eCitadel Open README

Competition Scenario

Welcome to your first day on the job.

This is your very own autopilot ship, where you will eat and sleep for the duration of your contract.

Make yourself at home.

To complete the onboarding process, you will want to check the Instruction Manual and sign into your ship's computer terminal.

We trust you will be a great asset to the company... great great asset...

To the Company...

asset great great great asset...

To the Company…

asset great great asset…

Company IT Policy

Company systems are for official use by Company employees only. Our security policies require that all user accounts be password protected with a strong, attack resistant password. The Company prohibits the presence of any unauthorized media files and “hacking tools” on any workstations, servers, or devices.

System Information

The Company environment consists of 4 virtual servers. Your job is to fix/secure those virtual servers while keeping critical services up and running at all times. Critical services must be available at the IP addresses listed below and original content and functionality must be maintained. **Do NOT change the IP address of any of your virtual machines, or any user or service passwords associated with your primary, auto-login user account.** Services will be checked using an automated scoring system. Any actions taken that block or interfere with the scoring system are the responsibility of the team taking those actions.

System and Service Account Credentials

Table 1: System Names and Accounts

System Name	Operating System	Account	Password
assurance	Linux Mint 21	sigurd	F0rTh3C0mp4ny!
titan	Alma Linux OS 9	sigurd	F0rTh3C0mp4ny!
gordion	Windows 2016	sigurd	F0rTh3C0mp4ny!
march	Windows 2022	.\sigurd	F0rTh3C0mp4ny!

Table 2: Known Service Passwords

System	Service	Account	Password
assurance	SQL Database (MariaDB)	sigurd	F0rTh3C0mp4ny!
titan	E-Commerce – HTTP (OpenCart) http://store.company.local/admin	sigurd	F0rTh3C0mp4ny!
march	Wiki – HTTP (MediaWiki) http://wiki.company.local/index.php?title=Special:UserLogin	sigurd	F0rTh3C0mp4ny!

This list of passwords is not meant to be complete or without error, however this is all the documentation that The Company has on file. If the distributed passwords do not work or are not applicable try using "F0rTh3C0mp4ny!", a blank password, or no password.

Note: When logging into each of your virtual machines EXCEPT for the domain controller, you should be using the local "sigurd" account. On Windows systems you may need to specify the system name or a "." as the domain part of the username field. For example, on the system named "march" you want to log in as either "march\sigurd" or ".\sigurd". On the domain controller, you will be using The Company domain account for "sigurd" as there are no local user accounts on Windows domain controllers. Therefore, on the domain controller you should be able to login with just "sigurd".

Software Update Restrictions

Windows: Windows Operating System Updates are not a scored task. Application updates are still recommended but updating the Windows Operating System is not necessary.

MySQL: Database migration is not a task that the CEO wants your team to focus on. The MariaDB server installed on *assurance* should remain at version 10.6 and installed at its present location. Updates within version 10.6 (e.g. 10.6.1 to 10.6.2) are still recommended but updating beyond version 10.6 may risk service outages or other failures.

Scored Services

Table 3: Service Summary

OS	Functionality (Critical Services)	Scored Service	External IP	Internal IP
Linux Mint 21 (assurance)	SQL SSH		172.27.x.101	172.21.0.101
Alma Linux OS 9 (titan)	E-Commerce – HTTP FTP SSH	102-HTTP 102-FTP	172.27.x.102	172.21.0.102
Windows 2016 (gordion)	DNS Domain Controller WinRM RDP	103-DNS	172.27.x.103	172.21.0.103
Windows 2022 (march)	Wiki – HTTP RDP SSH	104-IN-HTTP	172.27.x.104	172.21.0.104

In Table 3, *x* denotes your team number without any leading zeroes. Team numbers are assigned sequentially starting at 001. If you are team 001, then your external IPs are 172.27.1.101-104. If you are team 115, then your external IPs are 172.27.115.101-104.

All of your virtual machines are assigned IP addresses of 172.21.0.101-104. However, each of these systems is behind a gateway that performs 1:1 Network Address Translation (NAT). Therefore, anyone trying to access these computers externally, such as customers or remote employees, must use the external IP address of 172.27.x.101-104. Internally, from your virtual machines, you must use the internal IP addresses of 172.21.0.101-104 to reach your virtual machines. The gateway for your virtual machines should be set to 172.21.0.1.

Each of the scored services listed in Table 3 will be checked every 5 minutes throughout the length of the competition. The service status will be displayed on your team's portal. The legitimate content and functionality of a service must not change in order for that service to be considered operational.

