Domain Controlling

Group Policy with Active Directory

Ananth Jillepalli & Nagarjuna Nuthalapati

July 31, 2017
Version 2.2

University of Idaho

CS 539: Applied Security Concepts

Summary

A Domain Controller is a reference to any machine that runs on Windows Server operating system and has the active directory services installed. Active Directory and subsequently, Group Policies, are used to deploy diverse set of configurations for different domain clients (agent machines present in the domain). Using it, we can deploy security configurations for all users, and also allocate tailored permissions of use for users that do not have security clearance. In this tutorial, using activities and challenges, we will demonstrate remote configuration of domain clients with the use of most commonly used group policy objects.

Contents

1 Objectives of this Tutorial >

1. Remote management of client systems through group policies and active directory:
   (a) Credential management.
   (b) User Account management.
   (c) System Security management.
   (d) Client machine's default web browser management.
   (e) Auditing and remote registry access.

1. Simple and easy to guess passwords is the first vector of vulnerabilities exploited by hackers and attackers. As such, ensuring that there is a password policy in place, which makes it mandatory for the users of domain clients will reduce the exploitation through password guessing and cracking.

2. In Windows machines, the 'Guest' account is a serious vulnerability, if not properly configured. As such, a centralized policy enforcement should be in place to either properly configure guest accounts or to completely remove them from usage in domain's client machines.

3. System security is defined most basically by the protection provided from networks by a firewall. Even the best firewalls, when not configured or improperly configured, will lead to inefficient protection. As such, we should have the ability to implement policies defining firewall's behavior.

4. Modern Web Browsers are very powerful software applications. However, the functionality and capability comes at the cost of a host of vulnerabilities. As such, it is important for an administrator to be able in remotely managing client machines' web browsers for better security of the domain network.

5. Domain controller (server) itself is not any less vulnerable than most client systems. Though the credentials are kept very secret and access is severely restricted, it is often surprising to see how many servers get compromised. Worst part is, an administrator does not easily know that the server is compromised, without having some form of auditing. Registry access to client machines is required for quick recovery from manipulation attacks, which target windows registry entries.

2 Required Background <>

We assume that the reader of this tutorial has an extent of background knowledge in the following areas:

1. Working experience on usage of computers and software applications, like web browsers, and virtualization software.
2. Basic overall idea of computer networks, Internet, and remote controlled configurations deployment.
3. Fundamental knowledge of remote client networks
4. An overall idea on general issues like credential security, system security, etc.,

Due to restrictions on time and manpower resources, we are not able to make the ensuing tutorial to be completely self-contained from the perspective of a user. As such, the tutorial is best used when the user already has certain background skills and knowledge. The following are some areas where we expect the users of this tutorial to have some previous skills/knowledge:

1. Practical experience on using computers, installing and using common software applications (particularly web browsers, and virtualization software platforms). The tutorial does not explain how to navigate within the operating system's graphical user interface (GUI). Similarly, the tutorial also does not explain how to browse the Internet, how to install software applications, and how to use/navigate software applications.
2. An overall idea on the working of computer networks and Internet. The tutorial expects a user to understand common terms like "server/client", "links", "domains/forests", and "policy enforcement" etc.,
3. Fundamental or very basic idea on features of remote client networks' working. The tutorial expects a user to understand technical terms like "administrative template", "computer configuration deployment", "remote registry access", and "caches" etc.,
4. Also bit of exposure to IT professional functions would be very helpful in tackling the challenges efficiently. An overall brief idea on general computer-related issues like "credential security", "system security", "network security", "large-scale remote configuration" etc., will help a lot.

3 Hardware and Software Requirements <>

We recommend having at least the following hardware and software specifications for smooth execution of this tutorial's activities and challenges:

1. A computer which can at least boot 2 virtual machines (VMs) smoothly, with no noticeable lag and delay.
2. A functional virtualization software platform. For example, VMWare or VirtualBox.
3. A vanilla Windows Server 2012 R2 (Controller) VM and a vanilla Windows 10 VM (Client).

For the purpose of getting the best experience out of this tutorial, there are certain minimum hardware and software requirements that we recommend users have at their disposal. However, this tutorial can also be carried out in lower specifications than what is recommended, at the cost of inconvenience ranging from minor to very annoying..

1. A computer powerful enough to boot 2 virtual machines without any noticeable delay or log. That would mean at least a quad-core processor, 8 GB RAM, optimally two monitors (can be managed with one at the cost of inconvenience), and a functional keyboard and mouse.
2. It is always recommended to use a virtual machine to run tutorials like the one available in this document so as to not destabilize one's own workstation or personal machine's environment and software configurations. To that extent, we recommend having a virtualization software installed on machine, which can be used to generate virtual machines as needed.
3. The present tutorial can be followed only with Windows Server 2012 R2 and an another Windows client OS (7 or greater). We recommend using a vanilla (default installation) Windows 10 virtual machine acting as client and Windows Server 2012 R2 acting as server/domain controller.

   Note: Please go to part **2** of the **Appendix** section for information on resources and website links to access some of the required software for the tutorial.

4 Problem Statement: Enterprise Configuration<>

- In an enterprise, how can one remotely configure large number of computers using same platform like windows, using minimum human support and involvement?

