Practical Network Defense Labs

ABOUT

This document showcases my practical hands-on engagements in the eLearnSecurity HERA labs environment for the Network Defense Professional certification course. I utilized VMWare & Kali Linux. Total lab time consists of ~60hrs.

LAB TOPICS

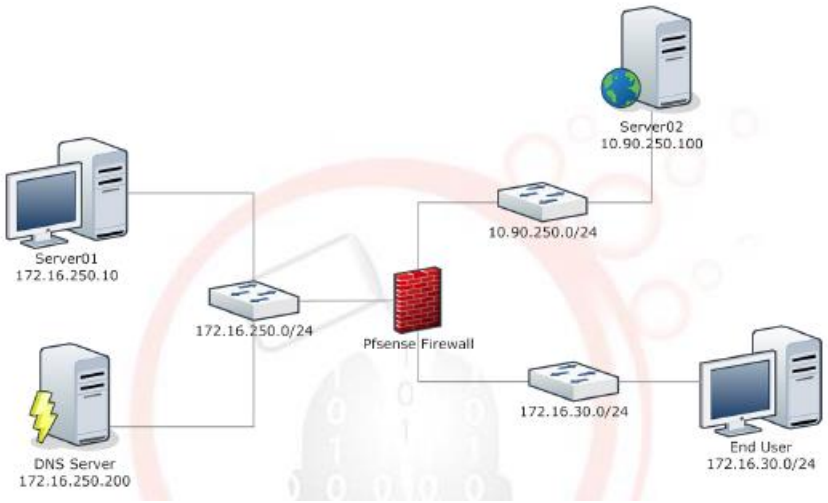
Configuring: ACL's, AD(DS), AD(CS), GPO's, WSUS, EMET, OpenVPN
Hardening Endpoints, Scanning & Remediating Vulnerabilities.

Contents

Lab 1 Access Control Lists

LAB DESCRIPTION

In the following lab, we will configure an access control list on a virtual firewall. You will be directly connected to the network 172.16.250.0/24.



Labs machines are not connected to the Internet, they are in a private testing environment just for you.

- Server01 is located at 172.16.250.10.
- Server02 is located at 10.90.250.100.
- Server02 is hosting several services.
- Internal DNS server is located at 172.16.250.200.
- The Developer machine is located at 172.16.30.245
- The pfSense firewall is located at 172.16.250.254.
- The internal end users are in subnet 172.16.30.0/24.

The 172.16.250.0/24 segment is on the pfsense LAN interface and the 172.16.30.0/24 segment is on the OPT1 interface.

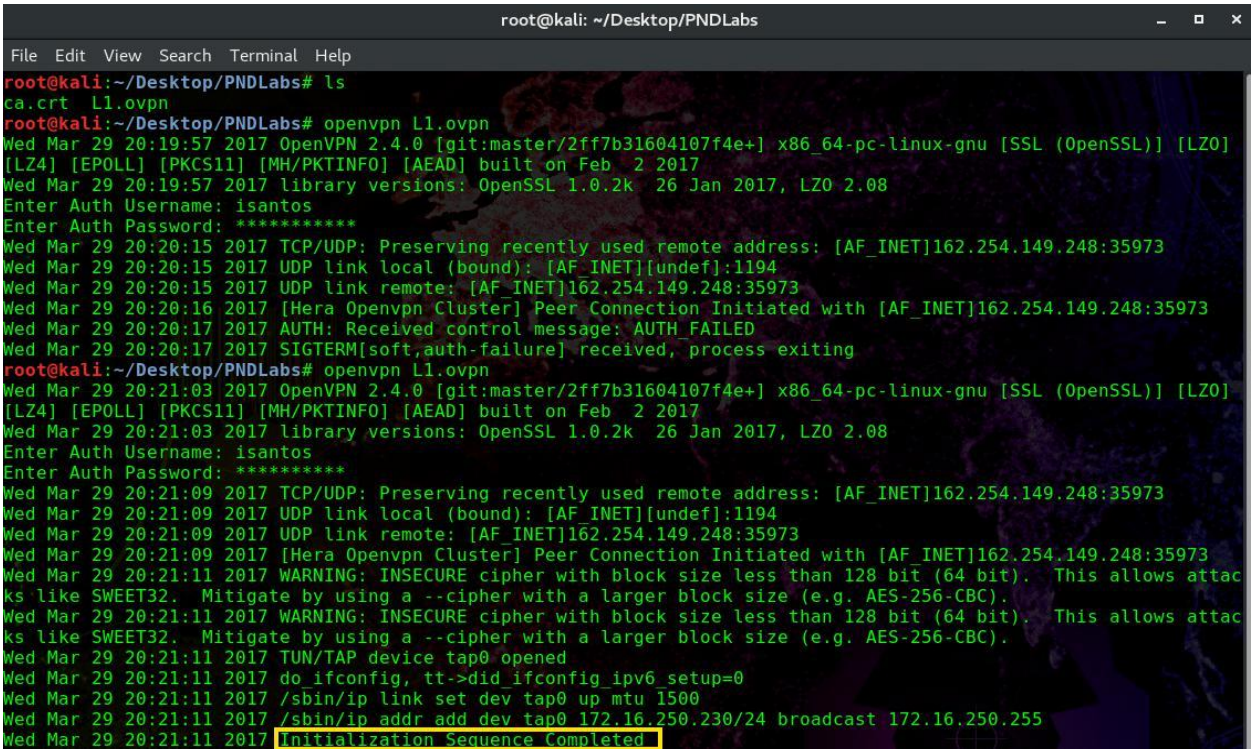
GOALS

- Become familiar with pfSense
- Learn to configure an ACL with least privilege

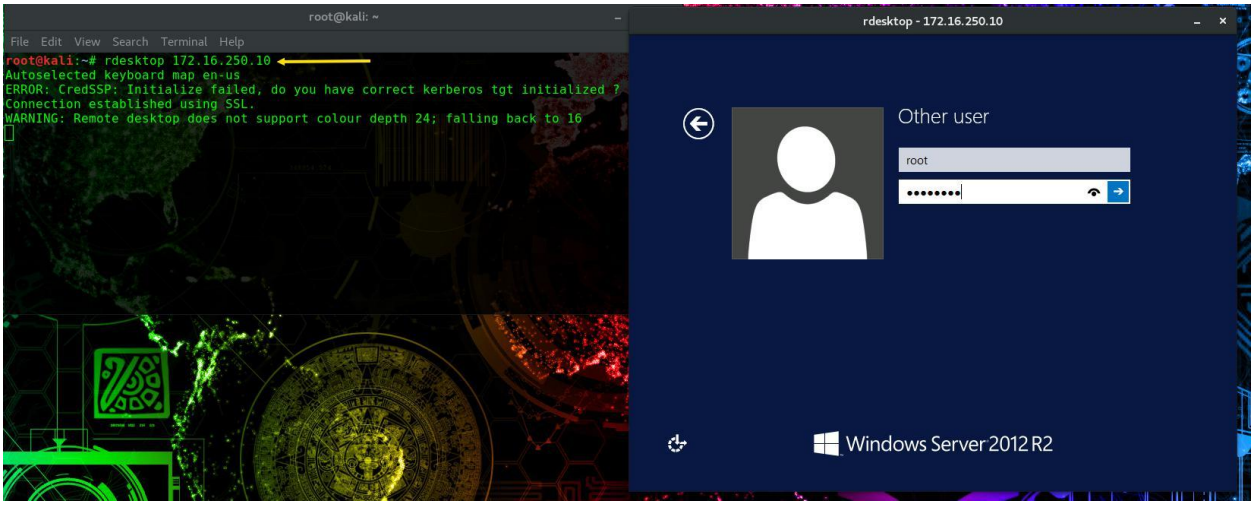
Task 1: Identify What Traffic the Firewall Passes

a) **Port Scan**: Run a port scan with Nmap against Server02 from Server01 to determine what traffic is being allowed through the firewall to the target server.

✓ First I established connection to the lab environment:

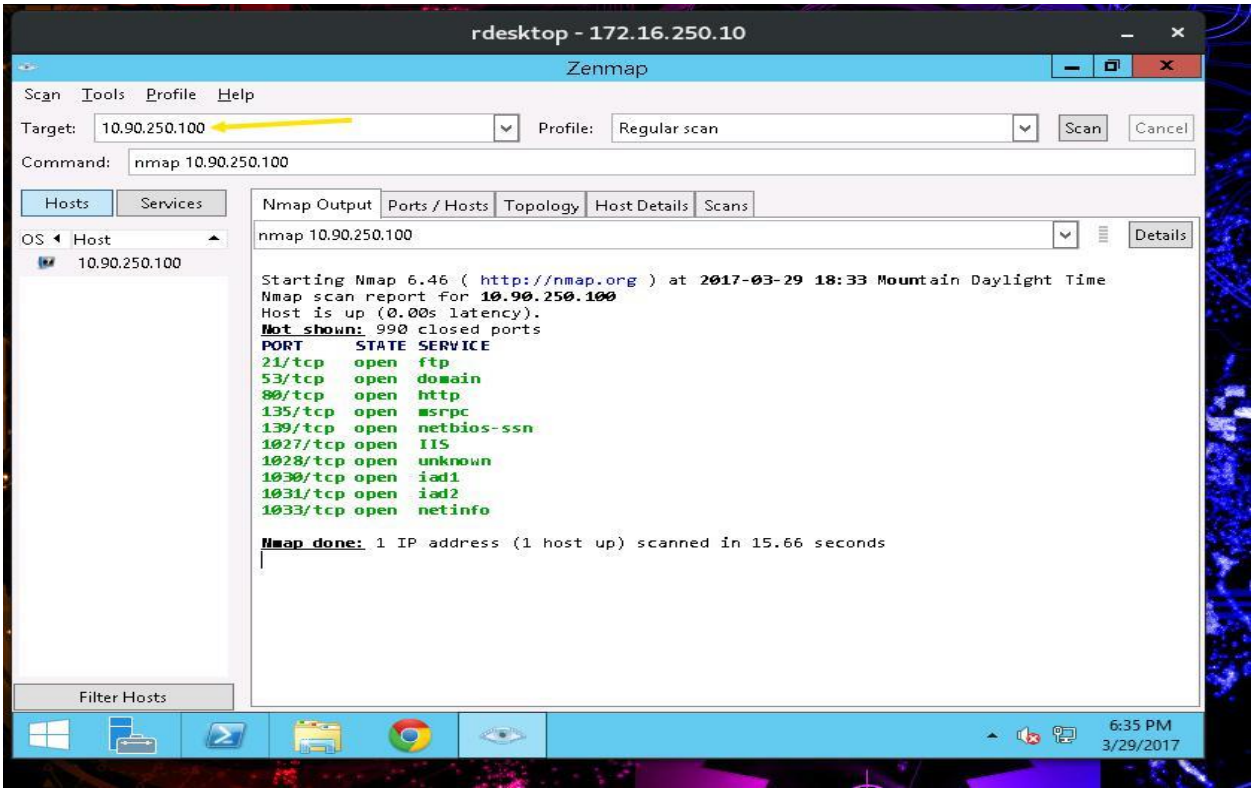


✓ I RDP'd into Server1 to run the server2 port scan:



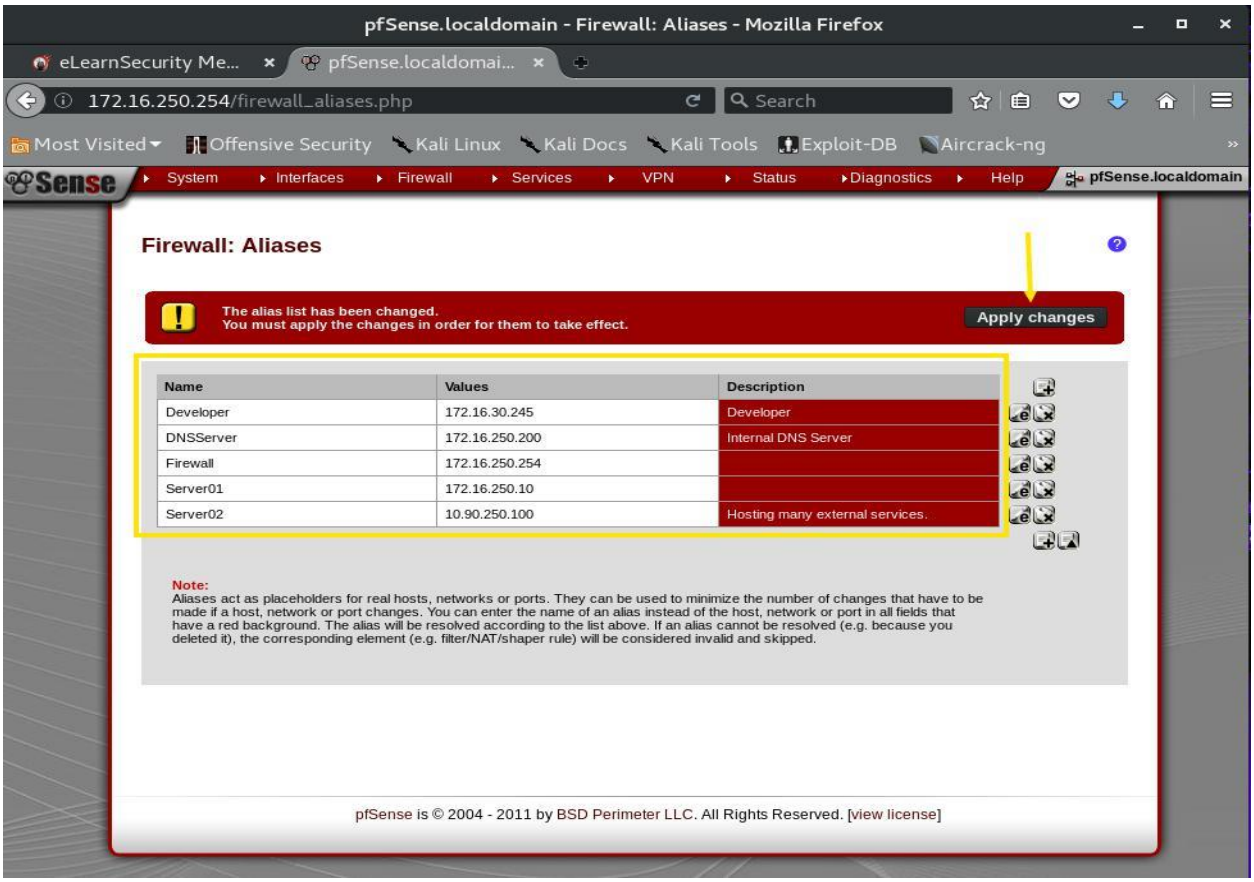
b) **Review Ports**: Identify which ports are being allowed outbound which are not needed. For this lab, assume end users will only need access to FTP and web browsing. The internal DNS server will need to be able to issue DNS requests outbound.

✓ I used Zenmap (nmap GUI) to conduct the port scan:



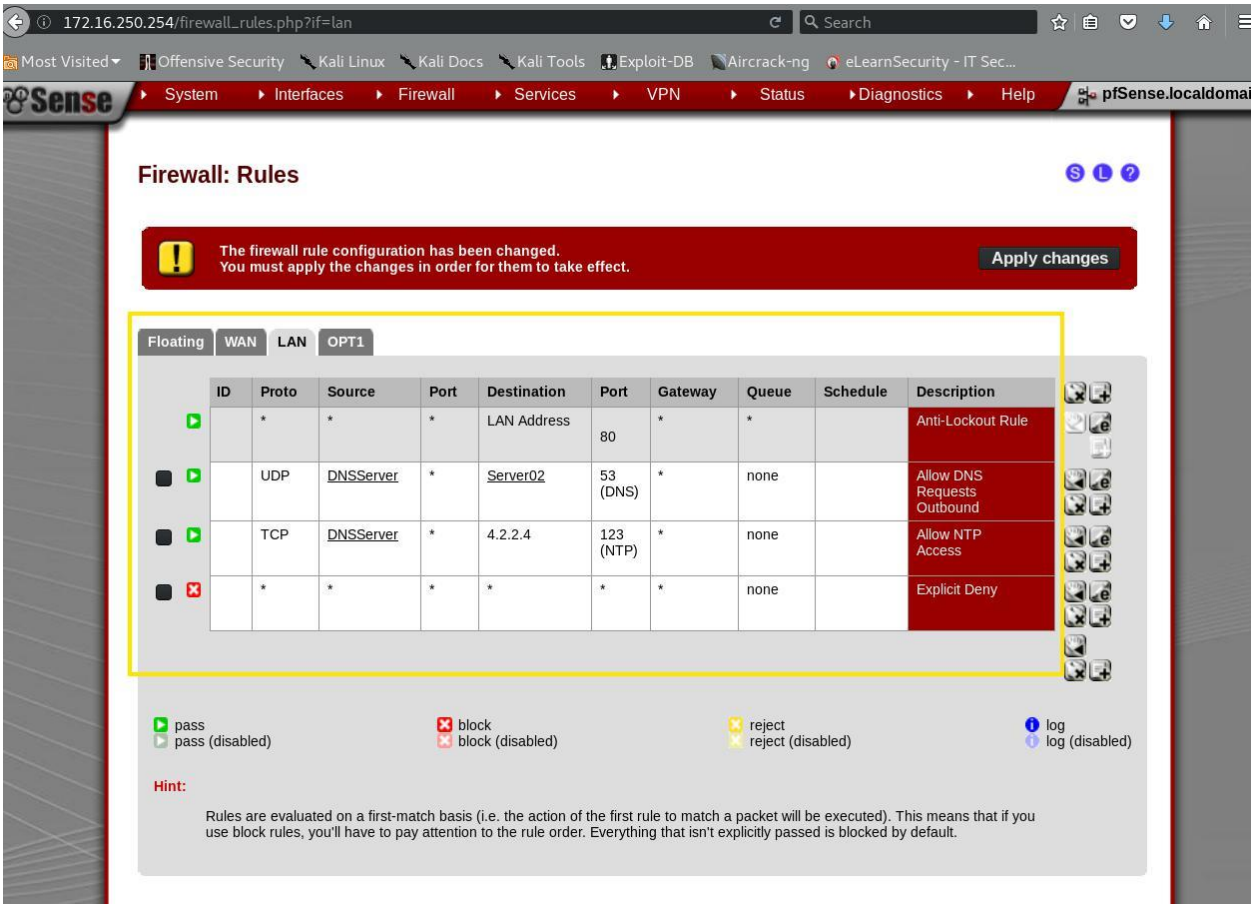
Task 2: Firewall Configuration

✓ I created an alias for each network/host in the network diagram (apply changes = commit):

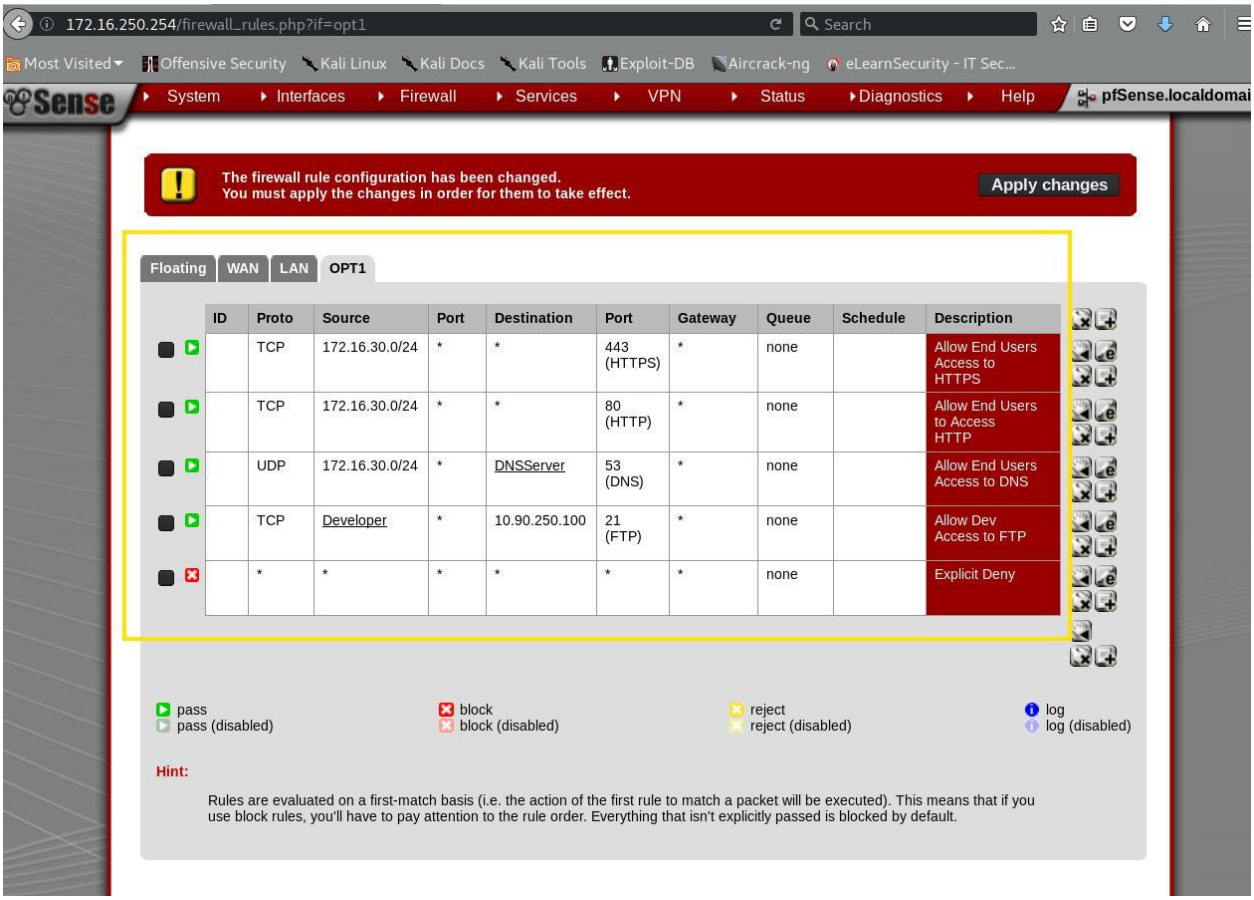


a) **ACL**: Configure the firewall rules to these specifications:
   i. The only device allowed to make outbound DNS requests is the internal DNS server.
   ii. The internal DNS server is only allowed to make DNS requests to 10.90.250.100.
   iii. The internal DNS server must also be able to use NTP to sync to 4.2.2.4.
   iv. The end users are only allowed to browse the internet and query the DNS Server (172.16.250.200).
   v. Management has declared an exception for the internal web developer at IP 172.16.30.245 to be able to use FTP to manage the company website.
   vi. The company website is located at 10.90.250.100.
   vii. End users and servers must not be allowed to use FTP.
   viii. All of the ports above 1024 outbound must be blocked.
   ix. Ensure any traffic not matched is logged when it is denied.

✓ My ACL setup for the LAN interface:

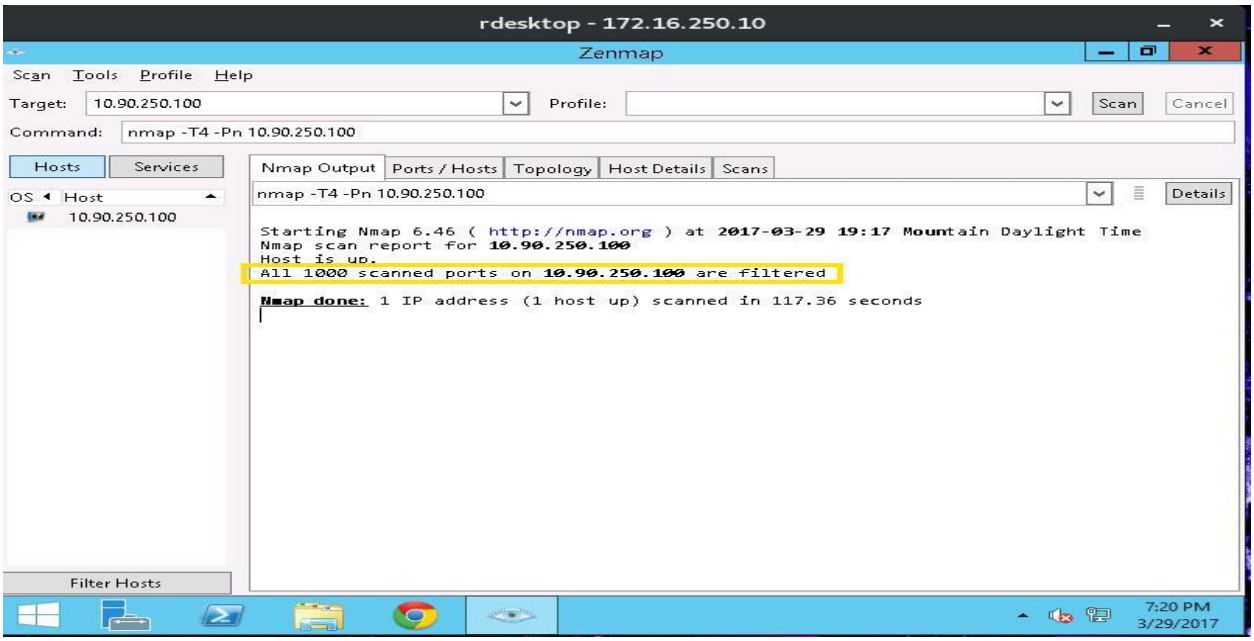


✓ My ACL setup for the OPT1 Interface:

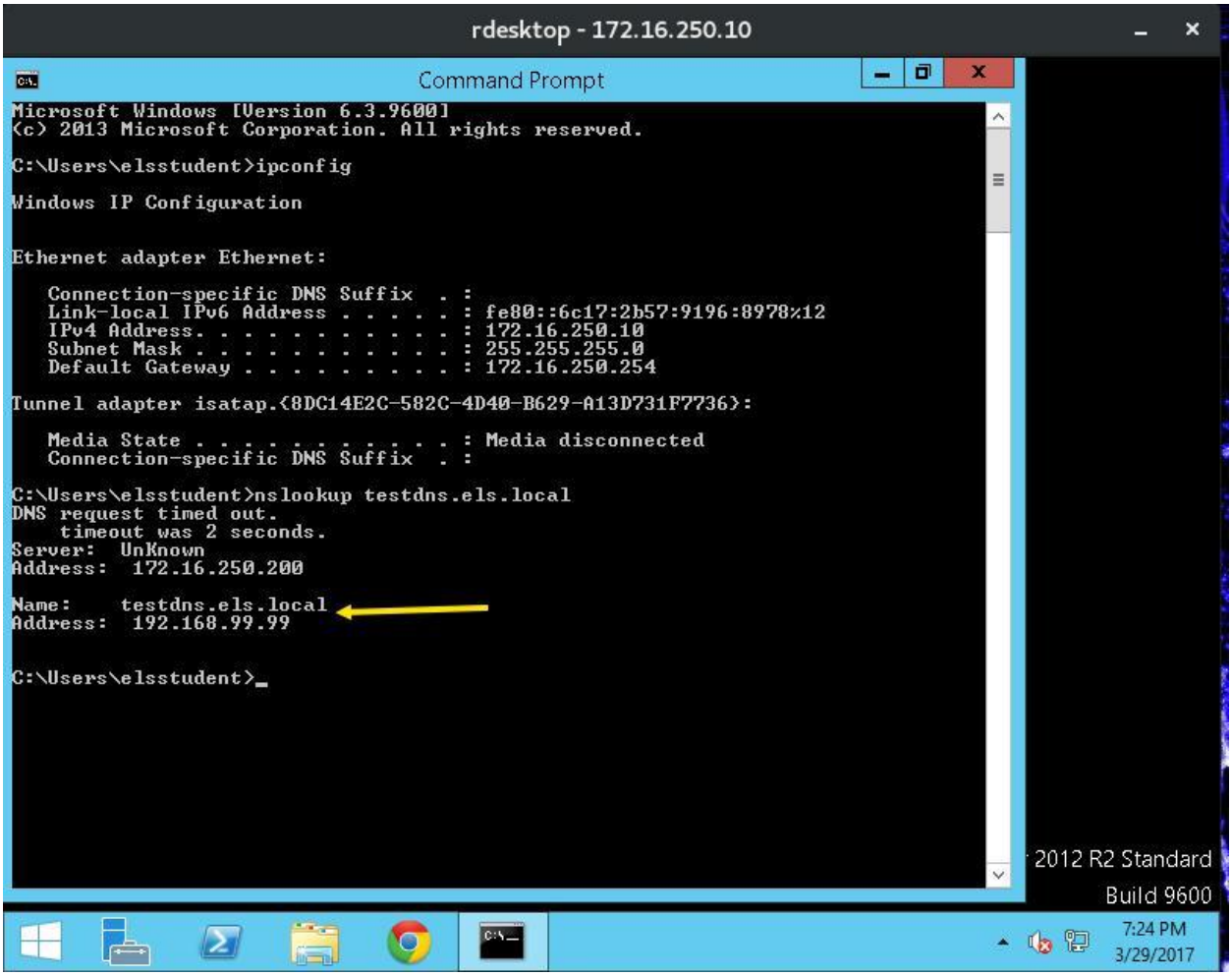


b) **Test DNS outbound**: Run a port scan again to confirm the available open ports from Server01. Resolve the host name "*testdns.els.local*" to confirm DNS is still allowed outbound as needed.

✓ The results of the port scan from server1 after the ACL changes, ports are now filtered:



✓ Testing the FQDN for testdns.els.local using nslookup:



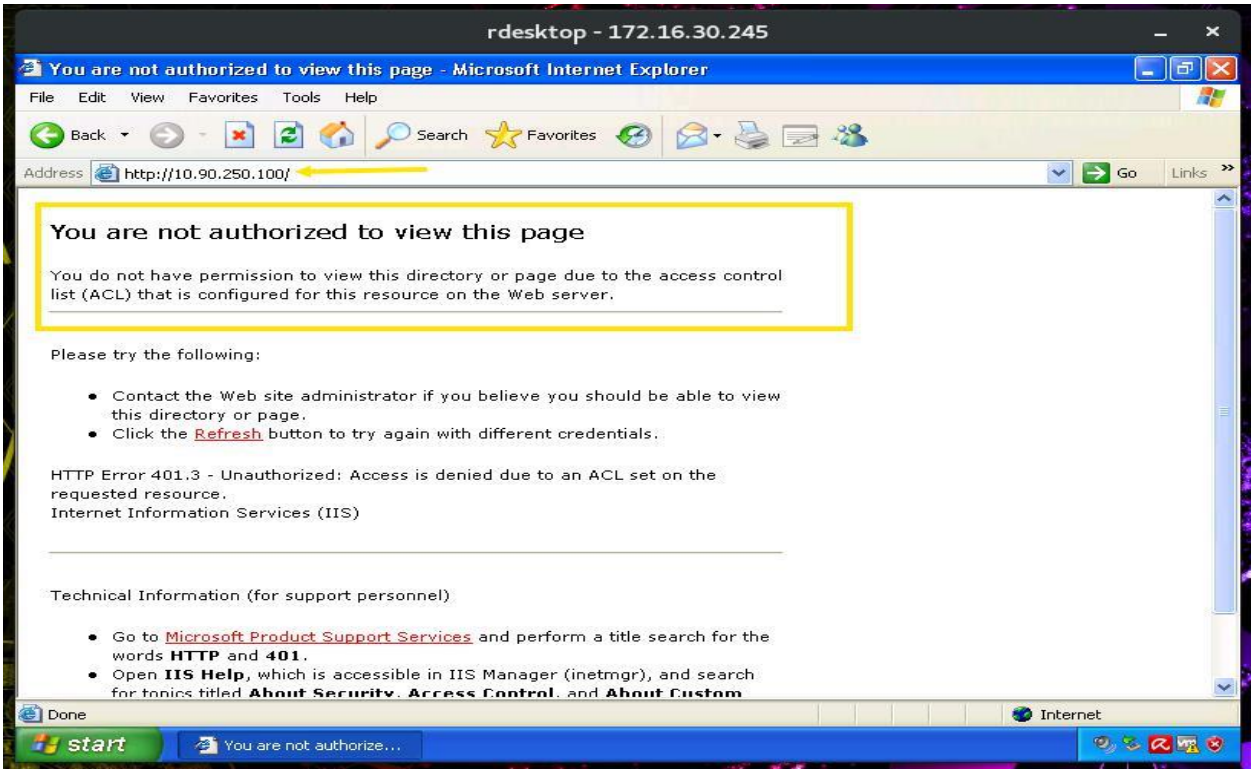
c) **Test EndUser Network**: Test the rules from the Developer machine (172.16.30.245). You can use RDP with the following credentials:

- Note: you need to change the firewall rules in order to allow RPD connections from your testing machine (172.16.250.XXX)

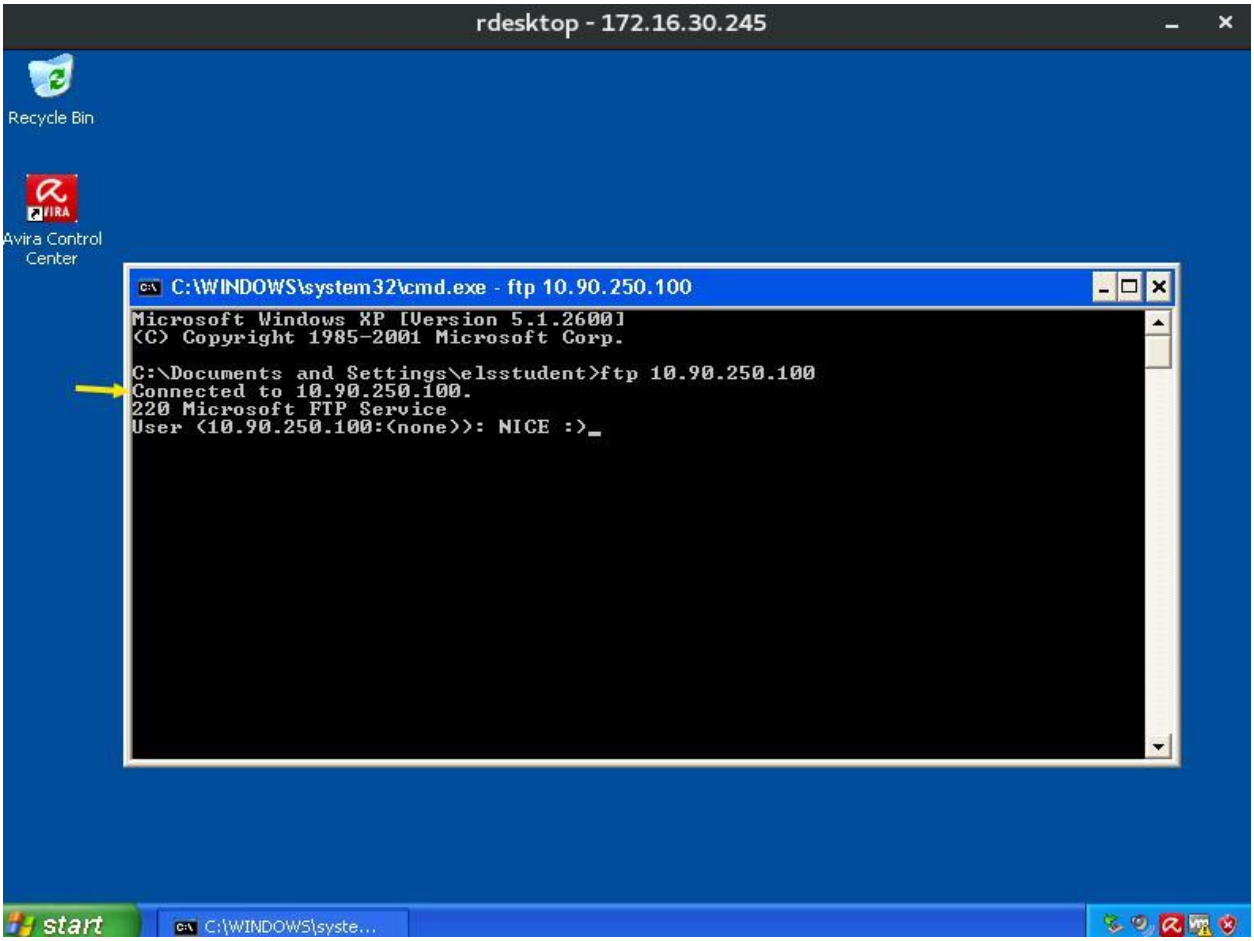
✓ I needed to change the ACL to enable RDP with the Developer host:

	TCP/UDP	172.16.250.230	*	Developer	3389 (MS RDP)	*	none		Allow Remote Access to Developer Machine

✓ Developer machine connected to web server, but denied access:



✓ Tested working connection to the FTP server:

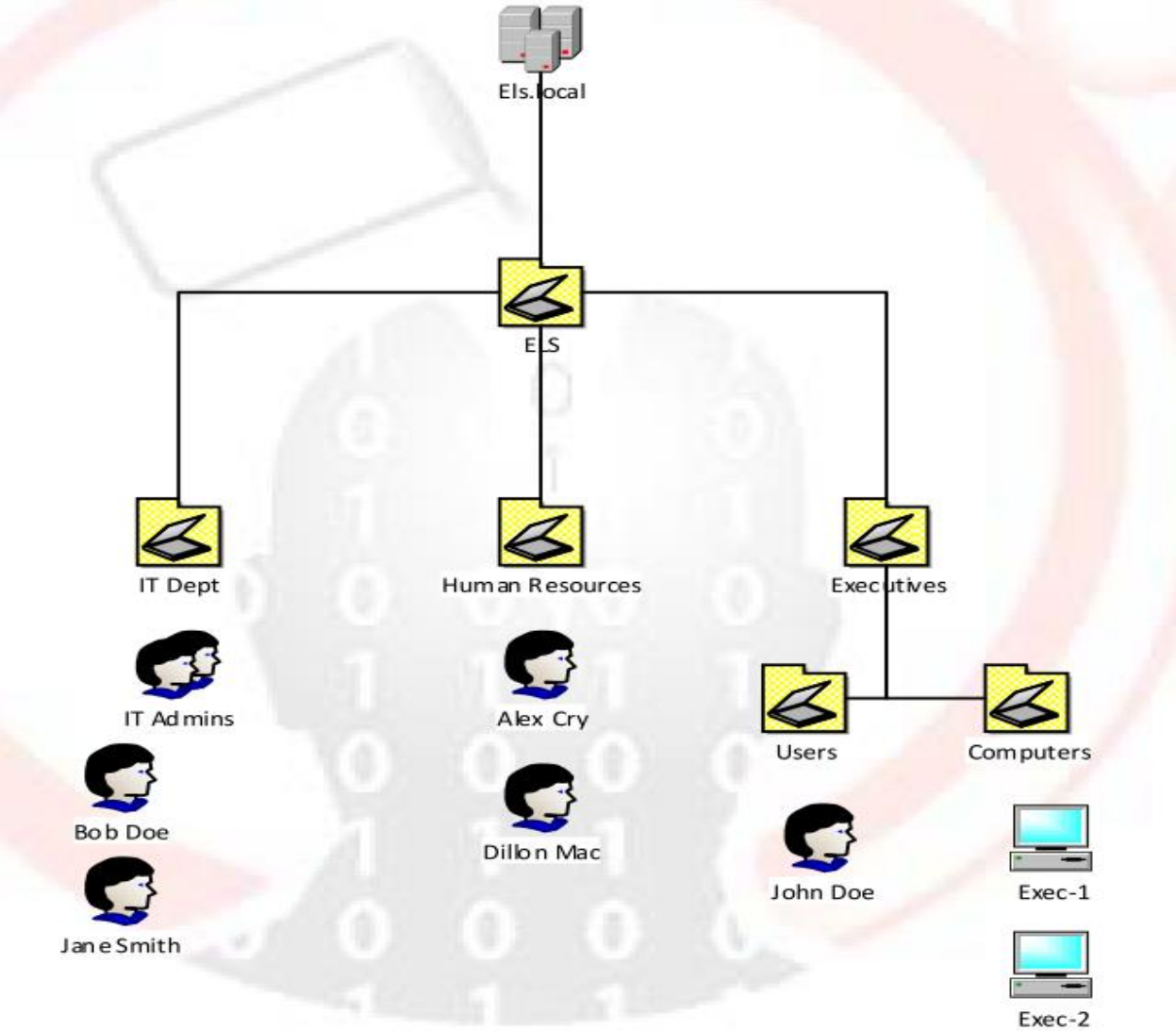


LAB 2 Active Directory

LAB DESCRIPTION

In the following lab, you can practice the management and securing techniques explained in the Practical Network Defense course – Active Directory.

