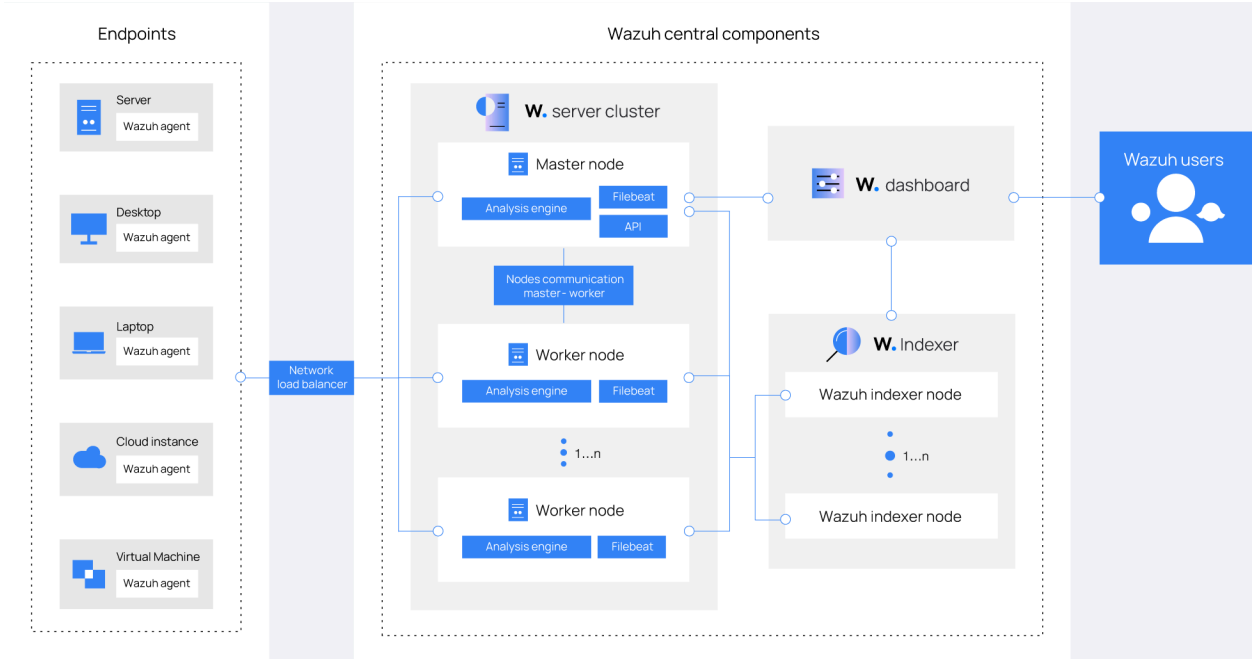
There are always new and evolving threats that target our environments. It is essential to detect these threats before they cause actual harm to people and livelihoods.

In this blog, we will cover how to build a simple SIEM environment to simulate attacks and give us an understanding of how vital detection is in identifying threats and creating defences against them. Links to all the software used, and relevant documentation will be in the references section at the end of the blog.

*If you get stuck at one point or another, please refer to the documentation. You will find solutions to your issues there.

Setting Up the Environment

We will need the host machine (your computer), a hypervisor, a manager server, and an endpoint to build the environment. I have attached an image showing the endpoint and manager server to better visualize the environment.



Source: https://documentation.wazuh.com/current/getting-started/architecture.html

The first thing we need to do is pick a hypervisor on which to build our environment. VirtualBox will be our hypervisor of choice, allowing us to set up the virtual machines.

We will use Wazuh as our manager server as it is open-source and well-supported. In this instance, I recommend using the OVA version to simplify your installation process. The OVA version is a standalone Linux virtual machine with Wazuh already installed.

