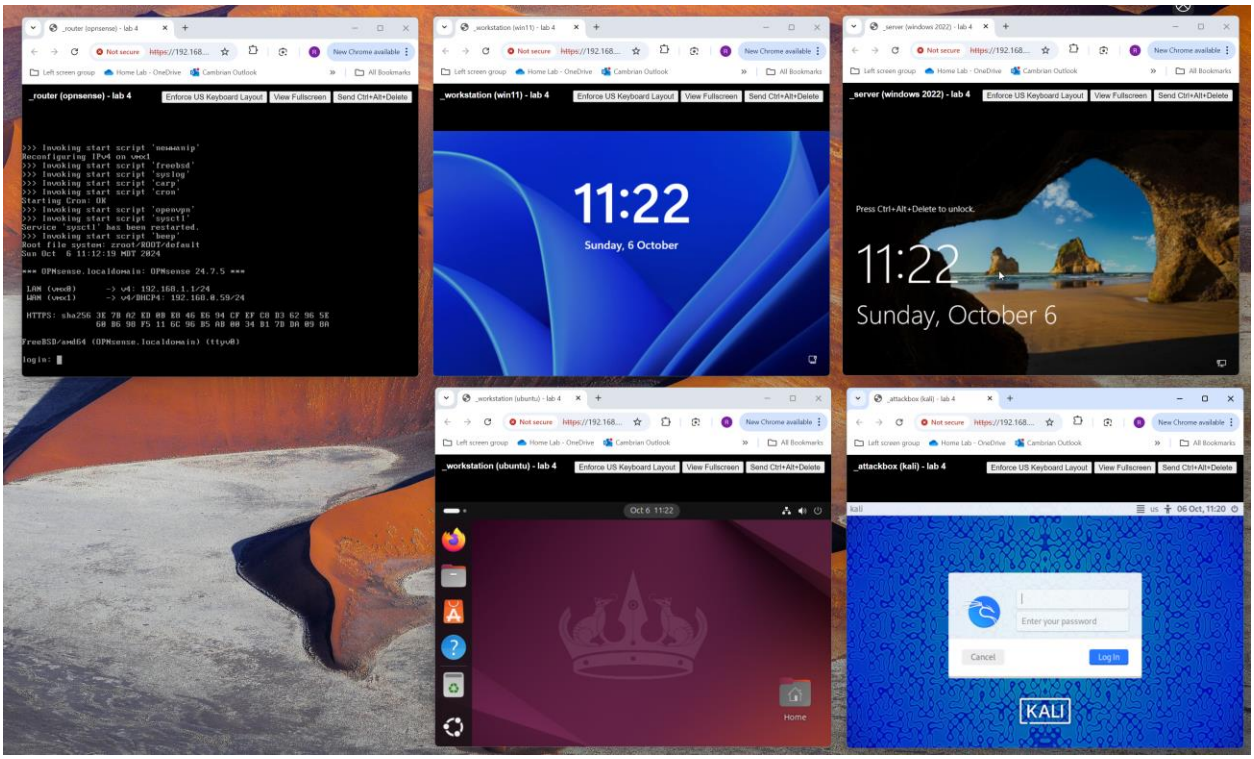
192.168.0.47

- _attackbox (kali) - lab 4
- _router (opnsense) - lab 4
- _server (windows 2022) - lab 4
- _workstation (ubuntu) - lab 4
- _workstation (win11) - lab 4

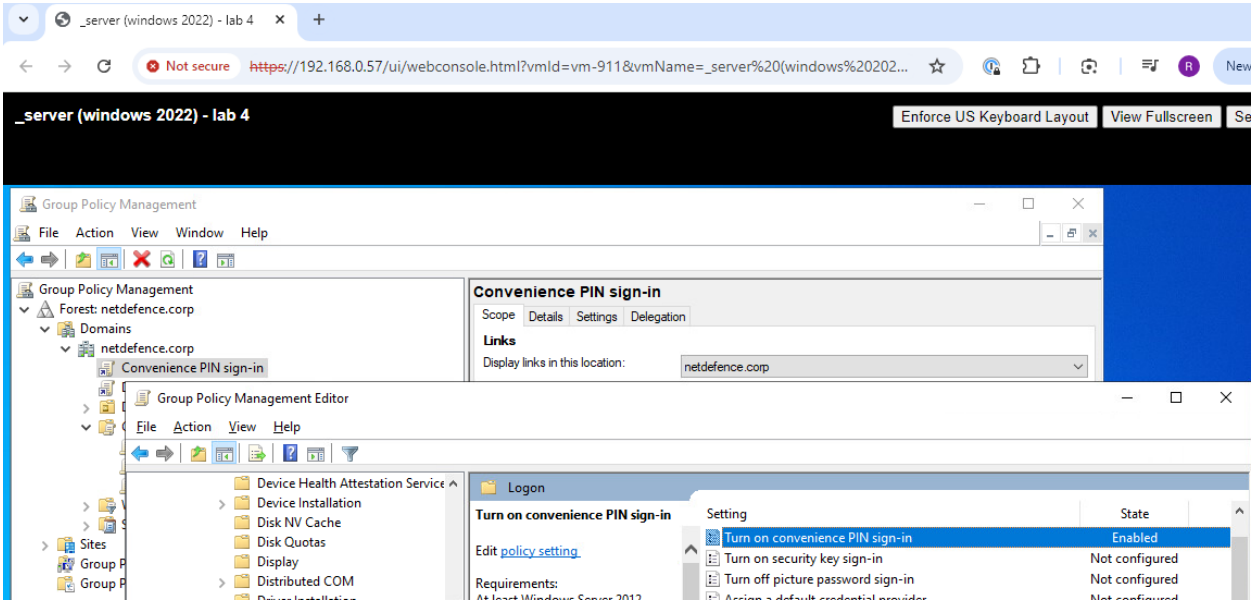


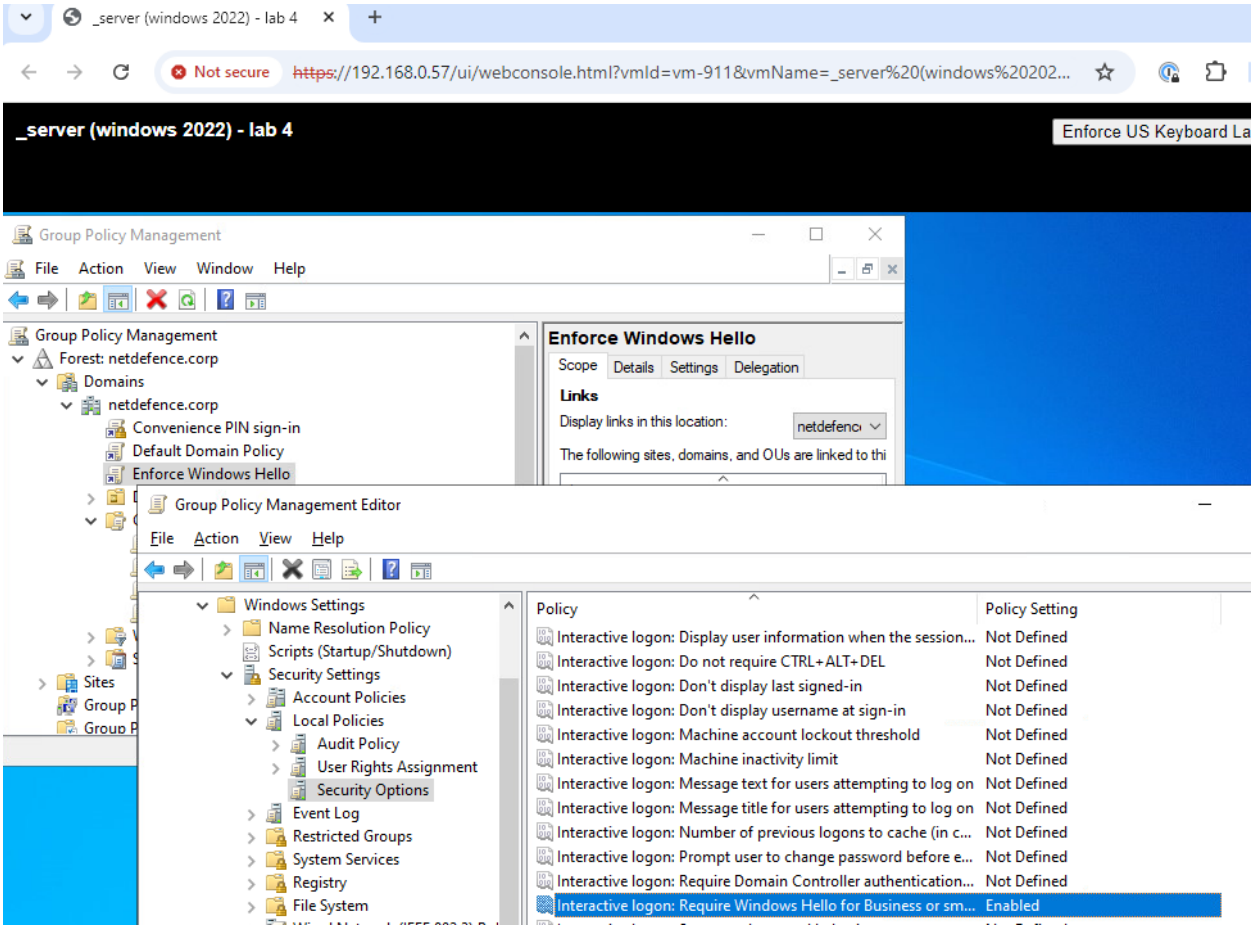
Part 1: Configure Multi-Factor Authentication on Windows 11 Enterprise

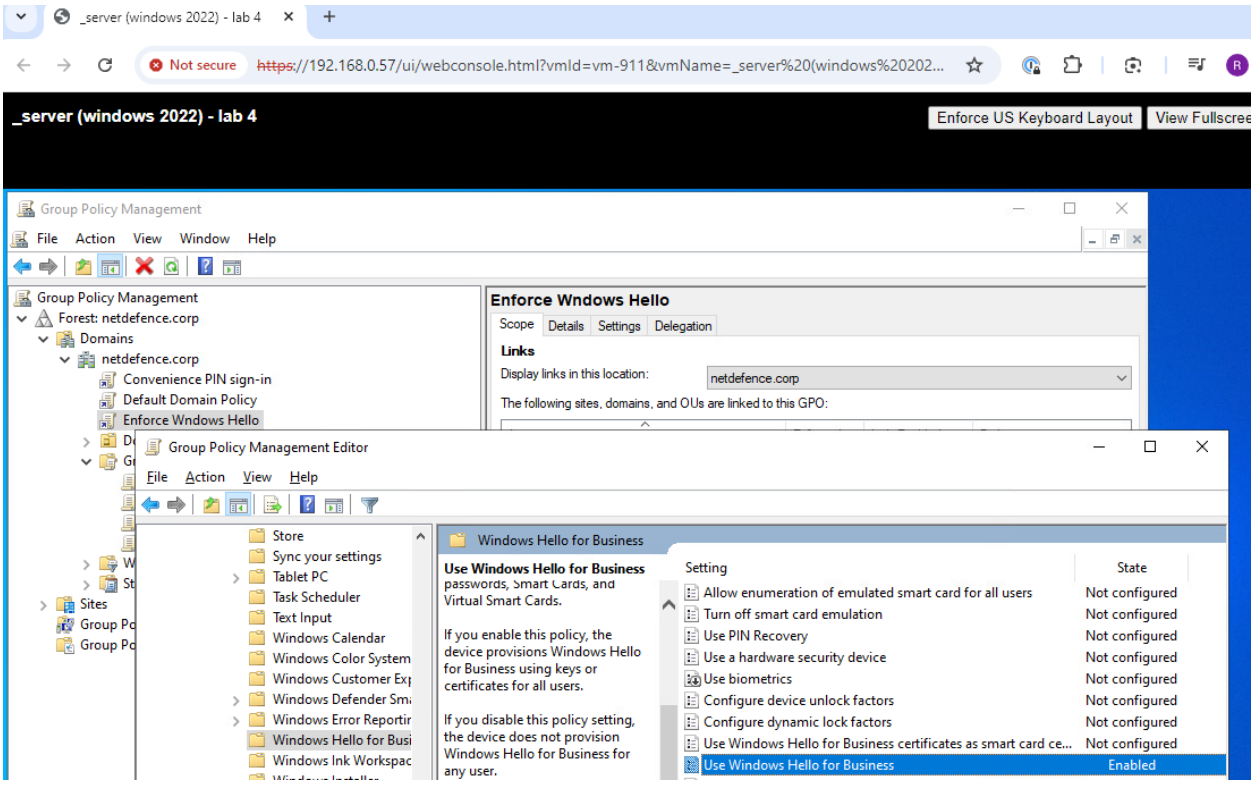
1. **Open Settings:**
    - Navigate to `Start` > `Settings` > `Accounts` > `Sign-in options`.
2. **Enable Windows Hello:**
    - Under `Windows Hello`, configure fingerprint, face recognition, or a PIN.
3. **Set Up MFA:**
    - Open `Microsoft Authenticator` app on your mobile device.
    - Sign in to your Microsoft account and follow the prompts to complete the setup.
4. **Verify MFA:**
    - Sign out and sign back in to ensure MFA is working.

