ST2612 Tutorial 4 (Week 12)

Recap of Practical 4, Lecture 4 (Part 2), Lecture 5

Learning objective of Practical 4:

* Verifying and complete the setup of the Domain DNS Server with root hints update and Reverse Lookup support.
* Hands on exercise on creation of reverse lookup zone and reverse lookup entries.
* Basic configurations of member server with the IIS role to publish web content.
* Hands on with Security Compliance Manager.
  + Understand the SCM as an offline tools that can help to maintain, design, security policies for an Enterprise. It covers both of the server and client level operating systems and some of the Microsoft Applications.
  + Understand that the online baseline update feature has been stopped, SCM can still be helpful.
  + SCM can obtain updated baselines from alternative source, such as the 'Microsoft Security Compliance Toolkit 1.0'.
  + Experience how the export to GPO feature can deploy customizable baselines to an actual target system.
* Hands on with configurations of GPO settings.
* Hands on with the GPRESULT command.
* Understand the operational concept of the gpupdate command. (i.e. by pulling instead of pushing).
* Experience the operational requirement and usage of RSoP. Lecture 4 (Part 2):
* Introduction to Group Policy
  + How Group Policy works ?
  + Identify the relationship between Group Policy Objects and Group Policy Containers.
* Highlights of common Group Policies
  + Account Policies
  + Audit Polices
  + User Rights
  + Security Options
* Policy Application Order and Troubleshooting
  + Block inheritance (Container option)
  + Enforced (GPO attribute)
  + Computer Configurations vs User Configurations compartments.

Lecture 5:

* Introduction to Patch Management
  + Patch Management vs Security Patch Management.
  + Patch Management Process
* Managing security updates with the Five Stages approach

1. Receive Security update Notification (Info only, no actual update)
2. Evaluate Risk
3. Evaluate Mitigation
4. Deploy Update Stage (Six Steps)
5. Monitor Systems

* Introduction to Windows Software Update Services (WSUS).
  + Multi-Tier structure
  + Advantages:
    - Operational
    - Security
  + Used as deployment and monitoring tools.
* Common approaches to resolve windows update issues.
  + Check Disk Space.
  + Direct download update from Windows Update Catalog.
  + Apply Windows Update Troubleshooter.

Self-evaluation Check list

* Briefly explain how the GPO Enforced option affects the Group Policy Precedence.
* Briefly explain how the Group policy block inheritance works.
* List 3 settings under the User Right Assignment Policies.

Shut down the computer

Log in locally

Remote Login

Login over the network

Backup

* How often the domain clients will get the updated Group Policies? Can we configure this settings? How?

90min

* How often the Domain Controllers will exchange/replicate updated Group Policies with each other? Can we configure this setting? How?

15s

* Describe how you can check / view the current active/effective GPOs applied to a client machine.
* The following is a question of ST2612 EXAM in AY2019/2020 S2. Try to answer it.

List three possible events that can trigger the process of applying the Computer Configuration Settings of a GPO to a specific domain workstation. (6 marks)

* In terms of security patch management, list the possible outcomes of a risk evaluation process of a new security patch.
* Which type of the following vulnerabilities may cause more damage to an organization: The one with the Critical severity rating or the one with the important severity rating?
* In your opinion, what is the most important testing criterion for a new patch?
* List 3 possible costs that should be factored in to the patch management operations.
* Identify the security advantages for using WSUS-like centralized windows update services for an Enterprise Network.
* Briefly describe two scenarios that the patch management manager would decide not to deploy a security patch (with the critical severity rating) to a mission critical production server.

Nano Test Questions (Will be given by your tutor).

(For each attempted question: Correct answer earns 1 mark. **Incorrect answer subtract 0.5 marks**)

(Maximum scores: 2 marks) Q1.

Q2.

Q3. Q4

Submit your answers to the Nano Test Journal before the end of the class.

~ That's All ~