Challenge 9 - Configuration Management Gone Awry - 5/7 | Mike Morris

Challenge 9 - Configuration Management Gone Awry - 5/7 | Mike Morris

We have a major problem on our hands. Several employees have reported issues with connecting to the network and haven’t been able to get their work done. I need this fixed ASAP.

Ashley Steele @asteele

Unfortunately, it looks like the MSP's automated configuration management tool ended up misconfiguring a few of our machines the last time it was run. Misconfiguration of these critical pieces of hardware has company-wide ramifications.

Jacqueline Smith @jsmith

Well, when did they say it would be fixed? We're not only losing out on employee productivity, but also on sales. We need to get a handle on this quickly!

Ashley Steele @asteele

That brings me to the issue at hand. The automated configuration management tool can not repair the network in its current state. It won't be able to identify some of the misconfigured boxes. The affected machines need to be reconfigured manually.

Jacqueline Smith @jsmith

Great! So you'll get right on it?

Ashley Steele @asteele

Well, not exactly. I'm not the most well-versed when it comes to networking. We need someone with more expertise to take on such a complex task. Maybe @playerone could lend a hand?

Jacqueline Smith @jsmith

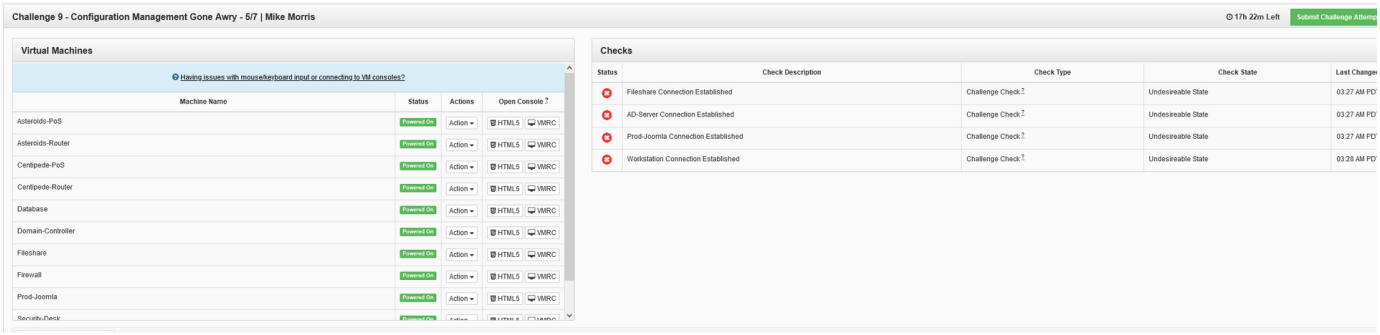
I don't care who gets this done, so long as my employees can return to work soon. Time is money!

Ashley Steele @asteele

@playerone, take a look around and figure out what boxes were misconfigured by the MSP's tool. Do whatever you need to do in order to get our employees back online. Thanks, we're counting on you!

NICE Challenge Dev Team @ncpdev

The meeting has concluded. Don’t worry about recording any meeting messages, as the meeting notes are available to you while attempting the challenge. If the challenge is still deploying, be patient. Most challenges take between 5-10 minutes to deploy. If the challenge is deployed, click “Begin Challenge” below!



Challenge Info:

Configuration Management Gone Awry

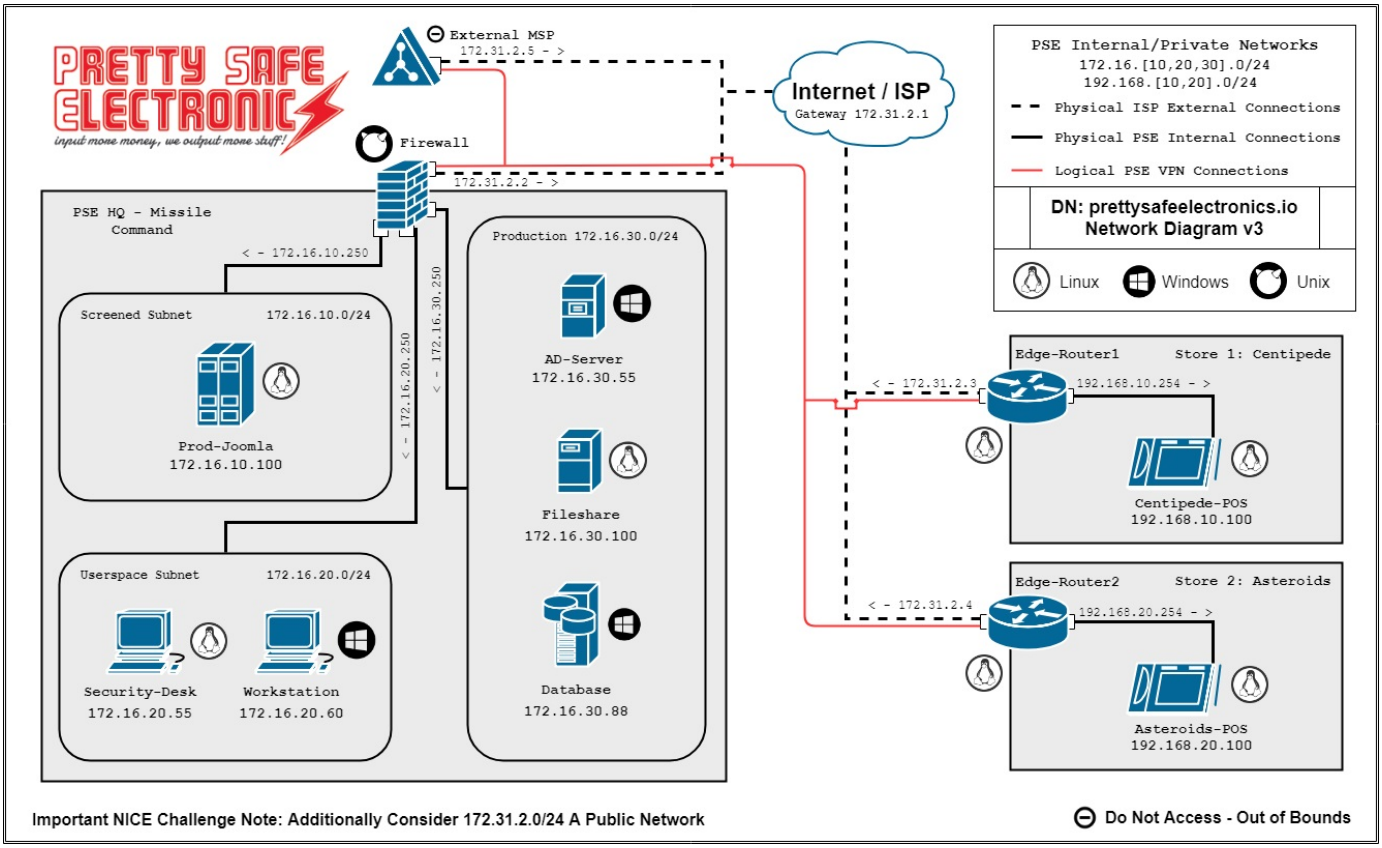
Author: Bailey Kasin
Framework Category: Protect and Defend
Specialty Area: Cybersecurity Defense Analysis
Work Role: Cyber Defense Analyst
Task Description: Examine network topologies to understand data flows through the network. (T0291)
Scenario

An error in our managed service providers automated configuration management software has caused considerable damage to our network. Multiple systems and network pathways are now misconfigured and unable to be reconfigured with the automated tool. This downtime is costing the company considerably in online sales, in store sales, and employee productivity. We need you to manually reconfigure the affected systems and networking equipment to get us back online.

Additional Information

More details and objectives about this challenge will be introduced during the challenge meeting, which will start once you begin deploying the challenge.
You will be able to check your progress during this challenge using the check panel within the workspace once the challenge is deployed. The checks within the check panel report on the state of some or all of the required tasks within the challenge.
Once you have completed the requested tasks, you will need to document the methodology you used with as much detail and professionalism as necessary. This should be done on the documentation tab within the workspace once the challenge is deployed. Below the main documentation section be sure to include a tagged list of applications you used to complete the challenge.

Network Map:



Please enter any tools, programs, and utilities used to complete the challenge.
Document all necessary steps and actions taken to complete the challenge in the field below.
Document as if you were writing documentation for the company. This information will be sent to your challenge Curator for review.* vim

Documentation: The challenge states I need to manually configure the Network settings and used this website below for referencing the commands used.
https://wiki.debian.org/NetworkConfiguration#A3_ways_to_configure_the_network

- **For the Joomla station,** I used $ sudo ip route add default via 172.16.10.250 as my solution and got the green checkmark
- **On the fileshare** I modified /etc/networks/interfaces as root and used vim to open/edit.(`# vim etc/networks/interfaces)`

I changed the interface ens32 from an incorrect ip address to the correct one being 172.16.30.100 using Network map for guidance.