You will be creating this Active Directory structure:



GOALS:

- Create and organize Active Directory accounts
- Create Group Policy Objects
- Link GPOs to appropriate Organizational Units

IMPORTANT NOTES

- During UAC prompts, enter the student account credentials.
- The domain controller is dc1.els.local at 10.10.250.5.
- The client pc is exec-1.els.local at 10.10.250.100.

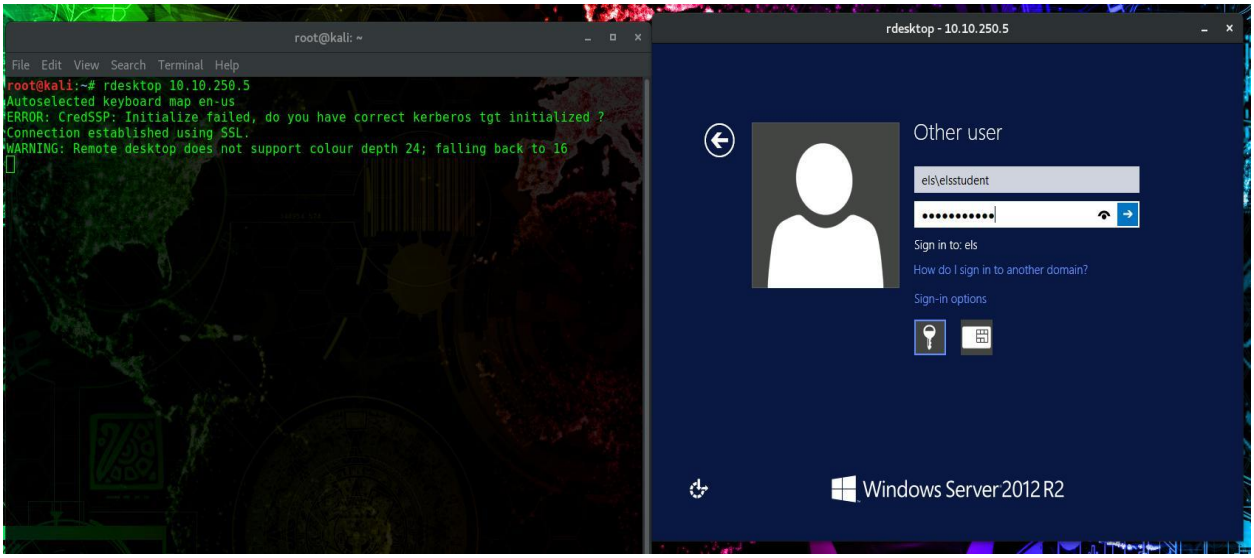
Task 1: Active Directory Users and Computers

The first step of this lab is to create the needed user accounts and organizational units for our environment.

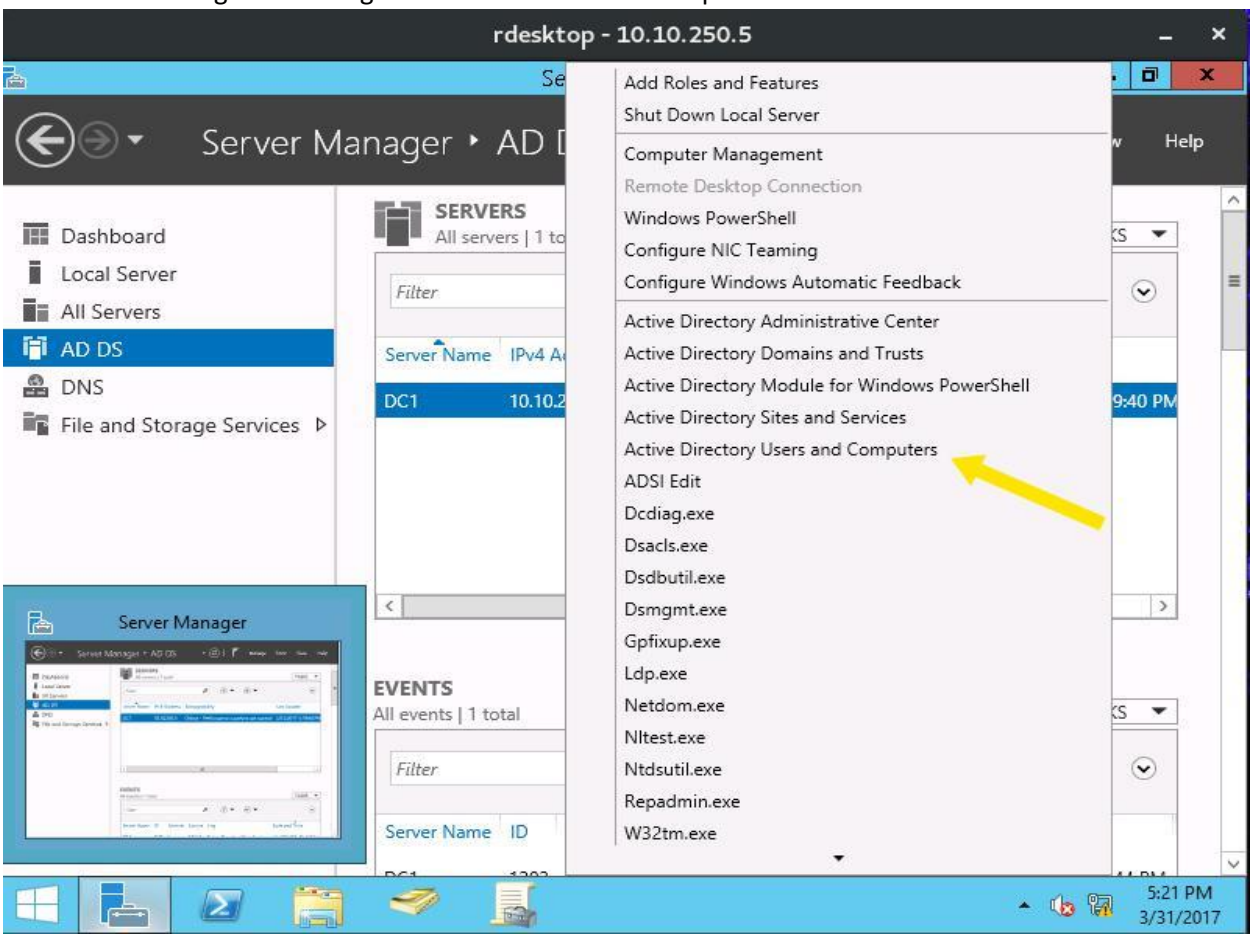
Task 1.1: Creating Organizational Units

Create multiple and nested organizational units based on the Active Directory diagram.

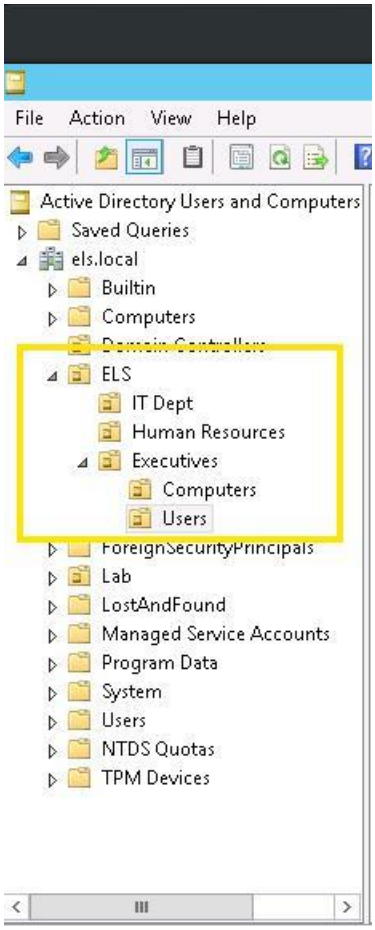
✓ I RDP'd into the domain controller:



✓ I opened server manager and navigated to the AD users & computers:



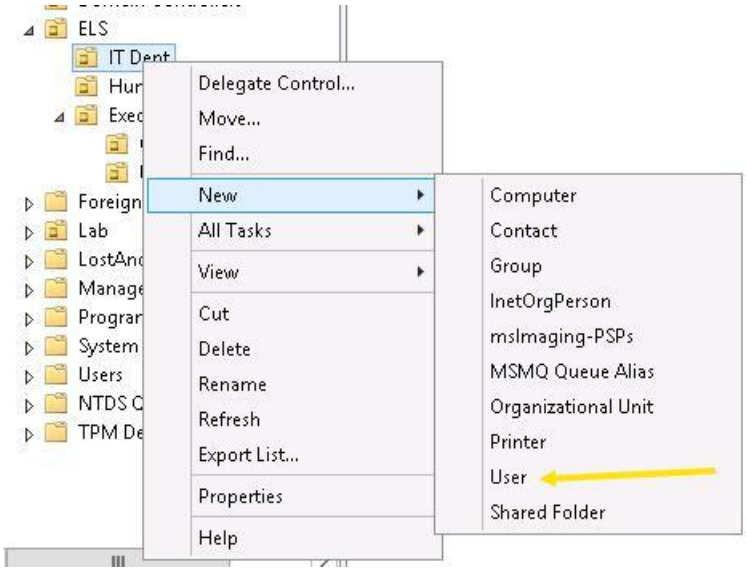
✓ I navigated the AD tree and added the OU's in the correct ELS section:



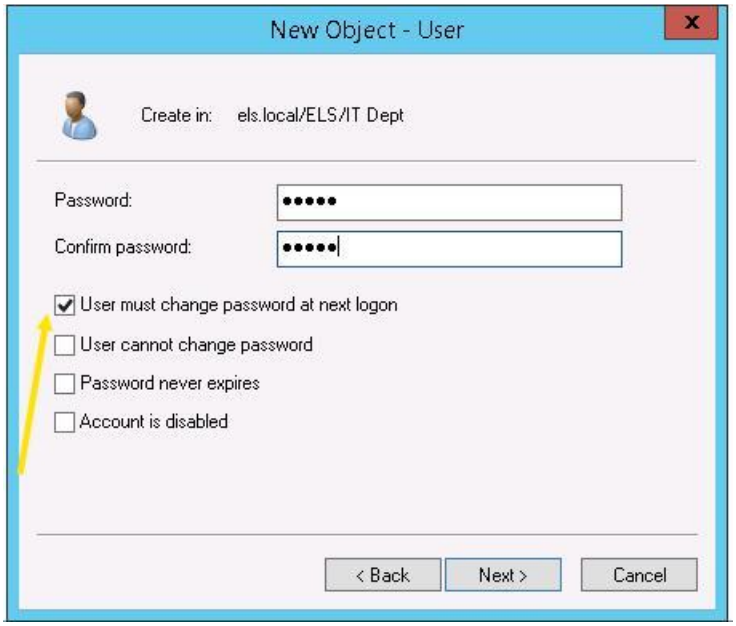
Task 1.2: Creating Accounts and Groups

- Create the missing users from the diagram.
- Add the users of the I.T. department into the IT Admins security group.
- Ensure new user accounts must change their password upon first login.
- Ensure the security group and computers are also placed in the appropriate organizational unit.

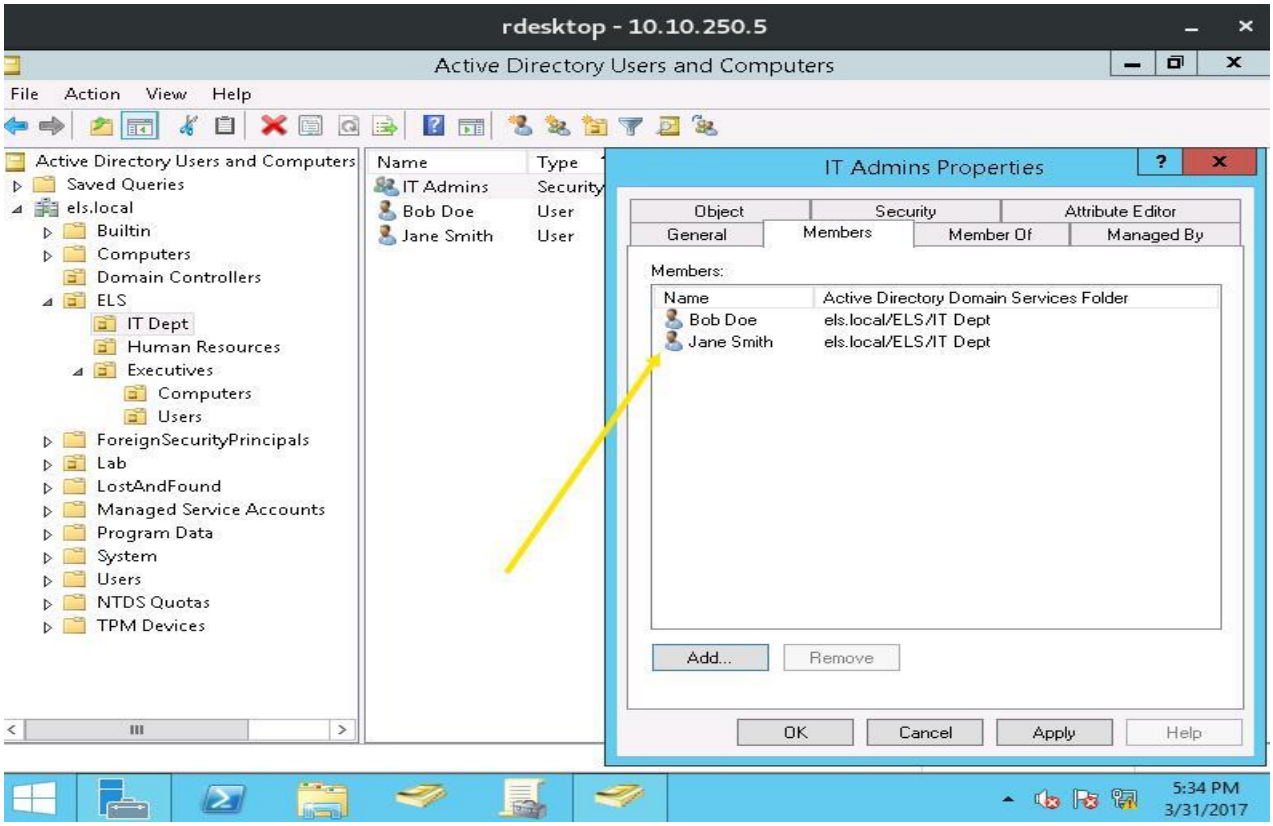
✓ I created the users based on the AD diagram:



✓ I enabled the change password at next login rule:



✓ I created an IT admins group and added the IT users:

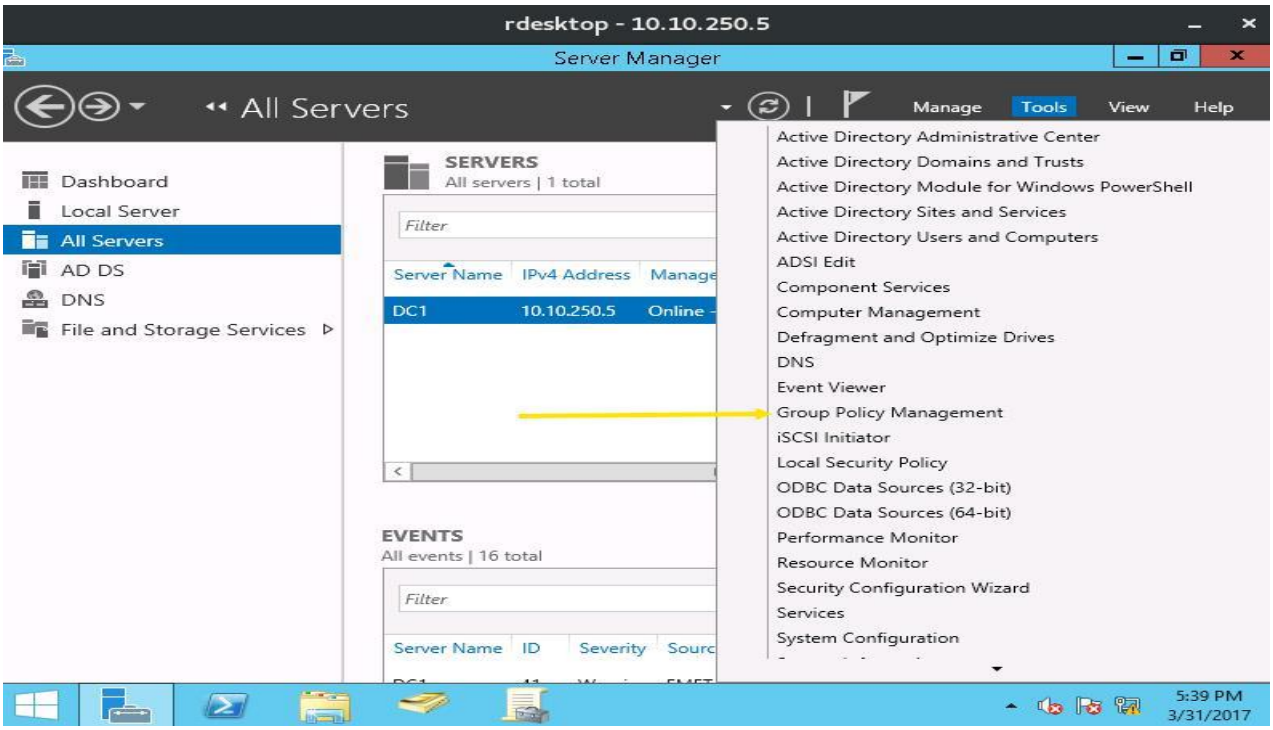


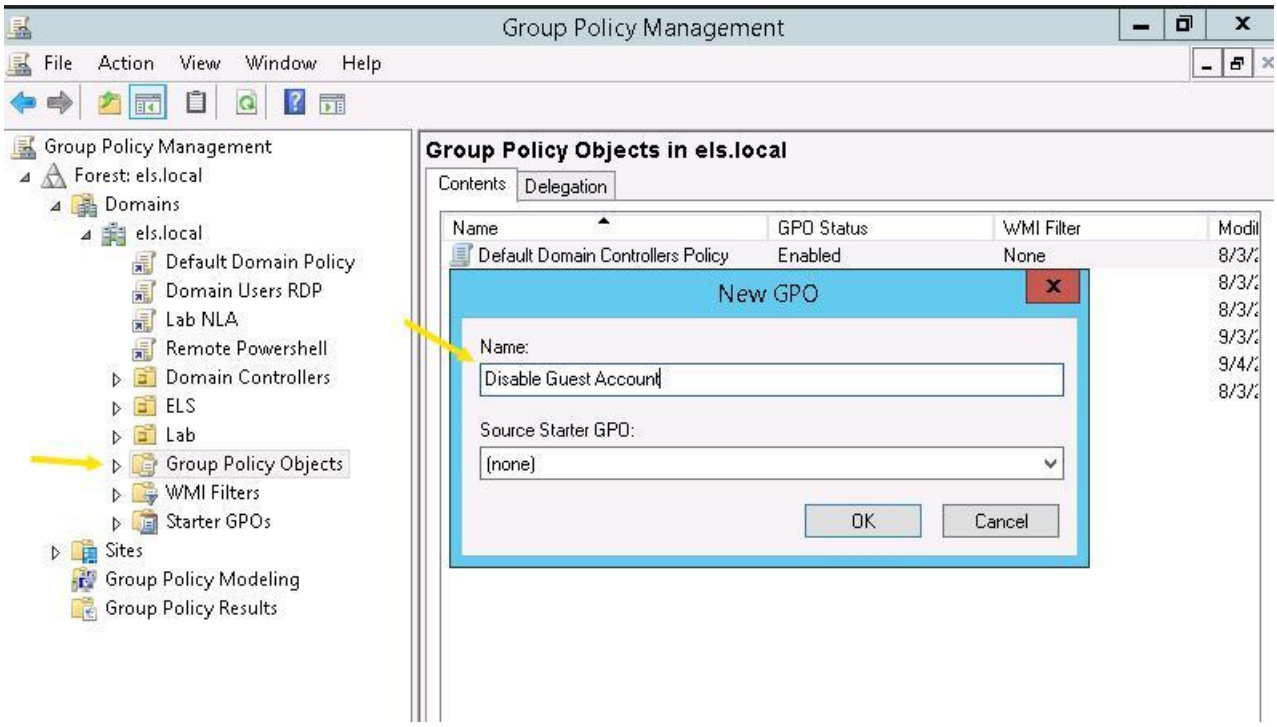
Task 2: Group Policy

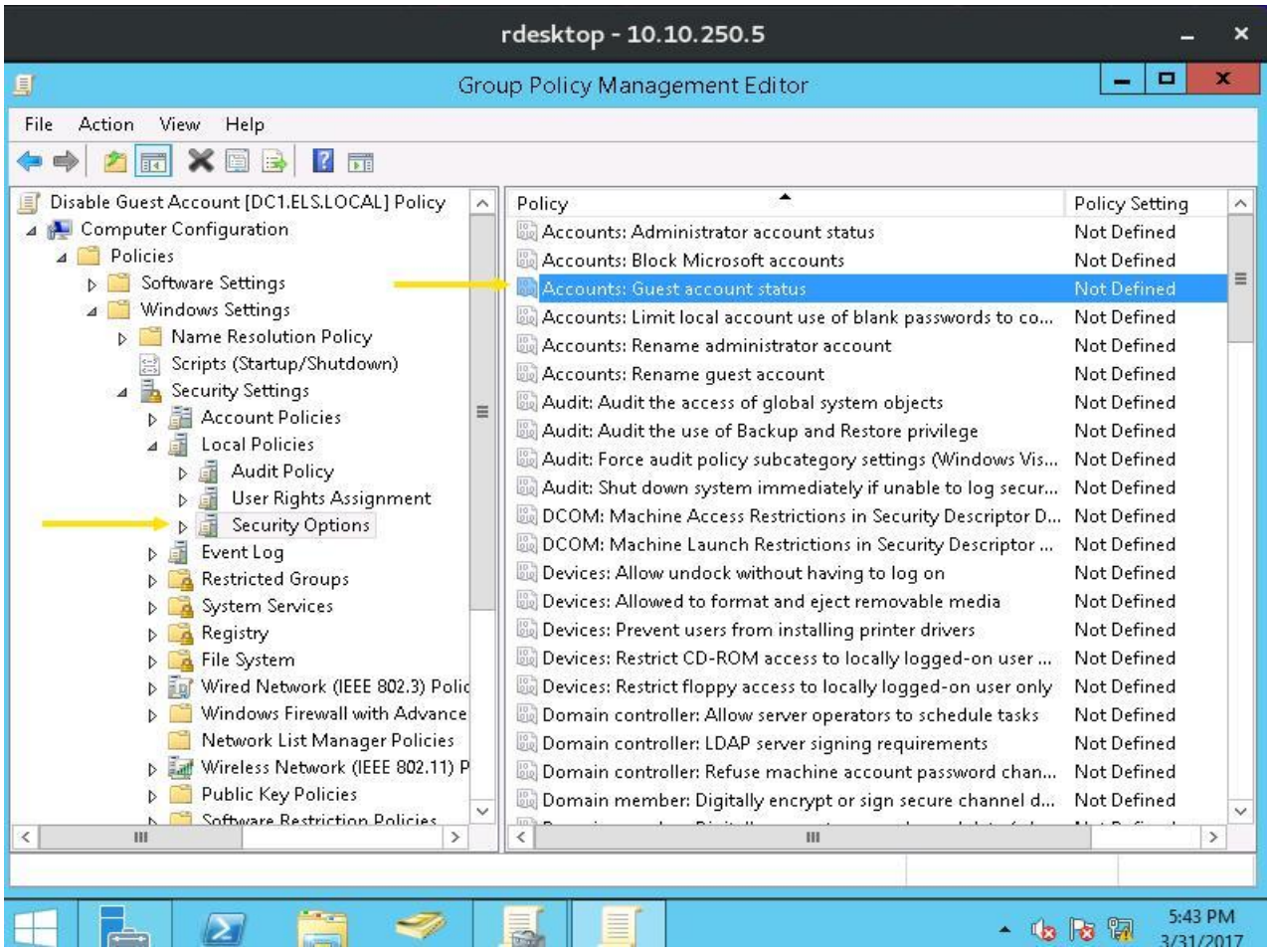
Task 2.1: Creating first computer GPO

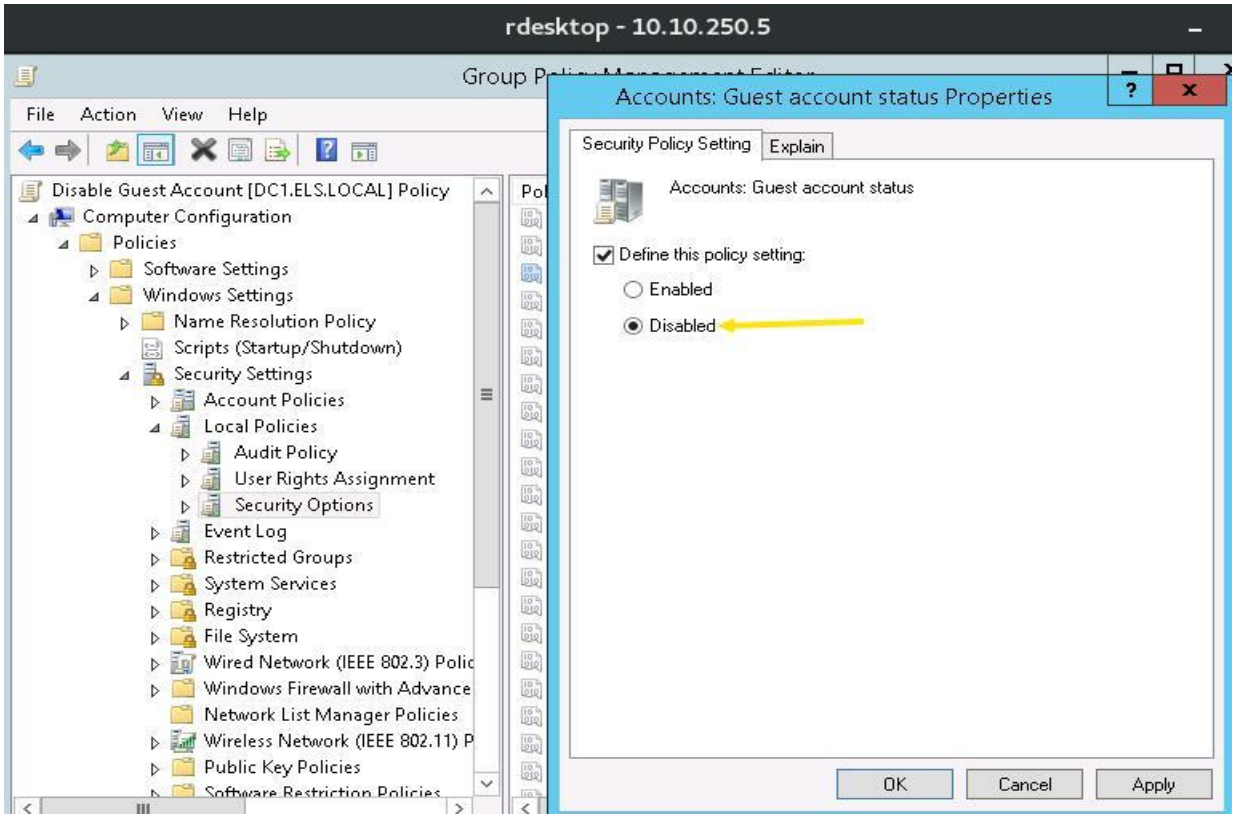
Create a computer-based GPO which disables the Guest account.

✓ I opened the Group Policy Management snap-in & created the Disable Guest Account GPO:


rdesktop - 10.10.250.5
Server Manager
All Servers
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
SERVERS
All servers | 1 total
Filter
Server Name
IPv4 Address
Manage
DC1
10.10.250.5
Online
EVENTS
All events | 16 total
Filter
Server Name
ID
Severity
Sourc
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
5:39 PM
3/31/2017


Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: els.local
Domains
els.local
Default Domain Policy
Domain Users RDP
Lab NLA
Remote Powershell
Domain Controllers
ELS
Lab
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in els.local
Contents
Delegation
Name
GPO Status
WMI Filter
Default Domain Controllers Policy
Enabled
None
New GPO
Name:
Disable Guest Account
Source Starter GPO:
(none)
OK
Cancel

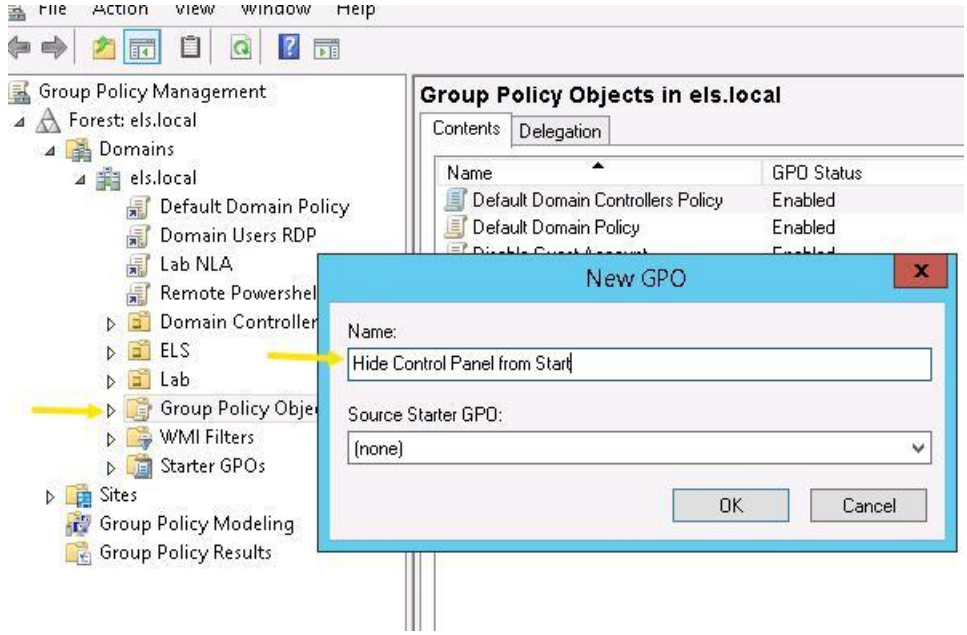

rdesktop - 10.10.250.5
Group Policy Management Editor
File Action View Help
Disable Guest Account [DC1.ELS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polic
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Policy
Policy Setting
Accounts: Administrator account status Not Defined
Accounts: Block Microsoft accounts Not Defined
Accounts: Guest account status Not Defined
Accounts: Limit local account use of blank passwords to co... Not Defined
Accounts: Rename administrator account Not Defined
Accounts: Rename guest account Not Defined
Audit: Audit the access of global system objects Not Defined
Audit: Audit the use of Backup and Restore privilege Not Defined
Audit: Force audit policy subcategory settings (Windows Vis... Not Defined
Audit: Shut down system immediately if unable to log secur... Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D... Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ... Not Defined
Devices: Allow undock without having to log on Not Defined
Devices: Allowed to format and eject removable media Not Defined
Devices: Prevent users from installing printer drivers Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ... Not Defined
Devices: Restrict floppy access to locally logged-on user only Not Defined
Domain controller: Allow server operators to schedule tasks Not Defined
Domain controller: LDAP server signing requirements Not Defined
Domain controller: Refuse machine account password chan... Not Defined
Domain member: Digitally encrypt or sign secure channel d... Not Defined
5:43 PM
3/31/2017

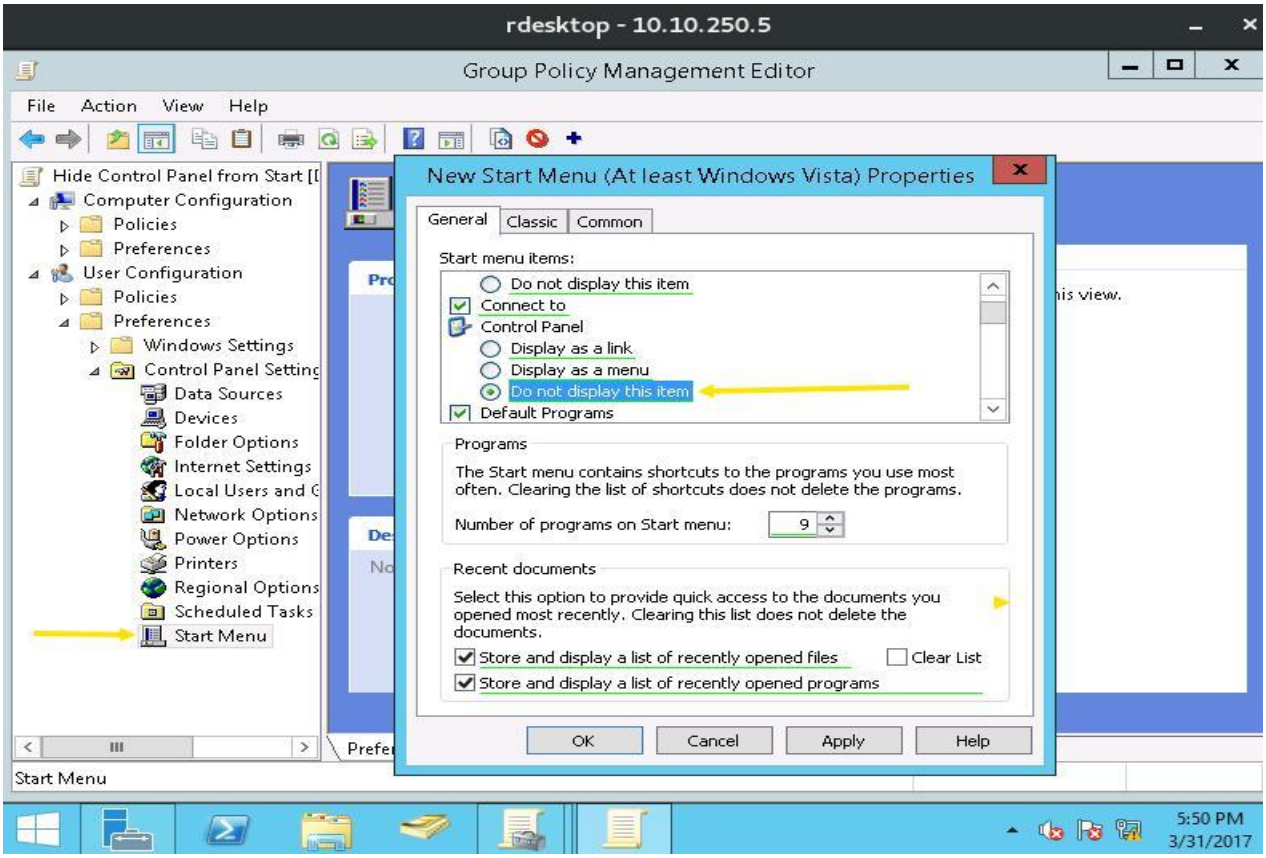

rdesktop - 10.10.250.5
File Action View Help
Disable Guest Account [DC1.ELS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polic
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Accounts: Guest account status Properties
Security Policy Setting
Explain
Accounts: Guest account status
Define this policy setting:
Enabled
Disabled
OK
Cancel
Apply

Task 2.2: Creating first user GPO

Create a user-based GPO which sets a preference to hide the Control Panel from the Start menu.

