Virtual Systems and Networking Concept Brief

William Pascoe

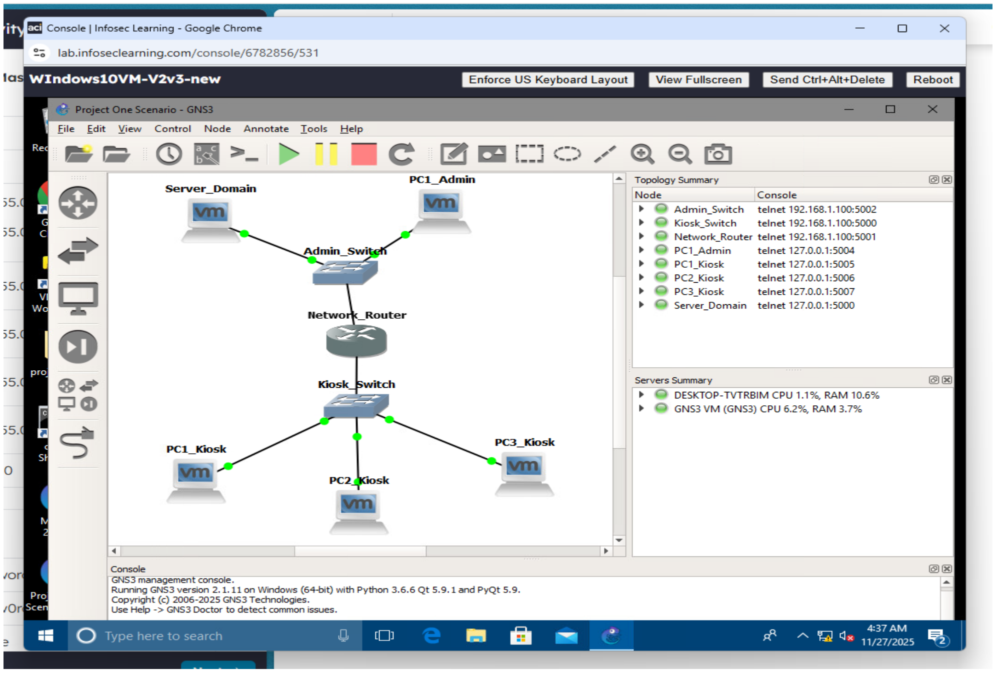
CYB-220 Netwrok Security

Jonathon Schumaker

November 27, 2025

Virtual Systems and Networking Concept Brief

Network Configuration



Topology Summary

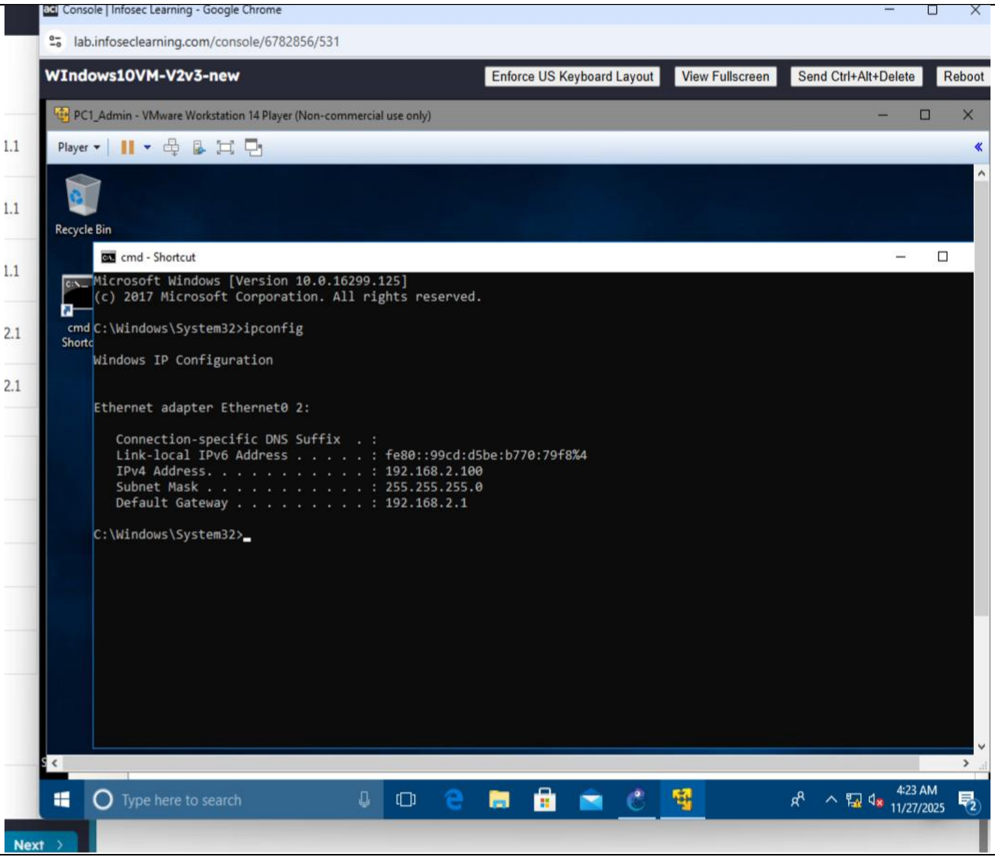
Node	Console
Admin_Switch	telnet 192.168.1.100:5002
Kiosk_Switch	telnet 192.168.1.100:5000
Network_Router	telnet 192.168.1.100:5001
PC1_Admin	telnet 127.0.0.1:5004
PC1_Kiosk	telnet 127.0.0.1:5005
PC2_Kiosk	telnet 127.0.0.1:5006
PC3_Kiosk	telnet 127.0.0.1:5007
Server_Domain	telnet 127.0.0.1:5000

