

# CompTIA PenTest+ Guide to Penetration Testing, 1e

## Module 2: Setting Up a Penetration Testing Lab

# Module Objectives

By the end of this module, you should be able to:

1. Explain the purpose of a penetration testing lab
2. Describe the role each virtual machine plays in a penetration testing lab
3. Describe how to set up a virtual machine

# Penetration Testing Lab Overview (1 of 4)

- A penetration testing lab is useful for an ethical hacker to have at their disposal
- Virtualized platforms are commonly used to create or host penetration testing labs
- The penetration testing lab provides a safe security testing environment

## Caution

*Throughout this course, learners are directed to download a variety of files from the Internet. Always make sure to scan each downloaded file with antivirus software. Threat actors are notorious for attempting to distribute malware as benign security tools and similar resources.*

# Penetration Testing Lab Overview (2 of 4)

## Key Terms

- Sandbox – isolated software testing environment; allows safer testing of security tools that can potentially be dangerous
- Virtual machine (VM) – virtual computing environment; digital version of a physical computer
- Target – any computing object that is being pen tested
- ISO file –single file that represents the content of an entire optical disc
- Open Virtual Appliance (OVA) – a VM that has been preconfigured and is available for deployment in a virtualized environment

# Penetration Testing Lab Overview (3 of 4)

The pen testing lab environment discussed throughout this text is designed for hands-on lab activities using the following virtual machines:

- Kali Linux
- Metasploitable2
- Microsoft Windows 7
- Microsoft Windows 10
- Microsoft Windows Server 2019
- Damn Vulnerable Web Application (DVWA)
- Axigen mail server

The virtualized lab environment requires at least 8 GB of memory with 16 GB recommended.

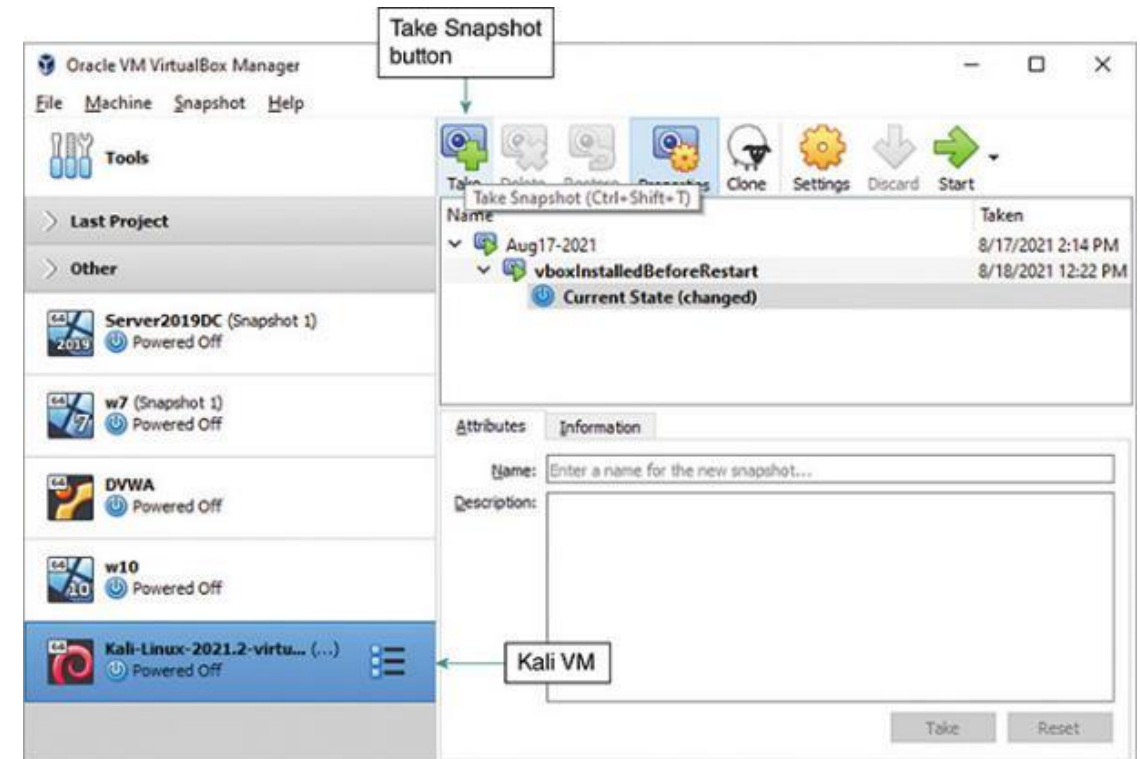
# Penetration Testing Lab Overview (4 of 4)