✓ I created the Hide Control Panel GPO:





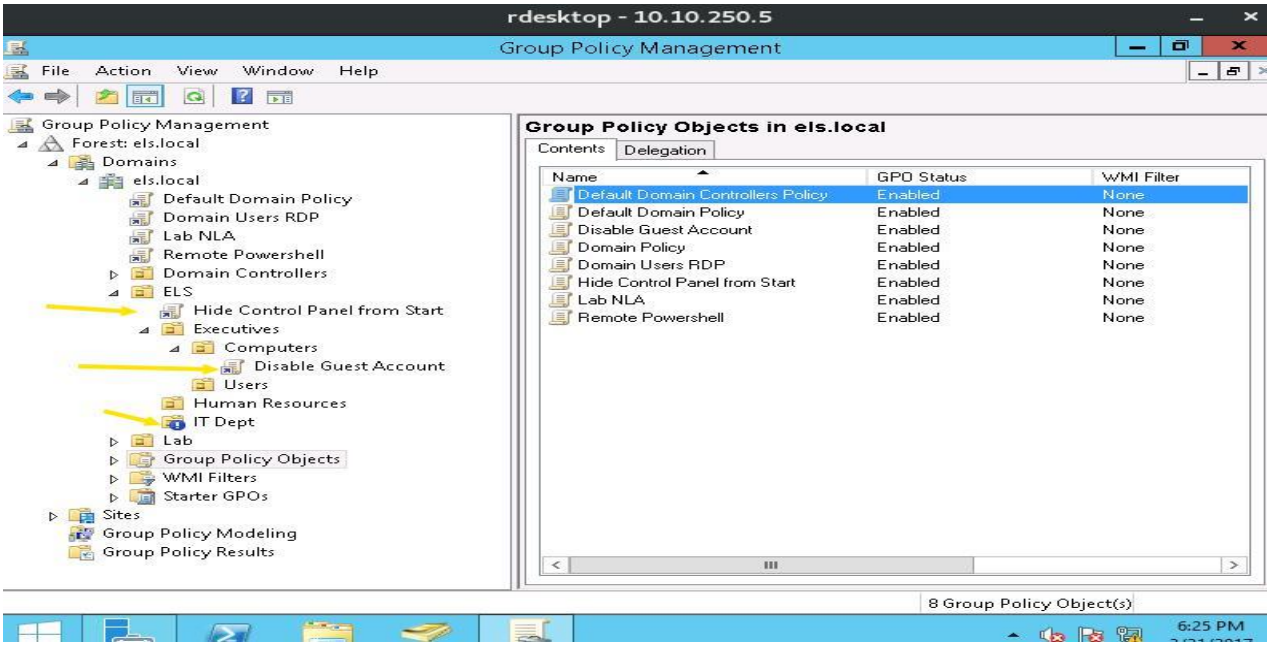
Task 2.3 Linking GPO's

Link the GPO's to:

- Disable the Guest account to the Executives' computers.

- Disable the control panel for all the users in the *ELS* OU except the IT Department ones.
- Make an exception for the IT Department: let them leave the Control Panel enabled. Ensure the IT OU is exempt from inherited GPOs.

✓ I linked the GPO's to the proper OU and did a "Block Inheritance" for IT:

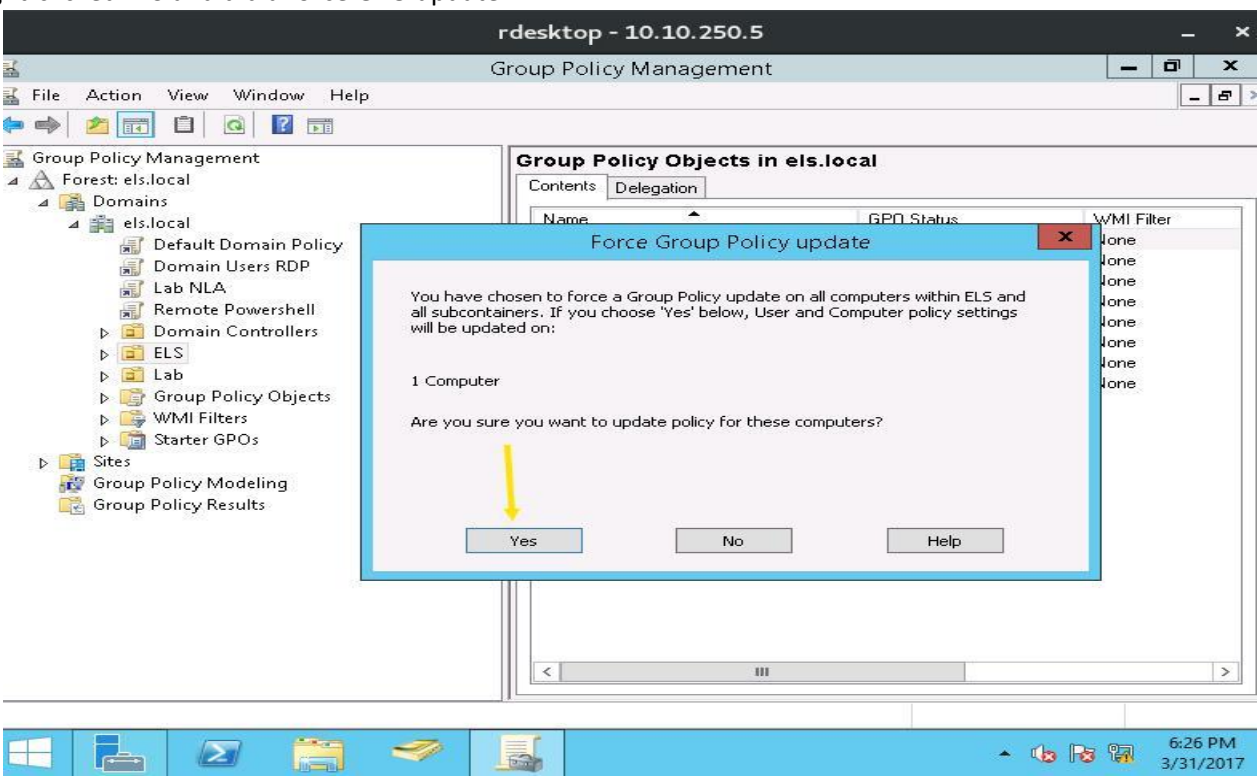


Task 3: Client Computers

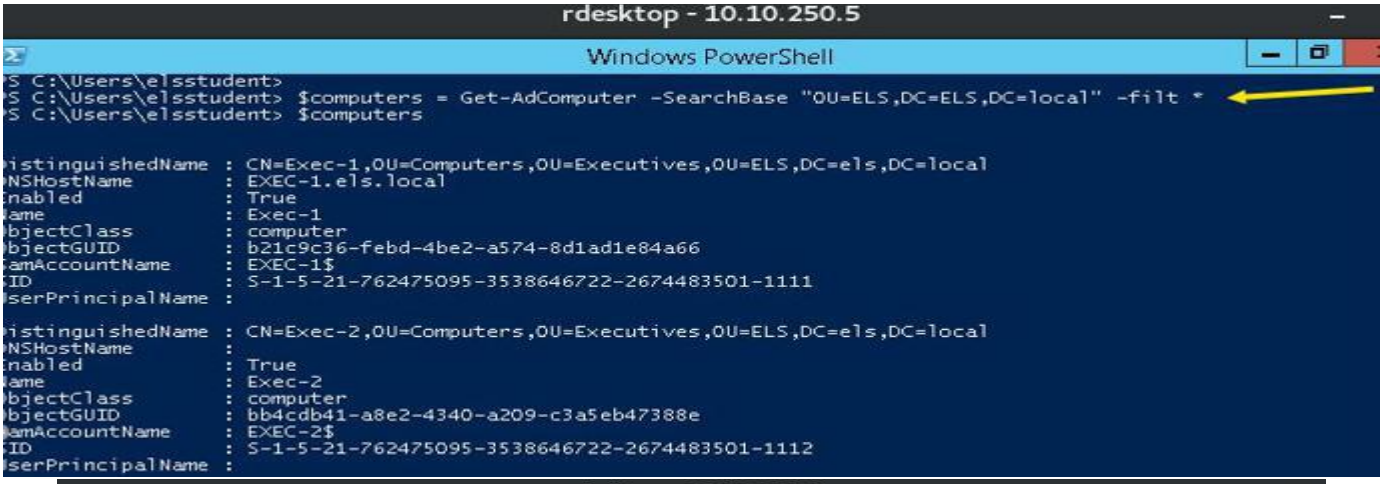
Task 3.1: Force client update

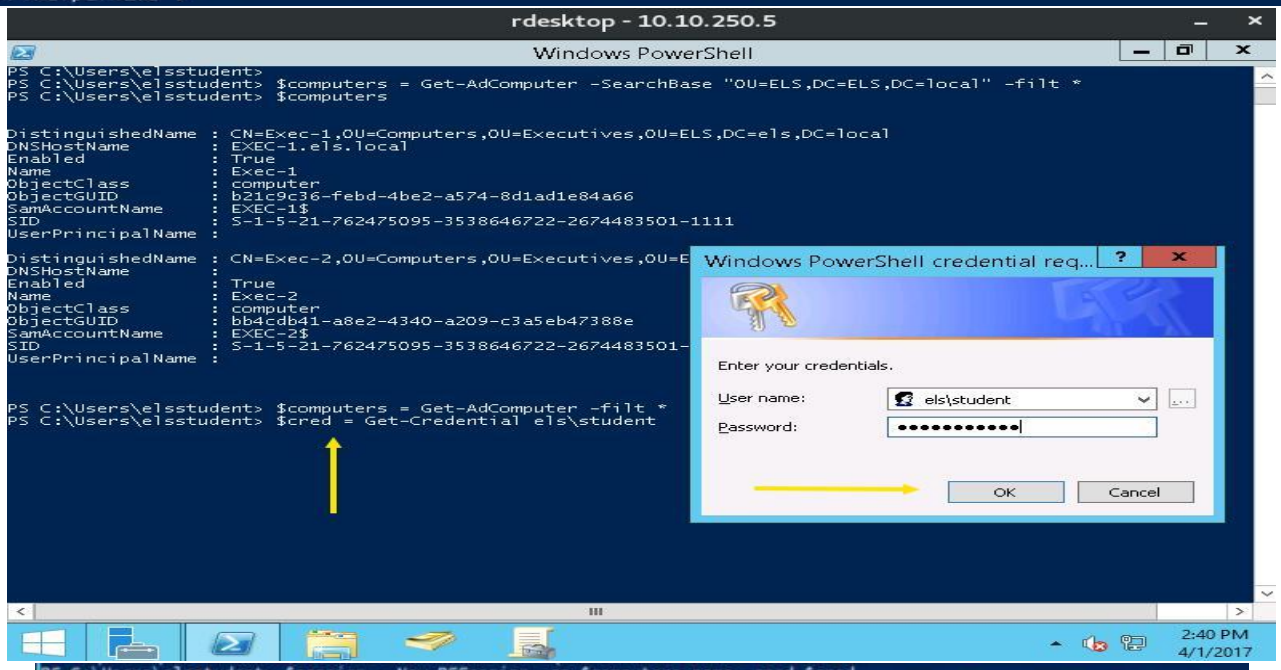
Login to the domain controller and force a policy update in the machines under the *ELS* OU.

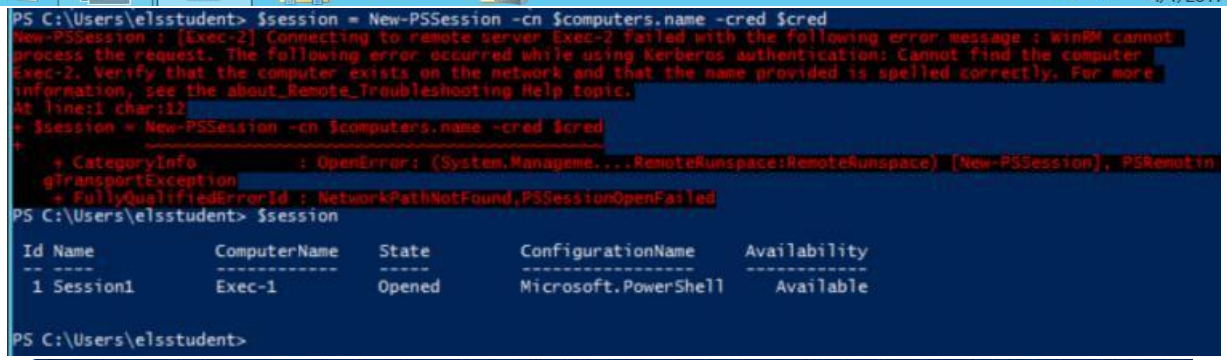
✓ I right-clicked ELS and did a force GPO update:

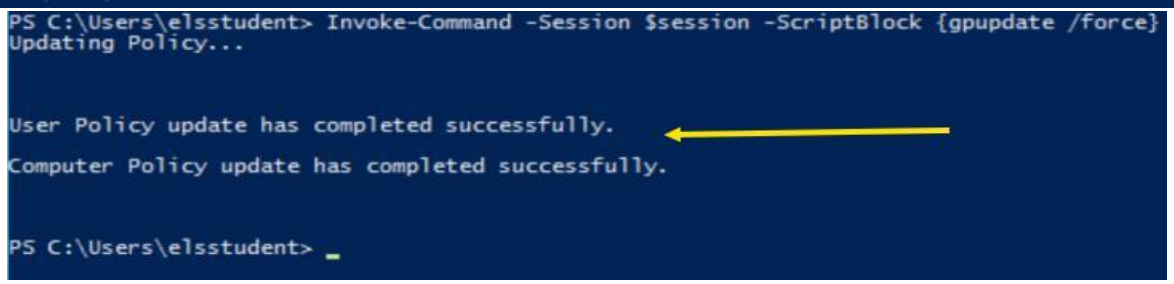


✓ I followed the additional PowerShell update example:





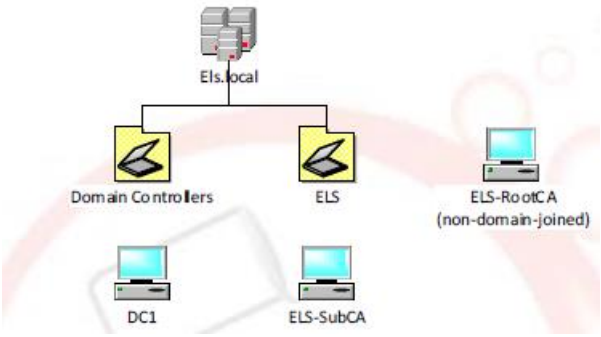




LAB 3 ADCS

LAB DESCRIPTION

In the following lab, you can practice setting up a basic PKI with Active Directory Certificate Services. You will setup an offline Root CA on a non-member server, setup a subordinate CA on a member server and then deploy the root certificate with Group Policy. You will be working with this Active Directory structure:



GOALS:

- Setup an offline Root CA with A.D. Certificate Services
- Setup a subordinate CA with A.D. Certificate Services
- Deploy the certificate with Group Policy to the ELS OU.

Important Note:

- The domain controller is dc1.els.local at 10.20.250.5
- The RootCA is els-rootca at 10.20.250.20
- The SubCa is els-subca.els.local at 10.20.250.21.

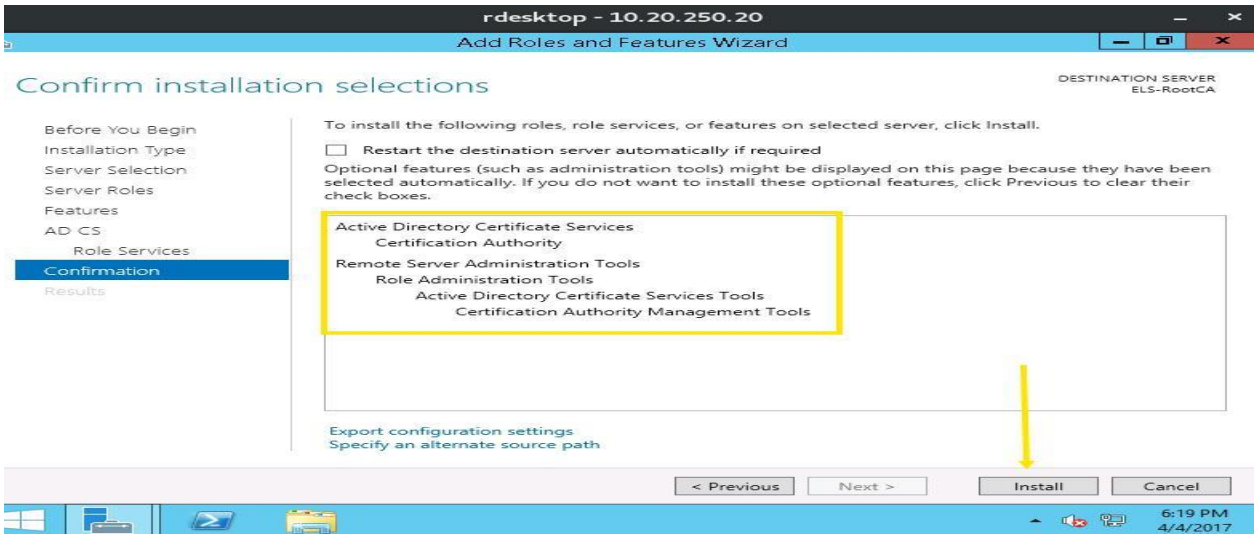
Task 1: Offline Root Certificate Authority

The first step of this lab is to setup the offline Root Certificate Authority.

Task 1.1: Install Active Directory Certificate Services

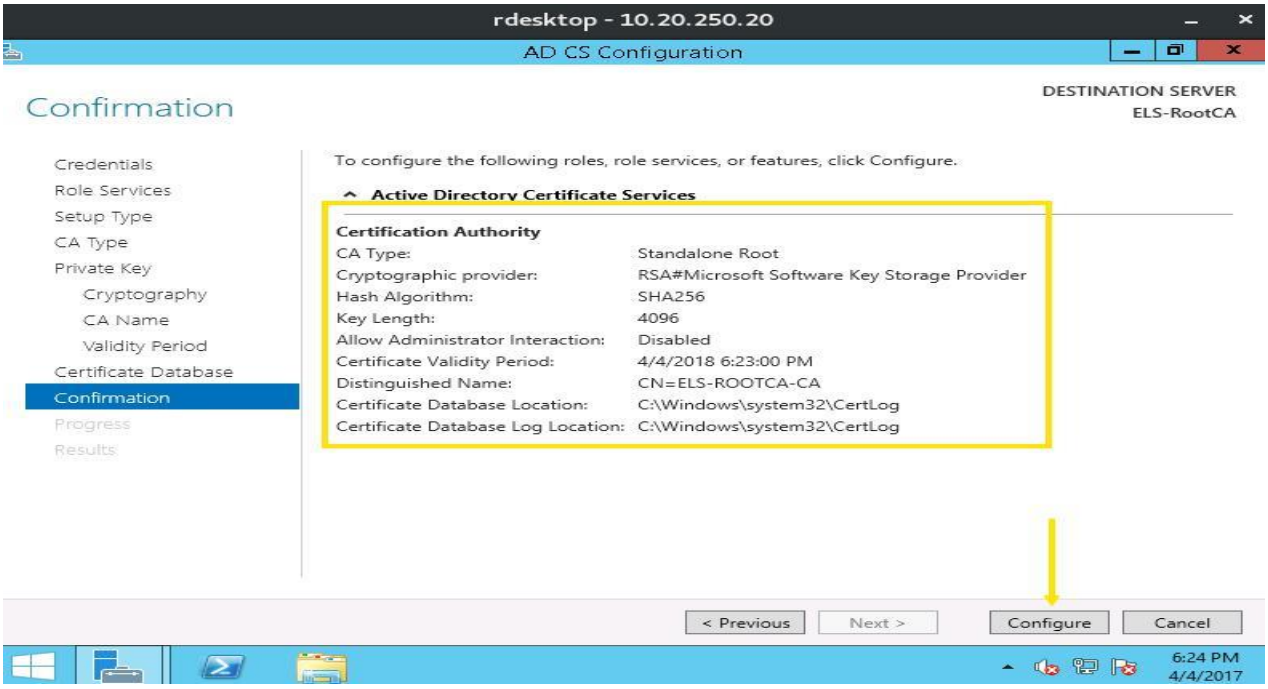
Install the Active Directory Certificate Services role with no additional role services.

✓ I installed ADCS:



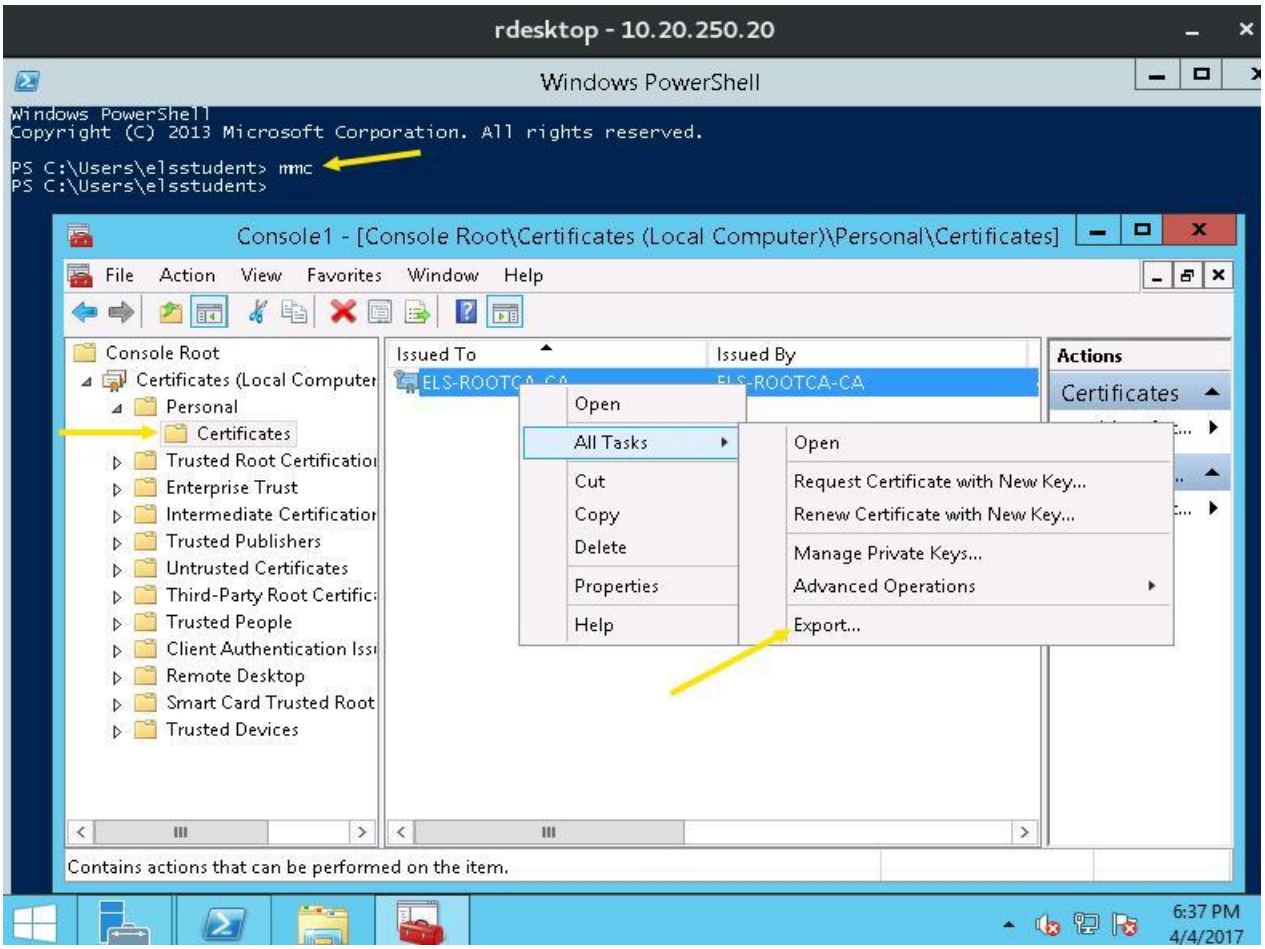
Task 1.2: Configure Certificate Services

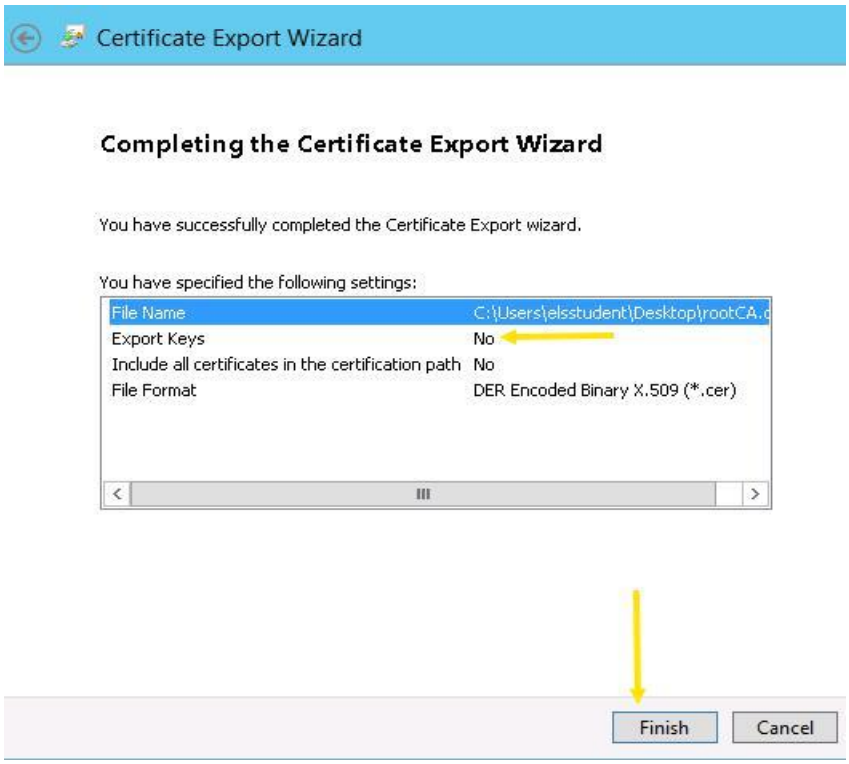
✓ I configured ADCS:



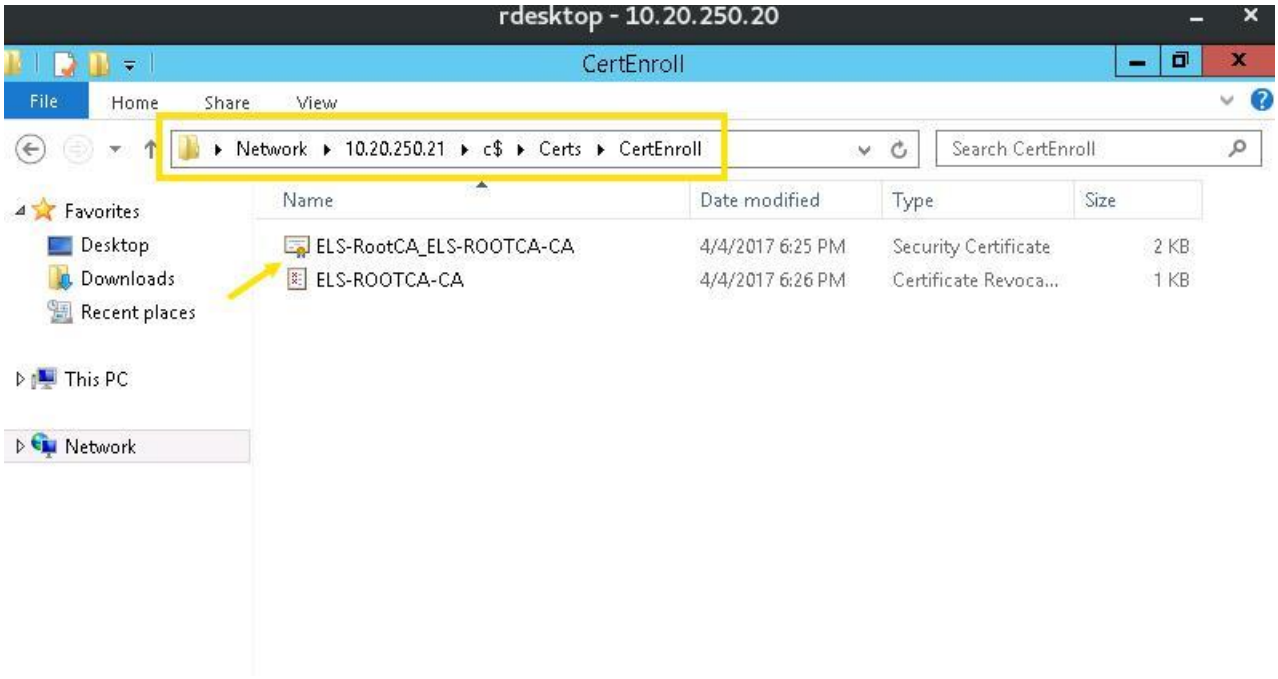
Task 1.3: Export Root CA Certificates

✓ Export the certificate:





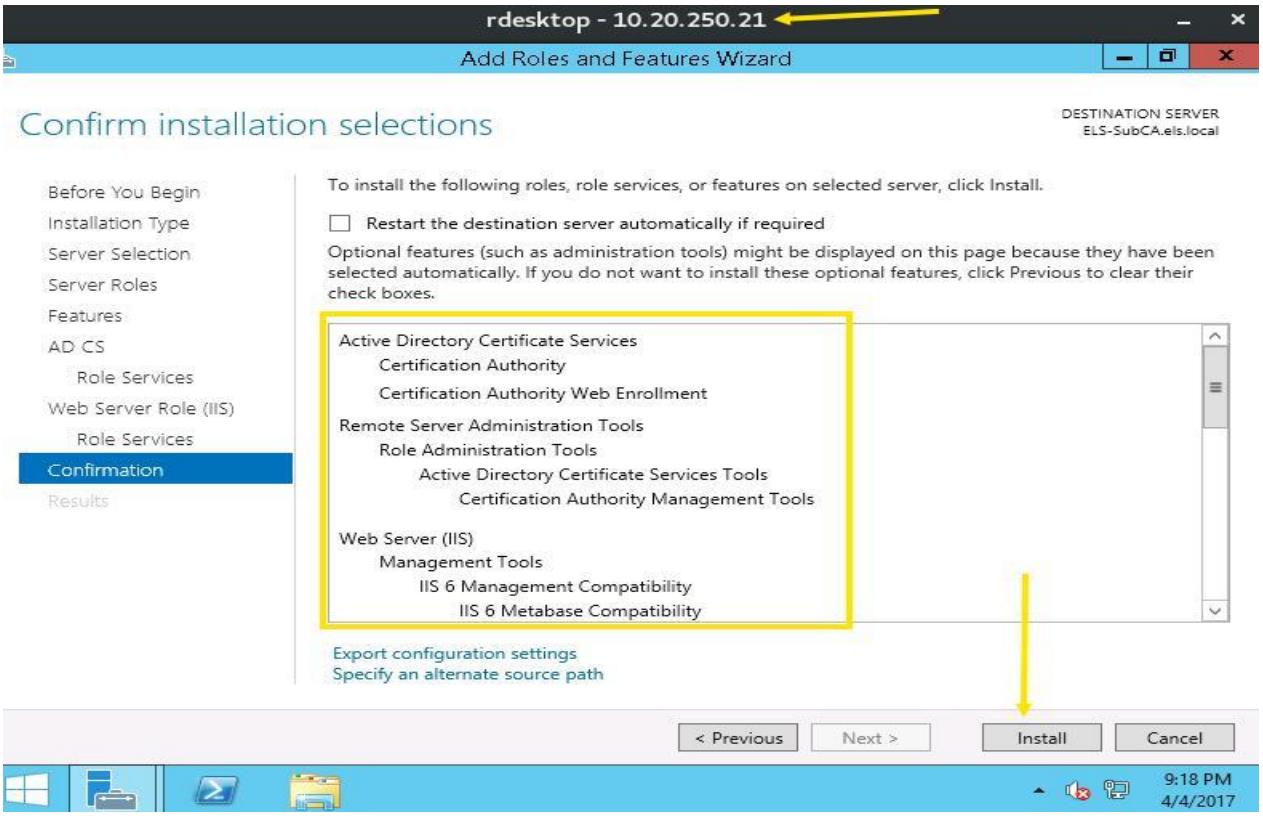
✓ I copied the exported certificate & files to the SubCa host (10.20.250.21) using admin share:



Task 2: Subordinate Certificate Authority

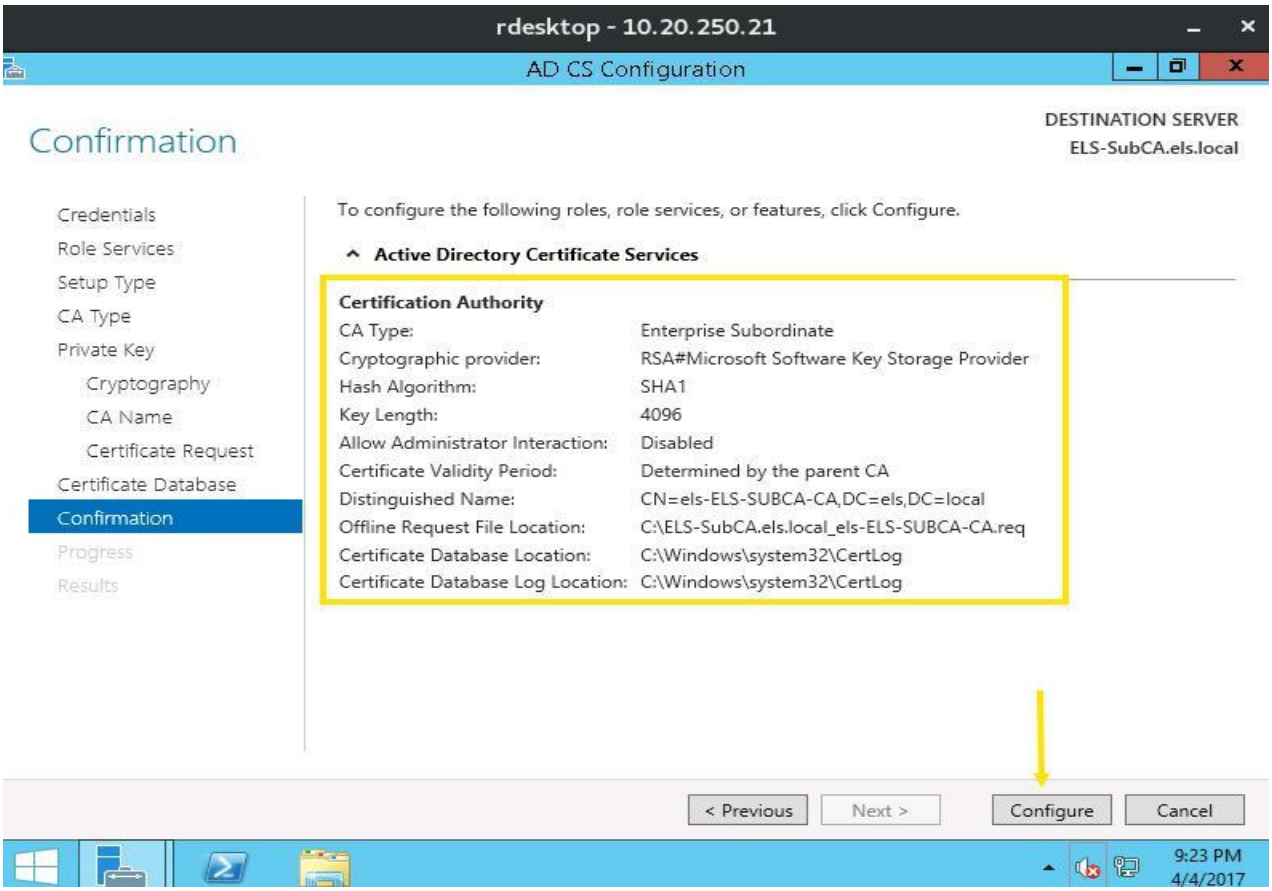
Task 2.1: Installing Certificate Services

✓ Install the Active Directory Certificate Services role on the SubCA server:



