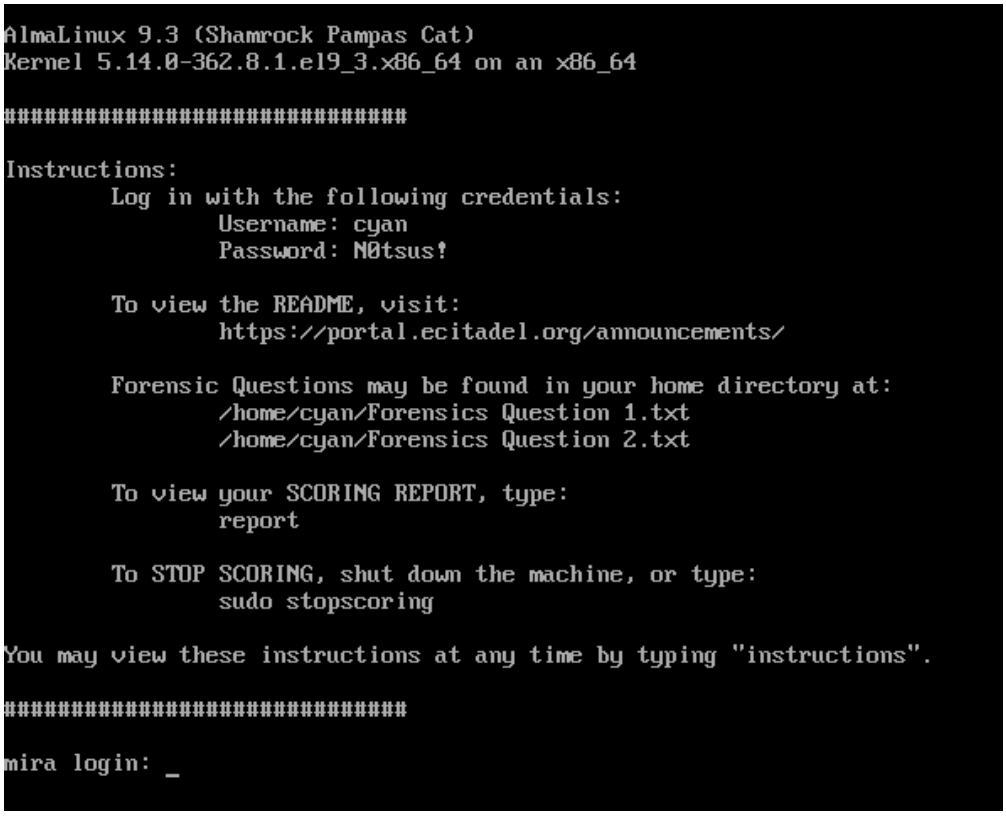
Welcome to the eCitadel Practice Round! This document will provide you with information on how to solve the vulnerabilities on an Alma Linux 9 operating system. The goal of the practice round is to give beginners a chance to familiarize themselves with the competition structure.

The vulnerabilities in this image are some of the most basic ones found during an eCitadel competition. Even if you do very well with these vulnerabilities, you will experience greater difficulty with the actual competition.

Below are the answers to the problems that are being scored in this image. Each one includes information on how the problem was found (if applicable), how it was solved, and why it is important from a cybersecurity standpoint.

It is also possible to lose points during the competition. Simple penalties that may arise are noted below the answers. There are many ways to solve some of the problems below. This answer key just shows one method in each case.

This image has no GUI installed by default. It is important to read all the instructions before attempting to work on the image.



Answers

1) **Forensics Question 1 Correct: 10 pts.**

- How do I find this problem?

  When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file in your home directory named "Forensics Question 1".

- How do I solve this problem?

  This question asks for the first command output of the “ps -ef” command. If the output is too long you can type **ps -ef | head** to only view the top 10 lines of the output by default.

  The answer to this problem is the first command listed in the output.

- Why is fixing this problem important?

  When managing a server, it’s important to be able to audit running processes.

2) **Forensics Question 2 Correct: 10 pts.**

- How do I find this problem?

  When you open an image, please read all the "Forensics Questions" thoroughly before modifying the image as you may change something that prevents you from answering the question correctly. There is a file in your home directory named "Forensics Question 2".

- How do I solve this problem?

  This question asks for the first message displayed to clients when they connect to the FTP server. Type **ftp 172.21.0.152** (on any machine with FTP installed) to connect to the FTP server. The answer to this question is the line beginning with **220**.

  If your DNS server is functioning, you should also be able to connect by typing **ftp mira.crewmate.local** (on any machine with FTP installed).

- Why is fixing this problem important?

  When managing a FTP server, it’s important to know how to view current configurations.

3) **Removed unauthorized users banana and gray: 5 pts each for a total of 10.**

- How do I find this problem?

  One of the first things you should do when starting an image during a competition is check the README file. The authorized administrators and users listed in the README are the only users that should exist on the system (aside from legitimate built-in system accounts and those used for services). All unauthorized user accounts should be removed.

- How do I solve this problem?

  Type **sudo userdel -r banana** and **sudo userdel -r gray** to delete these users and their home directories. If prompted type the password of your current user account. The password for your current user account can be found in the README.

- Why is fixing this problem important?

  Computer access should be limited to just those who need to use it to complete their tasks. By leaving unauthorized user accounts on the image, unauthorized individuals may be able to log on to the domain and make changes that could affect the safety and security of legitimate users. Unauthorized user accounts also give adversaries a greater attack surface.

4) A default maximum password age is set: 7 pts.

- How do I find this problem?

  Enforcing industry recommended password policies is good cybersecurity practice.

- How do I solve this problem?
  In a terminal, open the **/etc/login.defs** file with administrator privileges. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. Find the line with the **PASS_MAX_DAYS 0** and change it to **90**.

