Microsoft Azure Cloud Security Audit using PowerShell

Parag Kamra

Paragkamra1994@gmail.com

Senior Security Analyst

Introduction

Introduction to Cloud

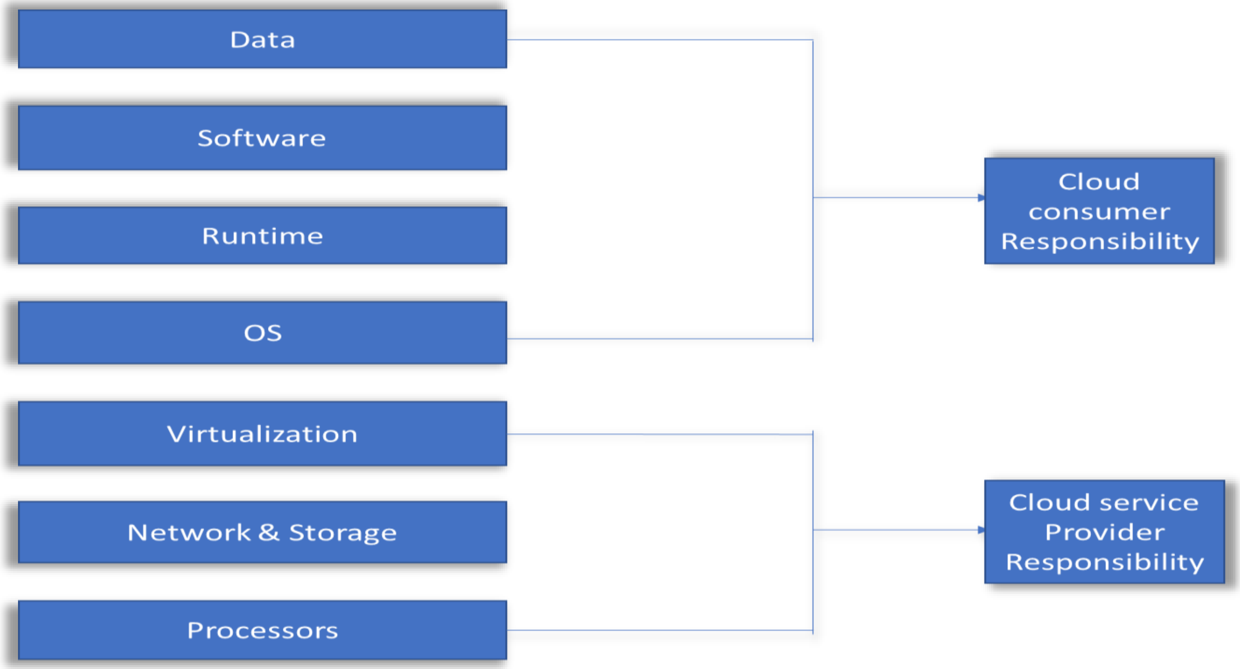
If we talk about cloud in very simple words we are moving our data center from on premises and hosting the applications, databases in Virtual Environment which we can access it from any location in all over the world. We are hosting our assets in shared infrastructure provided by Major Cloud service providers (CSP's) for example Amazon web services (AWS), Microsoft Azure and Google cloud platform. Cloud is very popular technology now days almost all the organizations are using cloud services i.e. Microsoft Office 365 which is SaaS Based Application.

Introduction to Microsoft Azure & Security

Microsoft Azure is a flexible, enterprise grade scale computing platform. It is a public cloud computing platform and they provide all three major services

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

Microsoft is very serious about security based on shared responsibility model on each service i.e. IaaS, PaaS, SaaS. Let's take one example on SaaS. SaaS is a software as a service model in this whole security is managed by Microsoft only for software including patch and vulnerability management the best example for this is Microsoft O365, but what about infrastructure as a service how Microsoft is sharing the responsibility with cloud consumer first let's talk about Infrastructure as a service, as name suggest a cloud consumer can build his own infrastructure on cloud including Virtual Machines, databases, Web Servers etc. let's refer the below screenshot of shared responsibility model on infrastructure as service (IaaS).