Servers Summary

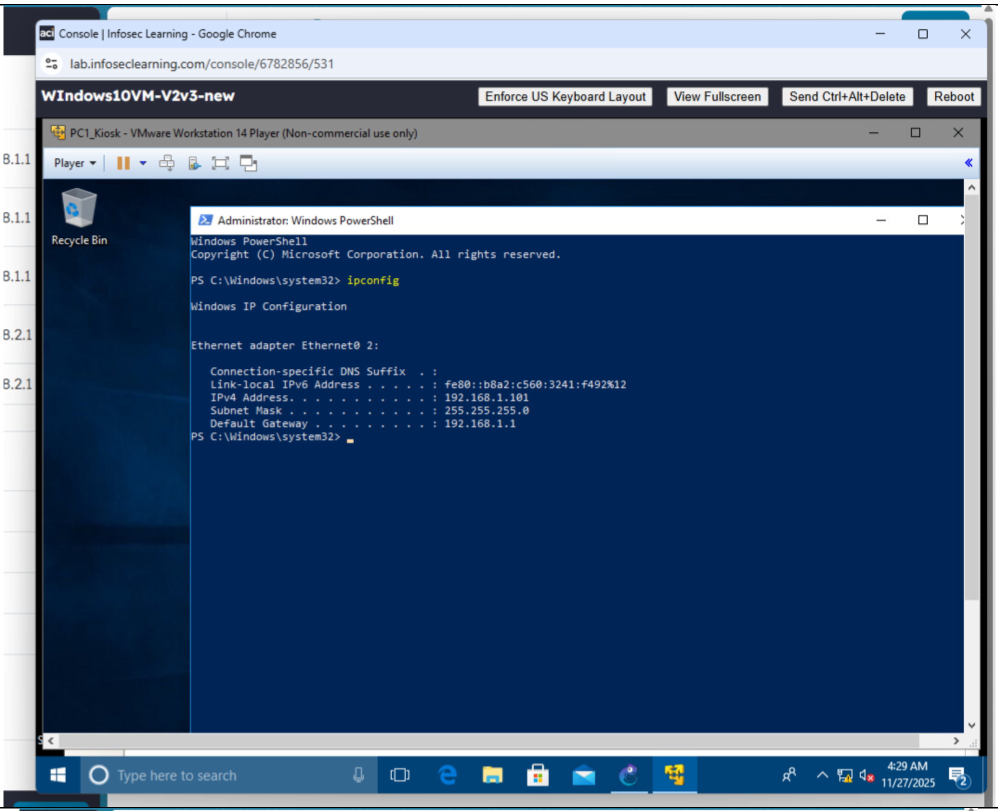
```
DESKTOP-TVTRBIM CPU 1.1%, RAM 10.6%
GNS3 VM (GNS3) CPU 6.2%, RAM 3.7%
```

