Configuring Identity and Access Management Controls

(CompTIA Security + SY – 601)

Objectives:

- To analyze potential indicators to determine the type of attack
- To implement identity and account management controls
- To implement authentication and authorization solutions
- To implement Public Key Infrastructure (PKIs)
- To use the appropriate tool to access organizational structure

Resources:

- Kali Virtual Machine (PT1-Kali VM)
- Windows Virtual Machine
- John The Ripper
- OpenSSL
- Command-line tools

Instructions:

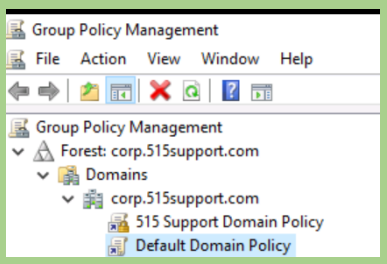
Security Policy

- Review the following written security requirements. Edit the Default Domain Policy Group Policy Group Policy Object to enforce the password and account lockout configurations. Edit the 515 Support Domain Policy to enforce the remaining security options

- Passwords will be changed every 60 days, and may not be changed more frequently than every one day. Passwords must be at least 12 characters in length. Passwords must meet complexity requirements. Users may not reuse the last 20 passwords.
- Accounts will be locked out for 10 minutes if an incorrect password is entered more than three times.
- Local guest user accounts will be disabled.
- Servers and workstations will not display the user name of the last user to log on.
- Servers and workstations will display the following title and message: "Warning" (title) "Authorized use only!" (message)

- Sign-in to the **DC1** Virtual Machine

- Use the **Group Policy Management** console to browse to the **corp.515support.com** domain object and observe the two existing GPOs: the **Default Domain Policy** and the **515 Support Domain Policy**



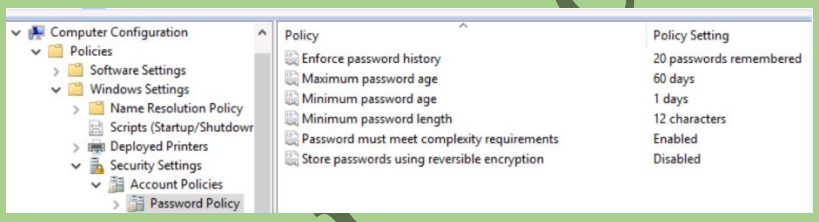
- Edit the existing **Default Domain Policy** to match to the password and account lockout requirements define above in the security requirements

▼ Settings locations
Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies
Password Policy:

- Password history
- Max password age
- Min password age
- Min password length
- Password must meet complexity requirements

Account Lockout Policy:

- Account lockout duration
- Account lockout threshold



- Edit the existing **515 Support Domain Policy** to match the guest account, logon message, and last user name requirements define above in the security requirements define above in the security requirements

▼ Settings locations
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options

- Accounts: Guest account status - disabled
- Interactive logon: Do not display last user name
- Interactive logon: Message text for users attempting to log on
- Interactive logon: Message title for users attempting to log on.

- From the administrator: Windows Powershell run the following command

```
gpupdate /force
```

```
PS C:\Windows\system32> gpupdate /force
Updating policy...
```

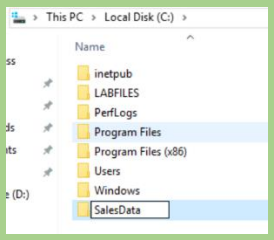
- From Administrator: Windows Powershell run the following command

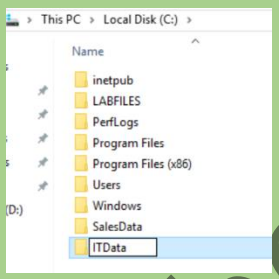
```
gpresult /H
C:\Users\Administrator\Desktop\GPreport.htm
```

```
PS C:\Windows\system32> gpresult /H C:\Users\Administrator\Desktop\GPreport.htm
```

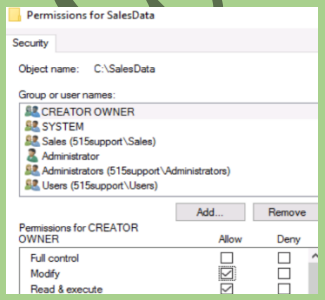
Manage Windows Permission

- Select the **DC1** Virtual Machine and then sign-in
- Create the following folders: **SalesData** and **ITData**





