Report Settimanale

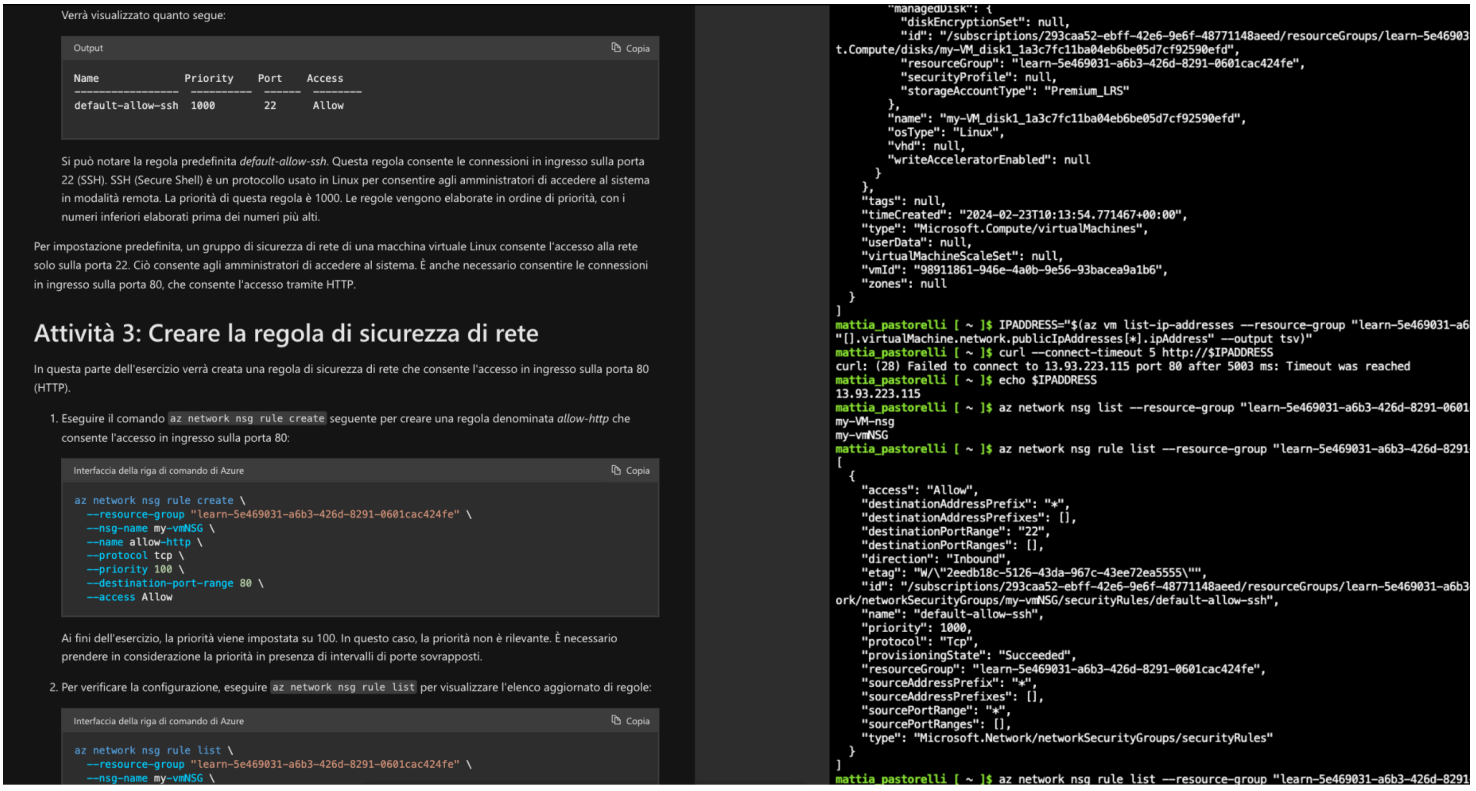
Questa settimana è stata incentrata sulla formazione per future certificazioni, quali:

- Cisco Certification Cybersecurity and Network Basics
- Azure Fundamentals Certification + possibile esame a pagamento

Inoltre, ho eseguito ricerche su altre tipologie di informazioni per successivi corsi formativi, quali Python, Certificazioni per Azure aggiuntive e AWS.

Di seguito un paio di screenshot degli argomenti trattati questa settimana:

AZURE:



Verrà visualizzato quanto segue:

Output — Copia

```
Name              Priority    Port    Access
----------------  ----------  ------  --------
default-allow-ssh  1000        22      Allow
```

Si può notare la regola predefinita *default-allow-ssh*. Questa regola consente le connessioni in ingresso sulla porta 22 (SSH). SSH (Secure Shell) è un protocollo usato in Linux per consentire agli amministratori di accedere al sistema in modalità remota. La priorità di questa regola è 1000. Le regole vengono elaborate in ordine di priorità, con i numeri inferiori elaborati prima dei numeri più alti.

Per impostazione predefinita, un gruppo di sicurezza di rete di una macchina virtuale Linux consente l'accesso alla rete solo sulla porta 22. Ciò consente agli amministratori di accedere al sistema. È anche necessario consentire le connessioni in ingresso sulla porta 80, che consente l'accesso tramite HTTP.