Data
Software
Runtime
OS
Virtualization
Network & Storage
Processors
Cloud consumer Responsibility
Cloud service Provider Responsibility

As you can see in above screenshot in the case of Infrastructure As a service the responsibilities are shared between cloud consumer and cloud service provider. In simple words the organization who is using cloud services infrastructure as a service they need to protect or secure their Operating systems, databases, web servers, firewalls, web-applications, API's etc. there are so many organizations who are using cloud services and they are not securing the cloud infrastructure which they are using as a datacenter. It is hard for security professional also to do audit of the cloud infrastructure they need to understand the cloud infrastructure and the services which are provided by cloud service providers, but now days securing the cloud infrastructure is very important and critical task for organizations. So, in the case of Microsoft azure we can use Azure PowerShell for doing the cloud Infrastructure audit.

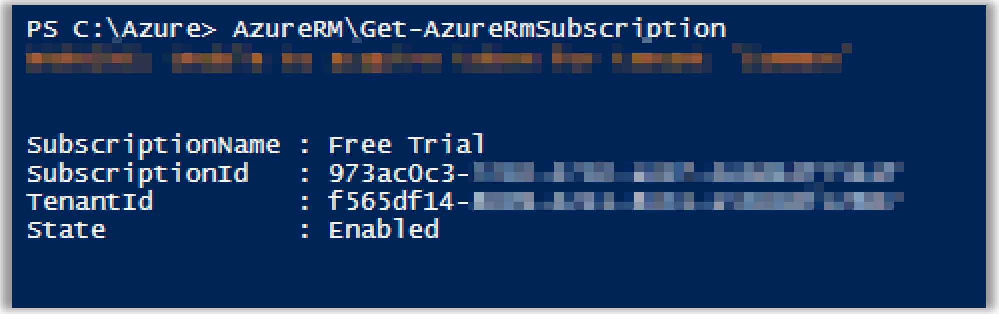
Introduction to Microsoft Azure PowerShell

As we all know PowerShell is very powerful and administrators are using it for automation and security professional are using it for post exploitation techniques. Azure PowerShell provides the sets of cmdlets that use the Azure Resources Manager model for managing the azure cloud services. Using Azure PowerShell we can create, update and delete the Virtual machines, change Network Security Groups which acts like a firewall in Azure.

Microsoft Azure Cloud Security Audit using Azure PowerShell

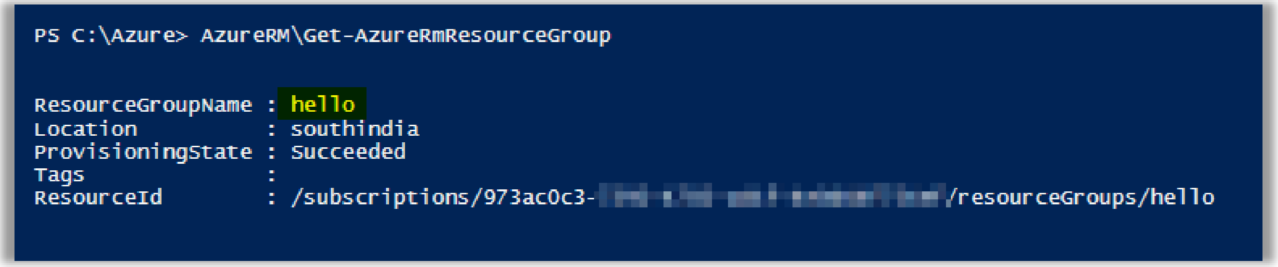
As a cloud security auditor it is very important to understand the security aspects of Microsoft Azure cloud and the services of Azure Cloud for example what is security groups, virtual networks etc. so, let's start with azure PowerShell for Microsoft cloud Security Audit.

1. First of all we need subscription id of an organization cloud account for accessing the azure resources subscription id is nothing but Azure Account unique id which is used for managing azure resources.



