Microsoft Defender for Cloud

Microsoft Defender for Cloud Playbook: Linux Detections

Version 3.0

Prepared by

Vasavi Pasula
Senior Program Manager
Defender for Cloud C+AI Security CxE

Reviewed by

Yuri Diogenes
Principal PM Manager
Defender for Cloud C+AI Security CxE

Introduction

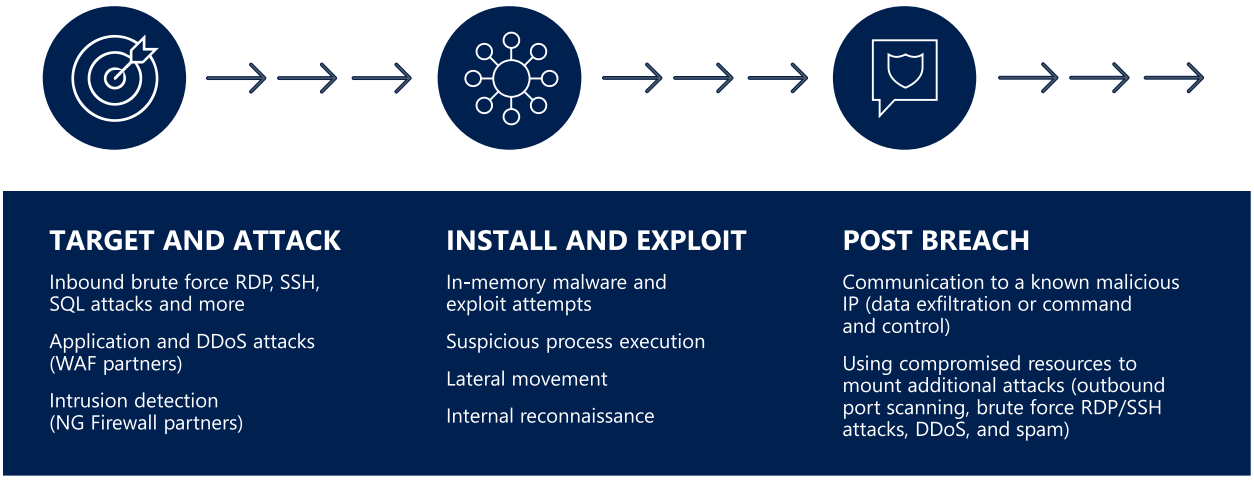
The goal of this document is to provide validation steps to simulate attacks against Linux VMs/Computers protecteded by Microsoft Defender for Cloud. You should use the steps described in this document in a *lab environment*, with the purpose to better understand the detection capabilities for Linux platform available in Microsoft Defender for Cloud.

Microsoft Defender for Cloud uses a variety of detection capabilities to alert customers to potential attacks targeting their environments. For Linux, Microsoft Defender for Cloud uses *auditd* to collect records from Linux machines. Auditd records are collected, aggregated into events, and enriched using the latest version of the Microsoft Monitoring Agent. Audit events are stored in your workspace and analyzed by Microsoft Defender for Cloud.

Microsoft Defender for Cloud employs advanced security analytics, which includes:

- **Integrated threat intelligence**: looks for known bad actors by using global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds.
- **Behavioral analytics**: applies known patterns to discover malicious behavior.
- **Anomaly detection**: uses statistical profiling to build an historical baseline. It alerts on deviations from established baselines that conform to a potential attack vector.

Using these analytics, Microsoft Defender for Cloud can help to disrupt the cyber kill chain by adding detection in different phases of the cyber kill chain as shown in the diagram below:



The example above shows some common alerts for each phase, and there are several more types of alerts. In this exercise, we will:

- Demonstrate an SSH brute force attack as part of the target and attack phase, and how Microsoft Defender for Cloud detects this type of attack.
- Demonstrate a suspicious compilation occurring in the installation and exploitation phase, and how Microsoft Defender for Cloud detects this type of attack.
- Demonstrate a remote shell execution as part of the post breach phase, and how Microsoft Defender for Cloud detects it this type of attack.