- Virtualization platform – an environment supporting virtual machines that act like computers with operating systems
- Oracle VirtualBox – the preferred virtualization platform used and referenced throughout this course
- Additional documentation and guidance is available through the course and online

# Setting Up the Kali Linux Virtual Machine (1 of 3)

## Downloading and Installing VirtualBox

- Detailed instructions for installing and configuring the pen testing lab environment are presented in this course
- Additional documentation is available online

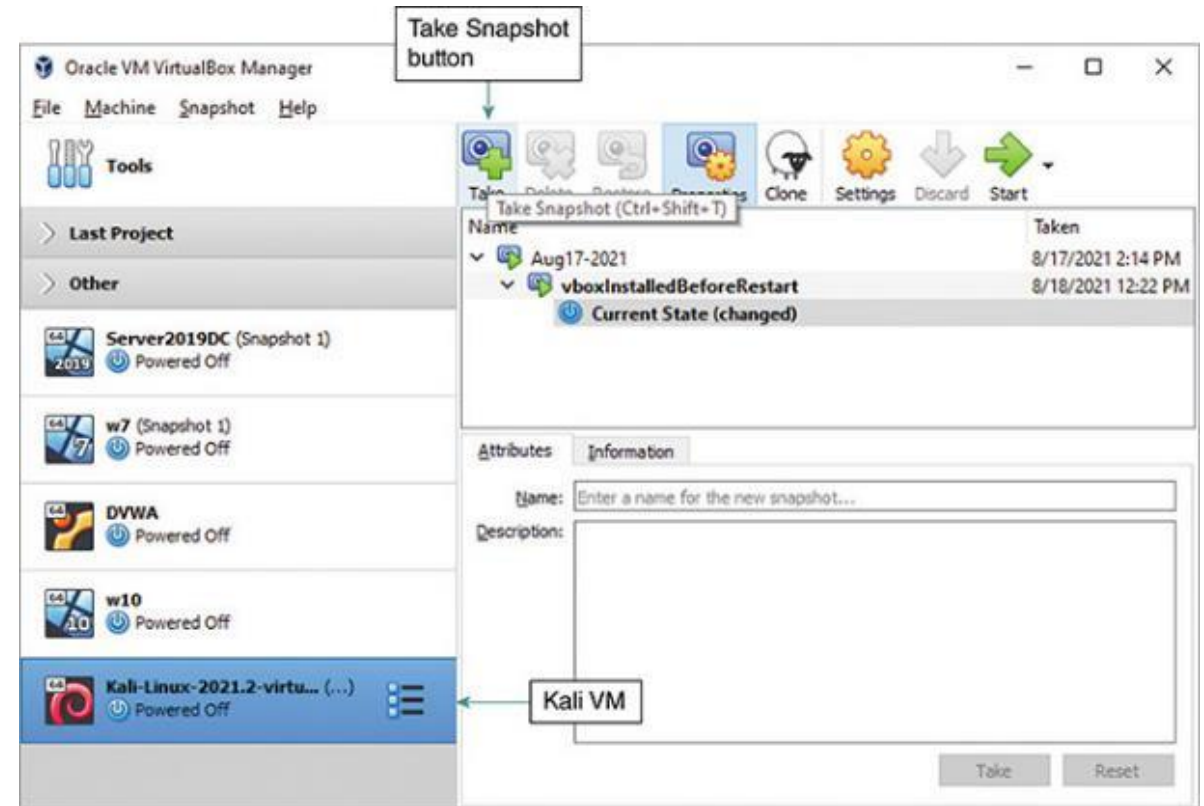


Oracle VirtualBox

# Setting Up the Kali Linux Virtual Machine (2 of 3)

## Downloading and Installing VirtualBox

- Virtualization platform developed by Oracle Corp
- Available for multiple hosts and architectures
  - x86 & Intel64/AMD64
  - Windows
  - Linux & Unix
  - Mac OS



Oracle VirtualBox



# Setting Up the Kali Linux Virtual Machine (3 of 3)

- Kali Linux is widely known and is the preferred platform for pen testing activities
- Free and freely available
- Available in OVA and ISO formats

# Discussion Activity 2-1

Some may argue that creating a ready-to-use hacking distribution, such as Kali Linux, is arming potential threat actors with tools to perform malicious activities against potentially vulnerable targets.