1. Most likely, organizations will fall victim to an exploit because of improper configuration of machines and incorrect assignment of usage permissions. Consider an example of a front desk administrative assistant unknowingly clicking a malicious script-attack link which floods the whole organization's machines with script-attack pop-ups because of improperly deployed machine configuration and incorrect allocation of machine usage permission to the administrative assistant.

2. Considering this problem, an organization's network administrator should assign only the minimum needed permissions to a user that are required to get his/her work done. In addition, the network administrator also has to configure each and every machine of the organization to protect against large-scale homogeneous attacks.

3. While the tasks mentioned above can be done easily in an organization with a couple of machines, such tasks would become exponentially expensive and time-taking as the size of organization increases. Even in a lower-middle sized organization with 5000 machines, it becomes very expensive to employ humans for the purpose of configuring machines and assigning permissions.

4. To address this problem, there are a few solutions, which will be briefly explained in the next slide.

5 Candidate Solutions: The Four Methods <>

1. Writing and deploying rule for each machine individually by Administrative staff.
2. Instead of hiring new staff, add the responsibility to existing unit supervisors.
3. Using third party software like Chef, Puppet, FreeIPA.
4. Using Microsoft Active Directory and Group Policy Objects.

1. The Administrative user can write set of rules for each group and the deployment of configurations and permissions can be manually done by human staff. This scenario might be acceptable for a start-up company with less than 20-25 machines, but highly expensive in an enterprise with bigger number of machines.
2. Instead of hiring dedicated staff for the deployment, we can merge the duties to that of a unit supervisor in each group and thus, required configurations and permissions can be assigned to every machine in a group by he group's supervisor. This process is less expensive than first, but it will bring down the production of supervisor's duties and there is also a increased risk of compromise/corruption within the supervisor.
3. Deployment of configurations and permission assignment can be done by using an additional third party software that connects to all the client machines and users. Software like Chef, Puppet and FreeIPA can be used to perform the above task. Chef and Puppet are configuration management tools that can deploy configurations remotely. Both Chef and Puppet have a high learning curve and are not GUI-based. As such, using those software methodologies requires training and higher pay of employees trained in them. FreeIPA can be considered as one fitting solution, but FreeIPA is limited to Linux-only operating systems.
4. We can use two services which are natively provided by the Windows operating system, which are Actives Directory and Group policy Objects in Windows Server. We can allocate a group of machines into a domain and for each domain, we can deploy configuration and allocate permissions. The only significant limitation for this solution is that Active Directory (AD) and Group Policy Objects (GPO) are only limited to Windows operating systems. FreeIPA tries to emulate the AD-GPO services on Linux, but is far less advanced.

6 Chosen Solution: Group Policy & Active Dir.<>

Group Policies through Active Directory:

1. Active Directory (AD) is a hierarchical management tool.
2. Group Policy (GP) is a large scale remote machine-configuration mechanism.
3. Domains are the clusters, on which GP operate.
4. Forest is a top layer hierarchy of tree structures.
5. Configure using group policies.

1. **Active Directory**: An Active Directory is a special purpose hierarchical database which is considered to be extensible and replicated. It is designed to handle a large number of search and read operations with significantly smaller number of changes and updates.
2. **Group Policy**: Group Policy in windows servers is a feature provided by the Windows that helps us to implement specific configuration for users. These group policy settings are linked to a Active directory container using a Group plicy objects.
3. **Domains**: A windows domain is a computer network, where all the users, computers, policies are registered with a central database know as Domain controller.
4. **Forest**: A tree is collection of one or more trees interlinked with a trust hierarchy. Forest is the top hierarchy of the tree structures.
5. The task of remote configuration starts by setting up the Domain in very initial stage. If we want to push our domain into a existing forest, we will include it in the forest. Else we create a new forest for our domain container. After, setting up domain and forest, we will add all the end clients systems that falls under the a group. Rules required for each group are configured into a group policy object and linked to the respective group.

7 Related Articles: GPO in News <>

1. Server 2012 makes GPO Editing easier (5th Dec. 2012). [1]
2. Windows Phone now supports GPO Editing. (20th June 2014) [2]
3. Windows patches critical security vulnerability. (11th Feb. 2015) [3]
4. Windows GPO Editing extended to LibreOffice. (12th Apr. 2015) [4]

1. Windows Server 2012 has three new features which enhance the functionality of GPO (Group Policy Objects) editing and make it easier to control domains using different object attributes through group policies. The enhancements are: Improved Troubleshooting, Remote Group Policy Updating, Infrastructure Status Management [1].

2. Windows Phone operating system, from version 8 onwards, have been made compatible with GPO editing mechanism, thus enhancing the diverse range of applications, which can be configured using group policy objects. Though growing, not all configurations are GPO compatible yet [2].

3. Critical Vulnerability in Group Policy had Windows computers stand at huge risk in first quarter of 2015. Publicly revealed after Microsoft patched the vulnerability, which could allow attackers to remotely execute code in the form of group policy objects. It was found and reported by JAS Global Advisors along with simMachines Security in January 2014. Unlike many popular application vulnerabilities, this was a design vulnerability and not an implementation vulnerability [3].

4. Group Policy template configuration has been made available for LibreOffice suite of tools, allowing GPO editing for LibreOffice on Windows a lot easier. Any of LibreOffice's 25,000 settings can be configured using GPO template through registry key modification [4].