Target Audience

This document is for IT and Security Professionals interested in a deep technical dive into how Microsoft Defender for Cloud detects threats. Use this document as either a hands-on guide or as a guide to validate security detections against attacks.

Scenario

In this scenario the attacker (VM1) will initiate by sending a SSH Brute Force attack against its target machine (VM2), after gaining access to it, it will start to compile a suspicious file and to finalize the attack, it will initiate a remote shell with another machine. For this example, the remote shell execution will be done against VM1. Optionally you could provision three VMs and perform the last step against VM3, but this is not mandatory.

Resources

You will need an Azure environment with at least two Linux Ubuntu Virtual Machine (VM), these VMs should have the following Linux distribution installed:

- VM1: Kali Linux obtained from Azure Marketplace.
- VM2: Ubuntu versions 12.04 LTS, 14.04 LTS or 16.04 LTS, 18.04 LTS, 20.04 LTS (for the latest list of supported Ubuntu versions, visit Supported platforms article).
    - VM2 is the only one that you should ensure that the Log Analytics agent is installed and operational.
    - Make sure to take note of the public IP address of this VM after provisioning it.

Note: for more information on how to provision a Linux VM in Azure, visit this article.

Considerations regarding your Azure Environment

VM1

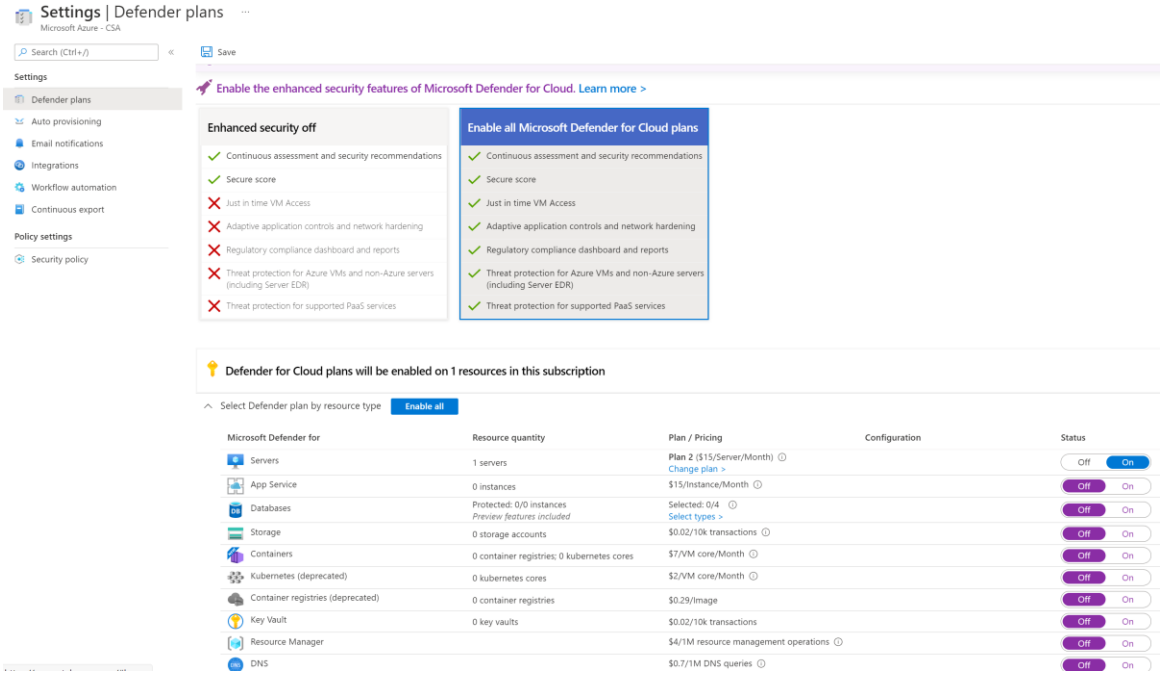
1. When provisioning this VM, make sure to enable external access through SSH.
2. Make sure to take note of the public IP address of this VM after provisioning it.