Task 2.2: Configuring Certificate Services

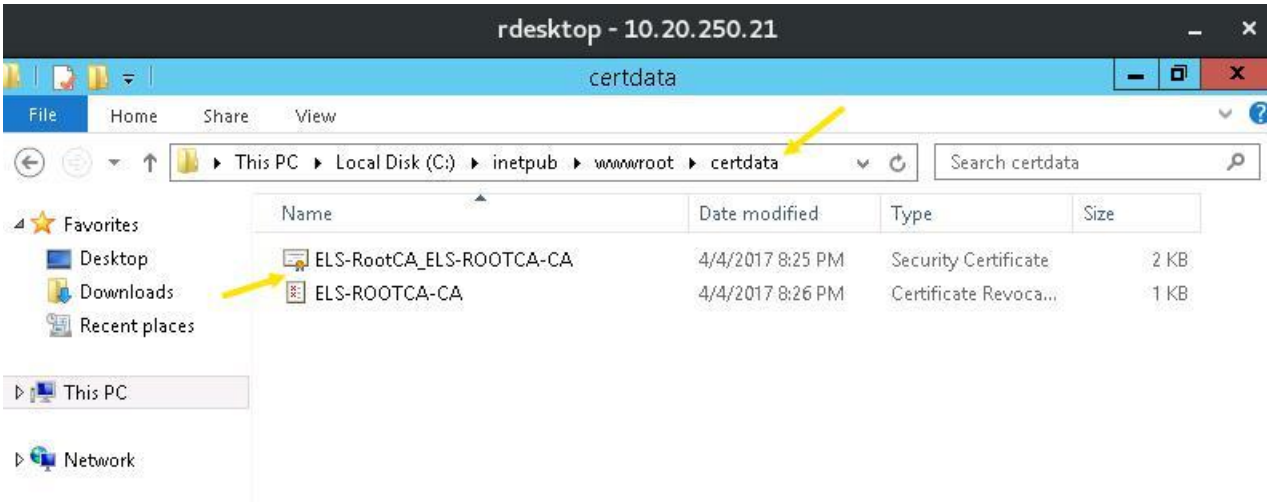
✓ Once installed, configure the role:

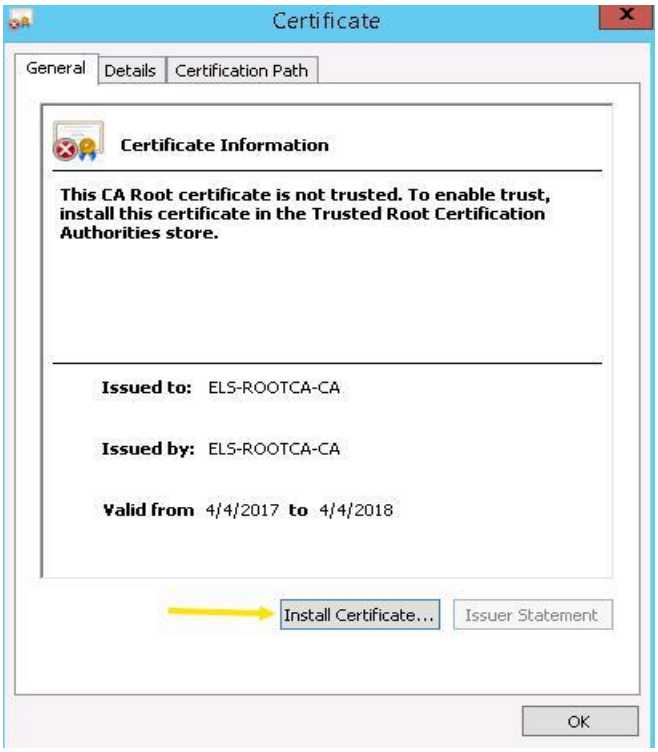


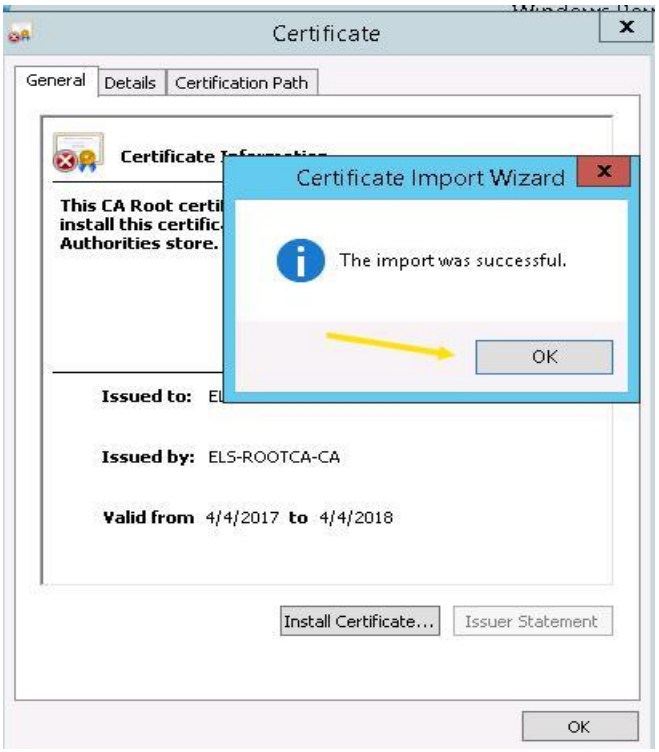
Task 2.3: Install Certificates and establish Subordinate CA

✓ Install the Root certificate and CRL on the SubCa and establish it as a subordinate CA:

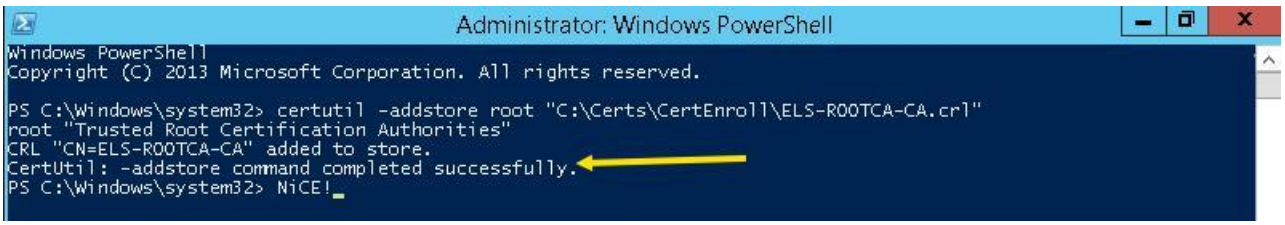
I had to navigate to the folder where I copied the RootCA files:



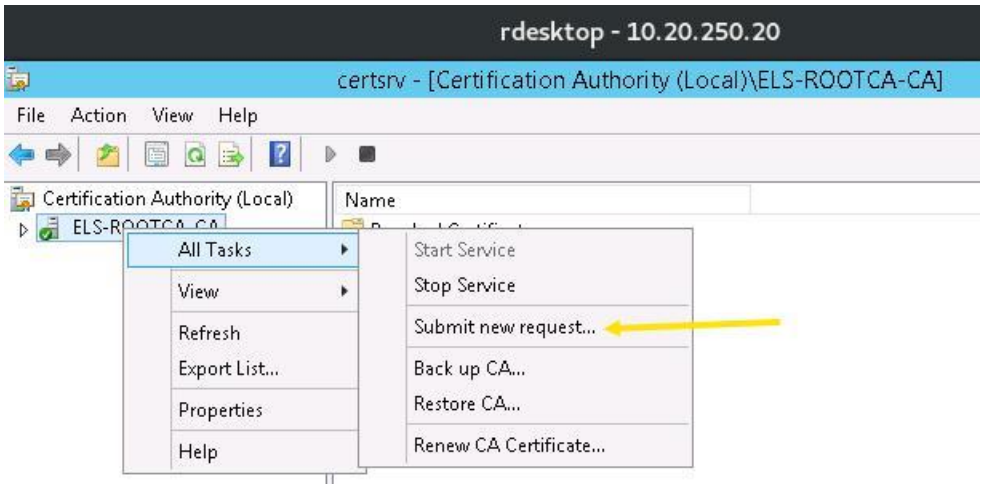




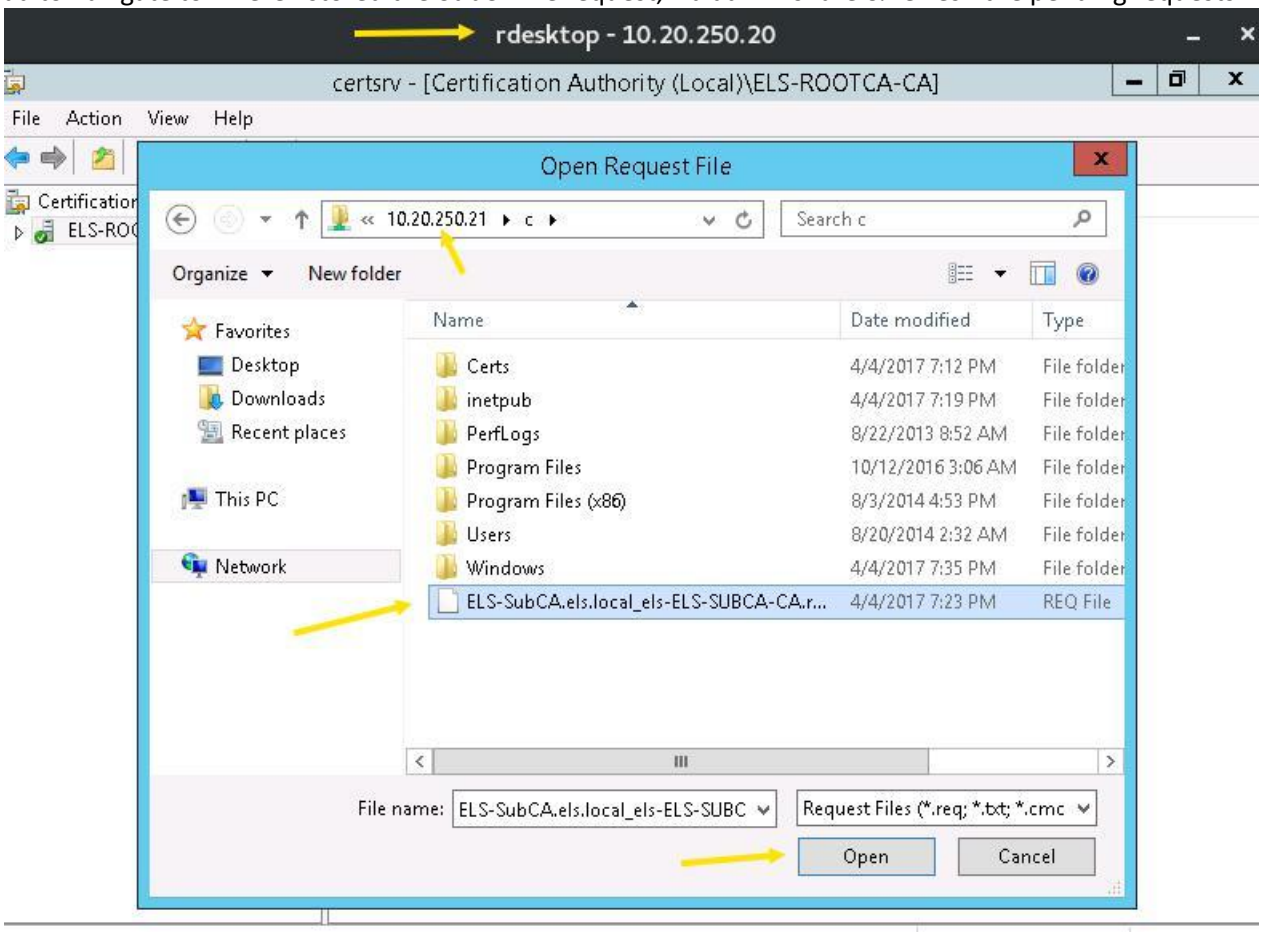
✓ I then added the CRL to the local store:

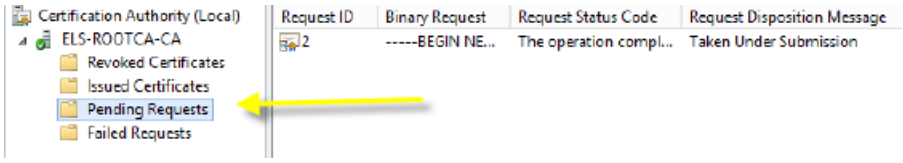


✓ I went back to the RootCA host and submit the new request:

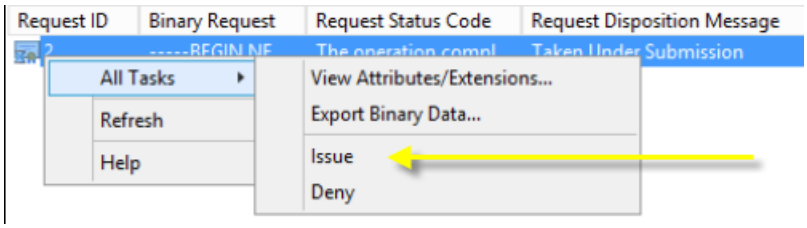


I then had to navigate to where I stored the SubCA file request, via admin share & refresh the pending requests:

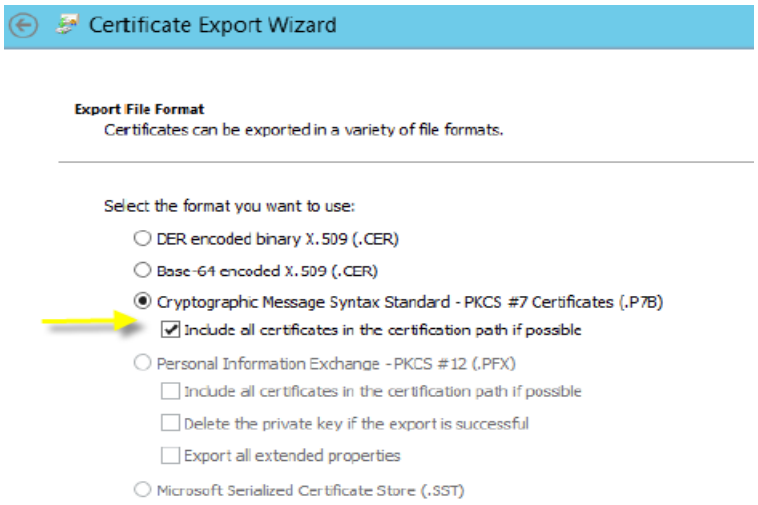




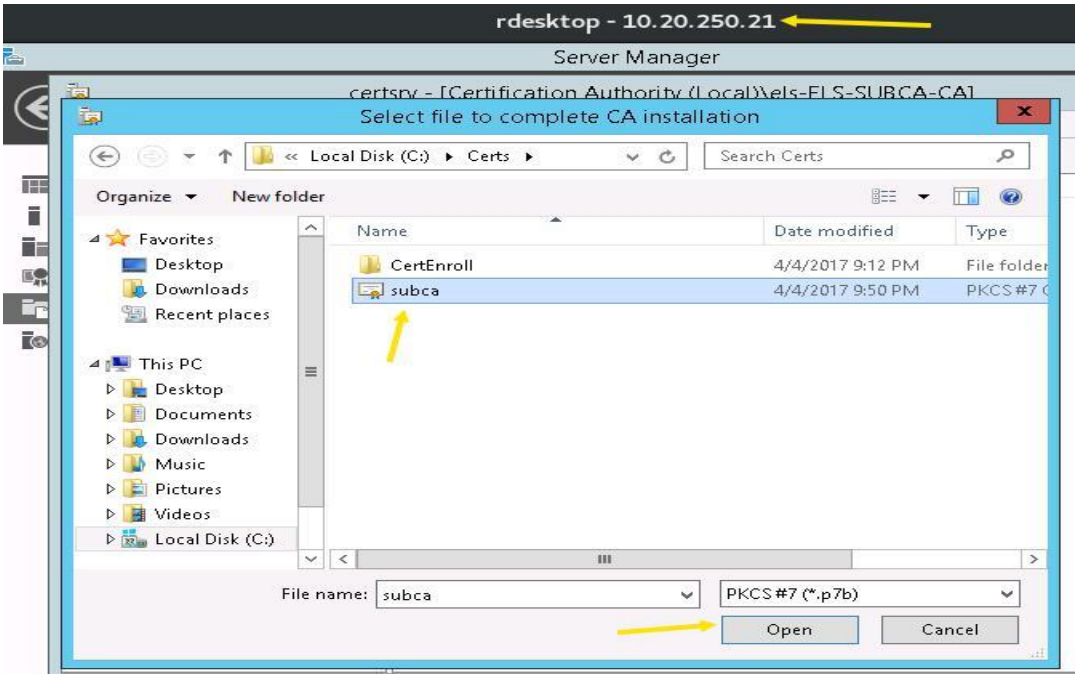
✓ I then issued the SubCA:



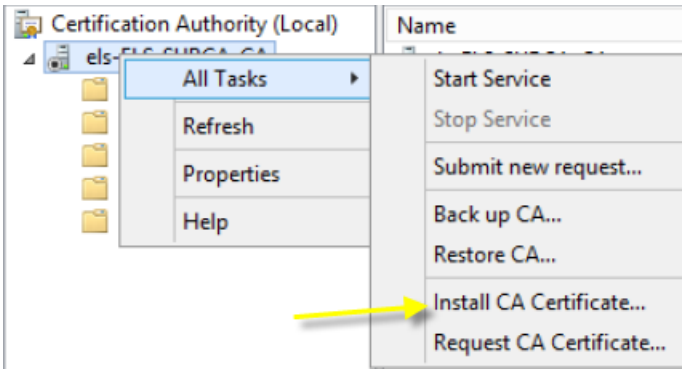
✓ I changed the format to P7B and included all the certificates in the path:

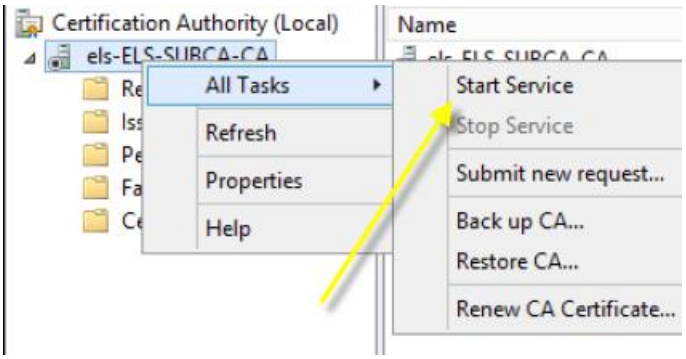


✓ Put the new SubCA cert to the right location:

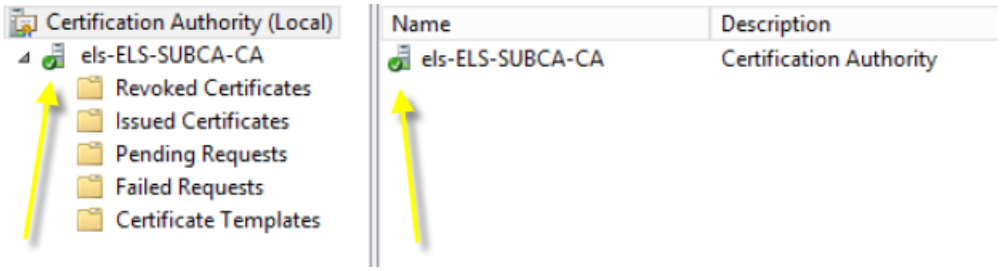


✓ I finished up the SubCA setup by opening the CA MMC → installing the CA cert → Start Srvice:





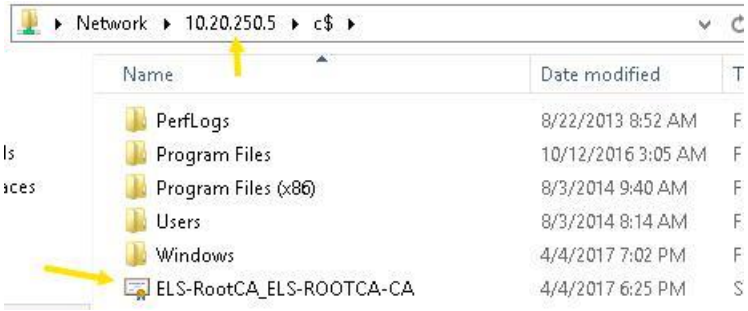
✓ We got the green check mark!



Task 3: Deploying Root Certificate

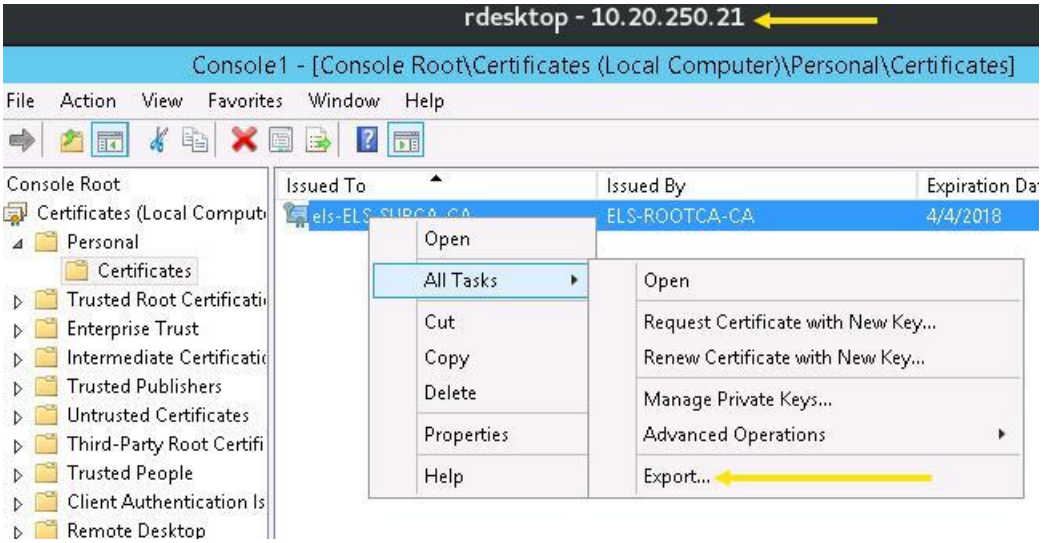
Task 3.1: Export Root CA to domain controller

✓ Copy the root certificate to the domain controller; you can use the admin share if needed.



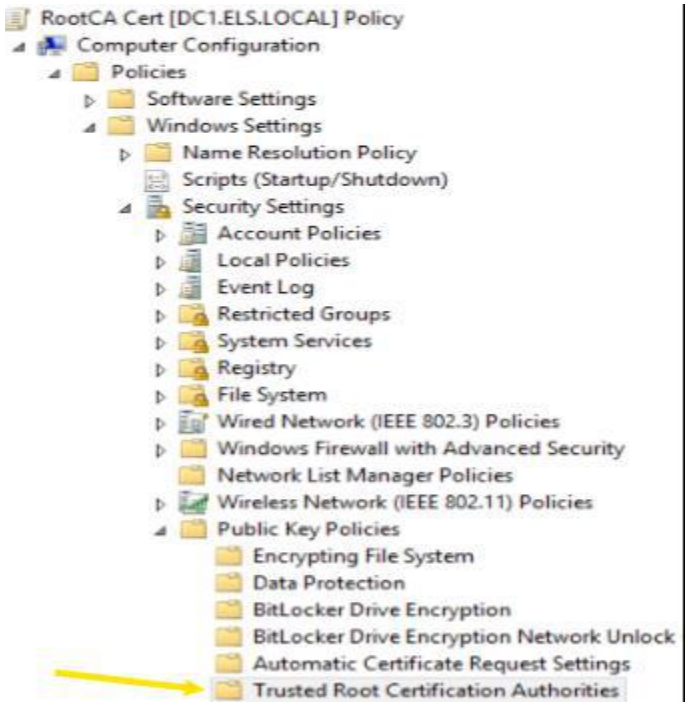
Task 3.2: Check if DC1 Trusts the Subordinate CA

✓ Copy the SubCa certificate on the Domain Controller, then verify that the DC does not trust SubCa.

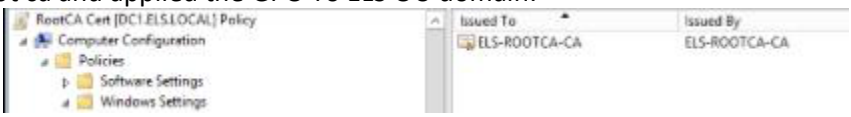


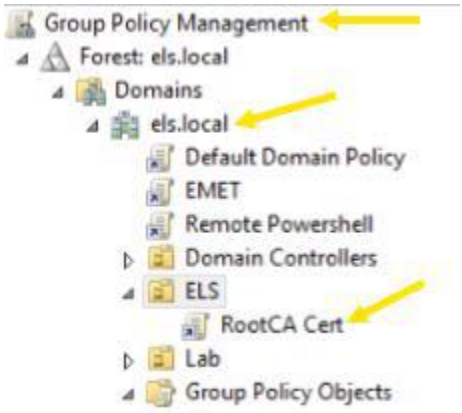
Task 3.3: Deploy Certificate with Group Policy

✓ Create a GPO which deploys the root certificate to the ELS OU.



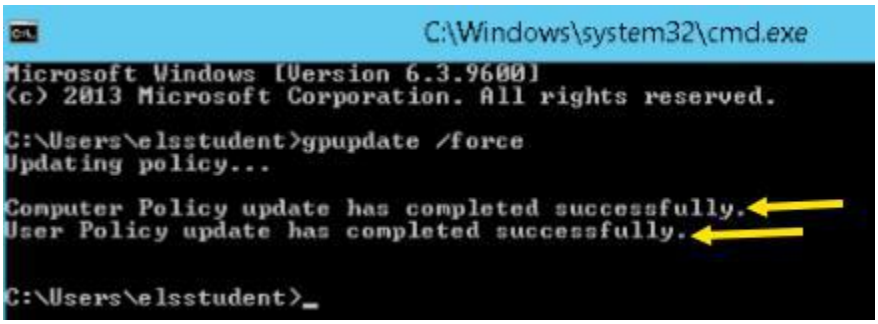
We made the trusted root ca and applied the GPO To ELS OU domain:





Task 3.4: Re-check DC1 Trust

✓ Force a group policy update and re-open the SubCa certificate. The DC should trust it.



LAB 4 WSUS

LAB DESCRIPTION

In the following lab, you can practice setting Windows Server Update Services.

GOALS

- Setup Windows Server Update Services.
- Setup WSUS GPOs.
- Check for updates against WSUS.

IMPORTANT NOTE

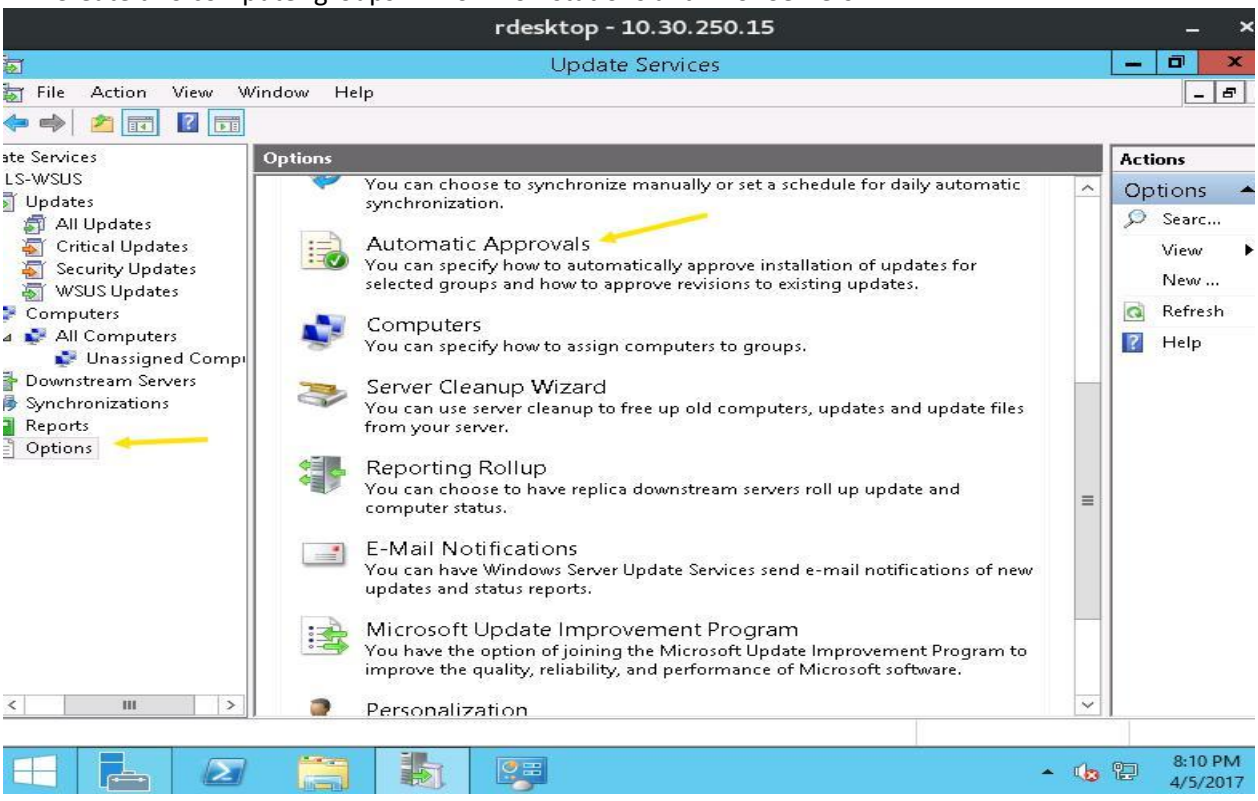
- Labs machines are not connected to the Internet, they are in a private testing environment just for you.
- The domain controller is dc1.els.local at 10.30.250.5
- The update server is at 10.30.250.15.
- The client machine (Win 7) is at 10.30.250.150
- The WSUS role is already installed on the update server.

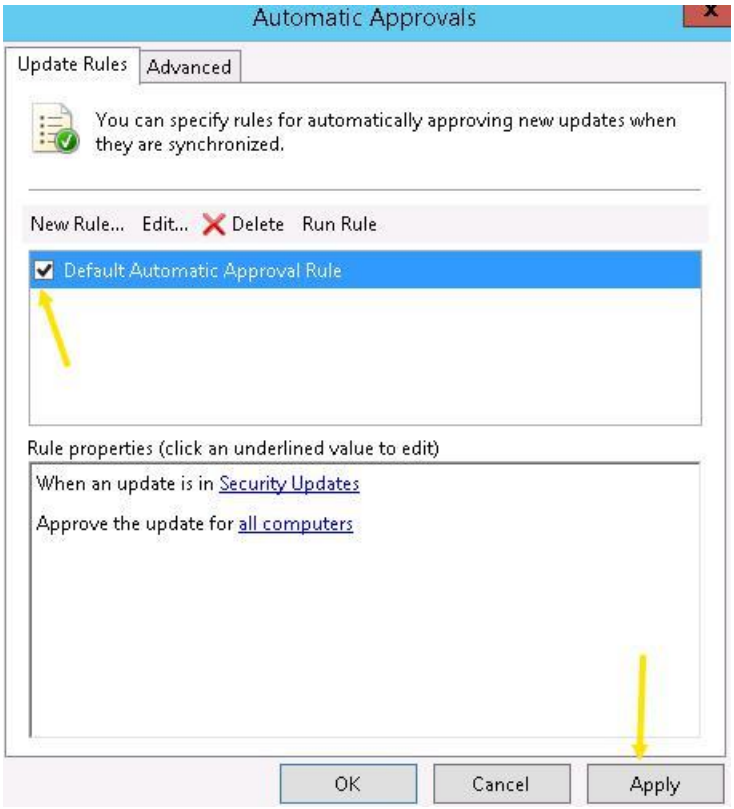
Task 1: Configure WSUS

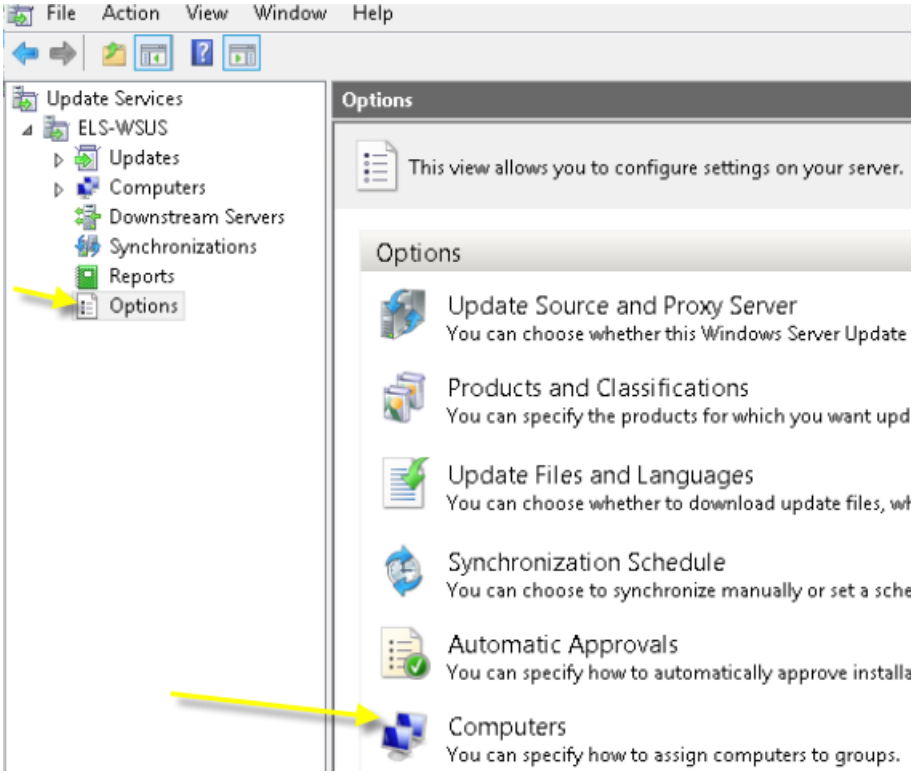
Task 1.1: Configure WSUS

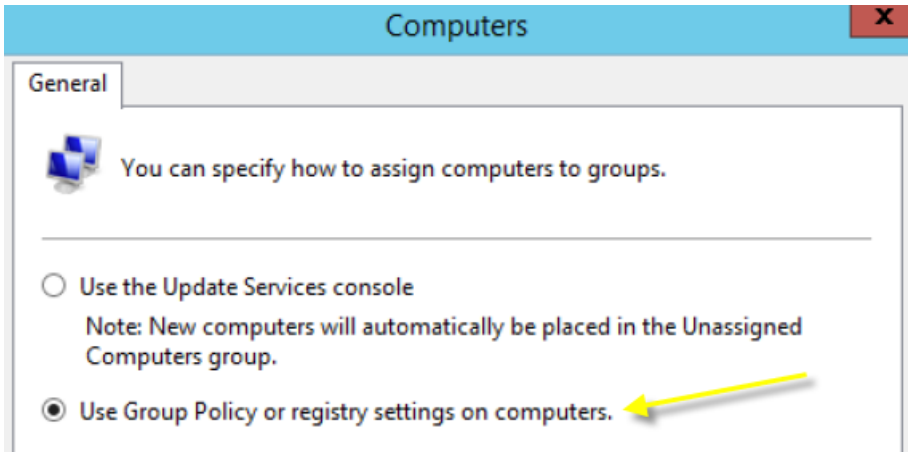
✓ Login to the Update Server and open WSUS. Configure WSUS to:

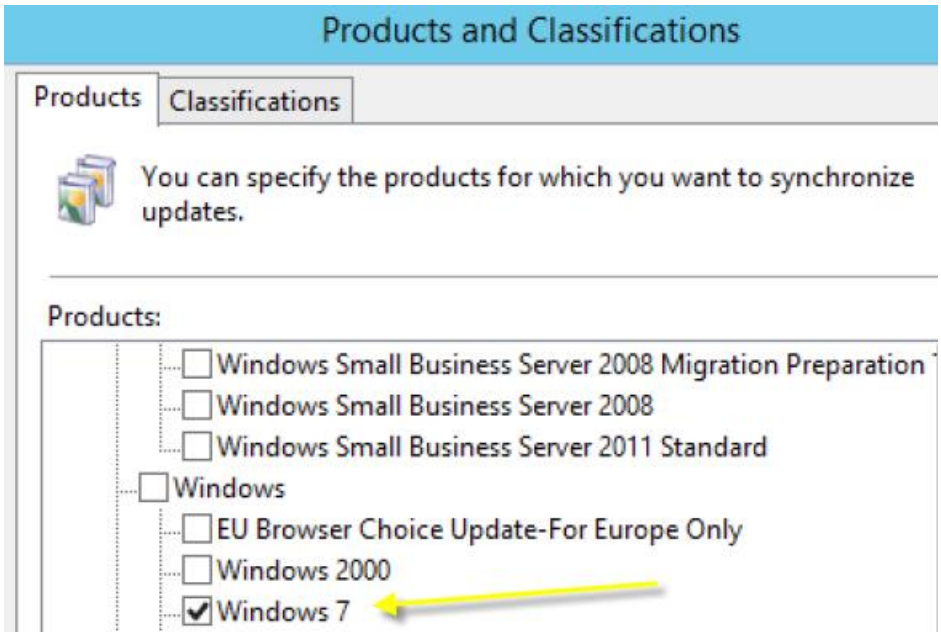
- Automatically approve only security updates for all computers
- Assign to computer groups based on GPO
- Sync for Windows 7 updates
- Approve all needed updates waiting for approval.
- Create two computer groups – 1 for Workstations and 1 for Servers.