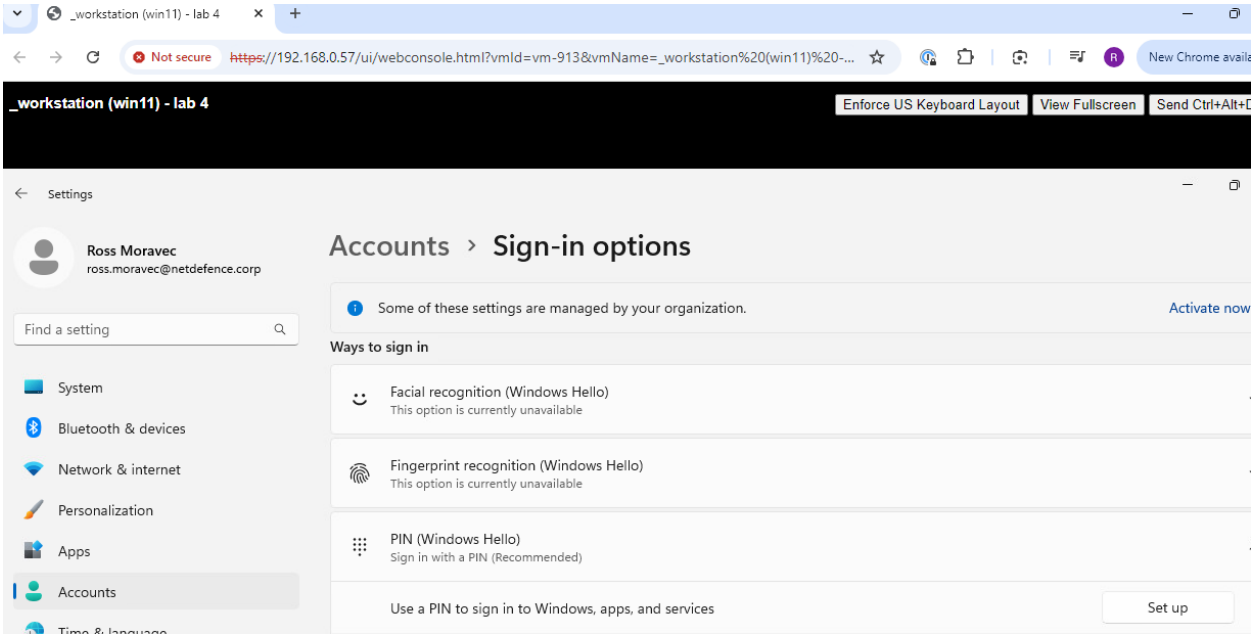
Deliverables:

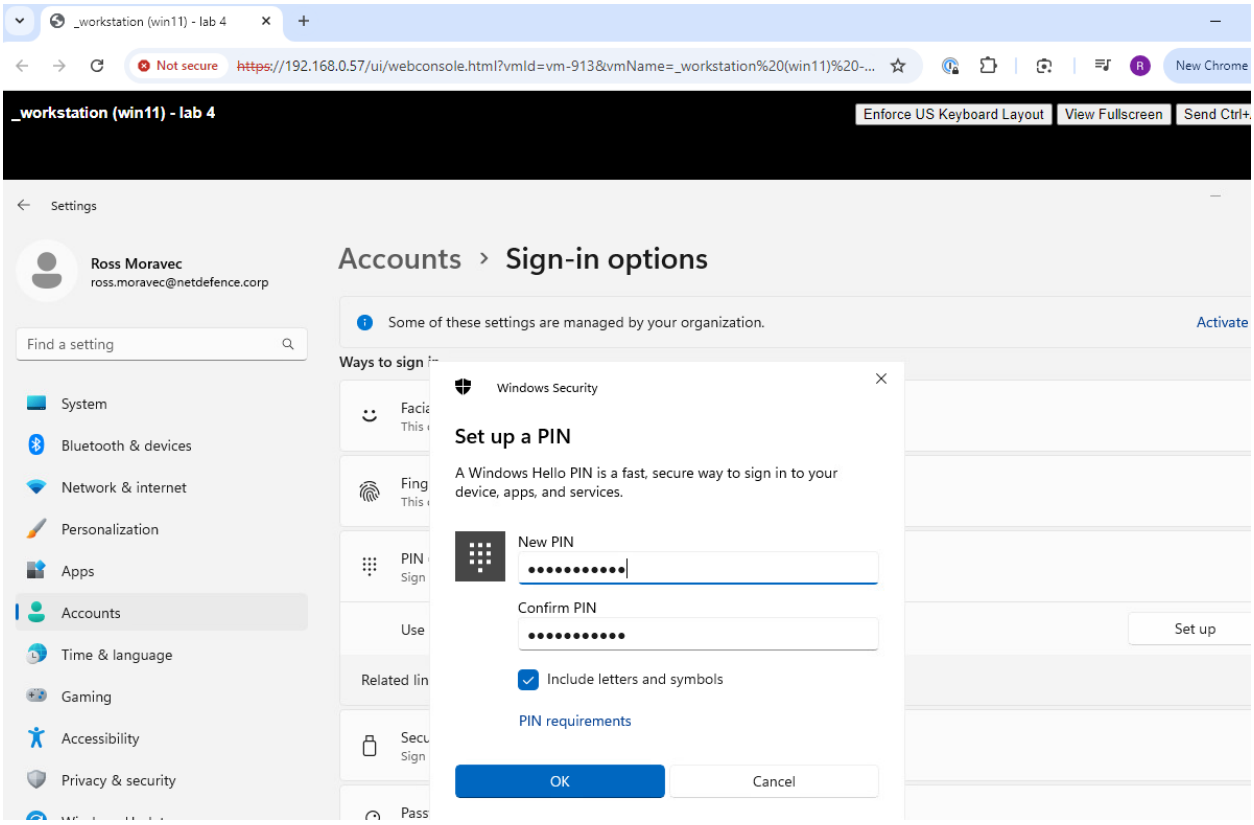
- Screenshot of the `Sign-in options` page showing configured Windows Hello.
- Screenshot of the MFA setup completion on the mobile device.

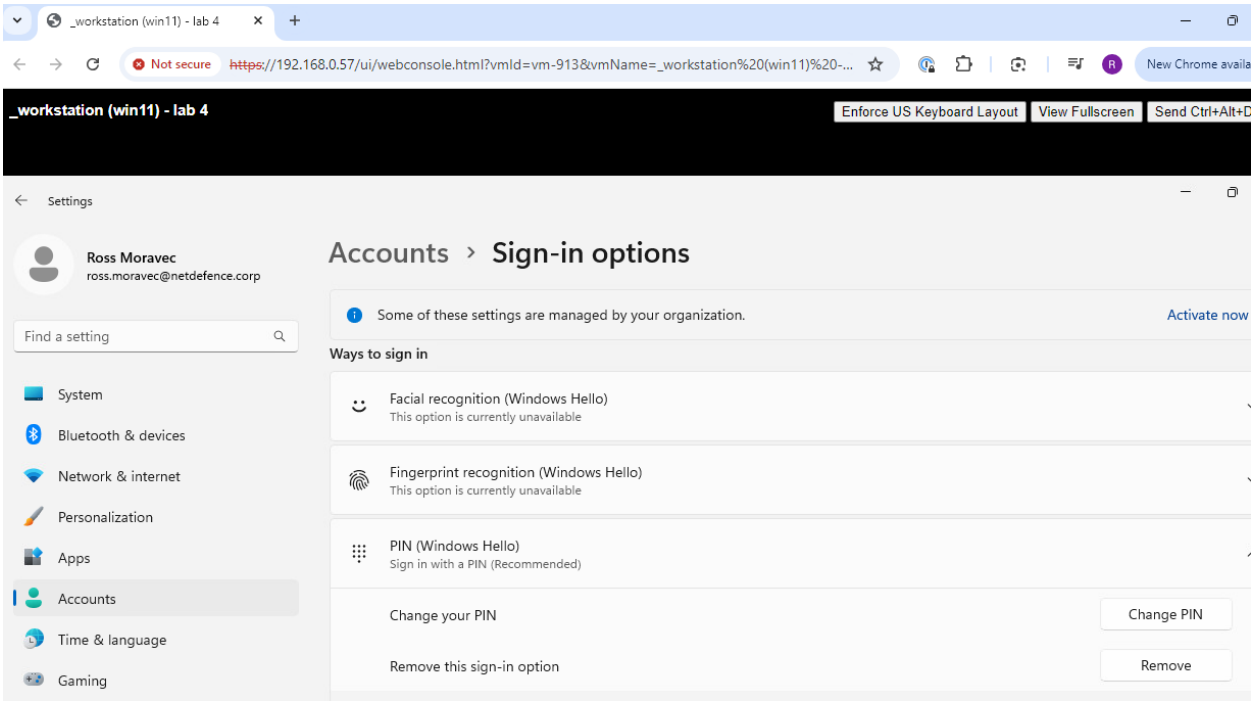


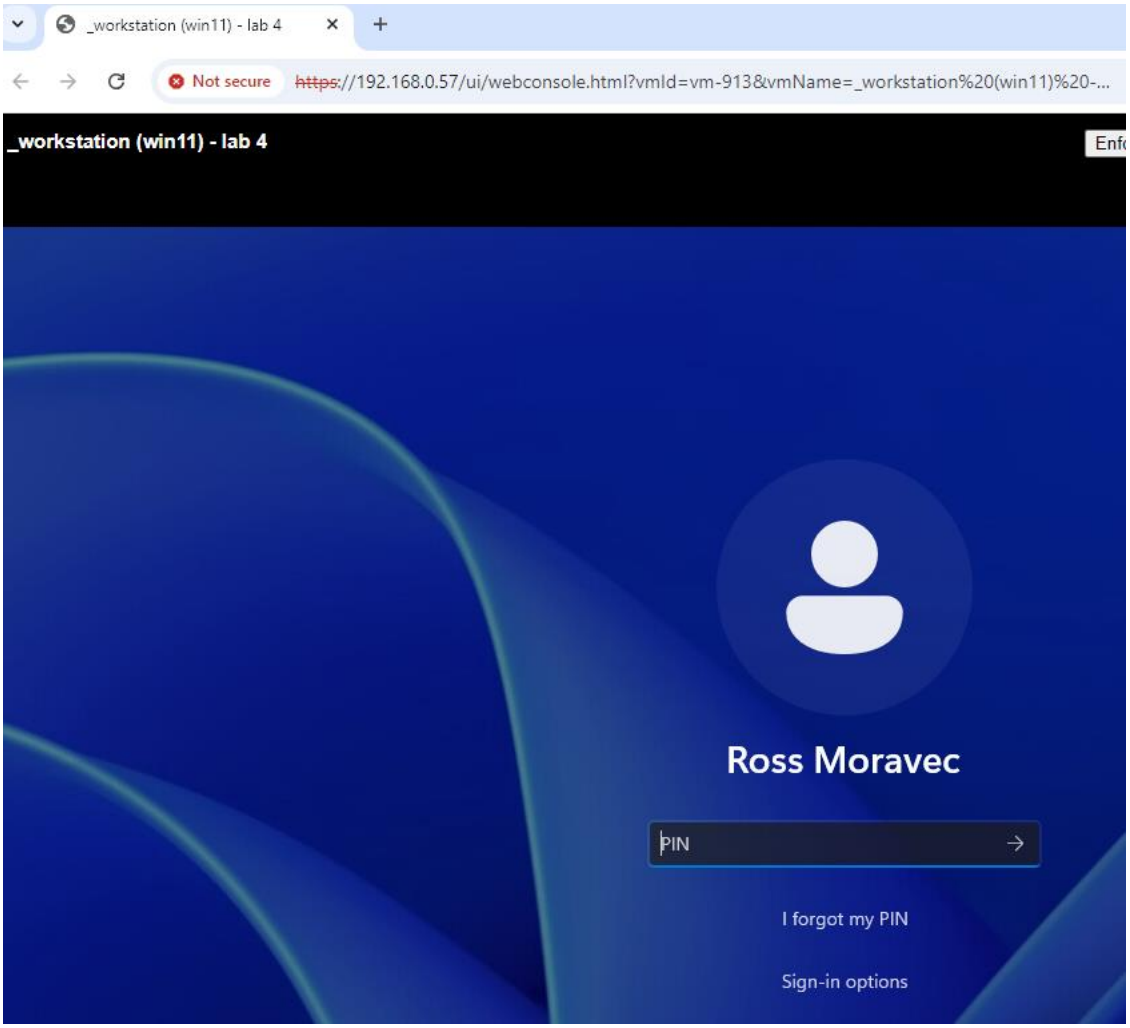

_server (windows 2022) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-911&vmName=_server%20(windows%20202...
_server (windows 2022) - lab 4
Enforce US Keyboard La
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: netdefence.corp
Domains
netdefence.corp
Convenience PIN sign-in
Default Domain Policy
Enforce Windows Hello
Enforce Windows Hello
Scope Details Settings Delegation
Links
Display links in this location:
netdefenc
The following sites, domains, and OUs are linked to thi
Group Policy Management Editor
File Action View Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Sites
Policy
Policy Setting
Interactive logon: Display user information when the session... Not Defined
Interactive logon: Do not require CTRL+ALT+DEL Not Defined
Interactive logon: Don't display last signed-in Not Defined
Interactive logon: Don't display username at sign-in Not Defined
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 Not Defined
Interactive logon: Message title for users attempting to log on Not Defined
Interactive logon: Number of previous logons to cache (in c... Not Defined
Interactive logon: Prompt user to change password before e... Not Defined
Interactive logon: Require Domain Controller authentication... Not Defined
Interactive logon: Require Windows Hello for Business or sm... Enabled


_server (windows 2022) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-911&vmName=_server%20(windows%20202...
_server (windows 2022) - lab 4
Enforce US Keyboard Layout
View Fullscree
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: netdefence.corp
Domains
netdefence.corp
Convenience PIN sign-in
Default Domain Policy
Enforce Wndows Hello
Sites
Enforce Wndows Hello
Scope Details Settings Delegation
Links
Display links in this location:
netdefence.corp
The following sites, domains, and OUs are linked to this GPO:
Group Policy Management Editor
File Action View Help
Store
Sync your settings
Tablet PC
Task Scheduler
Text Input
Windows Calendar
Windows Color System
Windows Customer Exp
Windows Defender Sma
Windows Error Reportir
Windows Hello for Busi
Windows Ink Workspac
Windows Hello for Business
Use Windows Hello for Business passwords, Smart Cards, and Virtual Smart Cards.
If you enable this policy, the device provisions Windows Hello for Business using keys or certificates for all users.
If you disable this policy setting, the device does not provision Windows Hello for Business for any user.
Setting
State
Allow enumeration of emulated smart card for all users
Not configured
Turn off smart card emulation
Not configured
Use PIN Recovery
Not configured
Use a hardware security device
Not configured
Use biometrics
Not configured
Configure device unlock factors
Not configured
Configure dynamic lock factors
Not configured
Use Windows Hello for Business certificates as smart card ce...
Not configured
Use Windows Hello for Business
Enabled


_workstation (win11) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmName=_workstation%20(win11)%20-...
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+D
Settings
Ross Moravec
ross.moravec@netdefence.corp
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Accounts › Sign-in options
Some of these settings are managed by your organization.
Activate now
Ways to sign in
Facial recognition (Windows Hello)
This option is currently unavailable
Fingerprint recognition (Windows Hello)
This option is currently unavailable
PIN (Windows Hello)
Sign in with a PIN (Recommended)
Use a PIN to sign in to Windows, apps, and services
Set up


_workstation (win11) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmName=_workstation%20(win11)%20-...
New Chrome
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+
Settings
Ross Moravec
ross.moravec@netdefence.corp
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Accounts › Sign-in options
Some of these settings are managed by your organization.
Activate
Ways to sign
Windows Security
Set up a PIN
A Windows Hello PIN is a fast, secure way to sign in to your device, apps, and services.
New PIN
Confirm PIN
Include letters and symbols
PIN requirements
OK
Cancel
Set up


_workstation (win11) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmName=_workstation%20(win11)%20-...
New Chrome availa
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+D
Settings
Ross Moravec
ross.moravec@netdefence.corp
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accounts › Sign-in options
Some of these settings are managed by your organization.
Activate now
Ways to sign in
Facial recognition (Windows Hello)
This option is currently unavailable
Fingerprint recognition (Windows Hello)
This option is currently unavailable
PIN (Windows Hello)
Sign in with a PIN (Recommended)
Change your PIN
Change PIN
Remove this sign-in option
Remove

