**Assignment:** Work with your IPA server to harden Server and work with Administrative Tools.

**Required Resources**

* CentOS Server (Created in Assignment 1)
* Linux Mint (Created in Assignment 1)
* Naming convention (Course Resources)

**Professional Documentation**

All documentation must be done in a **professional style**. It must include:

1. Title page
2. **Updateable** Table of Contents
3. Document introduction
4. Section introductions or description, each section must be clearly identified
5. Graphics or screenshots MUST include a title with a short description
6. Any direct or copied quotes or graphics MUST be properly credited in a footnote
7. ALL sources MUST be properly cited (APA format) and placed at the end of your document in a bibliography.
8. **NO** embedded, zipped or compressed files. \*\* All scripts must be converted to text before including them in your documentation. \*\*

**\*1 Professional Word Document ONLY.**

**Research and documentation sections** -Please complete all research and question responses in your own words. Research sections not completed in your own words may result in a mark of 0 for the section.

**NOTE:** Please do NOT copy and paste responses from internet, **even with a citation**. I expect each section or response to be in your own words. Be prepared to explain your responses and demonstrate your comprehension during the marking period.

**No marks** will be given for cited or credited information included in document.

**Marking and Assignment Notes:**

* ScreenshotsMUST include user or device identifying information.
* Screenshots MUST be added to your document in the order of creation.
* Documentation must meet Professionalism requirements.
* **Automatic mark of 0 - Assignment not submitted or work not original.**

<http://www.nscc.ca/docs/about-nscc/policies-procedures/policy-studentcodeofconduct.pdf>

<https://www.nscc.ca/docs/about-nscc/policies-procedures/policy-academicintegrity.pdf>

**NOTE: This assignment may require some adaption, research and troubleshooting.**

**Task 1 – Create a Glossary Section for your document.**

**Research Section – Review research requirements on page 1 and complete in your own words.**

NOTE: Please do NOT copy and paste from internet, even with a citation. I expect each glossary term to be in your own words. **Be prepared to explain your definition and responses.**

**\*\* I recommend completing this section before completing the remainder of the assignment as you will have a much better understanding of the material and data.**

* Create a Glossary section for your document and add as Appendix A.
* Research and define each of the following and include at least one example to demonstrate your knowledge and understanding.

1. Elasticsearch
2. rsyslog
3. REK/ELK
4. Logstash
5. Kibana

**Task 2 – Setup logging and Security for our IPA Server**

First we will setup logging on our IPA server to allow us to track modifications, logins, etc. as part of our security monitoring.

We will use Elastic Search and Kibana to manage and view our logs.

We will also grab a predefined Kibana setup in the form of a Docker Image.

In order to “Pull” the new image we must first install Docker.

* Install docker using the rpm repository

[Install Docker Engine on CentOS | Docker Docs](https://docs.docker.com/engine/install/centos/)

* Remember to test with hello-world (docker will update to latest version).
* Now we will “Pull” our image from docker.
* Use the following page to complete the ReadMe to install pull and install the [**rsyslog-elasticsearch-kibana**](https://github.com/pschiffe/rsyslog-elasticsearch-kibana#rsyslog-elasticsearch-kibana) image.

[GitHub - pschiffe/rsyslog-elasticsearch-kibana: Docker image for centralized logging based on CentOS 7 with rsyslog, elasticsearch and kibana.](https://github.com/pschiffe/rsyslog-elasticsearch-kibana)

* Now we will need to download the configuration file to redirect our Search Files to the correct location.
* [GitHub - pschiffe/ipa-log-config: Tool for log forwarding configuration on IPA servers and clients](https://github.com/pschiffe/ipa-log-config)
* Download the **ipa\_log\_config.py** configuration file and run it in the /etc/ipa/ directory with the following argument **--target IPAServerIP**
  + **Remember**, that you require the correct permissions in order to run a file.
* Setup a dashboard that shows User Login logs, and 3 other logs of your choice. Ensure each of your choice are populated with data. (See Announcement for Troubleshooting Option)

Now that we have setup some default logging for our IPA server lets add some additional security.

* Review the PowerPoint Presentations in BrightSpace for this module. Notice there are some hardening information and some helpful demos on how to configure some settings.
* Use the PowerPoint for this module as well as the internet to harden **3 separate areas** of your IPA server.
  + Ensure the hardening does NOT affect the function of your server.
  + Capture all your hardening details in your Install/Change Management Log.
  + Include a section for each change that clearly explains your choice for the hardening action. Make sure your explanation clearly defends your choice.
  + Test each of your hardening modifications after each one is implemented to confirm it works and does not impede the function of your server. Correct if required.
  + Include your testing instructions and results in your Install/Change Management log.
* **Stop**. Be prepared to demo your security or hardening changes.

**Task 3 - Using Administrative Tasks**

We just hired new staff for our Tech Office and would like to create a group and users who have permission to accomplish some management task on our Member Server.

**Working with sudoers and IPA**

sudoers is a file that stores the details of users privileges and can be modified to allow additional privileges for a user or group. *This is a system secure file so it can only be modified using the visudo command, otherwise security features will be lost.*

When working with IPA we may want some of our users to have elevated privileges in order to support our environment.