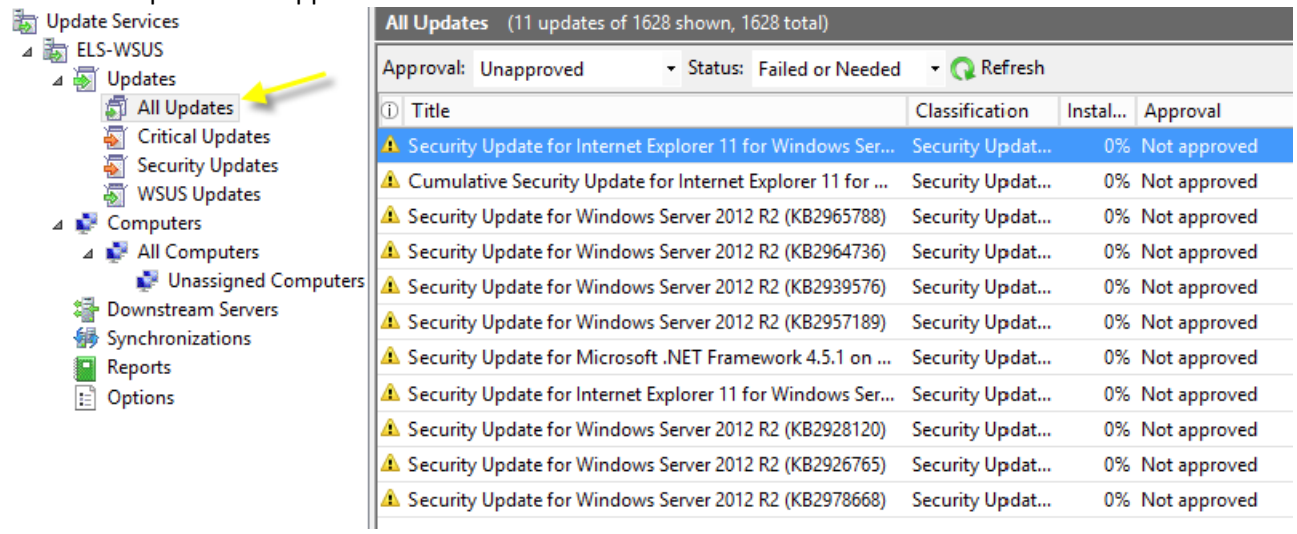

Automatic Approvals
Update Rules
Advanced
You can specify rules for automatically approving new updates when they are synchronized.
New Rule...
Edit...
Delete
Run Rule
Default Automatic Approval Rule
Rule properties (click an underlined value to edit)
When an update is in Security Updates
Approve the update for all computers
OK
Cancel
Apply

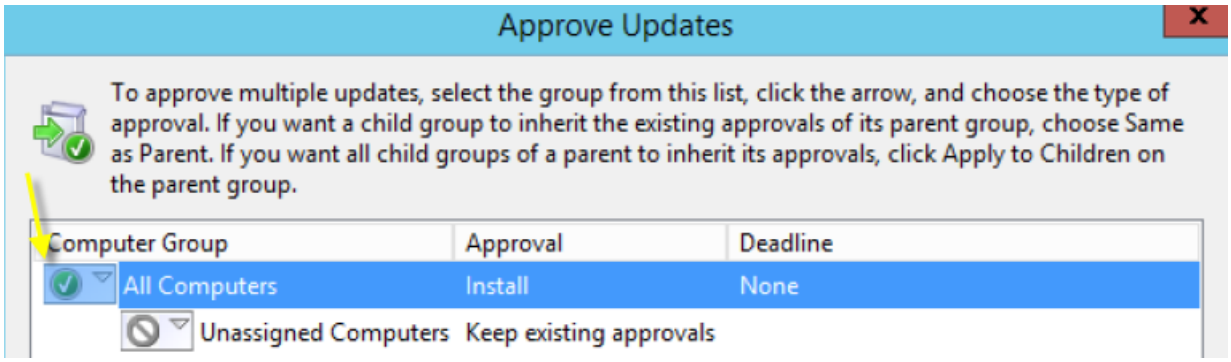

File
Action
View
Window
Help
Update Services
ELS-WSUS
Updates
Computers
Downstream Servers
Synchronizations
Reports
Options
Options
This view allows you to configure settings on your server.
Options
Update Source and Proxy Server
You can choose whether this Windows Server Update
Products and Classifications
You can specify the products for which you want upd
Update Files and Languages
You can choose whether to download update files, wh
Synchronization Schedule
You can choose to synchronize manually or set a sche
Automatic Approvals
You can specify how to automatically approve installa
Computers
You can specify how to assign computers to groups.

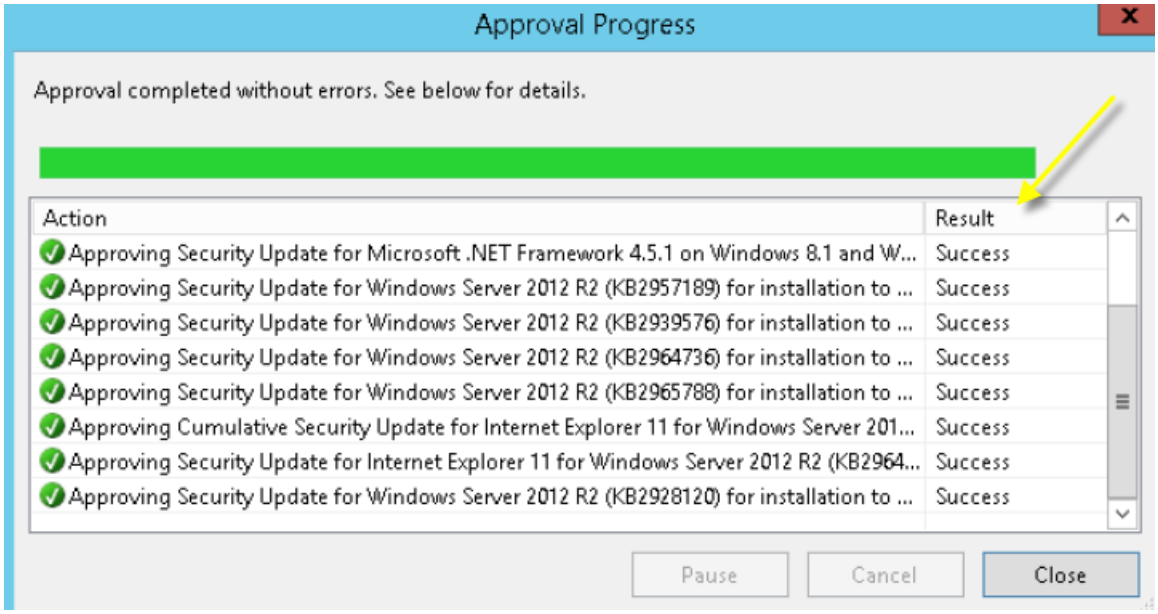




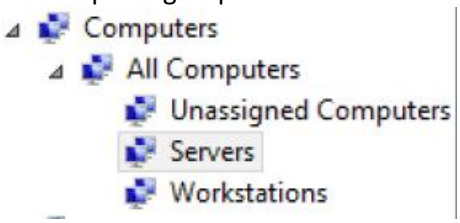
✓ I selected all updated for approval:







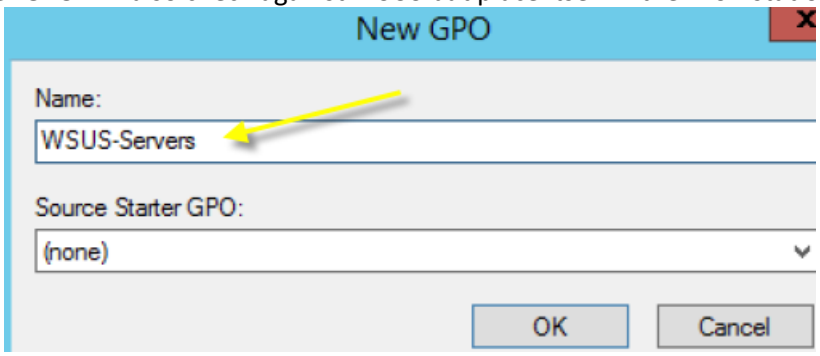
✓ Created the “Servers” & “Workstations” computer groups:

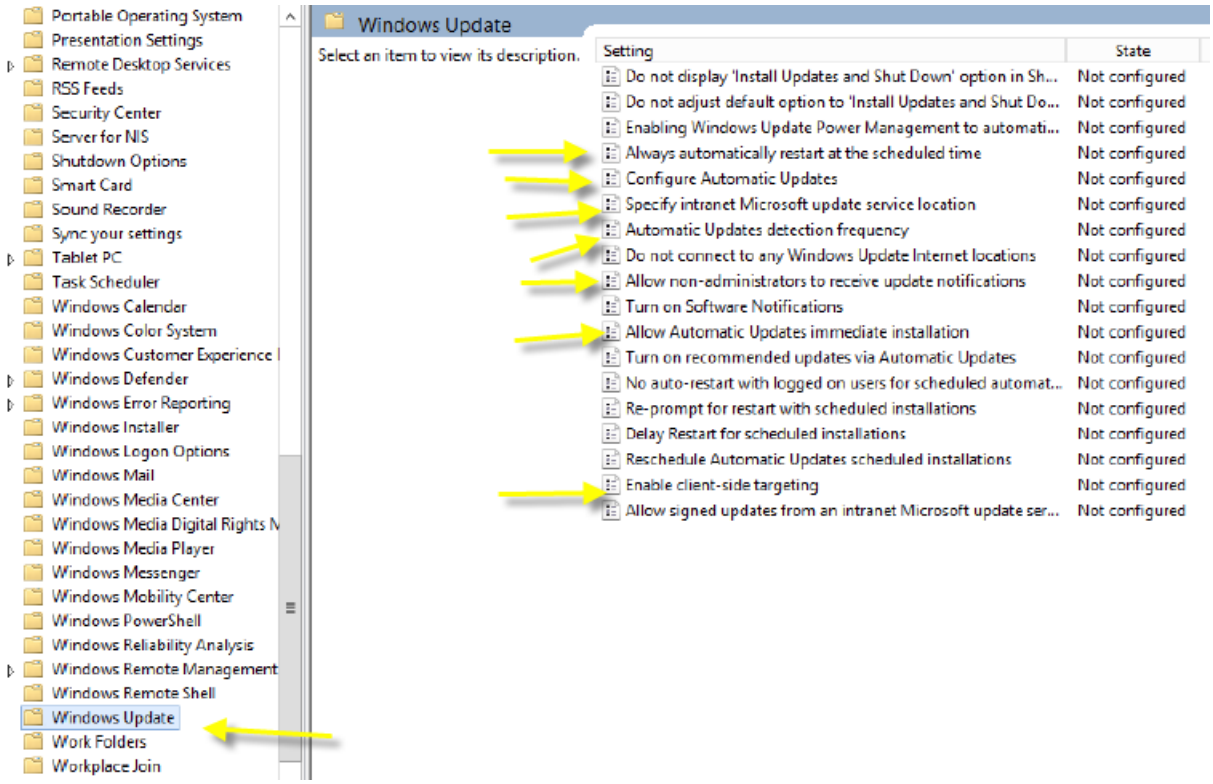


Task 2: Configure domain WSUS settings

Task 2.1: Create WSUS GPO

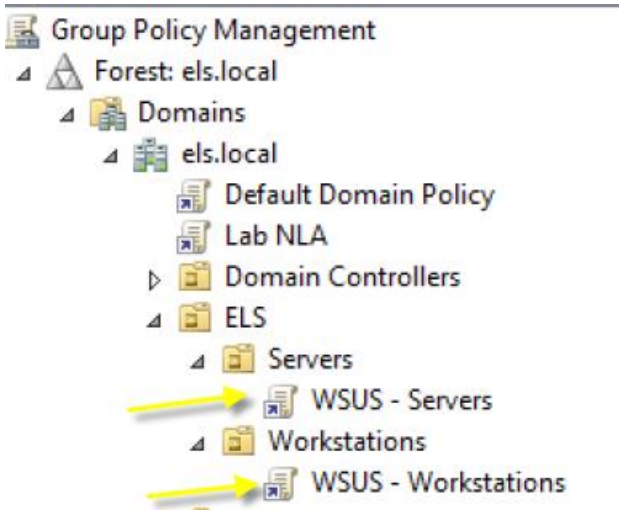
✓ Create two GPOs. One will tell the Servers OU to check against WSUS for updates and place itself in the Servers WSUS group. The other GPO will also check against WSUS but place itself in the Workstations WSUS group.





Task 2.2: Apply GPO to ELS OU

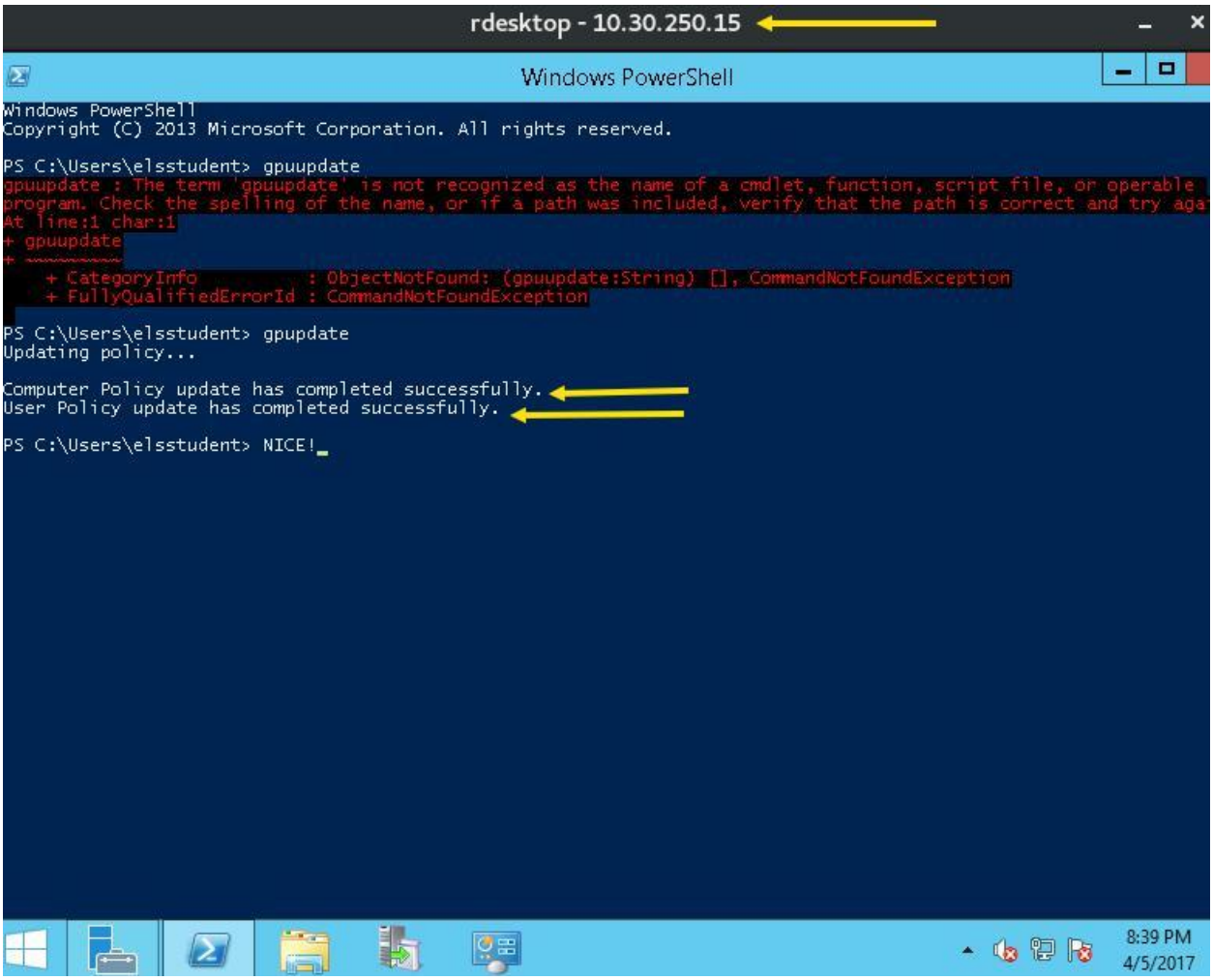
✓ Apply the WSUS-Servers GPO to the Server OU and the WSUS-Workstations GPO to the Workstations OU.



Task 3: Deploying Updates

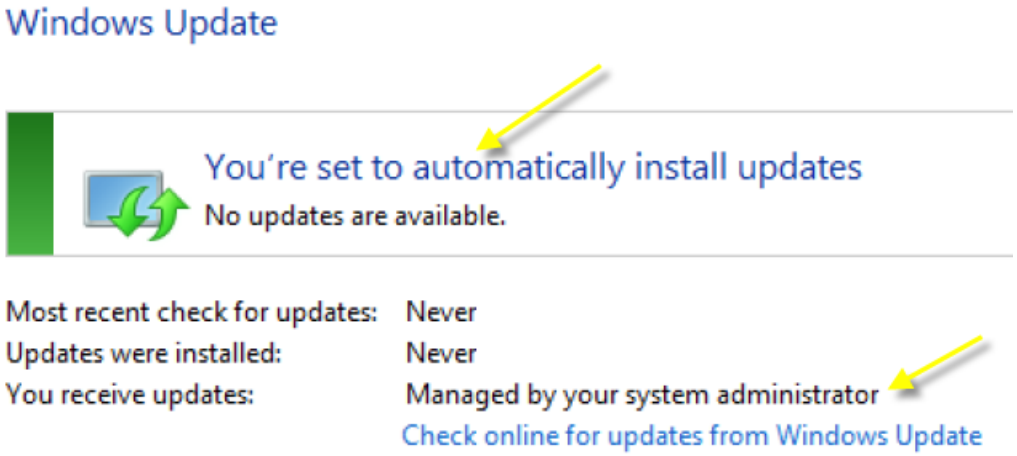
Task 3.1: Update Group Policy

✓ With the GPO applied to the OU, force an update of Group Policy on the Update Server and Windows 7 client.



Task 3.2: Check for updates against WSUS

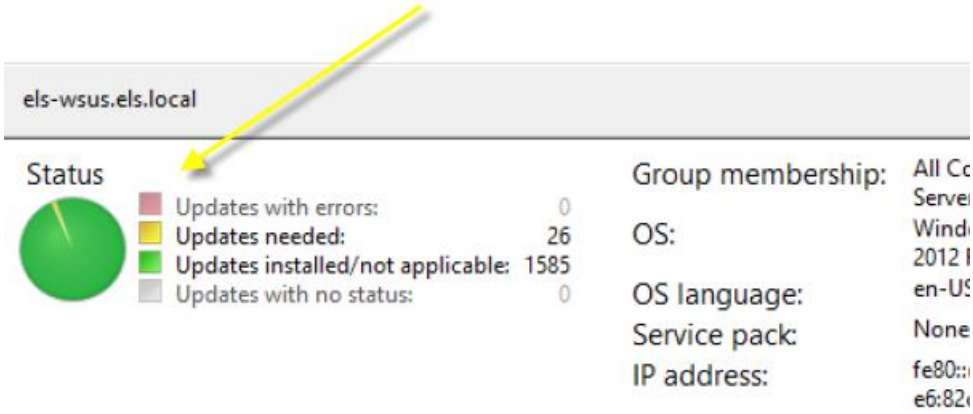
✓ Check for Windows Updates. Since the lab lacks an internet connection, if updates are shown then you know it has checked against WSUS.

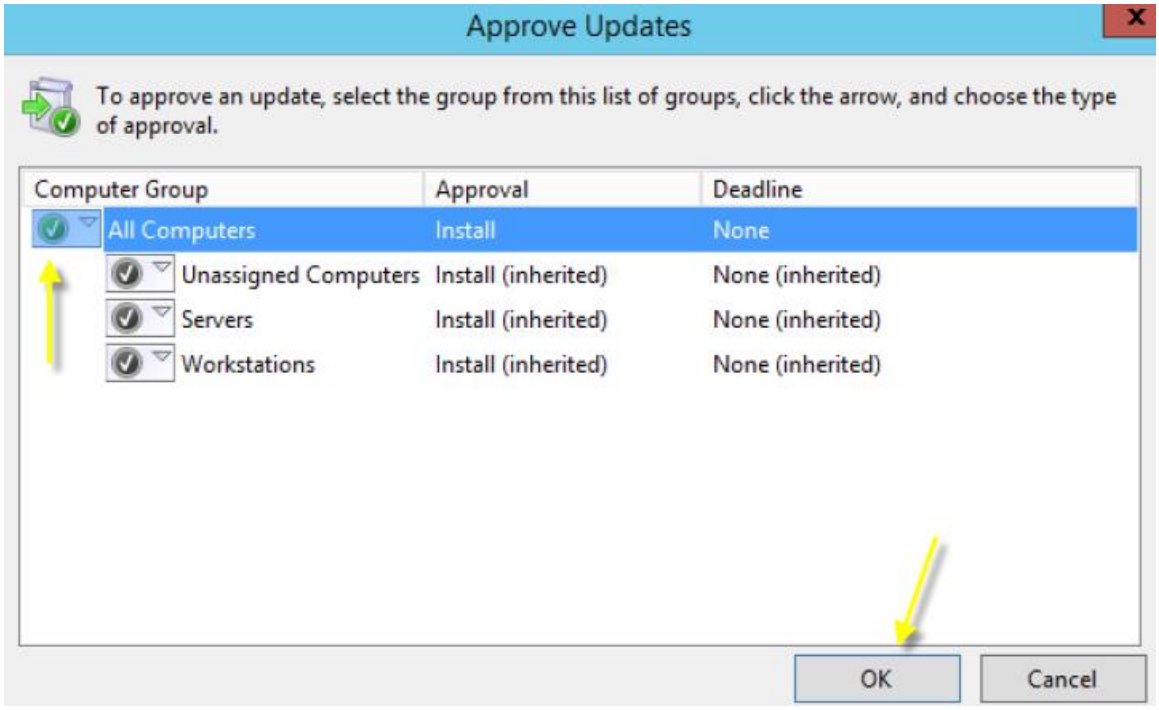


Task 3.3: Check WSUS Report

✓ Review the WSUS report to see the status of missing updates.


els-wsus.els.local
fe80::d54b:da4d:b5...
Windows Server 201...
98%


els-wsus.els.local
Status
Updates with errors: 0
Updates needed: 26
Updates installed/not applicable: 1585
Updates with no status: 0
Group membership:
OS:
OS language:
Service pack:
IP address:
None


Approve Updates
To approve an update, select the group from this list of groups, click the arrow, and choose the type of approval.
Computer Group
Approval
Deadline
All Computers
Install
None
Unassigned Computers
Install (inherited)
None (inherited)
Servers
Install (inherited)
None (inherited)
Workstations
Install (inherited)
None (inherited)
OK
Cancel

LAB 5 EMET

LAB DESCRIPTION

In the following lab, you can practice installing, deploying and controlling Microsoft EMET.

GOALS:

- Install EMET.
- Deploy EMET.
- Control EMET.
- Test EMET.

IMPORTANT NOTE

- Labs machines are not connected to the Internet, they are in a private testing environment just for you.
- The domain controller is dc1.els.local at 10.40.250.5
- The update server is at 10.40.250.15.
- The Windows 7 workstation is at 10.40.250.30.
- The WSUS role is already installed on the update server.

Task 1: Run the vulnerable application

On the desktop of els\elsstudent on the Windows 7 workstation you can find vulnecho.exe. The application is prone to a buffer overflow attack.

Task 2: Install EMET

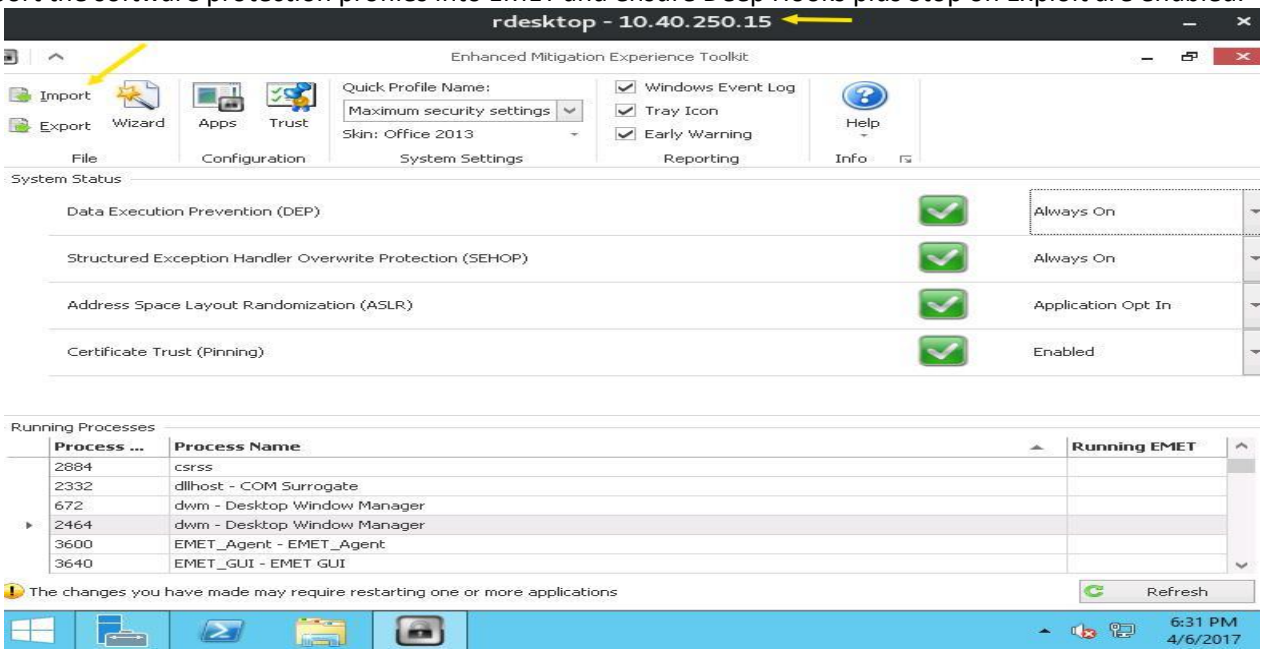
The first step of this lab is to setup EMET.

Task 2.1: Install EMET

✓ Install the application. It is located on the E: drive.

Tasks 2.2: Configure EMET

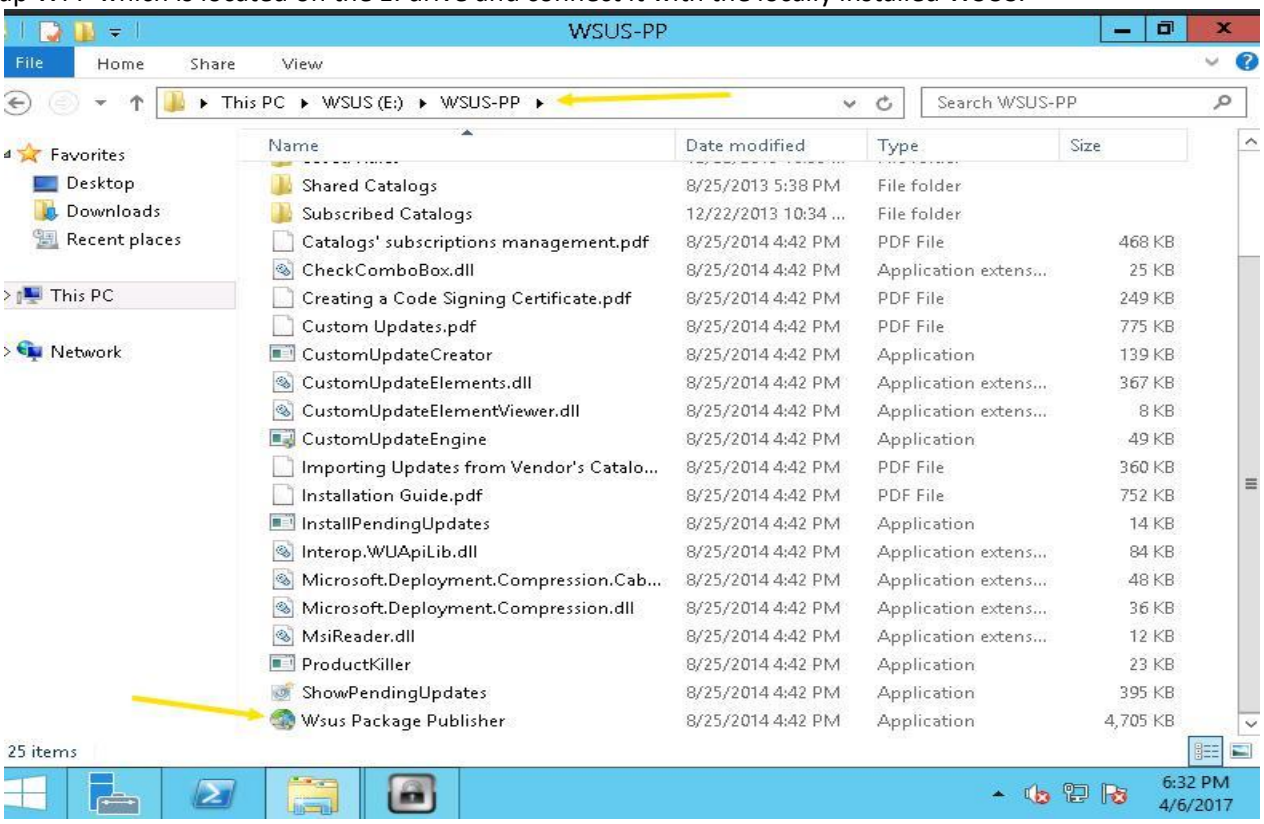
✓ Import the software protection profiles into EMET and ensure Deep Hooks plus Stop on Exploit are enabled.



Task 3: Deploy EMET

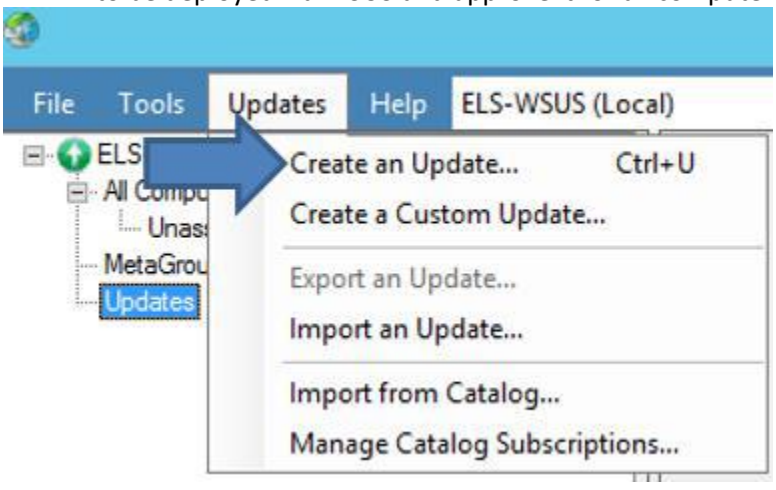
Task 3.1: Setup Windows Package Publisher

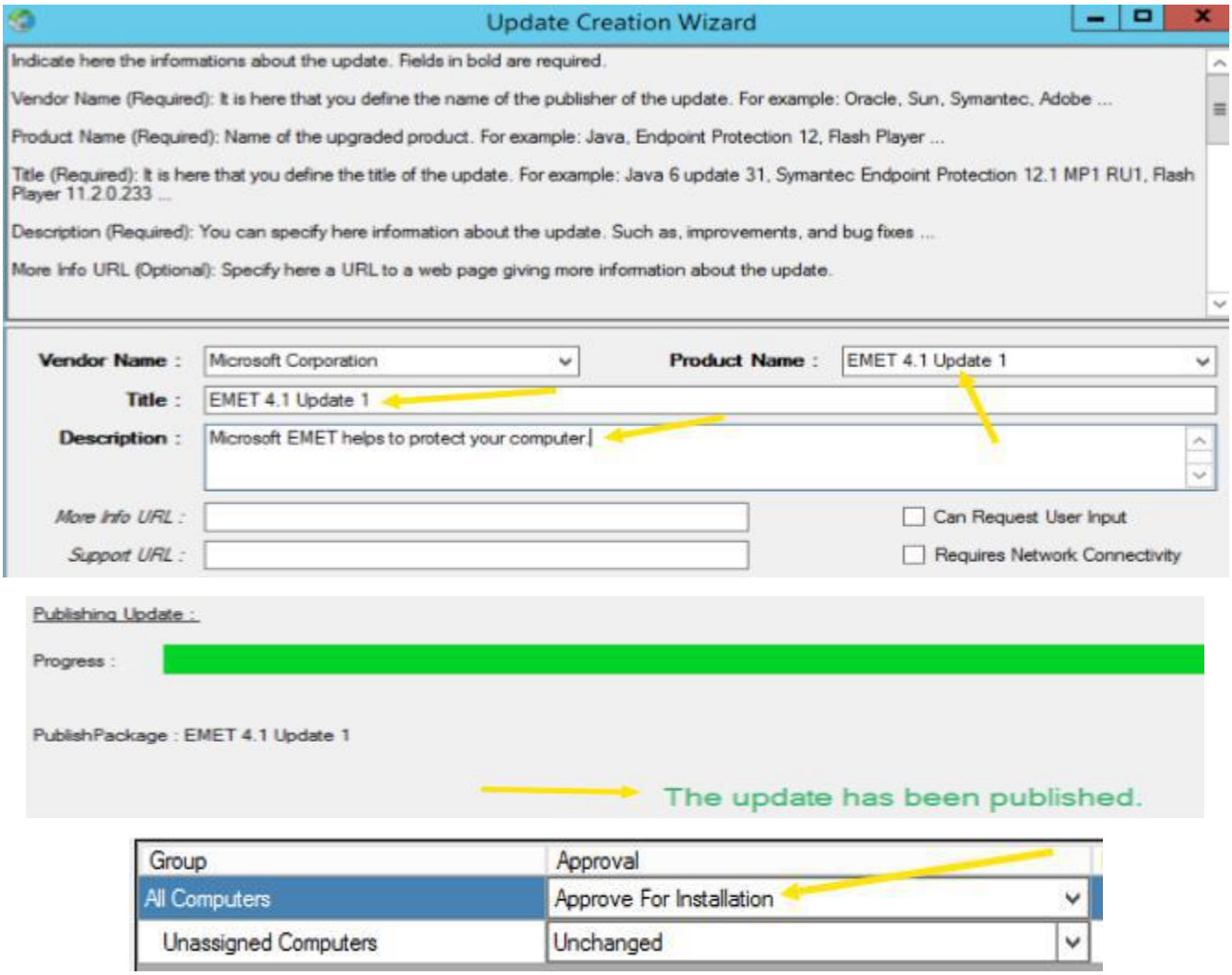
✓ Setup WPP which is located on the E: drive and connect it with the locally installed WSUS.



Task 3.2: Configure EMET deployment

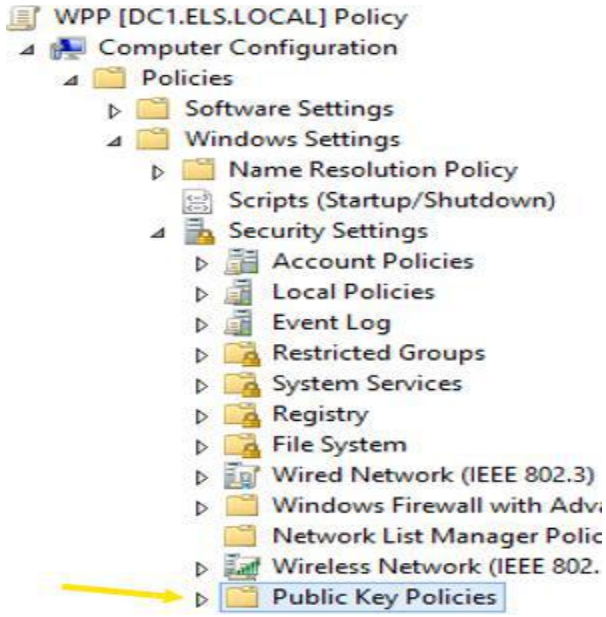
✓ Create an EMET update in WPP to be deployed via WSUS and approve it for all computer groups.