VM2

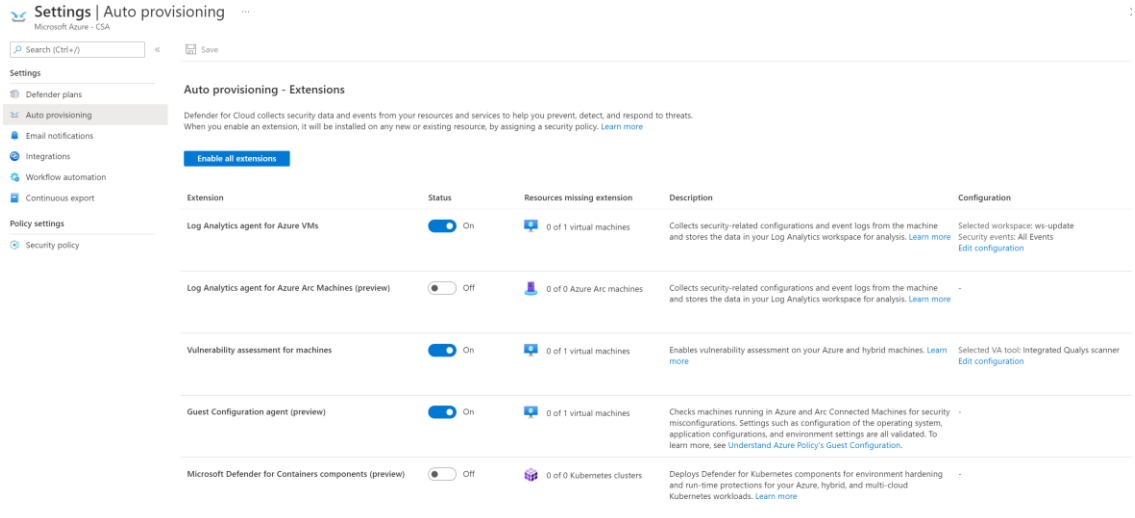
1. When provisioning this VM, make sure to enable external access through SSH.
2. Make sure to take note of the public IP address of this VM after provisioning it.
3. After provisioning VM2, check if auditd is running by using *service auditd status*
4. If the command fails, is because you don't have auditd installed. In this case, install auditd using the command *sudo apt install auditd*
5. Once it finishes, verify if auditd is running by using the same command that you used in step 1.
6. Create 5 local users account in this VM (use any name and password you want)

Microsoft Defender for Cloud

1. Defender for Cloud is enabled for free on all your Azure subscriptions when you visit the workload protection dashboard in the Azure portal for the first time. Enable enhanced security to extend the capabilities of the free mode to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. (The enhanced security features are free for the first 30 days.)
2. Enable Microsoft Defender for Servers at the subscription level, set it to **On**. Plan 2 is selected by default. (optionally you can disable other defender plans for this lab)

