

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

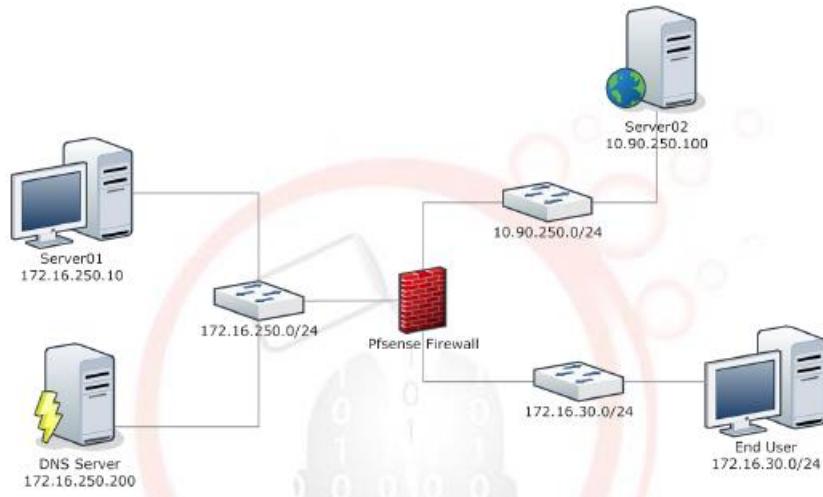
CONTENTS	2
<u>LAB 1 ACCESS CONTROL LISTS</u>	4
LAB DESCRIPTION	4
TASK 1: IDENTIFY WHAT TRAFFIC THE FIREWALL PASSES	4
TASK 2: FIREWALL CONFIGURATION	6
<u>LAB 2 ACTIVE DIRECTORY</u>	11
LAB DESCRIPTION	11
TASK 1: ACTIVE DIRECTORY USERS AND COMPUTERS	12
TASK 2: GROUP POLICY	14
TASK 3: CLIENT COMPUTERS	18
<u>LAB 3 ADCS</u>	20
LAB DESCRIPTION	20
TASK 1: OFFLINE ROOT CERTIFICATE AUTHORITY	20
TASK 2: SUBORDINATE CERTIFICATE AUTHORITY	22
TASK 3: DEPLOYING ROOT CERTIFICATE	27
<u>LAB 4 WSUS</u>	30
LAB DESCRIPTION	30
TASK 1: CONFIGURE WSUS	30
TASK 2: CONFIGURE DOMAIN WSUS SETTINGS	33
TASK 3: DEPLOYING UPDATES	34
<u>LAB 5 EMET</u>	37
LAB DESCRIPTION	37
TASK 1: RUN THE VULNERABLE APPLICATION	37
TASK 2: INSTALL EMET	37
TASK 3: DEPLOY EMET	38
TASK 4: DEPLOYMENT	41
<u>LAB 6 GROUP POLICY</u>	43
LAB DESCRIPTION	43
TASK 1: CREATE THE NEEDED GPOs	43
TASK 2: APPLY THE GPOs	45
TASK 3: TEST GPO SETTINGS	46

<u>LAB 7 ENDPOINT SECURITY</u>	48
LAB DESCRIPTION	48
TASK 1: WORKSTATION POLICIES	48
TASK 2: USER POLICIES	55
<u>LAB 8 VULNERABILITIES</u>	56
LAB DESCRIPTION	56
TASK 1: PORT SCAN	56
TASK 2:SCAN WITH NESSUS	57
<u>LAB 9 REMEDIATION</u>	60
LAB DESCRIPTION	60
TASK 1: IDENTIFY NESSUS-DISCOVERED VULNERABILITIES	60
TASK 2: REMEDIATION	61
TASK 3: VALIDATE REMEDIATION	63
<u>LAB 10 OPEN VPN</u>	64
LAB DESCRIPTION	64
TASK 1: CONNECT TO THE PFSENSE	65
TASK 2: CREATE AN INTERNAL CA	65
TASK 3: CREATE THE VPN USER AND ITS CERTIFICATE	65
TASK 4: CONFIGURE THE OPENVPN SERVER	66
TASK 5: EXPORT THE CLIENT CONFIGURATION	67
TASK 6: TEST THE TUNNEL	67

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.

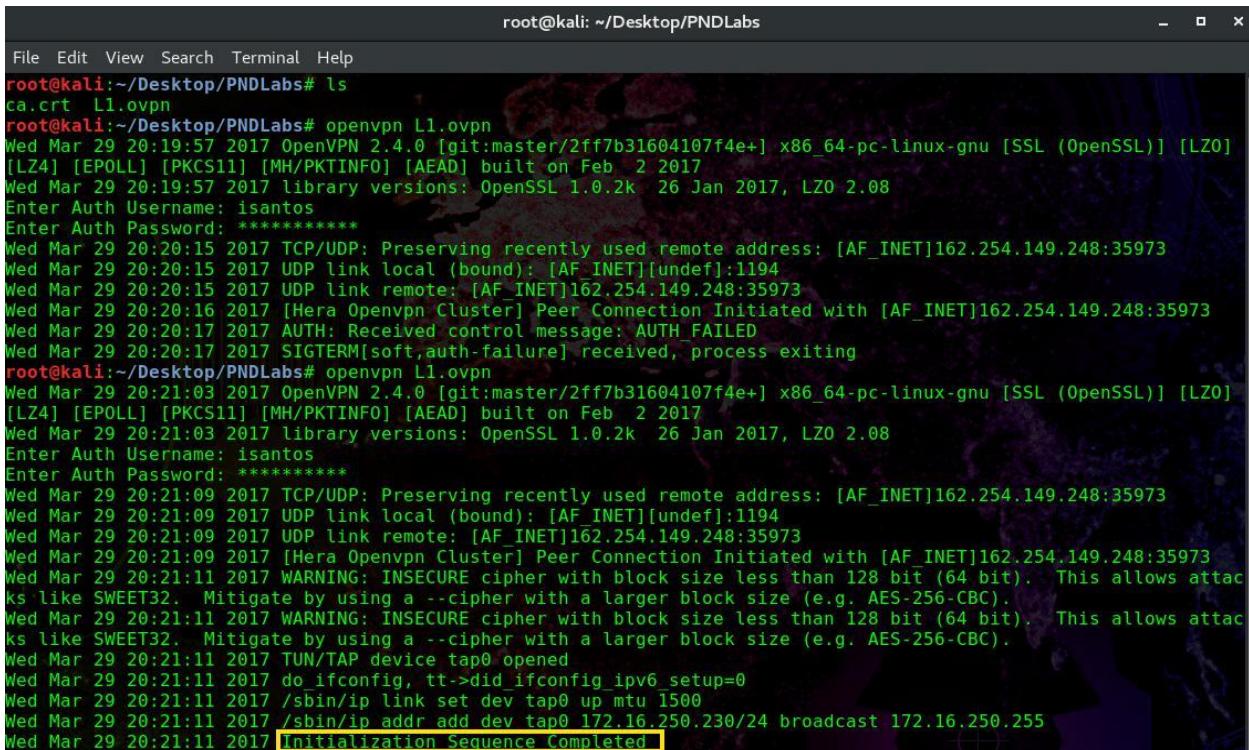
GOALS

- 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:

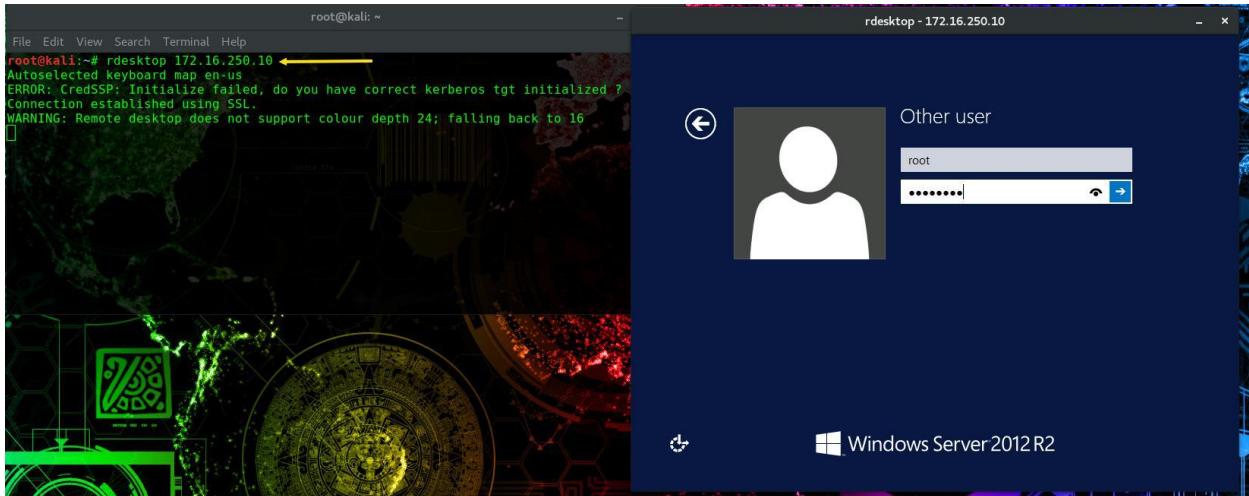


```

root@kali:~/Desktop/PNDLabs# ls
ca.crt  L1.ovpn
root@kali:~/Desktop/PNDLabs# openvpn L1.ovpn
Wed Mar 29 20:19:57 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Wed Mar 29 20:19:57 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: ****
Wed Mar 29 20:20:15 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:35973
Wed Mar 29 20:20:15 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Mar 29 20:20:15 2017 UDP link remote: [AF_INET]162.254.149.248:35973
Wed Mar 29 20:20:16 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:35973
Wed Mar 29 20:20:17 2017 AUTH: Received control message: AUTH FAILED
Wed Mar 29 20:20:17 2017 SIGTERM[soft,auth-failure] received, process exiting
root@kali:~/Desktop/PNDLabs# openvpn L1.ovpn
Wed Mar 29 20:21:03 2017 OpenVPN 2.4.0 [git:master/2ff7b31604107f4e+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 2 2017
Wed Mar 29 20:21:03 2017 library versions: OpenSSL 1.0.2k 26 Jan 2017, LZO 2.08
Enter Auth Username: isantos
Enter Auth Password: ****
Wed Mar 29 20:21:09 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:35973
Wed Mar 29 20:21:09 2017 UDP link local (bound): [AF_INET][undef]:1194
Wed Mar 29 20:21:09 2017 UDP link remote: [AF_INET]162.254.149.248:35973
Wed Mar 29 20:21:09 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:35973
Wed Mar 29 20:21:11 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-CBC).
Wed Mar 29 20:21:11 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-CBC).
Wed Mar 29 20:21:11 2017 TUN/TAP device tap0 opened
Wed Mar 29 20:21:11 2017 do_ifconfig, tt->do_ifconfig_ipv6_setup=0
Wed Mar 29 20:21:11 2017 /sbin/ip link set dev tap0 up mtu 1500
Wed Mar 29 20:21:11 2017 /sbin/ip addr add dev tap0 172.16.250.230/24 broadcast 172.16.250.255
Wed Mar 29 20:21:11 2017 Initialization Sequence Completed

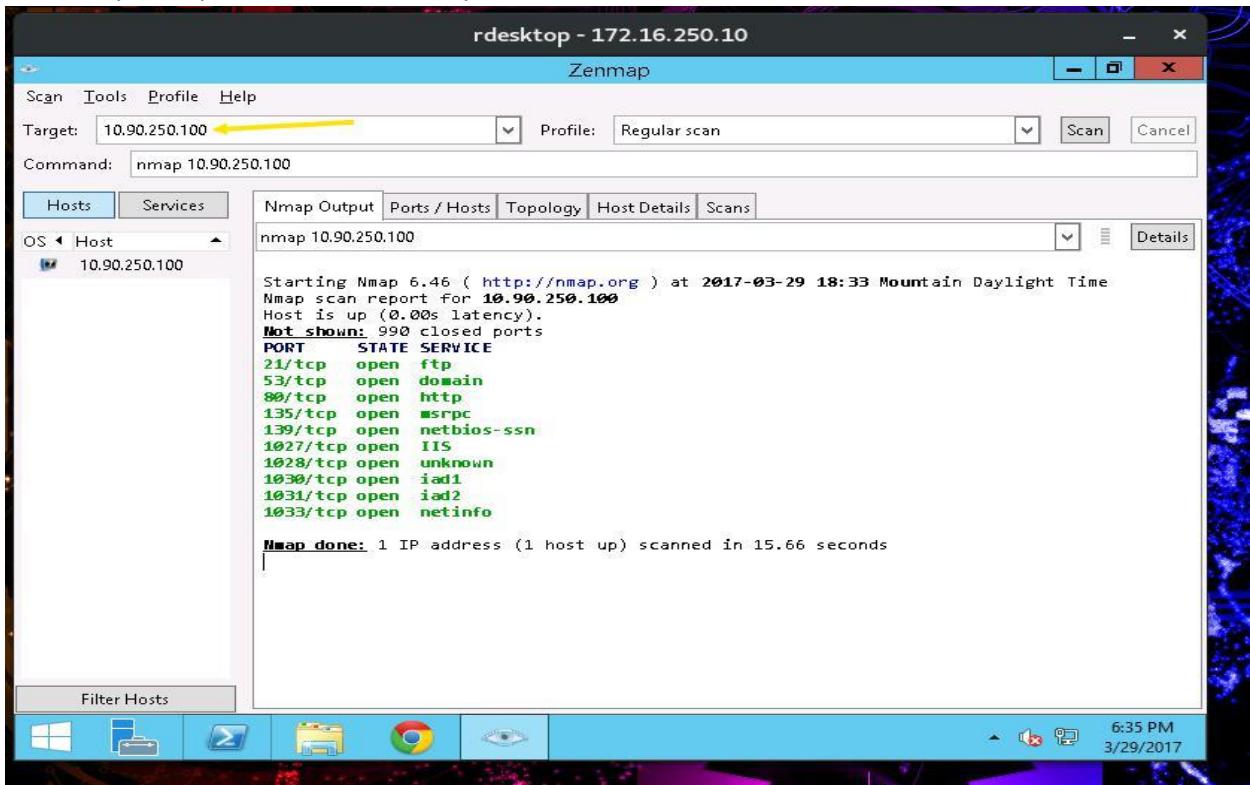
```

- ✓ 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):

The screenshot shows the pfSense Firewall: Aliases configuration page. The table lists the following aliases:

Name	Values	Description
Developer	172.16.30.245	Developer
DNSServer	172.16.250.200	Internal DNS Server
Firewall	172.16.250.254	
Server01	172.16.250.10	
Server02	10.90.250.100	Hosting many external services.

Note:
Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

- 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:

Floating	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	80	*	*			Anti-Lockout Rule
		UDP	DNSServer	*	Server02	53 (DNS)	*	none		Allow DNS Requests Outbound
		TCP	DNSServer	*	4.2.2.4	123 (NTP)	*	none		Allow NTP Access
		*	*	*	*	*	*	none		Explicit Deny

Legend:

- pass (green circle)
- block (red circle)
- reject (yellow circle)
- log (blue circle)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

- ✓ My ACL setup for the OPT1 Interface:

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	TCP	172.16.30.0/24	*	*	443 (HTTPS)	*	none		Allow End Users Access to HTTPS
2	TCP	172.16.30.0/24	*	*	80 (HTTP)	*	none		Allow End Users to Access HTTP
3	UDP	172.16.30.0/24	*	DNSServer	53 (DNS)	*	none		Allow End Users Access to DNS
4	TCP	Developer	*	10.90.250.100	21 (FTP)	*	none		Allow Dev Access to FTP
5	*	*	*	*	*	*	none		Explicit Deny

Legend: pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

- 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.

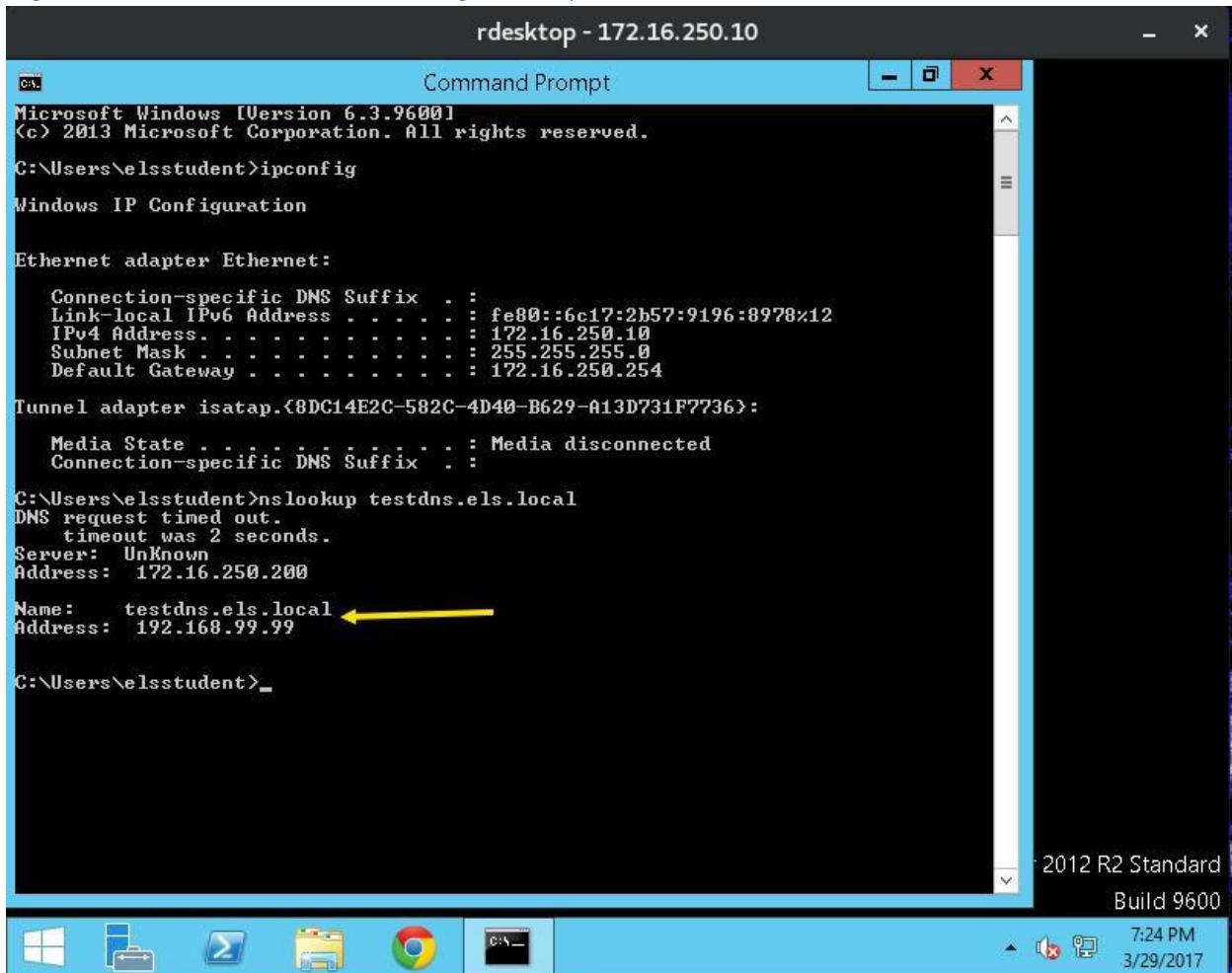
- ✓ The results of the port scan from server1 after the ACL changes, ports are now filtered:

```

rdesktop - 172.16.250.10
Zenmap
Scan Tools Profile Help
Target: 10.90.250.100
Profile: Scan Cancel
Command: nmap -T4 -Pn 10.90.250.100
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -Pn 10.90.250.100
Starting Nmap 6.46 ( http://nmap.org ) at 2017-03-29 19:17 Mountain Daylight Time
Nmap scan report for 10.90.250.100
Host is up.
All 1000 scanned ports on 10.90.250.100 are filtered
Nmap done: 1 IP address (1 host up) scanned in 117.36 seconds

```

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



```
rdesktop - 172.16.250.10
Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\elsstudent>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . . .
  Link-local IPv6 Address . . . . . : fe80::6c17:2b57:9196:8978%12
  IPv4 Address . . . . . : 172.16.250.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 172.16.250.254

Tunnel adapter isatap.{8DC14E2C-582C-4D40-B629-A13D731F7736}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .

C:\Users\elsstudent>nslookup testdns.els.local
DNS request timed out.
  timeout was 2 seconds.
Server: UnKnown
Address: 172.16.250.200

Name: testdns.els.local
Address: 192.168.99.99 ←

C:\Users\elsstudent>_
```

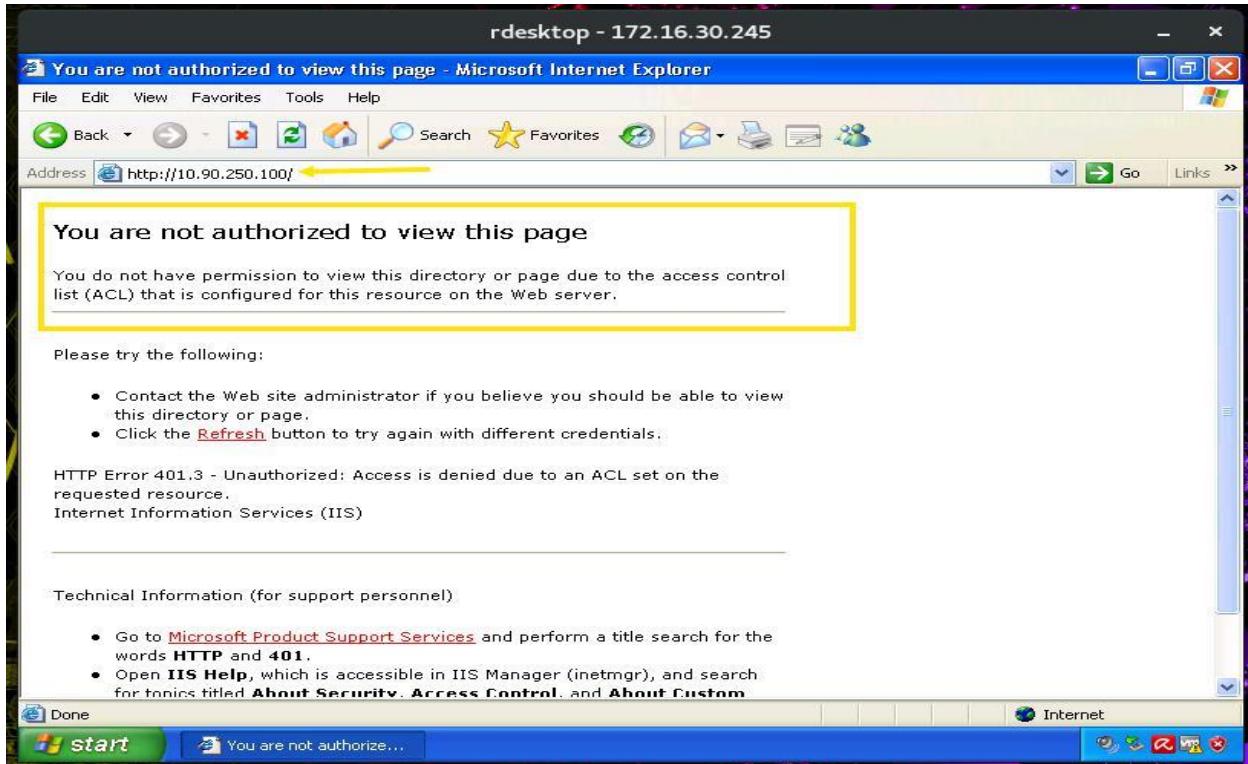
The screenshot shows a Windows Command Prompt window titled "rdesktop - 172.16.250.10". It displays the output of the "ipconfig" command, which shows network configuration for the "Ethernet" adapter. The "Address" field for the "IPv4 Address" is 172.16.250.10. The output also includes the result of the "nslookup testdns.els.local" command, which shows the name "testdns.els.local" and the address "192.168.99.99". A yellow arrow points to the address "192.168.99.99". The taskbar at the bottom shows various icons and the system tray indicates the date and time as "7:24 PM 3/29/2017".