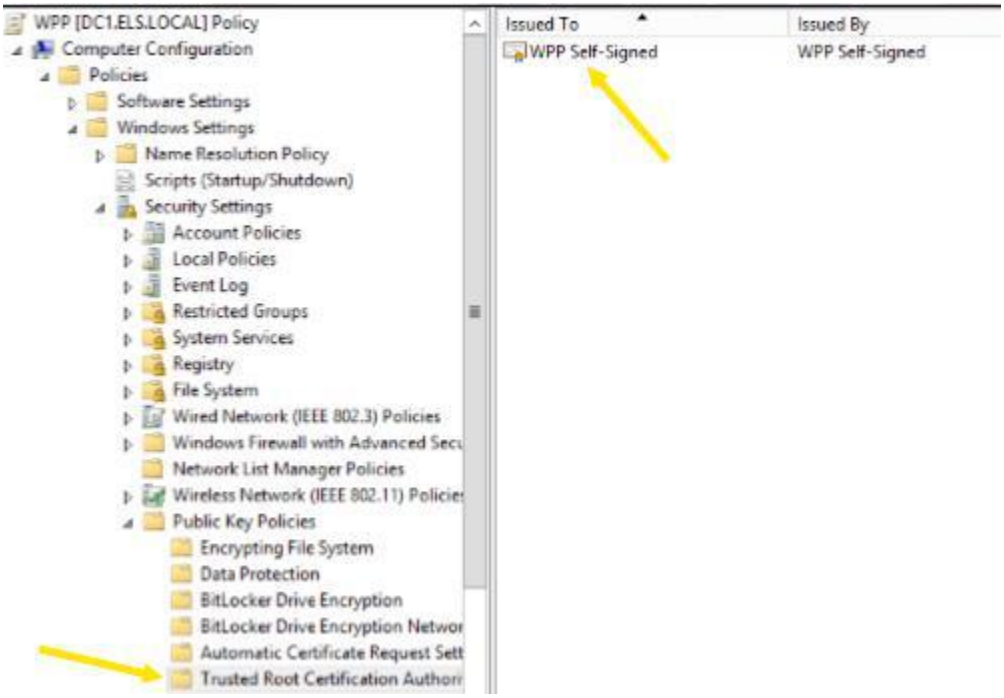


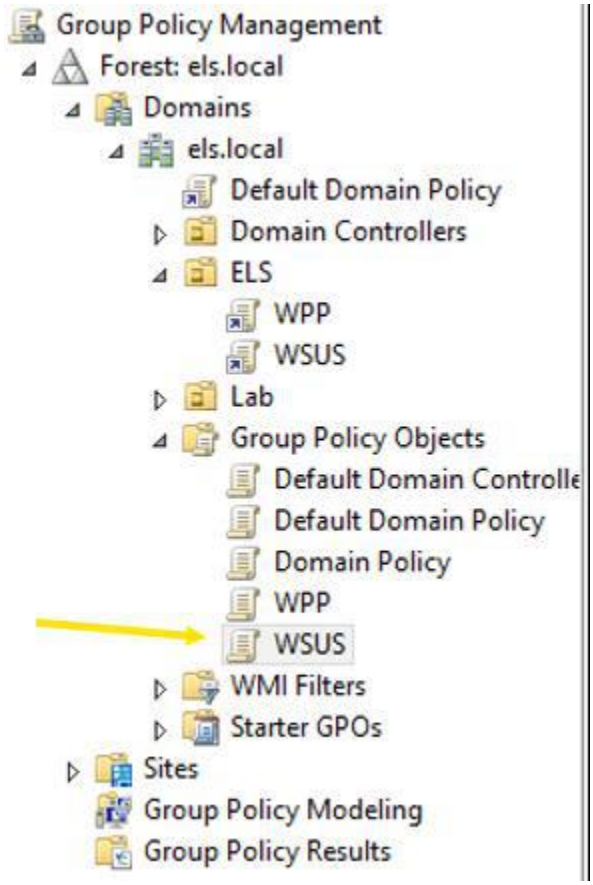


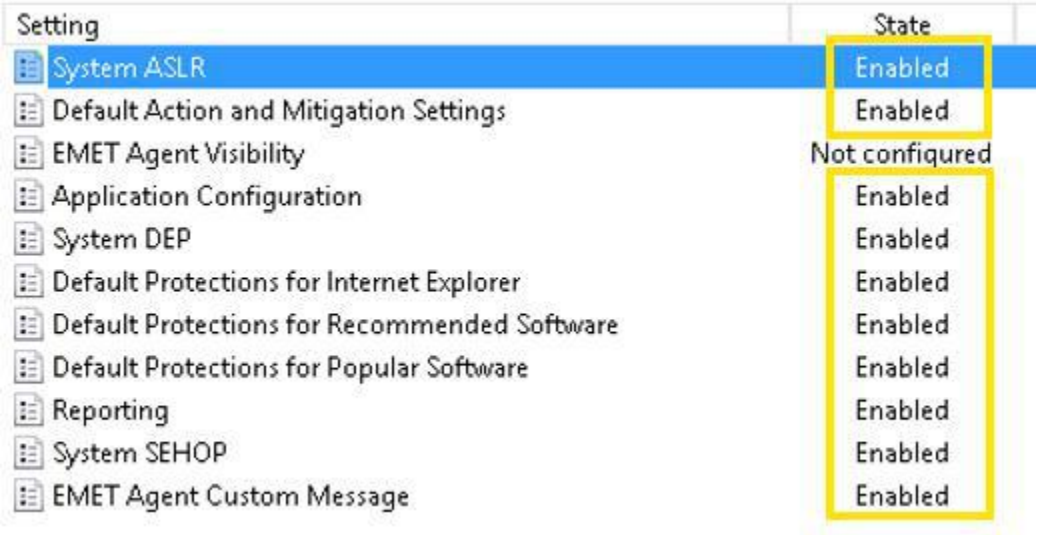
Task 3.3: Configure EMET GPO

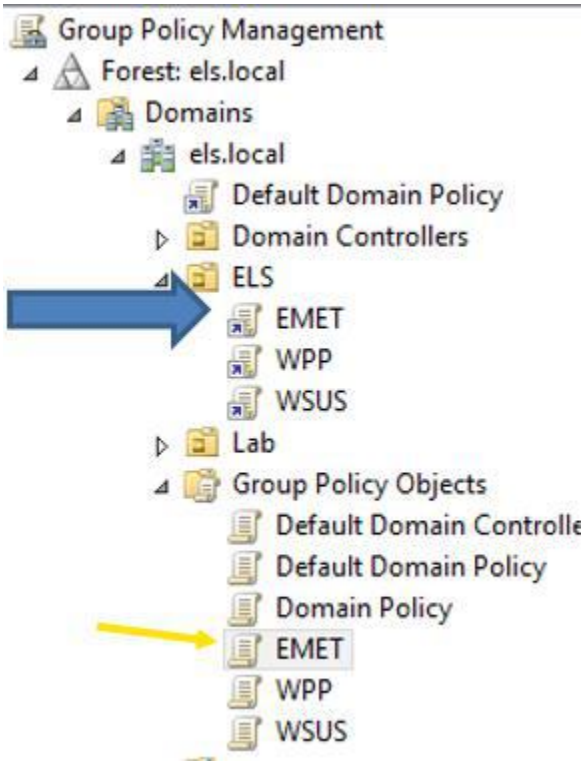
✓ Copy the Group Policy files from the Update Server to DC1 and import them into Group Policy. Create an EMET GPO and apply it to the ELS OU.




WPP [DC1.ELS.LOCAL] Policy
Computer Configuration
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) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Policie
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Networ
Automatic Certificate Request Sett
Trusted Root Certification Authori
Issued To
Issued By
WPP Self-Signed
WPP Self-Signed


Group Policy Management
Forest: els.local
Domains
els.local
Default Domain Policy
Domain Controllers
ELS
WPP
WSUS
Lab
Group Policy Objects
Default Domain Controlle
Default Domain Policy
Domain Policy
WPP
WSUS
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results

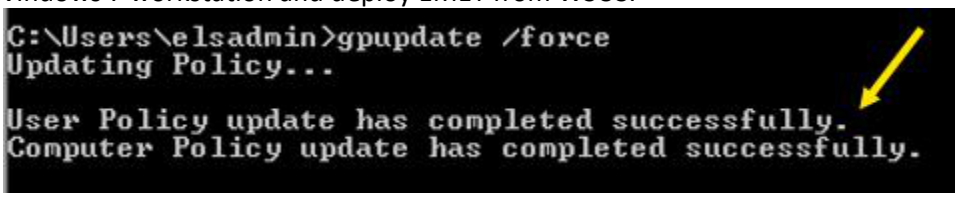


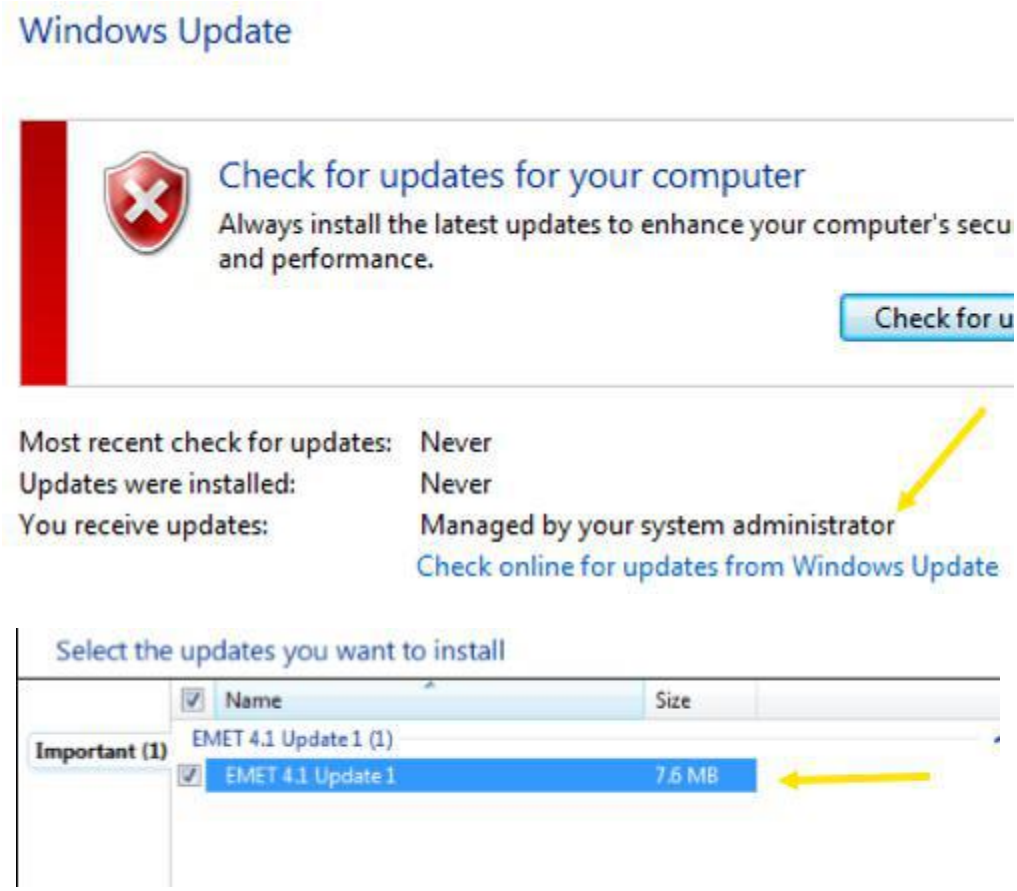


Task 4: Deployment

Task 4.1: Workstation Install

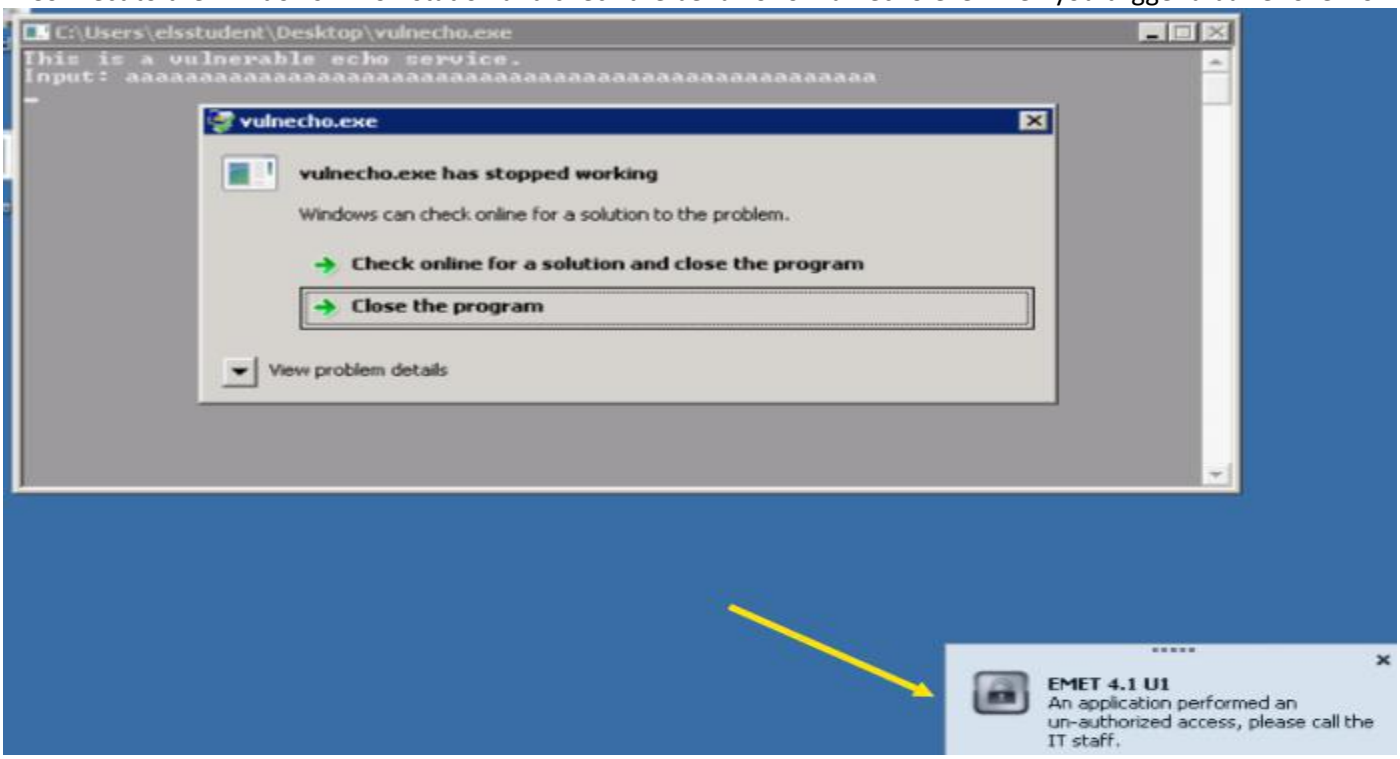
✓ Connect to the Windows 7 workstation and deploy EMET from WSUS.





Task 4.2: Test EMET

✓ Connect to the Windows 7 workstation and check the behavior of vulnecho.exe when you trigger a buffer overflow.



LAB 6 GROUP POLICY

LAB DESCRIPTION

In the following lab, you can practice setting up different Group Policy Objects and applying them.

GOALS:

- Setup multiple GPOs
- Apply them with correct ordering

IMPORTANT NOTE:

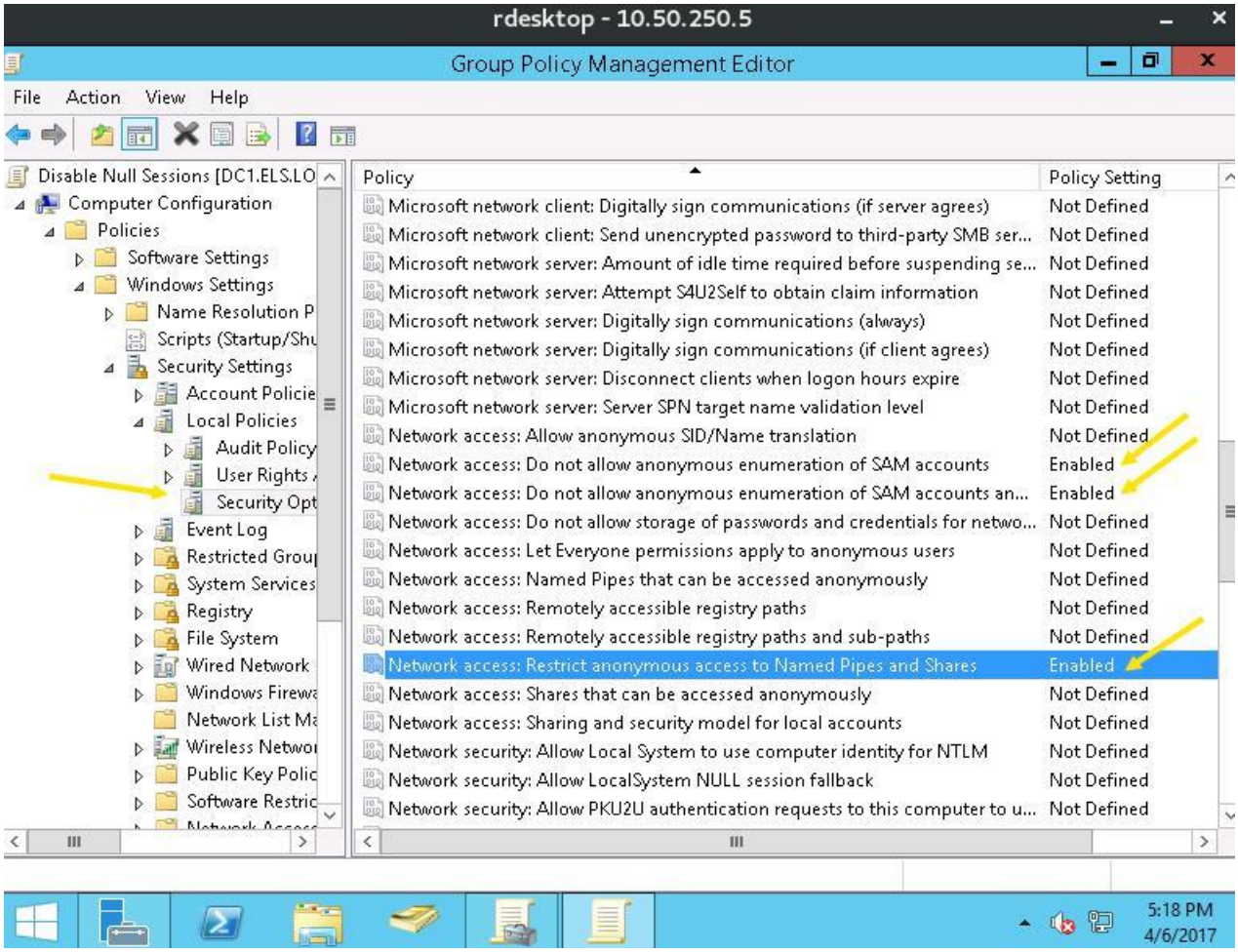
- Labs machines are not connected to the Internet, they are in a private testing environment just for you.
- The domain controller is dc1.els.local at 10.50.250.5
- One Windows 7 machine (Exec-1) is at 10.50.250.20.
- Another Windows 7 machine (EndUser) is at 10.50.250.25.

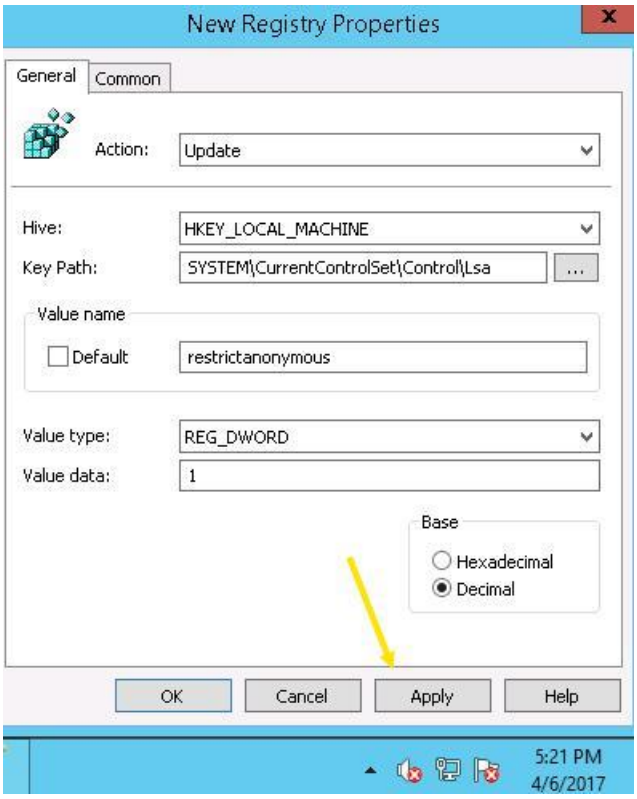
Task 1: Create the needed GPOs

The first step of this lab is to setup the GPOs as described. Each task should have its own GPO created; do not combine them all into one GPO.

Task 1.1: Null sessions

✓ Create a GPO which disables null sessions.





Task 1.2: RDP Timeout – 30 minutes

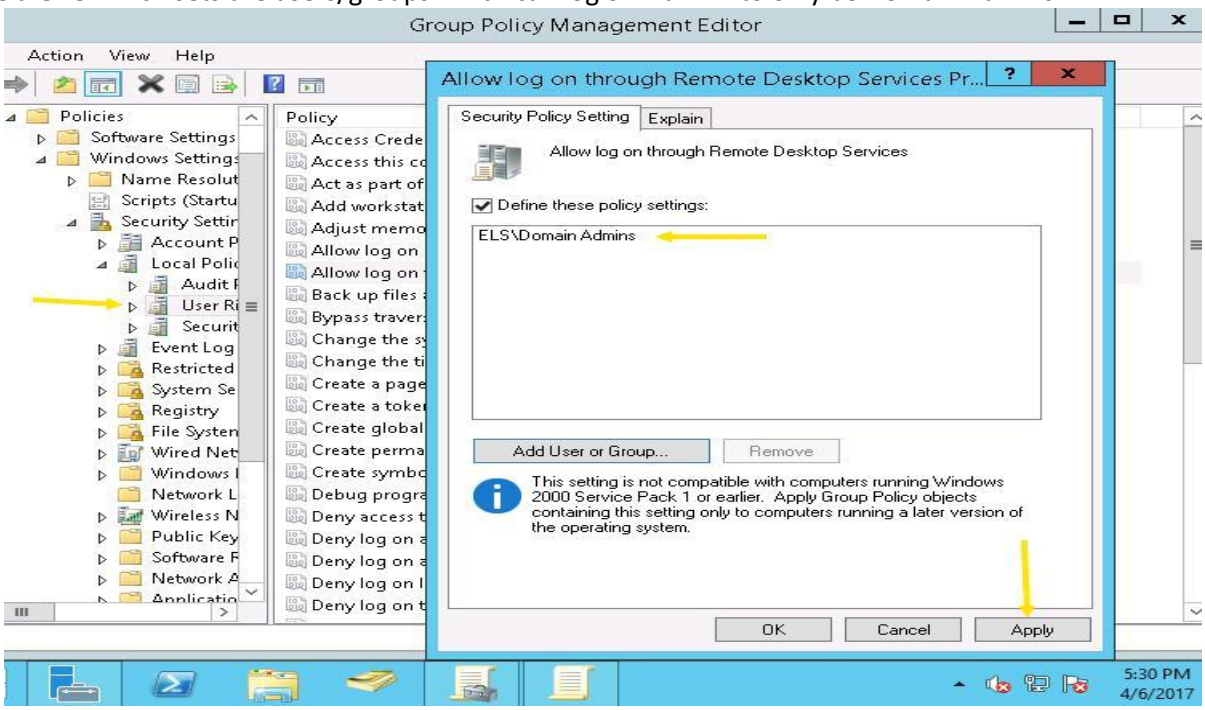
✓ Create a GPO which ends all inactive and disconnected RDP sessions after **30 minutes**. Set it to terminate the session once the timeout has been reached. Also set the **RDP encryption** level to **HIGH**.

Task 1.3: RDP Timeout – 60 minutes

✓ Create a GPO which ends all inactive and disconnected RDP sessions after **60 minutes**. Set it to terminate the session once the timeout has been reached.

Task 1.4: RDP Users – Domain Admins

✓ Create a GPO which sets the users/groups which can log on via RDP to only be Domain Admins.



Task 1.5: RDP Users – PC Support

✓ Create a GPO which sets the users/groups which can log on via RDP to be Domain Admins and PC Support.

Task 2: Apply the GPOs

Task 2.1: Null Sessions

✓ Apply the null sessions GPO so that ALL devices in the domain will receive and process it.

Task 2.2: RDP Timeout

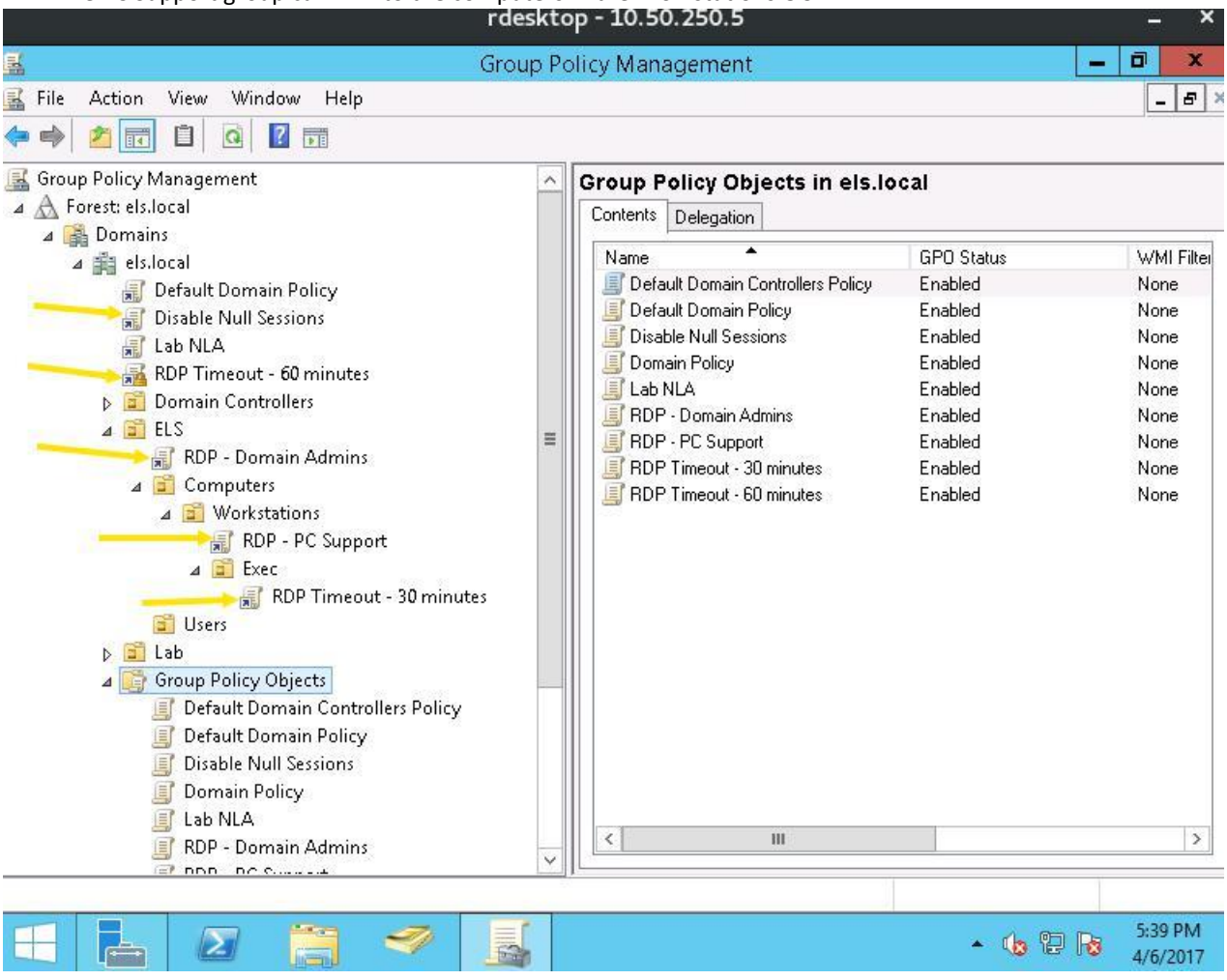
✓ Apply the two RDP configurations (A and B) GPOs to:

- Set the connection timeout for all the computers in the ELS domain to 60 minutes
- Enforces the RDP encryption level to HIGH on the exec workstations
- Try to do this in the least number of steps as possible.

Task 2.3: RDP Users

✓ Apply the RDP users GPOs, per the following objectives:

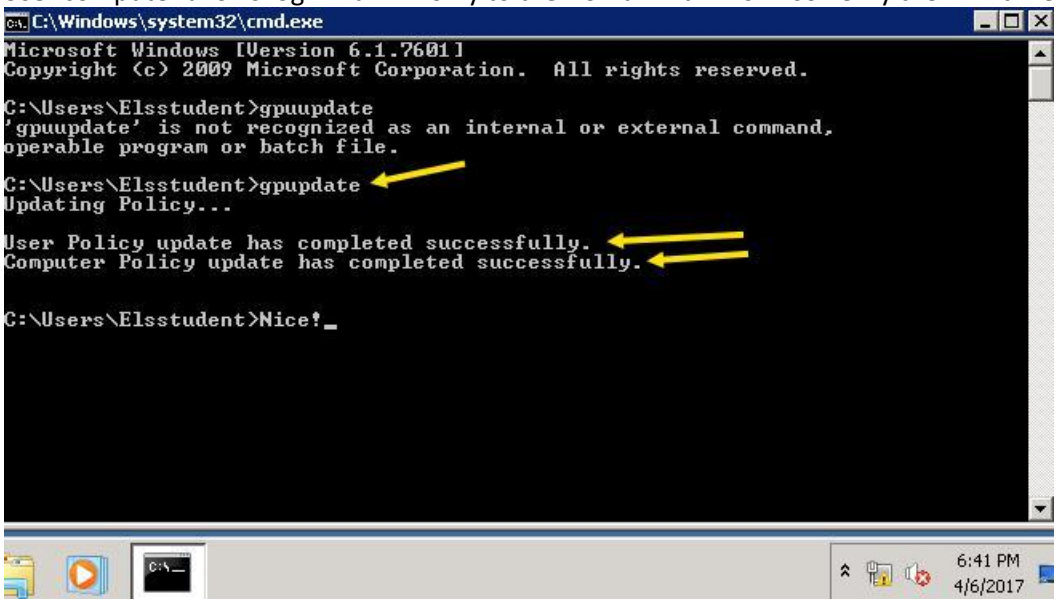
- The Domain Admins can connect via RDP to all computers in the domain
- The PC Support group can RDP to the computers in the Workstations OU

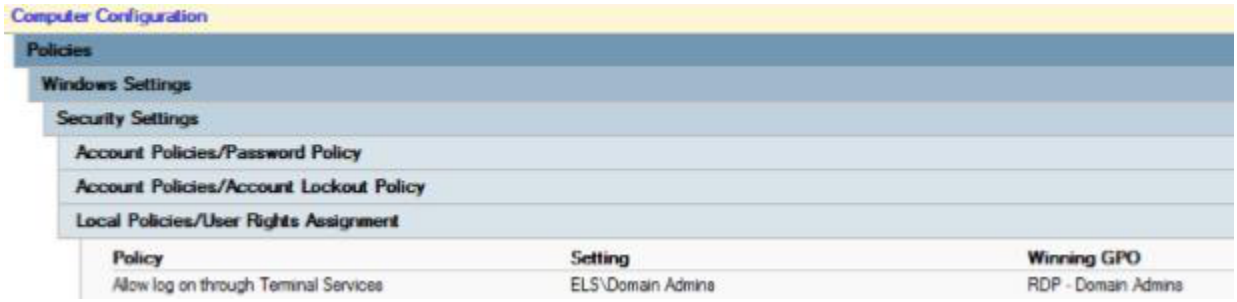


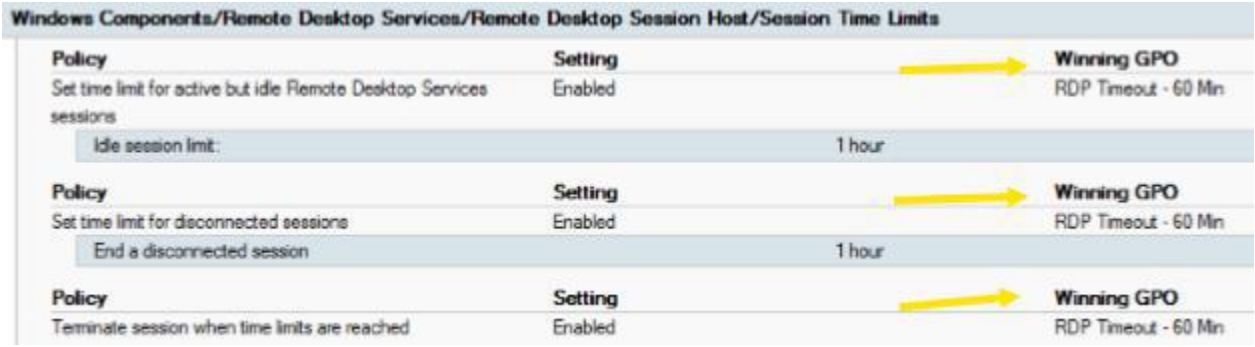
Task 3: Test GPO settings

Task 3.1: Check EndUser Computer

✓ Verify the EndUser computer allows login via RDP only to the Domain Admins. Also verify the RDP timeout settings.

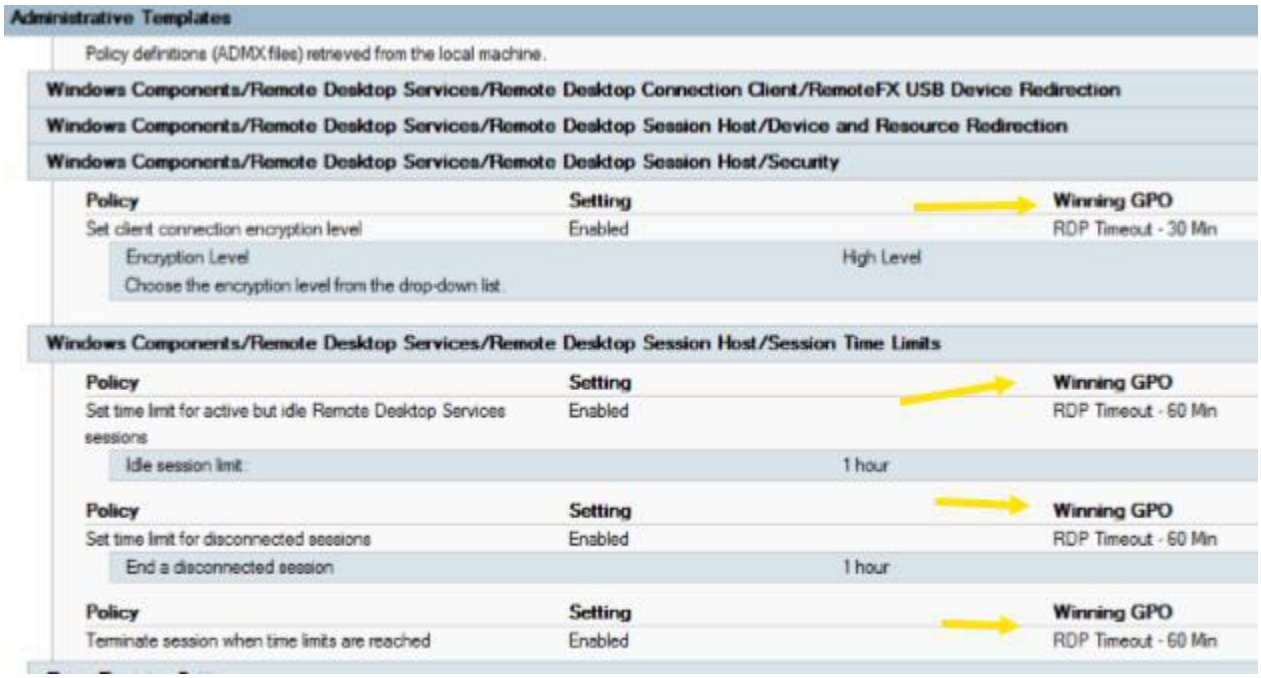


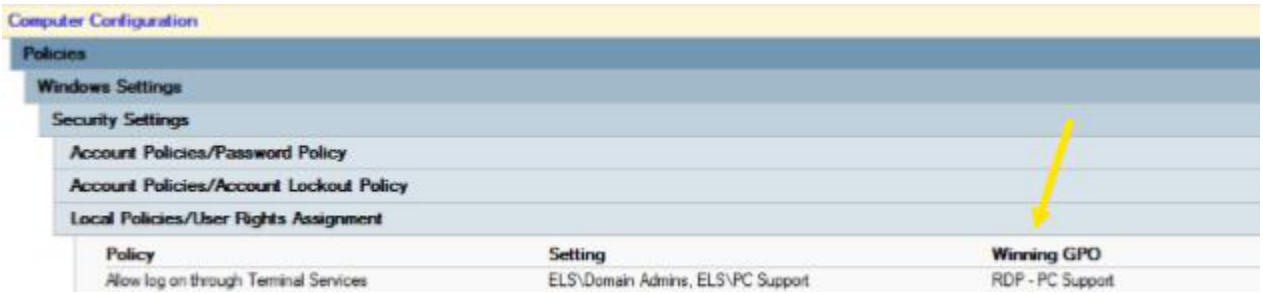




Task 3.2: Check EXEC-1 Computer

✓ Verify the EXEC-1 computer allows login via RDP to the Domain Admins and the PC Support members. Also verify the RDP encryption level is set to high and the RDP timeout settings are 60 minutes.


Administrative Templates
Policy definitions (ADMX files) retrieved from the local machine.
Windows Components/Remote Desktop Services/Remote Desktop Connection Client/RemoteFX USB Device Redirection
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Device and Resource Redirection
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security
Policy
Setting
Winning GPO
Set client connection encryption level
Enabled
RDP Timeout - 30 Min
Encryption Level
High Level
Choose the encryption level from the drop-down list.
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits
Policy
Setting
Winning GPO
Set time limit for active but idle Remote Desktop Services sessions
Enabled
RDP Timeout - 60 Min
Idle session limit:
1 hour
Policy
Setting
Winning GPO
Set time limit for disconnected sessions
Enabled
RDP Timeout - 60 Min
End a disconnected session
1 hour
Policy
Setting
Winning GPO
Terminate session when time limits are reached
Enabled
RDP Timeout - 60 Min


Computer Configuration
Policies
Windows Settings
Security Settings
Account Policies/Password Policy
Account Policies/Account Lockout Policy
Local Policies/User Rights Assignment
Policy
Setting
Winning GPO
Allow log on through Terminal Services
ELS\Domain Admins, ELS\PC Support
RDP - PC Support

LAB 7 ENDPOINT SECURITY

LAB DESCRIPTION

In the following lab, you can practice hardening a Windows client to protect it from malware, attack and end-user misuse.