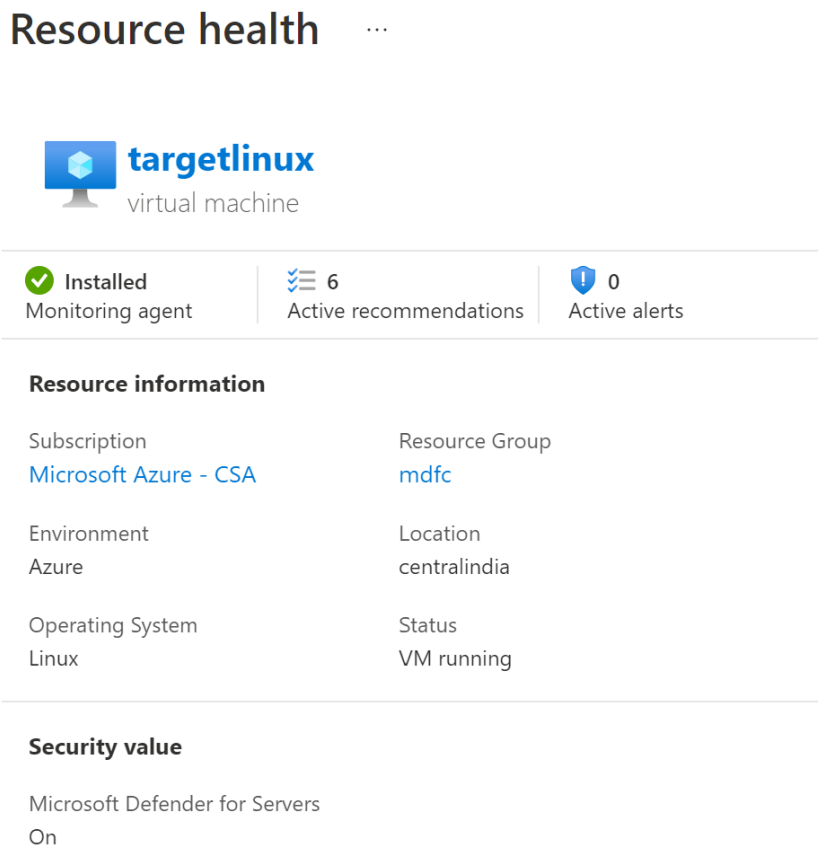


3. Ensure auto provisioning is on for the Log Analytics agent. Defender for Cloud deploys the agent on all supported Azure VMs and any new ones created. Read [Enable Data Collection]() article for more details on this.



4. Visit the VM resource health page which provides a snapshot view of the overall health of the VM. Read [Resource Health]. Review the Monitoring agent is installed on your machine and

Defender for Servers is **on** as shown in the screenshot below.



Note: it can take up to 12 to 14 hours to have the agent in a healthy state. Don't proceed to the tests unless it is healthy. If after 14 hours the status is not healthy, use the monitoring agent health issues table from the troubleshooting guide to address the issue.

Executing the Attack

The steps that follow are grouped in the different phases of the cyber kill chain mentioned in the Introduction section of this guide.

Cyber kill chain phase: Target and Attack

SSH brute force attack against Linux Servers is still a widely used method to establish the initial footprint. In 2018 attackers used the GoScanSSH to target public facing SSH servers, while avoiding those that were linked to government and military IP addresses. Without a monitoring system in place, the likelihood that this attack will succeed, and you will not be aware is high. If your workload is in Azure, you can reduce the likelihood that this attack will succeed, by using just-in-time VM access feature in Microsoft Defender for Cloud. To simulate how Microsoft Defender for Cloud will detect this attack, execute the steps below:

1. To launch the SSH brute force attack from the Kali Linux machine, you will need to use a built-in list of users and passwords. Since this is a very long list, you will create a reduced copy of this file. Logon to VM1 using SSH, and perform the following tasks

```
cd  /usr/share/wordlists

gzip -d rockyou.txt.gz

sudo cp rockyou.txt user.txt

sudo cp rockyou.txt pass.txt
```

2. Using your preferred text editor, open the user.txt file and leave only 20 entries in there (remove all other words). Once you finish, add the name of the 5 users that you created on VM2. Make sure to randomize the location, for example: insert one valid username after the fifth entry, another after the seventh entry and so on.

3. Repeat the same procedure but now for the file pass.txt. However, in this case, you will insert the valid passwords that you used for those five accounts that you created. Randomize the password in a different order that you randomize the user name.

4. Now that everything is in place, you can use Hydra to launch your attack against VM2. Type the command below, and replace <IP> for the VM2 public IP address:

```
hydra -I -L user.txt -P pass.txt <IP> -t 4 ssh
```

5. Wait until it finishes, and the result should show you the username and the password that was found.

Cyber kill chain phase: install and exploit

On this phase of the cyber kill chain, Microsoft Defender for Cloud will look for lateral movement, suspicious process execution, and other type of actions that are usually executed on this phase. An attacker could use this phase to launch a hacking tool to perform malicious operations.

1. Run the command below to simulate an attacker that is trying to start *logkeys* to set up the system to capture credentials and other useful information:

```
logkeys --start
```

Note: if you don't have *logkeys* installed, you will receive an error message, but for the purpose of this example, don't worry about the error message.