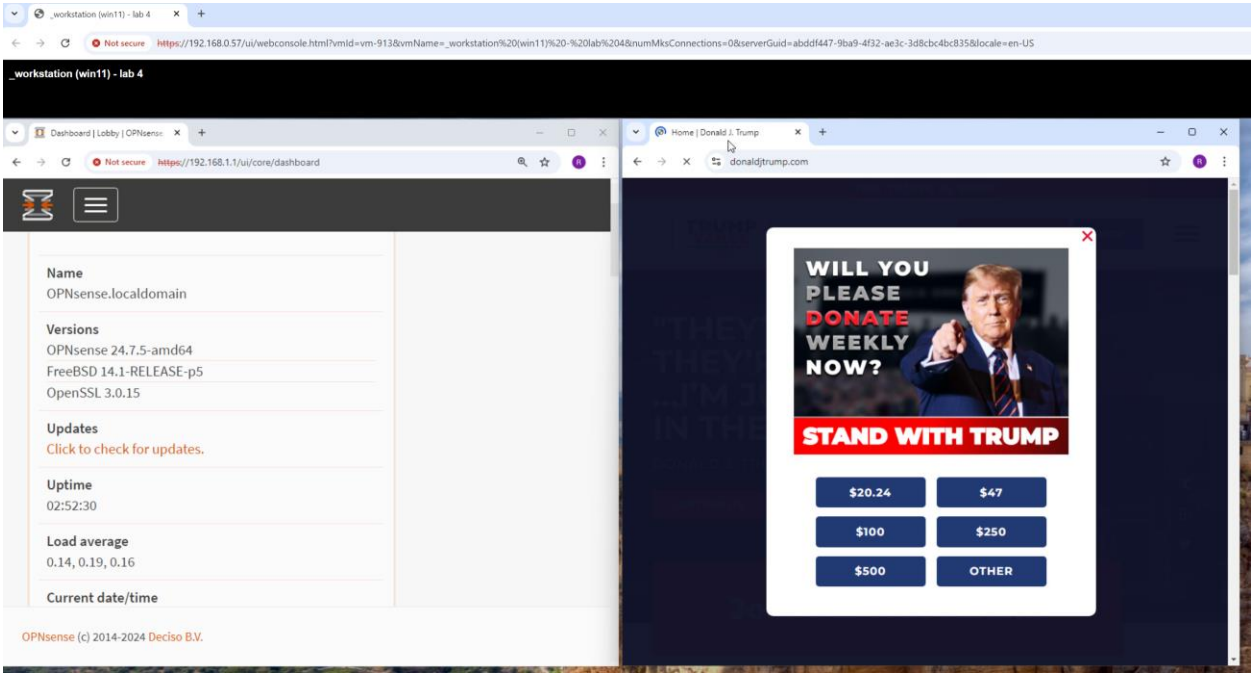


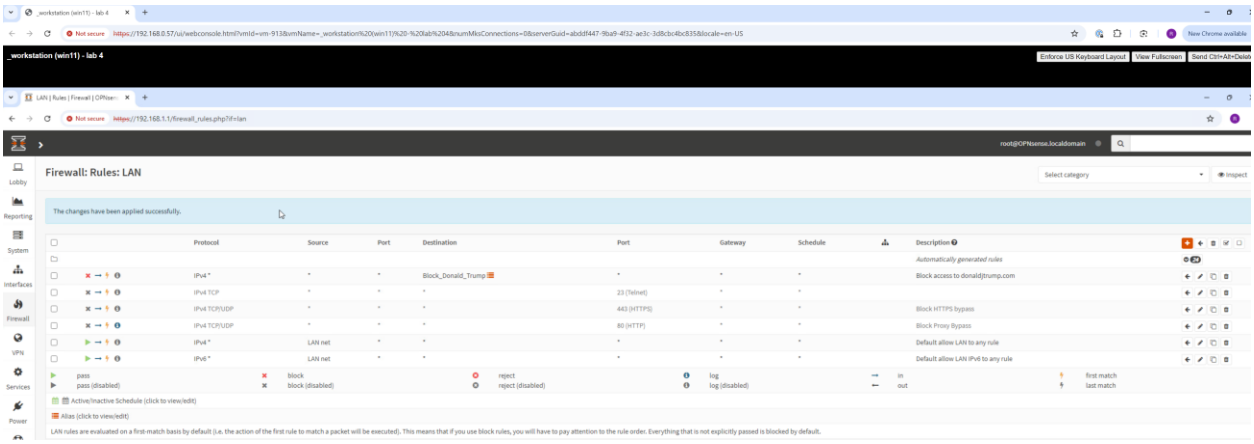
Part 2: Set Up Firewall Rules on OPNSense

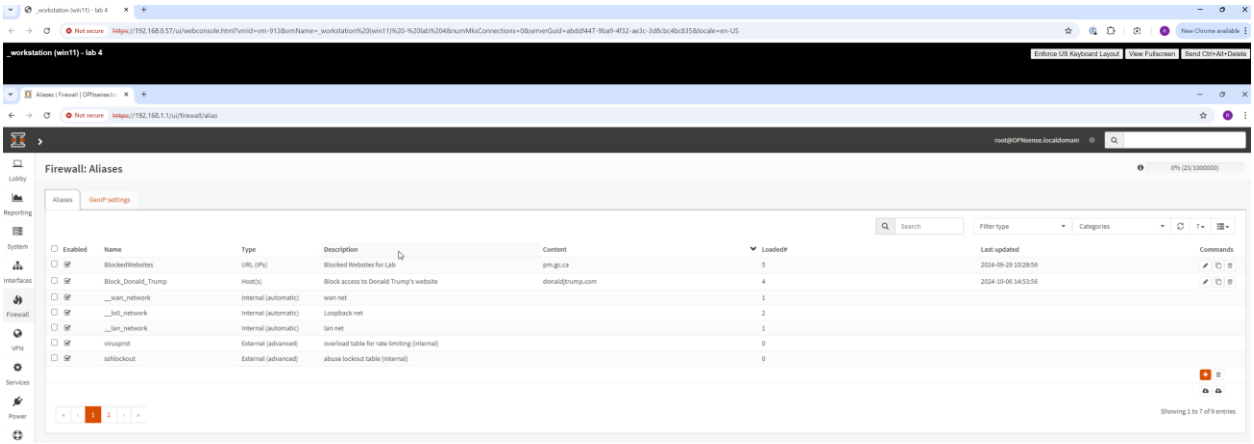
1. **Access OPNSense:**
   - Log in to OPNSense via a web browser using the IP address of the firewall.
2. **Navigate to Firewall Settings:**
   - Go to `Firewall` > `Rules` > `LAN`.
3. **Create New Rule:**
   - Click on `+ Add` to create a new rule.
   - Set `Action` to `Pass`, `Protocol` to `TCP/UDP`, and specify the source and destination as required.
4. **Apply Changes:**
   - Save and apply the changes.

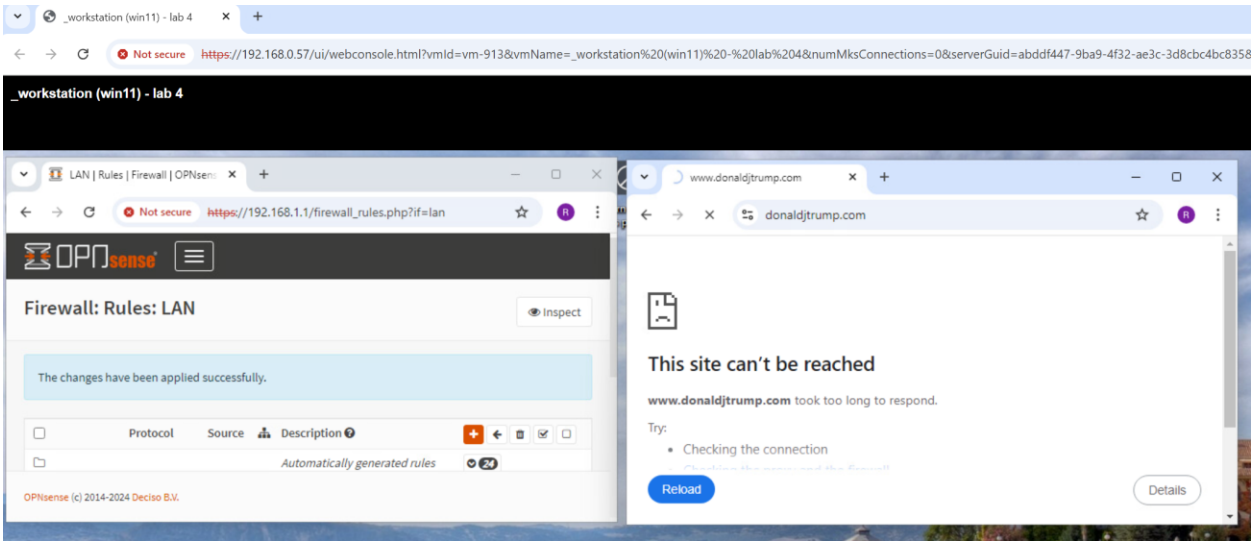
Deliverables:

- Screenshot of the firewall rules page showing the new rule.







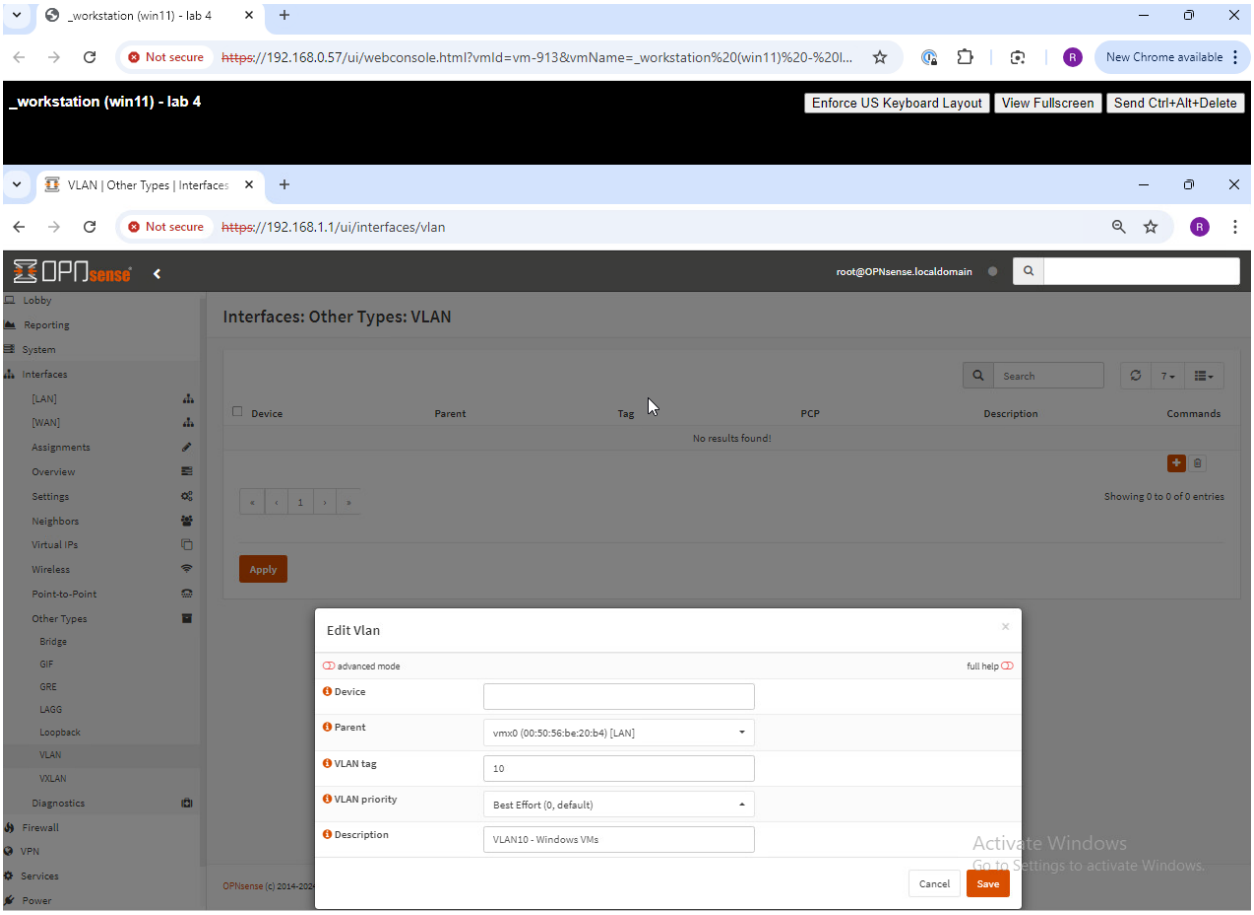


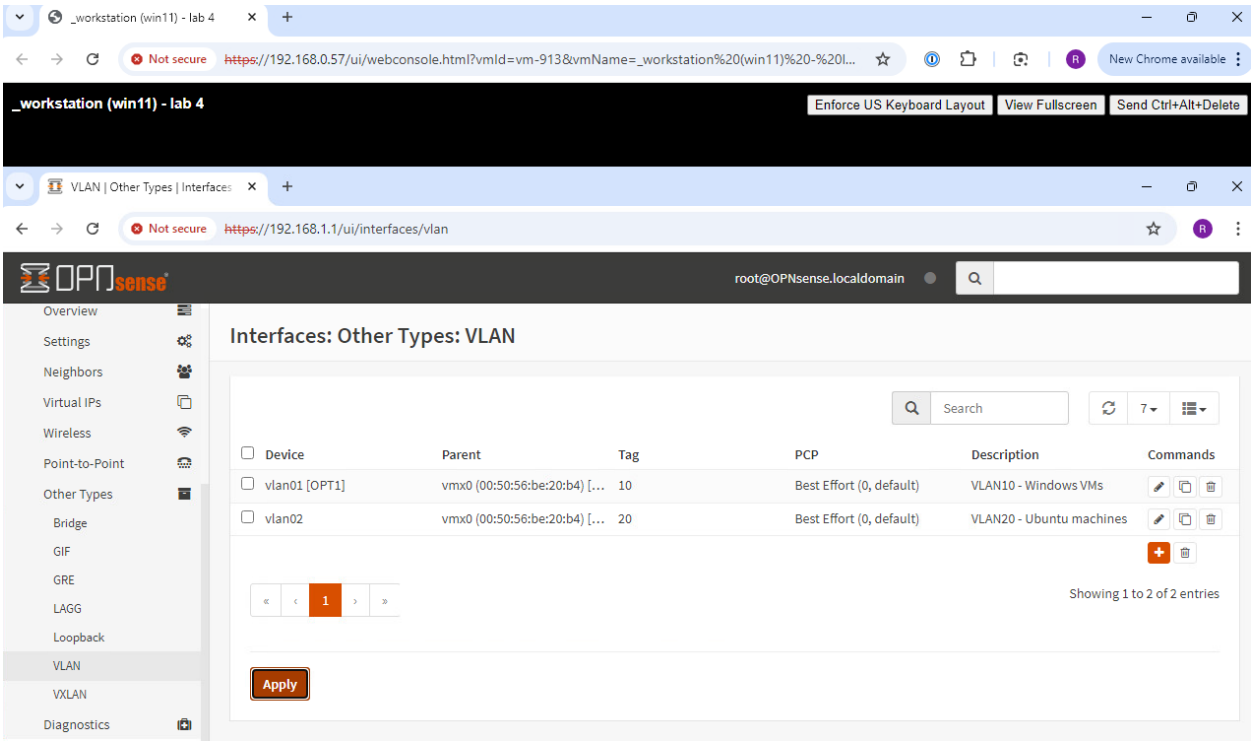
Part 3: Implement Network Segmentation using VLANs on OPNSense