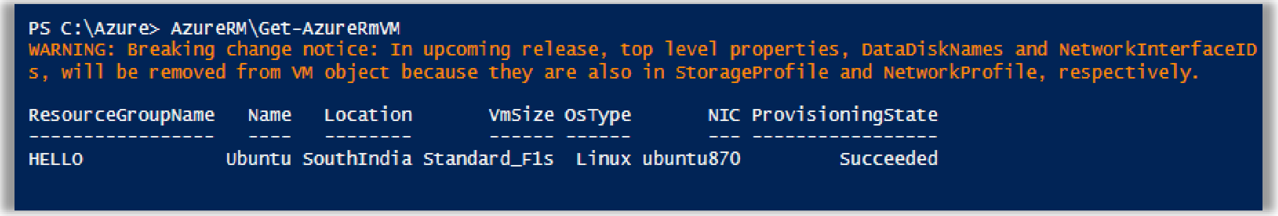
```
PS C:\Azure> AzureRM\Get-AzureRmSubscription
[redacted]


SubscriptionName : Free Trial
SubscriptionId   : 973ac0c3-[redacted]
TenantId         : f565df14-[redacted]
State            : Enabled
```

2. So, now next step is we want resource-group name from azure account. Resource group is a logical group in azure in which is used for deploying and maintaining the azure resources such as virtual machines, virtual network, storage network as a single entity.



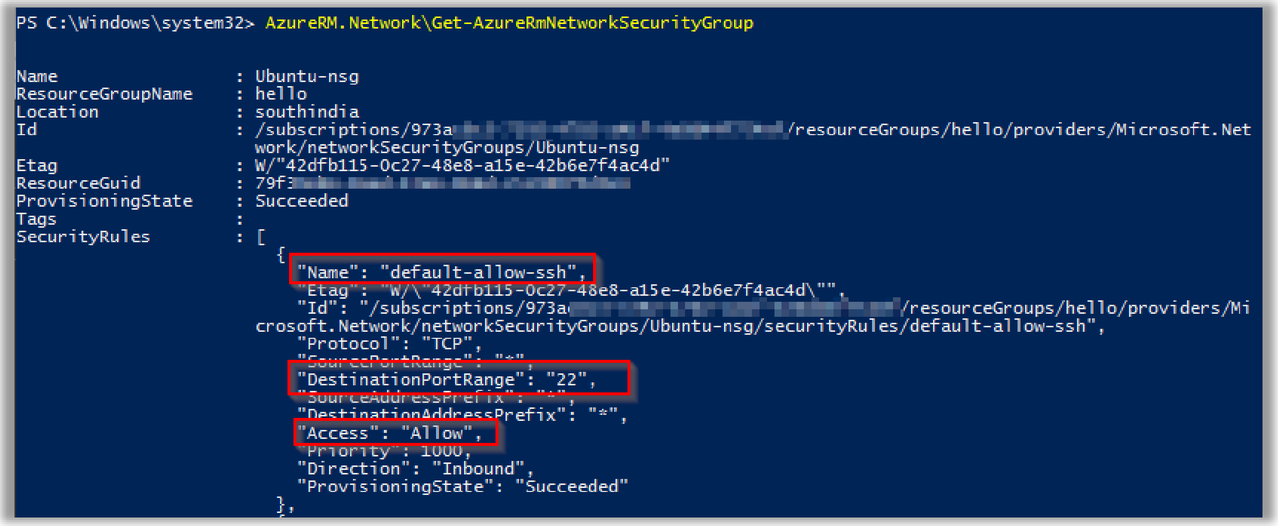
```
PS C:\Azure> AzureRM\Get-AzureRmResourceGroup


ResourceGroupName : hello
Location          : southindia
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/973ac0c3-[redacted]/resourceGroups/hello
```

3. So, now we now resource-group name is “hello” let’s check how many Virtual machines are running and what is the configuration of virtual machine and how the Network security group rules are set for example are any critical service is exposed to a public internet or not?