2. Attackers can also use this phase to perform internal recon and based on the data launch attack against other system within the internal network. For this example, the assumption is that the attacker already performed some internal recon using nmap to enumerate the servers and domain, and now he is going to use a hacking tool to launch an attack against one web server. Run the command below:

```
perl slowloris.pl -dns server.contoso.com
```

Note: you will receive an error message if you don't have this script on your system, but for the purpose of this example you don't need to worry about this error.

Cyber kill chain phase: post breach
On this phase of the cyber kill chain, attackers usually will communicate with command and control (C2) to either transfer data to C2 or download more malicious software. For this example, you will download the EICAR malware test file using WGET for the IP address. F

First, obtain the IP address of the target:

```
nslookup eicar.com
```

Now replace the XXX.XXX.XXX.XXX on the command below with the IP obtained from *nslookup*:

```
wget http://XXX.XXX.XXX.XXX/download/eicar.com
```

Once you finish, you can delete this test file:

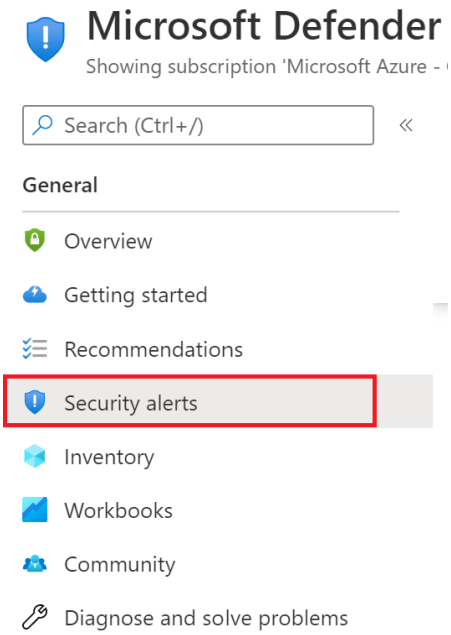
```
sudo rm eicar.com -f
```

Reviewing Microsoft Defender for Cloud Alerts

Now is time wo review the alerts generated by Microsoft Defender for Cloud during this simulation. Follow the steps below to do that:

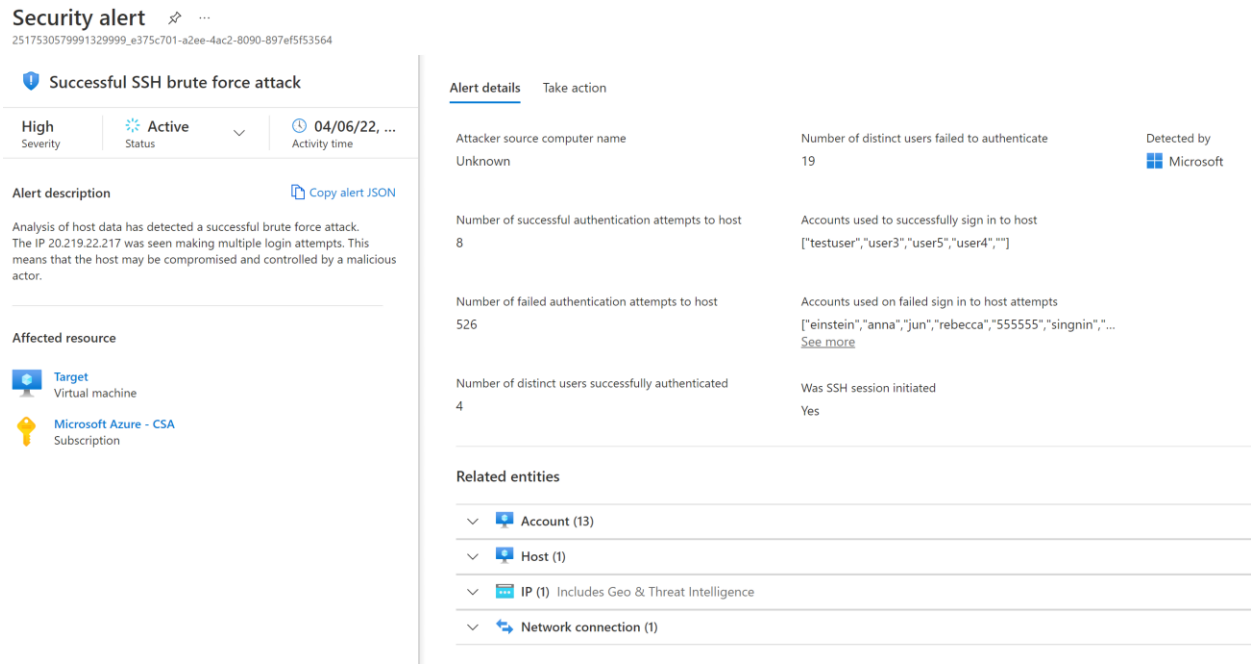
1. Open Microsoft Defender for Cloud dashboard

