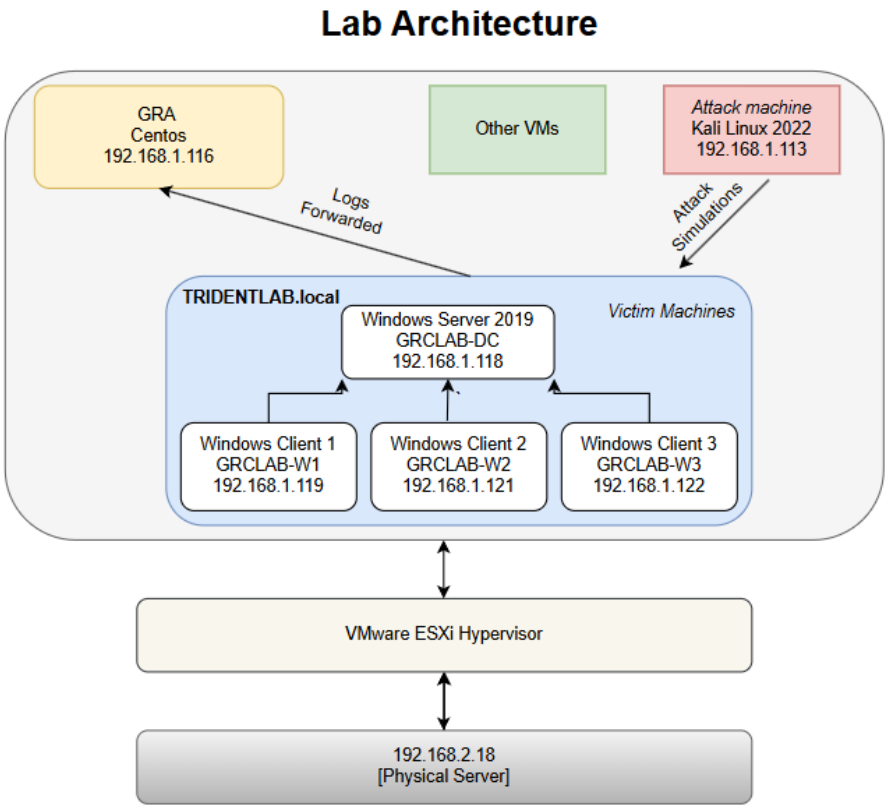
Introduction

The entire LAB Setup is on the Server: 192.168.2.18 . The VMware ESXi hypervisor is installed on the physical server which will serve all the virtualization needs.

The Lab Setup consists of a Domain Controller and 4 domain-joined machines which act as clients. The Windows Server 2019 is chosen to be the Domain Controller and the Windows 10 Enterprise machines, and Server 2016 are acting as clients. The above machines will be our victim machines. The latest Kali build is also installed which will be our attack machine. The goal of this exercise is to perform controlled attack simulations using our Kali machine on to the victim machines, capture these logs and send these logs to GRA for further analysis.



Lab Setup

Setting up the Domain Controller:

Let's, start by installing our **Windows Server 2019**. After the installation is complete, install VMware Tools which provides additional functionality like Time Synchronization, Snapshots etc.

The IP address of this machine is: **192.168.1.118**

Creds: {**Administrator**:**1qazxsW@!dc7}**

Let's change the name of our machine:

Click on start and enter 'View your PC name' -> Rename this PC -> **GRCLAB-DC** -> and restart this machine

This will be our domain controller. First, let's add the feature 'Active Directory Domain Services':

Goto Server Manager -> Manage -> Add Roles and Features

Click on Next -> Role-based or Feature Based -> Next -> select Active Directory Domain Services -> Next -> Add Features -> Next -> Install.

Next, look for the Yellow Notification flag on the Server Manager and click on it.

Select Promote this server to domain controller -> Add a new Forest -> "Name your domain here" – **TRIDENTLAB.local** -> Next
DSRM Password -> give it a password {**1qazxsW@!dsrm7**}
Keep clicking Next while keeping all defaults
Install and it the reboots machines

Login as MARVEL\Administrator

///Domain Controller Setup is now complete

Let's now setup **Windows 10 Enterprise** as Client Machines. The process is same for all client machines:

The installation process for this is same as any windows machine.

When sign in with Microsoft pops up -> Select Domain Join Instead

Client 1:
The IP address of this machine is **192.168.1.119**
Creds: {**athena:1qazxsW@!c1**}
> Install VMWare Tools
Restart Later
Let's change the name of our machine:

Click on start and enter 'View your PC name' -> Rename this PC -> **GRCLAB-W1** -> and restart this machine. Similarly, two more clients are setup

Client 2:

IP Address: **192.168.1.121**

Creds: {**artemis:1qazxsW@!c2**}

PC Name: **GRCLAB-W2**

Client 3:

IP Address: **192.168.1.122**

Creds: {**ares:1qazxsW@!c3**}

PC Name: **GRCLAB-W3**

Client 4:

IP Address: **192.168.1.111**

Creds: {**ares:1qazxsW@!c4**}

PC Name: **GRCLAB-W4**

///Workstation Setup is now complete

-----> Setup users, and policies

These settings are to be done on the domain controller:

Setup new users:
On the Server Manager -> Goto Tools -> Active Directory Users and Computers
Expand TRIDENTLAB.local
Right click -> New User
Create the same 3 users: athena, artemis and ares with same passwords as before.