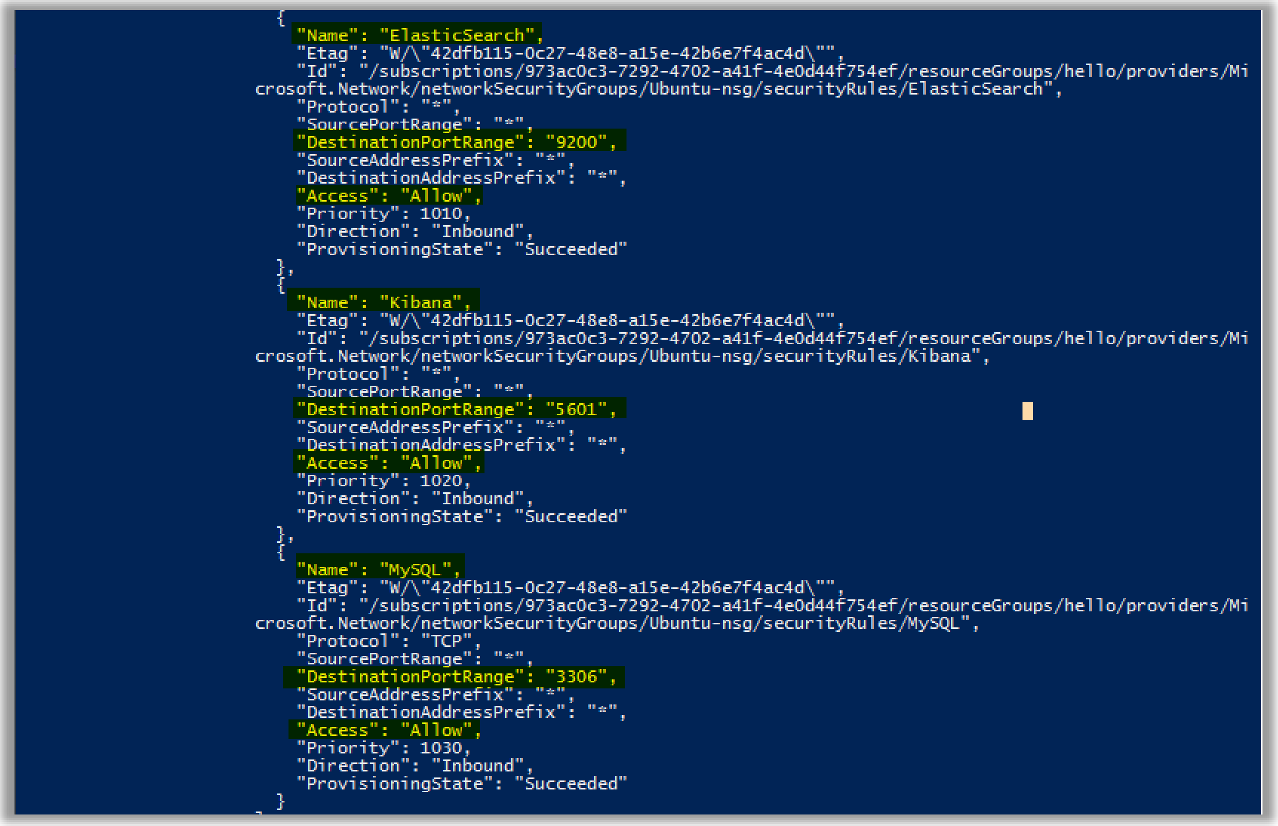


```
PS C:\Azure> AzureRM\Get-AzureRmVM
WARNING: Breaking change notice: In upcoming release, top level properties, DataDiskNames and NetworkInterfaceID
s, will be removed from VM object because they are also in StorageProfile and NetworkProfile, respectively.

ResourceGroupName   Name   Location      VmSize OsType      NIC ProvisioningState
-----------------   ----   --------      ------ ------      --- -----------------
HELLO             Ubuntu SouthIndia Standard_F1s  Linux ubuntu870         Succeeded
```