- 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)

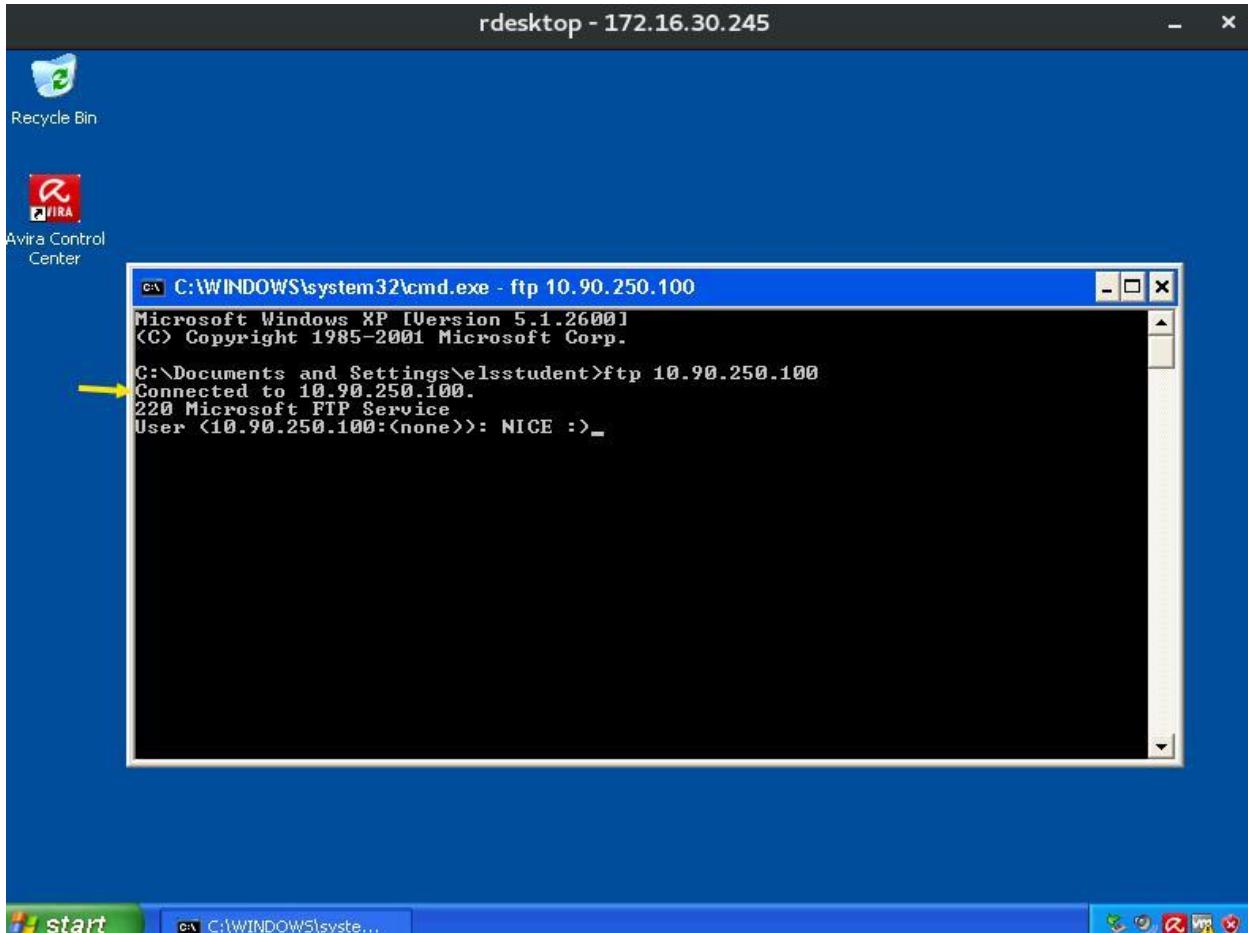
- ✓ I needed to change the ACL to enable RDP with the Developer host:

	TCP/UDP	172.16.250.230	*	<u>Developer</u>	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:

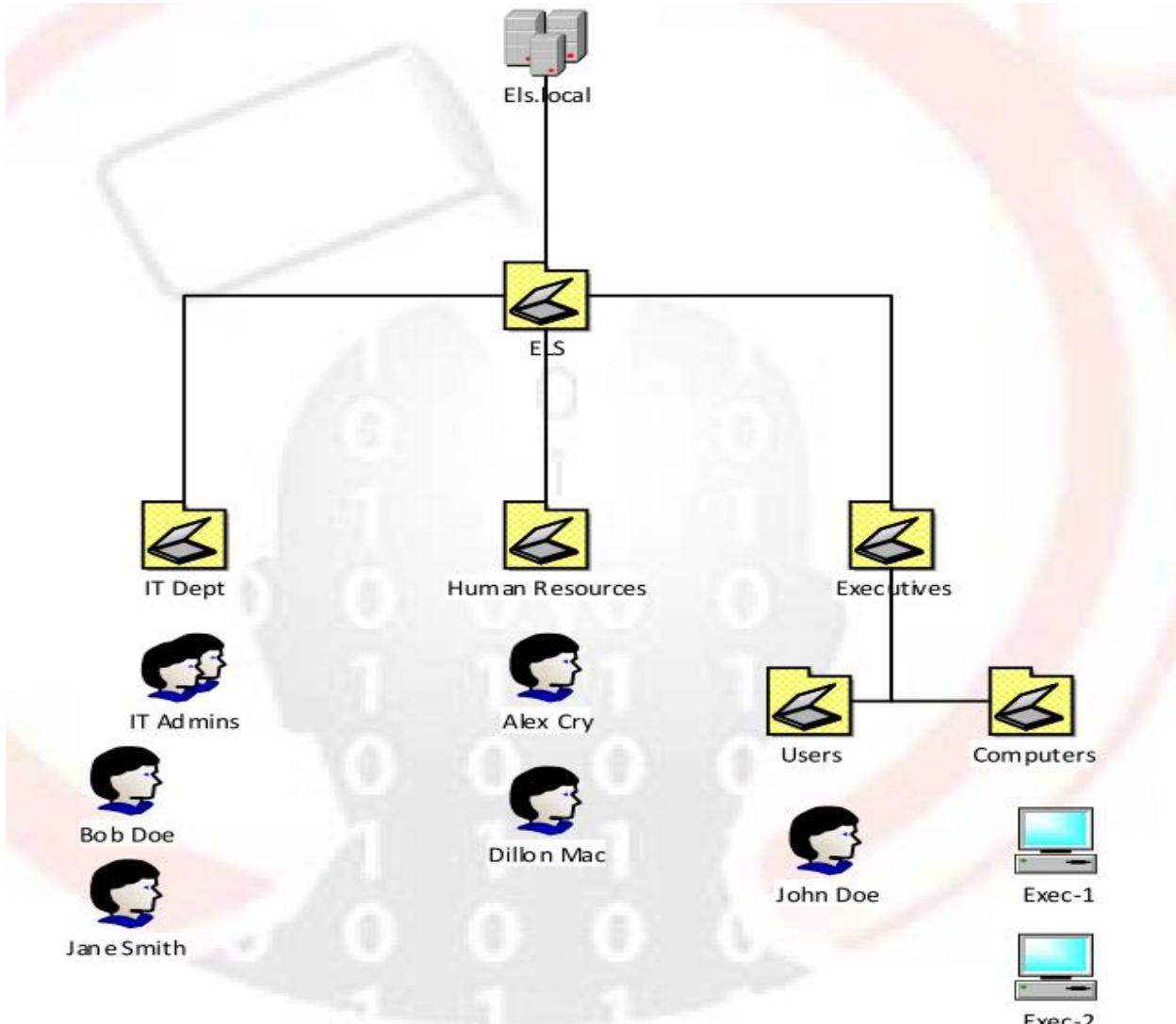


LAB 2 Active Directory

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.

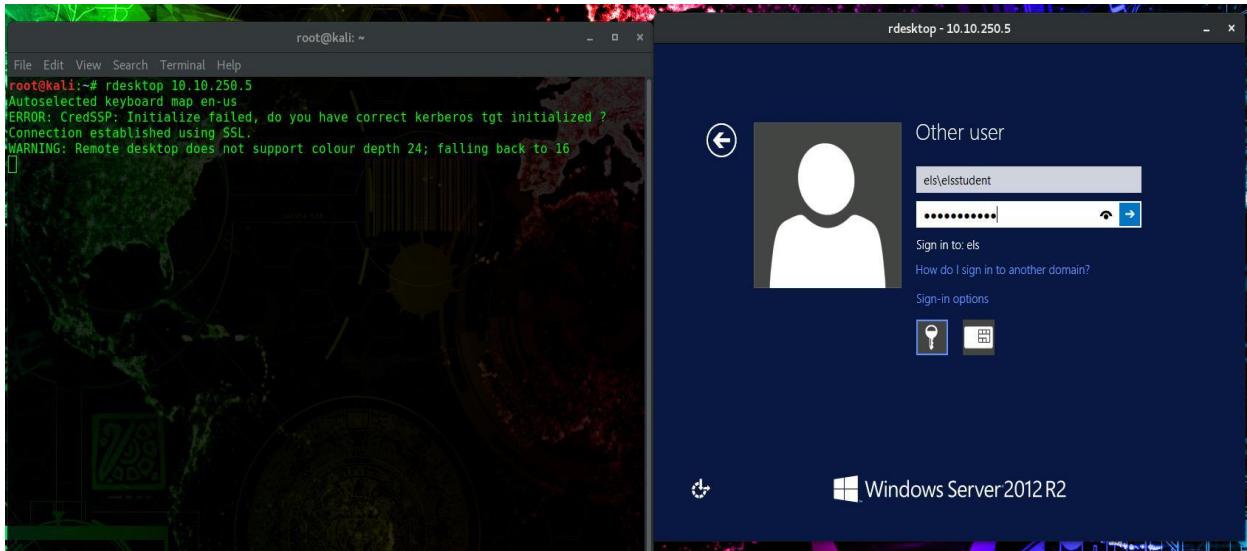
Task 1: Active Directory Users and Computers

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

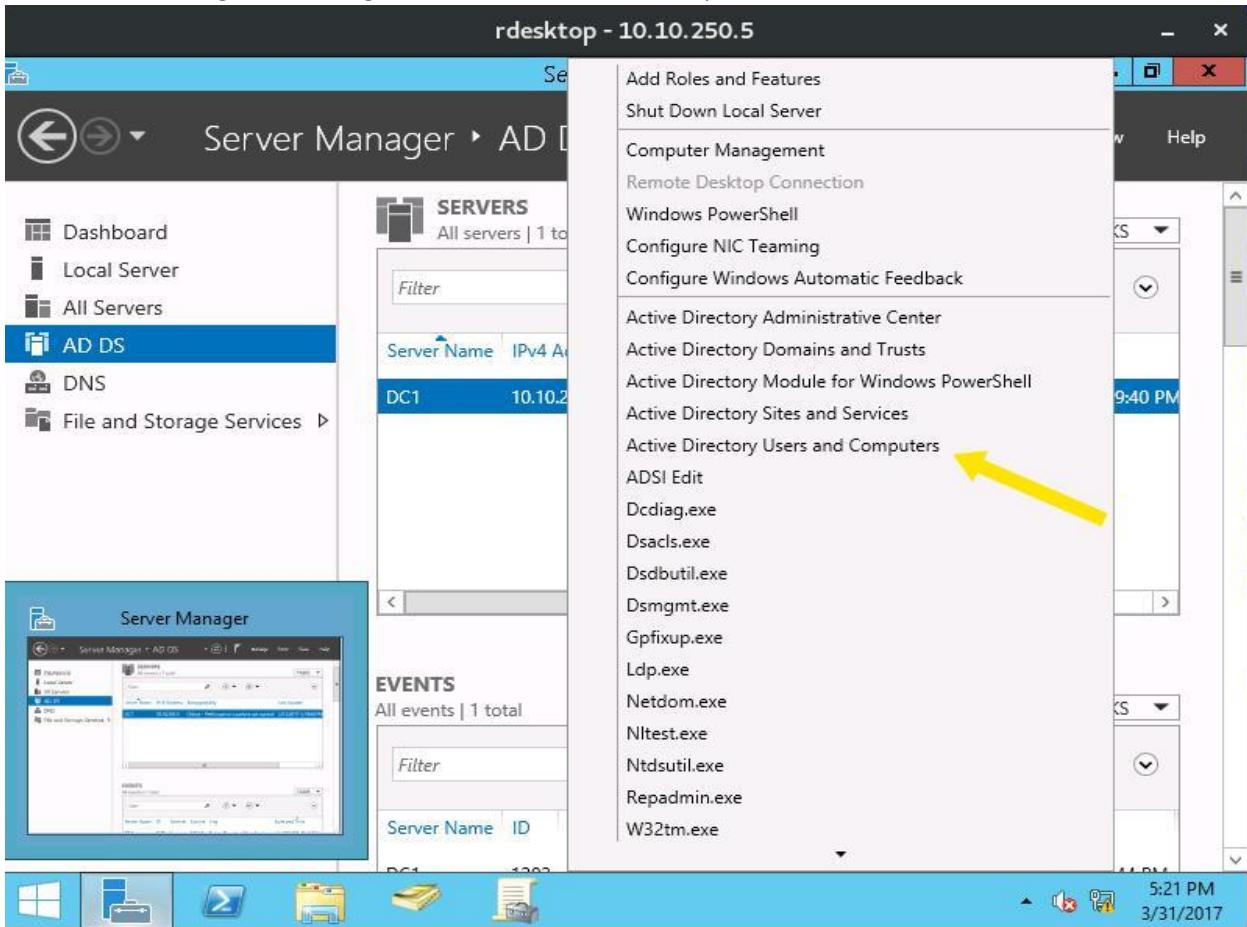
Task 1.1: Creating Organizational Units

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

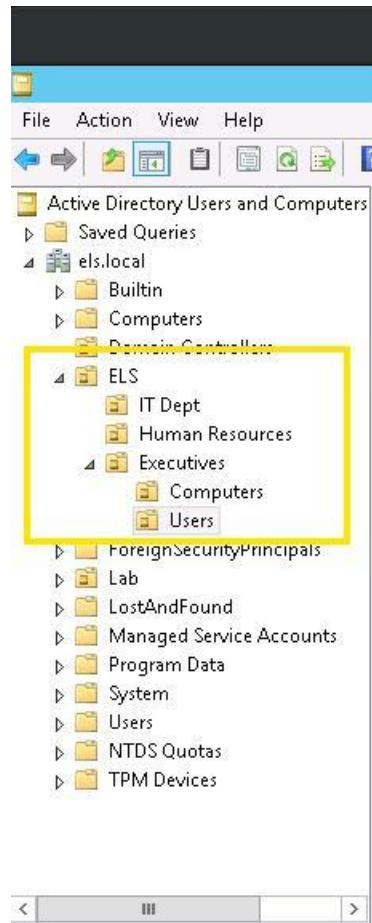
- ✓ I RDP'd into the domain controller:



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



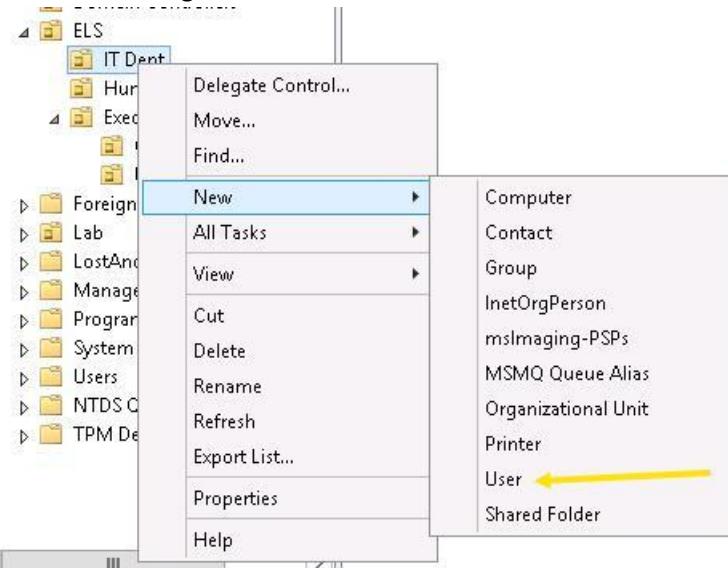
- ✓ I navigated the AD tree and added the OU's in the correct ELS section:



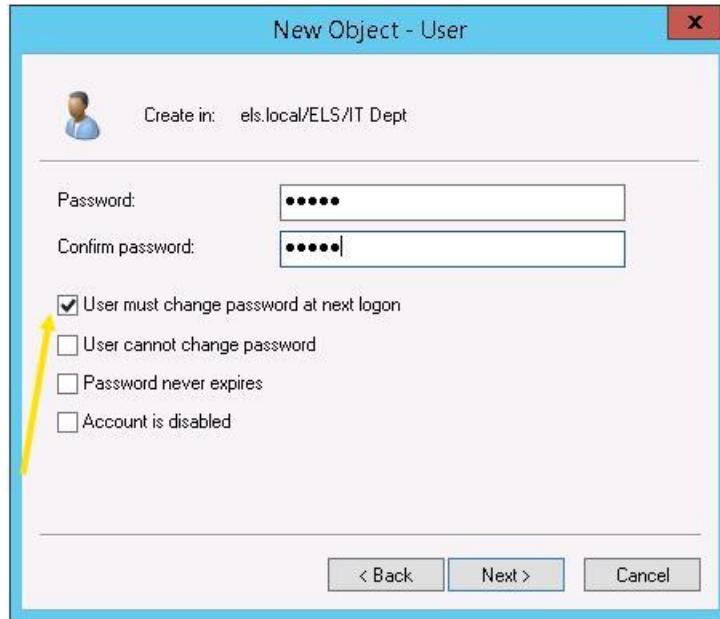
Task 1.2: Creating Accounts and Groups

- 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.

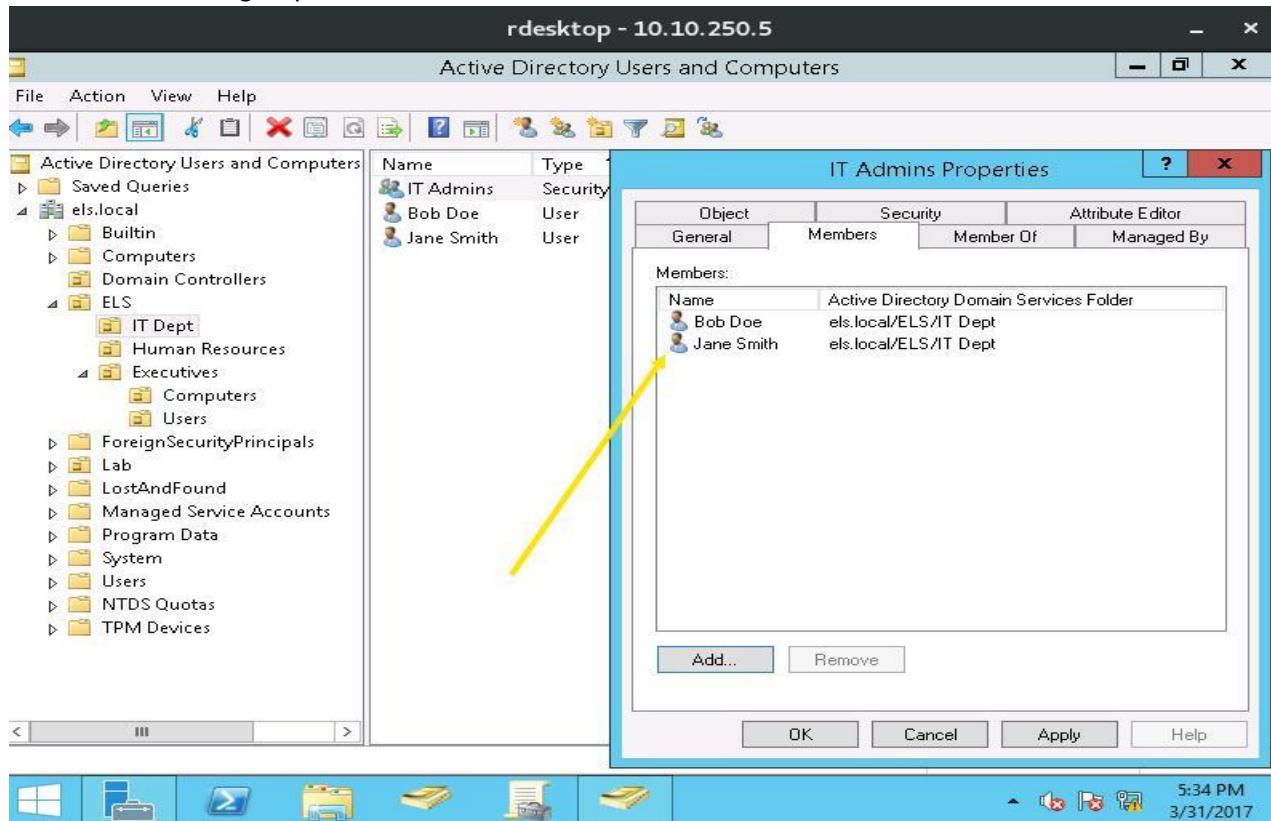
- ✓ I created the users based on the AD diagram:



- ✓ I enabled the change password at next login rule:



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

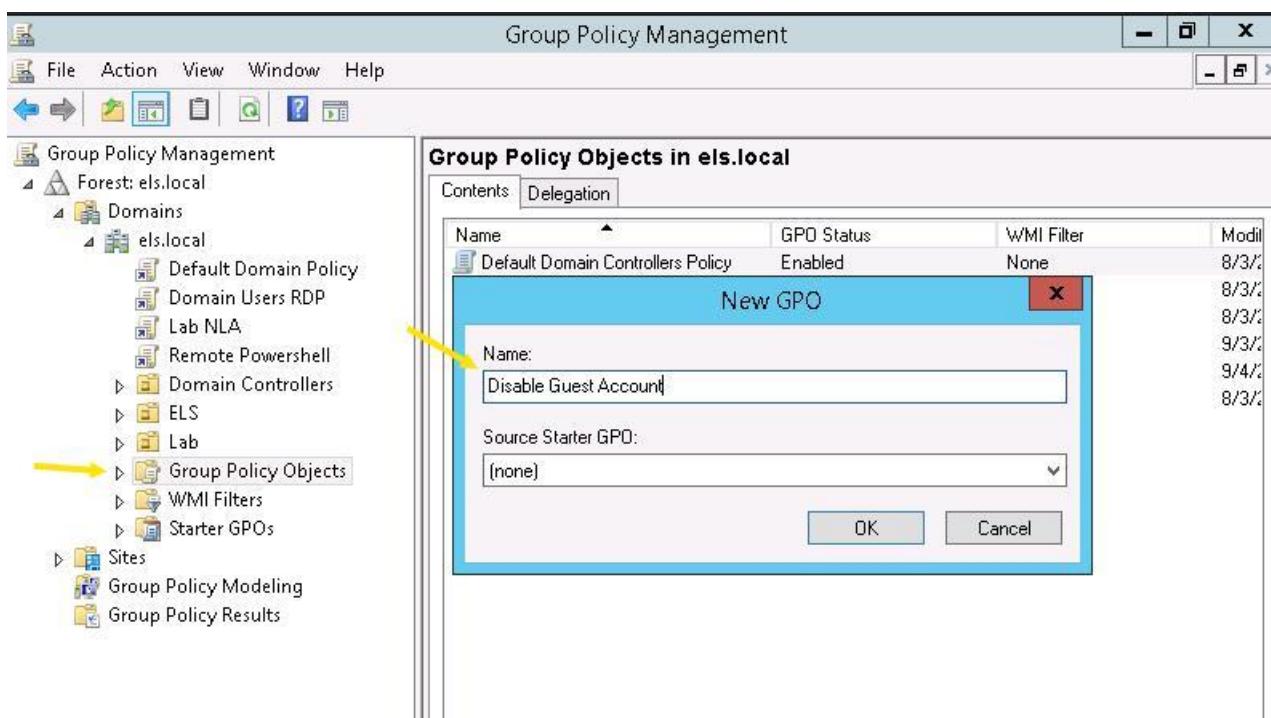
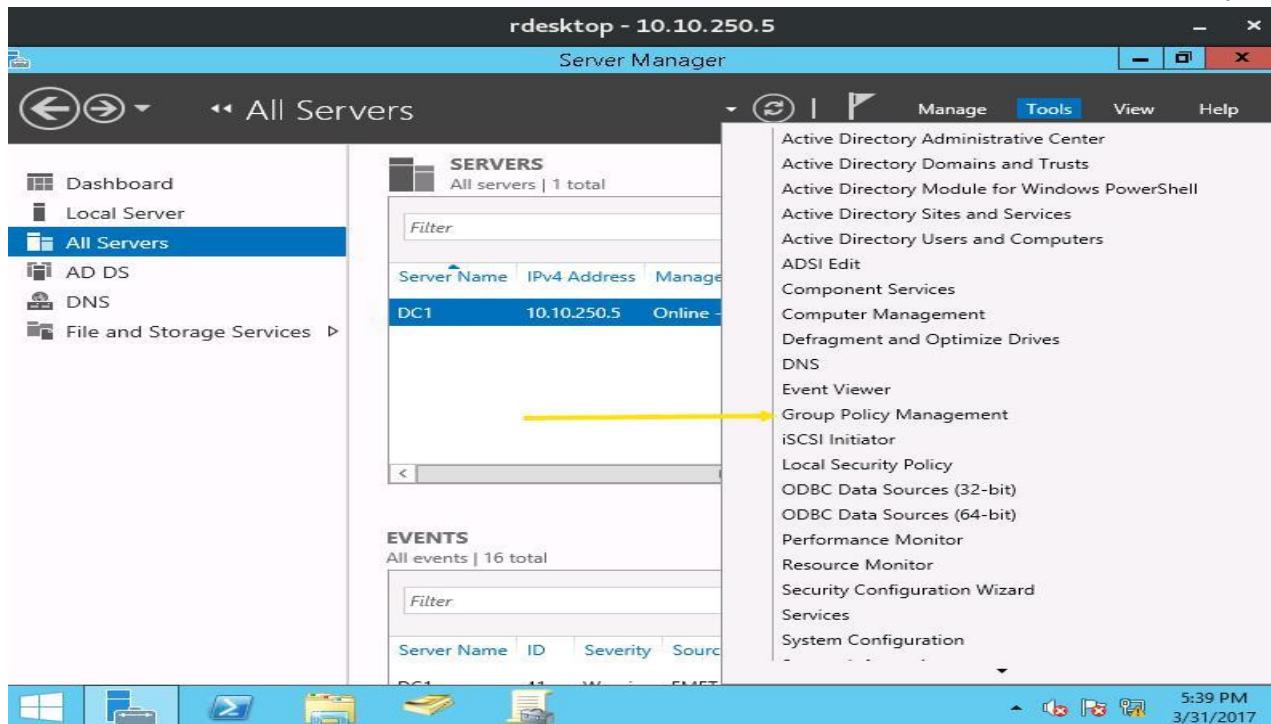