Console

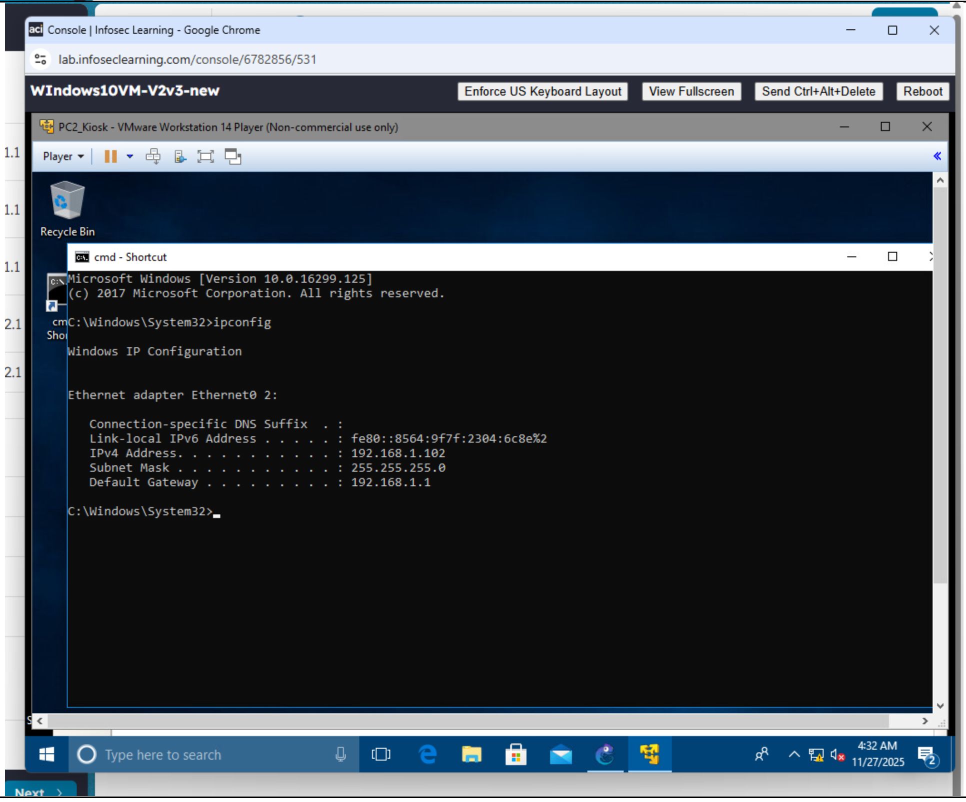
```
GNS3 management console.
Running GNS3 version 2.1.11 on Windows (64-bit) with Python 3.6.6 Qt 5.9.1 and PyQt 5.9.
Copyright (c) 2006-2025 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.
```


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/6782856/531
WIndows10VM-V2v3-new
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PC1_Admin - VMware Workstation 14 Player (Non-commercial use only)
Player
Recycle Bin
cmd - Shortcut
Type here to search
4:23 AM
11/27/2025
Next

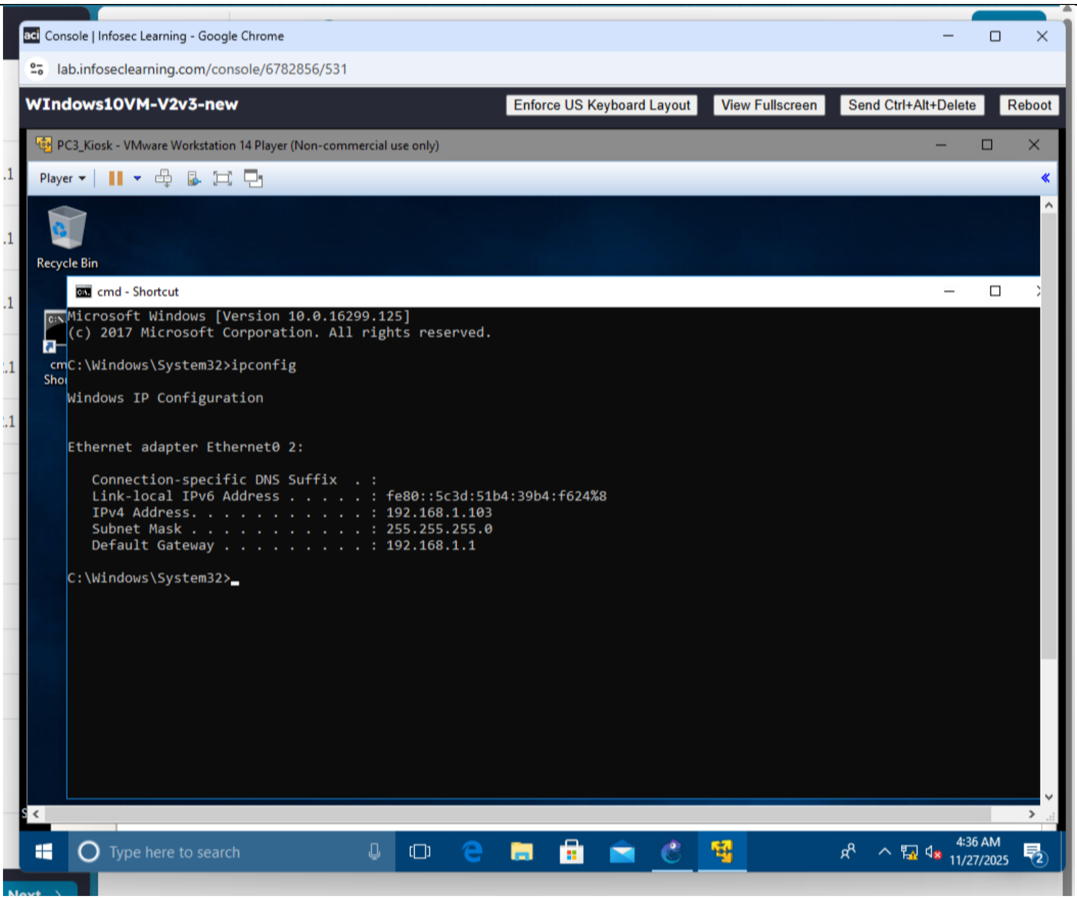
```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::99cd:d5be:b770:79f8%4
   IPv4 Address. . . . . . . . . . . : 192.168.2.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

C:\Windows\System32>_
```