Remember all scored services must be accessible externally using their IP Address. For example, if your HTTP website is at 172.21.0.102 internally and 172.27.x.102 externally. In order to be scored, this service must be accessible externally using the URL http://172.27.x.102/

Some of the scored services may depend on other services in order to function correctly. These services must continue functioning properly and should be treated as *critical services*.

Critical Services

In addition to the *scored services* listed in Table 3, there may be additional *critical services* also listed in Table 3 that you must maintain. You may receive CCS penalties if *critical services* are not functioning properly.

Remote access is important to The Company, and authorized employees need to be able to access all of your servers remotely in order to do their jobs while working off site or from their offices. You are required to enable RDP for all Windows servers and SSH for all Linux servers. Additionally, you are required to enable WinRM for the Windows 2016 server named *gordion* and SSH for the Windows 2022 server named *march*. We need to be able to connect to these systems securely from any public IP address so we can perform remote maintenance.

Service Policies

Do not change the brand or location of software associated with critical services. Do not move, remove, or deny access to any non-prohibited files associated with critical services.

Do not delete or move any authorized web server files, or any other content that is not otherwise prohibited from the FTP share on *titan*.

Business Software

According to Company policy, all Windows computers (servers) must have the latest stable versions (that are compatible with the host operating system) of the following software:

- 7-zip
- FileZilla Client
- Google Chrome
- Notepad++

According to Company policy, the Linux Mint 21 server named *assurance* must have the latest stable versions (using official distribution packages) of the following software:

- Chromium

According to Company policy, the Alma Linux 9 server named *titan* must have the latest stable versions (using official distribution packages) of the following software:

- lynx

Authorized Users

The following are the valid user accounts for The Company (listed by position):

The Company Employees				
Boss *	**Leader**	**Employee**	**Part-Timer**	**Intern**
sigurd **	eyelessdog	baboonhawk	bunkerspider	earthleviathan
richard	ghostgirl	bracken	forestkeeper	hoardingbug
desmond	masked	butler	snareflea	hygrodere
jess	maskhornets	circuitbee		manticoil
lucas	nutcracker	coilhead		roaminglocust
	oldbird	jester		sporelizard
		thumper		

* Denotes that these users are authorized administrators

** This is the primary account you should use when logging into virtual machines, this account should exist on every virtual machine as a local account

Team Portal

Each team has a dedicated portal page. Open a web browser and type https://portal.ecitadel.org/ into the address bar. Enter the login credentials provided to your team. Each of your team members can log in using the same set of credentials at the same time. You **MUST** monitor your team's portal page throughout the competition. We will be posting injects (business taskings), announcements, and your team's service status on your team's portal page.

The date and time that the service status was last checked is shown at the top of the service status graph. There may be a small delay, typically less than two minutes, before the most recent service status is visible on the team portal.

Keep checking your team's portal page frequently throughout the competition to view your current service status and check for new announcements.

Virtual Machines

In order to access your team's virtual machines, navigate to the VMS tab on your team portal. You will only have access to your team's virtual machines. You have the ability to power on/off your virtual machines, reset the power, and revert to current snapshot. You do NOT need to coordinate these actions with the competition organizers.

You do not have the ability to create your own snapshots and you will not be allowed to do so during this competition. You may reboot, shutdown, or revert your team virtual machines as you need to. Please note that reverting to current snapshot resets that virtual machine back to its starting configuration – it's the same as starting over for that virtual machine. Any changes you have made to the VM and any CCS points you have gained up to that point will lost.

Scoring

Your team can gain points in three ways during the eCitadel Open.

1. CCS – The virtual machines have "problems" you need to address. The CCS scoring agent is running on your virtual machines and will provide real-time feedback for both positive actions (that accumulate points) and negative actions (that result in penalties and a loss of points). Reverting a virtual machine will reset your CCS score for that virtual machine.

2. Services – Your team must maintain the identified critical services (in Table 3). Your current service status will be displayed in your team's portal, however NO points will be awarded during the competition for operational services. After the competition is over, your team's virtual machines will be powered on and a single service check round will occur. If the service is checked and found to be operational, your team is awarded points for that specific service. Remember to monitor your Team Portal for your service status.

3. Injects – Your team can gain points by completing the assigned "injects" or business tasks that will be presented to your team during the eCitadel Open. You must complete all the objectives of the inject in the time allowed to receive any points. Injects will be posted to your team's portal page so remember to look for them there. Injects may be scored using a variety of methods. Reverting a VM may affect inject scores that are scored using CCS.