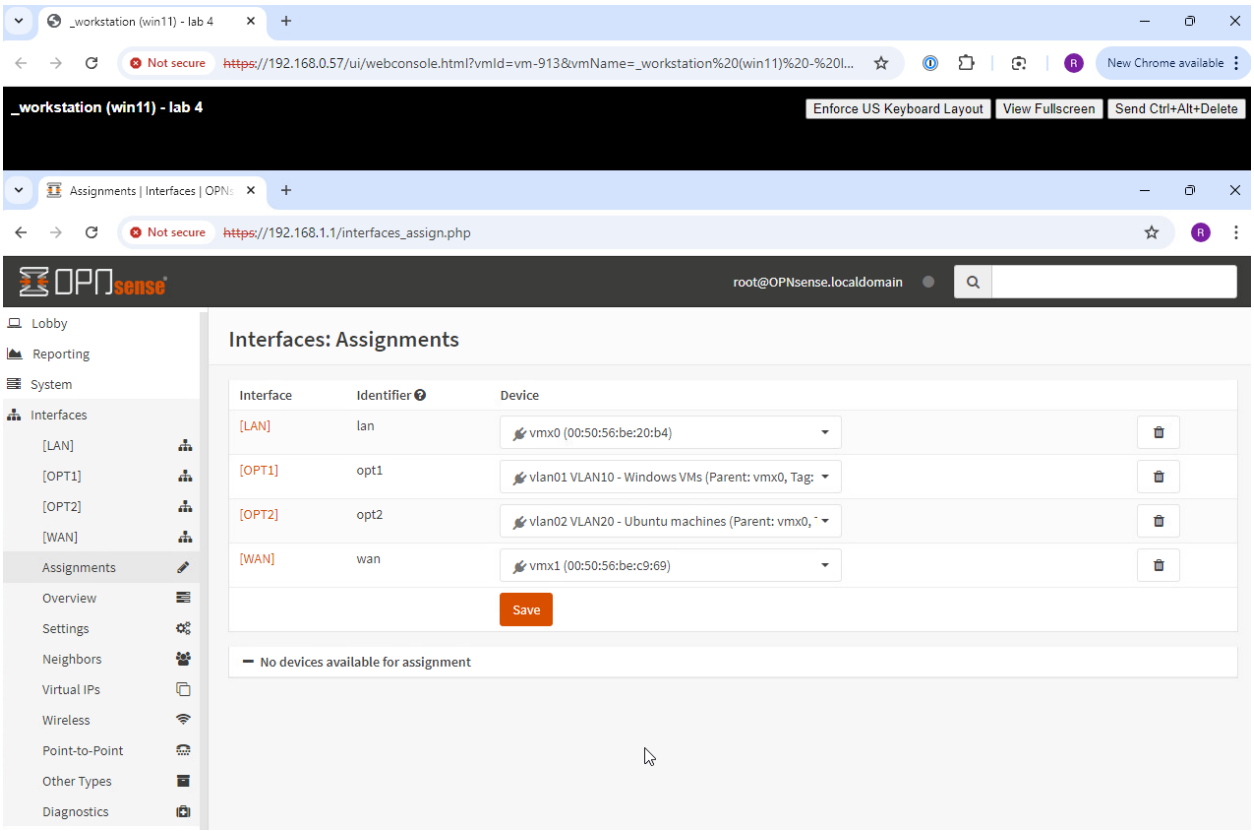
1. **Access VLAN Settings:**
   - Go to `Interfaces` > `Assignments` > `VLANs`.
2. **Create a New VLAN:**
   - Click `+ Add` to create a new VLAN.
   - Specify `Parent Interface`, `VLAN Tag`, and `Description`.
3. **Assign VLAN:**
   - Go to `Interfaces` > `Assignments` and assign the new VLAN to an interface.
4. **Configure VLAN Interface:**
   - Go to `Interfaces` > `(New VLAN)` and configure the interface settings.

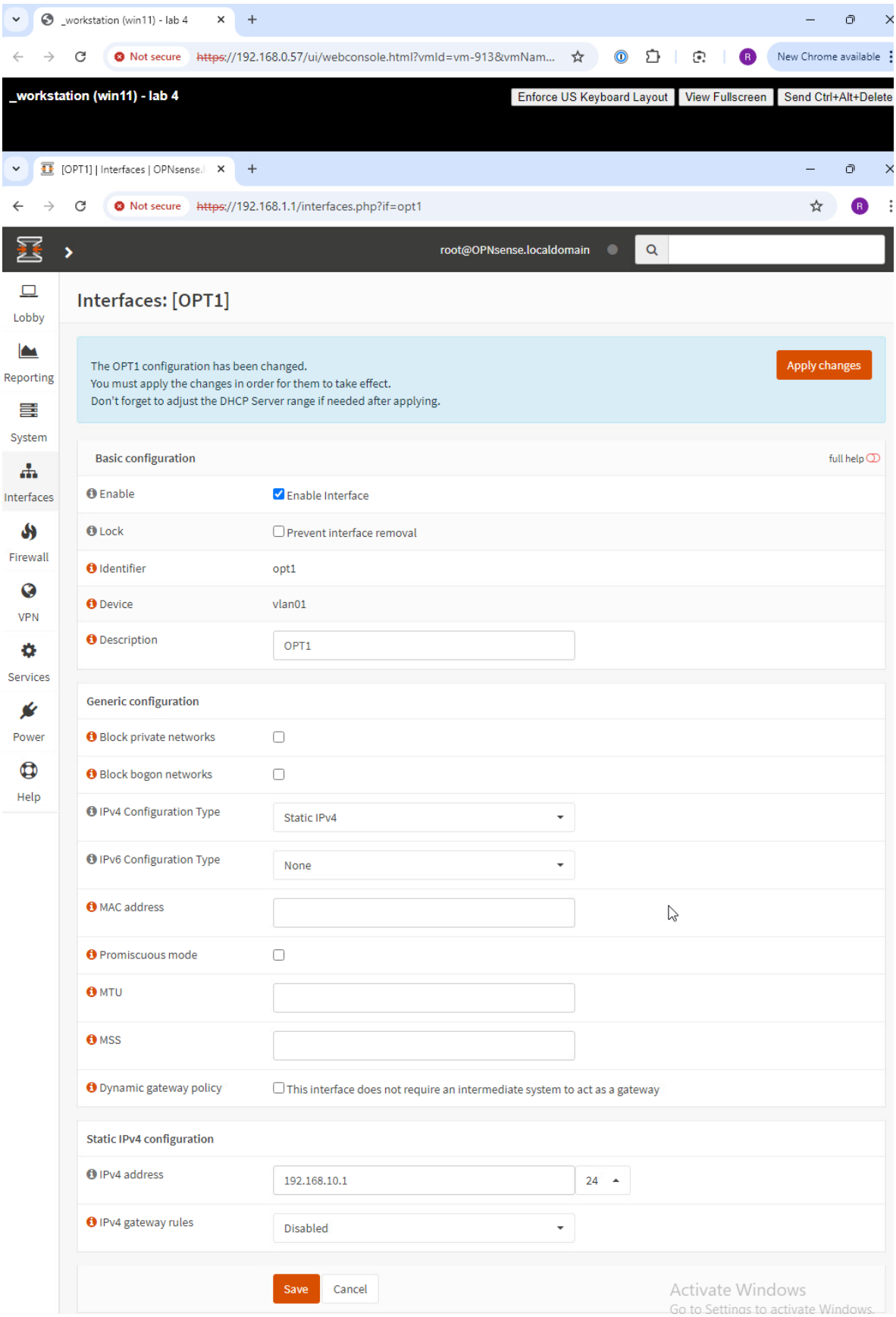
Deliverables:

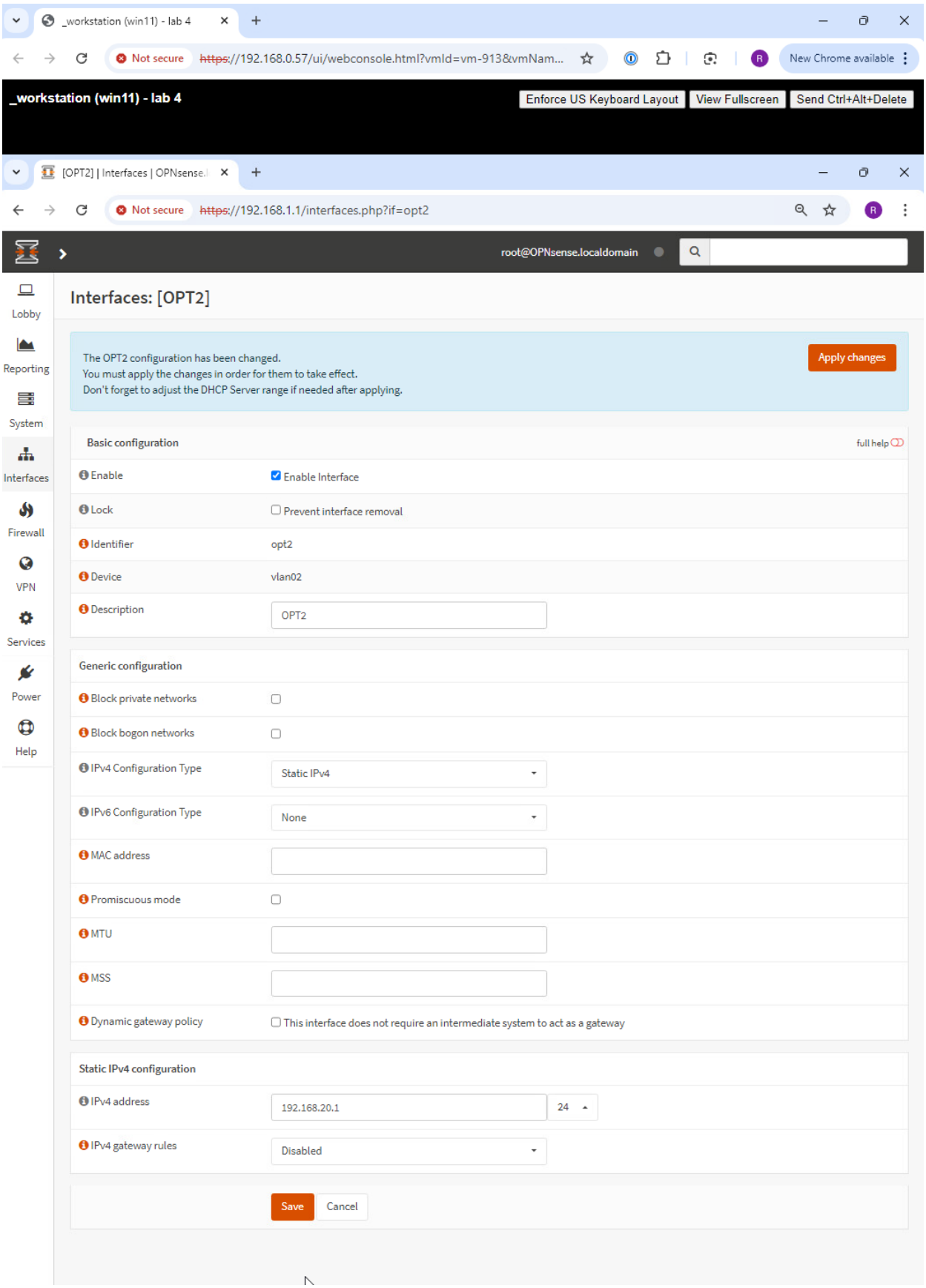
- Screenshot of the VLAN configuration page.
- Screenshot of the interface assignment page.

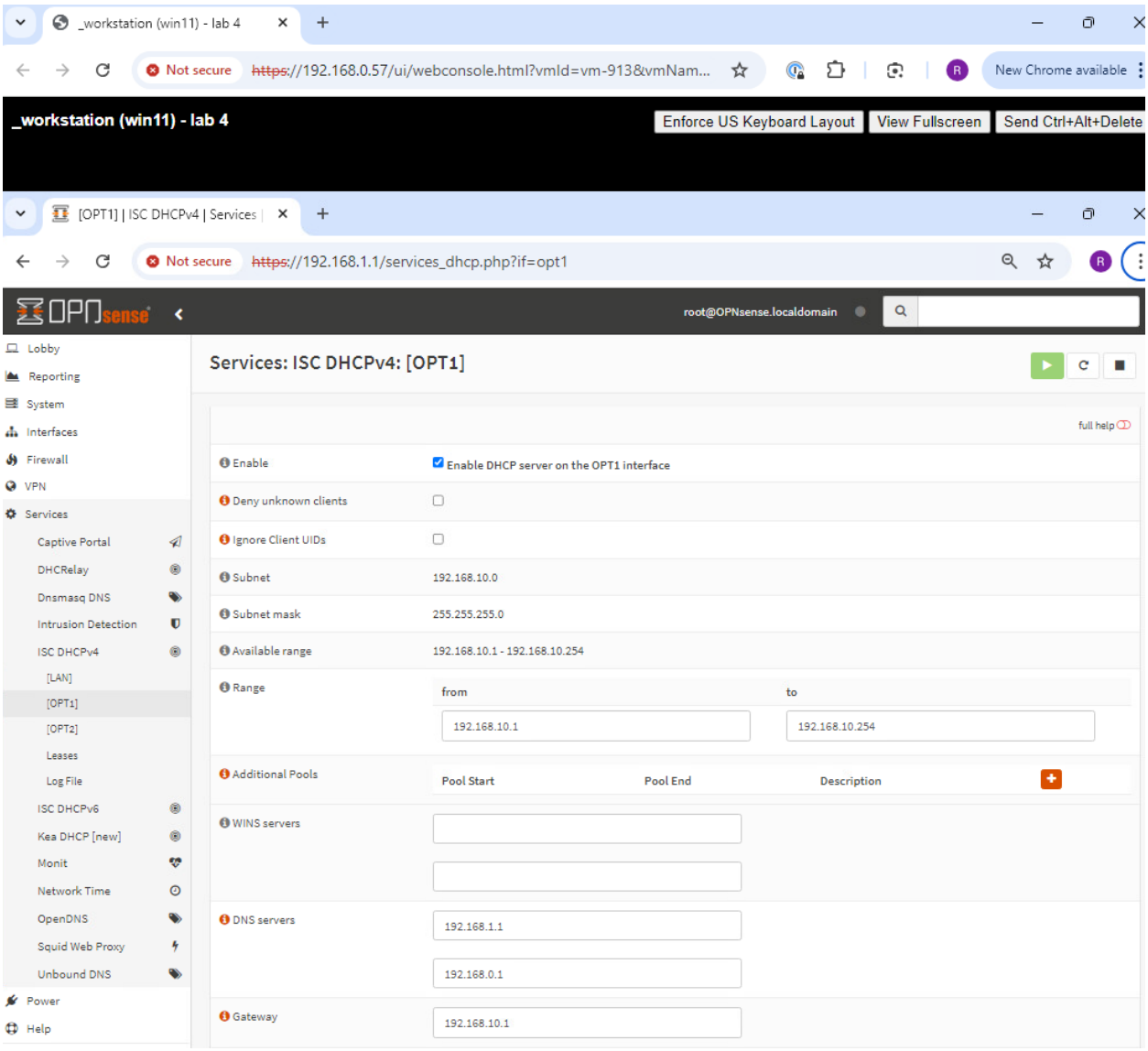

_workstation (win11) - lab 4
Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmName=_workstation%20(win11)%20-%20l...
New Chrome available
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
VLAN | Other Types | Interfaces
Not secure https://192.168.1.1/ui/interfaces/vlan
root@OPNsense.localdomain
Interfaces: Other Types: VLAN
Device
Parent
Tag
PCP
Description
Commands
No results found!
Showing 0 to 0 of 0 entries
Apply
Edit Vlan
advanced mode
full help
Device
Parent
vmx0 (00:50:56:be:20:b4) [LAN]
VLAN tag
10
VLAN priority
Best Effort (0, default)
Description
VLAN10 - Windows VMs
Cancel
Save
Activate Windows
Go to Settings to activate Windows.