Task 2: Group Policy

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

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) Policy
 - Windows Firewall with Advanced Firewall Policies
 - Network List Manager Policies
 - Wireless Network (IEEE 802.11) Policy
 - Public Key Policies
 - Software Restriction 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

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
 - Security Options
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - Wired Network (IEEE 802.3) Policy
 - Windows Firewall with Advanced Firewall Policies
 - Network List Manager Policies
 - Wireless Network (IEEE 802.11) Policy
 - Public Key Policies
 - Software Restriction Policies

Accounts: Guest account status Properties

Security Policy Setting Explain

Accounts: Guest account status

Define this policy setting:

Enabled

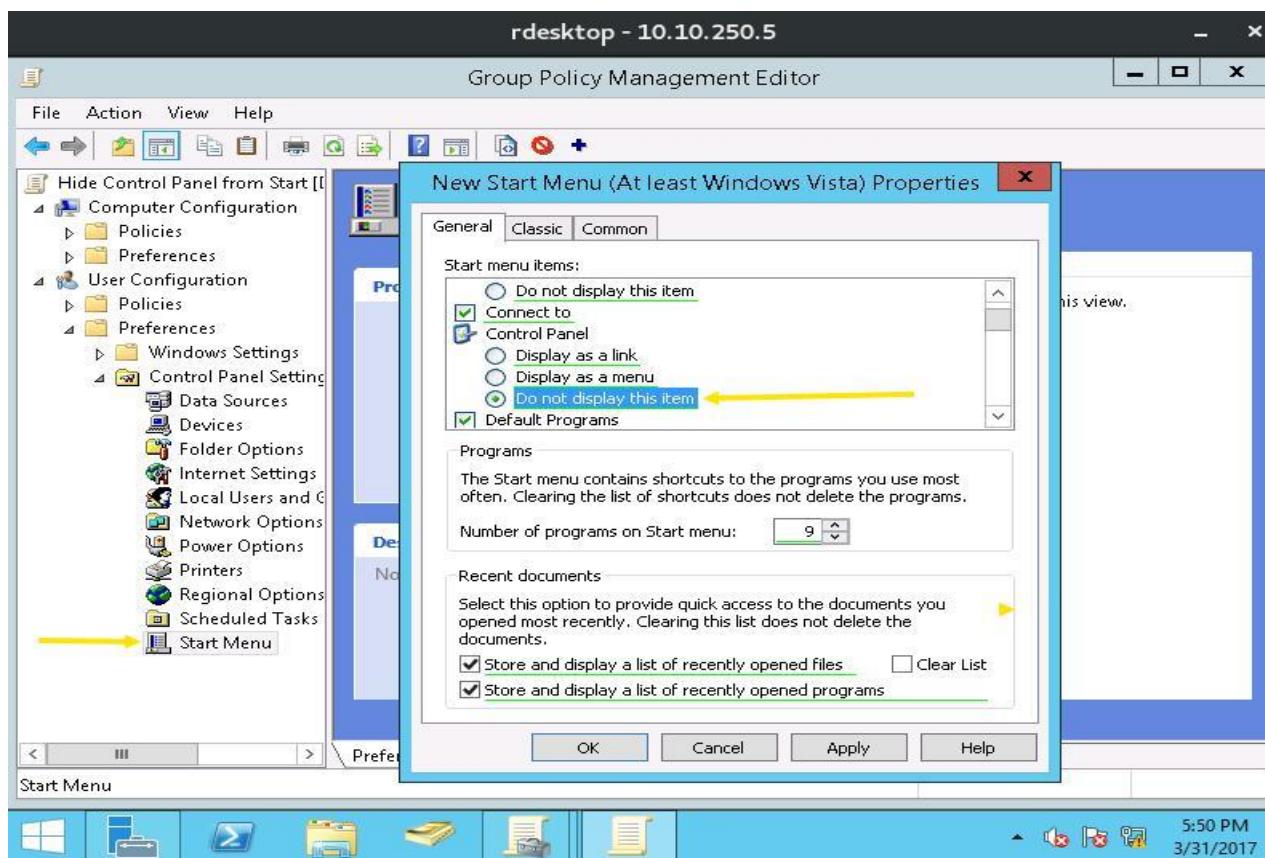
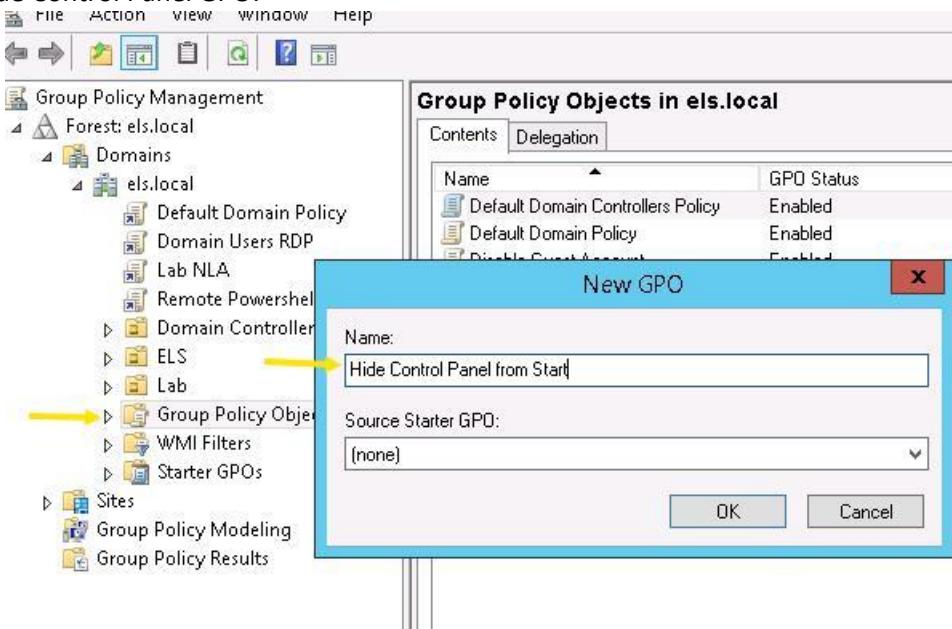
Disabled

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:

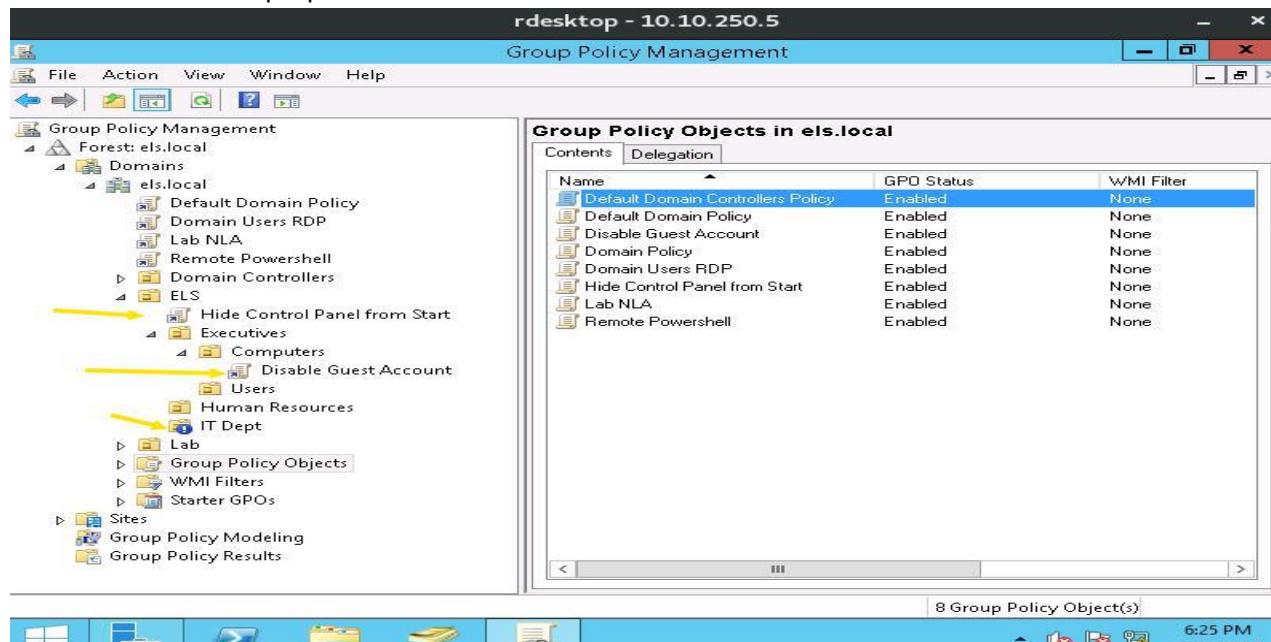


Task 2.3 Linking GPO's

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:

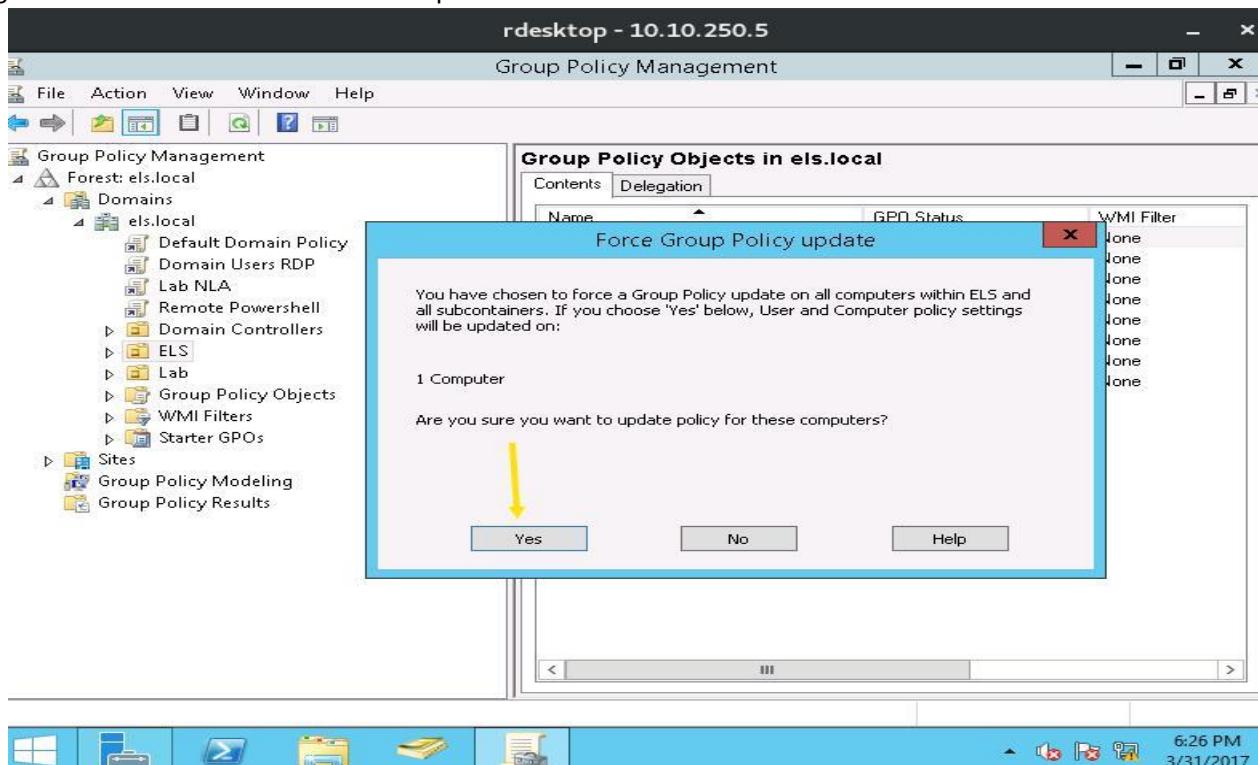


Task 3: Client Computers

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:

The screenshot shows a Windows PowerShell session on a remote desktop (rdesktop - 10.10.250.5) with several windows open. The top window displays the output of a command to get computers from a specific search base. A yellow arrow points to the command line. Below it, another window shows the same command output. A third window is a 'Windows PowerShell credential request' dialog box, prompting for a user name (els\student) and password. A yellow arrow points to the 'User name:' field. The bottom window shows the creation of a PowerShell session (\$session) using the \$cred object, which fails due to a WinRM connection error. It then attempts to invoke a command via the session, resulting in policy updates. Yellow arrows point to the success messages: 'User Policy update has completed successfully.' and 'Computer Policy update has completed successfully.'

```

PS C:\Users\elsstudent> $computers = Get-AdComputer -SearchBase "OU=ELS,DC=ELS,DC=local" -filt *
PS C:\Users\elsstudent> $computers

DistinguishedName : CN=Exec-1,OU=Computers,OU=Executives,OU=ELS,DC=els,DC=local
DNSHostName      : EXEC-1.els.local
Enabled          : True
Name             : Exec-1
ObjectClass      : computer
ObjectGUID       : b21c9c36-febd-4be2-a574-8d1ad1e84a66
SamAccountName   : EXEC-1$ 
SID              : S-1-5-21-762475095-3538646722-2674483501-1111
UserPrincipalName : 

DistinguishedName : CN=Exec-2,OU=Computers,OU=Executives,OU=ELS,DC=els,DC=local
DNSHostName      : EXEC-2.els.local
Enabled          : True
Name             : Exec-2
ObjectClass      : computer
ObjectGUID       : bb4cdcb41-a8e2-4340-a209-c3a5eb47388e
SamAccountName   : EXEC-2$ 
SID              : S-1-5-21-762475095-3538646722-2674483501-1112
UserPrincipalName : 

PS C:\Users\elsstudent> $computers = Get-AdComputer -SearchBase "OU=ELS,DC=ELS,DC=local" -filt *
PS C:\Users\elsstudent> $computers

DistinguishedName : CN=Exec-1,OU=Computers,OU=Executives,OU=ELS,DC=els,DC=local
DNSHostName      : EXEC-1.els.local
Enabled          : True
Name             : Exec-1
ObjectClass      : computer
ObjectGUID       : b21c9c36-febd-4be2-a574-8d1ad1e84a66
SamAccountName   : EXEC-1$ 
SID              : S-1-5-21-762475095-3538646722-2674483501-1111
UserPrincipalName : 

DistinguishedName : CN=Exec-2,OU=Computers,OU=Executives,OU=ELS,DC=els,DC=local
DNSHostName      : EXEC-2.els.local
Enabled          : True
Name             : Exec-2
ObjectClass      : computer
ObjectGUID       : bb4cdcb41-a8e2-4340-a209-c3a5eb47388e
SamAccountName   : EXEC-2$ 
SID              : S-1-5-21-762475095-3538646722-2674483501-1112
UserPrincipalName : 

PS C:\Users\elsstudent> $computers = Get-AdComputer -filt *
PS C:\Users\elsstudent> $cred = Get-Credential els\student

Windows PowerShell credential req...
Enter your credentials.
User name: els\student
Password: *****

OK Cancel

PS C:\Users\elsstudent> $session = New-PSSession -cn $computers.name -cred $cred
New-PSSession : [Exec-2] Connecting to remote server Exec-2 failed with the following error message : WinRM cannot process the request. The following error occurred while using Kerberos authentication: Cannot find the computer Exec-2. Verify that the computer exists on the network and that the name provided is spelled correctly. For more information, see the about_Remote_Troubleshooting Help topic.
At line:1 char:12
+ $session = New-PSSession -cn $computers.name -cred $cred
+               + CategoryInfo          : OpenError: (System.Management...RemoteRunspace:RemoteRunspace) [New-PSSession], PSRemotingTransportException
+               + FullyQualifiedErrorId : NetworkPathNotFound,PSSessionOpenFailed
PS C:\Users\elsstudent> $session

Id Name           ComputerName     State      ConfigurationName Availability
-- --            -----          -----      -----          -----
1 Session1       Exec-1          Opened     Microsoft.PowerShell Available

PS C:\Users\elsstudent>
PS C:\Users\elsstudent> Invoke-Command -Session $session -ScriptBlock {gpupdate /force}
Updating Policy...

User Policy update has completed successfully. ←
Computer Policy update has completed successfully.

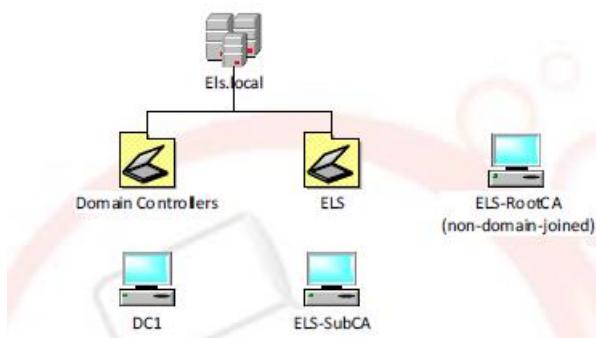
PS C:\Users\elsstudent>

```

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.

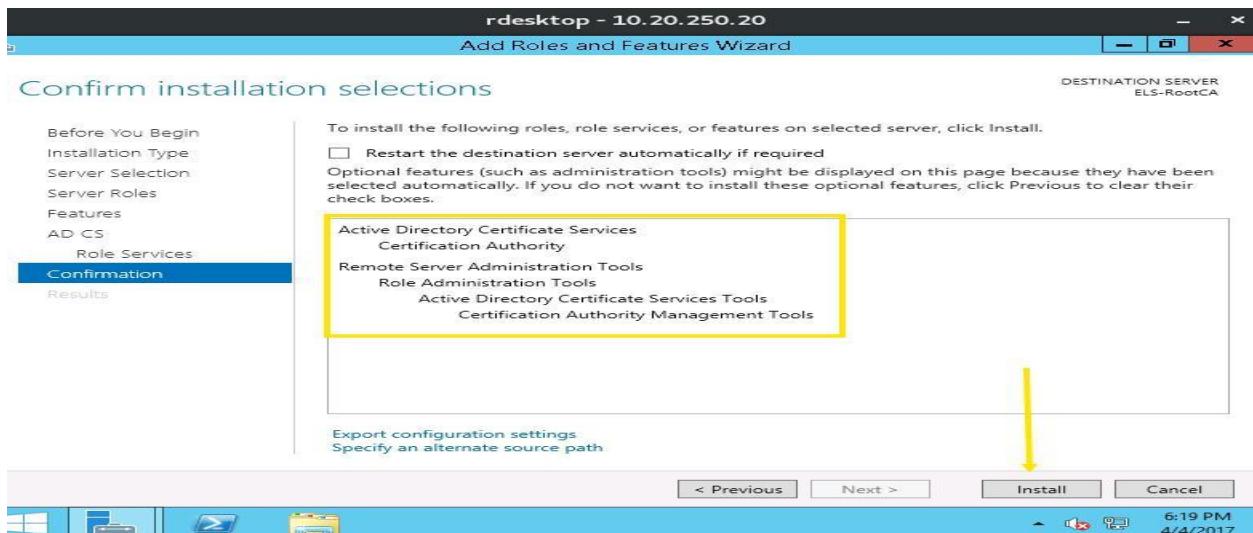
Task 1: Offline Root Certificate Authority

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

Task 1.1: Install Active Directory Certificate Services

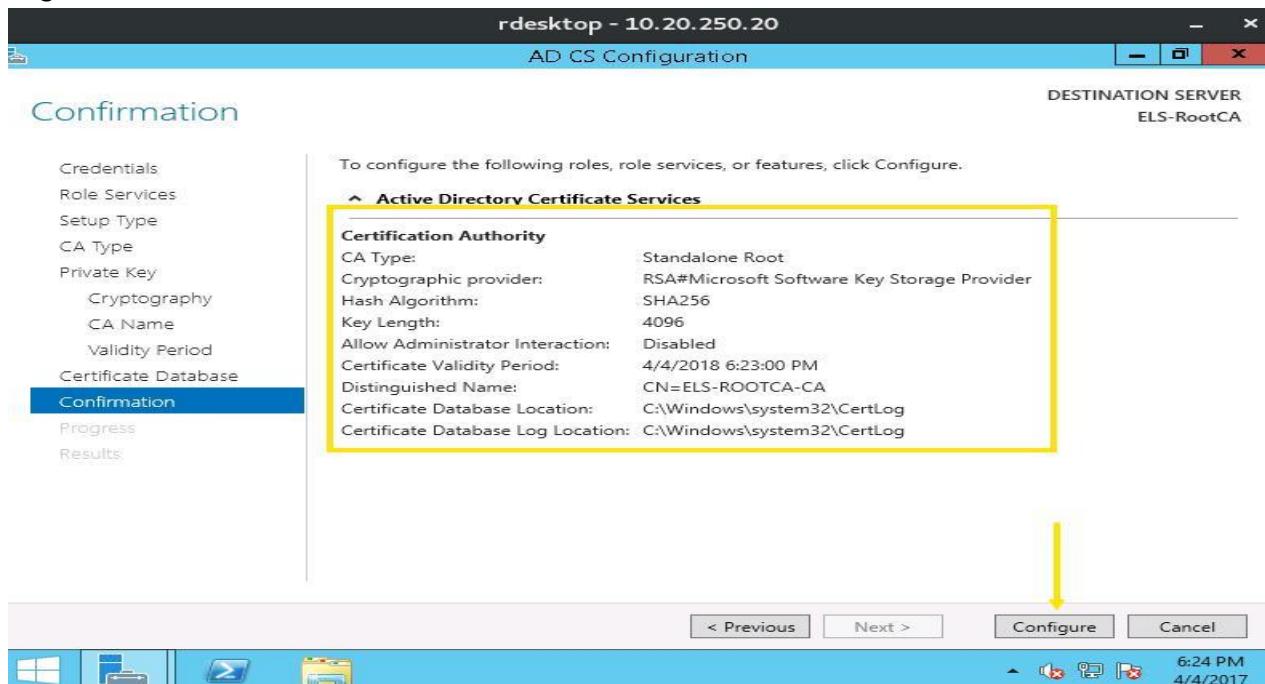
Install the Active Directory Certificate Services role with no additional role services.