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/6782856/531
WIndows10VM-V2v3-new
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PC1_Kiosk - VMware Workstation 14 Player (Non-commercial use only)
Player
Recycle Bin
Administrator: Windows PowerShell
B.1.1
B.1.1
B.1.1
B.2.1
B.2.1
Type here to search
4:29 AM
11/27/2025

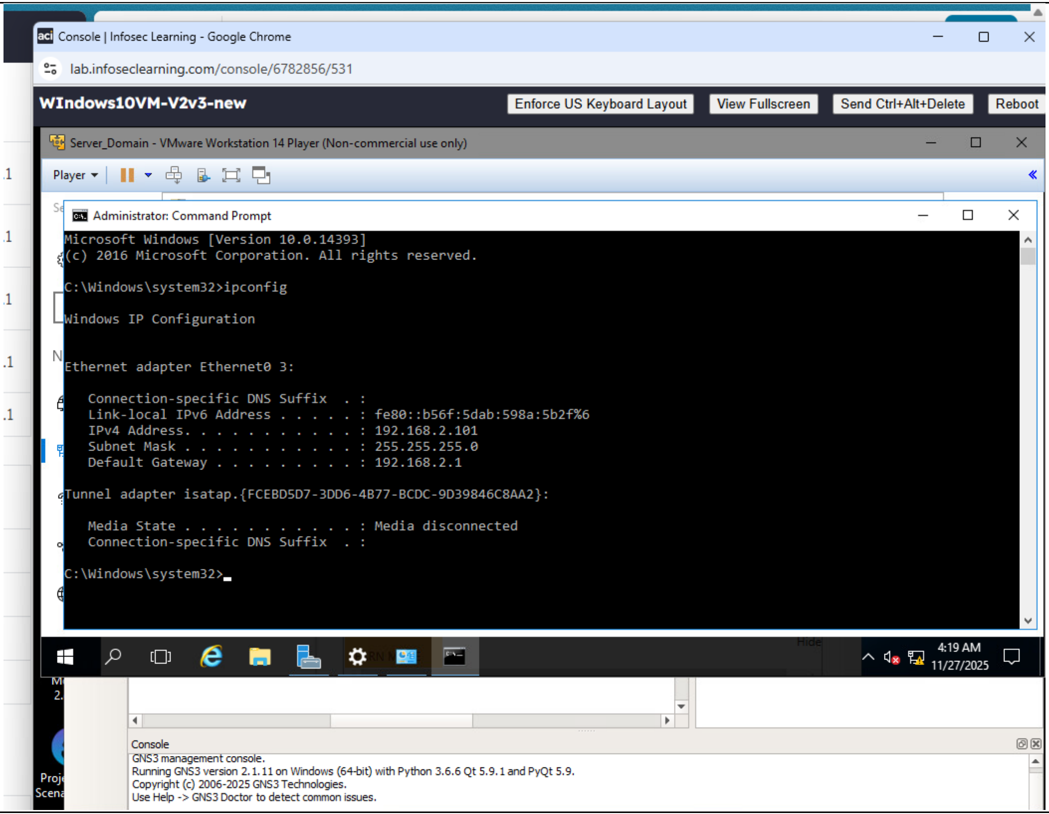
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b8a2:c560:3241:f492%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
PS C:\Windows\system32> _
```


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/6782856/531
WIndows10VM-V2v3-new
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PC2_Kiosk - VMware Workstation 14 Player (Non-commercial use only)
Player
Recycle Bin
cmd - Shortcut
1.1
1.1
1.1
2.1
2.1
Type here to search
4:32 AM
11/27/2025
Next