Others may argue that a freely available pen testing toolkit like Kali and offering it for use allows security engineers and those in blue team roles to more efficiently gain access to the tools malicious attackers have at their disposal.

Instructors may choose to divide learners into two groups to present arguments for and against the open access to pen testing tools to the tech community at large.

# Setting Up Targets (1 of 7)

- After Kali Linux is configured and running in Oracle VirtualBox, six target virtual machines will be created
- Installation and configuration steps are similar for target VMs
- Detailed and specific target VM instructions are provided throughout the course
- Care should be taken to ensure pen testing lab virtual machines are properly created to maintain isolation from the host computing environment

# Setting Up Targets (2 of 7)

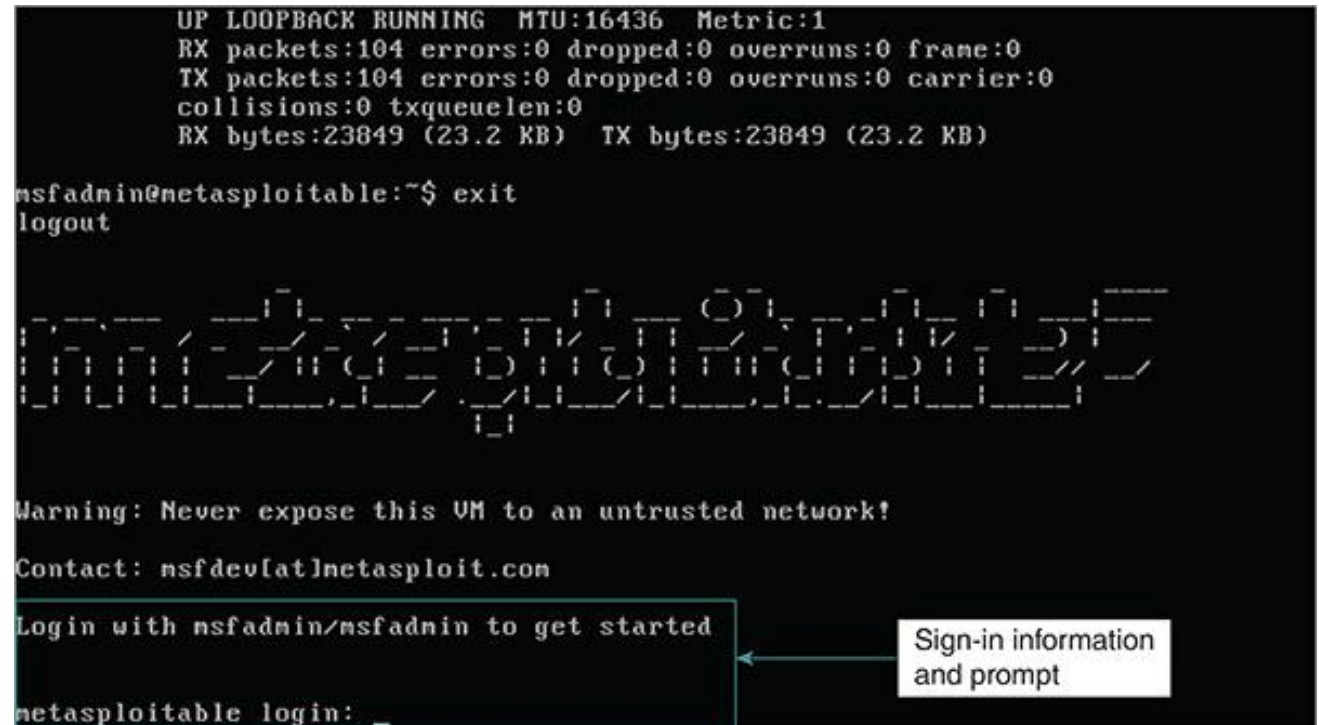
## Metasploitable

- Provided and owned by Rapid7
- Purposely constructed vulnerable security testing platform
- Virtual machine files supplied individually, not as an appliance platform
- Built on Ubuntu Linux

```
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:104 errors:0 dropped:0 overruns:0 frame:0
TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23849 (23.2 KB) TX bytes:23849 (23.2 KB)

msfadmin@metasploitable:~$ exit
logout

Warning: Never expose this VM to an untrusted network!
Contact: nsfdev[at]metasploit.com
Login with nsfadmin/nsfadmin to get started
metasploitable login: _
```