✓ I installed ADCS:

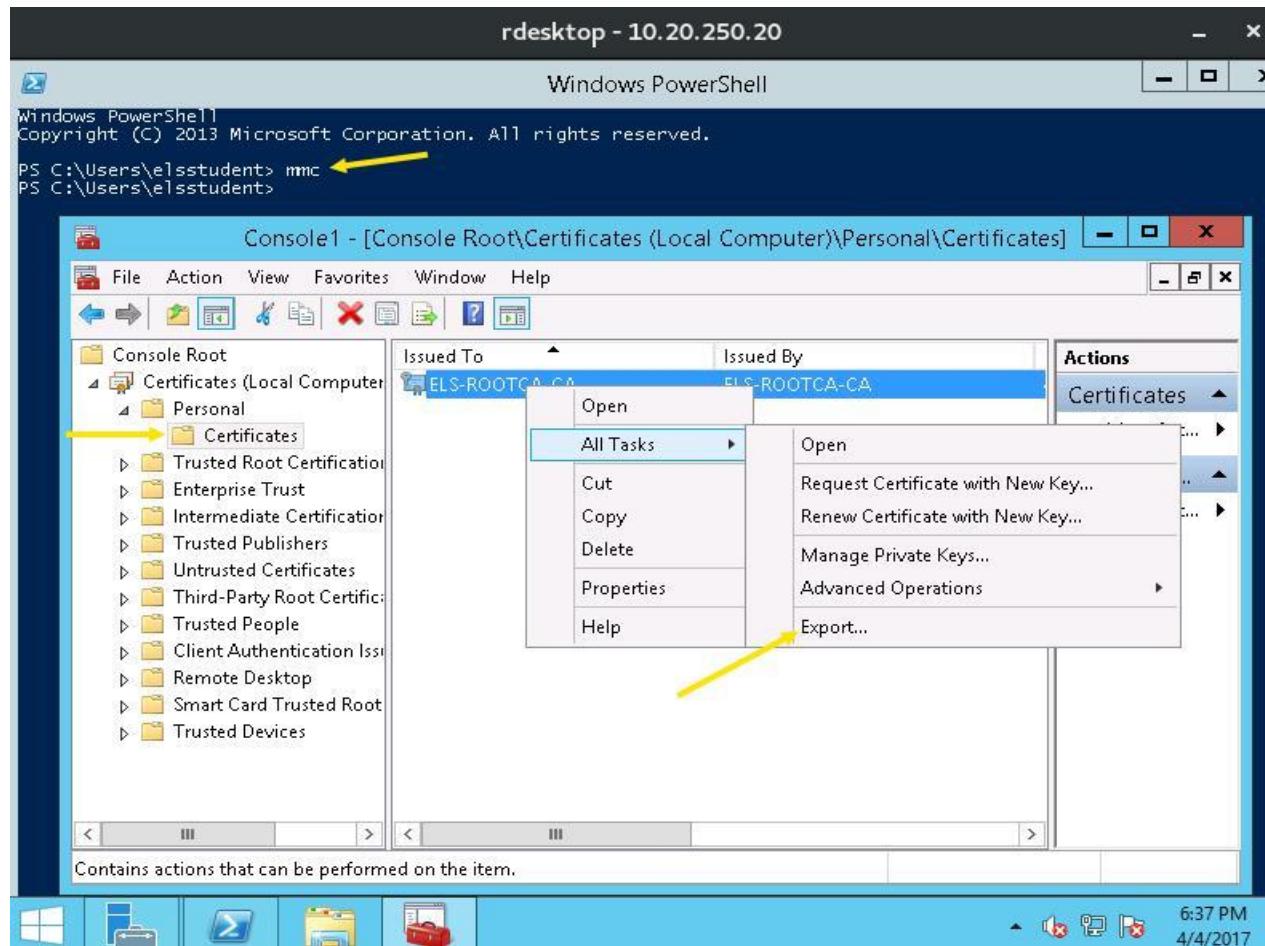


Task 1.2: Configure Certificate Services

- ✓ I configured ADCS:

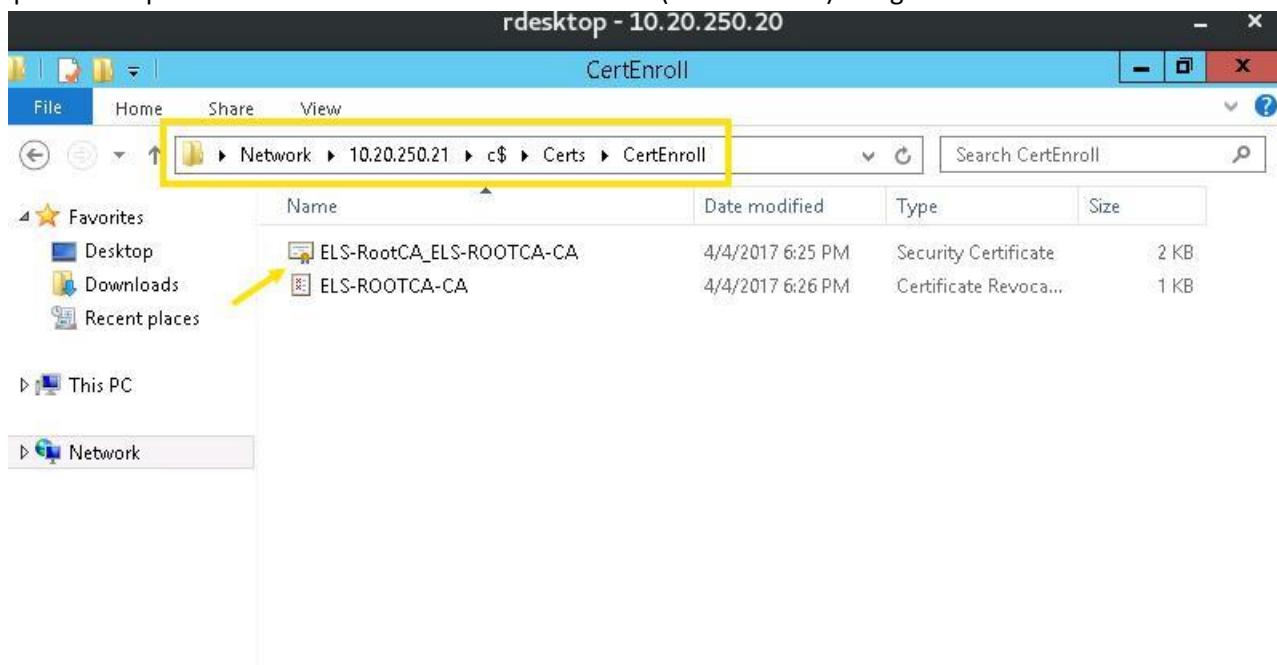
**Task 1.3: Export Root CA Certificates**

- ✓ Export the certificate:





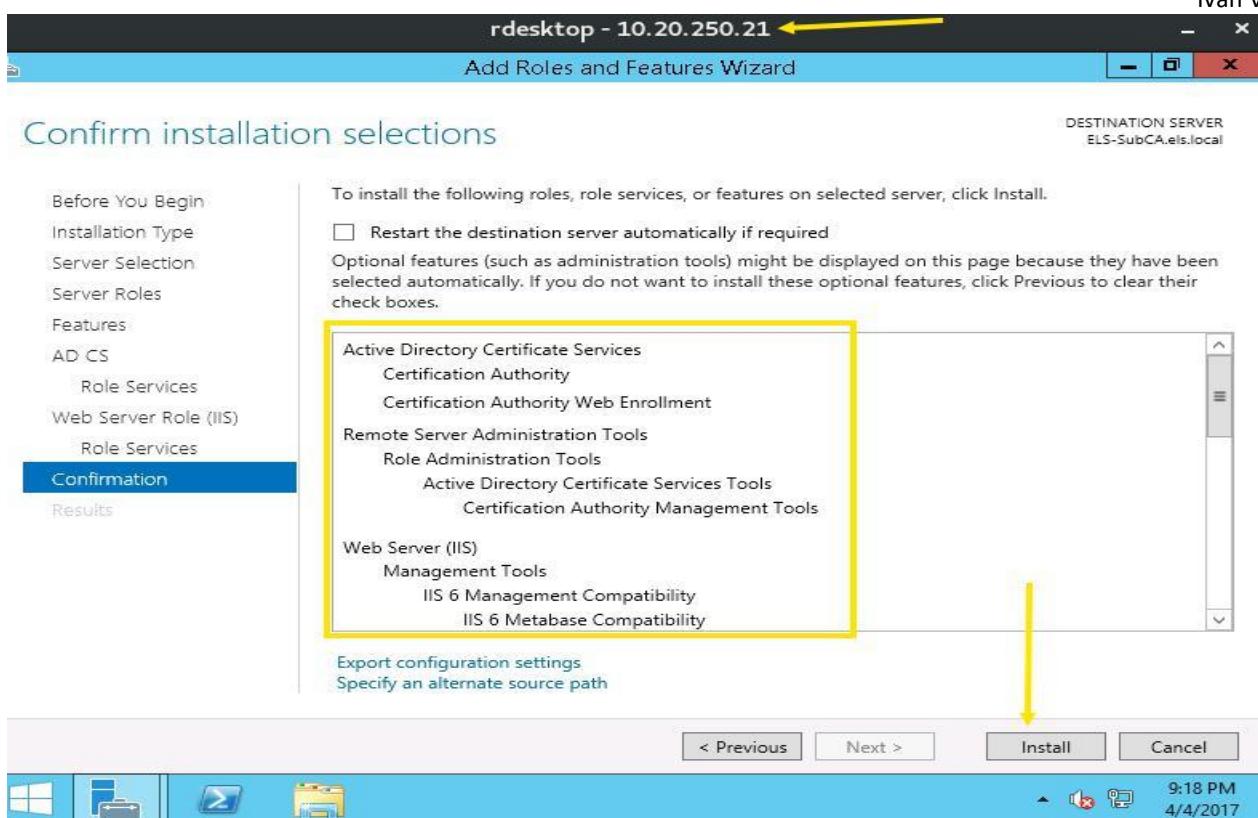
- ✓ I copied the exported certificate & files to the SubCa host (10.20.250.21) using admin share:



Task 2: Subordinate Certificate Authority

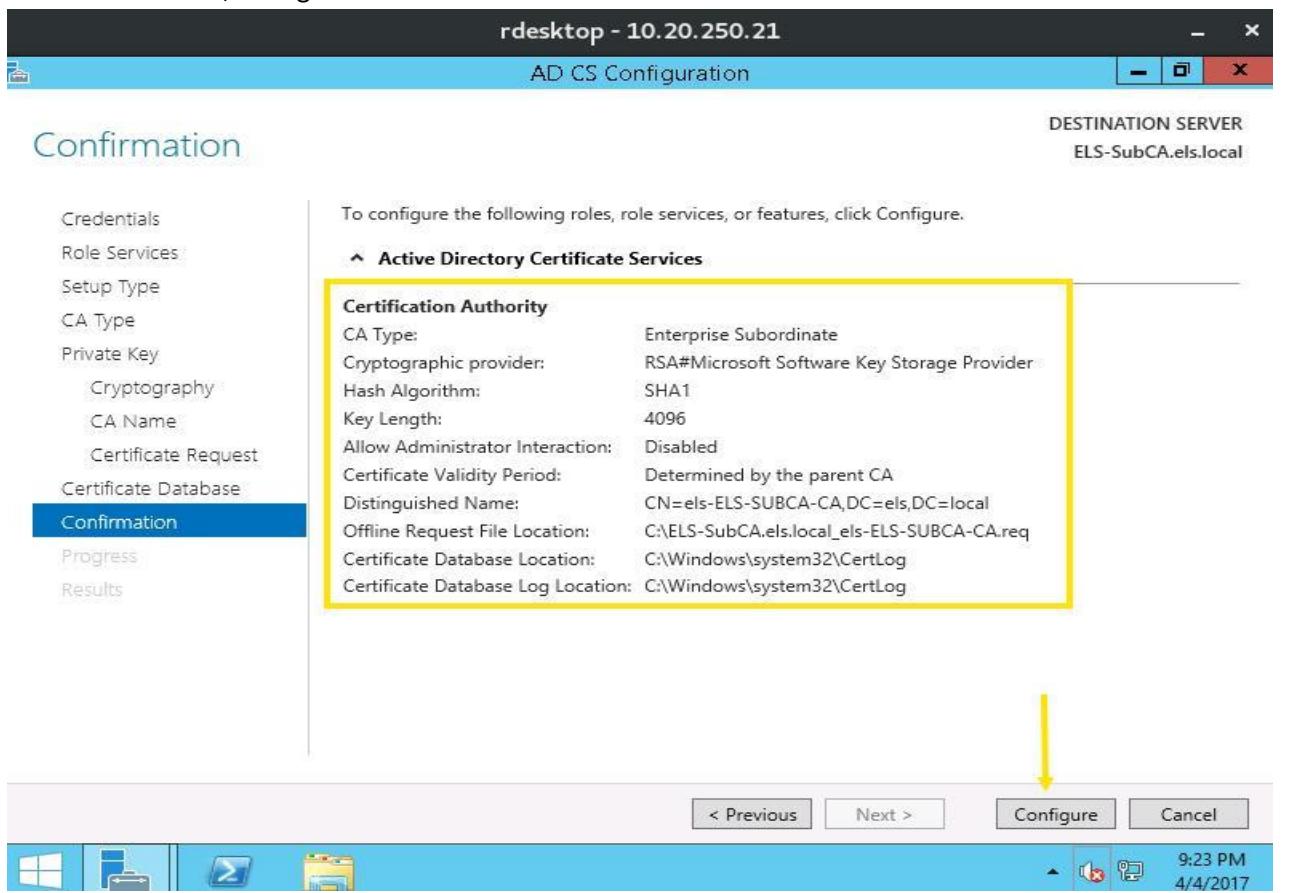
Task 2.1: Installing Certificate Services

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



Task 2.2: Configuring Certificate Services

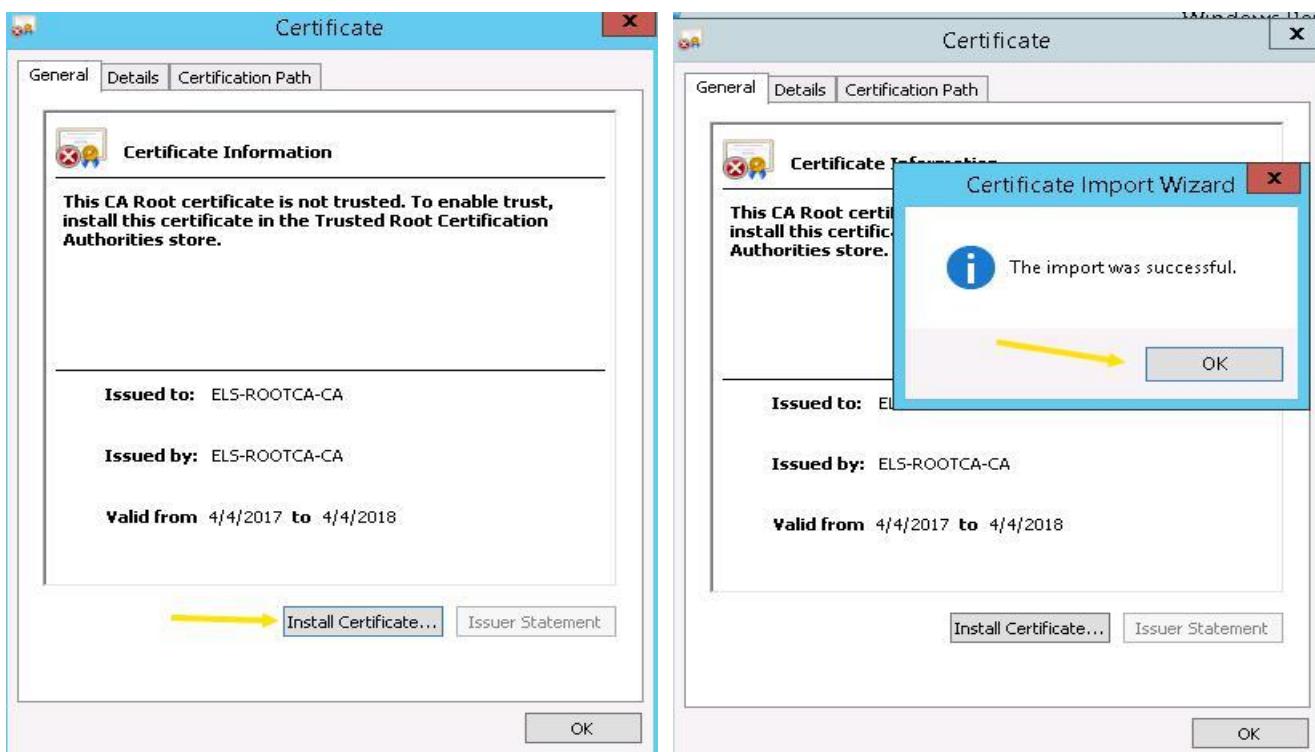
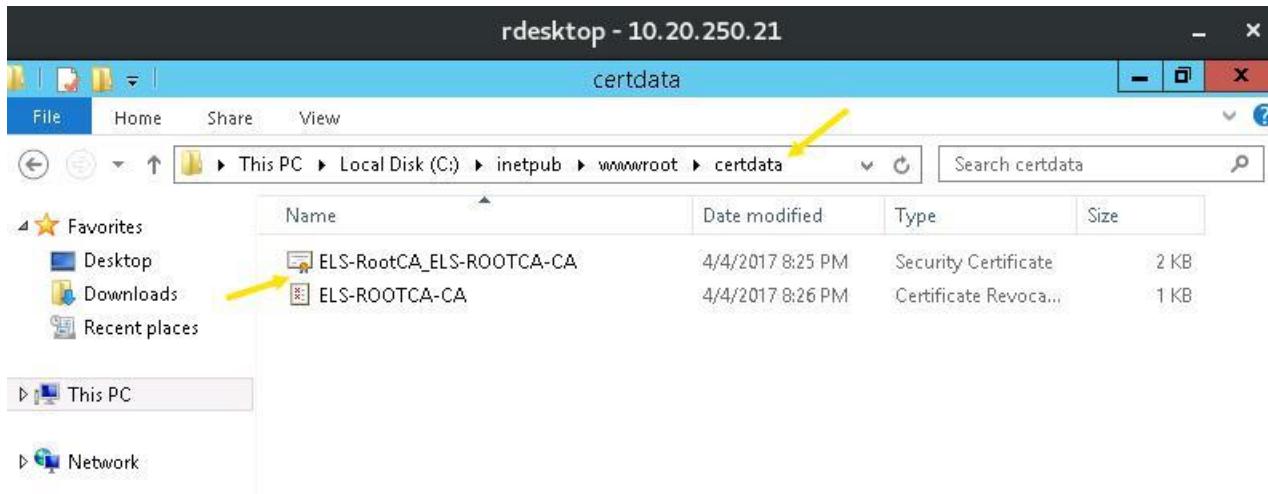
- ✓ Once installed, configure the role:



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:

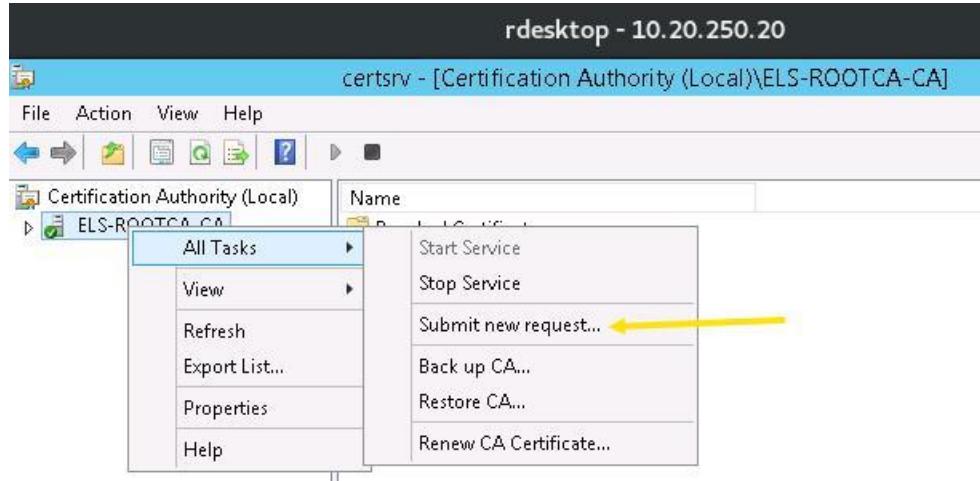


- ✓ I then added the CRL to the local store:

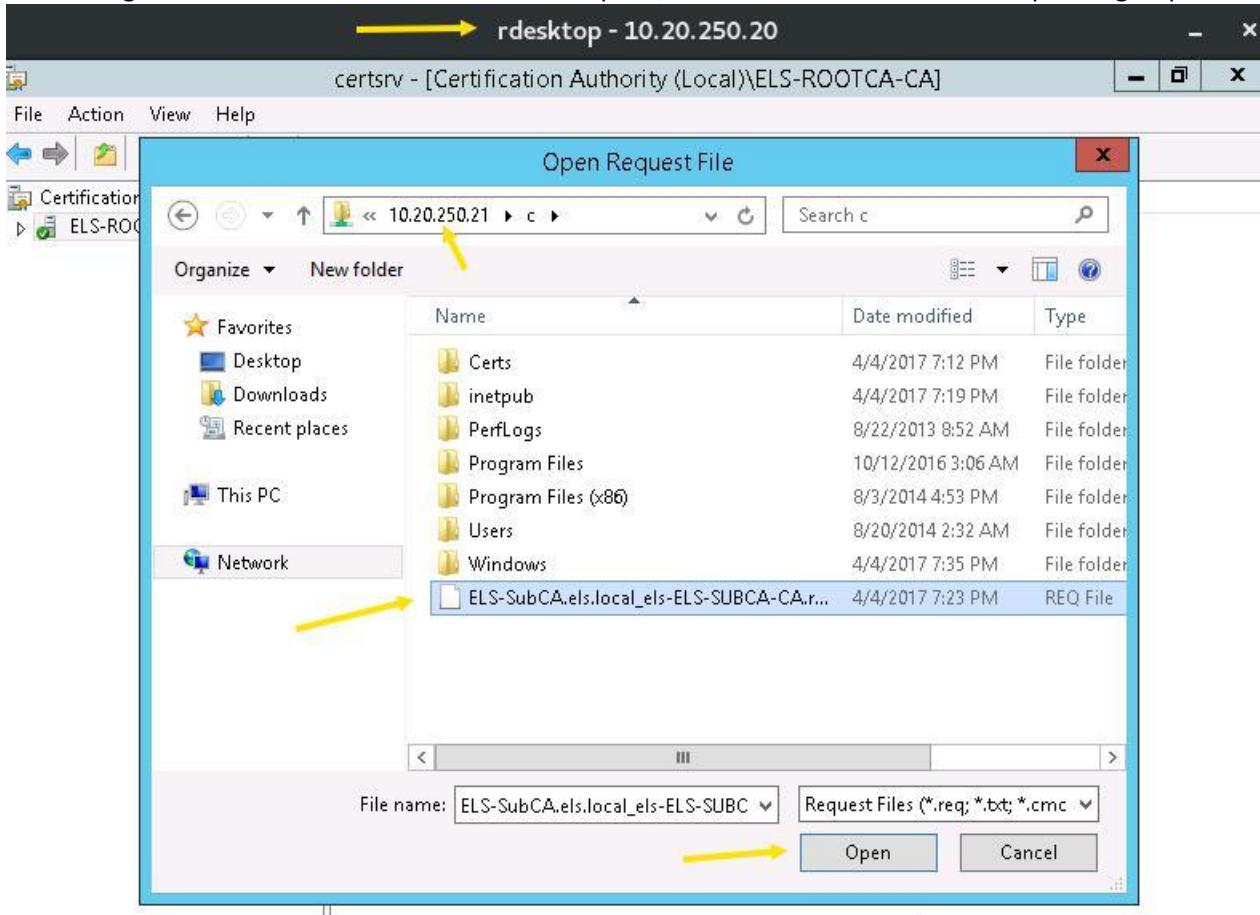
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