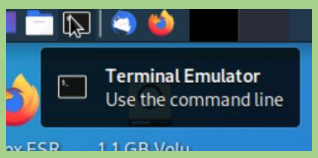
- A Help Desk ticket forwarded to you states that **Bobby** should be a member of the **Sales** group, and that the **Sales** group needs the **Modify** permission to the **SalesData** folder. Use file explorer and **Active Directory Users and Computer** to satisfy requirements



- A Help Desk ticket forwarded to you states that **Sam** should be *explicitly denied* access to the ITData folder. Configure the explicit deny permission

Configure Linux Permissions

- Select the PT1-Kali VM and the sign-in
- From the top bar, open the **Terminal Emulator** icon



- Create a user account named **Floyd**, and then set floyd's password as **Pa$$w0rd** by using the **adduser** command

```
root@KALI:~# useradd floyd
```

- Create a group named **Sales** by using the **groupadd** command

```
root@KALI:~# groupadd sales
```

- Create a directory named **/Salesinfo** using the **mkdir** command and then create a file in the **/Salesinfo** directory named **SalesPolicies.txt** by using the touch command

```
root@KALI:~# mkdir /SalesInfo/SalesPolicies.txt
```

- Configure **Floyd** with **rwx**, the Sales group with r-x, and all others with no access to the **/Salesinfo**, directory and all its contents by using the **chmod -R** command

```
○ chmod -R u=rwx,g=rx,o-rwx
  /SalesInfo
```

Audit a User Password

- Select the **PT1-Kali** VM and then sign-in
- From the top bar, open the **Terminal Emulator** icon
- Create an account named bobby and set **Pa$$w0rd** as the password by using the **adduser** command

```
root@KALI:~# adduser bobby
Adding user `bobby' ...
Adding new group `bobby' (1002) ...
Adding new user `bobby' (1001) with group `bobby' ...
Creating home directory `/home/bobby' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for bobby
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
```

- Extract the **/usr/share/wordlists/rockyou.txt.gz** word list file by using the gunzip command:

```
root@KALI:~# gunzip /usr/share/wordlists/rockyou.txt.gz
```

- Open the **rockyou.txt** wordlist file for editing (you may use vim or nano)

```
root@KALI: ~
123456
12345
123456789
password
iloveyou
princess
```

- Use the **i** key to enter the Vim's insert mode, and then add the password you set for Bobby above at the top of the file

```
root@KALI: ~
password
123456
12345
123456789
password
iloveyou
```

- Run the following command to create a text file of usernames and password hashes

```
root@KALI:~# john --wordlist=/usr/share/wordlists/rockyou.txt crack-this-file
```

- Run the following command to crack passwords

```
root@KALI:~# john --wordlist=/usr/share/wordlists/rockyou.txt crack-this-file
```

- Redirect the results of the **john –show crack-this-file** to a text file:

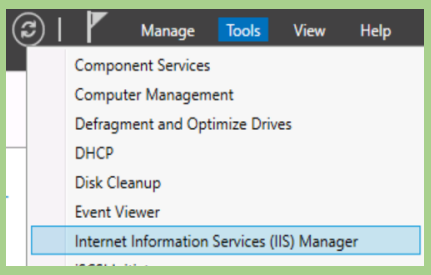
```
root@KALI:~# john --show crack-this-file > password-audit.txt
```

- Display the **password-audit.txt** file contents by using the cat command

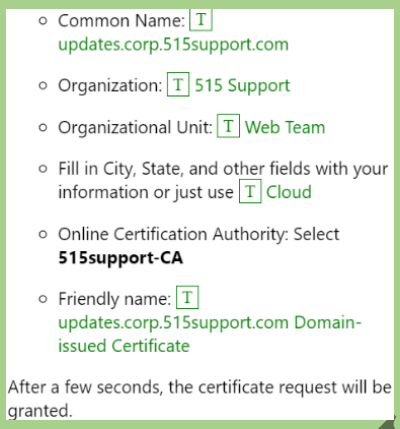
```
root@KALI:~# ls
crack-this-file  Documents  LOD     nmap.xsl           Pictures  set        Videos
Desktop          Downloads  Music   password-audit.txt Public    Templates
```

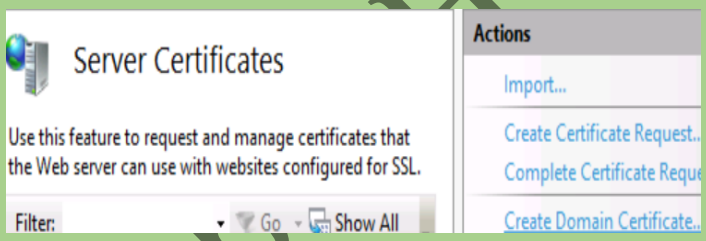
Request a Server Certificate

- Select the **MS1 VM** and then sign-in
- Open the Internet Information Service **(IIS)** Manager console