-----> Creating a File Share
In Server manager -> Click on File and Storage Services -> Shares
Click on Tasks -> New Share
Defaults -> Next -> 'Enter Name of the share here'
All Defaults -> create and close

-----> Turning off Windows Defender
Open Group Policy Management [Run as Admin]
Right click on TRIDENTLAB.local -> Create a GPO -> Name: Disable Windows Defender
Right click this policy and edit
Computer Configuration -> Policies -> Admin Temp -> Windows Components
Browse to Windows Defender Antivirus
Click on "Turn off Windows Defender Antivirus"
Enabled -> Apply -> OK

Make sure Policy Enforced is set to 'Yes'

Joining Machines to Domain

On client Machines:

Goto Network Status -> Change adapter options -> Goto your adapter properties -> change TCP/IPv4 properties -> change your DNS server to the IP address of DC – 192.168.1.118 in this case.

Next,

Click on start and enter 'domain' -> click on 'Access work or school' -> connect

At bottom -> Join this device to a local Active Directory domain
Type Domain Name -> TRIDENTLAB.local
User: Administrator
Pass: 1qazxsW@!dc7
SKIP the next prompt
Restart Now

In the login screen,

Select Other User [We are logging as athena]
User: athena
Pass: 1qazxsW@!c1
Login

Sign out now and sign in as admin
Select other user
TRIDENTLAB \administrator
pass: 1qazxsW@!dc7
login

The same process needs to be repeated on all four machines. If all the steps are completed successfully, On DC, in active directory users and computers, all 4 machines should show up in computers OU.

Other Tools Installed

Sysmon:

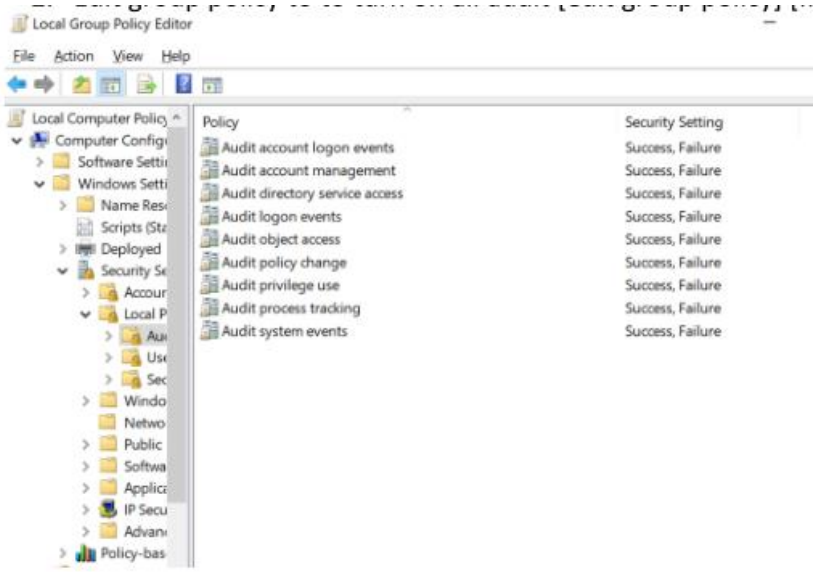
Sysmon is installed on all the victim machines for additional logging capabilities. It is setup with a popular configuration file.

https://github.com/SwiftOnSecurity/sysmon-config

Other Windows Auditing policies:

Set up a group policy on the domain controller to turn on additional windows auditing capabilities.

Set up all the below policies to log for success and failure.



Nxlog:

Nxlog is installed on all the victim machines to forward the captured logs to the target. The configuration file is already setup. Need to plug in the IP address and port to forward the logs to desired target.

Steps To Resolve the copy/paste issue between VM and host machine

Need to use a VMRC client and have the below configuration enabled in VM'S.

Steps:

1. Right-click the virtual machine and click **Edit Settings**.
2. Click the **VM Options** tab, symbol **Advanced**, and click **Edit Configuration**.
3. Fill in the **Name** and **Value** fields as mentioned below. After entering each one, click the **Add** button.

Name:	Value:
isolation.tools.copy.disable	FALSE
isolation.tools.paste.disable	FALSE
isolation.tools.setGUIOptions.enable	TRUE

Credentials Summarized

Domain Name: TRIDENTLAB.local

Alias	Hostname	OS	IP Address	Username	Password
Domain Controller	GRCLAB-DC	Windows Server 2019	192.168.1.118	Administrator	1qazxsW@!dc7
Client 1	GRCLAB-W1	Windows 10	192.168.1.119	athena	1qazxsW@!c1
Client 2	GRCLAB-W2	Windows 10	192.168.1.121	artemis	1qazxsW@!c2
Client 3	GRCLAB-W3	Windows 10	192.168.1.122	ares	1qazxsW@!c3
Client 4	GRCLAB-W4	Windows Server 2016	192.168.1.111	Administrator	1qazxsW@!c4
Kali Linux	kali	Kali Linux 2022	192.168.1.113	kali	kali
GRA Backend - root	centos	Centos 7	192.168.1.116	root	Gra4root!!!
GRA Backend - User				centos	Iamguru007
GRA Backend - SQL				root	UeBa_2020
GRA UI Login				graadmin	Iamguru007$

Other Details:

DC DSRM Password: 1qazxsW@!dsrm7

Default Gateway: 192.168.1.99

DHCP Server: 192.168.1.99

To login as a Domain User -> TRIDENTLAB\"*Username*"

To login as a local account -> In the username field simply enter **.**. The domain below will disappear, and switch to your local computer name. Then specify your local username after the **.**. It will use the local account with that username.

e.g -> .\athena