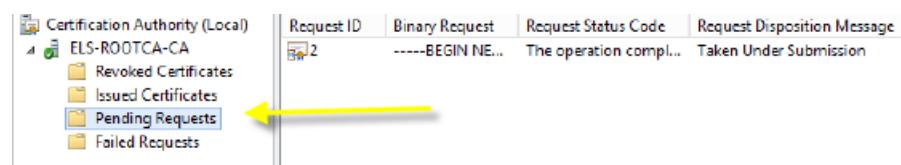
PS C:\Windows\system32> certutil -addstore root "C:\Certs\CertEnroll\ELS-ROOTCA-CA.crl"
root "Trusted Root Certification Authorities"
CRL "CN=ELS-ROOTCA-CA" added to store.
CertUtil: -addstore command completed successfully.
PS C:\Windows\system32> NiCE!
```

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

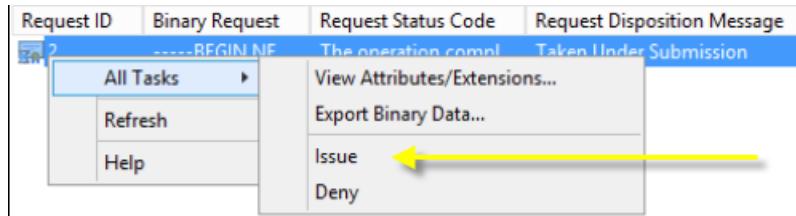


I then had to navigate to where I stored the SubCA file request, via admin share & refresh the pending requests:





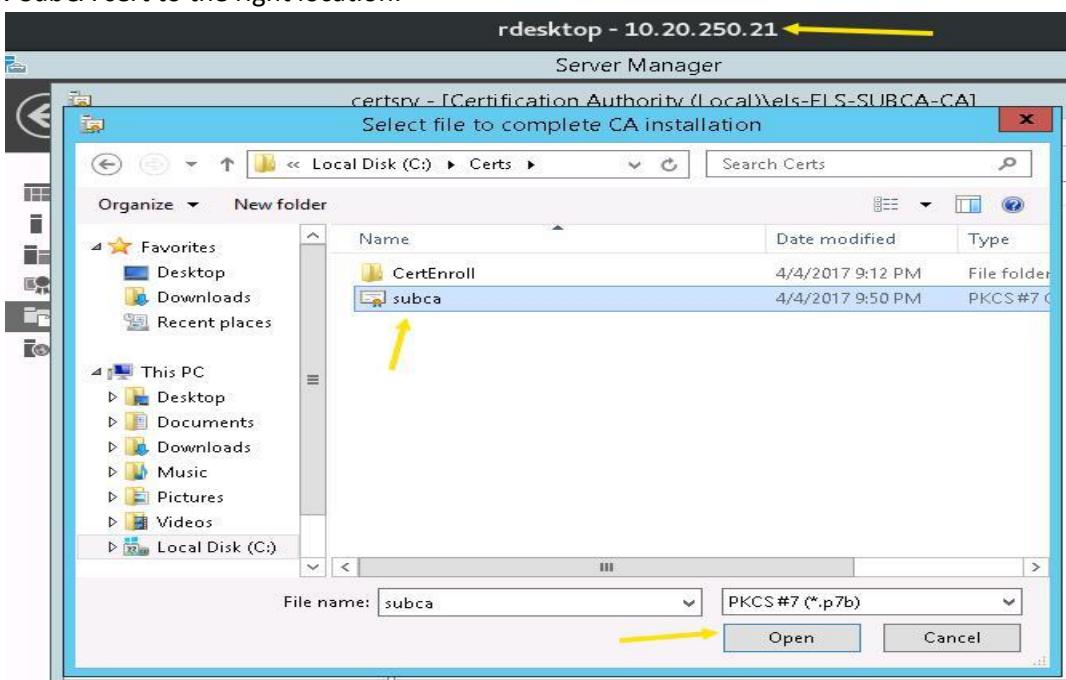
- ✓ I then issued the SubCA:



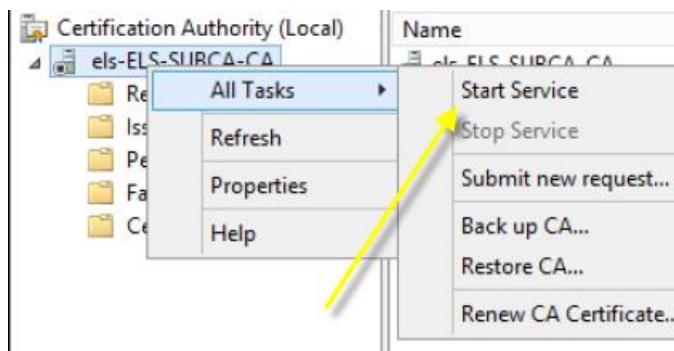
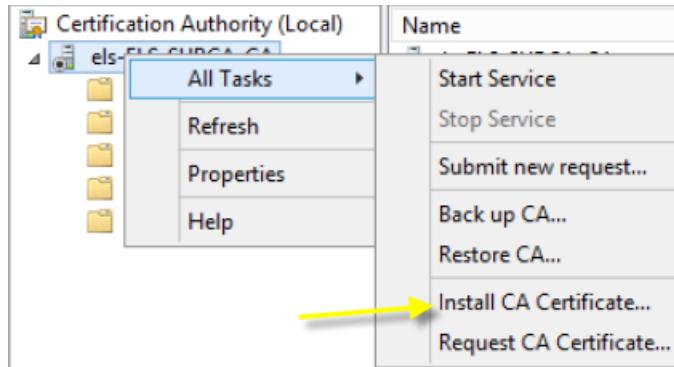
- ✓ I changed the format to P7B and included all the certificates in the path:



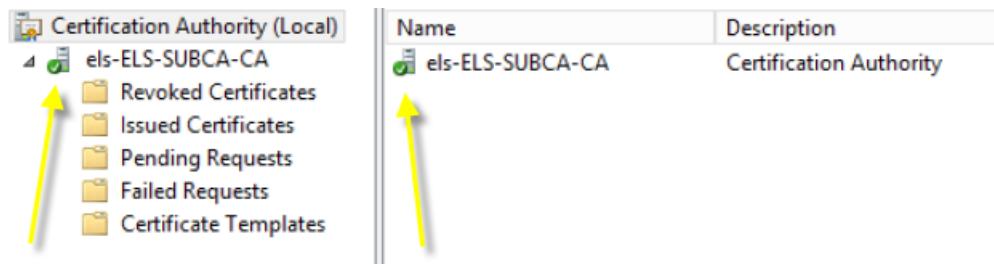
- ✓ Put the new SubCA cert to the right location:



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



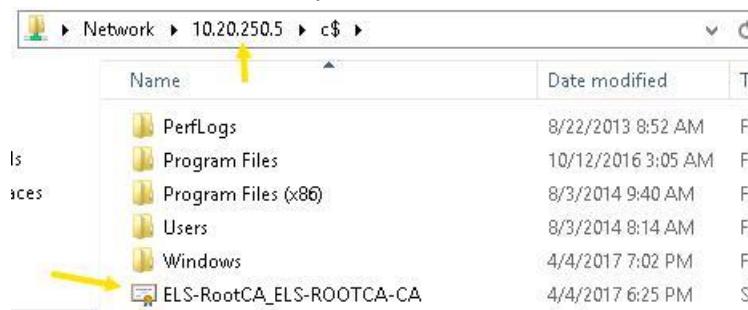
- ✓ We got the green check mark!



Task 3: Deploying Root Certificate

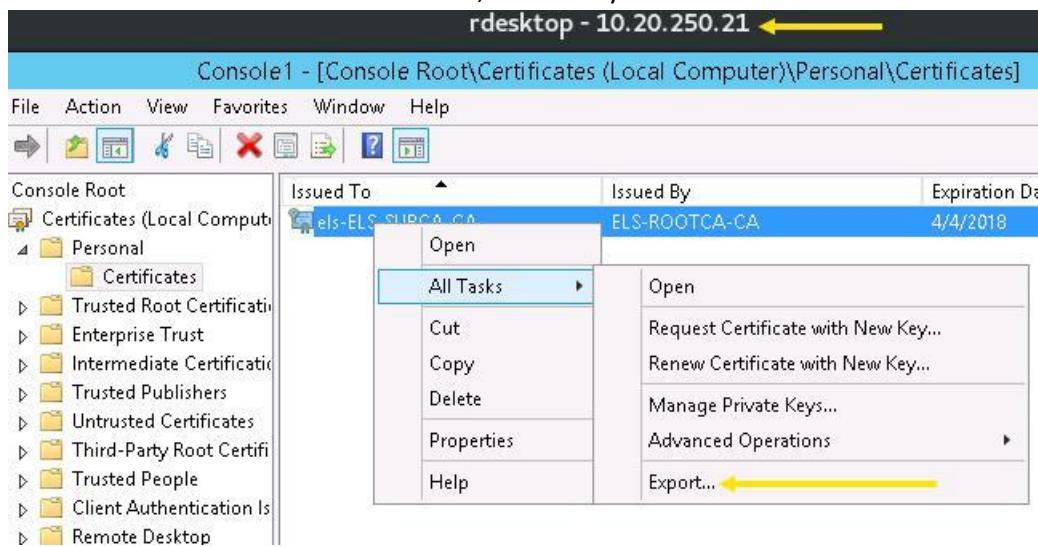
Task 3.1: Export Root CA to domain controller

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



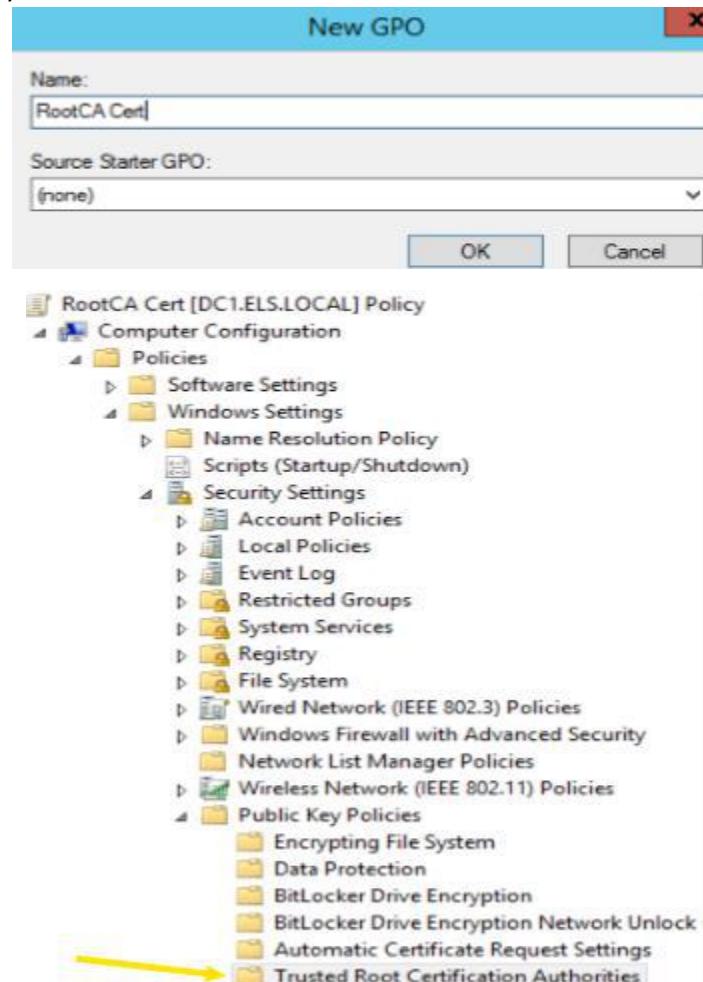
Task 3.2: Check if DC1 Trusts the Subordinate CA

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

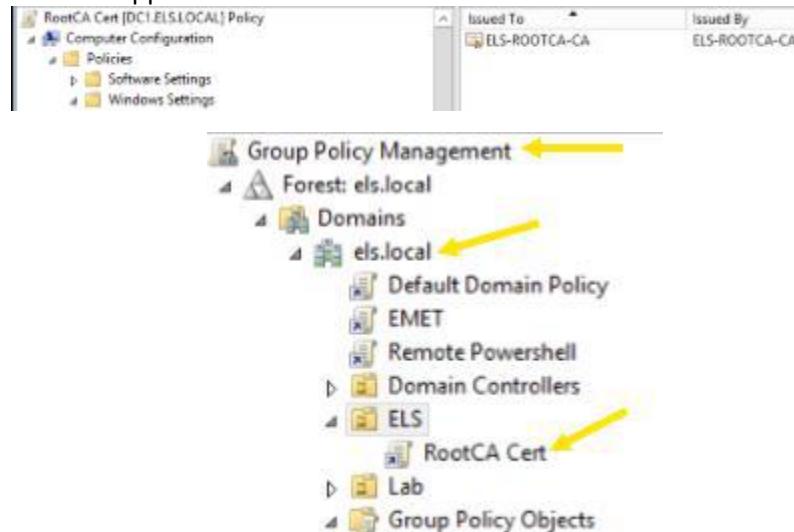


Task 3.3: Deploy Certificate with Group Policy

- ✓ 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.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\elsstudent>gpupdate /force
Updating policy...

Computer Policy update has completed successfully. ←
User Policy update has completed successfully. ←

C:\Users\elsstudent>_
```

The screenshot shows a Windows command prompt window titled 'cmd' with the path 'C:\Windows\system32\cmd.exe'. It displays the output of the 'gpupdate /force' command. Two yellow arrows point to the lines 'Computer Policy update has completed successfully.' and 'User Policy update has completed successfully.'.

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

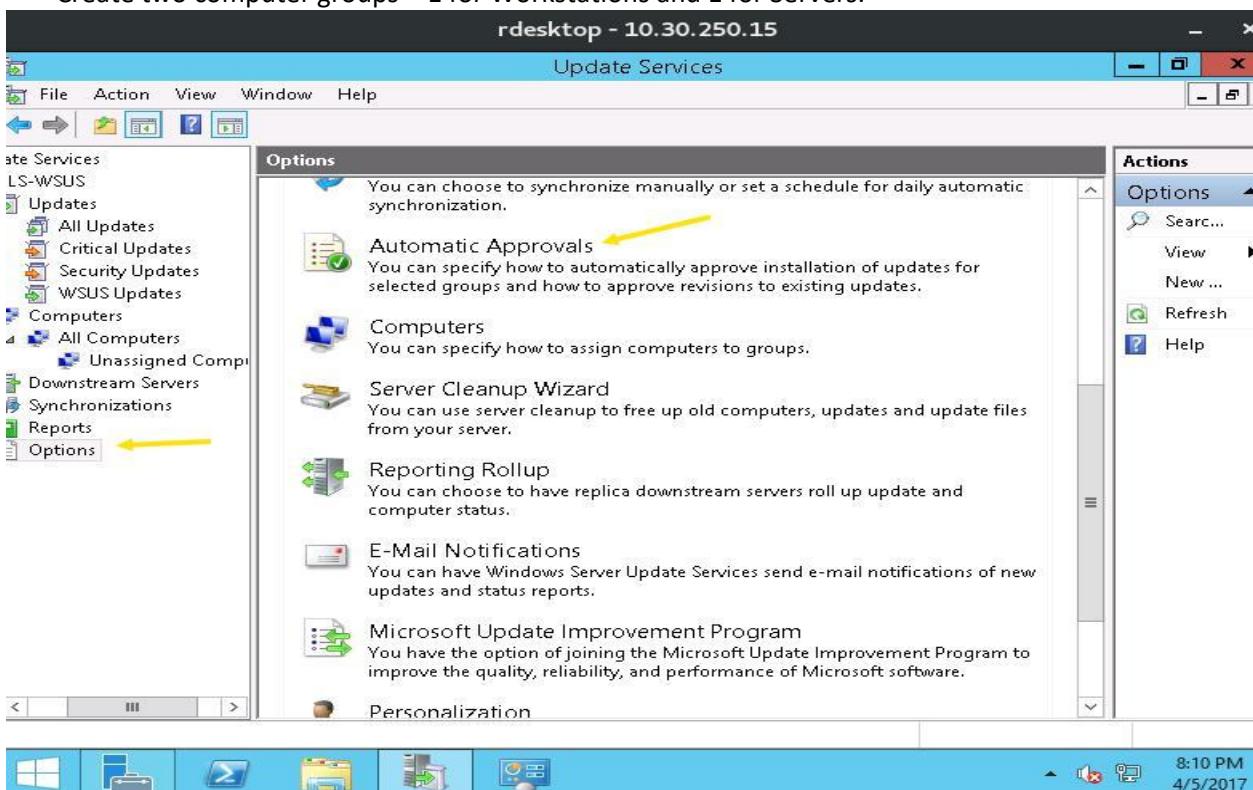
- Labs machines are not connected to the Internet, they are in a private testing environment just for you.
- The domain controller is dc1.els.local at 10.30.250.5
- The update server is at 10.30.250.15.
- The client machine (Win 7) is at 10.30.250.150
- The WSUS role is already installed on the update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

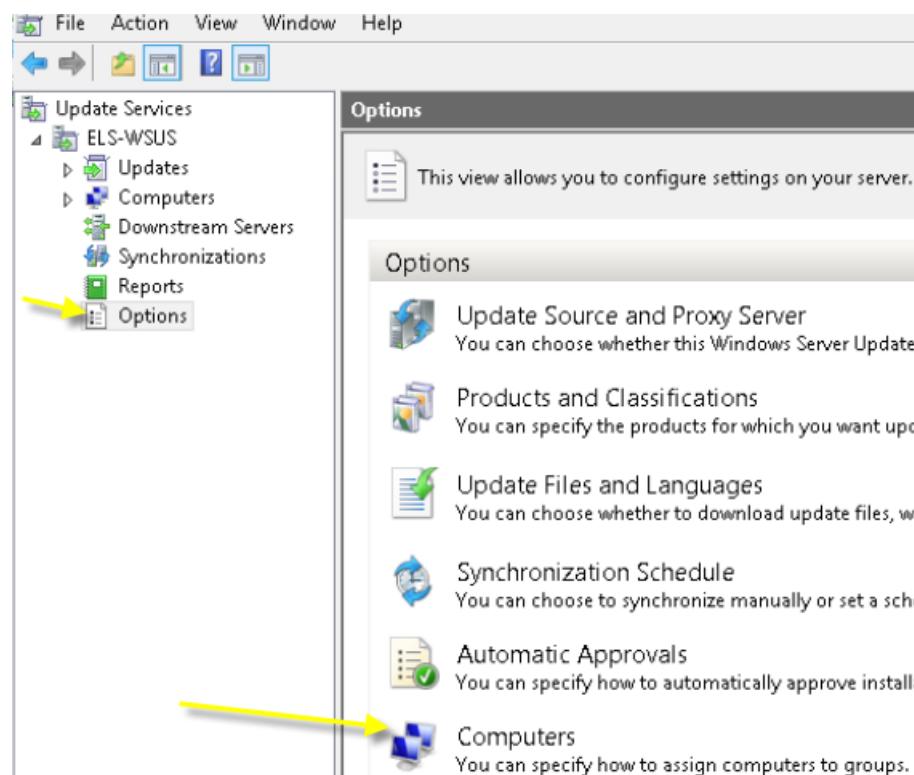
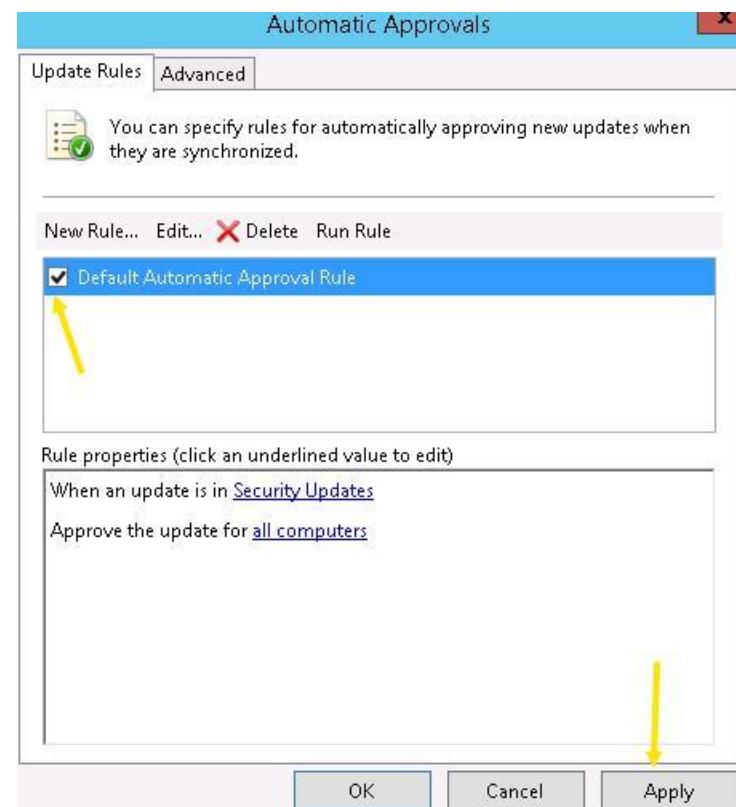
Task 1: Configure WSUS

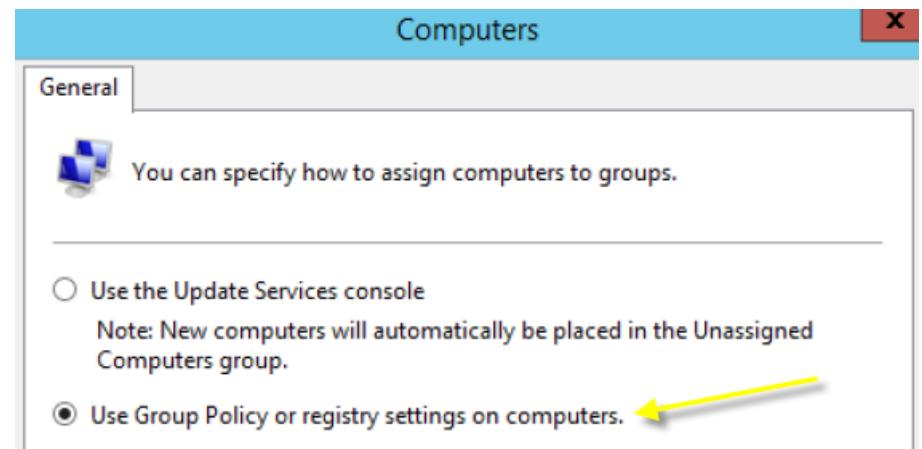
Task 1.1: Configure WSUS

- ✓ 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.







Products and Classifications

This screenshot shows the 'Products and Classifications' interface. The 'Products' tab is selected. It includes a note about specifying products for synchronization and a list of products under 'Products:'.

- Windows Small Business Server 2008 Migration Preparation
- Windows Small Business Server 2008
- Windows Small Business Server 2011 Standard
- Windows
 - EU Browser Choice Update-For Europe Only
 - Windows 2000
 - Windows 7

A yellow arrow points to the checked checkbox for 'Windows 7'.

- ✓ I selected all updated for approval:

The screenshot shows the 'Update Services' management interface. On the left, the navigation tree is expanded to show 'Updates' under 'ELS-WSUS'. A yellow arrow points to the 'All Updates' link. On the right, a table titled 'All Updates' lists 11 updates out of 1628 total, all of which are marked as 'Not approved'.

Title	Classification	Instal...	Approval
Security Update for Internet Explorer 11 for Windows Ser...	Security Updat...	0%	Not approved
Cumulative Security Update for Internet Explorer 11 for ...	Security Updat...	0%	Not approved
Security Update for Windows Server 2012 R2 (KB2965788)	Security Updat...	0%	Not approved
Security Update for Windows Server 2012 R2 (KB2964736)	Security Updat...	0%	Not approved
Security Update for Windows Server 2012 R2 (KB2939576)	Security Updat...	0%	Not approved
Security Update for Windows Server 2012 R2 (KB2957189)	Security Updat...	0%	Not approved
Security Update for Microsoft .NET Framework 4.5.1 on ...	Security Updat...	0%	Not approved
Security Update for Internet Explorer 11 for Windows Ser...	Security Updat...	0%	Not approved
Security Update for Windows Server 2012 R2 (KB2928120)	Security Updat...	0%	Not approved
Security Update for Windows Server 2012 R2 (KB2926765)	Security Updat...	0%	Not approved
Security Update for Windows Server 2012 R2 (KB2978668)	Security Updat...	0%	Not approved

To approve multiple updates, select the group from this list, click the arrow, and choose the type of approval. If you want a child group to inherit the existing approvals of its parent group, choose Same as Parent. If you want all child groups of a parent to inherit its approvals, click Apply to Children on the parent group.

Computer Group	Approval	Deadline
All Computers	Install	None
Unassigned Computers	Keep existing approvals	

Approval completed without errors. See below for details.

Action	Result
Approving Security Update for Microsoft .NET Framework 4.5.1 on Windows 8.1 and W...	Success
Approving Security Update for Windows Server 2012 R2 (KB2957189) for installation to ...	Success
Approving Security Update for Windows Server 2012 R2 (KB2939576) for installation to ...	Success
Approving Security Update for Windows Server 2012 R2 (KB2964736) for installation to ...	Success
Approving Security Update for Windows Server 2012 R2 (KB2965788) for installation to ...	Success
Approving Cumulative Security Update for Internet Explorer 11 for Windows Server 201...	Success
Approving Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB2964...	Success
Approving Security Update for Windows Server 2012 R2 (KB2928120) for installation to ...	Success

Pause Cancel Close

- ✓ 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.