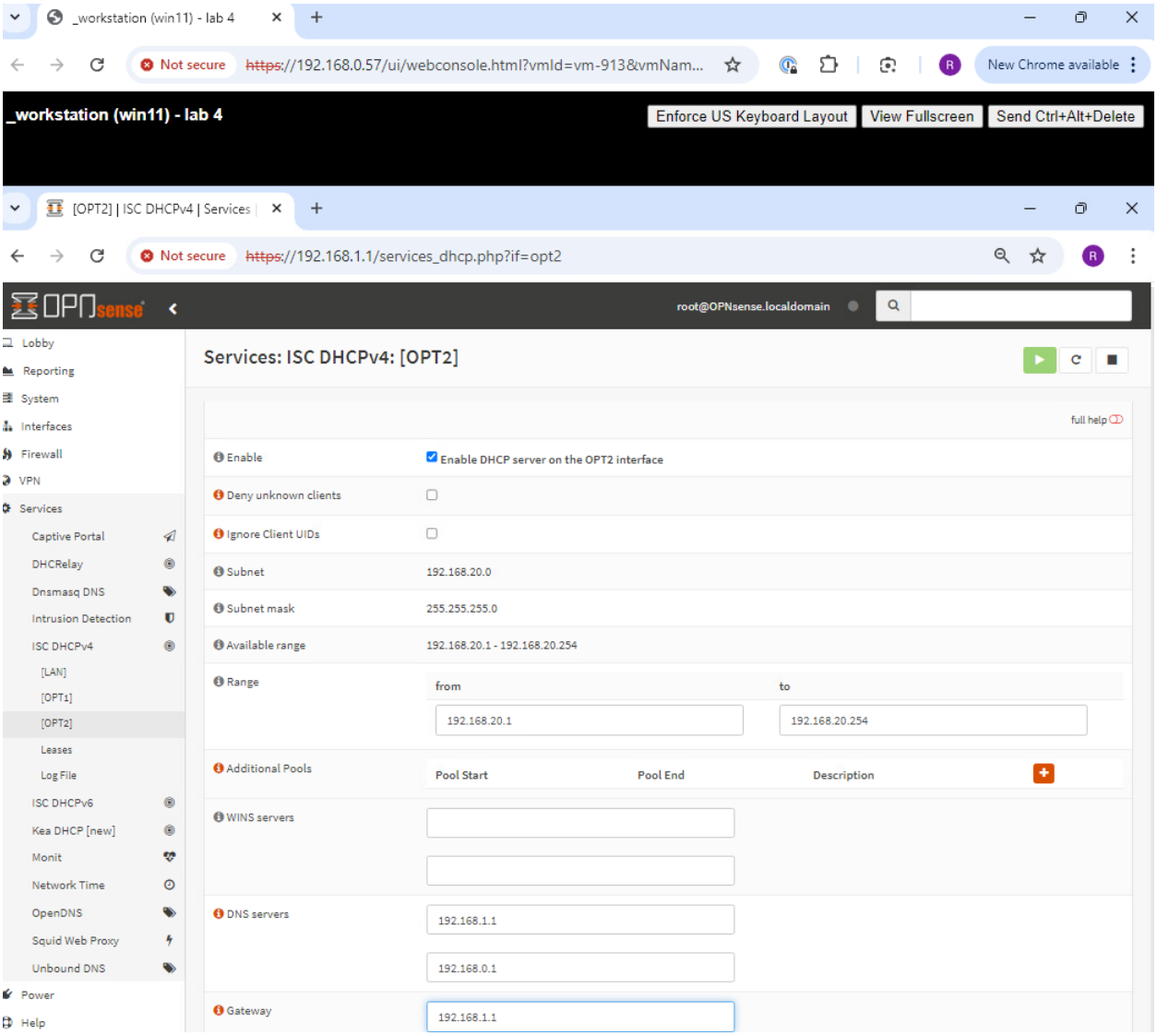

_workstation (win11) - lab 4
Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmName=_workstation%20(win11)%20-%20l...
New Chrome available
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
VLAN | Other Types | Interfaces
Not secure https://192.168.1.1/ui/interfaces/vlan
root@OPNsense.localdomain
Interfaces: Other Types: VLAN
Search
Device
Parent
Tag
PCP
Description
Commands
vlan01 [OPT1]
vmx0 (00:50:56:be:20:b4) [...
10
Best Effort (0, default)
VLAN10 - Windows VMs
vlan02
vmx0 (00:50:56:be:20:b4) [...
20
Best Effort (0, default)
VLAN20 - Ubuntu machines
Showing 1 to 2 of 2 entries
Apply


_workstation (win11) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmName=_workstation%20(win11)%20-%20l...
New Chrome available
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Assignments | Interfaces | OPN
Not secure
https://192.168.1.1/interfaces_assign.php
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
[LAN]
[OPT1]
[OPT2]
[WAN]
Assignments
Overview
Settings
Neighbors
Virtual IPs
Wireless
Point-to-Point
Other Types
Diagnostics
Interfaces: Assignments
Interface
Identifier
Device
[LAN]
lan
vmx0 (00:50:56:be:20:b4)
[OPT1]
opt1
vlan01 VLAN10 - Windows VMs (Parent: vmx0, Tag:
[OPT2]
opt2
vlan02 VLAN20 - Ubuntu machines (Parent: vmx0,
[WAN]
wan
vmx1 (00:50:56:be:c9:69)
Save
No devices available for assignment


_workstation (win11) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmNam...
New Chrome available
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
[OPT1] | Interfaces | OPNsense
Not secure
https://192.168.1.1/interfaces.php?if=opt1
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Power
Help
Interfaces: [OPT1]
The OPT1 configuration has been changed.
You must apply the changes in order for them to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.
Apply changes
Basic configuration
full help
Enable
Enable Interface
Lock
Prevent interface removal
Identifier
opt1
Device
vlan01
Description
OPT1
Generic configuration
Block private networks
Block bogon networks
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC address
Promiscuous mode
MTU
MSS
Dynamic gateway policy
This interface does not require an intermediate system to act as a gateway
Static IPv4 configuration
IPv4 address
192.168.10.1
24
IPv4 gateway rules
Disabled
Save
Cancel
Activate Windows
Go to Settings to activate Windows.


_workstation (win11) - lab 4
Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmNam...
New Chrome available
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
[OPT2] | Interfaces | OPNsense.
Not secure https://192.168.1.1/interfaces.php?if=opt2
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Power
Help
Interfaces: [OPT2]
The OPT2 configuration has been changed.
You must apply the changes in order for them to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.
Apply changes
Basic configuration
full help
Enable
Enable Interface
Lock
Prevent interface removal
Identifier
opt2
Device
vlan02
Description
OPT2
Generic configuration
Block private networks
Block bogon networks
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC address
Promiscuous mode
MTU
MSS
Dynamic gateway policy
This interface does not require an intermediate system to act as a gateway
Static IPv4 configuration
IPv4 address
192.168.20.1
24
IPv4 gateway rules
Disabled
Save
Cancel


_workstation (win11) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-913&vmNam...
New Chrome available
_workstation (win11) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
[OPT1] | ISC DHCPv4 | Services
Not secure
https://192.168.1.1/services_dhcp.php?if=opt1
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Captive Portal
DHCRelay
Dnsmasq DNS
Intrusion Detection
ISC DHCPv4
[LAN]
[OPT1]
[OPT2]
Leases
Log File
ISC DHCPv6
Kea DHCP [new]
Monit
Network Time
OpenDNS
Squid Web Proxy
Unbound DNS
Power
Help
Services: ISC DHCPv4: [OPT1]
full help
Enable
Enable DHCP server on the OPT1 interface
Deny unknown clients
Ignore Client UIDs
Subnet
192.168.10.0
Subnet mask
255.255.255.0
Available range
192.168.10.1 - 192.168.10.254
Range
from
to
192.168.10.1
192.168.10.254
Additional Pools
Pool Start
Pool End
Description
WINS servers
DNS servers
192.168.1.1
192.168.0.1
Gateway
192.168.10.1



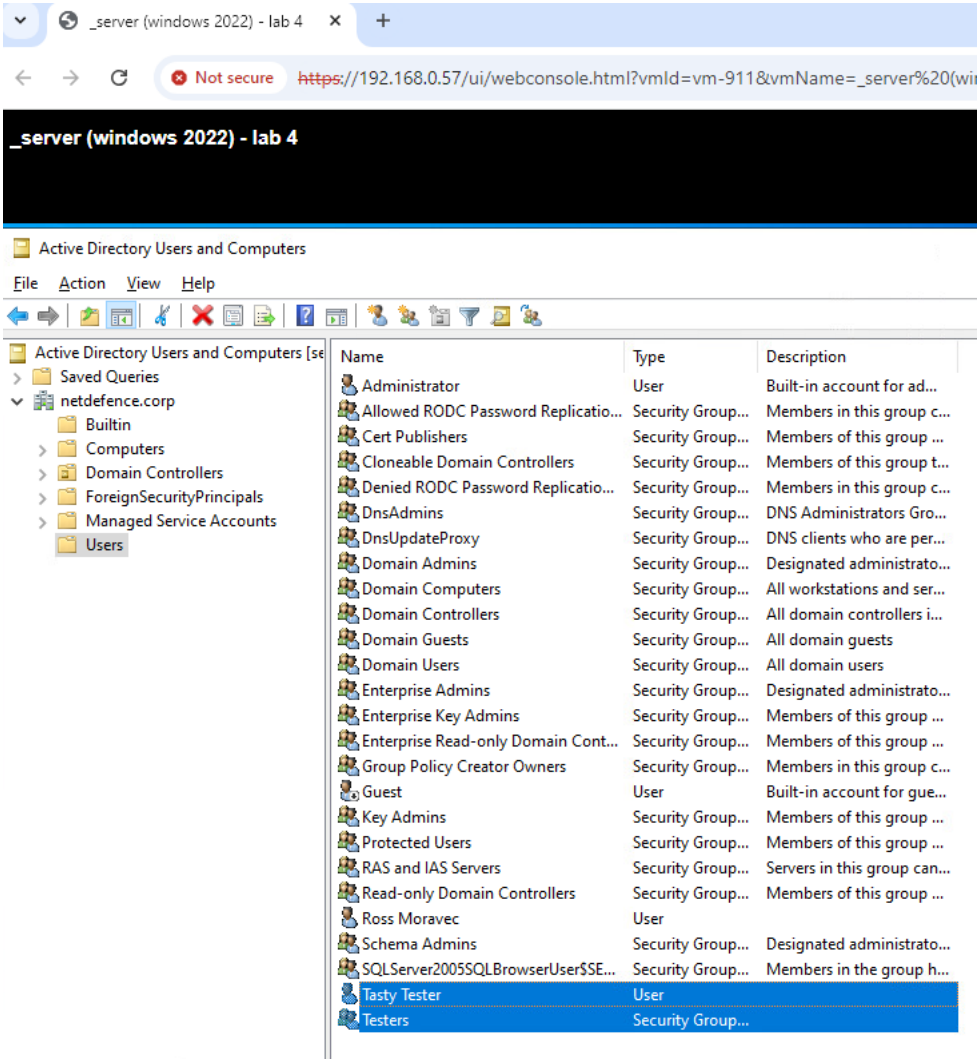
Part 4: Configure Role-Based Access Control (RBAC) on Windows Server 2022

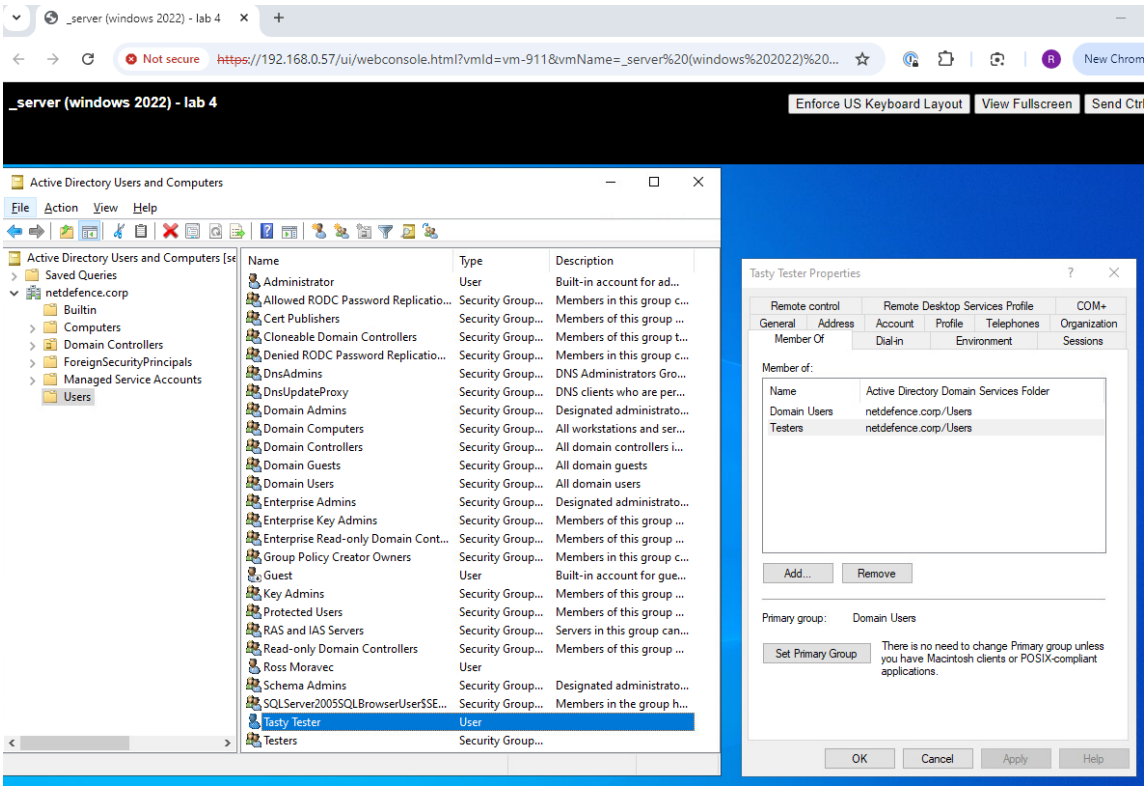
1. **Open Server Manager:**
   - Go to `Start` > `Server Manager`.
2. **Add Roles and Features:**
   - Navigate to `Manage` > `Add Roles and Features`.
   - Select `Role-based or feature-based installation`.
3. **Configure Active Directory:**
   - Install `Active Directory Domain Services`.
   - Promote the server to a domain controller.
4. **Create User Roles:**
   - Open `Active Directory Users and Computers`.