Ok. So now we now there is one virtual machine is running in “Hello” resource group. Let’s use another Azure PowerShell commands for check Network security groups which services are exposed over public internet if yes, what are the critical services are exposed over public internet.



```
PS C:\Windows\system32> AzureRM.Network\Get-AzureRmNetworkSecurityGroup


Name                   : Ubuntu-nsg
ResourceGroupName      : hello
Location               : southindia
Id                     : /subscriptions/973a[redacted]/resourceGroups/hello/providers/Microsoft.Net
                         work/networkSecurityGroups/Ubuntu-nsg
Etag                   : W/"42dfb115-0c27-48e8-a15e-42b6e7f4ac4d"
ResourceGuid           : 79f3[redacted]
ProvisioningState      : Succeeded
Tags                   :
SecurityRules          : [
                           {
                             "Name": "default-allow-ssh",
                             "Etag": "W/\"42dfb115-0c27-48e8-a15e-42b6e7f4ac4d\"",
                             "Id": "/subscriptions/973a[redacted]/resourceGroups/hello/providers/Mi
                         crosoft.Network/networkSecurityGroups/Ubuntu-nsg/securityRules/default-allow-ssh",
                             "Protocol": "TCP",
                             "SourcePortRange": "*",
                             "DestinationPortRange": "22",
                             "SourceAddressPrefix": "*",
                             "DestinationAddressPrefix": "*",
                             "Access": "Allow",
                             "Priority": 1000,
                             "Direction": "Inbound",
                             "ProvisioningState": "Succeeded"
                           },
```



```
  {
    "Name": "ElasticSearch",
    "Etag": "W/\"42dfb115-0c27-48e8-a15e-42b6e7f4ac4d\"",
    "Id": "/subscriptions/973ac0c3-7292-4702-a41f-4e0d44f754ef/resourceGroups/hello/providers/Mi
crosoft.Network/networkSecurityGroups/Ubuntu-nsg/securityRules/ElasticSearch",
    "Protocol": "*",
    "SourcePortRange": "*",
    "DestinationPortRange": "9200",
    "SourceAddressPrefix": "*",
    "DestinationAddressPrefix": "*",
    "Access": "Allow",
    "Priority": 1010,
    "Direction": "Inbound",
    "ProvisioningState": "Succeeded"
  },
  {
    "Name": "Kibana",
    "Etag": "W/\"42dfb115-0c27-48e8-a15e-42b6e7f4ac4d\"",
    "Id": "/subscriptions/973ac0c3-7292-4702-a41f-4e0d44f754ef/resourceGroups/hello/providers/Mi
crosoft.Network/networkSecurityGroups/Ubuntu-nsg/securityRules/Kibana",
    "Protocol": "*",
    "SourcePortRange": "*",
    "DestinationPortRange": "5601",
    "SourceAddressPrefix": "*",
    "DestinationAddressPrefix": "*",
    "Access": "Allow",
    "Priority": 1020,
    "Direction": "Inbound",
    "ProvisioningState": "Succeeded"
  },
  {
    "Name": "MySQL",
    "Etag": "W/\"42dfb115-0c27-48e8-a15e-42b6e7f4ac4d\"",
    "Id": "/subscriptions/973ac0c3-7292-4702-a41f-4e0d44f754ef/resourceGroups/hello/providers/Mi
crosoft.Network/networkSecurityGroups/Ubuntu-nsg/securityRules/MySQL",
    "Protocol": "TCP",
    "SourcePortRange": "*",
    "DestinationPortRange": "3306",
    "SourceAddressPrefix": "*",
    "DestinationAddressPrefix": "*",
    "Access": "Allow",
    "Priority": 1030,
    "Direction": "Inbound",
    "ProvisioningState": "Succeeded"
  }
```

Seriously, is it true? What I have identified in above screenshots the virtual machine is totally insecure and the reason is there are so many services which are exposed over public internet and services are very critical.

- SSH
- Elastic Search
- Kibana
- MySQL

As you can see in above screenshots these four Services are exposed over public internet anyone can try to make the connection on these services let's check what these services does.

- **SSH:** as all we know ssh is secure shell which is used for making connecting to the machine via SSH Keys and Password based authentication. By default, the password based authentication is enabled for Microsoft Azure Linux Virtual Machines. it means if attacker knows the Public IP Address of virtual machines attacker can try to do the brute force attack on SSH Server and if he gets successful he can compromise the hosts. So, it is never recommended to expose the SSH Server over the internet.

- **Elastic Search:** Elastic Search is very famous now a day. Elastic search can be used to search all kind of documents in the case of ELK stack "elastic search, logstash, kibana" elastic search is used for store the data for example logs and if the elastic search server service is exposed to an internet. Attackers can try to target elastic search service for checking weak passwords and try to do brute force attack.