```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8564:9f7f:2304:6c8e%2
   IPv4 Address. . . . . . . . . . . : 192.168.1.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Windows\System32>_
```


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/6782856/531
WIndows10VM-V2v3-new
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PC3_Kiosk - VMware Workstation 14 Player (Non-commercial use only)
Player
Recycle Bin
cmd - Shortcut
Type here to search
4:36 AM
11/27/2025

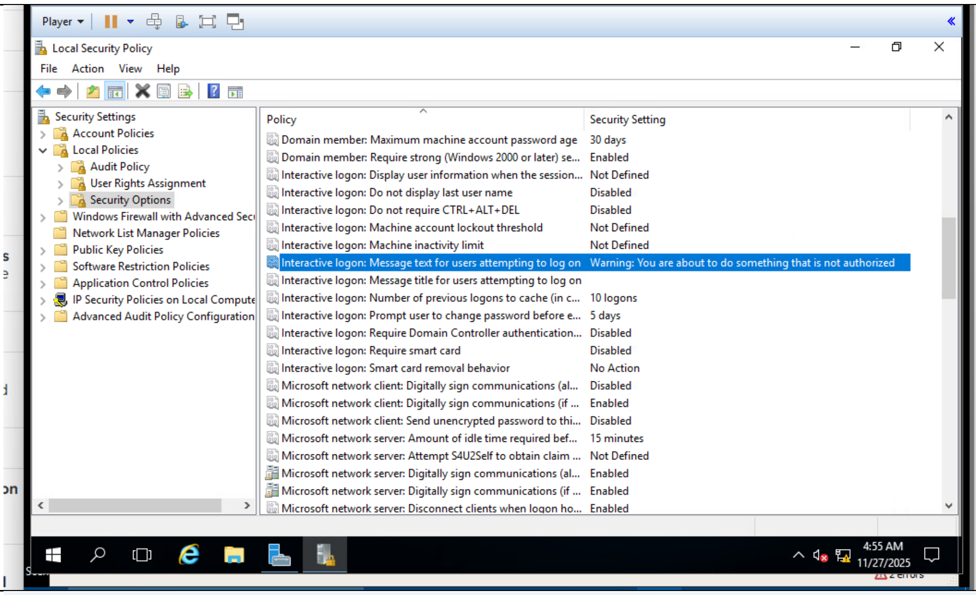
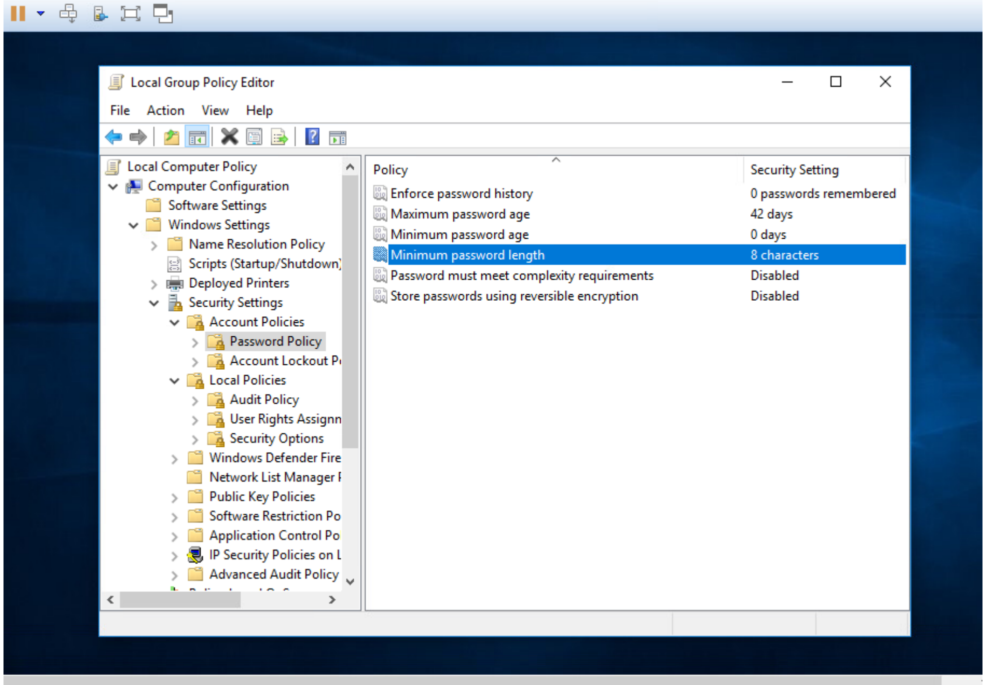
```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5c3d:51b4:39b4:f624%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Windows\System32>_
```


Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/6782856/531
WIndows10VM-V2v3-new
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Server_Domain - VMware Workstation 14 Player (Non-commercial use only)
Player
Administrator: Command Prompt
4:19 AM
11/27/2025
Console

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b56f:5dab:598a:5b2f%6
   IPv4 Address. . . . . . . . . . . : 192.168.2.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

Tunnel adapter isatap.{FCEBD5D7-3DD6-4B77-BCDC-9D39846C8AA2}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>_
```

```
GNS3 management console.
Running GNS3 version 2.1.11 on Windows (64-bit) with Python 3.6.6 Qt 5.9.1 and PyQt 5.9.
Copyright (c) 2006-2025 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.
```