* If required log into your IPA Server
* Create a new **user** group:
  + Group = sysops (description = System Operators)

Now we will setup our sudo abilities for our new group.

* Select Policy -> Sudo -> Sudo Rules
* Create a new rule with the following settings:
  + Name = Sysop.sudo
  + Description = Elevated commands available for sysops.
  + Options:
    - Add new option= !authenticate
  + Who = sysops group
  + Access this host = ipaworkstations
  + Run this command = Any Command
  + As whom = Anyone
  + Save your settings

Now we will setup our sudo commands for our new rule (sysop.sudo rule created above).

* Add the following commands:
  + sudo su
  + sudo update

Now we will test our new group.

* Add the Aisha Anton to the sysops group.
* Log into your client and run the sudo su command
* Log out and log back in as Bruce Brown and run the same command as Bruce.
* Ensure the new group settings are current.

We have successfully setup our Sysop Group, let’s make a few more modifications.

* Create two (2) more additional sudo commands to your sysop.sudo rule created above.
* Confirm they work by logging in as both Aisha Anton and Bruce Brown.
* **Stop**. Be prepared to demo your sysop group and sudo commands.

**Task 4 - Setup printing between your IPA Server and your IPA Client.**

Now that we have established a server/client relationship lets setup some additional resources.

* If required, update your IPA Server
* Now we will install samba and setup smb
  + Confirm samba is installed
  + Confirm the smb service is enabled and started.
    - If not loaded or enabled please do so.
  + Confirm the cups service is enabled and started.
    - If not loaded or enabled please do so.
  + Capture the commands and results with screenshots and add them to your Change Management Log.

*Additional Learning: cups (Common UNIX Printing System) allows your computer to act as a print server.* [*https://linuxconfig.org/linux-cups-tutorial-for-beginners*](https://linuxconfig.org/linux-cups-tutorial-for-beginners)

Configure your smb.conf file to set it up for our new print server (IPA Server)

* Modify your /etc/samba/smb.conf to match the settings below:

A white background with black text

Description automatically generated

Now we will need to restart our smb service to update it with the new information

* **Record** the modification and the command to restart your Samba smb service and add it to your Change Management Log.

Now that you have installed Samba and setup SMB we will setup our printing share.

**Note: For security reasons, you will be prompted several times throughout this process for your password.**

* In your Application/ Sundry, open your Printer Settings application
  + Under Server select Settings and modify to “Publish Shared printers connected to the system”
  + When given the option select “Adjust Firewall”
* Now let’s Add a network printer (you may need to adjust the firewall)
  + Network Printer /
  + AppSocket/HP JetDirect
  + Printer IP: 192.168.208.201
  + Leave the port set to 9100
  + Select forward

Your server will take some time to search for all the drivers installed on your CentOS node

* Choose Driver and configure as noted below:
  + Select printer from database
  + HP (forward)
  + Model = Laserjet p3005dn
  + Driver = HP Laserjet p3005dn pcl3, hpcups 3.15.9
  + forward
  + No Duplexer installed
  + forward
  + Printer shortname = PR+YourInitials+01 (ex. PRMAD01)
  + Description = HP Laserjet p3005dn
  + Location = Copy Room 1
  + Apply
  + **Do NOT print a test page as the printer does not actually exist**

Now we will need to add our shared printer to our IPA Client.

* Log on to your IPA Client as Aisha Anton
* Under Administration, open Print Settings
* Confirm your printer is listed.

It is important to keep an up to date record of all changes and modifications made to your server and have a reliable copy available as backup.

* Take a final snapshot of your servers and client in the **OFF** state
* Create a “**Gold**” copy of your new server on your portable drive
* Capture a screenshot of your Gold copy properties and add it to your documentation.
* Update your Install/Change Management Log for your IPA Server
* Submit your Install/Change Management Log as part of your formal documentation.
* Upload your documentation to Brightspace

Marking Rubric

|  |  |
| --- | --- |
| **Value** | **Task** |
|  | **Comprehensive Marking** |
| 3 | Kibana Web Portal Available with correct Port |
| 8 | Kibana dashboard available with User Login details and 3 other populated logs. |
| 9 | Demo Server hardened in 3 separate areas. |
| 3 | Sudo rule created with correct:   * Name: * Description: * Who: * Access: * Run this command= Any * As whom = Anyone |
| 3 | Sudo commands created for:   * Sudo su * 2 additional commands |
| 8 | Demo successful Sudo commands   * Sudo su (2 marks) * 2 additional commands (6 marks) |
| 2 | Printer setup on IPA server |
| 4 | Printer properly deployed to IPA Client |
| 2 | Snapshot of IPA Server and Client |
| **42** | **Total Marks for comprehensive** |
|  | **Documentation as submitted to Brightspace** |
| 15 | Research and Glossary terms (research rubric) |
| 8 | Change log contains all configurations, details, requirements and tests for your server hardening. |
| 6 | Change Management log contains all required changes, configurations and notes but is NOT a copy paste from assignment. |
| 2 | Screenshot of Gold copy properties for IPA Server including location, creation and modification dates and size. |
| 2 | Document Creation and Professionalism |
| **33** | **Total Marks for D2L Submissions** |
|  |  |
| **75** | **Total Assignment Marks.** |