

# Azure Security Center

## Security Center Playbook: Linux Detections

Version 2.0

### ***Prepared by***

**Yuri Diogenes**

Senior Program Manager

Microsoft C+AI Security CxE

@yuridiogenes

***Reviewed by***

Ram Pliskin, Senior Program Manager (Microsoft Azure Security Center ILDC)

John Booth, Senior Security Software Engineer (Microsoft Threat Intelligence)

Mor Weinberger, Security Software Engineer (Microsoft Azure Security Center, ILDC)

Nicholas DiCola, Principal Program Manager, Microsoft C+AI Security CxE

Tiander Turpijn, Senior Program Manager, Microsoft C+AI Security CxE

Andrew Harris, Principal Program Manager, Microsoft C+AI Security CxE

This document is provided “as is.” MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Microsoft, Azure, and Windows are trademarks of the Microsoft group of companies. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## Introduction

The goal of this document is to provide validation steps to simulate attacks against Linux VMs/Computers monitored by Azure Security Center (“Security Center”). 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 Security Center.

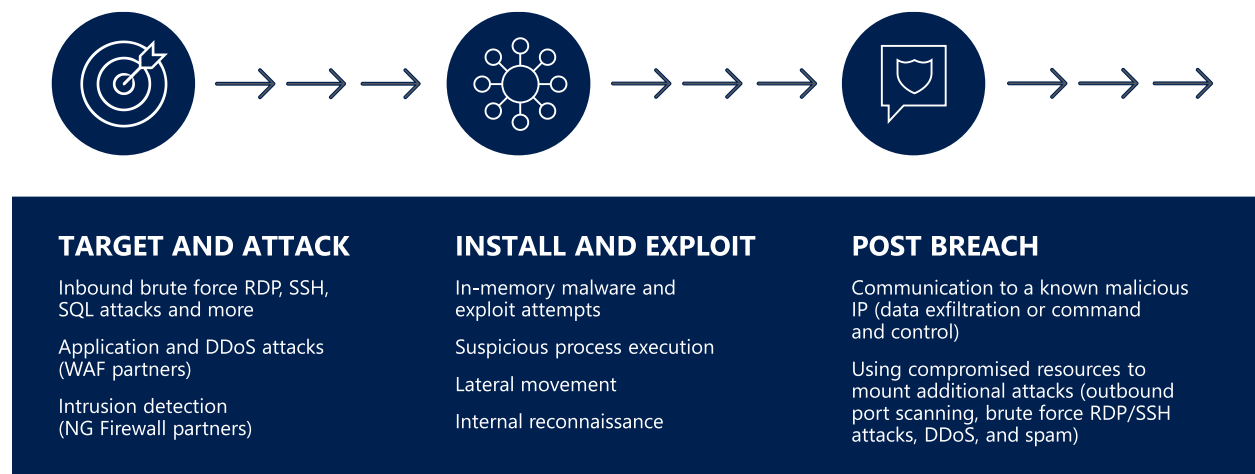
Security Center uses a variety of [detection capabilities](#) to alert customers to potential attacks targeting their environments. For Linux, Security Center uses *auditd* framework to collect records from Linux machines, however it does not require the *auditd* daemon to be running. Auditd records 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 Security Center. When threats are detected, a Security Center alert like the one below is generated.

**Note:** for the latest version of the Linux agent, visit this [page](#).

Security Center 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, Security Center 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 in this exercise, we will:

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

## Target Audience

This document is for IT and Security Professionals interested in a deep technical dive into how Security Center 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 (for the latest list of supported Ubuntu versions, visit [Supported platforms in Azure Security Center](#) article).
  - VM2 is the only one that you should ensure that the Security Center 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 password authentication
  - 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 password authentication
  - Enable external access through SSH.
2. Make sure to take note of the public IP address of this VM after provisioning it.
3. Create 5 local users account in this VM (use any name and password you want). These users will be used during the first exercise (SSH brute force attack)

## Security Center

- After provisioning this VM, enable Azure Security Center in the subscription level, and the agent will be automatically installed on the VM. Read [Enable Data Collection](#) article for more details on this.
  - If you are using an existing subscription with Azure Security Center already enabled, and auto provision is off due business reasons, you need to install the agent manually. Refer to [this article](#) for more information on how to install.
- If you are not using Azure Security Center Standard tier yet, you will need to [migrate your Security Center](#) subscription to Standard (Free Trial is valid for 60 days)
- Before proceeding, open Security Center dashboard, go to Compute & apps option in the left pane, Click **VMs & Computers** tab, click in the VM where Ubuntu is installed (VM2) and make sure that the **Monitoring State** field is showing as **Monitored by Azure Security Center**. Also review the Monitoring agent health issues and Install monitoring agent on your machine's assessments are showing as **healthy**, as shown in the example below:

^ information	
RESOURCE NAME	UBVM1
RESOURCE GROUP	MYORGCST
SUBSCRIPTION	Free Trial
VERSION	Compute
WORKSPACE	defaultworkspace
MONITORING STATE	Monitored by Azure Security Center
OPERATING SYSTEM	Linux
SYSTEM UPDATES	Microsoft (Last scan time - 9/28/2018 5:16 AM)
SECURITY CONFIGURATIONS	Microsoft (Last scan time - 9/27/2018 9:13 AM)

^ Recommendation list	
<a href="#">Recommendations</a>	<a href="#">Passed assessments (5)</a> <a href="#">Unavailable assessments (3)</a>
DESCRIPTION	STATUS
🔧 Troubleshoot missing scan data on your machines	🟢 Healthy
🔧 Restart your machines to apply system updates	🟢 Healthy
🔧 Resolve monitoring agent health issues on your machines	🟢 Healthy
🔧 Install system updates on your machines	🟢 Healthy

**Note:** it can take up to 12 to 14 hours to have the agent in 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. To reduce this time, you can provision a new VM with the agent already installed, you can use [this ARM template](#) as an example of how to accomplish this task.