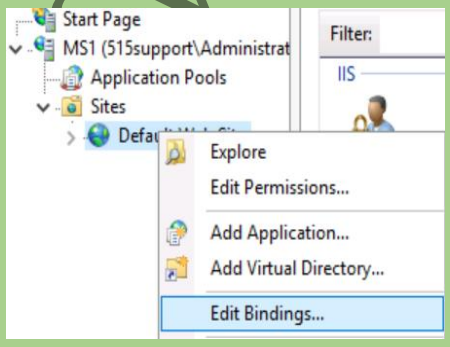


- Select the **Server Certificate** applet
- In the Action pane, select **Create Domain Certificate**. Complete the create certificate wizard by entering the following information

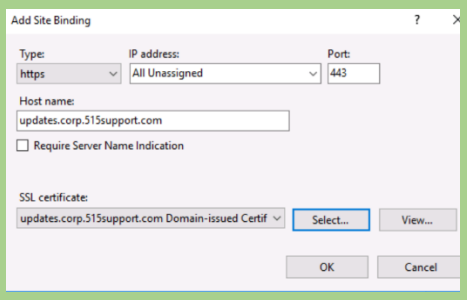




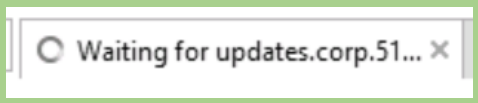
- In the Properties of the Default Web Sites, select **Edit Bindings**



- Add site bindings for **https** that uses a hostname of updates.corp.515support.com **Domain-issued certificate SSL certificate**



- Remove the **http** entry
- Close the dialog box, and then return to the main IIS console
- In the Internet Explorer attempt to connect to https://updates.corp.515support.com if prompted, select OK to acknowledge the warning



- You should see the **515 Support User Portal** web page

Manage Certificates by Using OpenSSL

- Select the **PT1-Kali** VM and sign-in
- From the top bar, open the **Terminal Emulator** icon
- Create a directory named **keys** in the root user's directory, and then use the **cd** command to change to the **keys** directory

```
root@KALI:~# cd keys
root@KALI:~/keys# op
```

- Generate a private key and extract public to create a **certificate signing request**

```
root@KALI:~/keys# openssl genrsa -out corp.515support.com.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.............................+++++
.........................................+++++
e is 65537 (0x010001)
```

- Enter the **public key**
- Use the **ls** command to display the **public key file**

```
root@KALI:~/keys# ls
corp.515support.com.key  corp.515support.com_public.key
```

- Display the public key files

```
root@KALI:~/keys# cat corp.515support.com_public.key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA1+OuC8Wz8UEr0ZKJFlhfSRnOrPRArdnGJGyHOMgTQU
Jw5lmwxVM4NgZtQGgdEbTMcCZgOQ6ePp+JOz4vpsi0Fdas9UYz6JRltf/b
hy88gay8e0Xu8hrcKxP5Dm49KsCN7DC8eLdQD4heCFy3jcF7CZ220cBCiJ
```

- Generate a certificate signing request

```
root@KALI:~/keys# openssl req -new -key corp.515support.com.key -out corp.515support
.com.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:515 Support
Organizational Unit Name (eg, section) []:WebServices.
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:admin@515support.com
```

- Run the **ls** command to display the **.csr** file

```
root@KALI:~/keys# ls
corp.515support.com.csr  corp.515support.com.key  corp.515support.com_public.key
```

Observations:

- Policies for password and account lockout were effectively applied.
- Permissions were correctly assigned to users and groups as specified.
- Linux user and group permissions were configured successfully.
- Password audit for user Bobby was completed using John The Ripper.
- Domain certificate was successfully created and applied in IIS, ensuring secure HTTPS access.
- Public and private keys were generated and certificate signing request was completed using OpenSSL.

Results:

- Successfully implemented security policies and configurations for both Windows and Linux environments.
- Managed permissions and conducted password audits to ensure security compliance.
- Configured and validated server certificates and public key infrastructure.

Conclusion:

This lab demonstrated comprehensive identity and access management, combining policy enforcement, permission management, password auditing, and PKI implementation to secure both Windows and Linux environments effectively.

Future Work:

- Automate policy and permission management through scripting.
- Integrate multi-factor authentication (MFA) for enhanced security.
- Explore advanced PKI configurations and certificate management automation.