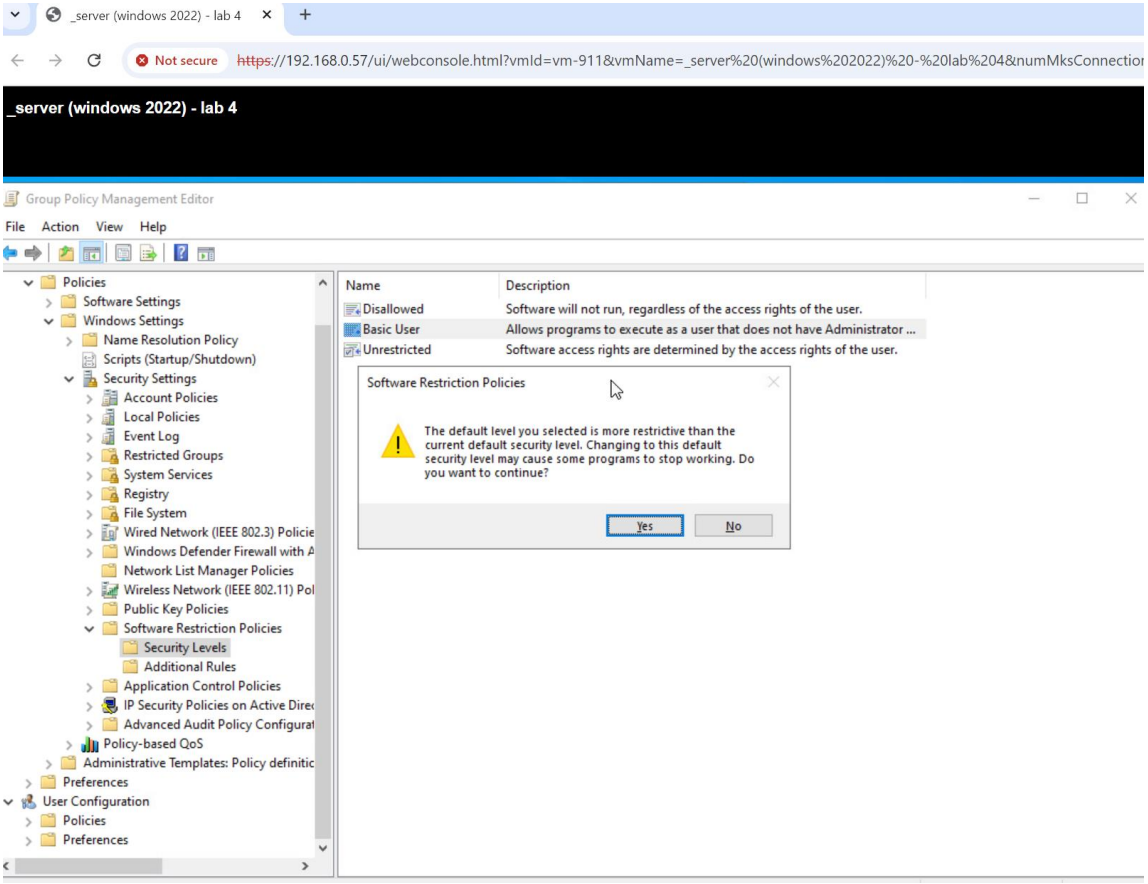
- Create new roles and assign permissions.

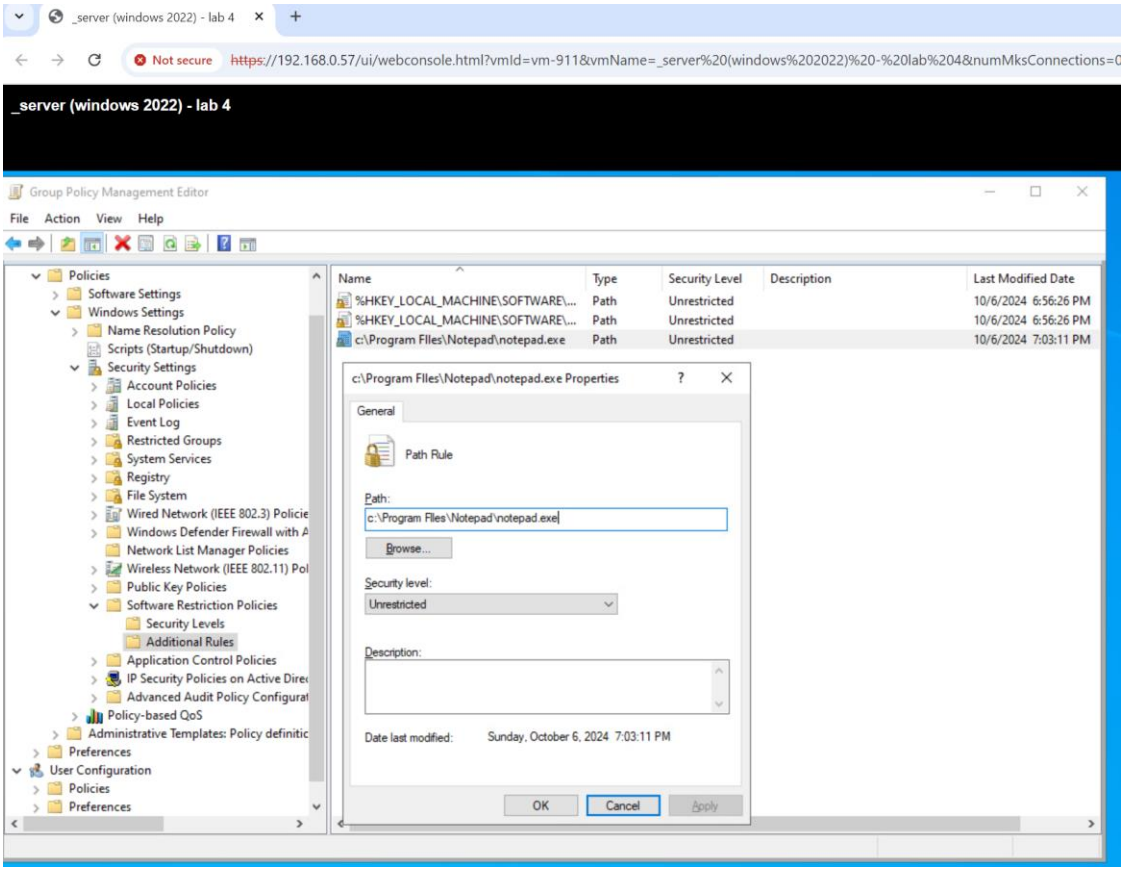
Deliverables:

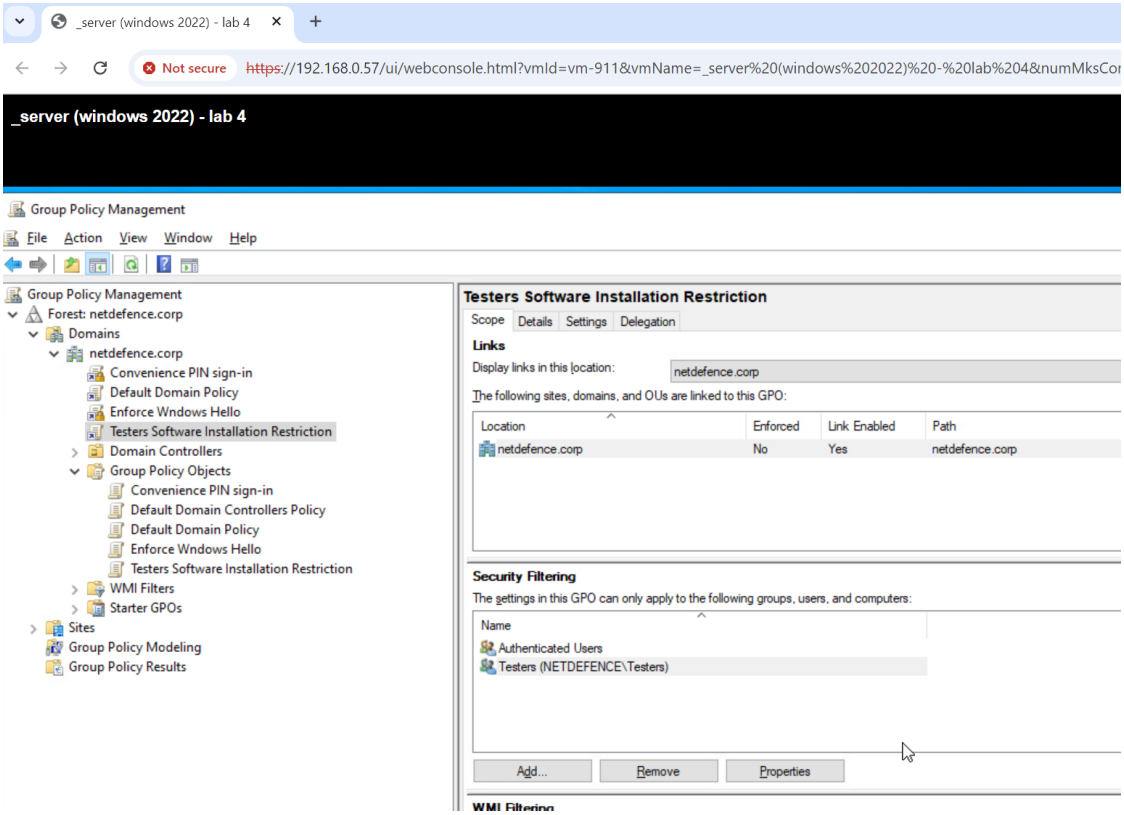
- Screenshot of the Active Directory setup page.
- Screenshot of user roles and permissions.




_server (windows 2022) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-911&vmName=_server%20(windows%202022)%20...
_server (windows 2022) - lab 4
Enforce US Keyboard Layout
View Fullscreen
Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [se
Saved Queries
netdefence.corp
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name Type Description
Administrator User Built-in account for ad...
Allowed RODC Password Replicatio... Security Group... Members in this group c...
Cert Publishers Security Group... Members of this group ...
Cloneable Domain Controllers Security Group... Members of this group t...
Denied RODC Password Replicatio... Security Group... Members in this group c...
DnsAdmins Security Group... DNS Administrators Gro...
DnsUpdateProxy Security Group... DNS clients who are per...
Domain Admins Security Group... Designated administrato...
Domain Computers Security Group... All workstations and ser...
Domain Controllers Security Group... All domain controllers i...
Domain Guests Security Group... All domain guests
Domain Users Security Group... All domain users
Enterprise Admins Security Group... Designated administrato...
Enterprise Key Admins Security Group... Members of this group ...
Enterprise Read-only Domain Cont... Security Group... Members of this group ...
Group Policy Creator Owners Security Group... Members in this group c...
Guest User Built-in account for gue...
Key Admins Security Group... Members of this group ...
Protected Users Security Group... Members of this group ...
RAS and IAS Servers Security Group... Servers in this group can...
Read-only Domain Controllers Security Group... Members of this group ...
Ross Moravec User
Schema Admins Security Group... Designated administrato...
SQLServer2005SQLBrowserUser$SE... Security Group... Members in the group h...
Tasty Tester User
Testers Security Group...
Tasty Tester Properties
Remote control
Remote Desktop Services Profile
COM+
General Address Account Profile Telephones Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Domain Users
netdefence.corp/Users
Testers
netdefence.corp/Users
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help


_server (windows 2022) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-911&vmName=_server%20(windows%202022)%20-%20lab%204&numMksConnectio
_server (windows 2022) - lab 4
Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policie
Windows Defender Firewall with A
Network List Manager Policies
Wireless Network (IEEE 802.11) Pol
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Application Control Policies
IP Security Policies on Active Direc
Advanced Audit Policy Configurat
Policy-based QoS
Administrative Templates: Policy definitic
Preferences
User Configuration
Policies
Preferences
Name Description
Disallowed Software will not run, regardless of the access rights of the user.
Basic User Allows programs to execute as a user that does not have Administrator ...
Unrestricted Software access rights are determined by the access rights of the user.
Software Restriction Policies
The default level you selected is more restrictive than the current default security level. Changing to this default security level may cause some programs to stop working. Do you want to continue?
Yes
No


_server (windows 2022) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-911&vmName=_server%20(windows%202022)%20-%20lab%204&numMksConnections=0
_server (windows 2022) - lab 4
Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policie
Windows Defender Firewall with A
Network List Manager Policies
Wireless Network (IEEE 802.11) Pol
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Application Control Policies
IP Security Policies on Active Direc
Advanced Audit Policy Configurat
Policy-based QoS
Administrative Templates: Policy definitic
Preferences
User Configuration
Policies
Preferences
Name
Type
Security Level
Description
Last Modified Date
%HKEY_LOCAL_MACHINE\SOFTWARE\...
Path
Unrestricted
10/6/2024 6:56:26 PM
%HKEY_LOCAL_MACHINE\SOFTWARE\...
Path
Unrestricted
10/6/2024 6:56:26 PM
c:\Program Files\Notepad\notepad.exe
Path
Unrestricted
10/6/2024 7:03:11 PM
c:\Program Files\Notepad\notepad.exe Properties
General
Path Rule
Path:
c:\Program Files\Notepad\notepad.exe
Browse...
Security level:
Unrestricted
Description:
Date last modified:
Sunday, October 6, 2024 7:03:11 PM
OK
Cancel
Apply