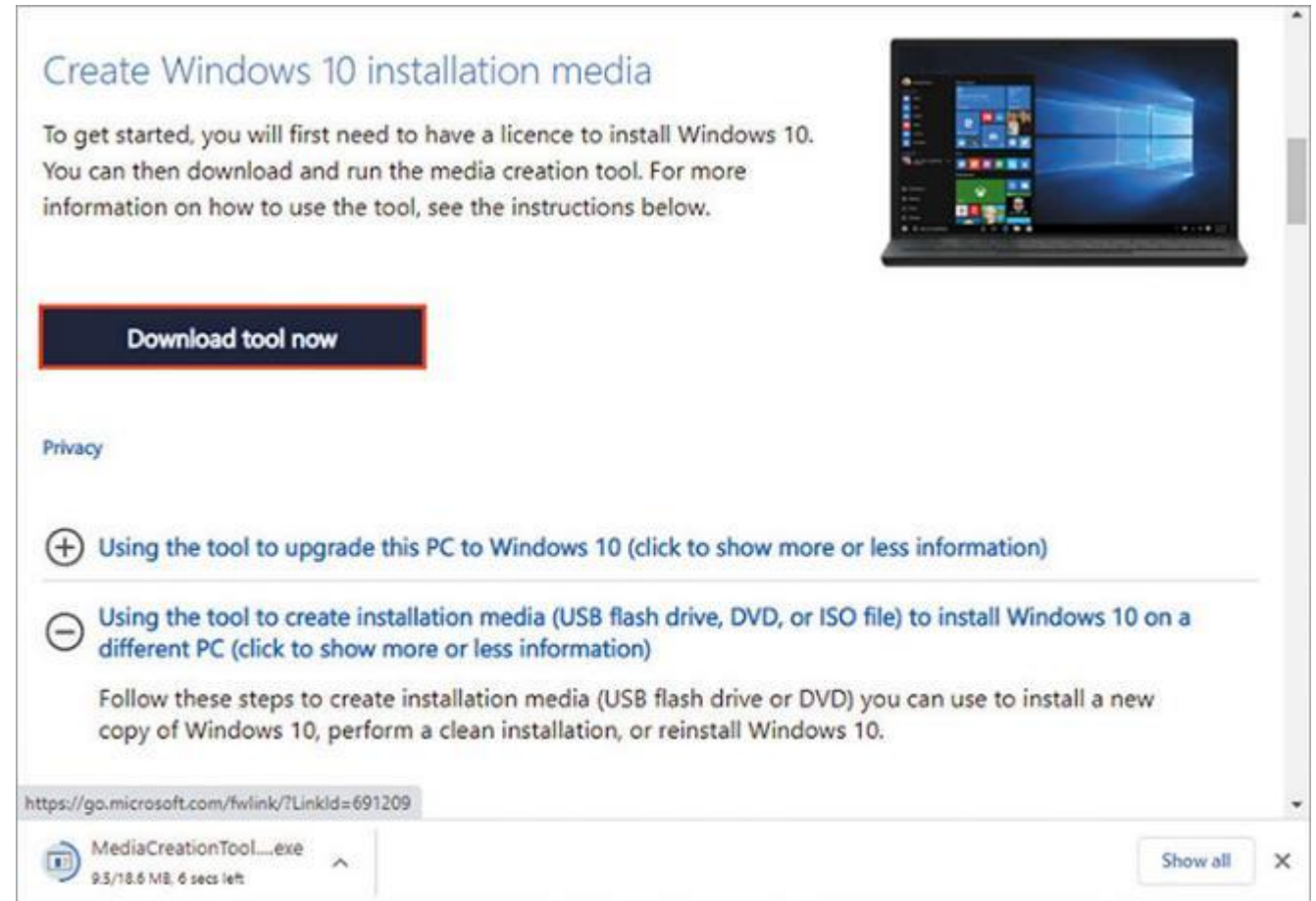


Metasploitable login screen with login info

# Setting Up Targets (3 of 7)

## Microsoft Windows 7

- End of product life January 2020
- 12% market share as of book writing
- Inherently vulnerable due to lack of support