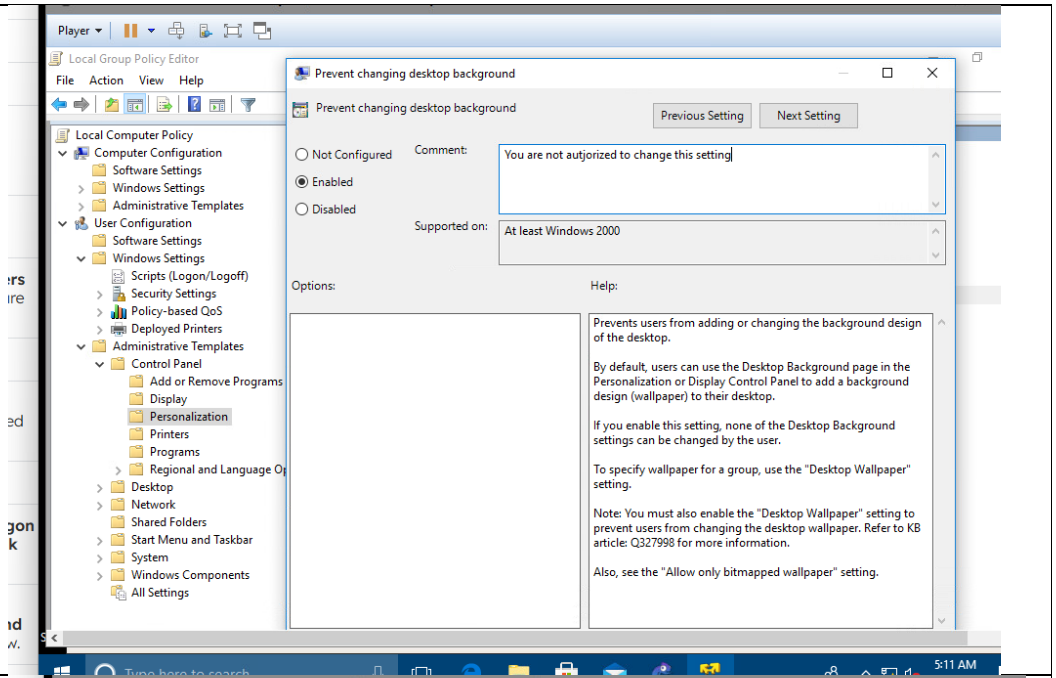
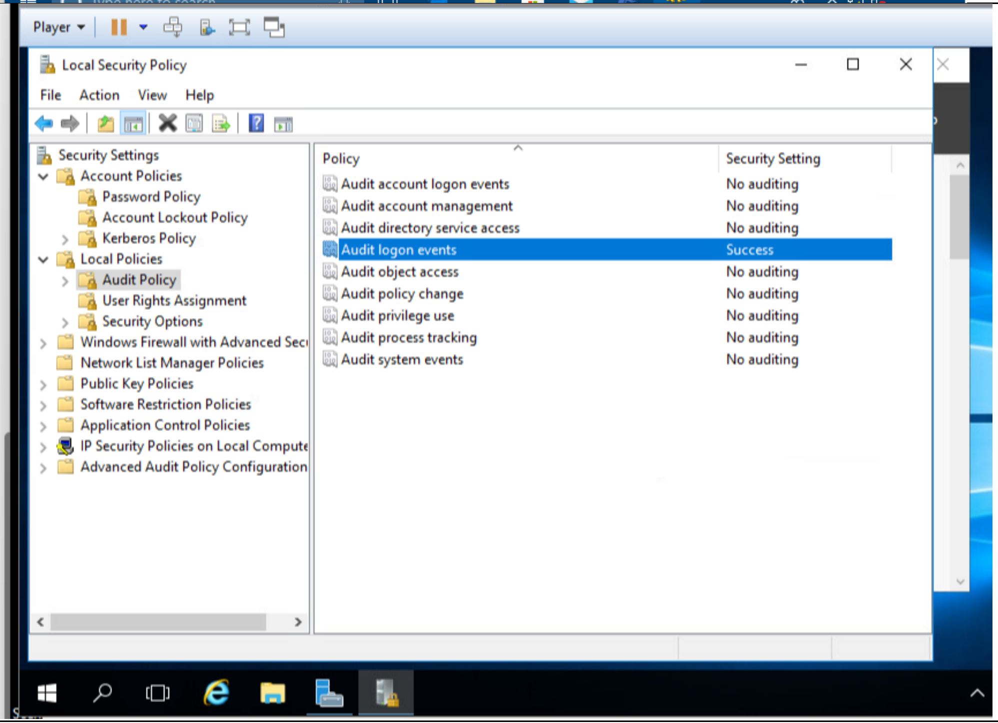
Group Policy Changes

Change Windows User Account Control (UAC) prompt	
Change local password policy setting.	