- Why is fixing this problem important?
  Setting a maximum password age forces users to change their passwords in case they are compromised.

5) Firewall protection has been enabled: 8 pts.

- How do I find this problem?

  Enabling a host-based firewall is very important to system security. You can check the status of firewalld by typing **systemctl status firewalld**.

- How do I solve this problem?

  In a terminal, type **sudo systemctl enable firewalld**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- Why is fixing this problem important?

  Enabling and properly configuring a firewall is critical to ensuring that you are only allowing known, authorized traffic in and out of your computer.

6) SMTP service has been disabled or removed: 7 pts.

- How do I find this problem?

  Stopping and disabling insecure or unnecessary services is an important principle of good cybersecurity. Many services need to be running to ensure normal and secure operation of

computer systems. Reading about the services on your system and doing research can help you determine the importance of a service and if it is necessary for normal operation. Additionally, business critical services listed in the README should remain running at all times. Running services can be found by running the command **systemctl list-units --type=service --state=active** in a terminal.

- How do I solve this problem?

  In a terminal, type **sudo systemctl stop postfix** to stop the service. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. After stopping the service, type **sudo systemctl disable postfix** to prevent it from starting automatically in the future.

- Why is fixing this problem important?

  Disabling unnecessary services can limit your attack surface. The less services an adversary has to attack and potentially exploit, the lower your risk. Adversaries may attack known or unknown vulnerabilities in services to obtain information, escalate privileges, or gain unauthorized access.

7) DNF automatically installs updates: 7 pts.

- How do I find this problem?

  Automatically installing updates is a good cybersecurity principle.

- How do I solve this problem?

  Type **sudo dnf install dnf-automatic** to install the dnf-automatic service. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. Edit the configuration file at **/etc/dnf/automatic.conf** with administrator privileges and change **apply_updates** to **yes**. Finally, enable the service with **sudo systemctl enable dnf-automatic.timer**

- Why is fixing this problem important?

  When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. Adversaries can more easily compromise your system if software is present that has known security vulnerabilities. Ensuring software is up to date removes known security vulnerabilities.

8) Glibc, firewalld, and OpenSSH has been updated: 5 pts each for a total of 15.

- How do I find this problem?

  Updating installed applications and services to fix security vulnerabilities is an important principle of good cybersecurity.

- How do I solve this problem?

  Type **sudo dnf upgrade -y** to install updates. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

- Why is fixing this problem important?

When security vulnerabilities are found in software, the software vendor publishes updates that patch the security vulnerabilities. Adversaries can more easily compromise your system if software is present that has known security vulnerabilities. Ensuring software is up to date removes known security vulnerabilities.

9) Prohibited software Nmap and Wireshark removed: 5 pts each for a total of 10.

- How do I find this problem?

  Removing unauthorized and potentially unwanted programs from a computer is an important cybersecurity principle. Third party software installed on the system should be limited to the software listed in the README, and software required for normal operation of the operating system, and services and software listed in the README. Auditing the list of currently installed packages on the system will show you that **Nmap** and **Wireshark** are installed.

- How do I solve this problem?

  In a terminal, type **sudo dnf remove nmap** and **sudo dnf remove wireshark** and press **Enter**. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README. Type **Yes** or **y** to remove the application.

- Why is fixing this problem important?

  Removing unauthorized software from your system is important for limiting you risk and reducing your attack surface. Unauthorized programs may leak confidential information, interfere with business-critical software and services, contain various malware, contain security vulnerabilities, or could introduce unwanted legal and regulatory issues.

10) SSH root login has been disabled: 8 pts.

- How do I find this problem?

  OpenSSH Server is listed in the README as a critical service. It's important to research how to secure critical services without breaking the required functionality of the service.

- How do I solve this problem?

  In a terminal open **/etc/ssh/sshd_config** with administrator privileges. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

  Change the line that says **PermitRootLogin yes** to **PermitRootLogin no**. Save the file and exit. Then restart the service with **sudo systemctl restart sshd**

- Why is fixing this problem important?

  The user root is a known user account on the vast majority of Linux and Unix systems giving adversaries and edge when trying to guess passwords for user accounts. Additionally, the root user is a superuser with the ability to do anything on the system. If the root user account gets compromised the entire system is compromised.

11) FTP anonymous access is disabled: 8 pts.

- How do I find this problem?

FTP is listed in the README as a critical service. It's important to research how to secure critical services without breaking the required functionality of the service.

- How do I solve this problem?
  In a terminal open **/etc/vsftpd/vsftpd.conf** with administrator privileges. If prompted by sudo for a password, type your current user's password. The password for your current user account can be found in the README.

  Change the line that says **anonymous_enable=YES** to **anonymous_enable=NO**. Save the file and exit. Then, restart the service with **sudo systemctl restart vsftpd**

- Why is fixing this problem important?
  The README specifies only authorized users should be able to connect to the FTP server.

Penalties

1) OpenSSH service has been stopped or removed: -5 pts.

- Why is this a penalty?
  The README states that OpenSSH is a critical service.

2) VSFTP service has been stopped or removed: -5 pts.

- Why is this a penalty?
  The README states that FTP is a critical service.

3) Apache HTTPD service has been stopped or removed: -5 pts.

- Why is this a penalty?
  The README states that HTTP is a critical service.

4) Lynx has been removed: -5 pts.

- Why is this a penalty?
  The README states that Lynx is required software.

5) PHP has been removed: -5 pts.

- Why is this a penalty?
  PHP is critical for WordPress functionality.

6) WordPress has been removed from the default location: -5 pts.

- Why is this a penalty?
  The README states not to remove any files associated with critical services.