

[illegible]

<b>Name</b>	ServerSpec: Automating Configuration Tests
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2072">https://attackdefense.com/challengedetails?cid=2072</a>
<b>Type</b>	DevSecOps Basics: Compliance as Code

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

## Challenge Description

[Serverspec](#) is open-source software that is used to perform configuration tests on remote systems. It performs tests on the remote systems using SSH.

A Kali CLI machine (kali-cli) with serverspec and a remote test server machine (test-server) are provided to the user. The configuration test file for this test server is kept in the home directory of the root user. The credentials of the test servers are given below:

Username	Password
root	password1

**Objective:** Run tests using Serverspec to check if the remote system is configured properly!

### Instructions:

- The configuration file is provided at /root/serverspec\_example/spec/test-server/ directory
- The remote server is running and can be reached on “test-server” hostname

## Solution

**Step 1:** Change to the serverspec\_example directory present in the home directory of the user.

**Commands:**

```
cd serverspec_example  
ls -lah
```

```
root@kali-cli:~# cd serverspec_example/  
root@kali-cli:~/serverspec_example#  
root@kali-cli:~/serverspec_example# ls -lah  
total 20K  
drwxr-xr-x 3 root root 4.0K Sep 15 09:37 .  
drwx----- 1 root root 4.0K Sep 15 09:37 ..  
-rw-r--r-- 1 root root 685 Sep 15 09:15 Rakefile  
-rw-r--r-- 1 root root 31 Sep 15 09:15 .rspec  
drwxr-xr-x 3 root root 4.0K Sep 15 09:27 spec  
root@kali-cli:~/serverspec_example#
```

**Step 2:** Check the configuration file provided in the test-server directory located inside the spec directory.

**Commands:**

```
cd spec/test-server/  
ls -lah
```

```
root@kali-cli:~/serverspec_example# cd spec/test-server/  
root@kali-cli:~/serverspec_example/spec/test-server#  
root@kali-cli:~/serverspec_example/spec/test-server# ls -lah  
total 12K  
drwxr-xr-x 2 root root 4.0K Sep 15 09:15 .  
drwxr-xr-x 3 root root 4.0K Sep 15 09:27 ..  
-rw-r--r-- 1 root root 227 Sep 15 09:15 sample_spec.rb  
root@kali-cli:~/serverspec_example/spec/test-server#
```

**Step 3:** Check the contents of sample\_spec.rb.

**Commands:** cat sample\_spec.rb

```
root@kali-cli:~/serverspec_example/spec/test-server# cat sample_spec.rb
require 'spec_helper'

describe package 'wget' do
  it { should be_installed }
end

describe package 'openssh-server' do
  it { should be_installed }
end

describe user 'ubuntu' do
  it { should exist }
end
root@kali-cli:~/serverspec_example/spec/test-server#
```

sample\_spec.rb file is the configuration file that contains the configuration tests for the remote system. The configuration contains the following checks:

- If wget utility is installed
- If openssh server is installed
- If the user ubuntu exists

**Step 4:** Run the configuration tests on the remote server machine (test-server) using rake.

**Command:** rake spec

```
root@kali-cli:~/serverspec_example/spec/test-server# rake spec
(in /root/serverspec_example)
/usr/bin/ruby2.5 -I/var/lib/gems/2.5.0/gems/rspec-support-3.9.3/lib:/var/lib/gems/2.5.0/gems/rspec-core-3.9.2/lib /var/lib/gems/2.5.0/gems/rspec-core-3.9.2/exe/rspec --pattern spec/test-server/\*_spec.rb

Package "wget"
/var/lib/gems/2.5.0/gems/specinfra-2.82.19/lib/specinfra/backend/ssh.rb:82:in `create_ssh': Passing nil, or [nil] to Net::SSH.start is deprecated for keys: user
root@test-server's password:
```

Enter the credentials of the test-server which have been provided in the challenge description.

### Credentials:

- **Username:** root
- **Password:** password1

```
root@kali-cli:~/serverspec_example/spec/test-server# rake spec
(in /root/serverspec_example)
/usr/bin/ruby2.5 -I/var/lib/gems/2.5.0/gems/rspec-support-3.9.3/lib:/var/lib/gems/2.5.0/gems/rspec-core-3.9.2/lib /var/lib/gems/2.5.0/gems/rspec-core-3.9.2/exe/rspec --pattern spec/test-server/\*_spec.rb

Package "wget"
/var/lib/gems/2.5.0/gems/specinfra-2.82.19/lib/specinfra/backend/ssh.rb:82:in `create_ssh': Passing nil, or [nil] to Net::SSH.start is deprecated for keys: user
root@test-server's password:
  is expected to be installed

Package "openssh-server"
  is expected to be installed

User "ubuntu"
  is expected to exist

Finished in 3.19 seconds (files took 0.47384 seconds to load)
3 examples, 0 failures

root@kali-cli:~/serverspec_example/spec/test-server#
```

All tests passed successfully.

**Step 5:** Now to see the failure, modify the configuration file. Add a new test case to check if port 80 on test-server is in listen state

```
require 'spec_helper'

describe package 'wget' do
  it { should be_installed }
end

describe package 'openssh-server' do
  it { should be_installed }
end

describe user 'ubuntu' do
  it { should exist }
end
```



```
describe port(80) do
  it { should be_listening }
end
```

The test marked in bold is the recently added test.

**Step 6:** Run the tests on the test-server while passing the credentials.

**Command:** rake spec

```
Port "80"
  is expected to be listening (FAILED - 1)

Failures:

  1) Port "80" is expected to be listening
     On host `test-server'
     Failure/Error: it { should be_listening }
       expected Port "80" to be listening
       sudo -p 'Password: ' /bin/sh -c ss\ -tunl\ \|\ grep\ -E\ --\ :80\\\

     # ./spec/test-server/sample_spec.rb:16:in `block (2 levels) in <top (required)>'

Finished in 2.99 seconds (files took 0.47735 seconds to load)
4 examples, 1 failure

Failed examples:

rspec ./spec/test-server/sample_spec.rb:16 # Port "80" is expected to be listening

/usr/bin/ruby2.5 -I/var/lib/gems/2.5.0/gems/rspec-support-3.9.3/lib:/var/lib/gems/2.5.0/gems/rspec-core-3.9.2/lib:/var/lib/gems/2.5.0/gems/rspec-core-3.9.2/exe/rspec --pattern spec/test-server/\*_spec.rb failed
root@kali-cli:~/serverspec example/spec/test-server#
```

As expected, the test failed. The details can be observed in the output.

## Learnings

Conduct configuration tests on remote systems ServerSpec.