Player
Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
4:55 AM
11/27/2025
2 errors

Policy	Security Setting
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Warning: You are about to do something that is not authorized
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Enabled
Microsoft network server: Digitally sign communications (if ...	Enabled
Microsoft network server: Disconnect clients when logon ho...	Enabled

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Change desktop background user rights assignment (disable non-admin change capability).	
Configure local audit policy setting.	

Prevent changing desktop background

○ Not Configured
● Enabled
○ Disabled

Comment: You are not autjorized to change this setting

Supported on: At least Windows 2000

Options:

Help:

Prevents users from adding or changing the background design of the desktop.

By default, users can use the Desktop Background page in the Personalization or Display Control Panel to add a background design (wallpaper) to their desktop.

If you enable this setting, none of the Desktop Background settings can be changed by the user.

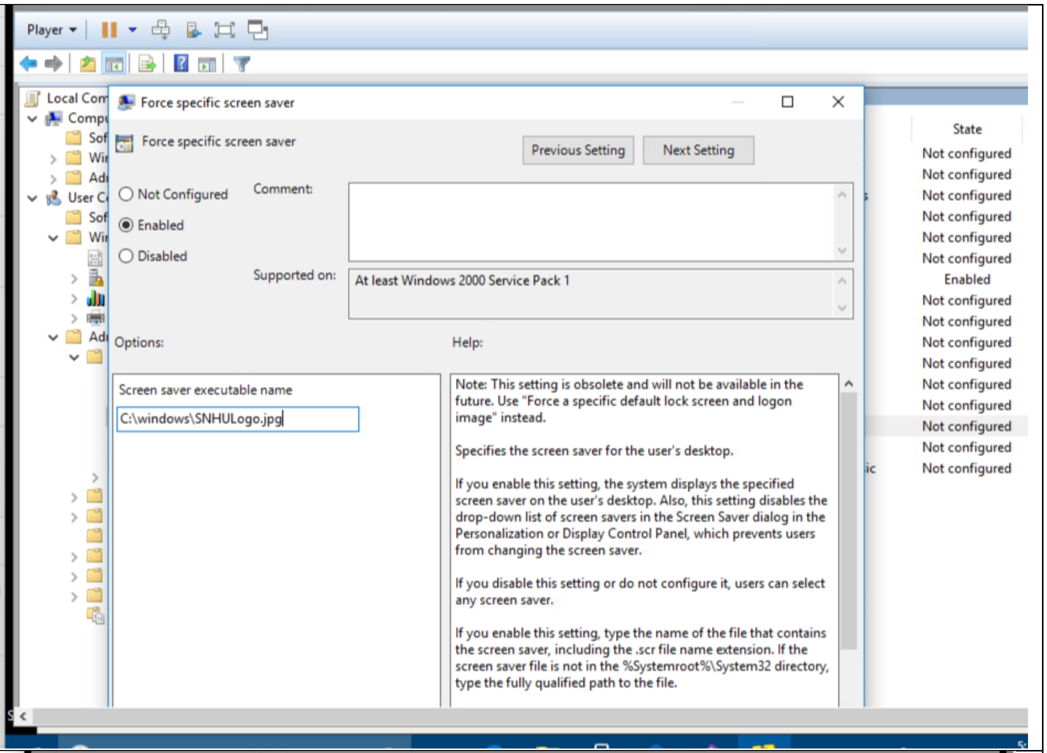
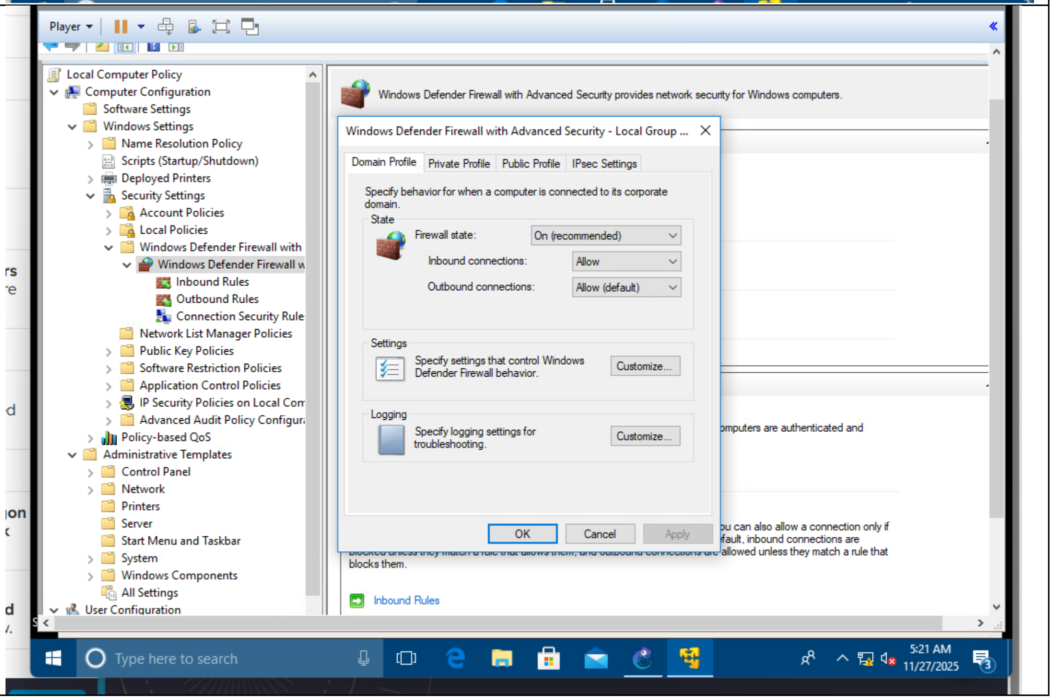
To specify wallpaper for a group, use the "Desktop Wallpaper" setting.