8 Outline of Tutorial <>

- Intro to Domains, Clients and Systems.
- Hands-on exercises in GP configuration.
- Activities and Challenges:
  1. Common Security & Group-Policy Configurations.
  2. Firewall Management and Configuring Internet Explorer/Edge through Administrative Templates.
  3. Credentials, Authentication and Session Management.
  4. Secure Management of Domain Controllers & Clients.

The main purpose of this tutorial is to learn the art of controlling domain clients through domain controller, using group policy editing through active directory feature. Our narrowed focus approach will target the following aspects of GPO Editing:

1. **Common Security Enhancing Group-Policy Configurations:** With regards to this particular theme, we will learn using a hands-on approach as on how to disable password cache, disabling guest accounts, disabling LAN Manager (LM) and New Technology LAN Manager (NTLM), and finally disabling LM hash storage mechanism to restrict attack vector scope.
2. **Firewall Management, Configuring IE/ME through Administrative Templates:** Towards the fulfillment of this module's theme, we will learn how to remotely manage firewall configurations for domain clients in a domain and also we will learn remote configuring Internet Explorer and Microsoft Edge through GUI-based implementation of Administrative (ADM) Templates.
3. **Credentials, Authentication and Session Management:** With respect to this module's theme, we will learn how to manage credentials of domain clients like setting password length and setting password history. Managing authentication services like Kerboros protocol and Session management like account lockout threshold and etc., are also part of this module.
4. **Secure Management of Domain Clients:** Secure management of client systems in a domain can be done through many methods. In this module, we will learn how to disable task manager in client systems, how to setup auditing on domain controller and last, but not the least, we will also have a quick look at securely and remotely editing domain clients' Windows configurations by accessing Windows Registry on client systems.

9 Questions: Questions 1,2 <>

Q1: How many settings does LibreOffice have at large?

Q2: Since which version of Windows Phone, has it been made compatible with group policy objects?

Answer to Q1:
25000 Configurations, all compatible with group policy object editing.

Answer to Q2:
Since Windows Phone 8.1.

10 Background: Domains and Forests <>

Domains are:

1. Units of Partition.
2. Containers of Active Directory objects.
3. A group collection of client systems.

Forests are:

1. Distributed databases.
2. A top layer hierarchical structure of domain containers.

1. Domains are units of single partitions in a forest and each domain consists of its' respective active directory objects (users, computers, and groups). There will be a domain administration group for each and every domain, that has full control over the domain. We can say that if an object falls into a domain, then generally, it can be controlled by that particular domain's administrator. [14]

2. Every client system, in a particular domain, can be configured by linking the client system with a group policy object, using the respective group configurations. All the rules in GPO list are applicable only for the objects residing in a particular domain container.

3. A forest is a distributed database and is a top layer hierarchical structure of domain containers, which are considered to be functional units in the forest structure. Each domain container in the forest stores and manages it own active directory objects. Domain containers are also considered to be core functional units in the forest structure, each domain container in a forest is used primarily to manage their respective Active Directory objects.

11 Setting up the VMs <>

The tutorial requires one server OS and one non-server OS. For that purpose, we recommend using:

- A vanilla Windows 7/8/8.1/10 VM (We will be using Windows 10 EDU version). Also, this VM will be referred to as "non-server" VM in subsequent slides.
- A vanilla Windows 2012 R2 Server. This VM will be referred to as "server" VM.

We assume that the user following this tutorial has administrator-level privileges(*).

NOTE: It is recommended to assign static IP address to both the VMs. Click HERE [15] to visit an article, which brilliantly explains with pictures, about the process of assigning static IP addresses to machines.

NOTE 2: For the non-server VM's Default Gateway and Preferred DNS Server attributes, it is also recommended to assign a value same as the static IP address of Server VM.

* This tutorial cannot be replicated successfully without administrator level rights because the activities and challenges involved in the tutorial all require administrator rights.

12 Background Activity: Setting up Domain <>

1. In this slide, we will see step-by-step instructions on how to setup a Domain.
2. Followed by instructions on how to assign a system as domain controller.

Setting up a domain:
Boot up the Windows 2012 R2 Server VM. Once it starts up, follow:

1. Open "Server Manager" and navigate to "Dashboard". Click on "Manage" in the top-right part of server manager.
2. From the list of options, select "Add Roles and Features" option. Click on "Next" in the *Before You Begin* section.
3. In the *Select installation type* section of Add Roles and Features Wizard, click on **Role-based or feature-based installation** radio button and proceed by clicking on next.
4. In the *Select destination server* section, click on **Select a server from the server pool** radio button and subsequently, select the corresponding server (which should be a Microsoft Windows Server 2012 R2, if this tutorial is being followed). Proceed by clicking on next.
5. In the *Select server roles* section, check the boxes beside **Active Directory Domain Services** and **DNS Server** roles in the "Roles" list. Proceed by clicking on next.
6. In the *Select server roles* section, the "Add Roles and Features Wizard" will already have some features checked, which it deems necessary for the previously selected roles to work. These default checked features are sufficient. Proceed by clicking on next.
7. Skip the *Active Directory and Domain Services* section by clicking next.

8. In the *Confirm installation selections screen*, check the box beside **Restart destination server automatically if required**. Finish the selection mechanism by clicking on "Install" button.

9. In the subsequent screen, after installation, click on "Close" and restart the operating system if the wizard does not automatically restart the OS.

Assigning a system as Domain Controller:
Boot up the same Windows 2012 R2 Server VM, as above. Once it starts up, follow:

1. Open "Server Manager" and navigate to "Dashboard". Click on the flag-like looking icon, in the top-right part of server manager, to the left of "Manage".

2. From the list of options, click on the "Promote this server to a domain controller" option.

3. In the *Deployment Configuration* section of Active Directory Domain Services Configuration Wizard, click on radio button beside **Add a new forest** and in the text form field, give a name for forest in the format `blah.blahblah`. The tutorial will use the name `radicl.security`. Proceed by clicking on "Next" button.

4. In the *Domain Controller Options* section, let the default selections stay and do not change or add anything. In case Active Directory services fail, we can log into system using a password, called as Directory Services Restore Mode (DSRM) password. Give a password and re-type it for confirmation. Proceed by clicking on next.

5. In the *DNS Options* section, we will not be doing anything. Proceed by clicking next.

6. In the *Additional Options* section, the wizard will automatically assign a NetBIOS name in a few seconds. If `radicl.security` was used as the forest name, then, the NetBIOS will most likely be assigned as `RADICL`. If wanted, any name can be used, by changing the assigned value to desired name. However, just for the sake of consistency with the tutorial, `RADICL` is recommended. Proceed by clicking on next.

7. In the *Paths* section, the path for database, log files and SYSVOL are requested. Default assignment of path is usually good enough for most purposes. Proceed forward by clicking on next.

8. In the *Review Options* section, review the selection and proceed by clicking on next.

9. In the subsequent section titled *Prerequisites Check*, let the check be carried out. It takes a few minutes and then it shows either if all prerequisite checks passed or if some failed. If the tutorial was followed closely all through, prerequisite checks should pass successfully, without any errors, but with two warnings.

10. Proceed by clicking on "Install". After installation, the wizard should automatically restart the OS. If not, restart it manually.

13 Background Activity: Adding Clients <>

1. Clients are end users in a domain.
2. They have to be compliant towards the policies set by the domain controller of their resident domain.
3. In this section, we will take a look at the process of adding clients to a domain.

Adding Clients to the Domain:
Boot up the Windows non-server VM. Once it starts up, follow:

1. Go to *System Properties* by right clicking on the Windows icon (usually at the left-most position of task-bar) and by selecting "System" from the resultant pop-up list of items. For Windows 7, *System Properties* can be accessed by right clicking "Computer" icon or button in start menu and selecting "Properties".
2. In the subsequent dialogue box, click on "Change Settings" hyper-link, which is present to the right of the screen under *Computer name, domain, and workgroup settings* section.
3. In the *System Properties* wizard, under *Computer Name* tab, look for "Change" button beside the text *To rename the computer...* and click on the button.
4. In the *Computer Name/Domain Changes* dialogue box, look for a section called *Member of* and select the radio button beside *Domain:* field entry tag. A grayed out text field form will be rejuvenated, in which the forest name should be entered (as created in the previous slide), which would be **radicl.security** for this tutorial's purposes.
5. One will, most likely, be prompted to enter the login credentials of the administrator account belonging to the domain controller system (the 2012 R@ server machine). Enter the credentials, and after validating them, a pop-up box will notify of the success in adding a client machine to the domain.
6. A restart will be needed in order to implement the domain changes.

Thus, adding of client machines to a domain can be achieved by following the above mentioned steps. Now, let us move on with the activities and challenges.

14 Activity: Disabling Password Cache <>

1. Disable password cache in the Domain Controller.
2. Disable password cache in the Client Systems.

Password cache is temporary copy of the password, which is stored internally during an active session, thus creating a potential vector for exploitation of systems through mechanism of stealing password from caches. As such, it is highly recommended to disable password cache in any system, as any data item (not just password) stored in a system, is a data item which is vulnerable to a hacker's attack.

1. **Disable password cache in the Domain Controller:**

   Boot up the Windows server VM. Once it starts up, follow:

   (a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

   (b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

   (c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

   (d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

   (e) Expand Domain Controllers within the populated sub-folders.

   (f) Right click on "Default Domain Controllers Policy" and select "Edit...".

   (g) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

   (h) Subsequently, double click on "Policies".

(i) Next, double click on "Windows Settings".

(j) Followed by double clicking "Security Settings".

(k) Next, double click on "Local Policies".

(l) Finally, click on "Security Options" twice.

(m) In the resultant populated list of group policy objects, search for `Network Access: Do not allow storage of password and credentials for network authentication` and click twice on the item.

(n) In the subsequent pop up box, check the box beside *Define this policy setting:* and click on the radio button beside "Enabled".

2. **Disable password cache in the Client Systems:**

Boot up the Windows server VM. Once it starts up, follow:

(a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

(b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

(c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

(d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

(e) Consequently, right click on "Default Domain Policy" and select "Edit...".

(f) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

(g) Subsequently, double click on "Policies".

(h) Next, double click on "Windows Settings".

(i) Followed by double clicking "Security Settings".

(j) Next, double click on "Local Policies".

(k) Finally, click on "Security Options" twice.

(l) In the resultant populated list of group policy objects, search for `Network Access: Do not allow storage of password and credentials for network authentication` and double-click on the item.

(m) In the subsequent pop up box, check the box beside *Define this policy setting:* and click on the radio button beside "Enabled".

With that, we have enabled two group policies (which are effective on domain controller itself and client machines in domain as well), to not allow storage of password caches and credentials with respect to network authentication.

15 Activity: Disabling Guest User <>

Rationale behind disabling a guest user features:

- Fair amount of access to a system is provided for guest accounts.
- By default, guest users shares same amount of storage, as a standard user.
- Guest users can enter into a system without credentials being absolutely required.

If guest users are enabled, then our system grants fair amount of access to the guest user. To reduce the potential of exploit by a large margin, it is highly recommended to disable guest user logins. Through this activity, we will demonstrate how to disable guest user logins remotely, using group policy object editing.

1. **Disabling Guest User in the Domain Controller:**

   Boot up the Windows server VM. Once it starts up, follow:

   (a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

   (b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

   (c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

   (d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

   (e) Expand Domain Controllers within the populated sub-folders.

   (f) Right click on "Default Domain Controllers Policy" and select "Edit...".

   (g) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

   (h) Subsequently, double click on "Policies".

   (i) Next, double click on "Windows Settings".

(j) Followed by double clicking "Security Settings".

(k) Next, double click on "Local Policies".

(l) Finally, click on "Security Options" twice.

(m) In the resultant populated list of group policy objects, search for `Accounts: Guest account status` and click on the item twice.

(n) In the subsequent pop up box, check the box beside *Define this policy setting:* and click on the radio button beside "Disabled".

2. **Disabling Guest User in Client Systems:**

Boot up the server VM. Once it starts up, follow:

(a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

(b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

(c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

(d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

(e) Consequently, right click on "Default Domain Policy" and select "Edit...".

(f) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

(g) Subsequently, double click on "Policies".

(h) Next, double click on "Windows Settings".

(i) Followed by double clicking "Security Settings".

(j) Next, double click on "Local Policies".

(k) Finally, click on "Security Options" twice.

(l) In the resultant populated list of group policy objects, search for `Accounts: Guest account status` and double-click on the item.

(m) In the subsequent pop up box, check the box beside *Define this policy setting:* and click on the radio button beside "Disabled".

With that, we have enabled two group policies (which are effective on domain controller itself and client machines in domain as well), to disable guest user logins completely.

16 Activity: Forcing NTLM v2 <>

- LAN Manager(LM) and version 1 of New Technology LAN Manager(NTLM) are vulnerable to exploits.
- Particularly vulnerable to 'Reflection' attack and 'Pass The Hash' exploit.
- Windows Server 2012 R2 provides substitute module, NTLM v2, which is relatively very secure.
- As such, we disable LM and NTLM v1 to force the machines to use nothing but NTLM v2.

In this activity, we will demonstrate forcing NTLM v2 while disabling LM and NTLM v1, remotely using Group Policy Object editing.

1. **Forcing NTLM v2 in the Domain Controller:**

   Boot up the Windows server VM. Once it starts up, follow:

   (a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

   (b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

   (c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

   (d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

   (e) Expand Domain Controllers within the populated sub-folders.

   (f) Right click on "Default Domain Controllers Policy" and select "Edit...".

   (g) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

   (h) Subsequently, double click on "Policies".

   (i) Next, double click on "Windows Settings".

   (j) Followed by double clicking "Security Settings".

(k) Next, double click on "Local Policies".

(l) Finally, click on "Security Options" twice.

(m) In the resultant populated list of group policy objects, search for `Network security: LAN Manager authentication level` and click on the item twice.

(n) In the subsequent pop up box, check the box beside *Define this policy setting:* and from the drop down list, select *Send NTLMv2 response only. Refuse LM & NTLM.*

2. **Disabling Guest User in Client Systems:**

Boot up the server VM. Once it starts up, follow:

(a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

(b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

(c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

(d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

(e) Consequently, right click on "Default Domain Policy" and select "Edit...".

(f) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

(g) Subsequently, double click on "Policies".

(h) Next, double click on "Windows Settings".

(i) Followed by double clicking "Security Settings".

(j) Next, double click on "Local Policies".

(k) Finally, click on "Security Options" twice.

(l) In the resultant populated list of group policy objects, search for `Network security: LAN Manager authentication level` and click on the item twice.

(m) In the subsequent pop up box, check the box beside *Define this policy setting:* and from the drop down list, select *Send NTLMv2 response only. Refuse LM & NTLM.*

With that, we have enabled two group policies (which are effective on domain controller itself and client machines in domain as well), to force the machines into using NTLM v2 and disabling LM & NTLM v1 module usage.

17 Activity: LM password hashes <>

- LM password hashes are easy to crack
- Particularly vulnerable to 'Rainbow tables' attack, 'One way function' cracking attacks, 'Brute force' attack, and 'Replay the hash(Man-in-Middle)' attack.
- As such, we configure the machines to not store LM hashes anymore.

LM password hashes can be easily converted into the original plain text password, and a hacker can find them easily on a disk using some of the many Hash dump tool. As a result, it is highly recommended not to store them in the system. In this activity we will demonstrate how to disable storage of LM hash passwords, remotely using group policy object editing

1. **Disabling storage of LM hashes in the Domain Controller:**

   Boot up the Windows server VM. Once it starts up, follow:

   (a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

   (b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

   (c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

   (d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

   (e) Expand Domain Controllers within the populated sub-folders.

   (f) Right click on "Default Domain Controllers Policy" and select "Edit...".

   (g) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

   (h) Subsequently, double click on "Policies".

(i) Next, double click on "Windows Settings".

(j) Followed by double clicking "Security Settings".

(k) Next, double click on "Local Policies".

(l) Finally, click on "Security Options" twice.

(m) In the resultant populated list of group policy objects, search for `Network security: Do not store LAN Manager hash value on next password change` and click on the item twice.

(n) In the subsequent pop up box, check the box beside *Define this policy setting:* and click on the radio button beside "Enabled".

2. **Disabling storage of LM hashes in Client Systems:**

Boot up the server VM. Once it starts up, follow:

(a) Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

(b) Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

(c) Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

(d) After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

(e) Consequently, right click on "Default Domain Policy" and select "Edit...".

(f) In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

(g) Subsequently, double click on "Policies".

(h) Next, double click on "Windows Settings".

(i) Followed by double clicking "Security Settings".

(j) Next, double click on "Local Policies".

(k) Finally, click on "Security Options" twice.

(l) In the resultant populated list of group policy objects, search for `Network security: Do not store LAN Manager hash value on next password change` and click on the item twice.

(m) In the subsequent pop up box, check the box beside *Define this policy setting:* and click on the radio button beside "Enabled".

With that, we have enabled two group policies (which are effective on domain controller itself and client machines in domain as well), to force the machines into using NTLM v2 and disabling LM & NTLM v1 module usage.

18 Questions: Quiestions - 3,4 <>

Q3: Why are we trying to disable the storage of LM password hashes?

Q4: What is the reason behind Enterprises having multiple domain controllers in a single domain container?

Answer to Q3:
LM password hashes are easy to crack in order to obtain plain text passwords and a hacker can find them easily using a hash dump tool if they are stored on disk.

Answer to Q4:
In a single Domain controller model, if the domain controller gets compromised, then whole domain is under the purview of attacker. Or if the domain controller gets taken down, the entire domain container will have their domain features rendered non-functional. Therefore, it is always better to have more than one domain controller in a domain container.

19 Challenge I: Configuring Firewalls <>

1. Remotely configure Firewalls of Client systems, using group policy object editing for the following requirement configurations:
   (a) Enable logging.
   (b) Log dropped connections.
   (c) Log successful connections.
   (d) Set a custom path for log file.
   (e) Set maximum threshold size of the log.

Hint: Firewall is a part of Network Connections components and is usually controlled by administrators using templates

20 Challenge II: Internet Explorer/EDGE <>

1. Disable JavaScript in IE for domain clients from domain controller, using group policy object editing.
2. Block all Cookies in Edge for domain clients from domain controller, using group policy object editing.

Hint: JavaScript in IE is called as 'Active Scripting' and is a part of Internet Zone in the Control Panel of IE, and is usually controlled by administrators using templates.

21 Challenge III: Credentials Management <>

1. Set the following credential policy for domain clients, using group policy object editing:
   (a) Set minimum password length to 10 letters.
   (b) Set maximum Password Age to 30 days.

Hint: Password management is one of the critical account security settings in all of the available Windows settings.

22 Challenge IV: Authentication & Sessions <>

1. Set the following Authentication and Session management policy remotely, for clients from domain controller, using group policy object editing:

   (a) Lock out account after 4 invalid attempts

Bonus: Set maximum lifetime for "kerboros user ticket renewal" as 1 day

Hint: If you were able to finish Challenge III - Credentials Management, you should be able to complete this challenge. Keen observation is they key, perhaps?

23 Challenge V: Disable Task Manager <>

1. From domain controller, disable Task Manager for Client systems using group policy object editing.

Hint: Users have their configurations in a separate location, from the ones belonging to computers. Task Manager is disabled by administrators through templates. Ctrl+Alt+Del combination of keys is the most usual method of accessing Task Manager.

24 Challenge VI: Enabling Auditing <>

From domain controller, set the following policies for domain controller:

1. Enable Domain controller system's logon events auditing (For both successful and failed attempts).
2. Enable Domain controller system's policy change auditing (For both successful and failed attempts).

Hint: Since we are configuring domain controller from domain controller itself, we can assume that the required policy objects will be classified as 'Local Policies'. And auditing is a security setting of windows computers.

25 Challenge VII: Remote Registry Access <>

1. Remote Registry Access

   (a) Remotely access Clients machine's Windows Registry from the Domain Controller.

Hint: Enable Remote Registry feature in default domain policy for clients from controller. Client system's firewall generally blocks when someone tries to access its windows registry, so add an exception in Client's local group policy. Open registry editor from domain controller and connect to client registry.

26 Conclusion <

1. Secure configuration of for both domain controller and clients is important.
2. A Domain controller can issue group policies for all the domain clients and itself.
3. Even with secure configuration, no system is immune to exploitations.

1. A securely configured domain controller and substandard configurations for client systems is a terrible pitfall, to be avoided at all costs. Similarly, a well configured network of clients and a poorly configured domain controller will put the entire network at risk, which is to be highly avoided.
2. Thus, through the usage of group policy objects deployed with the help of active directory, we are able to configure both domain controller and client systems through domain controller, reducing the vulnerability vectors in both clients and controllers.
3. Even with secure configurations, there are many exploitations being carried out. Never being sloppy in system security and not taking even a minute detail for granted with regards to a system's security are needed along with secure configurations.

27 Appendix: Solutions and Change-log <

1. **Solutions to the Challenges:**
   (a) **Challenge I:**
      i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).
      ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.
      iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.
      iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).
      v. Consequently, right click on "Default Domain Policy" and select "Edit...".
      vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.
      vii. Subsequently, double click on "Policies".
      viii. Next, double click on "Administrative Templates".
      ix. Followed by double clicking "Network".
      x. Then, double click on "Network Connections".
      xi. Next, double click on "Windows Firewall".
      xii. Finally, click on "Domain Profile" twice.
      xiii. All the required group policy objects are available in the list of items present in the resultant screen.

(b) **Challenge II:**

Disabling JavaScript in Internet Explorer:

i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

v. Consequently, right click on "Default Domain Policy" and select "Edit...".

vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

vii. Subsequently, double click on "Policies".

viii. Next, double click on "Administrative Templates".

ix. Followed by double clicking "Windows Components".

x. Then, double click on "Internet Explorer".

xi. Next, double click on "Internet Control Panel".

xii. Subsequently, click on "Security Page" twice.

xiii. Finally, double-click on "Internet Zone".

xiv. The group policy object item is `Allow active scripting`.

xv. Double click the object item and select the "Enable" radio button, in the rejuvenated drop-down list, select the option "Disable".

Regarding Microsoft Edge Group Policies: During the era of Microsoft Windows Server 2012 R2, Edge browser was not released, as such, Edge cannot be configured through group policy objects from Server 2012 R2. However, Edge browser can still be configured from the Group Policy Management Editor of Client machine directly. The process of which, is as follows:

Block all Cookies in Microsoft Edge:

i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

v. Consequently, right click on "Default Domain Policy" and select "Edit...".
vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.
vii. Subsequently, double click on "Policies".
viii. Next, double click on "Administrative Templates".
ix. Followed by double clicking "Windows Components".
x. Then, double click on "Internet Explorer".
xi. Next, double click on "Internet Control Panel".
xii. Subsequently, click on "Security Page" twice.
xiii. Finally, double-click on "Internet Zone".
xiv. The group policy object item is `Allow active scripting`.
xv. Double click the object item and select the "Enable" radio button, in the rejuvenated drop-down list, select the option "Disable".

(c) **Challenge III:**

i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).
ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.
iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.
iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).
v. Consequently, right click on "Default Domain Policy" and select "Edit...".
vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.
vii. Subsequently, double click on "Policies".
viii. Next, double click on "Windows Settings".
ix. Followed by double clicking "Security Settings".
x. Then, double click on "Account Policies".
xi. Next, double click on "Password Policies".
xii. In this repository, there is the group policy objects needed to achieve challenge's requirements.

(d) **Challenge IV:**

i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).
ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

v. Consequently, right click on "Default Domain Policy" and select "Edit...".

vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

vii. Subsequently, double click on "Policies".

viii. Next, double click on "Windows Settings".

ix. Followed by double clicking "Security Settings".

x. Then, double click on "Account Policies".

xi. Next, double click on "Account Lockout Policies".

xii. In this repository, there is the group policy object needed to achieve challenge's requirements and also the bonus challenge requirement.

(e) **Challenge V:**

i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

v. Consequently, right click on "Default Domain Policy" and select "Edit...".

vi. In the *Group Policy Management Editor*, double click on "User Configuration" option in the middle pane.

vii. Subsequently, double click on "Policies".

viii. Next, double click on "Administrative Templates".

ix. Followed by double clicking "System".

x. Then, double click on "Ctrl + Alt + Delete options".

xi. In this repository, there is the group policy object needed to achieve challenge's requirements.

(f) **Challenge VI:**

i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

v. Consequently, right click on "Default Domain Controllers Policy" and select "Edit...".

vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

vii. Subsequently, double click on "Policies".

viii. Next, double click on "Windows Settings".

ix. Followed by double clicking "Security Settings".

x. Then, double click on "Local Policies".

xi. Next, double click on "Audit Policy".

xii. In this repository, there are all the group policy objects needed to achieve challenge's requirements.

(g) **Challenge VII:**

i. Open *Group Policy Management* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

v. Consequently, right click on "Default Domain Controllers Policy" and select "Edit...".

vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

vii. Subsequently, double click on "Policies".

viii. Next, double click on "Windows Settings".

ix. Followed by double clicking "System Services".

x. Then, double click on "Local Policies".

xi. Using the appropriate group policy object, "Enable Remote Registry", enable the functionalities of remote registry access.

Next, follow the following steps on Domain Controller:

i. Open *gpedit.msc* wizard (usually found by typing in `Group Policy` keyword into the search bar of windows).

ii. Once in the wizard box, expand the **Forest: radicl.security** (or whatever forest name was assigned earlier) which can be found in the left pane, under *Group Policy Management* categorization.

iii. Once *Forest: radicl.security* is expanded, within the resultant populated folders, expand the folder called as **Domains**.

iv. After expanding the domains folder inside forest, expand the domain radicl.security (or whatever name was assigned earlier).

v. Consequently, right click on "Default Domain Controllers Policy" and select "Edit...".

vi. In the *Group Policy Management Editor*, double click on "Computer Configuration" option in the middle pane.

vii. Subsequently, double click on "Administrative Templates".

viii. Next, double click on "Network".

ix. Then, double click on "Network Connection".

x. Subsequently, double click on "Windows Firewall".

xi. Finally, click on "Domain Profile" twice.

xii. In this repository, there is the "Allow Remote Administration Exception", using which, we should permit the remote administration on the particular domain.