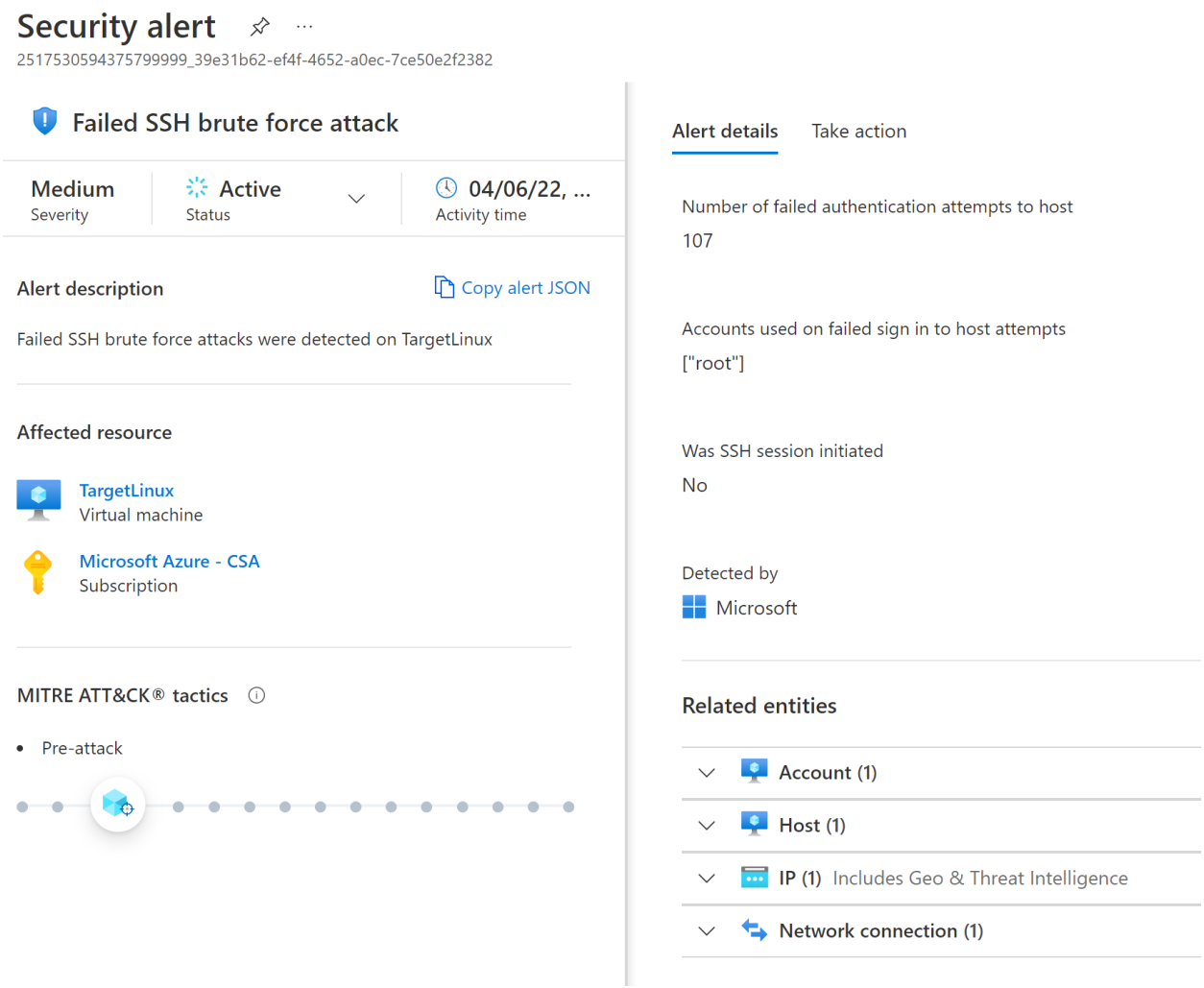
2. On the left pane, click Security Alerts