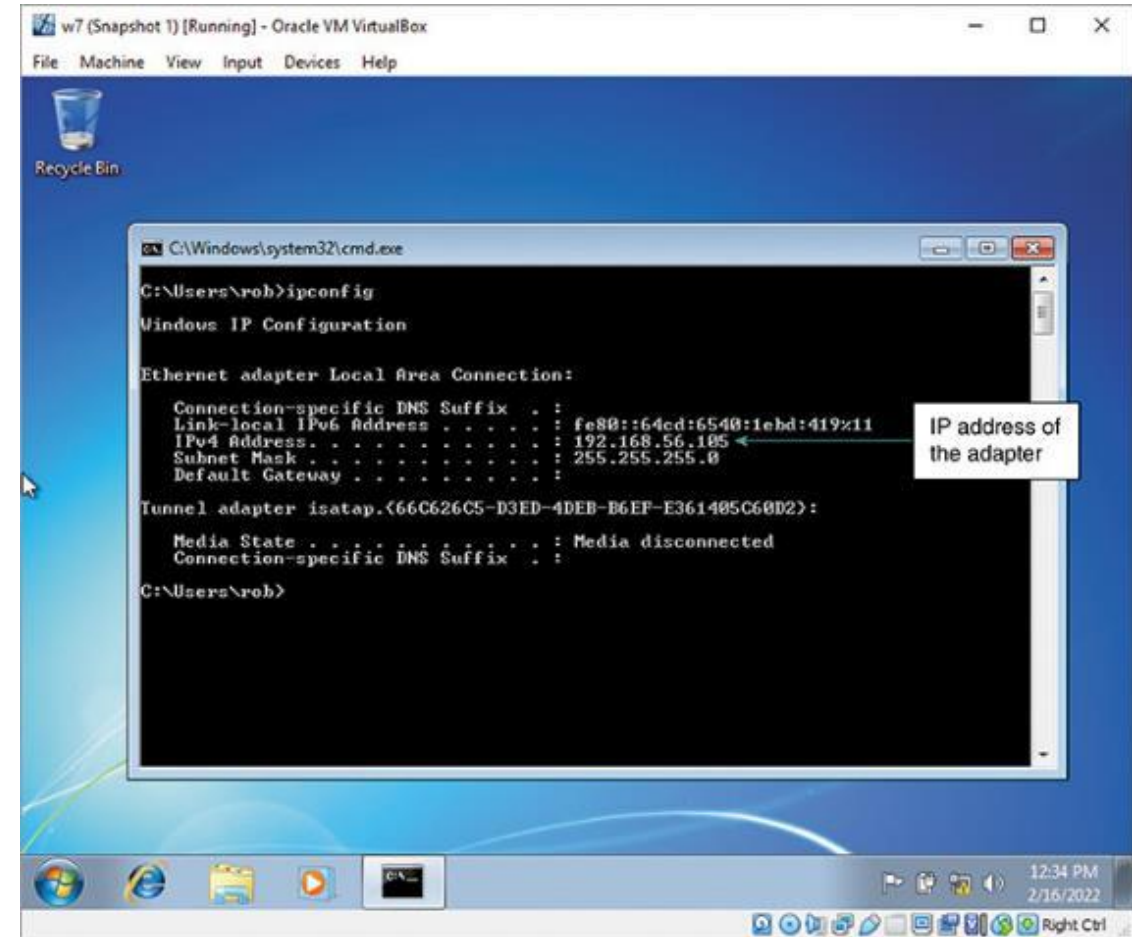


Downloading the Media Creation Tool for Windows 10

# Setting Up Targets (4 of 7)

## Microsoft Windows 10

- Runs on 1.3 billion devices worldwide
- Commonly used and encountered during pen tests