Note: You must also enable the "Desktop Wallpaper" setting to prevent users from changing the desktop wallpaper. Refer to KB article: Q327998 for more information.

Also, see the "Allow only bitmapped wallpaper" setting.

Local Security Policy

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	Success
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Configure default logon banner (warning that requires direct affirmation to continue).	 Force specific screen saver Force specific screen saver Previous Setting Next Setting ○ Not Configured ● Enabled ○ Disabled Comment: Supported on: At least Windows 2000 Service Pack 1 Options: Screen saver executable name C:\windows\SNHULogo.jpg Help: Note: This setting is obsolete and will not be available in the future. Use "Force a specific default lock screen and logon image" instead. Specifies the screen saver for the user's desktop. If you enable this setting, the system displays the specified screen saver on the user's desktop. Also, this setting disables the drop-down list of screen savers in the Screen Saver dialog in the Personalization or Display Control Panel, which prevents users from changing the screen saver. If you disable this setting or do not configure it, users can select any screen saver. If you enable this setting, type the name of the file that contains the screen saver, including the .scr file name extension. If the screen saver file is not in the %Systemroot%\System32 directory, type the fully qualified path to the file. State Not configured Not configured Not configured Not configured Not configured Not configured Enabled Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured
Change default Windows firewall profile.	 Windows Defender Firewall with Advanced Security provides network security for Windows computers. Windows Defender Firewall with Advanced Security - Local Group ... Domain Profile Private Profile Public Profile IPsec Settings Specify behavior for when a computer is connected to its corporate domain. State Firewall state: On (recommended) Inbound connections: Allow Outbound connections: Allow (default) Settings Specify settings that control Windows Defender Firewall behavior. Customize... Logging Specify logging settings for troubleshooting. Customize... OK Cancel Apply Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Windows Defender Firewall with Windows Defender Firewall w Inbound Rules Outbound Rules Connection Security Rule Network List Manager Policies Public Key Policies Software Restriction Policies Application Control Policies IP Security Policies on Local Com Advanced Audit Policy Configur Policy-based QoS Administrative Templates Control Panel Network Printers Server Start Menu and Taskbar System Windows Components All Settings User Configuration Type here to search 5:21 AM 11/27/2025

Justification for Virtual Systems

There are several benefits to using virtualization technology in sandboxing. One great benefit is that it can be an isolated system. If you are unsure if it will run properly or cause any issues you can separate it from the production environment while you conduct your testing. Once you have configured the way you need to have it you can make those changes in the production version. Another benefit is if it doesn't work right, you can easily scrap it. By not using your production version and changes that aren't up to the standards can be removed and started over. It is simple as rolling back to a clone of a well-known version. A third benefit is cross platform testing. You can create virtual machines of different operating systems to see how the program will run in different environments.

Along with benefits of using virtualization there are also drawbacks to using it as well. One of these is higher resource usage. You need to have more CPU, RAM and power to be able to run multiple sandboxes at a time. Another drawback is increased complexity. VM's add another layer of to an environment because they need to be configured properly in order to closely mimic production environments.

One way that virtualization can be used other than sandboxing is server virtualization. A company can consolidate multiple physical servers into a single physical machine, which improves hardware utilization and allows for flexible management of server resources. Another thing that can be used for is network virtualization. One can create virtual networks that are independent of the underlying physical hardware, enhancing cloud scalability and management.

References: