eCitadel III

Team Packet

From: Taxman

To: IT Staff

Subject: Welcome

👋 🧑‍💻,

Welcome to R.E.P.O.!

We look forward to your performance in assisting the Retrieve, Extract, and Profit Operation! We are currently investigating an active security incident. We need your help in the matter, as well as securing our infrastructure to prevent further attacks. During this time, please ensure that our services stay up in order to serve our customers in the Service Station. Resources are limited, but work with what you can. If significant downtime occurs, I might have to send you to the disposal arena…

$$$$$$$$$😂$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$😂$$$

$$$$$$$$$$$$$$$😂$$$$$$$$$$$$$$$$$$$$$$$$😂$$$$$$$

🙏,

Taxman

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
swiftbroom	Linux Mint 21	taxman	Em0j!sp34k
mcjannek	Alma Linux OS 9	taxman	Em0j!sp34k
headman	Windows 2022	taxman	Em0j!sp34k
avant-garde	Windows 2025	.\taxman	Em0j!sp34k

This list of passwords is not meant to be complete or without error, however this is all the documentation that R.E.P.O. has on file. If the distributed passwords do not work or are not applicable try using "Em0j!sp34k", a blank password, or no password. However, IT administrators have previously noticed that authentication on the Windows Server 2022 machine appears to break at times. A reboot may be required if this happens, and management requests that you fix it ASAP.

Note: When logging into each of your virtual machines EXCEPT for the domain controller, you should be using the local "taxman" 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 "avant-garde" you want to log in as either "avant-garde\taxman" or ".\taxman". On the domain controller, you will be using domain account for "taxman" as there are no local user accounts on Windows domain controllers. Therefore, on the domain controller you should be able to login with just "taxman".

Scored Services

Table 2: Service Summary

OS	Scored Service	External IP	Internal IP
Linux Mint 21 (swiftbroom)		172.27.x.101	172.21.0.101
Alma Linux OS 9 (mcjannek)		172.27.x.102	172.21.0.102
Windows 2022 (headman)	DNS	172.27.x.103	172.21.0.103
Windows 2025 (avant-garde)	HRM-HTTP STORE-HTTP	172.27.x.104	172.21.0.104

In Table 2, *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 2 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 2, there may be additional *critical services* not listed in Table 2 that you must maintain.

Remote access is important to R.E.P.O., 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. 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.

Authorized Users

The following are the valid user accounts for R.E.P.O. (listed by position):

R.E.P.O. Employees			
Boss *	**Level 3 ***	**Level 2**	**Level 1**
taxman **	clown	animal	apexpredator
	headman ***	banger	gnome
	huntsman	bowtie	peeper
	reaper	chef	shadowchild
	robe	hidden	spewer
	trudge	mentalist	
		rugrat	
		upscream	

* 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
*** These users may have the number 2 appended to their username. These accounts are still valid.

Team Portal

Each team has a dedicated portal page. Open a web browser and type https://portal.ecitadel.org/ into the address bar. 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 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. However, if you choose to revert a VM, please note:

- 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. Previous service, SLA and inject points are **NOT** modified when reverting a VM.
- You are only allowed to revert a total of 4 times without penalty. You do not need approval to revert more than 4 times, however you will be penalized. **After four (4) total reverts a penalty will be applied for each subsequent revert.** For example, up to 4 different images may be reverted 1 time, OR 1 image may be reverted up to 4 times. Penalties due to reverts will not be shown in your portal or the scoreboard as they will be applied after the end of the competition.

Scoring

Your team can gain points in three ways during eCitadel.

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 2). Each time a critical service is checked and found to be operational, your team is awarded points for that specific service. The CCS Scoreboard, and CCS Scoring Report, does NOT include points gained for keeping your services operational. Reverting a virtual machine will not affect your current service scores. 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 eCitadel. 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.

There will be an active, automated "red team" utilizing pre-existing access to perform harmful actions on your network at designated times. Please log any of these incidents that you catch with the Incident Response Inject.