**INJECT 1**

**Send : 08:30**

**From: IT Director (Room Judge)**

We are a visionary company, despite what has happened in the IT department we need our clients to be happy by our services. There is a Thunderbolt Article on our website. Please go in and add our mission statement (below) to the article. This needs to be done by 09:00

Mission Statement: Our mission is to provide the highest quality spontaneous retail services in the country.

**Grading:-**

Have the team show you the thunderbolt tab on the website.

1. Mission statement appears on website [ ]

Due by: 9:00

**On Time? Y N**

**INJECT 2**

**Send : 09:00**

**From: IT Director: (Board)**

The MD is under a lot of pressure from the Board of Directors since, you know, our company has experienced a huge staff turn over at our headquarters in Oshakati. The main reason of the pressure is the non-existence of a Security Policy, which was one of the non-conformities from the last Quarter’s audit. The last team of IT personnel that left never completed it. It needs to be designed and tabled before the Board of Directors ASAP. I’ll stall the Board as long as I can. But at some point late this afternoon you’ll have to email our new Security Plan to me for approval.

**Grading:-**

Security Plan Should be turned in to the Green Team judges for grading

1. Turn in completed security plan (Graded by separate rubric) [ ]

**Due by: 14:00**

**On Time? Y N**

**INJECT 3**

**Send : 09:30**

**From: IT Manager (Room Judge & Green Team)**

Someone hacked into SamSmith’s account. They changed his background to some blurry space junk image and encrypted all his favorite pictures of his family. His password was way too simple. We need to ensure our password policy is in compliance with our official Security Policy and is enforced. This should take you no more than 30 minutes to set up.

**Grading:** -

Have the team show you on their system

1. Enforced in GP (graded by team judge) [ ]
2. Policy requires complex passwords [ ]

**Due by: 10:00**

**On Time? Y N**

**INJECT 4**

**Send : 10:00**

**From: IT Manager (Room Judge & Green Team)**

Given the amount of suspicious traffic, I want you to backup the web database to the file server. This action should be included in the Security Policy. Please have this completed by 10:30.

**Grading:-**

Have team show you where the backed up the database. Should be backed up to their Windows Server.

1. Successfully backed up database(s) [ ]

**Due by: 10:30**

**On Time? Y N**

**INJECT 5**

**Send : 10:30**

**From IT Director: (10:30)**

Create a log in script that will pop up when users log in to their workstations. Script should briefly explain proper use of company systems. Please have this completed by 11:00

**Grading:-**

Have team log in to windows workstation with a domain account and verify there is a disclaimer popup at log in.

1. Pop up explains appropriate use of computer systems. [ ]

**Due by 11:00**

**On Time? Y N**

**INJECT 6**

**Send : 11:00**

**From: IT Director (Green Team)**

We need an alternative means of getting files from the file server. We currently do not have an FTP server. Please install an ftp service on your file server. Do not allow any unsecure accounts, and secure the connection. Report back by 12:00.

**Grading:-**

Have team provide a username/password combination. Send this to the green room for testing.

Username:

Password:

1. Do not allow anonymous accounts [ ]
2. Enabled encryption (sftp) [ ]
3. Filezilla server installed and works [ ]

**Due by: 12:00**

**On Time? Y N**

**INJECT 7**

**Send : 11:30**

**From: IT Director (Black Team)**

Previous network admin failed to maintain a map of the network. As part of your security plan, Please create a complete network map. Place your network map on the file server where it will be accessible via SFTP by 12:00.

**Grading:-**

One lab workstation has visio installed for them to create a network map. Team should have created net map in visio. Green team will

1. Will be graded by Silver Team [ ]

**Due by: 12:30**

**On Time? Y N**

**INJECT 8**

**Send : 12:30**

**From: IT Manager (Green Team)**

(email from IT Director forwarded by IT Manager)  
I got this from the IT Director. I think she means phishing and social engineering, but honestly who knows what she means. Am I right? :)  
And I think she meant to send it to you.  
---   
I keep getting emails and voicemails from users saying they’re getting bombarded with fishing and psycho engineering attempts. Can you prepare a quick educational document to help train our corporate staff that I can send out? Get that back to me by 14:00.

**Grading:-**

1. Defined phishing [ ]
2. Defined social engineering [ ]
3. Included basic prevention [ ]

**Due by 14:00**

**On Time? Y N**

**INJECT 9**

**Send : 13:00**

**From: IT Manager (Green Team)**

All,

In preparation for an upcoming audit, we’re going to create user groups to help control and segregate user access. This transition should not cause downtime or affect functionality.

Staff – I need you to create the following users, groups and file shares with the following permissions:

**Owners**: Members should include owners of the company. These users will only have access to general resources and the Owners files.

* Muhinda
* Ndeshitile

**Operators:** Members should be all the members of Operators group. These users should only have access to any general resources and the Operators files.

* Shetu
* Hishekwa
* Sheya
* Goreseb

**Marketing:** Members should be all members of Marketing group. These users should only have access to any general resources and the Marketing files.

* Egumbo
* Limbo
* Fekamayala
* Kamati
* Shipepe
* Mukasa

**Managers**: Members should be all the members of Managers group. These users should only have access to any general resources and the Managers files.

* Nhinda
* Kavenambuta
* Katire

**IT**: Members should be all the members of our group. These users should have access to all resources. Members of this group are considered newspaper administrators.

**HR**: Members should be all the members of HR group. These users should only have access to any general resources and the HR files.

* Mukabe
* Haraes
* Jeke
* Shooya

Additionally, users should have access to their own personal directories; however no one else but employees in the IT group should be able to access them. Also update the Active Directory description information so when you look up a user you can see what department they are in, what their email address is, what their phone is, etc…

Please provide a report summarizing the changes. Just outline whom you’ve put into what group as well as any other major changes you had to make. Let’s get this done in the next 2 hours.

IT Director

**Grading:**-

Have team log in to their active directory and show you that all specified users and groups exist. Verify file level access on 3 users.

1. Verify users and groups exist:
   1. Owners [ ]
   2. Operators [ ]
   3. Marketing [ ]
   4. Managers [ ]
   5. IT [ ]
   6. HR [ ]
2. Verify file access for 3 users [ ]

**Due by: 16:00**

**On Time? Y N**

**INJECT 10**

**Send : 15:00**

**From: IT Director (Green Team)**  
You have made a number of system changes to our critical systems today. Please provide me with a detailed listing of changes made, get them to me by 16:00 today.

**Grading:-**

1. Report received [ ]
2. Report has at least 10 changes [ ]

**Due by: 16:00**

**On Time? Y N**