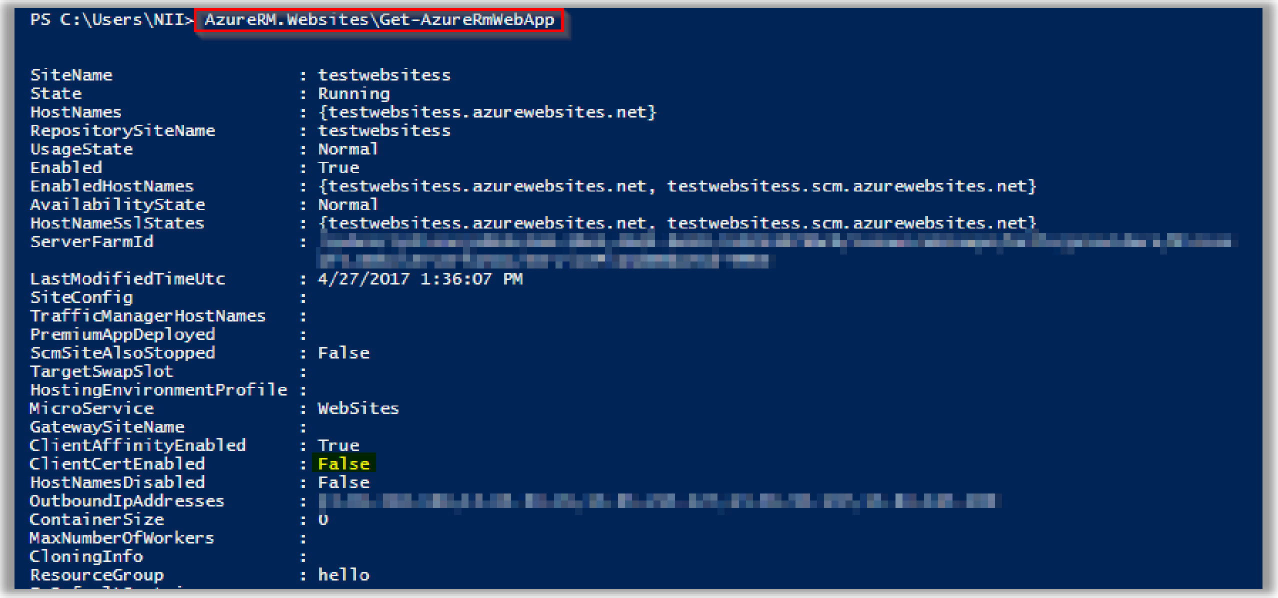
- **Kibana:** Kibana is a visualization tool for visualize the data and search the data from elastic search server. By default there is no authentication for kibana and if this service is exposed over public internet. An attacker can access the kibana server and delete the logs etc.

- **MySQL:** we all know what is MySQL Service and exposing this service to public network it would be a serious issue because an attacker can try to compromise the MySQL database and damage the whole data even he can dump it or delete the data also.

4. Ok so let's move on to check whether any web application is running or not if it is running whether it is on HTTP or HTTPS. Below is the command which is used for get the status of application.

```
AzureRM.Websites\Get-AzureRmWebApp
```

Below screenshot shows the one application is installed in cloud and the application is not configured for Mutual Authentication, But the question is why TLS Mutual authentication is important for securing web-application.



```
PS C:\Users\NII> AzureRM.Websites\Get-AzureRmWebApp


SiteName                  : testwebsitess
State                     : Running
HostNames                 : {testwebsitess.azurewebsites.net}
RepositorySiteName        : testwebsitess
UsageState                : Normal
Enabled                   : True
EnabledHostNames          : {testwebsitess.azurewebsites.net, testwebsitess.scm.azurewebsites.net}
AvailabilityState         : Normal
HostNameSslStates         : {testwebsitess.azurewebsites.net, testwebsitess.scm.azurewebsites.net}
ServerFarmId              : [redacted]

LastModifiedTimeUtc       : 4/27/2017 1:36:07 PM
SiteConfig                :
TrafficManagerHostNames   :
PremiumAppDeployed        :
ScmSiteAlsoStopped        : False
TargetSwapSlot            :
HostingEnvironmentProfile :
MicroService              : WebSites
GatewaySiteName           :
ClientAffinityEnabled     : True
ClientCertEnabled         : False
HostNamesDisabled         : False
OutboundIpAddresses       : [redacted]
ContainerSize             : 0
MaxNumberOfWorkers        :
CloningInfo               :
ResourceGroup             : hello
```

So, you have admin panel in your application and it is used for administrating the application. On other hand it is pretty sensitive place. If someone gained access it would be not good. But what if admin panel was not reachable by anyone but you can access. so, the way could require TLS Mutual authentication in this client itself authenticate himself on server side with client side certificate.

Conclusion

This is a short writeup on azure cloud security audit with PowerShell which show without using 3rd party tools we can check lots of security related issues in azure cloud for example databases, virtual network issues etc.