GOALS:

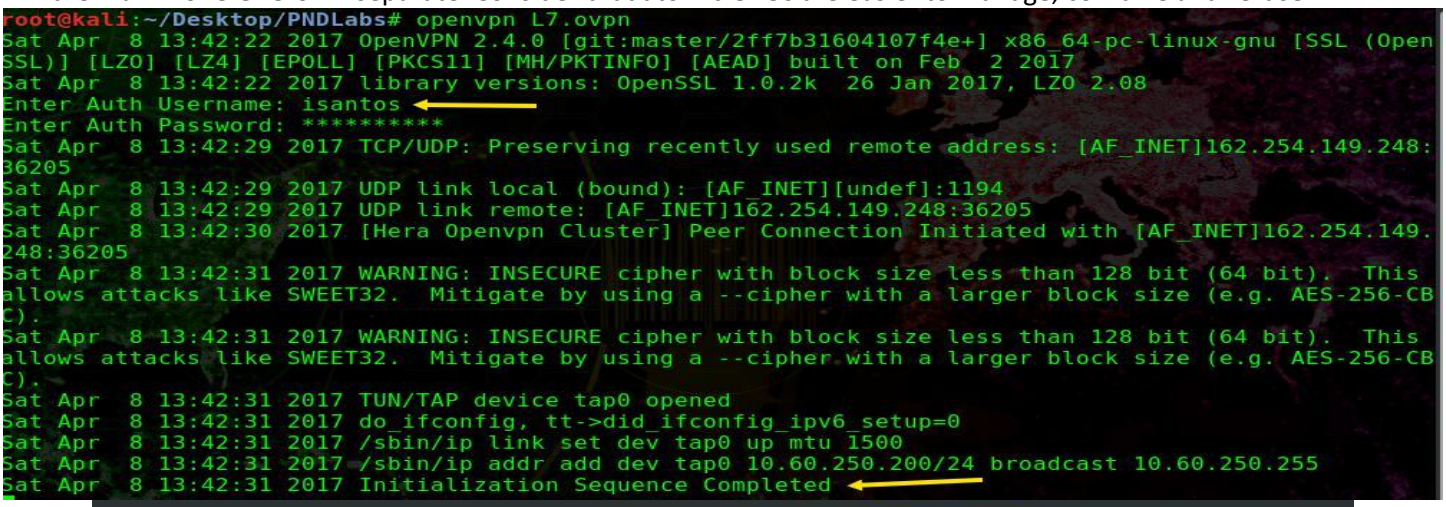
- Harden the workstation using computer policies
- Restrict user activity using user policies

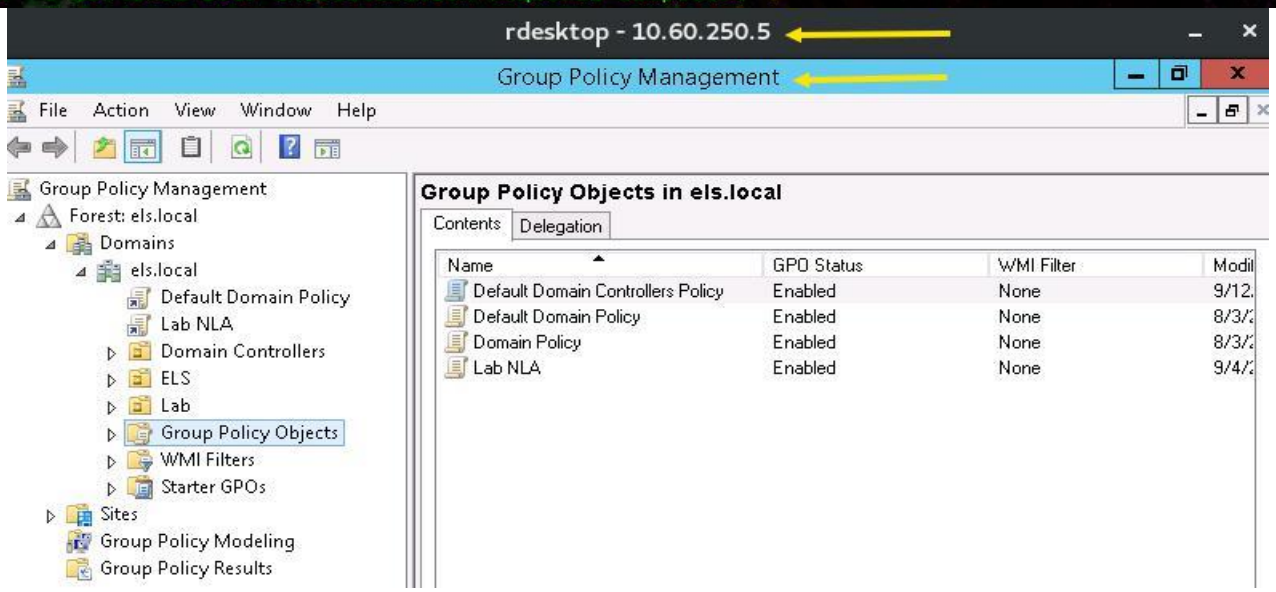
IMPORTANT NOTE:

- Labs machines are not connected to the Internet.
- The domain controller is dc1.els.local at 10.60.250.5
- The Windows 7 workstation is at 10.60.250.20
- Server01 is at 10.60.250.25.

Task 1: Workstation Policies

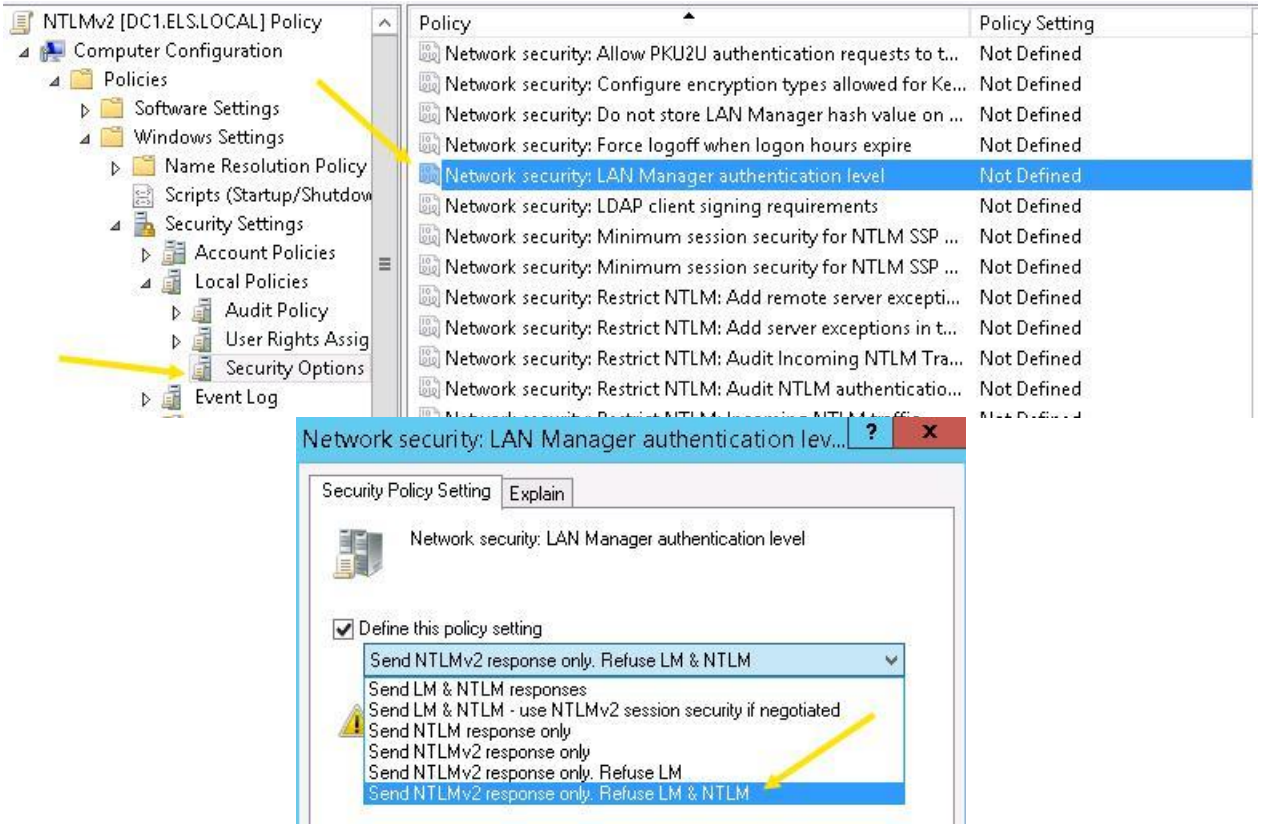
✓ The first step of this lab is to setup workstation policies to harden the endpoint. For these policies, you can place them all in one GPO or in separate. Consider that atomic GPOs are easier to manage, combine and re-use.





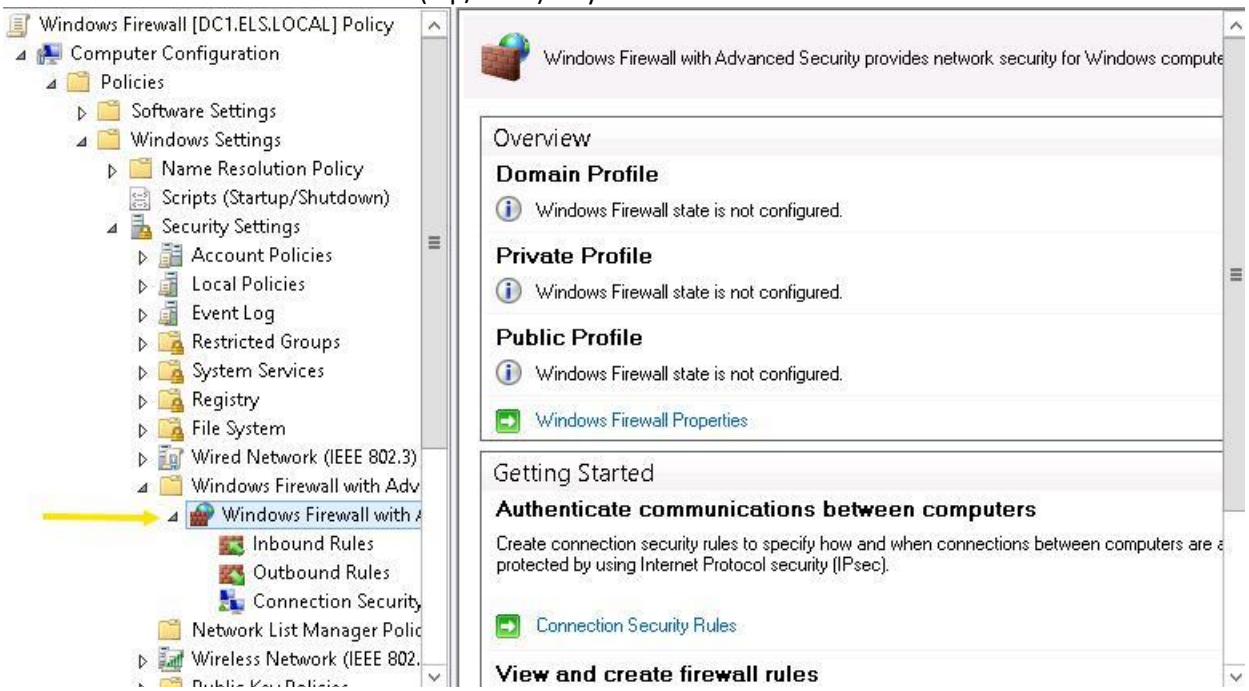
Task 1.1: NTLMv2

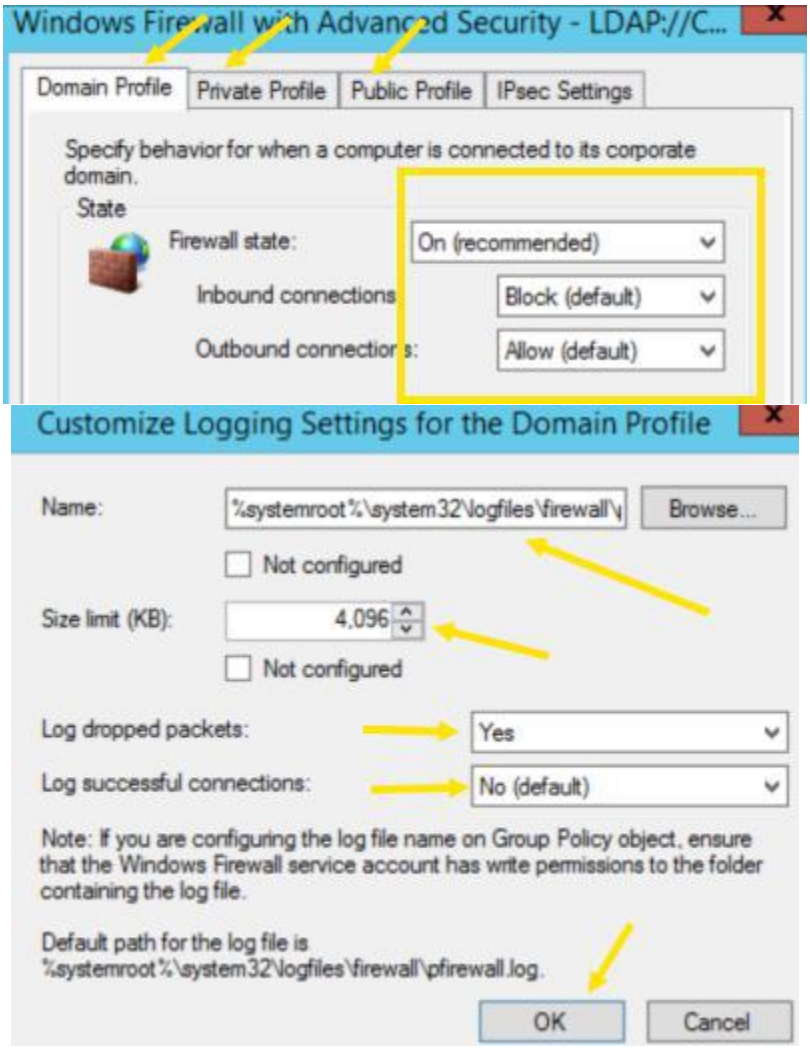
✓ Create a policy that enforces NTLMv2 and rejects LM authentication.



Task 1.2: Windows Firewall

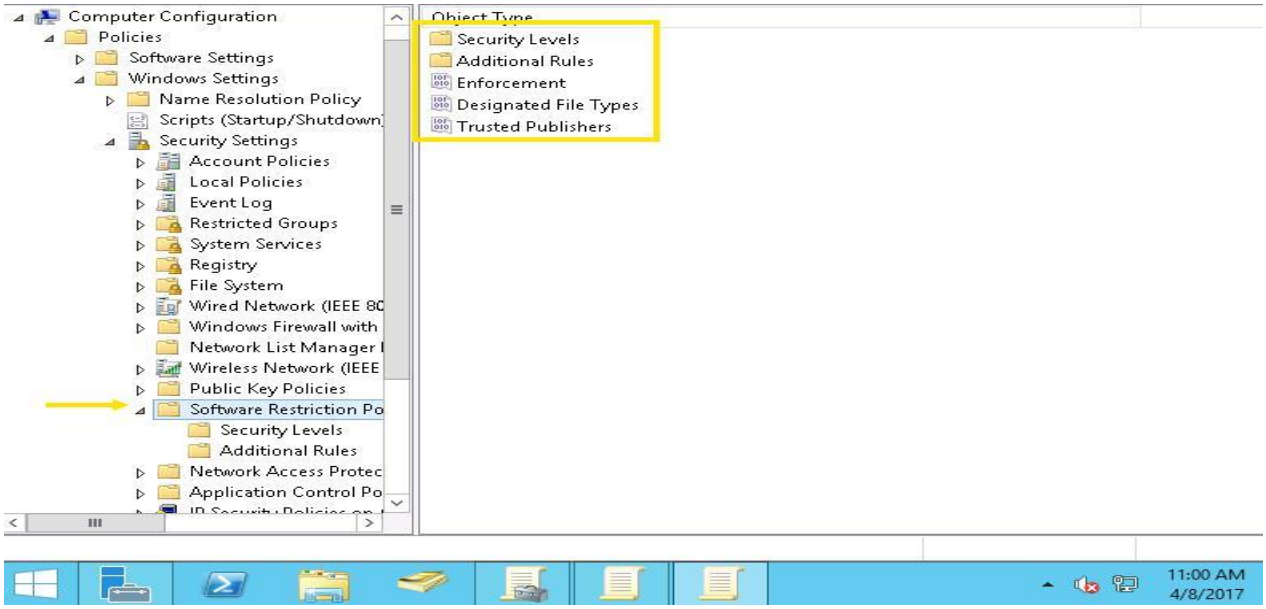
✓ Create a policy which forces the Windows Firewall to stay enabled for all network profiles. Make sure you also create a firewall rule which allows RPD (tcp/3389) so you can connect to the workstation later.

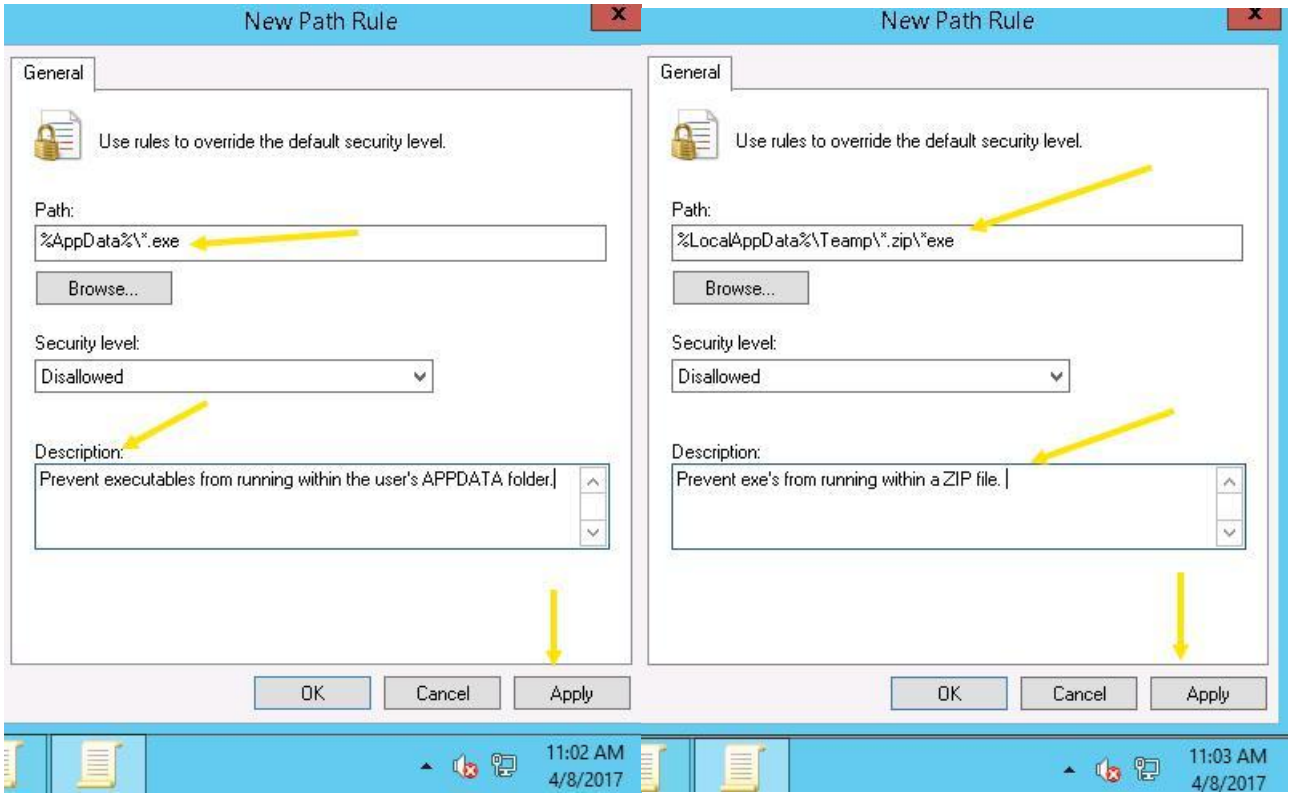




Task 1.3: Software Restrictions

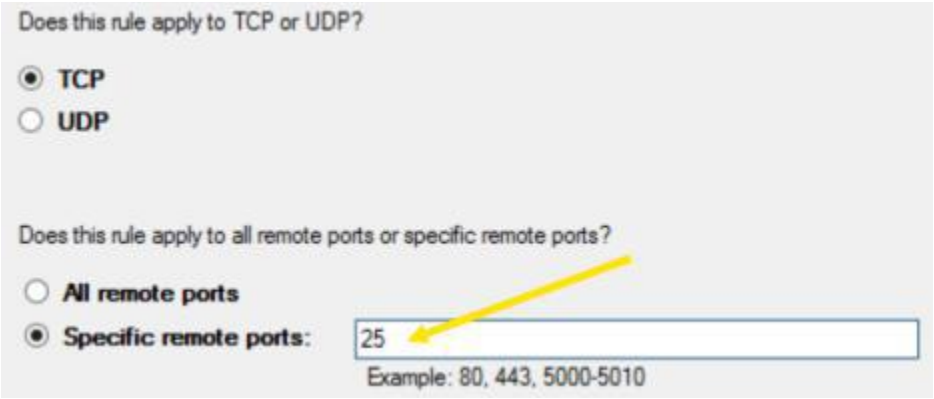
✓ Assume you have learned many recent strains of malware infect systems by running an executable from the APPDATA folder. Create a policy which blocks this execution. Also, block .exe files from being run from inside a .zip file within the APPDATA folder.





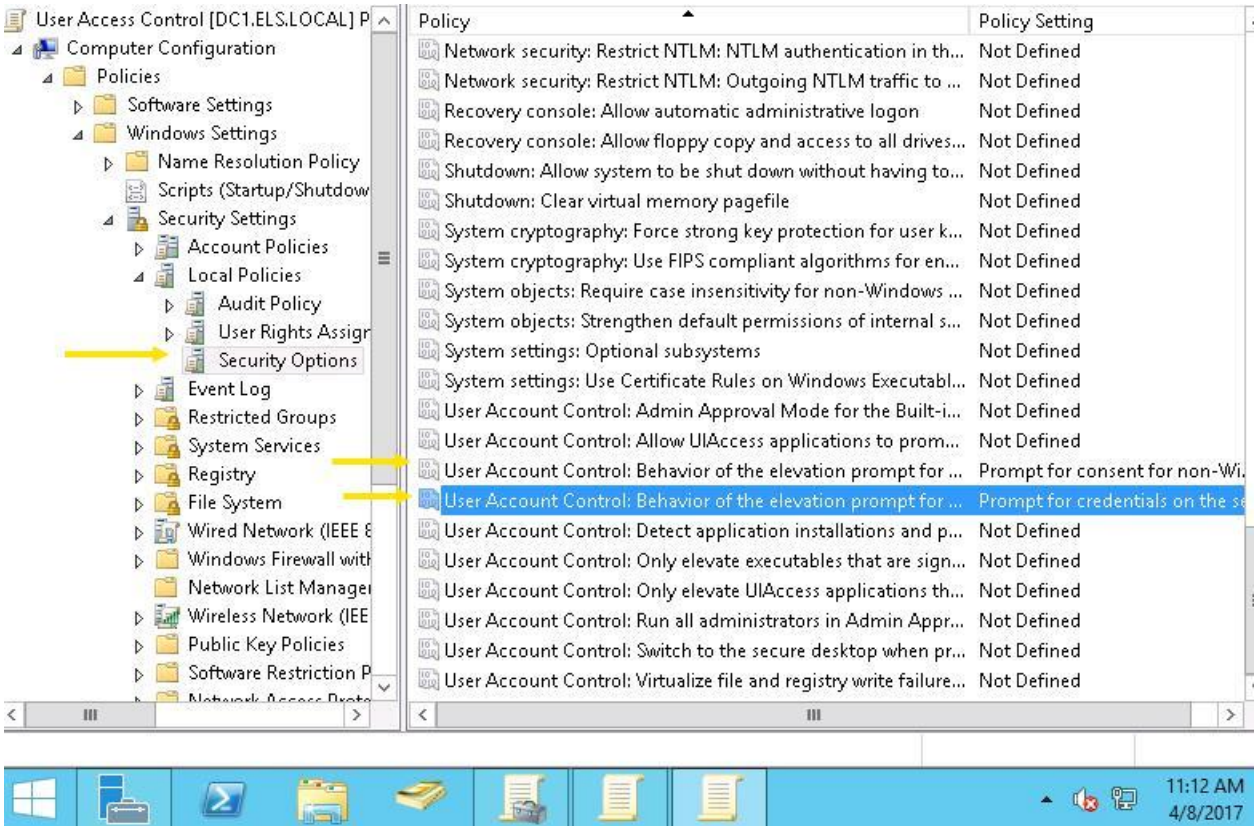
Task 1.4: Trojan Spam

✓ Assume the network hosts an email server and your public IP has been blacklisted due to an internal workstation being infected and sending out a ton of spam. You have remediated the workstation and created a new rule in the perimeter firewall to block this traffic. For good measure, create a policy which blocks outbound port 25 access via Windows Firewall.



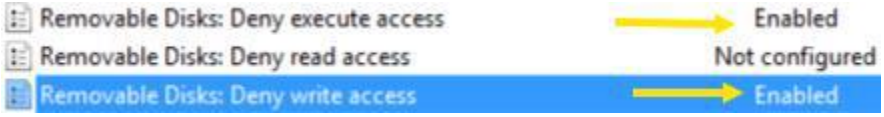
Task 1.5: User Access Control

Assume you have discovered some of the helpdesk analysts have disabled UAC while troubleshooting workstation but neglected to re-enable it. To counter this, create a policy which enforces UAC and the secure desktop.



Task 1.6: Removable Media

Create a policy which allows users to read from removable storage but cannot write to or execute from them.



Task 1.7: Test Settings before Chance

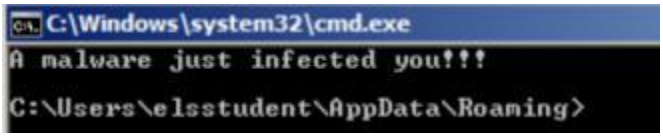
✓ Login to the Windows 7 workstation (10.60.250.20) and test:

- Can you disable UAC?
- Try to telnet to Server01 (10.60.250.5) on port 25. What happens?
- What happens when you try to run the sample malware executable in the %AppData% directory? Note: the sample malware is harmless, but has been written to be detectable by nearly every antivirus.

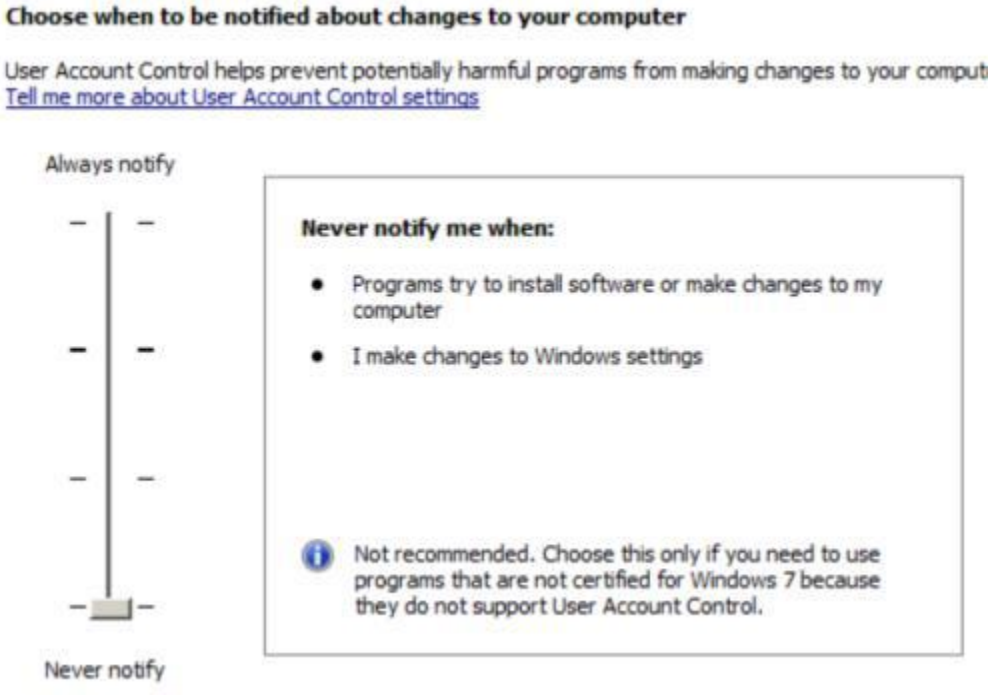
We can edit the firewall state:

Telnet is enabled:

The Malware file is able to run via the %APPDATA% search:

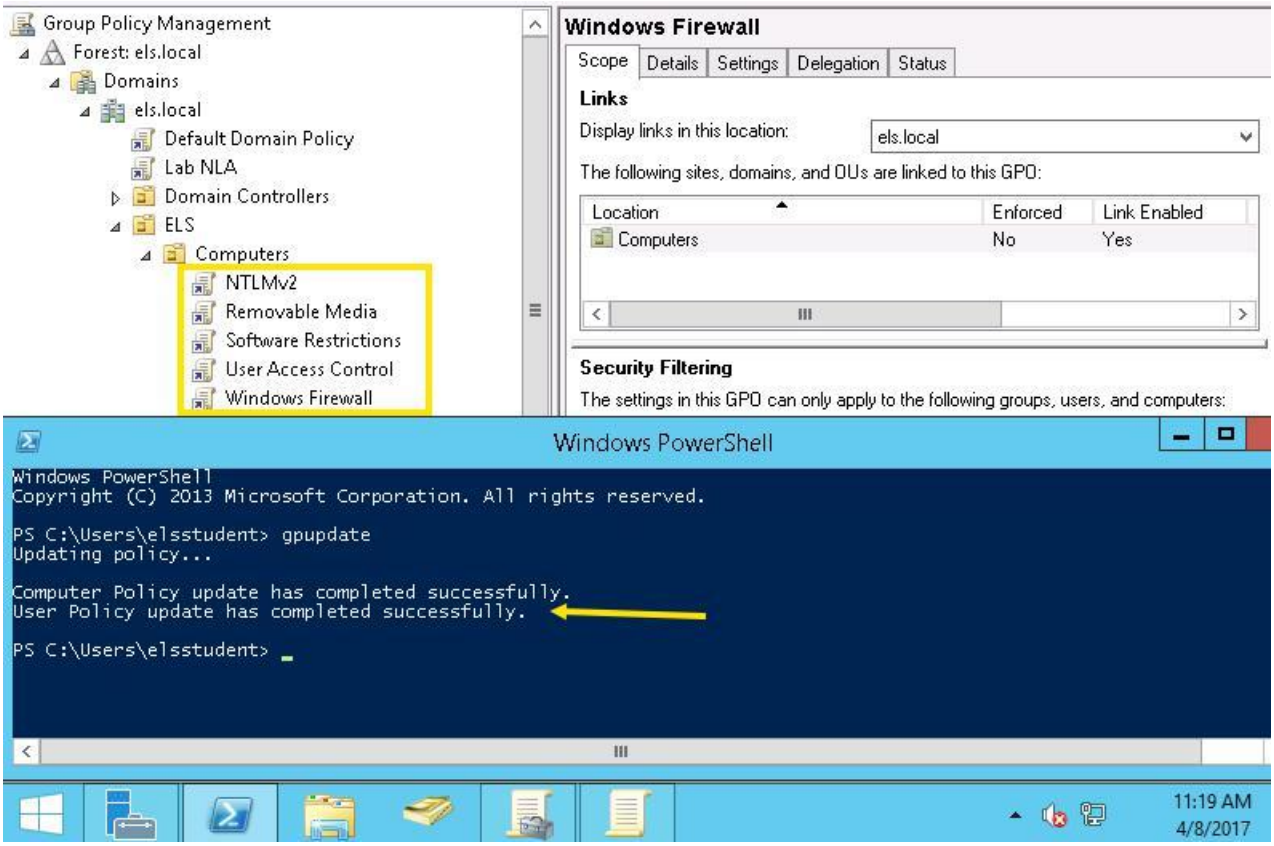


We are able to disable UAC:

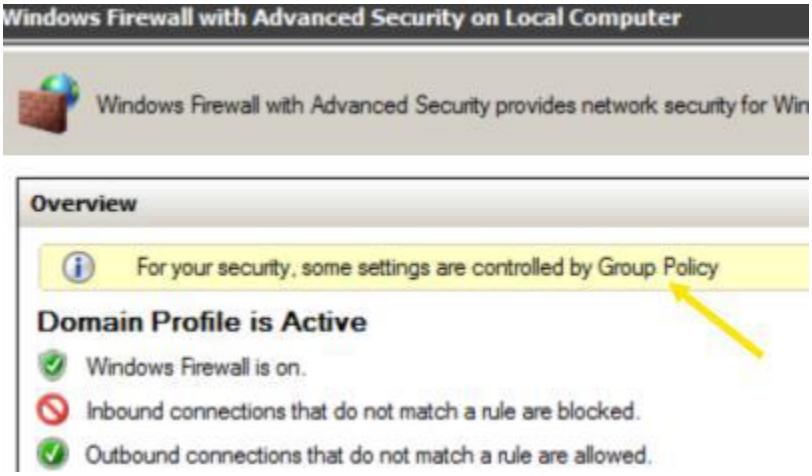


Task 1.8: Apply GPO and Test

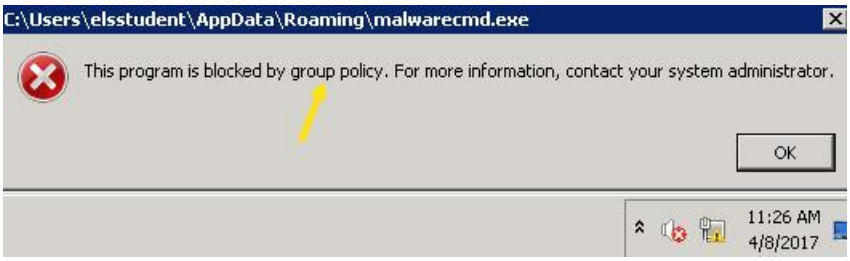
✓ Apply this GPO to the ELS > Computers OU. Login to the Windows 7 workstation via RDP and test the settings after running gpupdate. Try to do the same actions of Task 1.7 and verify the behavior of the machine.



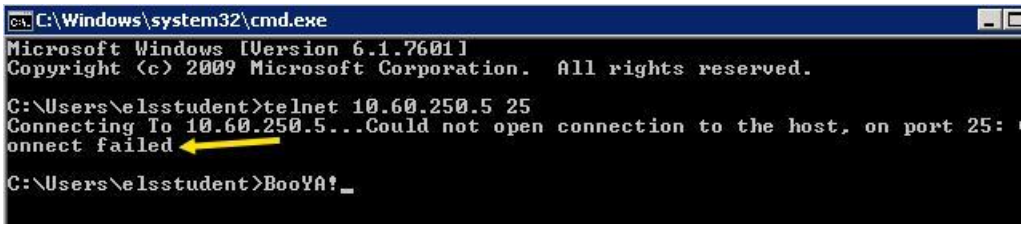
Can't change the firewall:



%APPDATA% malware file is blocked:



Telnet disabled:

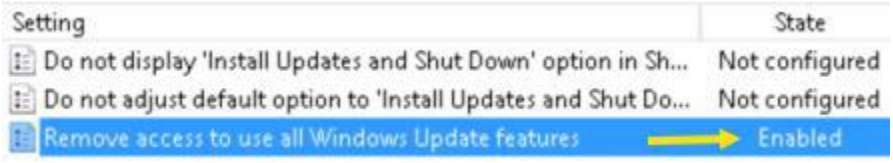


If you are a local admin user, you can still disable UAC. HOWEVER, it will be re-enabled anytime Group Policy refreshes:

Task 2: User Policies

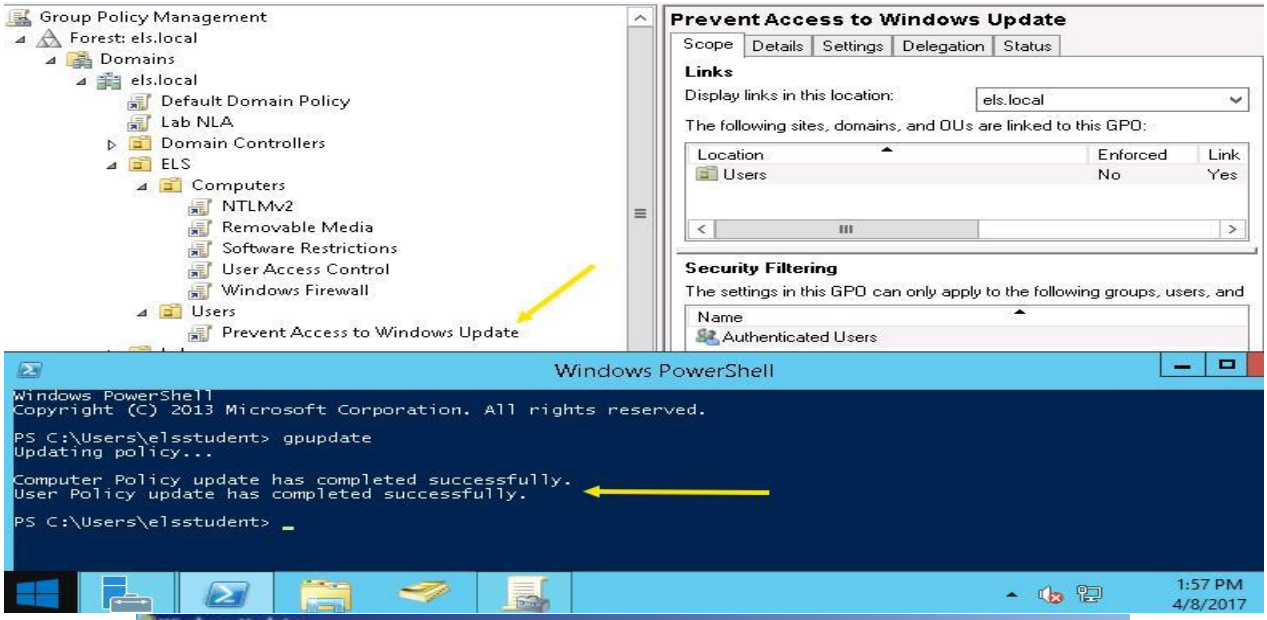
Task 2.1: Windows Update

✓ Assume you have a patch management system and policy. Because of this, create a policy which blocks the end user from being able to access Windows Update.