I also noticed the gateway being incorrect and changed that to 172.16.30.250

and the last digit in the netmask had an extra 255 , changed that to 0.

used `:wq` then `Enter` to save and exit vim.

To verify

`ip r`

noticed it was still down used `sudo ifup ens32`

and showed changes made and working correctly.

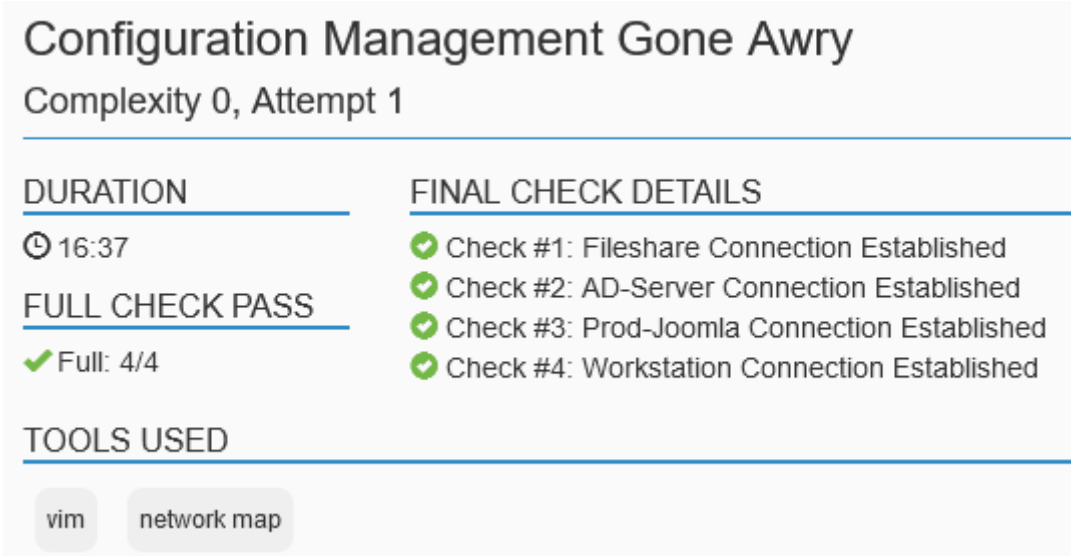
- **I logged into Domain Controller machine,** right clicked on network icon, ran Windows Network Diagnostics. Problem found: DHCP is not enabled for "Ethernet0". Fixed problem.

This did not make the check green so I looked around in Network Connections. Noticed the wrong IP v4 address so I manually added the correct settings by right clicking on Ethernet0>Properties>Click on Internet Protocol Version 4(TCP/IPv4)>Properties> Use the following IP address : IP Address: 172.16.30.55, Subnet mask: 255.255.255.0 Default Gateway: 172.16.30.255, Use the Following DNS server address 8.8.8.8 and click ok. (Found the settings using Network Map that corresponds to AD-Server.

- Tried logging into Workstation VM but an error stating 'failed to connect' because it doesn't have network access, so you can't log in to the domain. MS actually has the answer there in the help section they display stating WORKSTATION\user will work . I logged into the machine using WORKSTATION\playerone as the username (as other user option). Ran Windows Network Diagnostics, It states to change the TCP/IP settings for the "Ethernet0" adapter.

Went into Network Connections by right clicking on Network Connection icon and clicking on Open Network and Internet Settings. >Changed adapter Options > Ethernet0>Properties> Internet protocol Version 4(TCP/Ipv4)>Properties

Under General tab I changed the incorrect IP address, Subnet mask, Default gateway to the correct IP address, Subnet mask and Default gateway using the Network Map for guidance. I also changed the DNS address to the correct DNS settings (Domain Controllers IP Address). Clicked OK to save settings.



PDF Provided upon request

NICE Framework & CAE KU Mapping

NICE Framework KSAK0001.

Knowledge of computer networking concepts and protocols, and network security methodologies.K0004.

Knowledge of cybersecurity and privacy principles.K0005. Knowledge of cyber threats and vulnerabilities.K0060.

Knowledge of operating systems.K0061. Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).K0167.

Knowledge of system administration, network, and operating system hardening techniques.K0221.

Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).K0318.

Knowledge of operating system command-line tools.K0332. Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.CAE Knowledge UnitsBasic NetworkingCybersecurity FoundationsCybersecurity PrinciplesIT Systems Components Operating Systems Administration Operating Systems Concepts