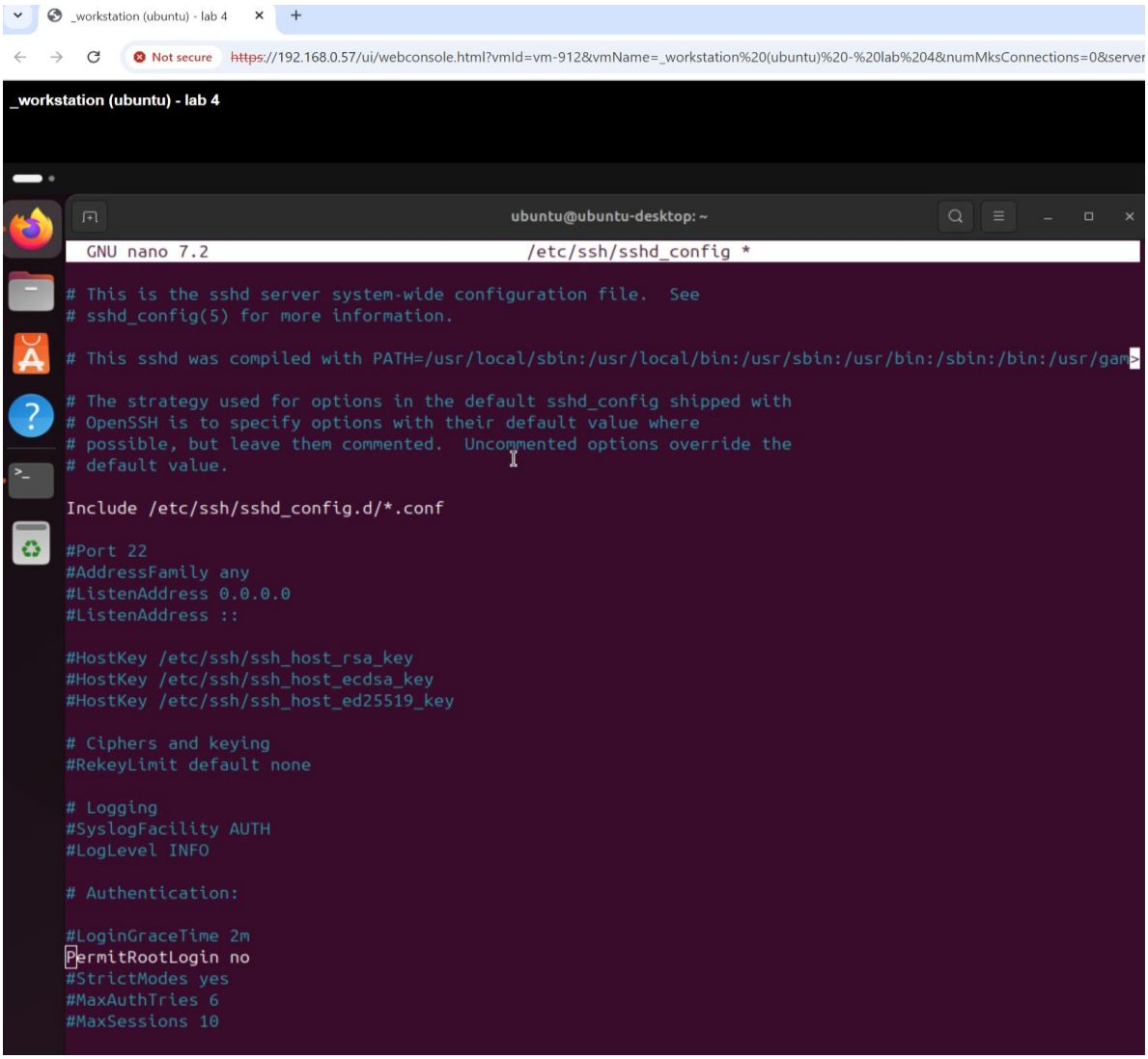

_server (windows 2022) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-911&vmName=_server%20(windows%202022)%20-%20lab%204&numMksCon
_server (windows 2022) - lab 4
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: netdefence.corp
Domains
netdefence.corp
Convenience PIN sign-in
Default Domain Policy
Enforce Wndows Hello
Testers Software Installation Restriction
Domain Controllers
Group Policy Objects
Convenience PIN sign-in
Default Domain Controllers Policy
Default Domain Policy
Enforce Wndows Hello
Testers Software Installation Restriction
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Testers Software Installation Restriction
Scope
Details
Settings
Delegation
Links
Display links in this location:
netdefence.corp
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
Path
netdefence.corp
No
Yes
netdefence.corp
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Testers (NETDEFENCE\Testers)
Add...
Remove
Properties
WMI Filtering

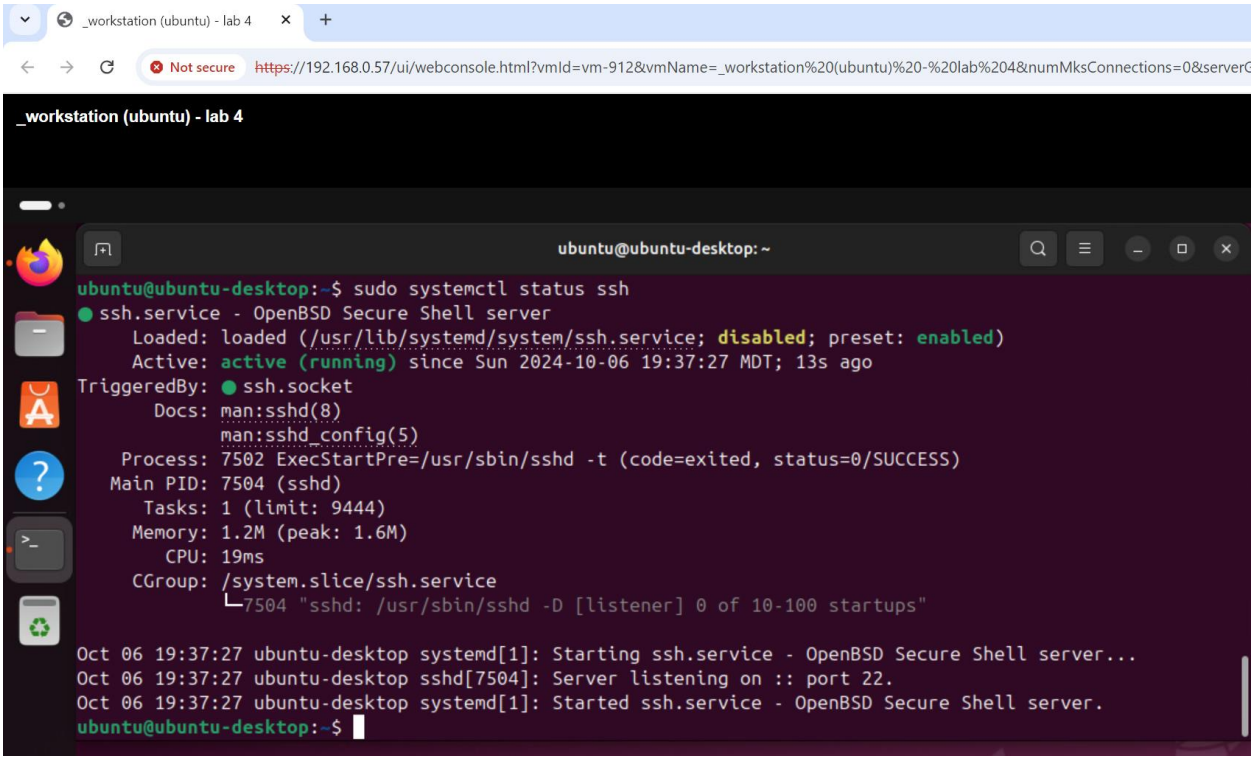
Part 5: Secure Remote Access using SSH on Ubuntu Desktop

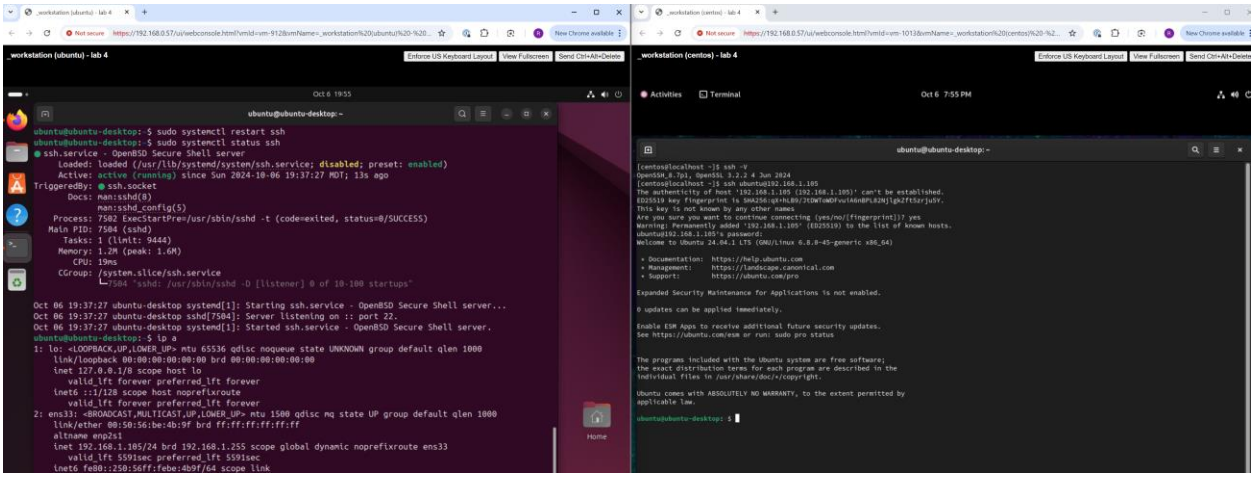
1. **Install SSH Server:**
    - Open Terminal and run `sudo apt update` and `sudo apt install openssh-server`.
2. **Configure SSH:**
    - Edit the SSH config file using `sudo nano /etc/ssh/sshd_config`.
    - Ensure `PermitRootLogin` is set to `no` and configure other security settings as needed.
3. **Restart SSH Service:**
    - Run `sudo systemctl restart ssh`.
4. **Test SSH Access:**
    - Attempt to connect from another machine using `ssh username@IP`.

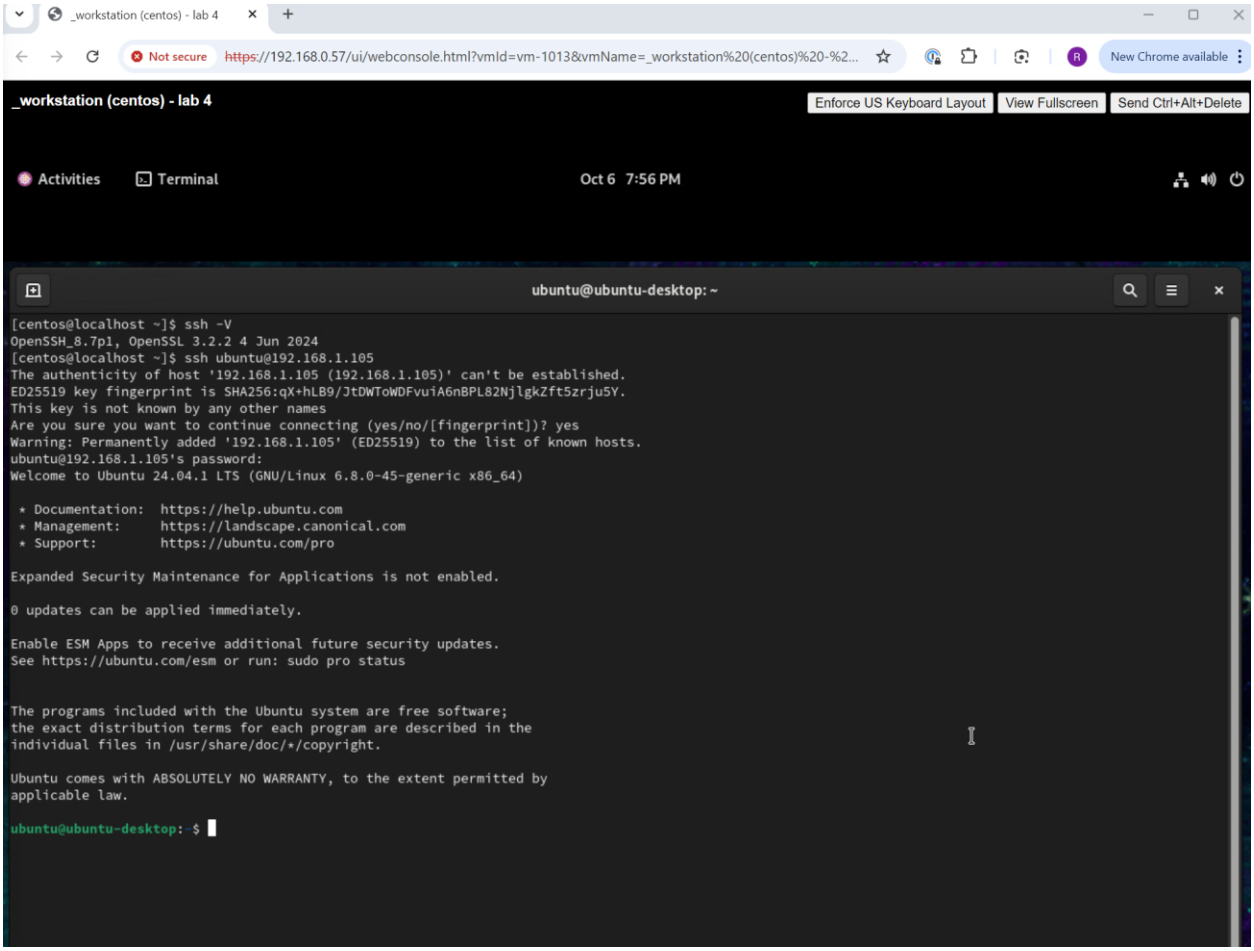
Deliverables:

- Screenshot of the terminal showing SSH configuration.
- Screenshot of successful SSH login from another machine.