New GPO

Name:

Source Starter GPO:

OK Cancel

The screenshot shows the Group Policy Management Editor. On the left, a tree view lists various policy categories. A yellow arrow points to the 'Windows Update' node under 'Work Folders'. Another yellow arrow points to the 'Configure Automatic Updates' setting in the main pane, which is part of a larger list of policy settings.

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.

The screenshot shows the Group Policy Management interface. It displays a hierarchy of OUs: Forest: els.local > Domains > els.local > ELS > Servers and Workstations. Two GPOs are applied: 'WSUS - Servers' to the 'Servers' OU and 'WSUS - Workstations' to the 'Workstations' OU. Yellow arrows point to each of these GPOs.

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.

A screenshot of a Windows PowerShell window titled "rdesktop - 10.30.250.15". The window shows the following command history:

```

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\elsstudent> gpupdate
gpupdate : The term 'gpupdate' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ gpupdate
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (gpupdate:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\elsstudent> gpupdate
Updating policy...

Computer Policy update has completed successfully. ←
User Policy update has completed successfully. ←

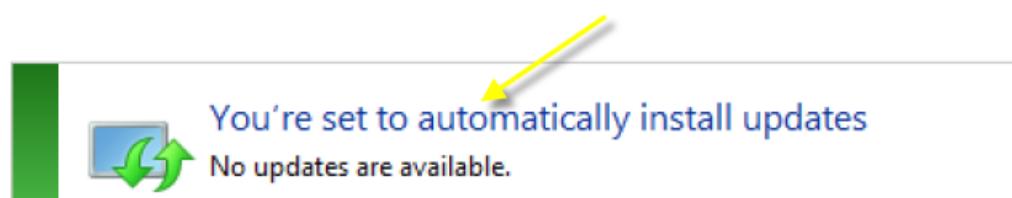
PS C:\Users\elsstudent> NICE!_
```

The window includes a taskbar at the bottom with icons for File Explorer, Task View, Start, Taskbar settings, and a search bar. The system tray shows the date and time as 8:39 PM 4/5/2017.

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.

Windows Update



Most recent check for updates: Never

Updates were installed: Never

You receive updates: Managed by your system administrator

[Check online for updates from Windows Update](#)



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%

Status

	Updates with errors:	0
Updates needed:	26	Group membership: All Computers
Updates installed/not applicable:	1585	OS: Windows Server 2012 R2 Standard
Updates with no status:	0	OS language: en-US

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

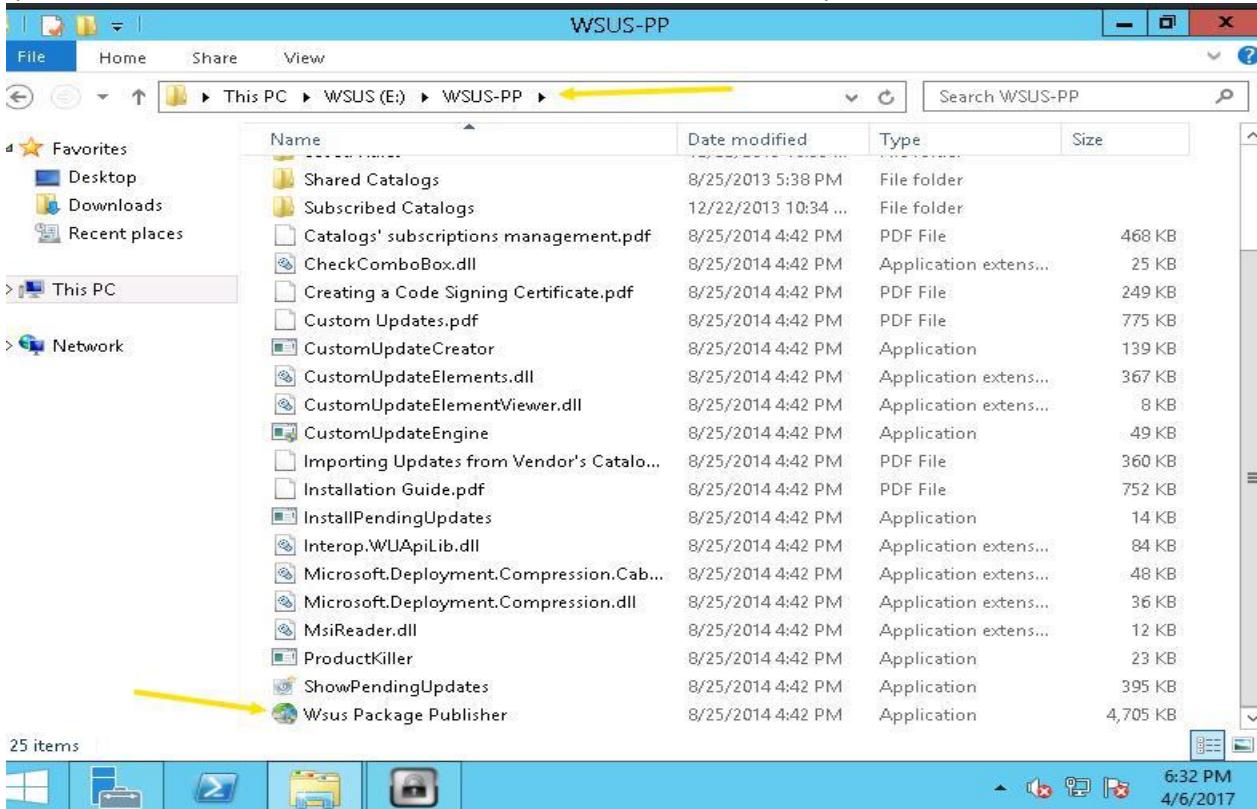
- ✓ Import the software protection profiles into EMET and ensure Deep Hooks plus Stop on Exploit are enabled.

Process ...	Process Name	Running EMET
2884	csrss	
2332	dllhost - COM Surrogate	
672	dwm - Desktop Window Manager	
2464	dwm - Desktop Window Manager	
3600	EMET_Agent - EMET_Agent	
3640	EMET_GUI - EMET GUI	

Task 3: Deploy EMET

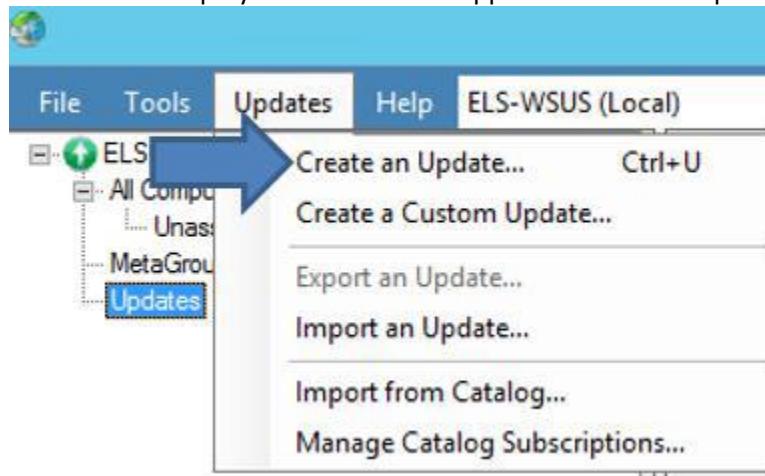
Task 3.1: Setup Windows Package Publisher

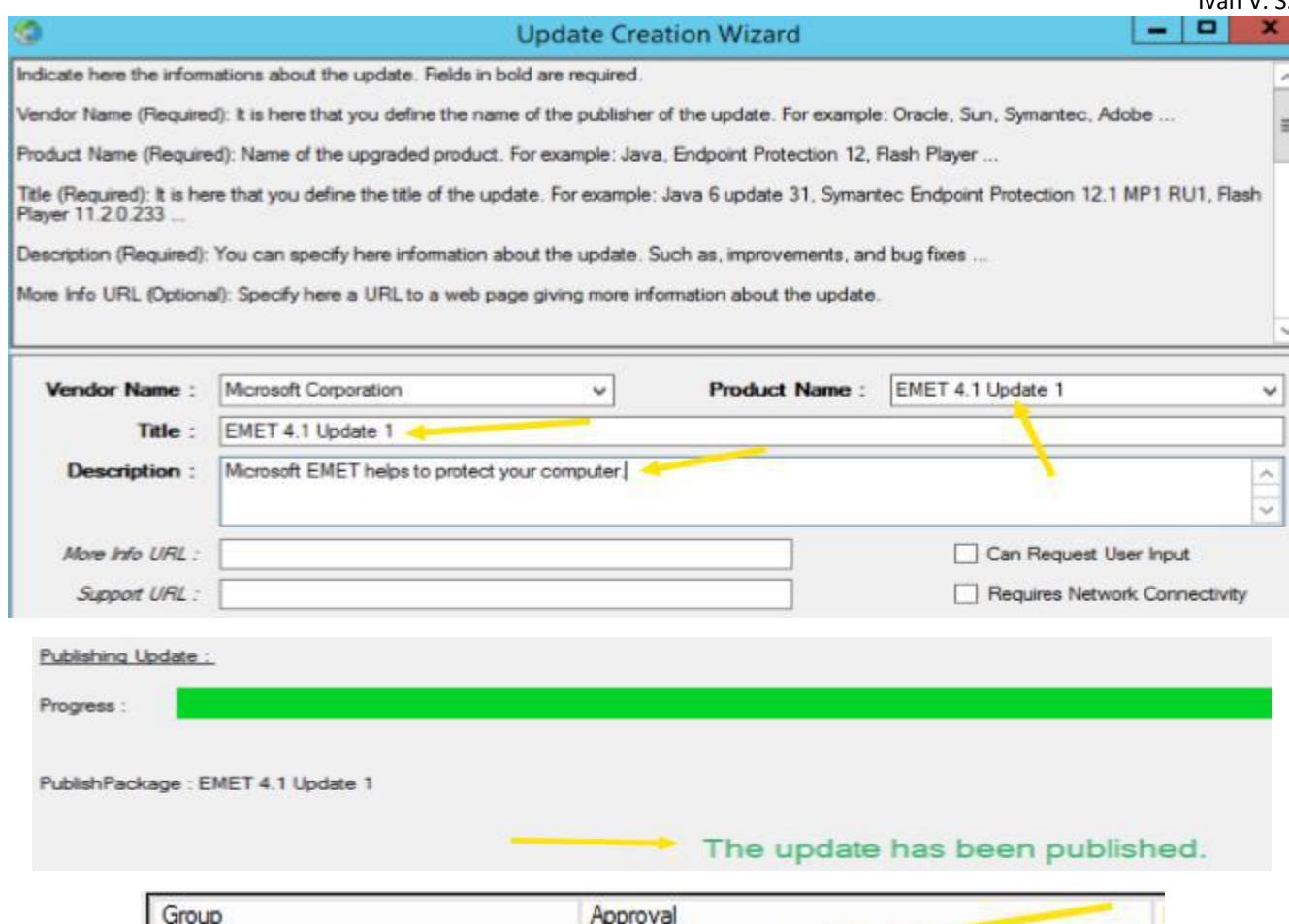
- ✓ Setup WPP which is located on the E: drive and connect it with the locally installed WSUS.



Task 3.2: Configure EMET deployment

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

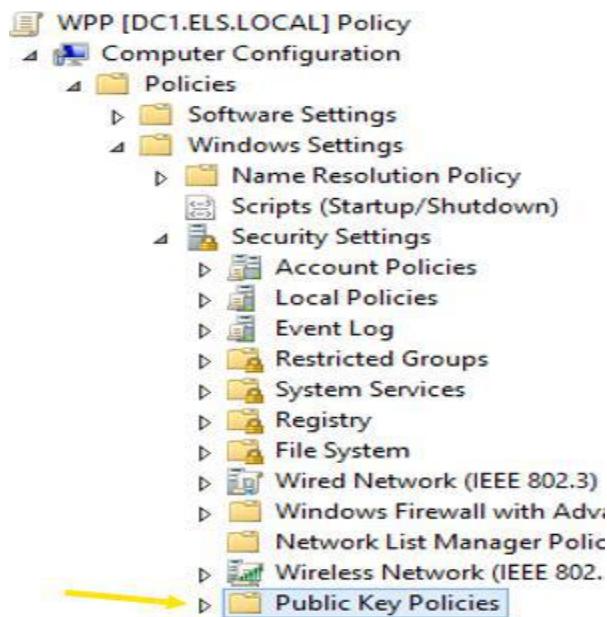




Group	Approval
All Computers	Approve For Installation
Unassigned Computers	Unchanged

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.

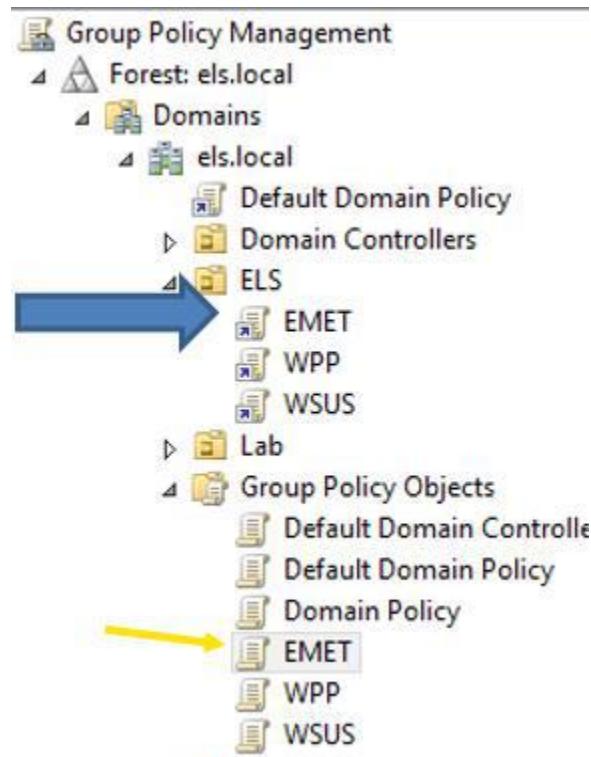


The screenshot shows two windows side-by-side. The left window is titled 'Group Policy Management' and displays a tree view of a domain structure. The right window is titled 'WPP [DC1.ELS.LOCAL] Policy' and shows a list of Group Policy Objects (GPOs) with columns for 'Issued To' and 'Issued By'. A yellow arrow points from the 'Group Policy Management' window to the 'WPP' GPO in the 'Issued To' column of the right window.

Group Policy Management

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

Setting	State
System ASLR	Enabled
Default Action and Mitigation Settings	Enabled
EMET Agent Visibility	Not configured
Application Configuration	Enabled
System DEP	Enabled
Default Protections for Internet Explorer	Enabled
Default Protections for Recommended Software	Enabled
Default Protections for Popular Software	Enabled
Reporting	Enabled
System SEHOP	Enabled
EMET Agent Custom Message	Enabled