Attività 3: Creare la regola di sicurezza di rete

In questa parte dell'esercizio verrà creata una regola di sicurezza di rete che consente l'accesso in ingresso sulla porta 80 (HTTP).

1. Eseguire il comando `az network nsg rule create` seguente per creare una regola denominata *allow-http* che consente l'accesso in ingresso sulla porta 80:

Interfaccia della riga di comando di Azure — Copia

```
az network nsg rule create \
  --resource-group "learn-5e469031-a6b3-426d-8291-0601cac424fe" \
  --nsg-name my-vmNSG \
  --name allow-http \
  --protocol tcp \
  --priority 100 \
  --destination-port-range 80 \
  --access Allow
```

Ai fini dell'esercizio, la priorità viene impostata su 100. In questo caso, la priorità non è rilevante. È necessario prendere in considerazione la priorità in presenza di intervalli di porte sovrapposti.

2. Per verificare la configurazione, eseguire `az network nsg rule list` per visualizzare l'elenco aggiornato di regole:

Interfaccia della riga di comando di Azure — Copia

```
az network nsg rule list \
  --resource-group "learn-5e469031-a6b3-426d-8291-0601cac424fe" \
  --nsg-name my-vmNSG \
```


```
        "managedDisk": {
          "diskEncryptionSet": null,
          "id": "/subscriptions/293caa52-ebff-42e6-9e6f-48771148aeed/resourceGroups/learn-5e46903
t.Compute/disks/my-VM_disk1_1a3c7fc11ba04eb6be05d7cf92590efd",
          "resourceGroup": "learn-5e469031-a6b3-426d-8291-0601cac424fe",
          "securityProfile": null,
          "storageAccountType": "Premium_LRS"
        },
        "name": "my-VM_disk1_1a3c7fc11ba04eb6be05d7cf92590efd",
        "osType": "Linux",
        "vhd": null,
        "writeAcceleratorEnabled": null
      }
    },
    "tags": null,
    "timeCreated": "2024-02-23T10:13:54.771467+00:00",
    "type": "Microsoft.Compute/virtualMachines",
    "userData": null,
    "virtualMachineScaleSet": null,
    "vmId": "98911861-946e-4a0b-9e56-93bacea9a1b6",
    "zones": null
  }
]
mattia_pastorelli [ ~ ]$ IPADDRESS="$(az vm list-ip-addresses --resource-group "learn-5e469031-a6
"[].virtualMachine.network.publicIpAddresses[*].ipAddress" --output tsv)"
mattia_pastorelli [ ~ ]$ curl --connect-timeout 5 http://$IPADDRESS
curl: (28) Failed to connect to 13.93.223.115 port 80 after 5003 ms: Timeout was reached
mattia_pastorelli [ ~ ]$ echo $IPADDRESS
13.93.223.115
mattia_pastorelli [ ~ ]$ az network nsg list --resource-group "learn-5e469031-a6b3-426d-8291-0601
my-VM-nsg
my-vmNSG
mattia_pastorelli [ ~ ]$ az network nsg rule list --resource-group "learn-5e469031-a6b3-426d-8291
[
  {
    "access": "Allow",
    "destinationAddressPrefix": "*",
    "destinationAddressPrefixes": [],
    "destinationPortRange": "22",
    "destinationPortRanges": [],
    "direction": "Inbound",
    "etag": "W/\"2eedb18c-5126-43da-967c-43ee72ea5555\"",
    "id": "/subscriptions/293caa52-ebff-42e6-9e6f-48771148aeed/resourceGroups/learn-5e469031-a6b3
ork/networkSecurityGroups/my-vmNSG/securityRules/default-allow-ssh",
    "name": "default-allow-ssh",
    "priority": 1000,
    "protocol": "Tcp",
    "provisioningState": "Succeeded",
    "resourceGroup": "learn-5e469031-a6b3-426d-8291-0601cac424fe",
    "sourceAddressPrefix": "*",
    "sourceAddressPrefixes": [],
    "sourcePortRange": "*",
    "sourcePortRanges": [],
    "type": "Microsoft.Network/networkSecurityGroups/securityRules"
  }
]
mattia_pastorelli [ ~ ]$ az network nsg rule list --resource-group "learn-5e469031-a6b3-426d-8291
```

CISCO:

Networking Academy

Certificate of Course Completion

Mattia Pastorelli

has successfully achieved student level credential for completing the Introduction to Cybersecurity course.

The student was able to proficiently:

- Explain the basics of being safe online, including what cybersecurity is and its potential impact.
- Explain the most common cyber threats, attacks, and vulnerabilities.
- Explain how to protect oneself while online.
- Explain how organizations can protect their operations against these attacks.
- Access a variety of information and resources to explore the different career options in cybersecurity.

Networking Academy
Verified
Introduction to Cybersecurity

Scan to Verify

February 20, 2024

Laura Quintana

Laura Quintana
Vice President and General Manager
Cisco Networking Academy