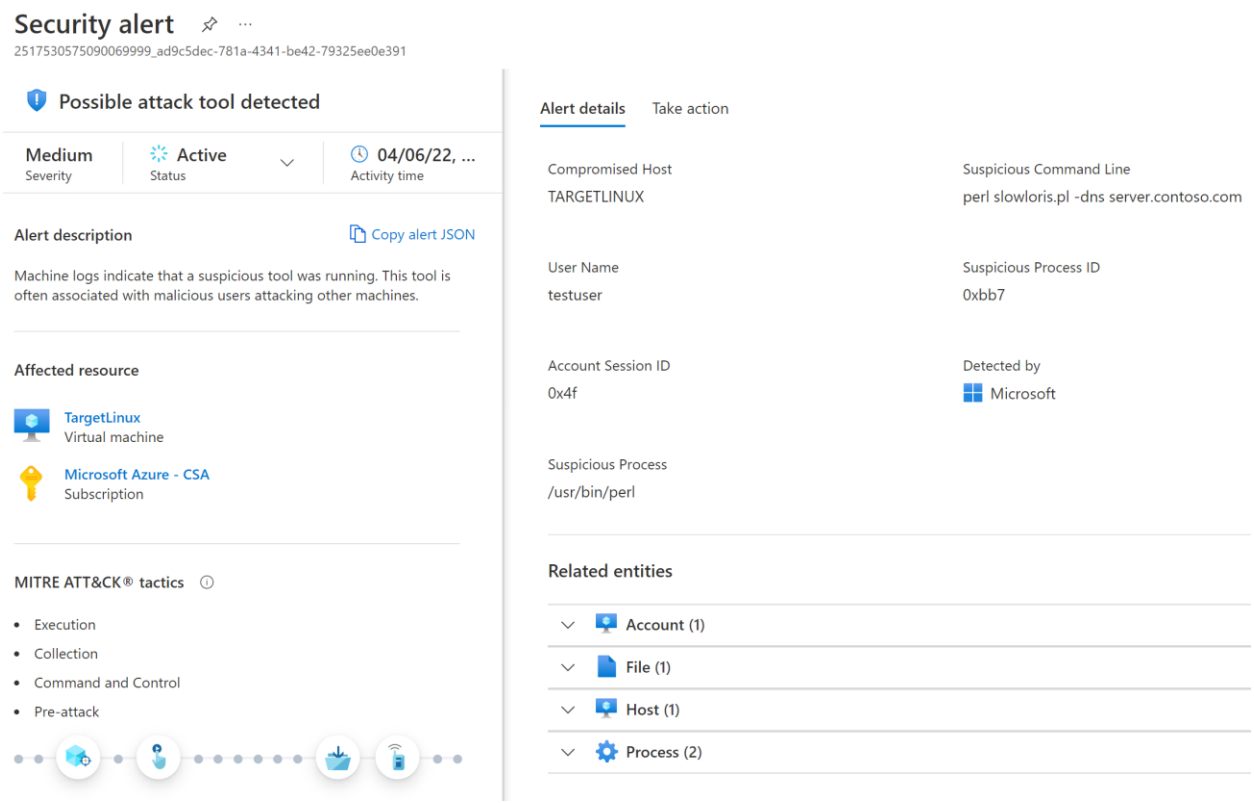
3. Organize the alerts by date by clicking on the **Activity start time** column and start reviewing it.