## 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 Security Center. To simulate how Security Center 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
sudo 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 (you may need to use sudo) 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 in your Kali VM, 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, Security Center 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. The commands that follows must be executed in VM2 (Ubuntu VM):

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 because Security Center will detect anyway.

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. The commands that follows must be executed in VM2 (Ubuntu VM):

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
```

**Note:** if you have issues download eicar.com, try download eicar.txt (same command line, just change the extension).

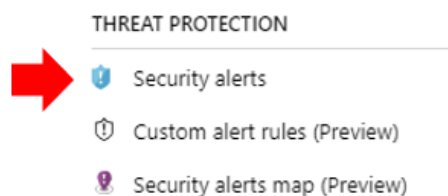
Once you finish, you can delete this test file:

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

## Reviewing Security Center Alerts

Now is time to review the alerts generated by Security Center during this simulation. Follow the steps below to do that:

1. Open Azure Security Center dashboard.
2. On the left pane, click **Security Alerts**.



3. Organize the alerts by date by clicking on the **Date** column, and start reviewing it.





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

Successful SSH brute force attack
UBVM2

Learn more

### General information

DESCRIPTION	Analysis of host data has detected a successful brute force attack against UBVM2. The IP 23.96.19.31 was seen making multiple login attempts. Successful logins were made from that IP with the following user(s): ysis. This means that the host may be compromised and controlled by a malicious actor.
DETECTION TIME	Friday, September 28, 2018, 8:40:16 AM
SEVERITY	<span style="color: red;">!</span> High
STATE	Active
ATTACKED RESOURCE	UBVM2
SUBSCRIPTION	Free Trial
DETECTED BY	 Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	 Virtual Machine



**Note:** this attack may take a little longer to appear in the dashboard.

Next you will see the *logkeys* detections through the **Potential credential access tool detected** alert. In this alert's description you may see another process name (instead of *logkeys*) in case you don't have this tool. In the example that follows, the process *python3.6*.

Possible credential access tool detected
UBVM2

Learn more

### General information

DESCRIPTION	Machine logs indicate that the suspicious process: '/usr/bin/python3.6' was running on UBVM2. This tool is often associated with attacker attempts to access credentials.
DETECTION TIME	Monday, October 1, 2018, 8:50:03 AM
SEVERITY	<span style="color: orange;">!</span> Medium
STATE	Active
ATTACKED RESOURCE	UBVM2
SUBSCRIPTION	Free Trial
DETECTED BY	 Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	 Virtual Machine
ACCOUNT SESSION ID	0x2
SUSPICIOUS COMMAND LINE	/usr/bin/python3 /usr/lib/command-not-found -- logkeys
SUSPICIOUS PROCESS ID	0x7eab




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:

## Possible attack tool detected

UBVM2


[Learn more](#)

### General information

DESCRIPTION	Machine logs indicate that the suspicious process: '/usr/bin/perl' was running on UBVM2. This tool is often associated with malicious users attacking other machines in some way.
DETECTION TIME	Monday, October 1, 2018, 8:44:04 AM
SEVERITY	 Medium
STATE	Active
ATTACKED RESOURCE	<a href="#">UBVM2</a>
SUBSCRIPTION	<a href="#">Free Trial</a>
DETECTED BY	 Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	 Virtual Machine
ACCOUNT SESSION ID	0x2
SUSPICIOUS COMMAND LINE	perl slowloris.pl -dns server.contoso.com
SUSPICIOUS PROCESS ID	0x7cbe




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.

## Detected suspicious file download

UBVM2


[Learn more](#)

### General information

DESCRIPTION	Analysis of host data has detected suspicious download of remote file on UBVM2.
DETECTION TIME	Monday, October 1, 2018, 4:04:53 PM
SEVERITY	 Low
STATE	Active
ATTACKED RESOURCE	<a href="#">UBVM2</a>
SUBSCRIPTION	<a href="#">Free Trial</a>
DETECTED BY	 Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	 Virtual Machine
ACCOUNT SESSION ID	0x2
SUSPICIOUS PROCESS	/usr/bin/wget
SUSPICIOUS COMMAND LINE	wget http://[REDACTED]/download/eicar.com
SUSPICIOUS PROCESS ID	0x1475

## Conclusion

In this exercise we demonstrated how Security Center Linux Detections can be used to detect diverse types of attacks in a Linux system. Security Center 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

- [Azure Security Center Documentation Page](#)
- [Azure Security Center Playbook: Security Alerts](#)
- [Azure Security Center Playbook: Hunting Threats](#)
- [Azure Security Center Threat Protection](#)
- [Azure Security Center Security Alert Reference Guide](#)