Task 4: Deployment

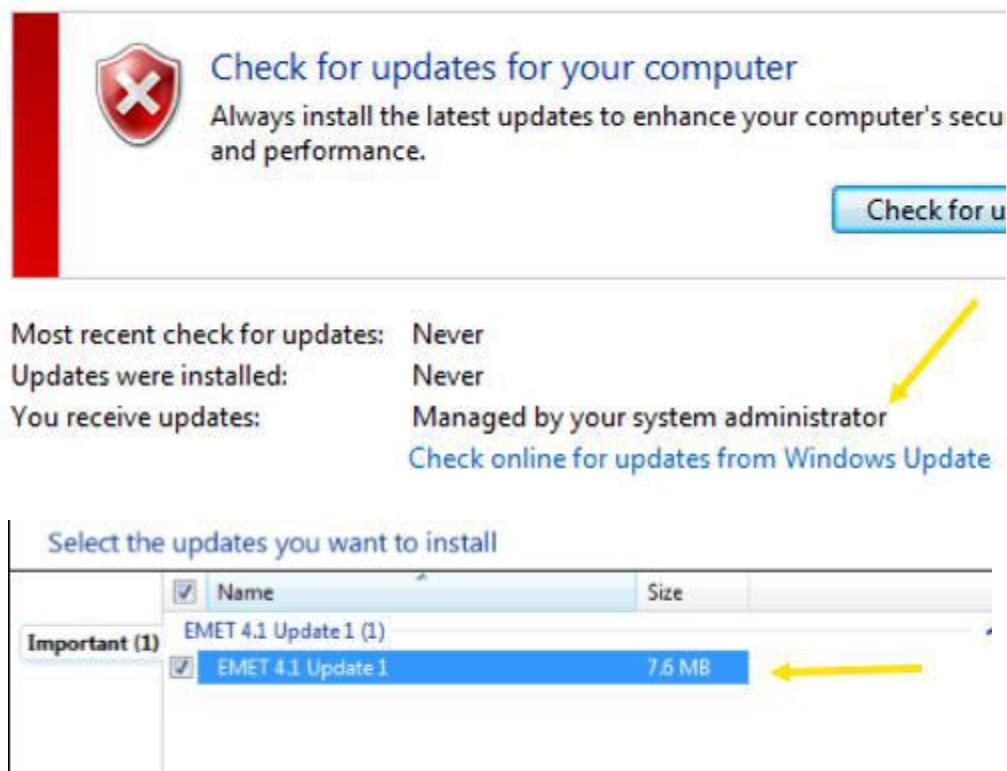
Task 4.1: Workstation Install

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

```
C:\Users\elsadmin>gpupdate /force
Updating Policy...
User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

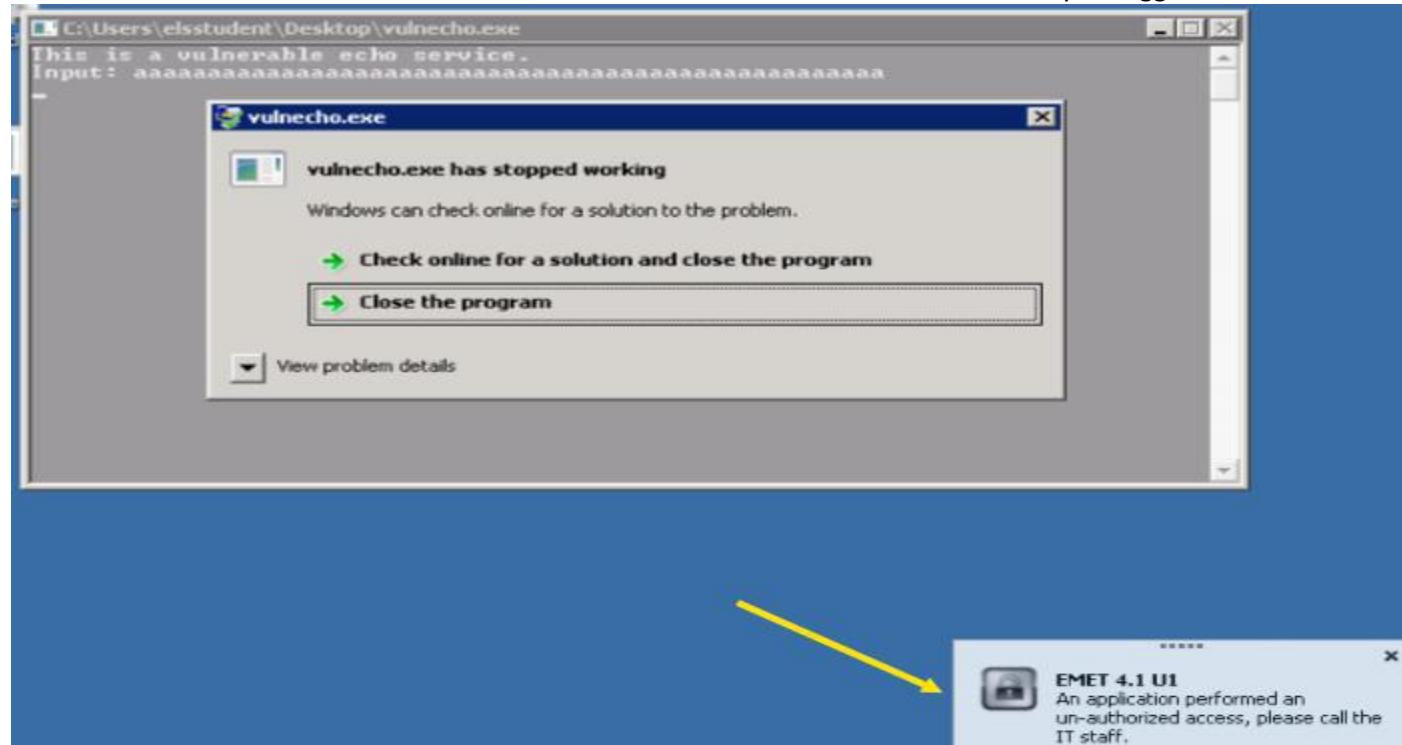
A yellow arrow points from the bottom right of the text area to the word 'successfully' in the final line of the command output.

Windows Update



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

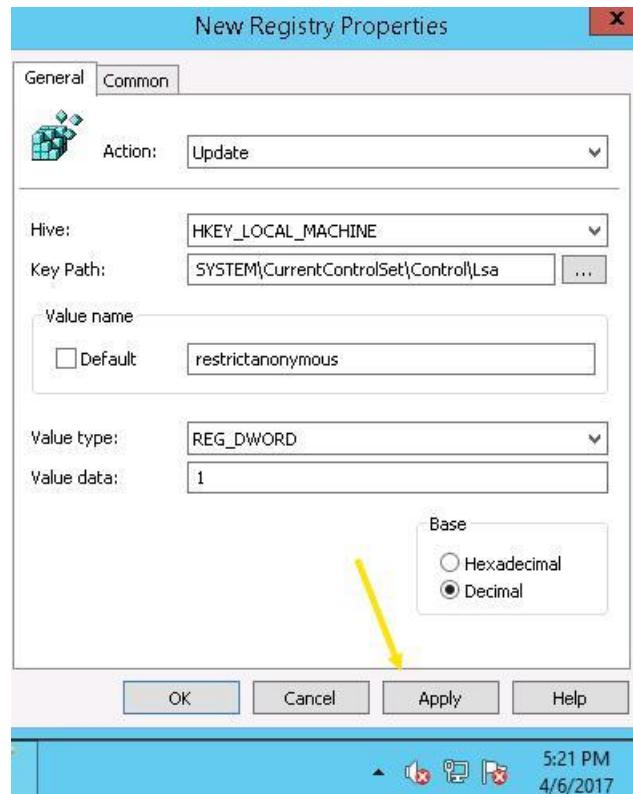
The first step of this lab is to setup the GPOs as described. Each task should have its own GPO created; do not combine them all into one GPO.

Task 1.1: Null sessions

- ✓ Create a GPO which disables null sessions.

The screenshot shows the 'Group Policy Management Editor' window titled 'rdesktop - 10.50.250.5'. The left pane displays the GPO structure under 'Computer Configuration' > 'Policies' > 'Local Policies' > 'Security Options'. The right pane lists policy settings with their current state. Several settings are highlighted with yellow arrows pointing to them, indicating they are being modified or checked. The highlighted settings include:

Policy Setting	Current State
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined
Microsoft network client: Send unencrypted password to third-party SMB ser...	Not Defined
Microsoft network server: Amount of idle time required before suspending se...	Not Defined
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Not Defined
Microsoft network server: Digitally sign communications (if client agrees)	Not Defined
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts an...	Enabled
Network access: Do not allow storage of passwords and credentials for netwo...	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Not Defined
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Not Defined
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to this computer to u...	Not Defined



Task 1.2: RDP Timeout – 30 minutes

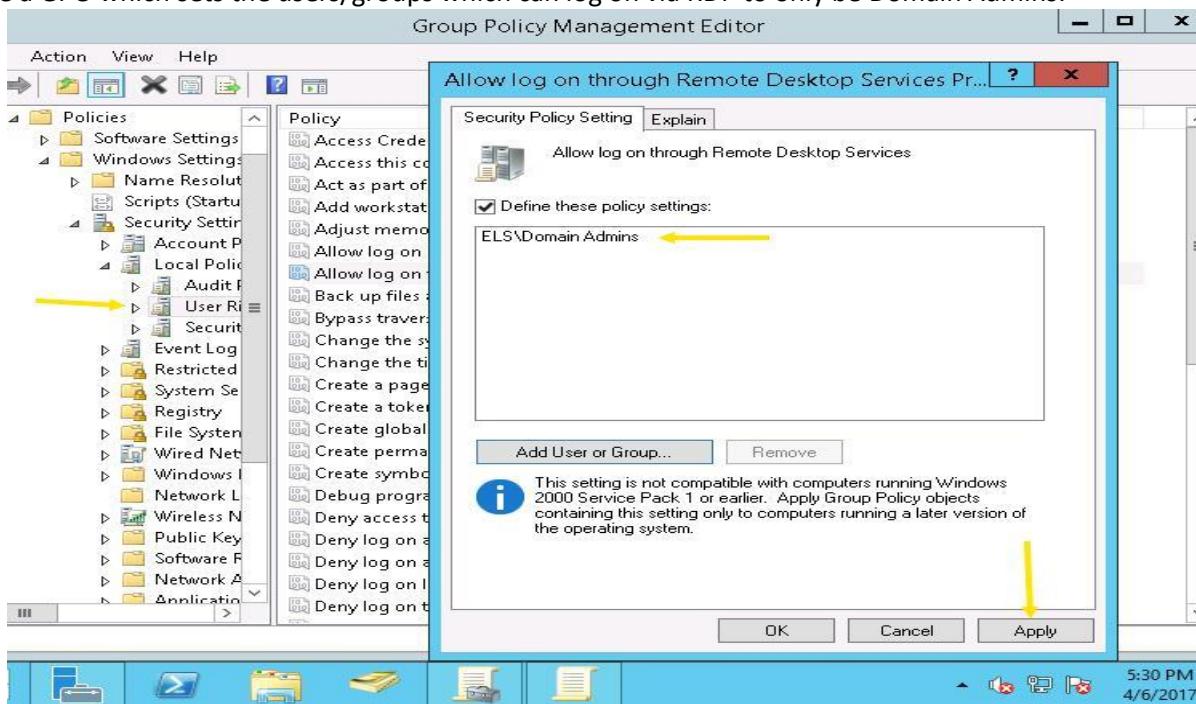
- ✓ Create a GPO which ends all inactive and disconnected RDP sessions after **30 minutes**. Set it to terminate the session once the timeout has been reached. Also set the **RDP encryption** level to **HIGH**.

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.

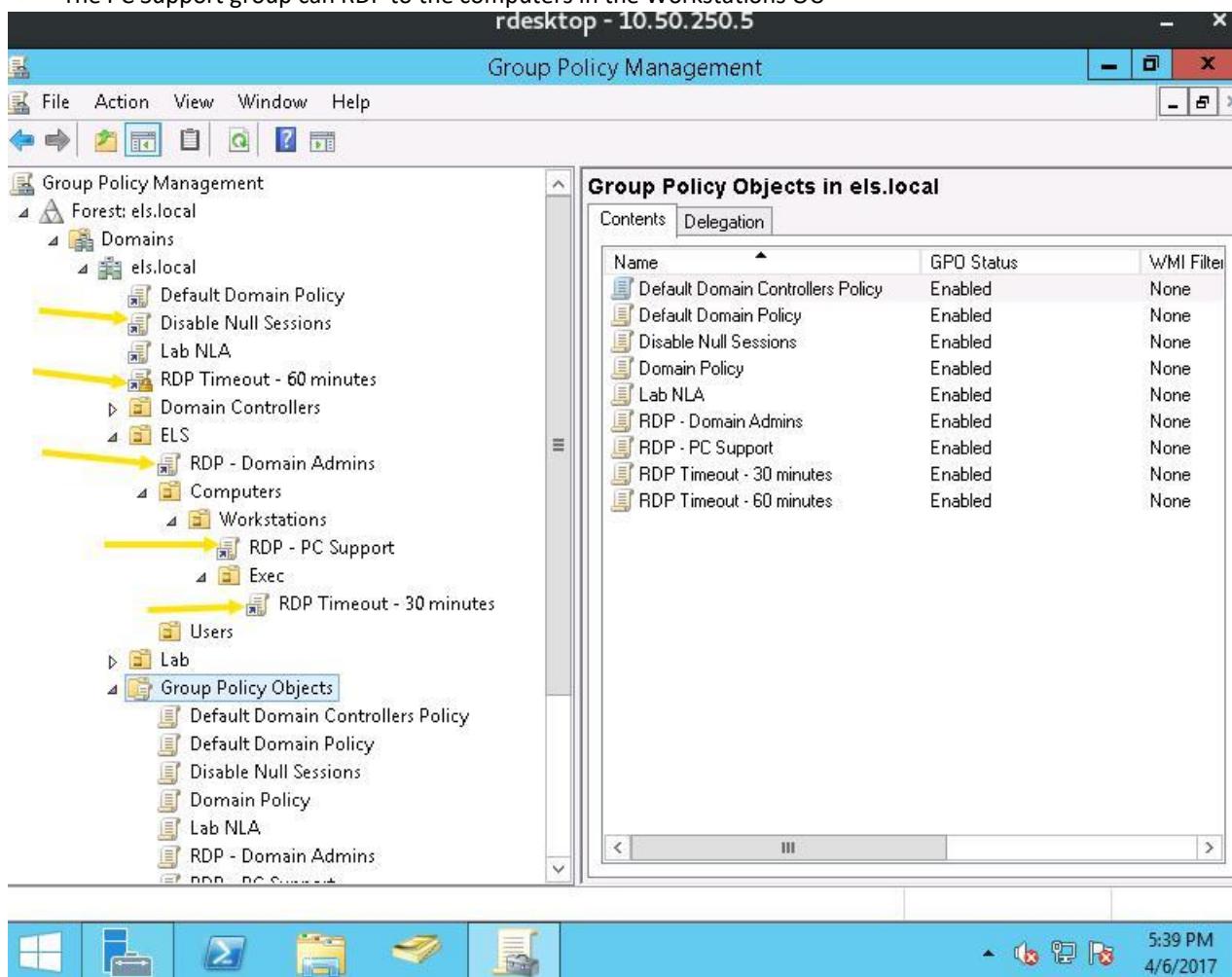
Task 2.2: RDP Timeout

- ✓ 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

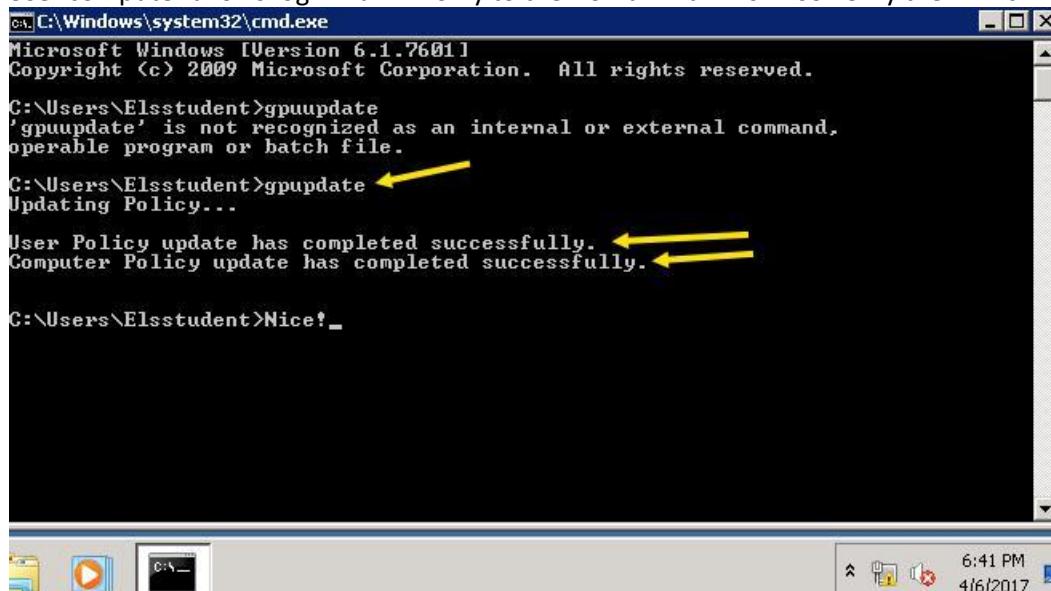
- ✓ Apply the RDP users GPOs, per the following objectives:
 - The Domain Admins can connect via RDP to all computers in the domain
 - The PC Support group can RDP to the computers in the Workstations OU



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.



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Elsstudent>gpupdate
'gpupdate' is not recognized as an internal or external command,
operable program or batch file.

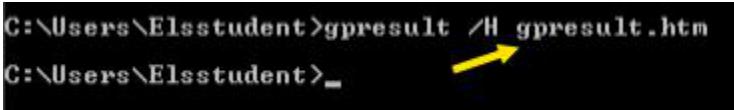
C:\Users\Elsstudent>gpupdate
Updating Policy...

User Policy update has completed successfully. ←
Computer Policy update has completed successfully. ←

C:\Users\Elsstudent>Nice!_

```

6:41 PM
4/6/2017



```

C:\Users\Elsstudent>gresult /H gresult.htm
C:\Users\Elsstudent>_

```

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	RDP - Domain Admins

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

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 Set client connection encryption level	Setting Enabled Encryption Level Choose the encryption level from the drop-down list	Winning GPO RDP Timeout - 30 Min High Level
Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits		
Policy Set time limit for active but idle Remote Desktop Services sessions	Setting Enabled Idle session limit:	Winning GPO RDP Timeout - 60 Min 1 hour
Policy Set time limit for disconnected sessions	Setting Enabled End a disconnected session	Winning GPO RDP Timeout - 60 Min 1 hour
Policy Terminate session when time limits are reached	Setting Enabled	Winning GPO 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 Allow log on through Terminal Services	Setting ELS\Domain Admins, ELS\PC Support	Winning GPO 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

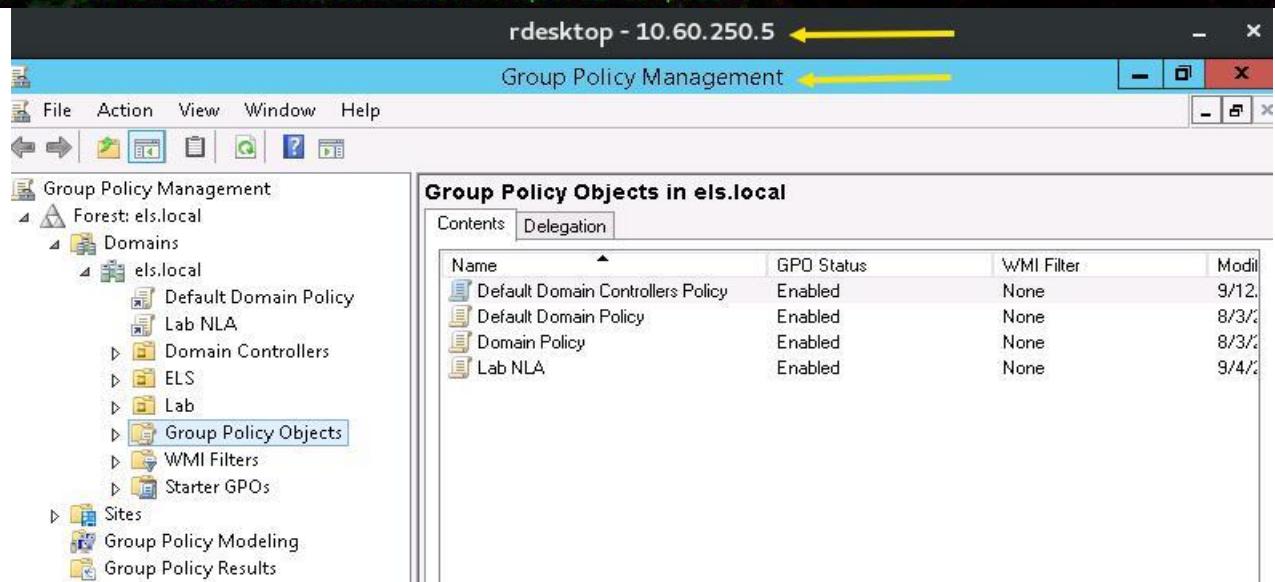
IMPORTANT NOTE:

- 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.

```
root@kali:~/Desktop/PNDLabs# openvpn L7.ovpn
Sat Apr  8 13:42:22 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 13:42:22 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.08
Enter Auth Username: isantos ←
Enter Auth Password: *****
Sat Apr  8 13:42:29 2017 TCP/UDP: Preserving recently used remote address: [AF_INET]162.254.149.248:36205
Sat Apr  8 13:42:29 2017 UDP link local (bound): [AF_INET][undef]:1194
Sat Apr  8 13:42:29 2017 UDP link remote: [AF_INET]162.254.149.248:36205
Sat Apr  8 13:42:30 2017 [Hera Openvpn Cluster] Peer Connection Initiated with [AF_INET]162.254.149.248:36205
Sat Apr  8 13:42:31 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 13:42:31 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 13:42:31 2017 TUN/TAP device tap0 opened
Sat Apr  8 13:42:31 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Sat Apr  8 13:42:31 2017 /sbin/ip link set dev tap0 up mtu 1500
Sat Apr  8 13:42:31 2017 /sbin/ip addr add dev tap0 10.60.250.200/24 broadcast 10.60.250.255
Sat Apr  8 13:42:31 2017 Initialization Sequence Completed ←
```



Task 1.1: NTLMv2

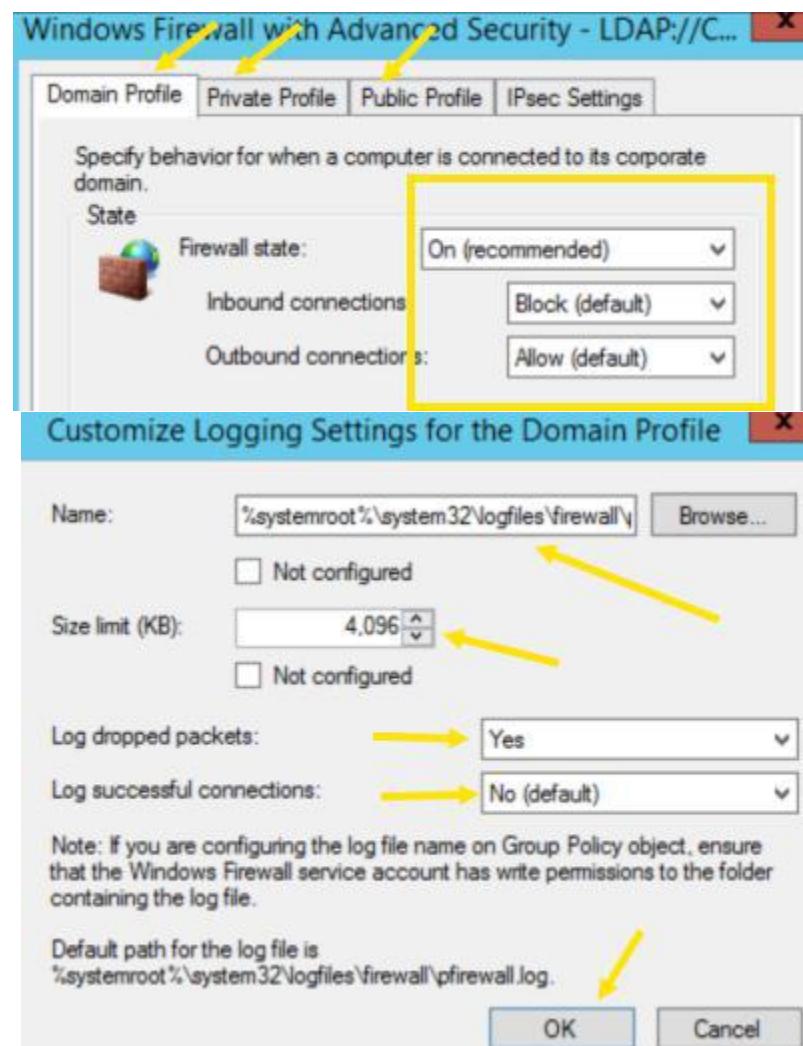
- ✓ Create a policy that enforces NTLMv2 and rejects LM authentication.

The screenshot shows the 'NTLMv2 [DC1.ELS.LOCAL] Policy' node in the left navigation pane. A yellow arrow points from the 'Policies' folder under 'Computer Configuration' to the 'Network security: LAN Manager authentication level' policy in the main list. Another yellow arrow points from the 'Security Options' folder to the same policy. The 'Network security: LAN Manager authentication level' policy is selected, and its details are shown in the right-hand pane. The 'Security Policy Setting' tab is active, displaying the setting 'Send NTLMv2 response only. Refuse LM & NTLM' with a checked checkbox labeled 'Define this policy setting'. A dropdown menu below the setting shows several options, with 'Send NTLMv2 response only. Refuse LM & NTLM' highlighted in blue, indicated by a yellow arrow.

Task 1.2: Windows Firewall

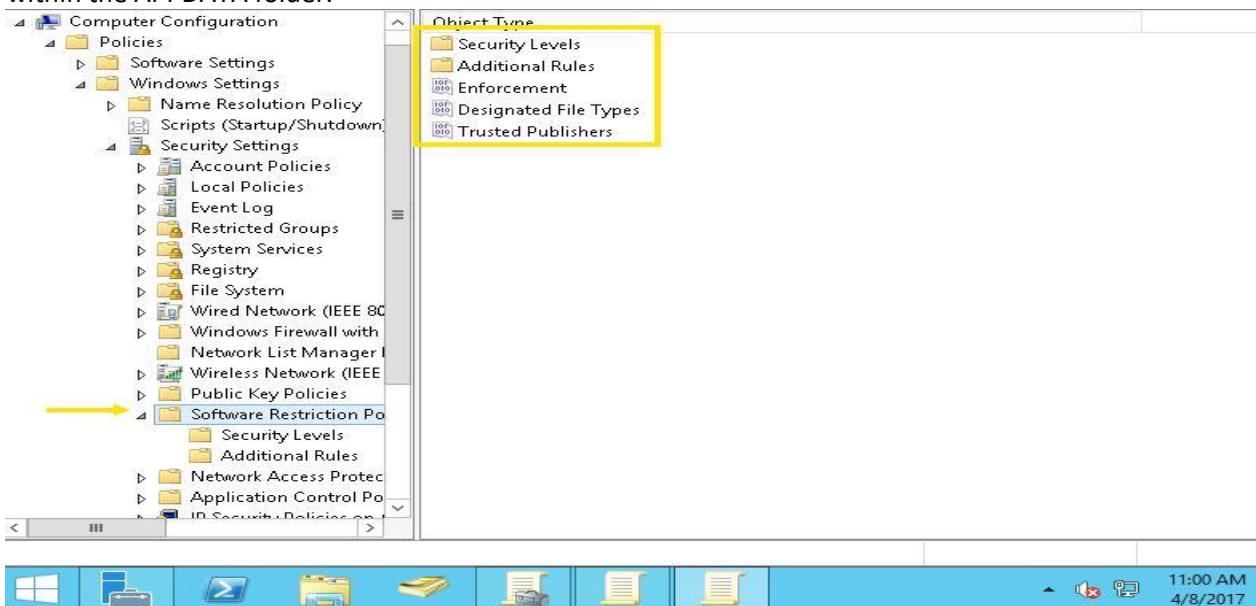
- ✓ Create a policy which forces the Windows Firewall to stay enabled for all network profiles. Make sure you also create a firewall rule which allows RPD (tcp/3389) so you can connect to the workstation later.

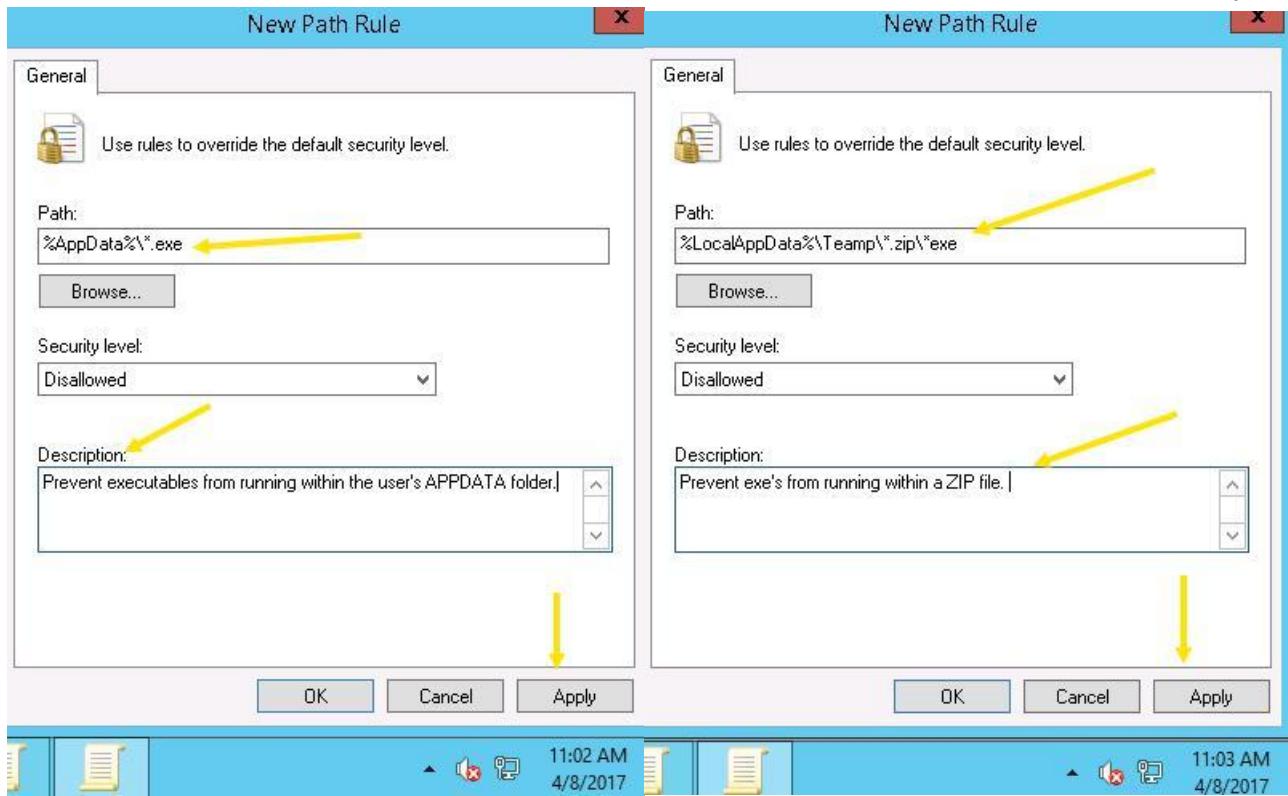
The screenshot shows the 'Windows Firewall [DC1.ELS.LOCAL] Policy' node in the left navigation pane. A yellow arrow points from the 'Windows Firewall with Adv...' folder to the right-hand pane, which displays the 'Windows Firewall with Advanced Security' interface. The interface includes sections for 'Overview', 'Domain Profile' (status: not configured), 'Private Profile' (status: not configured), and 'Public Profile' (status: not configured). Under 'Getting Started', there is a section titled 'Authenticate communications between computers' with a note about creating connection security rules. At the bottom, there is a link to 'View and create firewall rules'.



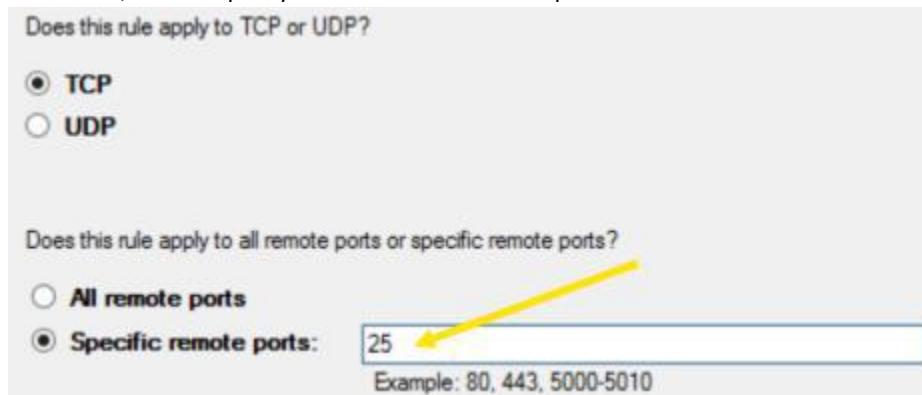
Task 1.3: Software Restrictions

- ✓ 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.