Notice that the alerts you will receive correspond to the SSH brute force attack simulation. In the description of this attack, you will see the username that successfully login via SSH.

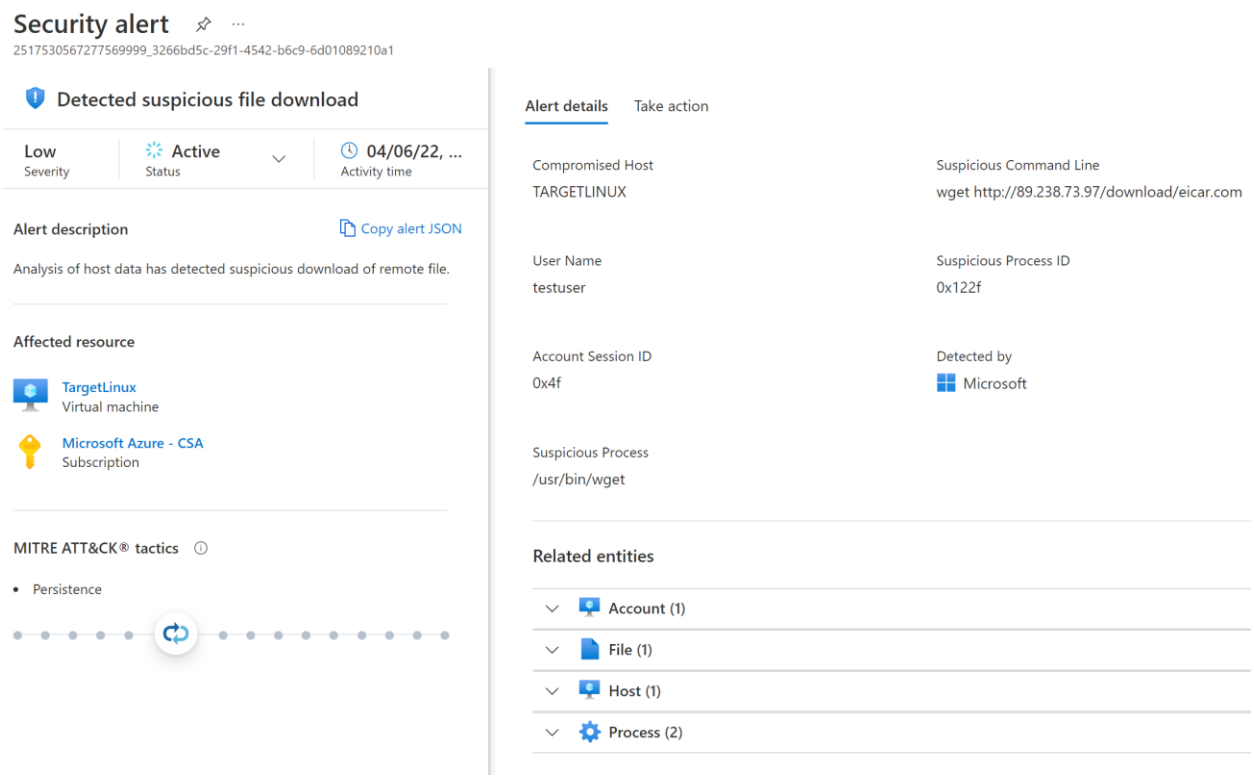




Next you will see hacking tool detection, through the **Possible attack tool detected** alert. This alert shows the details about the command line, and the suspicious process ID, as shown below:



The last alert from the list is the **Detected suspicious file download**, which has the details about the command line that was executed to download the malware test file.



Conclusion

In this exercise we demonstrated how Microsoft Defender for Cloud Linux Detections can be used to detect diverse types of attacks in a Linux system. Microsoft Defender for Cloud detections capabilities can be used to detect suspicious processes, dubious login attempts, kernel module loading/unloading, and other activities that could indicate that a machine is under attack or have been breached.

Other resources

- Microsoft Defender for Cloud Documentation Page
- Microsoft Defender for Cloud – Whats New
- Microsoft Defender for Server Plans
- Investigate a Security Alert
- Automate responses to Microsoft Defender for Cloud triggers