In the last phase, we need to do the following:

i. Open *Windows Registry Editor* wizard (usually found by typing in ``regedit" keyword into the search bar of windows).

ii. Click on "File" drop-down menu and choose "Connect Network Registry" option by clicking on it.

iii. Click on the "Advanced" button.

iv. Click on "Find Now" button.

v. Select the desired client system from search results and click on the "OK" button.

2. **Tutorial-Related Resources:**

   A free virtualization software platform - VirtualBox - CLICK ME.

   An evaluation copy of Windows Server 2012 R2 - Microsoft - CLICK ME

   A Windows 10 VM with Microsoft Edge - CLICK ME

3. **Change-Log:**

Group Policies with Active Directory Tutorial			
Ver.	**Date**	**Authors**	**Changes**
v1	Feb. 24th 2016	Ananth Jillepalli and Nagajuna Nuthalapati	First draft of tutorial.
v2	Jun. 13th 2016	Ananth Jillepalli	Major content additions and remodeled the structure.
v2.1	May 31st 2016	Ananth Jillepalli	Added appendix and other minor enhancements.
v 2.2	July 31st 2017	Ananth Jillepalli	Changed the licensing from CC BY-NC-ND 4.0 to CC BY-NC-SA 4.0

References

[1] J. Peter Bruzzese, "3 ways Windows Server 2012 makes Group Policy Easier", last accessed 22nd Feb. 2016, http://www.tomshardware.com/news/firefox-tracking-protection-private-browsing,30484.html, 5th DECEMBER 2012.

[2] David Scammell, "Windows Phone 8.x is for Business!", last accessed on 22nd Feb. 2016, https://community.spiceworks.com/topic/236221-windows-phone-8-x-is-for-business, 20th JUNE 2014.

[3] Lucian Constantin, "Critical Vulnerability in Group Policy Puts Windows Computers at Risk", last accessed on 22nd Feb. 2016, http://www.cio.com/article/2883134/critical-vulnerability-in-group-policy-puts-windows-computers-at-risk.html, 11th FEBRUARY 2015.

[4] Sam Tuke, "Good news for Windows Server Administrators: Group Policy template for LibreOffice available", last accessed on 22nd Feb. 2016, https://www.collaboraoffice.com/community-news/new-group-policy-template/, 12th APRIL 2015.

[5] Microsoft Technet, "Deploying Windows Firewall Settings With Group Policy", last accessed on 22nd Feb. 2016, https://technet.microsoft.com/en-us/library/bb490626.aspx, 17th DECEMBER 2005.

[6] Microsoft Technet, "AD DS Auditing Step-by-Step Guide", last accessed on 22nd Feb. 2016, https://technet.microsoft.com/en-us/library/cc731607(WS.10).aspx, 15th MARCH 2010.

[7] Security Watch - Microsoft Technet, "Using SCW on Windows Server 2008", last accessed on 22nd Feb. 2016, https://technet.microsoft.com/en-us/magazine/2008.03.securitywatch.aspx, 13th SEPTEMBER 2008.

[8] Paul Schnackenburg, "Microsoft Security Compliance Manager: Security Settings Simplified", last accessed on 22nd Feb. 2016, https://technet.microsoft.com/en-us/magazine/hh489604.aspx, 4th DECEMBER 2012.

[9] Microsoft Download Center, "Microsoft Security Compliance Manager", last accessed on 22nd Feb. 2016, https://www.microsoft.com/en-sg/download/details.aspx?id=16776, 2016.

[10] Microsoft Technet, "Microsoft Security Compliance Manager - Key Features", last accessed on 22nd Feb. 2016, https://technet.microsoft.com/en-us/library/cc677002.aspx, 28th JANUARY 2013.

[11] Center for Internet Security, "CIS Microsoft Windows Server 2012 Benchmarks", last accessed on 22nd Feb. 2016, https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_Server_2012_Benchmark_v1.0.0.pdf, 17th DECEMBER 2012.

[12] Microsoft Technet, "Building Your First Domain Controller on 2012 R2", last accessed on 22nd Feb. 2016, http://social.technet.microsoft.com/wiki/contents/articles/22622.building-your-first-domain-controller-on-2012-r2.aspx, 6th MAY 2014.

[13] Microsoft Technet, "Securing Domain Controllers Against Attack", last accessed on 22nd Feb. 2016, https://technet.microsoft.com/en-us/library/dn535497.aspx, 16th JULY 2013.

[14] Microsoft Technet, "How Domains and Forests Work", last accessed on 22nd Feb. 2016, https://technet.microsoft.com/en-us/library/cc783351(v=ws.10).aspx, 19th NOVEMBER 2014.

[15] Brian Burgess, "How to assign a static IP address in Windows OS (XP to 10)", last accessed on 27th Jun. 2016, http://www.howtogeek.com/howto/19249/how-to-assign-a-static-ip-address-in-xp-vista-or-windows-7/, 10th NOVEMBER 2013.