Task 2.1: Apply GPO and Test

✓ Apply the GPO to the ELS > Users group, then login to the Windows 7 workstation via RDP. You can login using ELSSTUDENT and you can also login using one of the standard user accounts in the ELS > Users OU (just reset their password). When testing these settings, consider ELSSTUDENT is a Domain Admin whereas the other user is a standard user.



LAB 8 Vulnerabilities

LAB DESCRIPTION

In the following lab, you will practice identifying vulnerabilities on Windows machines. You will first see how to identify them manually with NMAP then find them in a more automated way using a vulnerability scanner.

GOALS:

- Identify open services with NMAP
- Identify vulnerabilities with Nessus

IMPORTANT NOTE:

- Labs machines are not connected to the Internet, they are in a private testing environment just for you.
- The domain controller is dc1.els.local at 10.70.250.5
- The target server is server01.els.local at 10.70.250.20

Task 1: Port Scan

The first step of this lab is to identify open and possible vulnerable services.

```
root@kali:~/Desktop/PNDLabs# openvpn L8.ovpn
Sat Apr  8 18:20:36 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Sat Apr  8 18:20:36 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: **********
Sat Apr  8 18:20:42 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]66.232.115.228:3
4199
Sat Apr  8 18:20:42 2017 UDP link local (bound): [AF_INET][undef]:1194
Sat Apr  8 18:20:42 2017 UDP link remote: [AF_INET]66.232.115.228:34199
Sat Apr  8 18:20:42 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]66.232.115.2
28:34199
Sat Apr  8 18:20:43 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This
allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sat Apr  8 18:20:43 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This
allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sat Apr  8 18:20:43 2017 TUN/TAP device tap0 opened
Sat Apr  8 18:20:43 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sat Apr  8 18:20:43 2017 /sbin/ip link set dev tap0 up mtu 1500
Sat Apr  8 18:20:43 2017 /sbin/ip addr add dev tap0 10.70.250.200/24 broadcast 10.70.250.255
Sat Apr  8 18:20:43 2017 Initialization Sequence Completed
```

Task 1.1: NMAP

✓ Run NMAP against DC1 and Server01 to identify open ports and services.

```
root@kali:~# nmap -sV 10.70.250.20

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-08 18:24 EDT
Nmap scan report for 10.70.250.20
Host is up (0.098s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          BisonWare BisonFTPd 3.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:50:56:A1:0C:36 (VMware)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.27 seconds
```

```
root@kali:~# nmap -sV 10.70.250.5

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-08 18:26 EDT
Nmap scan report for 10.70.250.5
Host is up (0.11s latency).
Not shown: 982 filtered ports
PORT    STATE SERVICE      VERSION
53/tcp  open  domain       Microsoft DNS
80/tcp  open  http         Microsoft IIS httpd 8.5
88/tcp  open  kerberos-sec Microsoft Windows Kerberos (server time: 2017-04-08 22:26:59Z)
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: els.local, Site: Default-
First-Site-Name)
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: ELS)
464/tcp open  kpasswd5?
593/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp open  tcpwrapped
3268/tcp open ldap         Microsoft Windows Active Directory LDAP (Domain: els.local, Site: Default-
First-Site-Name)
3269/tcp open tcpwrapped
3389/tcp open ms-wbt-server Microsoft Terminal Service
49154/tcp open msrpc       Microsoft Windows RPC
49155/tcp open msrpc       Microsoft Windows RPC
49157/tcp open ncacn_http  Microsoft Windows RPC over HTTP 1.0
49158/tcp open msrpc       Microsoft Windows RPC
49159/tcp open msrpc       Microsoft Windows RPC
MAC Address: 00:50:56:A1:01:CB (VMware)
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.00 seconds
```

Task 2:Scan with Nessus

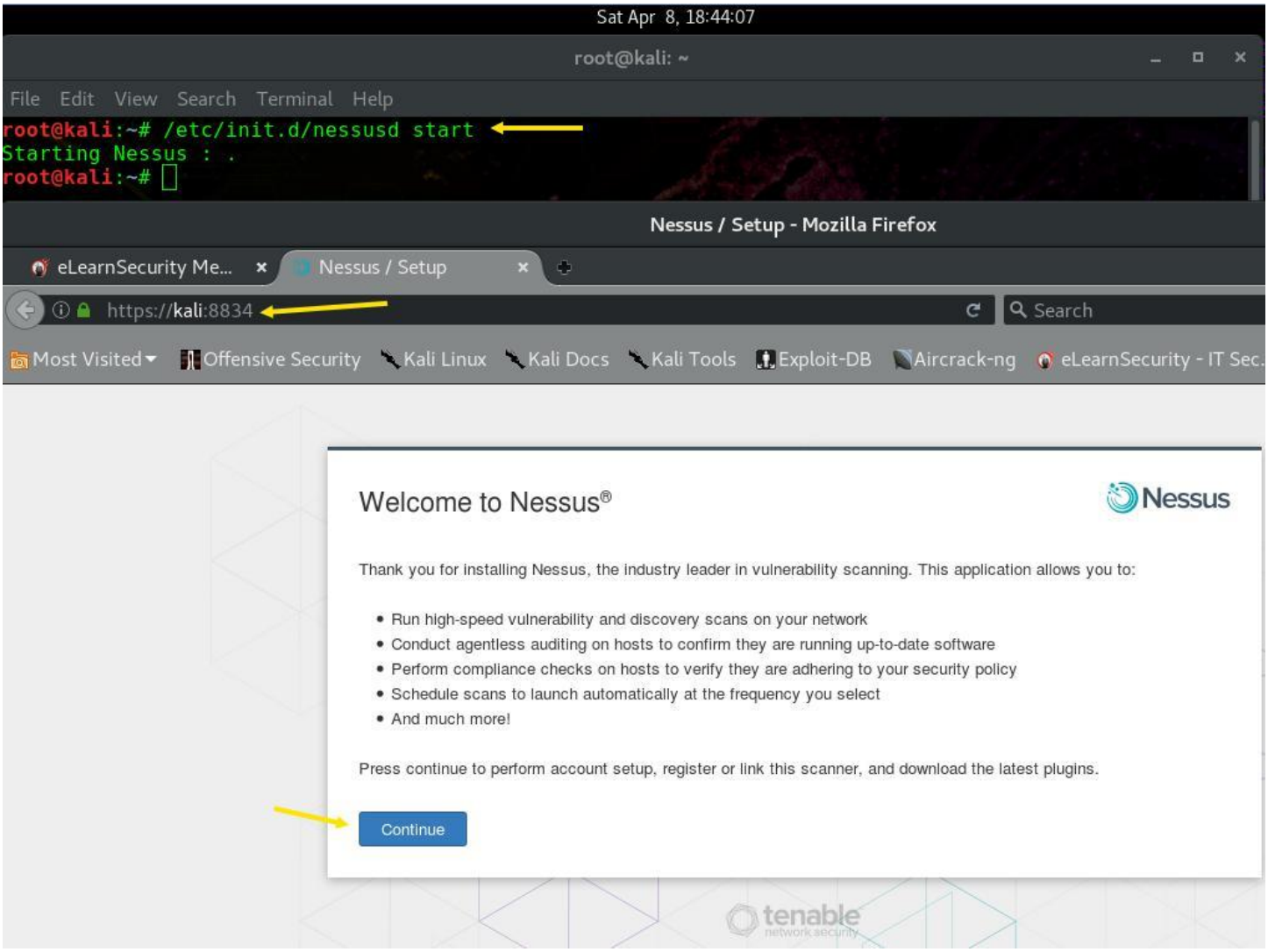
```
Sat Apr  8, 18:41:00
                                    root@kali: ~/Downloads
File  Edit  View  Search  Terminal  Help
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
Nessus-6.10.4-debian6_amd64.deb
root@kali:~/Downloads# dpkg -i Nessus-6.10.4-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 342990 files and directories currently installed.)
Preparing to unpack Nessus-6.10.4-debian6_amd64.deb ...
Unpacking nessus (6.10.4) ...
Setting up nessus (6.10.4) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.10.4 [build M20089] for Linux
Copyright (C) 1998 - 2016 Tenable Network Security, Inc

Processing the Nessus plugins...
[##################################################]

All plugins loaded (1sec)

 - You can start Nessus by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (232-22) ...
root@kali:~/Downloads#
```

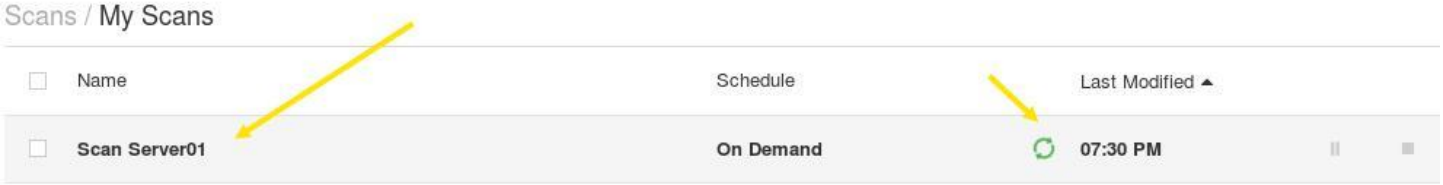


Task 2.1: Setup Options Profile

✓ Setup a scan profile to use in an unauthenticated scan.

Task 2.2: Create and run Scan

✓ Setup a new scan using the scan profile and scan Server01.



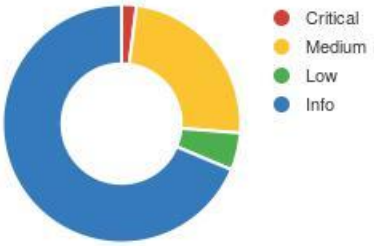
Task 2.3: Review Findings

✓ Review the vulnerability report from Nessus. Are there any highly vulnerable services?

Scan Details

Name:	Scan Server01
Status:	Completed
Policy:	UnAuthenticated NEtwork Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 7:29 PM
End:	Today at 7:38 PM
Elapsed:	9 minutes
Targets:	10.70.250.20

Vulnerabilities



Scan Server01

CURRENT RESULTS: TODAY AT 7:38 PM

Configure | Audit Trail | Launch | Export

Scans > Hosts 1 | Vulnerabilities 41 | History 1

Severity	Plugin Name	Plugin Family	Count
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Cod...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Proto...	Windows	2
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-th...	Windows	1
MEDIUM	SMB Signing Disabled	Misc.	1
MEDIUM	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	General	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MEDIUM	SSL Certificate with Wrong Hostname	General	1

LAB 9 Remediation

LAB DESCRIPTION

In the following lab, we will run an authenticated scan and look at our options for remediation the discovered vulnerabilities.

GOALS:

- Identify vulnerabilities with Nessus
- Remediate vulnerabilities

IMPORTANT NOTE:

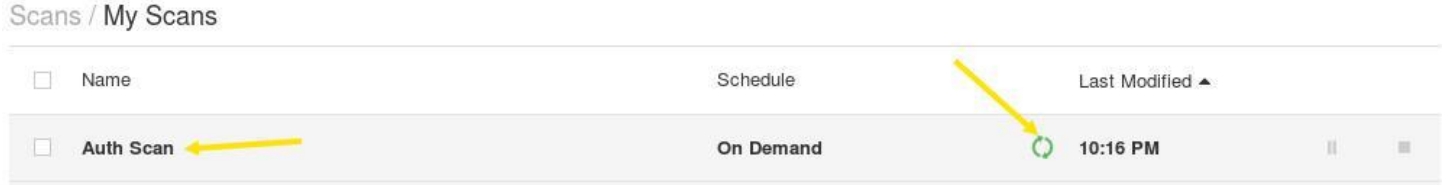
- Labs machines are not connected to the Internet, they are in a private testing environment just for you.
- The domain controller is dc1.els.local at 10.80.250.5
- The target server is server01.els.local at 10.80.250.20

Task 1: Identify Nessus-discovered Vulnerabilities

```
root@kali:~/Desktop/PNDLabs# openvpn L9.ovpn
Sat Apr  8 22:13:43 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Sat Apr  8 22:13:43 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: **********
Sat Apr  8 22:13:48 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:
36212
Sat Apr  8 22:13:48 2017 UDP link local (bound): [AF_INET][undef]:1194
Sat Apr  8 22:13:48 2017 UDP link remote: [AF_INET]162.254.149.248:36212
Sat Apr  8 22:13:48 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.
248:36212
Sat Apr  8 22:13:49 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This
allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sat Apr  8 22:13:49 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This
allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sat Apr  8 22:13:49 2017 TUN/TAP device tap0 opened
Sat Apr  8 22:13:49 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sat Apr  8 22:13:49 2017 /sbin/ip link set dev tap0 up mtu 1500
Sat Apr  8 22:13:49 2017 /sbin/ip addr add dev tap0 10.80.250.200/24 broadcast 10.80.250.255
Sat Apr  8 22:13:49 2017 Initialization Sequence Completed
```

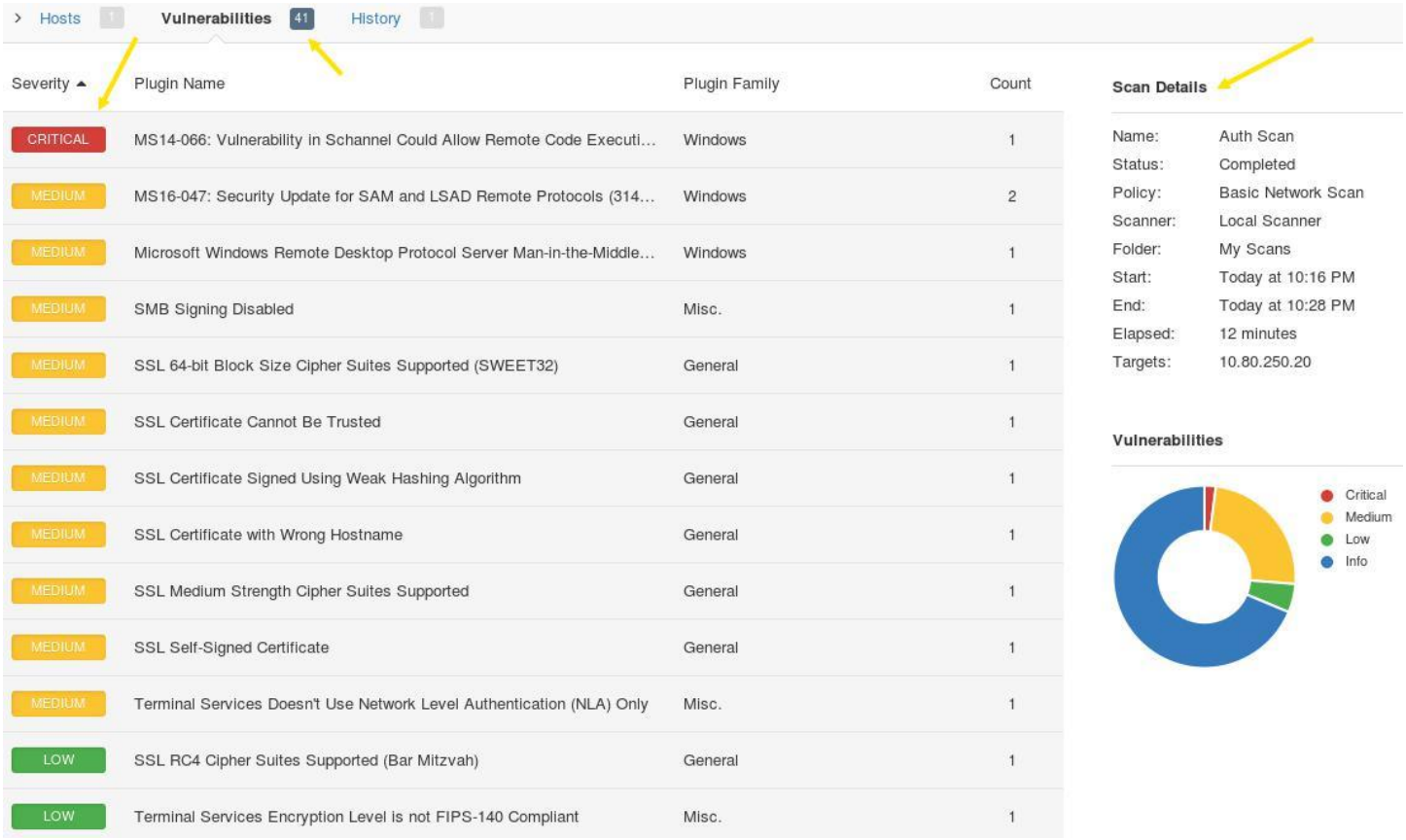
Task 1.1: Run Authenticated Scan

✓ Run an authenticated scan against Server01.



Tasks 1.2: Review Report

✓ Review the vulnerability report from Nessus to discover what vulnerabilities you can remediate.



Hosts 1 | Vulnerabilities 41 | History 1

Severity	Plugin Name	Plugin Family	Count
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Executi...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (314...	Windows	2
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle...	Windows	1
MEDIUM	SMB Signing Disabled	Misc.	1
MEDIUM	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	General	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MEDIUM	SSL Certificate with Wrong Hostname	General	1
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
MEDIUM	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Misc.	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1
LOW	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1

Scan Details

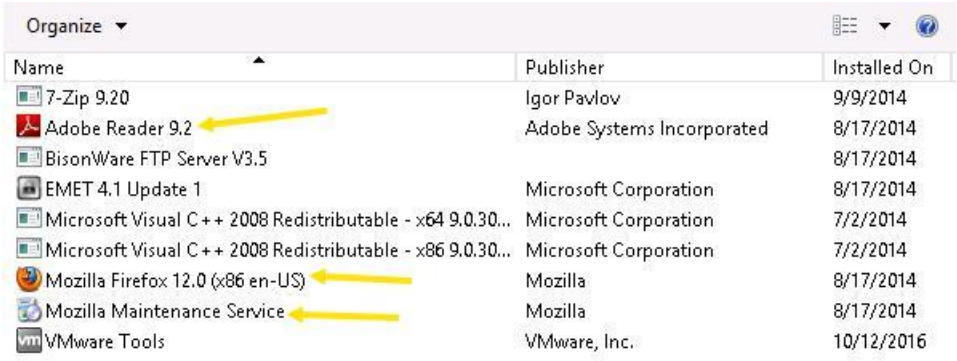
Name:	Auth Scan
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 10:16 PM
End:	Today at 10:28 PM
Elapsed:	12 minutes
Targets:	10.80.250.20

Vulnerabilities

Task 2: Remediation

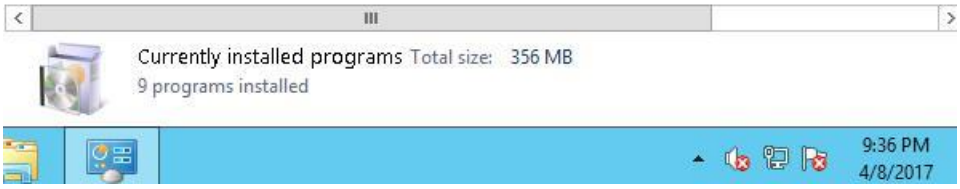
Task 2.1: Remove End of Support Software

✓ Remove unneeded and end of support software. Remember that the FTP server is used by an internal production application.



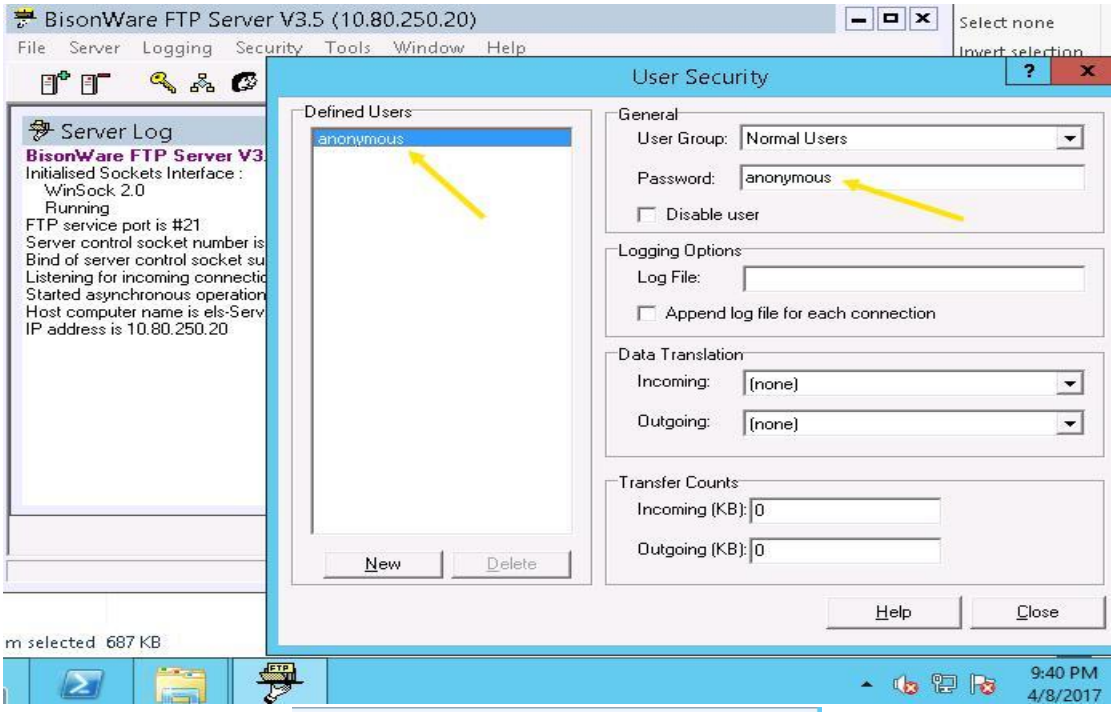
Organize

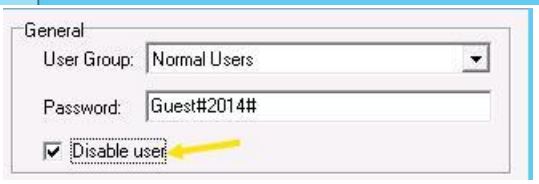
Name	Publisher	Installed On
7-Zip 9.20	Igor Pavlov	9/9/2014
Adobe Reader 9.2	Adobe Systems Incorporated	8/17/2014
BisonWare FTP Server V3.5		8/17/2014
EMET 4.1 Update 1	Microsoft Corporation	8/17/2014
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30...	Microsoft Corporation	7/2/2014
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30...	Microsoft Corporation	7/2/2014
Mozilla Firefox 12.0 (x86 en-US)	Mozilla	8/17/2014
Mozilla Maintenance Service	Mozilla	8/17/2014
VMware Tools	VMware, Inc.	10/12/2016



Task 2.2: Remediate FTP findings

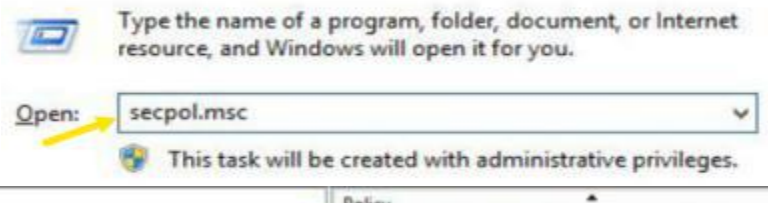
✓ Remediate any FTP related findings (other than patching it).

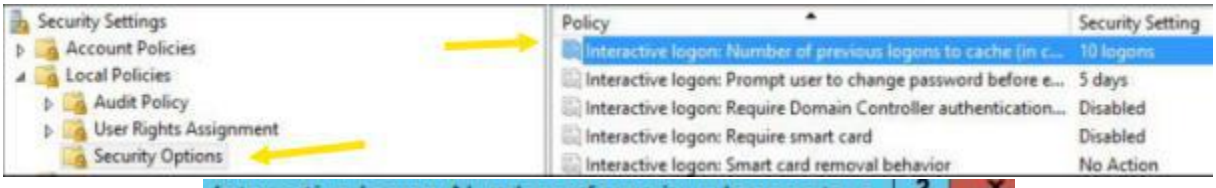


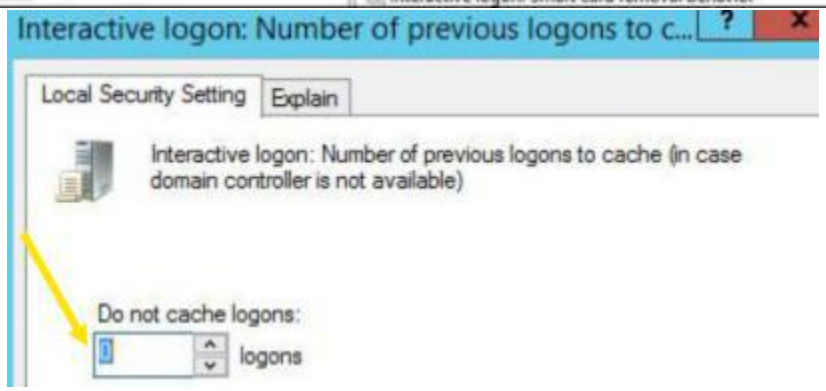


Task 2.3: Remediate Windows configuration vulnerabilities

✓ A few vulnerabilities discovered relating to the Windows configuration as opposed to patches. Remediate these.







Task 3: Validate Remediation

Task 3.1: Follow up Nessus Scan

✓ Run the authenticated scan again to validate the remediation of the vulnerabilities you worked to correct.

There are less:

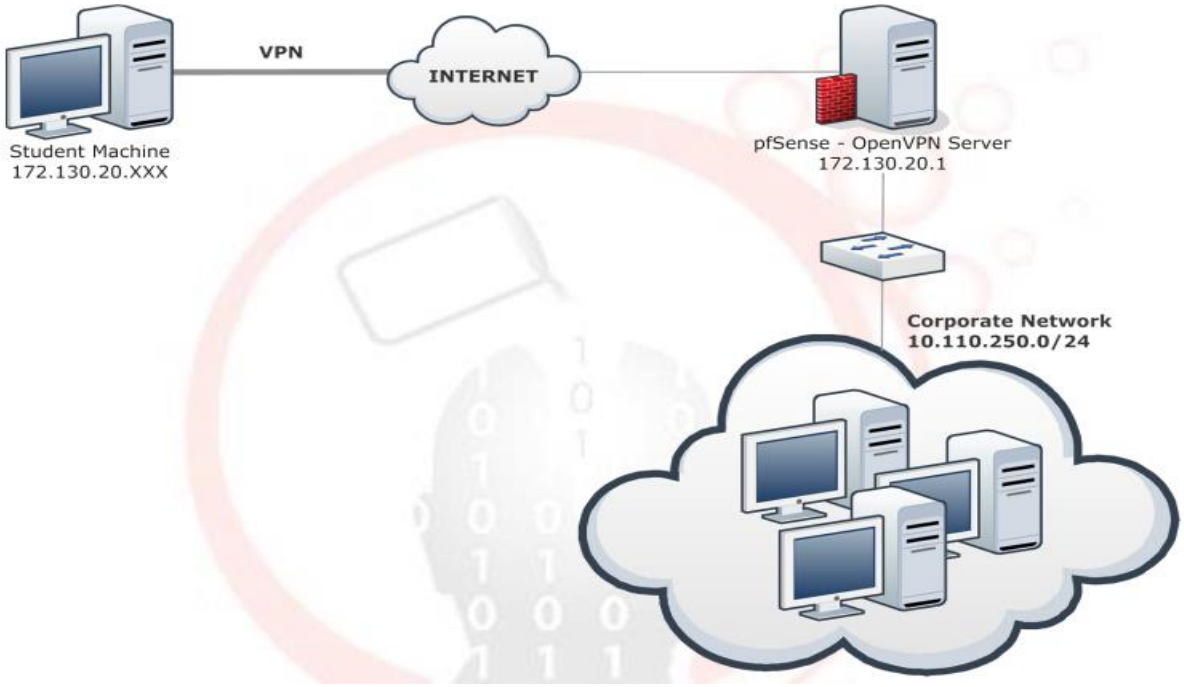
All highs – medium are patch related now:

Severity	Plugin Name	Plugin Family	Count
HIGH	Microsoft Windows Update Reboot Required	Windows	1
HIGH	MS14-051: Cumulative Security Update for Internet Explorer (29...	Windows : Microsoft Bulletins	1
MEDIUM	MS KB2960358: Update for Disabling RC4 in .NET TLS	Windows	1
MEDIUM	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow El...	Windows : Microsoft Bulletins	1
MEDIUM	MS14-047: Vulnerability in LRPC Could Allow Security Feature By...	Windows : Microsoft Bulletins	1

LAB 10 Open VPN

LAB DESCRIPTION

In the following lab, you will configure an OpenVPN server running on pfSense. The following diagram shows the network configuration. The IP address 172.130.20.1 is the *public* IP address of the pfSense box that runs OpenVPN.



GOALS:

Configure pfSense and OpenVPN server in order to allow external machine to be directly connected in the LAN/Corporate network (10.110.250.0/24).

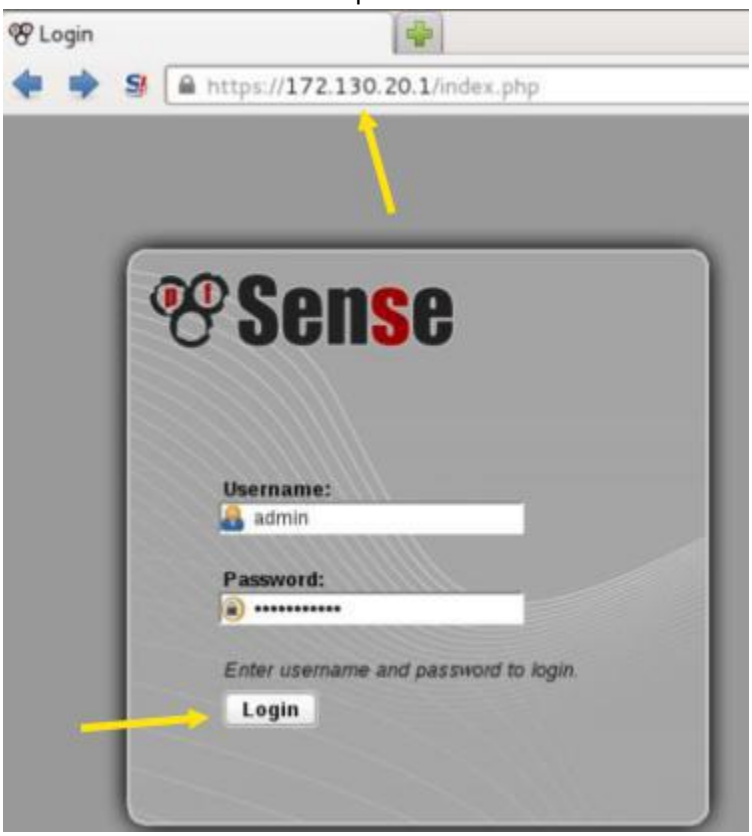
IMPORTANT NOTE:

- The pfSense firewall is located at 172.130.20.1.
- The LAN / Corporate network subnet is 10.110.250.0/24.

```
root@kali:~/Desktop/PNDLabs# openvpn L10.ovpn
Sun Apr  9 12:05:01 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (Open
SSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb  2 2017
Sun Apr  9 12:05:01 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: **********
Sun Apr  9 12:05:07 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:
36221
Sun Apr  9 12:05:07 2017 UDP link local (bound): [AF_INET][undef]:1194
Sun Apr  9 12:05:07 2017 UDP link remote: [AF_INET]162.254.149.248:36221
Sun Apr  9 12:05:07 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.
248:36221
Sun Apr  9 12:05:08 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This
allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sun Apr  9 12:05:08 2017 WARNING: INSECURE cipher with block size less than 128 bit (64 bit).  This
allows attacks like SWEET32.  Mitigate by using a --cipher with a larger block size (e.g. AES-256-CB
C).
Sun Apr  9 12:05:08 2017 TUN/TAP device tap0 opened
Sun Apr  9 12:05:08 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sun Apr  9 12:05:08 2017 /sbin/ip link set dev tap0 up mtu 1500
Sun Apr  9 12:05:08 2017 /sbin/ip addr add dev tap0 172.130.20.200/24 broadcast 172.130.20.255
Sun Apr  9 12:05:08 2017 Initialization Sequence Completed
```

Task 1: Connect to the pfSense

✓ Connect to the pfSense box via the web interface. The pfSense IP address is 172.130.20.1.

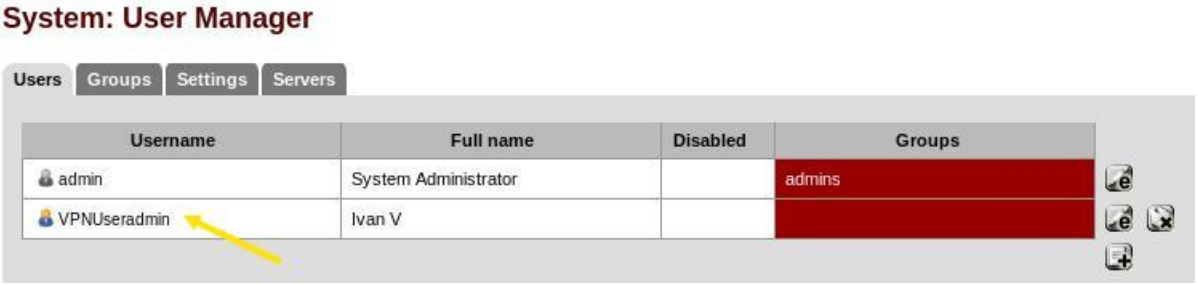


Task 2: Create an Internal CA

✓ The first step for setting an openVPN server is to create an internal CA. You can do it in the pfSense "*Cert Manager*".

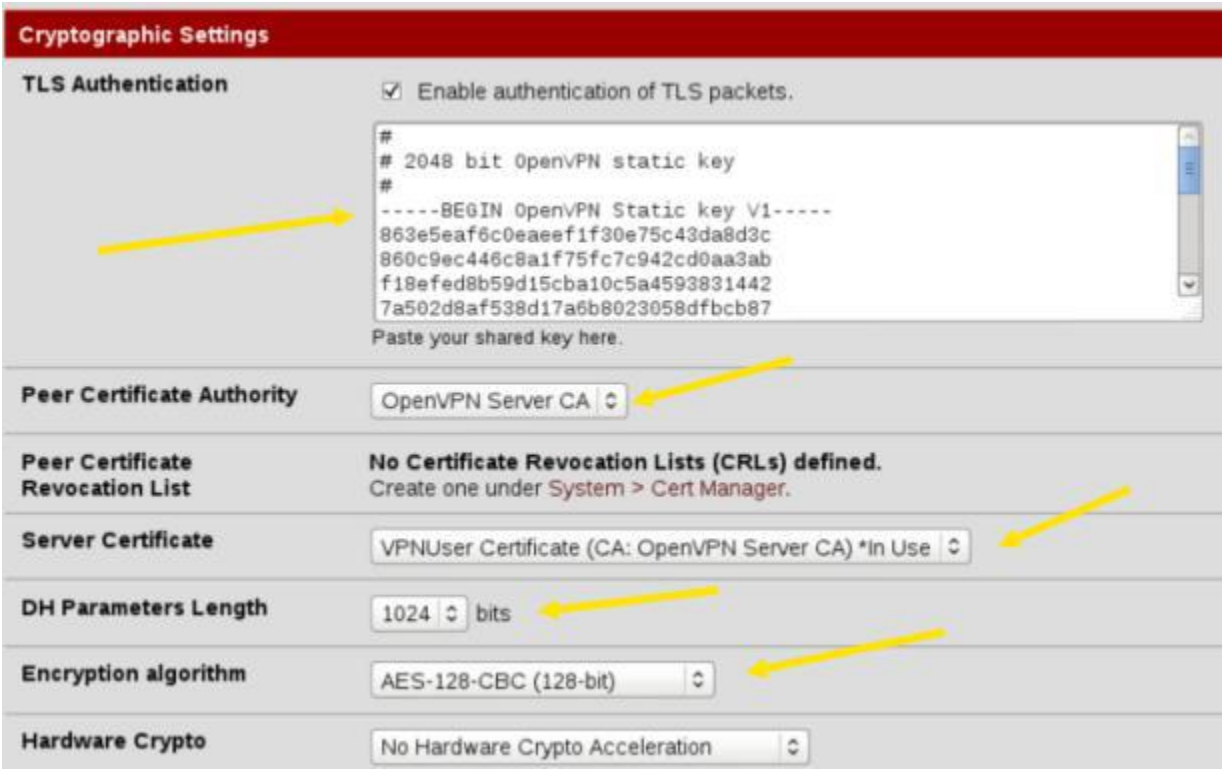
Task 3: Create the VPN user and its certificate

✓ Create a new user for the VPN connection. The credential will be used later on for establishing the connection.



Task 4: Configure the OpenVPN Server

✓ Run the openVPN wizard to configure and start the openVPN server.



Task 5: Export the client configuration

✓ Export and install the client configuration installer from pfSense.

Client Install Packages

User	Certificate Name	Export
VPNUser	VPNUser Certificate	- Standard Configurations: Archive Config Only - Inline Configurations: Android OpenVPN Connect (iOS/Android) Others - Windows Installers: 2.3-x86 2.3-x64 - Mac OSX: Viscosity Bundle

Task 6: Test the tunnel

✓ Connect to the tunnel and test that the connection works by running a ping against the LAN/Corporate machine 10.110.250.50