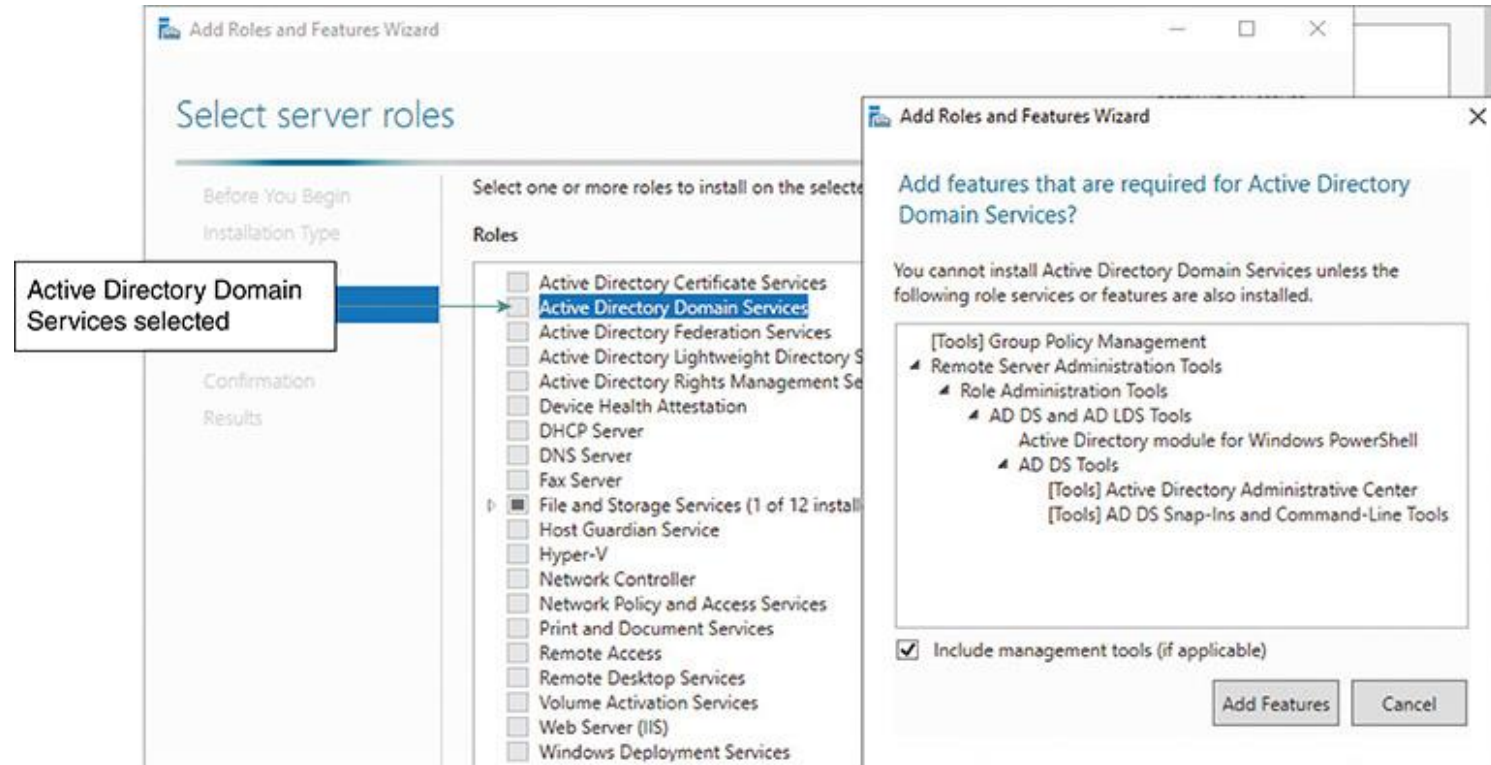
Windows 10 as virtual machine



# Setting Up Targets (5 of 7)

## Windows Server 2019

- Functions as Domain Controller running Active Directory
- Microsoft owns 48% market share as of book writing
- Trial license available for 180 days