Policy	Policy Setting
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives...	Not Defined
Shutdown: Allow system to be shut down without having to...	Not Defined
Shutdown: Clear virtual memory pagefile	Not Defined
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Not Defined
System objects: Require case insensitivity for non-Windows ...	Not Defined
System objects: Strengthen default permissions of internal s...	Not Defined
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Windows Executabl...	Not Defined
User Account Control: Admin Approval Mode for the Built-i...	Not Defined
User Account Control: Allow UIAccess applications to prom...	Not Defined
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials on the se
User Account Control: Detect application installations and p...	Not Defined
User Account Control: Only elevate executables that are sign...	Not Defined
User Account Control: Only elevate UIAccess applications th...	Not Defined
User Account Control: Run all administrators in Admin Appr...	Not Defined
User Account Control: Switch to the secure desktop when pr...	Not Defined
User Account Control: Virtualize file and registry write failure...	Not Defined

Task 1.6: Removable Media

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

Removable Disks: Deny execute access	Enabled
Removable Disks: Deny read access	Not configured
Removable Disks: Deny write access	Enabled

Task 1.7: Test Settings before Change

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

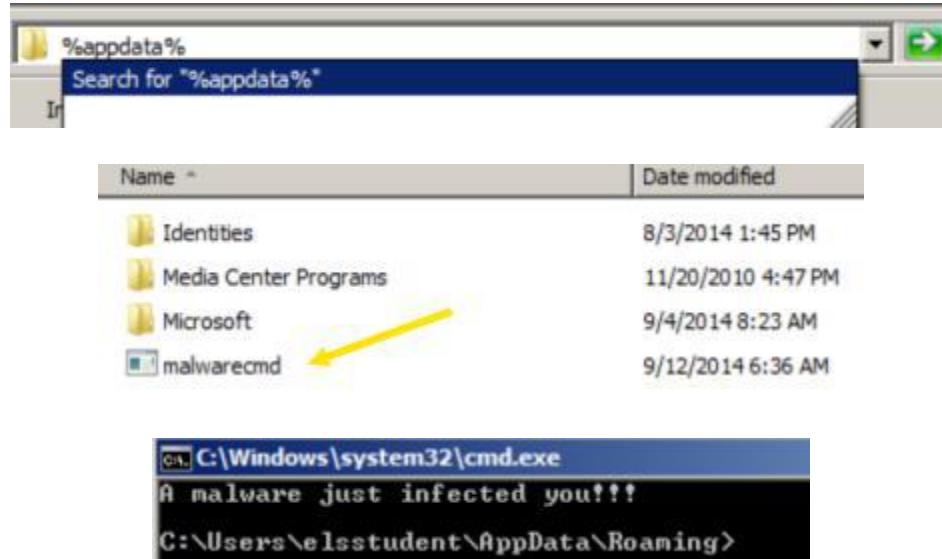
- Can you disable UAC?
- Try to telnet to Server01 (10.60.250.5) on port 25. What happens?
- What happens when you try to run the sample malware executable in the %AppData% directory? Note: the sample malware is harmless, but has been written to be detectable by nearly every antivirus.

We can edit the firewall state:

Telnet is enabled:



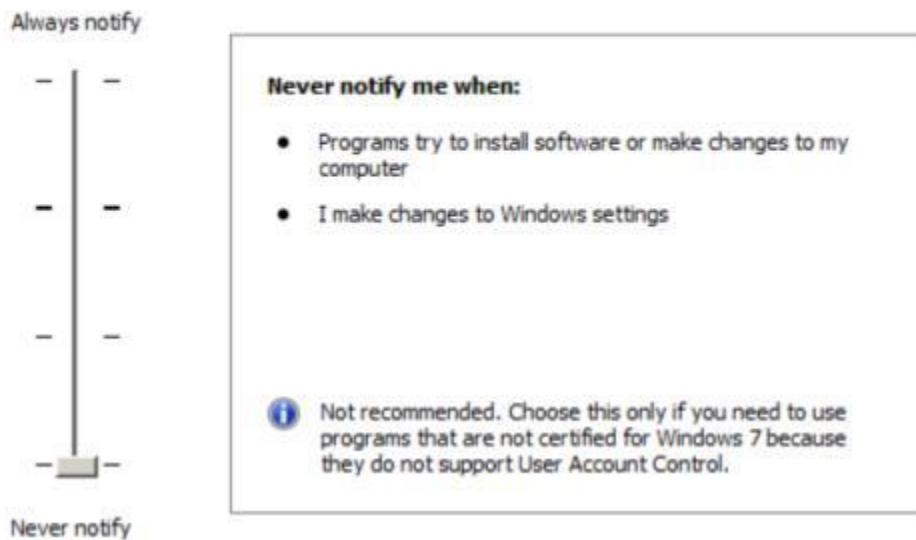
The Malware file is able to run via the %APPDATA% search:



We are able to disable UAC:

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer
[Tell me more about User Account Control settings](#)



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.

The screenshot shows two windows side-by-side. On the left is the 'Group Policy Management' console under 'Forest: els.local'. A yellow box highlights the 'Computers' node under 'ELS'. Inside this node, the 'Windows Firewall' item is also highlighted with a yellow box. On the right is the 'Windows Firewall' properties window. It shows a table with one row: 'Location' (Computers), 'Enforced' (No), and 'Link Enabled' (Yes). Below this is a 'Security Filtering' section with the note: 'The settings in this GPO can only apply to the following groups, users, and computers:'.

Windows PowerShell

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\elsstudent> gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully. ←
```

PS C:\Users\elsstudent>

11:19 AM
4/8/2017

Can't change the firewall:

The screenshot shows the 'Windows Firewall with Advanced Security on Local Computer' window. It displays an 'Overview' section with a message: 'For your security, some settings are controlled by Group Policy'. Below this, it says 'Domain Profile is Active' with three status items: 'Windows Firewall is on.' (green checkmark), 'Inbound connections that do not match a rule are blocked.' (red circle with a slash), and 'Outbound connections that do not match a rule are allowed.' (green checkmark).

%APPDATA% malware file is blocked:

The screenshot shows a dialog box from 'C:\Users\elsstudent\AppData\Roaming\malwarecmd.exe'. It contains the message: 'This program is blocked by group policy. For more information, contact your system administrator.' An 'OK' button is at the bottom right. The taskbar at the bottom shows the date and time: 11:26 AM 4/8/2017.

Telnet disabled:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\elsstudent>telnet 10.60.250.5 25
Connecting To 10.60.250.5...Could not open connection to the host, on port 25: connect failed
C:\Users\elsstudent>BooYAH!
```

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.

Setting	State
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured
Do not adjust default option to 'Install Updates and Shut Do...	Not configured
Remove access to use all Windows Update features	Enabled

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.

The screenshot shows the Group Policy Management console. On the left, under 'Forest: els.local > Domains > els.local > ELS > Users', there is a policy named 'Prevent Access to Windows Update'. A yellow arrow points from this policy to the right pane. The right pane is titled 'Prevent Access to Windows Update' and shows the 'Links' tab. It displays a table with one row: 'Location: Users', 'Enforced: No', and 'Link: Yes'. Below this is the 'Security Filtering' section, which lists 'Name: Authenticated Users'.

The screenshot shows a Windows PowerShell window. The command 'gpupdate' is run, and the output shows: 'Computer Policy update has completed successfully.' and 'User Policy update has completed successfully.' A yellow arrow points from the PowerShell output to the status bar at the bottom, which shows '1:57 PM 4/8/2017'.

The screenshot shows the Windows Control Panel. Under 'System and Security', the 'Windows Update' link is selected. A yellow arrow points from the status bar at the bottom to the message in the center of the window, which reads: 'Some settings are managed by your system administrator. More information.'

The screenshot shows the 'Windows Update' interface. On the left, there are links: 'Control Panel Home', 'Check for updates', 'Change settings', 'View update history', 'Restore hidden updates', and 'Updates: frequently asked questions'. On the right, it shows the 'Windows Update' status: 'Most recent check for updates: Never', 'Updates were installed: Never', and 'You receive updates: For Windows only.'

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 (OpenSSL)] [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]66.232.115.228:34199
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]66.232.115.228:34199
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-CBC).
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-CBC).
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# █
```

Sat Apr 8, 18:44:07

root@kali: ~

```
File Edit View Search Terminal Help
root@kali:~# /etc/init.d/nessusd start ←
Starting Nessus : .
root@kali:~# 
```

Nessus / Setup - Mozilla Firefox

eLearnSecurity Me... x Nessus / Setup x

https://kali:8834 ←

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng eLearnSecurity - IT Sec.

Welcome to Nessus®

Nessus

Thank you for installing Nessus, the industry leader in vulnerability scanning. This application allows you to:

- Run high-speed vulnerability and discovery scans on your network
- Conduct agentless auditing on hosts to confirm they are running up-to-date software
- Perform compliance checks on hosts to verify they are adhering to your security policy
- Schedule scans to launch automatically at the frequency you select
- And much more!

Press continue to perform account setup, register or link this scanner, and download the latest plugins.

Continue

tenable network security

Task 2.1: Setup Options Profile

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

Policies / All Policies

<input type="checkbox"/> Name ▾	Last Modified	Type	<input type="checkbox"/>	X
<input type="checkbox"/> UnAuthenticated NEtwork Scan	07:25 PM	<input type="checkbox"/> Template	<input type="checkbox"/>	X

Task 2.2: Create and run Scan

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

Scans / My Scans

<input type="checkbox"/> Name	Schedule	Last Modified ▾
<input type="checkbox"/> Scan Server01	On Demand	<input type="checkbox"/> 07:30 PM

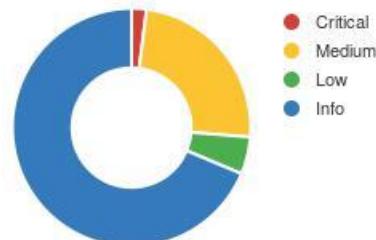
Task 2.3: Review Findings

- ✓ 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

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

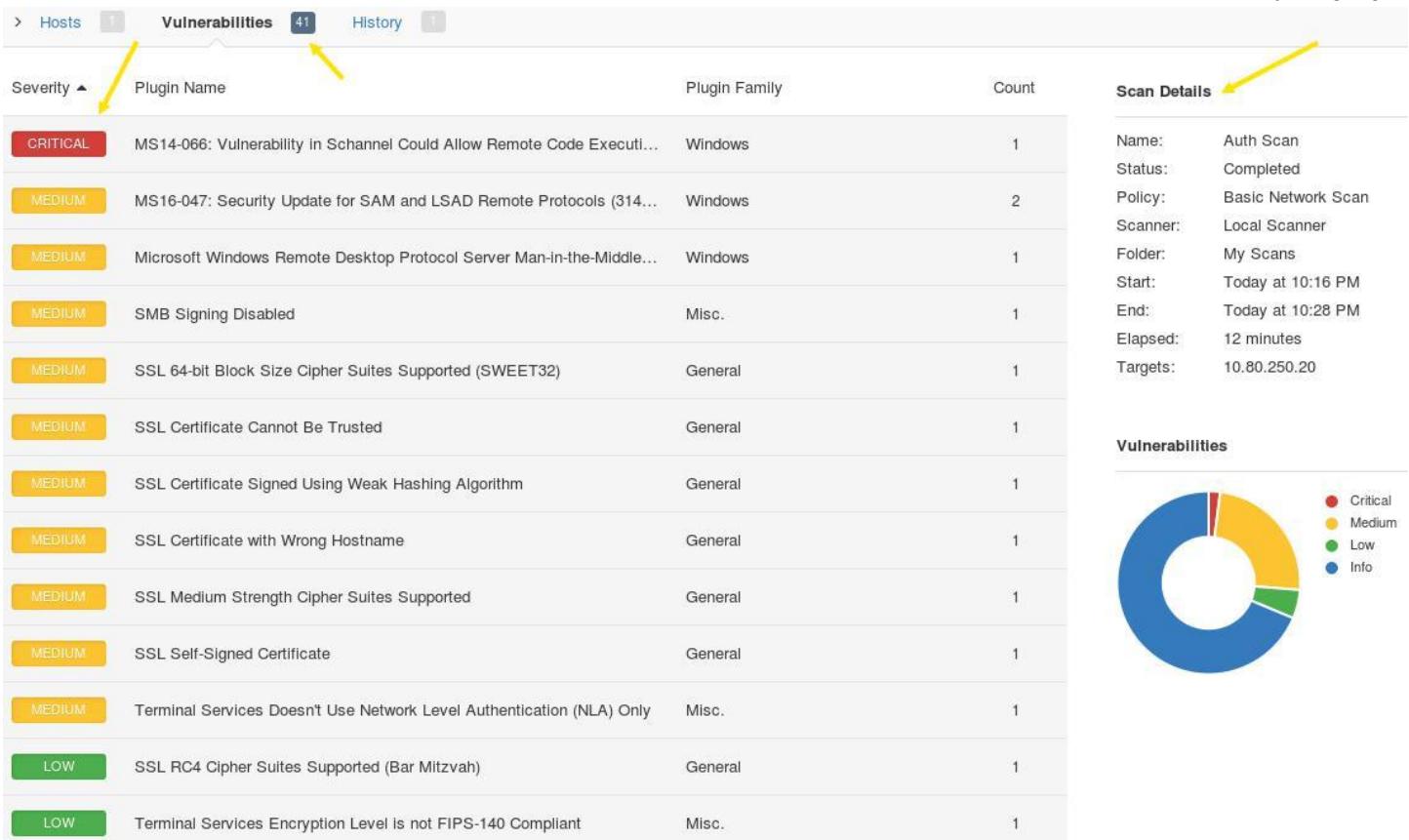
- ✓ Run an authenticated scan against Server01.

Scans / My Scans

<input type="checkbox"/> Name	Schedule	Last Modified ▲
<input type="checkbox"/> Auth Scan	On Demand	10:16 PM

Tasks 1.2: Review Report

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

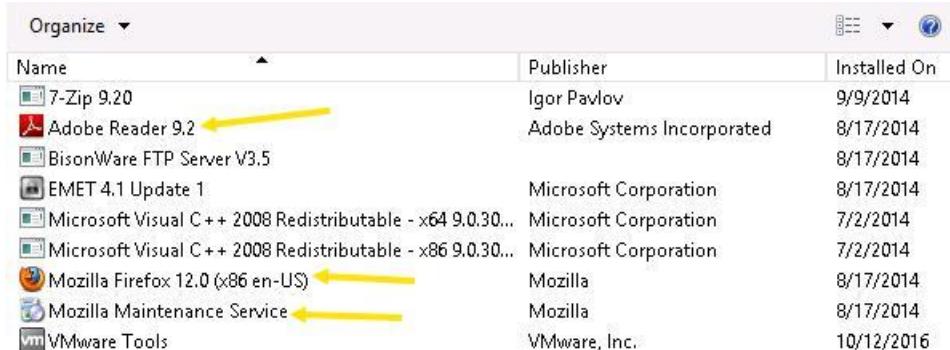


Severity	Plugin Name	Plugin Family	Count	Scan Details
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Executi...	Windows	1	Name: Auth Scan Status: Completed Policy: Basic Network Scan Scanner: Local Scanner Folder: My Scans Start: Today at 10:16 PM End: Today at 10:28 PM Elapsed: 12 minutes Targets: 10.80.250.20
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	

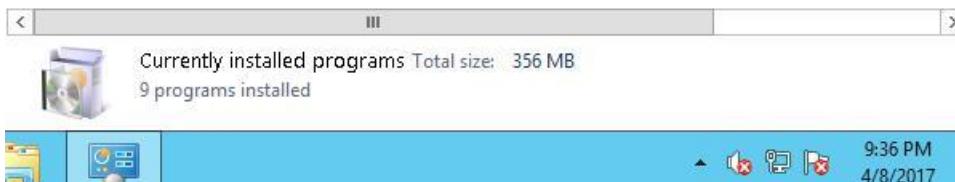
Task 2: Remediation

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.

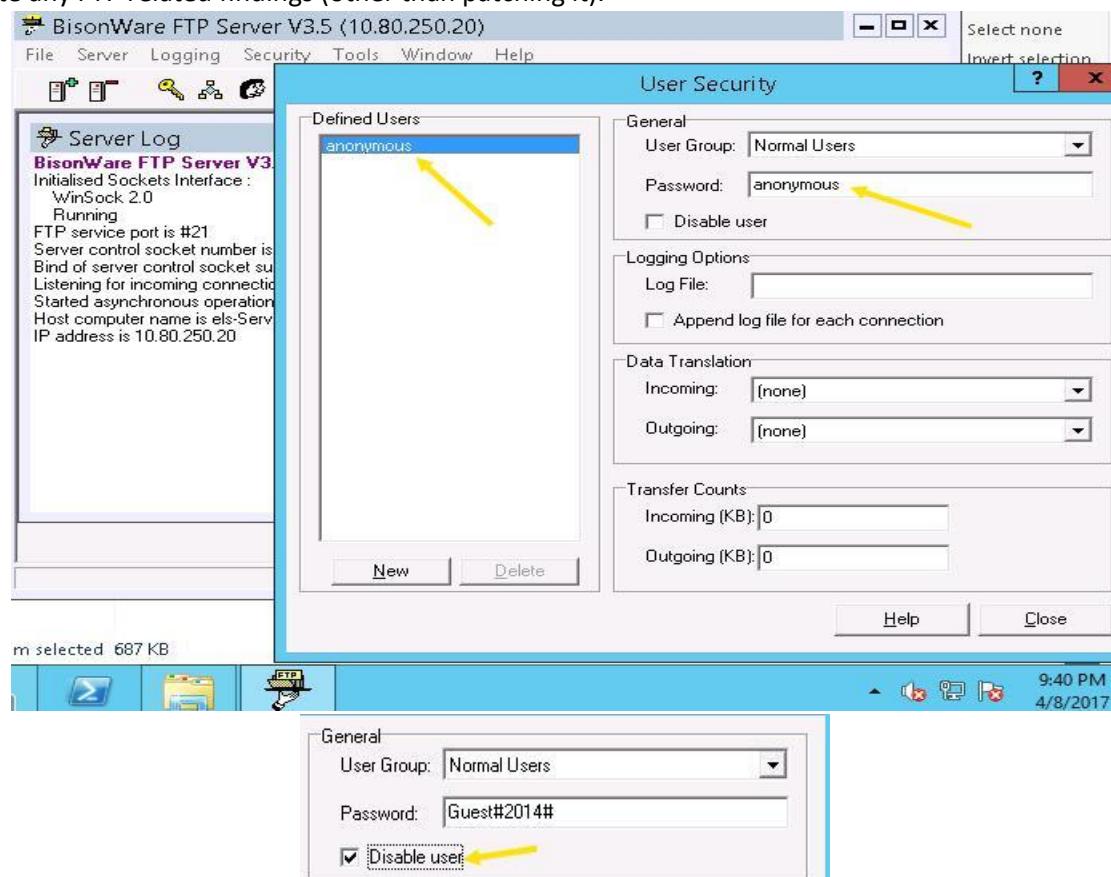


Name	Publisher	Installed On
7-Zip 9.20	Igor Pavlov	9/9/2014
Adobe Reader 9.2	Adobe Systems Incorporated	8/17/2014
BisonWare FTP Server V3.5		8/17/2014
EMET 4.1 Update 1	Microsoft Corporation	8/17/2014
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30...	Microsoft Corporation	7/2/2014
Microsoft Visual 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.

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: secpol.msc

This task will be created with administrative privileges.

Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options

Policy	Security Setting
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before each logon	5 days
Interactive logon: Require Domain Controller authentication	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action

Interactive logon: Number of previous logons to cache (in case domain controller is not available) ? x

Local Security Setting Explain

Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Do not cache logons: 10 logons

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.

Scans / My Scans

<input type="checkbox"/> Name	Schedule	Last Modified 
<input type="checkbox"/> Auth Scan	On Demand	 10:53 PM

There are less:



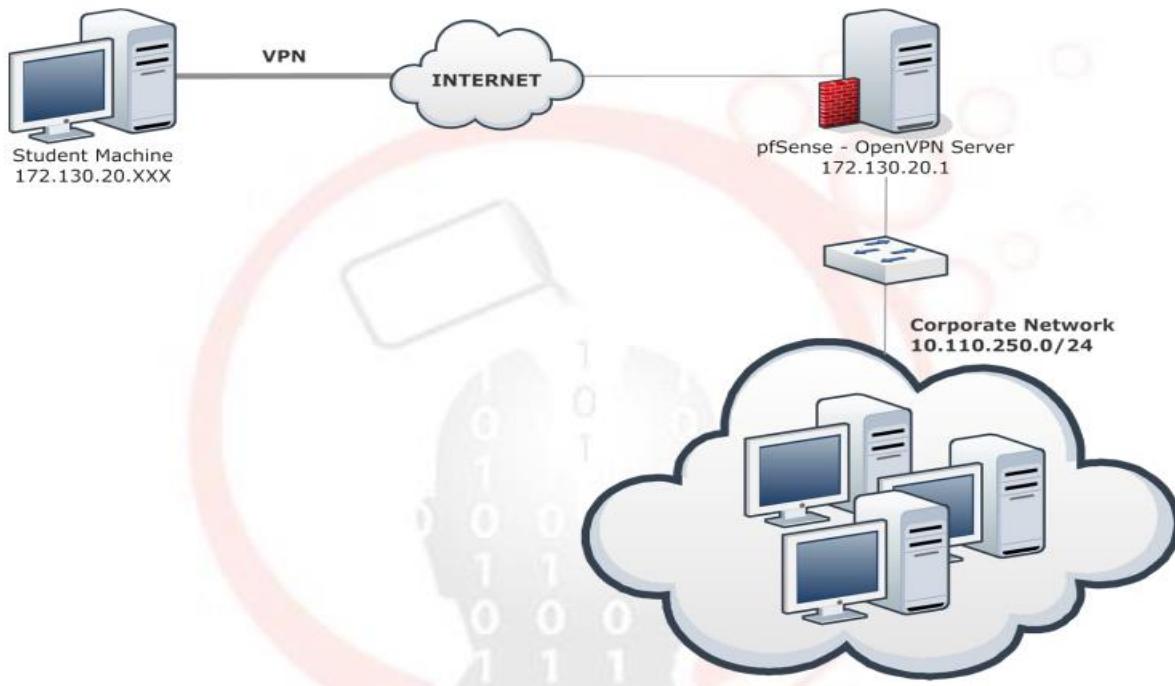
All highs – medium are patch related now:

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".

System: Certificate Authority Manager

CAs Certificates Certificate Revocation				
Name	Internal	Issuer	Certificates	Distinguished Name
OpenVPN Server CA	YES	self-signed	0	emailAddress=els@elearnsecurity.com, ST=Texas, O=ELS, L=Austin, CN=internal-ca, C=US Valid From: Tue, 28 Mar 2017 20:10:36 +0000 Valid Until: Fri, 26 Mar 2027 20:10:36 +0000

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.

System: User Manager

Users	Groups	Settings	Servers
Username	Full name	Disabled	Groups
admin	System Administrator		admins
VPNUseradmin	Ivan V		

Task 4: Configure the OpenVPN Server

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

General information

Disabled	<input type="checkbox"/> Disable this server
Server Mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Local Database
Protocol	UDP
Device Mode	tap
Interface	WAN
Local port	39500
Description	Corporate OpenVPN Server You may enter a description here for your reference (not parsed).

Cryptographic Settings

TLS Authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets. # # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 863e5eaf6c0eaeeef1f30e75c43da8d3c 860c9ec446c8a1f75fc7c942cd0aa3ab f18efed8b59d15cba10c5a4593831442 7a502d8af538d17a6b8023058dfbcb87 Paste your shared key here.
Peer Certificate Authority	OpenVPN Server CA
Peer Certificate Revocation List	No Certificate Revocation Lists (CRLs) defined. Create one under System > Cert Manager.
Server Certificate	VPNUser Certificate (CA: OpenVPN Server CA) *In Use
DH Parameters Length	1024 bits
Encryption algorithm	AES-128-CBC (128-bit)
Hardware Crypto	No Hardware Crypto Acceleration

Task 5: Export the client configuration

- ✓ Export and install the client configuration installer from pfSense.

OpenVPN: Client Export Utility

User	Certificate Name	Export
VPNUser	VPNUser Certificate	<ul style="list-style-type: none"> - Standard Configurations: - Archive Config Only - Inline Configurations: - Windows Installers: - Mac OSX: <p>2.3-x86 2.3-x64</p>

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

```
C:\Users\els>ping 10.110.250.50
Pinging 10.110.250.50 with 32 bytes of data:
Reply from 10.110.250.50: bytes=32 time=364ms TTL=127
Reply from 10.110.250.50: bytes=32 time=182ms TTL=127
Reply from 10.110.250.50: bytes=32 time=184ms TTL=127
Reply from 10.110.250.50: bytes=32 time=183ms TTL=127

Ping statistics for 10.110.250.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 182ms, Maximum = 364ms, Average = 228ms
```