_workstation (ubuntu) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-912&vmName=_workstation%20(ubuntu)%20-%20lab%204&numMksConnections=0&server
_workstation (ubuntu) - lab 4
ubuntu@ubuntu-desktop: ~
GNU nano 7.2 /etc/ssh/sshd_config *
This is the sshd server system-wide configuration file. See
sshd_config(5) for more information.
This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/gam
The strategy used for options in the default sshd_config shipped with
OpenSSH is to specify options with their default value where
possible, but leave them commented. Uncommented options override the
default value.
Include /etc/ssh/sshd_config.d/*.conf
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
Ciphers and keying
#RekeyLimit default none
Logging
#SyslogFacility AUTH
#LogLevel INFO
Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10


_workstation (ubuntu) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-912&vmName=_workstation%20(ubuntu)%20-%20lab%204&numMksConnections=0&serverG
_workstation (ubuntu) - lab 4
ubuntu@ubuntu-desktop: ~
ubuntu@ubuntu-desktop:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
Active: active (running) since Sun 2024-10-06 19:37:27 MDT; 13s ago
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
Process: 7502 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 7504 (sshd)
Tasks: 1 (limit: 9444)
Memory: 1.2M (peak: 1.6M)
CPU: 19ms
CGroup: /system.slice/ssh.service
└─7504 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Oct 06 19:37:27 ubuntu-desktop systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 06 19:37:27 ubuntu-desktop sshd[7504]: Server listening on :: port 22.
Oct 06 19:37:27 ubuntu-desktop systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
ubuntu@ubuntu-desktop:~$


_workstation (ubuntu) - lab 4
_workstation (centos) - lab 4
ubuntu@ubuntu-desktop: ~
ubuntu@ubuntu-desktop:~$ sudo systemctl restart ssh
ubuntu@ubuntu-desktop:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
Active: active (running) since Sun 2024-10-06 19:37:27 MDT; 13s ago
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
Process: 7502 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 7504 (sshd)
Tasks: 1 (limit: 9444)
Memory: 1.2M (peak: 1.6M)
CPU: 19ms
CGroup: /system.slice/ssh.service
└─7504 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Oct 06 19:37:27 ubuntu-desktop systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 06 19:37:27 ubuntu-desktop sshd[7504]: Server listening on :: port 22.
Oct 06 19:37:27 ubuntu-desktop systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
ubuntu@ubuntu-desktop:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 00:50:56:be:4b:9f brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 192.168.1.105/24 brd 192.168.1.255 scope global dynamic noprefixroute ens33
valid_lft 5591sec preferred_lft 5591sec
inet6 fe80::250:56ff:febe:4b9f/64 scope link
Home
_workstation (centos) - lab 4
Activities
Terminal
Oct 6 7:55 PM
ubuntu@ubuntu-desktop: ~
[centos@localhost ~]$ ssh -V
OpenSSH_8.7p1, OpenSSL 3.2.2 4 Jun 2024
[centos@localhost ~]$ ssh ubuntu@192.168.1.105
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.
ED25519 key fingerprint is SHA256:qX+NL89/2tDWTmNDFvwlA6nBPL02Njgk2ft5zrju5Y.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.105' (ED25519) to the list of known hosts.
ubuntu@192.168.1.105's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
ubuntu@ubuntu-desktop: $

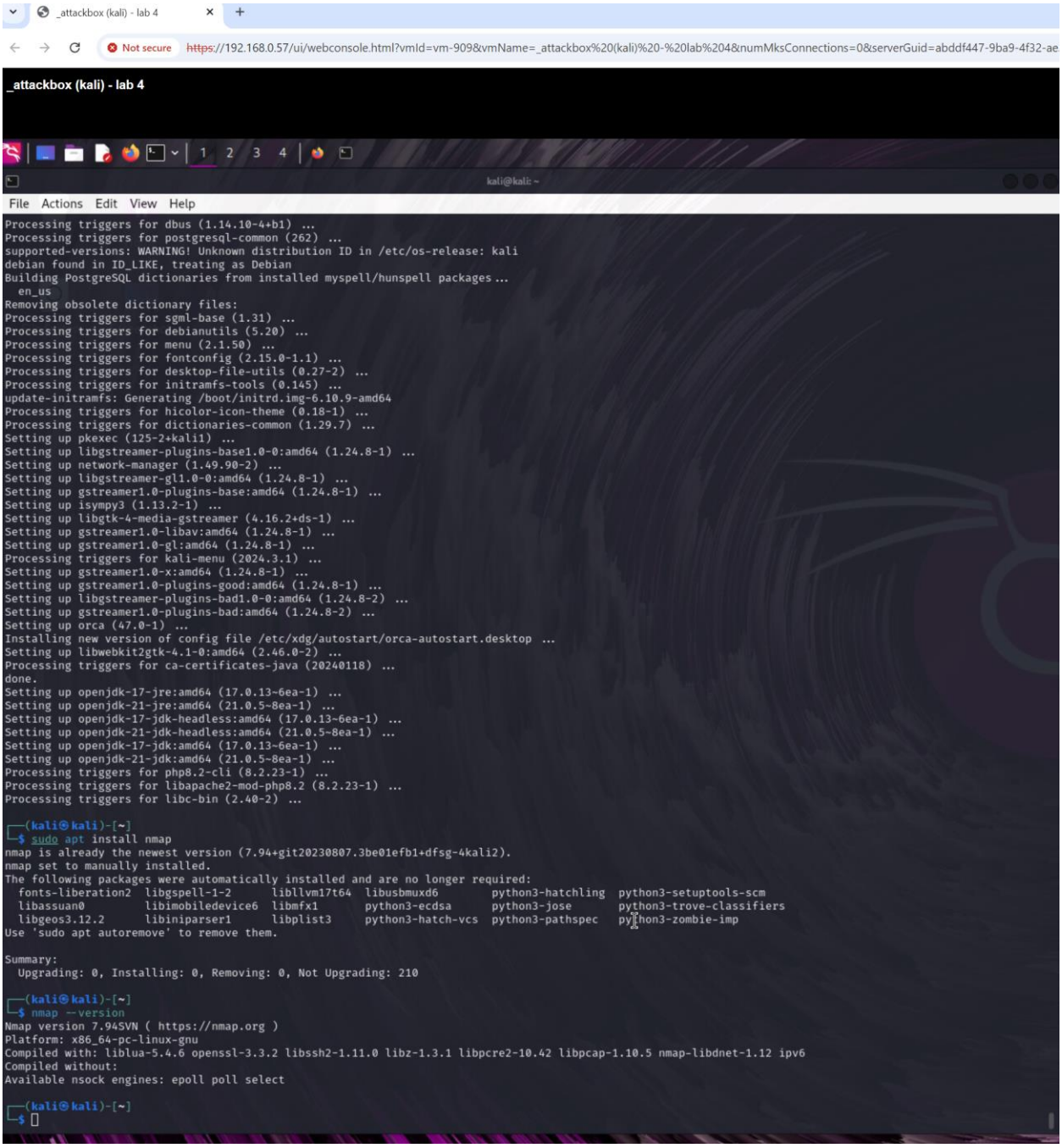


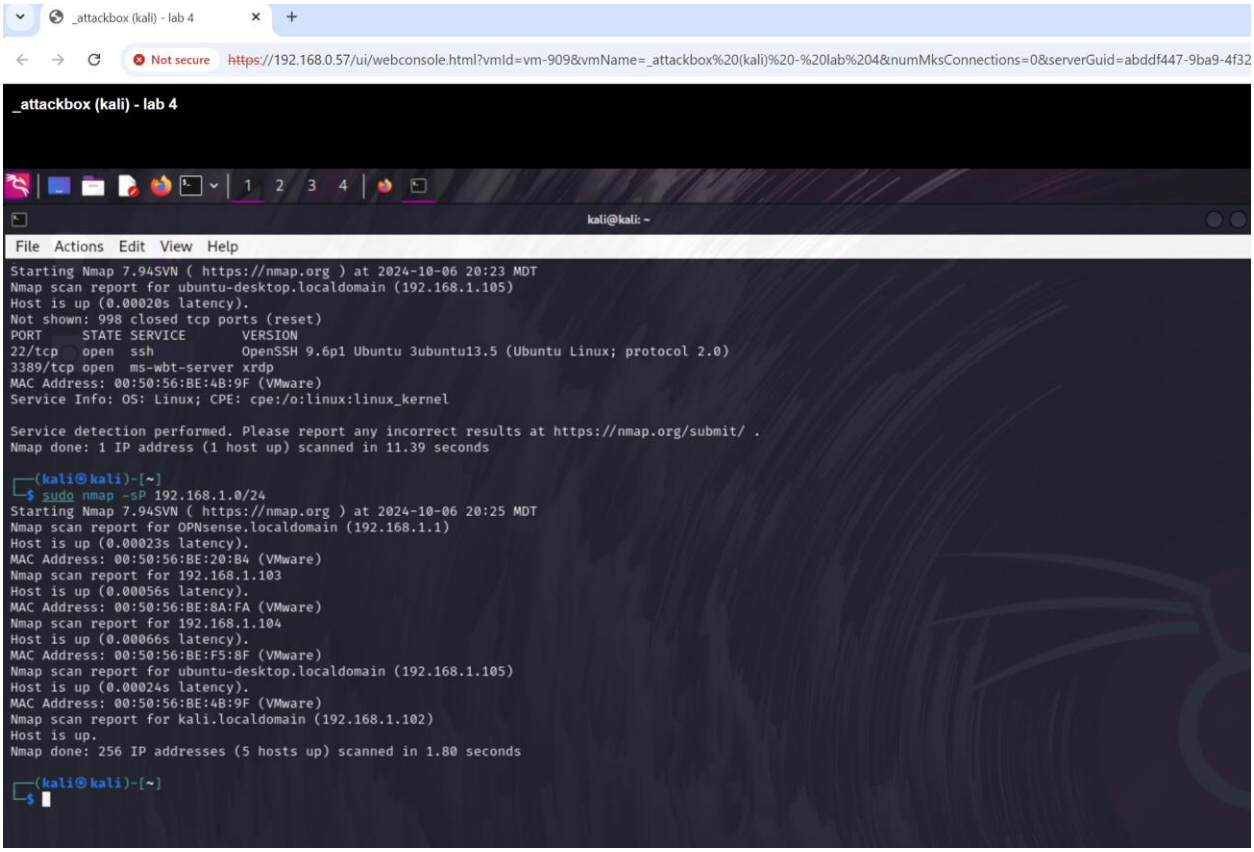
Part 6: Perform a Security Scan using Kali Linux

1. **Update Kali Linux:**
   - Open Terminal and run `sudo apt update && sudo apt upgrade`.
2. **Install Nmap:**
   - Run `sudo apt install nmap`.
3. **Perform a Network Scan:**
   - Use `nmap -sV <target-ip>` to scan the network for open ports and services.
4. **Analyze Results:**
   - Review the scan results for potential vulnerabilities.

Deliverables:

- Screenshot of the terminal showing Nmap installation.
- Screenshot of the Nmap scan results.


_attackbox (kali) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-909&vmName=_attackbox%20(kali)%20-%20lab%204&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae
_attackbox (kali) - lab 4
1 2 3 4
kali@kali: ~
File Actions Edit View Help
Processing triggers for dbus (1.14.10-4+b1) ...
Processing triggers for postgresql-common (262) ...
supported-versions: WARNING! Unknown distribution ID in /etc/os-release: kali
debian found in ID_LIKE, treating as Debian
Building PostgreSQL dictionaries from installed myspell/hunspell packages...
en_us
Removing obsolete dictionary files:
Processing triggers for sgml-base (1.31) ...
Processing triggers for debianutils (5.20) ...
Processing triggers for menu (2.1.50) ...
Processing triggers for fontconfig (2.15.0-1.1) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for initramfs-tools (0.145) ...
update-initramfs: Generating /boot/initrd.img-6.10.9-amd64
Processing triggers for hicolor-icon-theme (0.18-1) ...
Processing triggers for dictionaries-common (1.29.7) ...
Setting up pkexec (125-2+kali1) ...
Setting up libgstreamer-plugins-base1.0-0:amd64 (1.24.8-1) ...
Setting up network-manager (1.49.90-2) ...
Setting up libgstreamer-gl1.0-0:amd64 (1.24.8-1) ...
Setting up gstreamer1.0-plugins-base:amd64 (1.24.8-1) ...
Setting up isympy3 (1.13.2-1) ...
Setting up libgtk-4-media-gstreamer (4.16.2+ds-1) ...
Setting up gstreamer1.0-libav:amd64 (1.24.8-1) ...
Setting up gstreamer1.0-gl:amd64 (1.24.8-1) ...
Processing triggers for kali-menu (2024.3.1) ...
Setting up gstreamer1.0-x:amd64 (1.24.8-1) ...
Setting up gstreamer1.0-plugins-good:amd64 (1.24.8-1) ...
Setting up libgstreamer-plugins-bad1.0-0:amd64 (1.24.8-2) ...
Setting up gstreamer1.0-plugins-bad:amd64 (1.24.8-2) ...
Setting up orca (47.0-1) ...
Installing new version of config file /etc/xdg/autostart/orca-autostart.desktop ...
Setting up libwebkit2gtk-4.1-0:amd64 (2.46.0-2) ...
Processing triggers for ca-certificates-java (20240118) ...
done.
Setting up openjdk-17-jre:amd64 (17.0.13~6ea-1) ...
Setting up openjdk-21-jre:amd64 (21.0.5~8ea-1) ...
Setting up openjdk-17-jdk-headless:amd64 (17.0.13~6ea-1) ...
Setting up openjdk-21-jdk-headless:amd64 (21.0.5~8ea-1) ...
Setting up openjdk-17-jdk:amd64 (17.0.13~6ea-1) ...
Setting up openjdk-21-jdk:amd64 (21.0.5~8ea-1) ...
Processing triggers for php8.2-cli (8.2.23-1) ...
Processing triggers for libapache2-mod-php8.2 (8.2.23-1) ...
Processing triggers for libc-bin (2.40-2) ...
┌──(kali㉿kali)-[~]
└─$ sudo apt install nmap
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-4kali2).
nmap set to manually installed.
The following packages were automatically installed and are no longer required:
fonts-liberation2 libgspell-1-2 libllvm17t64 libusbmuxd6 python3-hatchling python3-setuptools-scm
libassuan0 libimobiledevice6 libmfx1 python3-ecdsa python3-jose python3-trove-classifiers
libgeos3.12.2 libiniparser1 libplist3 python3-hatch-vcs python3-pathspec python3-zombie-imp
Use 'sudo apt autoremove' to remove them.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 210
┌──(kali㉿kali)-[~]
└─$ nmap --version
Nmap version 7.94SVN (https://nmap.org)
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.3.2 libssh2-1.11.0 libz-1.3.1 libpcre2-10.42 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
┌──(kali㉿kali)-[~]
└─$


_attackbox (kali) - lab 4
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-909&vmName=_attackbox%20(kali)%20-%20lab%204&numMksConnections=0&serverGuid=abddf447-9ba9-4f32
_attackbox (kali) - lab 4
1 2 3 4
kali@kali: ~
File Actions Edit View Help
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-06 20:23 MDT
Nmap scan report for ubuntu-desktop.localdomain (192.168.1.105)
Host is up (0.00020s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
3389/tcp open ms-wbt-server xrdp
MAC Address: 00:50:56:BE:4B:9F (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.1.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-06 20:25 MDT
Nmap scan report for OPNsense.localdomain (192.168.1.1)
Host is up (0.00023s latency).
MAC Address: 00:50:56:BE:20:B4 (VMware)
Nmap scan report for 192.168.1.103
Host is up (0.00056s latency).
MAC Address: 00:50:56:BE:8A:FA (VMware)
Nmap scan report for 192.168.1.104
Host is up (0.00066s latency).
MAC Address: 00:50:56:BE:F5:8F (VMware)
Nmap scan report for ubuntu-desktop.localdomain (192.168.1.105)
Host is up (0.00024s latency).
MAC Address: 00:50:56:BE:4B:9F (VMware)
Nmap scan report for kali.localdomain (192.168.1.102)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.80 seconds
┌──(kali㉿kali)-[~]
└─$