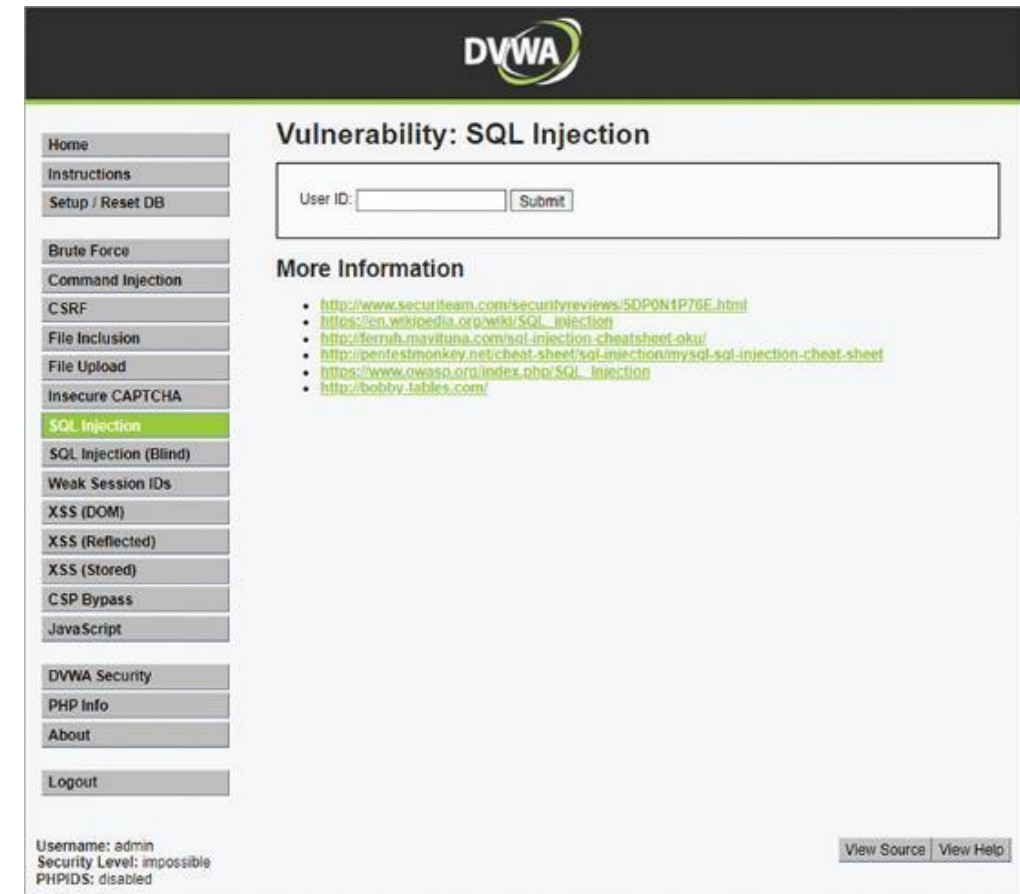


Add Roles and Features Wizard in Server 2019

# Setting Up Targets (6 of 7)

## Damn Vulnerable Web Application (DVWA)

- Intentionally vulnerable web app platform for security testing
- Runs on Linux operating system
- Freely available



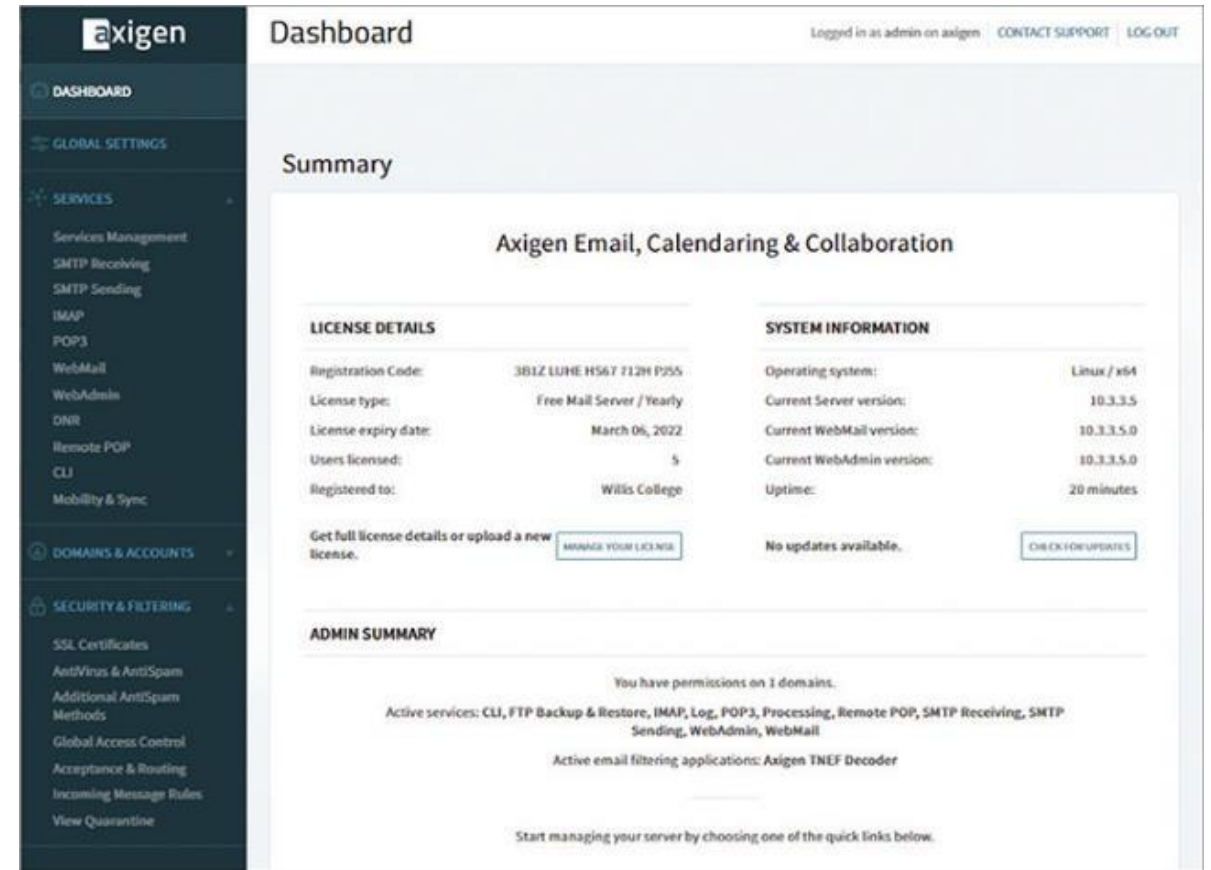
DVWA open in a web browser



# Setting Up Targets (7 of 7)

## Axigen Mail Server

- Fully functional mail server trial
- Available for download as virtual appliance (OVA)
- Linux operating system



Axigen WebAdmin dashboard

# Knowledge Check Activity 2-1

Which of the following penetration testing lab target systems is not designed to be targeted or is inherently vulnerable to pen testing activities?

- a. Windows 7
- b. Windows Server 2019
- c. Metasploitable
- d. DVWA

# Knowledge Check Activity 2-1: Answer

**Which of the following penetration testing lab target systems is not designed to be vulnerable or is inherently vulnerable to pen testing activities?**

**Answer: Windows Server 2019**

Microsoft's Windows Server 2019 is still widely used as a server platform and support is still offered by Microsoft and is not designed to be vulnerable or is inherently vulnerable to pen testing activities and tools.

# Self Assessment

A penetration testing lab is very useful tool for aspiring ethical hackers and professional pen testers alike to have access to. Such a lab lists the steps needed to build a penetration testing lab like the virtualized lab built in this module.

What components are required to build a safe, reliable, and isolated penetration testing lab for conducting ethical hacking practice exercises like those provided by this course? What steps are necessary in building the pen test lab?

# Summary

Now that the lesson has ended, you should be able to:

- Explain the purpose of a penetration testing lab
- Describe the role each virtual machine plays in a penetration testing lab
- Describe how to set up a virtual machine