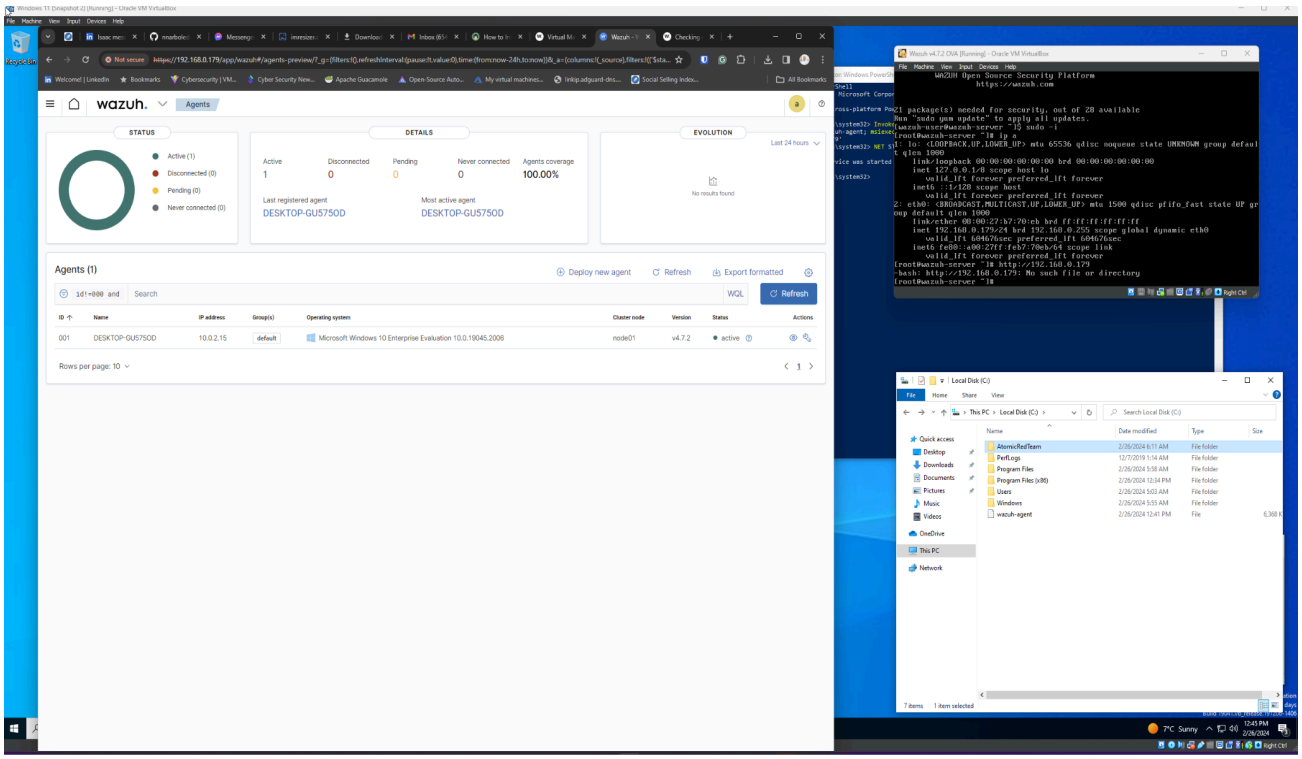
Windows will be used as the operating system for the endpoint machine. This machine is where we will set up our agent and simulate the attacks.

The final step in setting up the environment is setting up an agent on the endpoint so you can access the Wazuh dashboard on a browser on your host machine. Once the installation is complete, you can check the dashboard by entering a browser and inputting your server manager's IP address.

Attack Simulation Using Invoke-Atomic

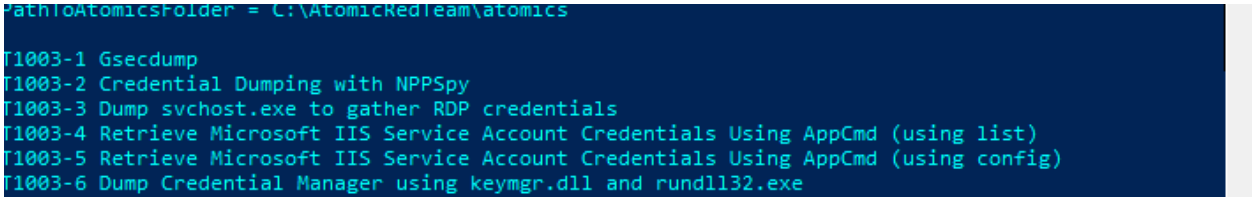
Invoke-Atomic is a repository of attack simulations based on the MITRE ATT&CK framework. Cybersecurity professionals need to understand the relevant threats to their environment. Frameworks are great tools for threat research, and simulations allow us to make tweaks and create new detections.

We will install both the execution framework and the atomics folder to access the attack simulations locally. At this point, it would be beneficial to check that we have everything we need to start running the simulations. Please see the image below to check if you have all the components before moving forward.

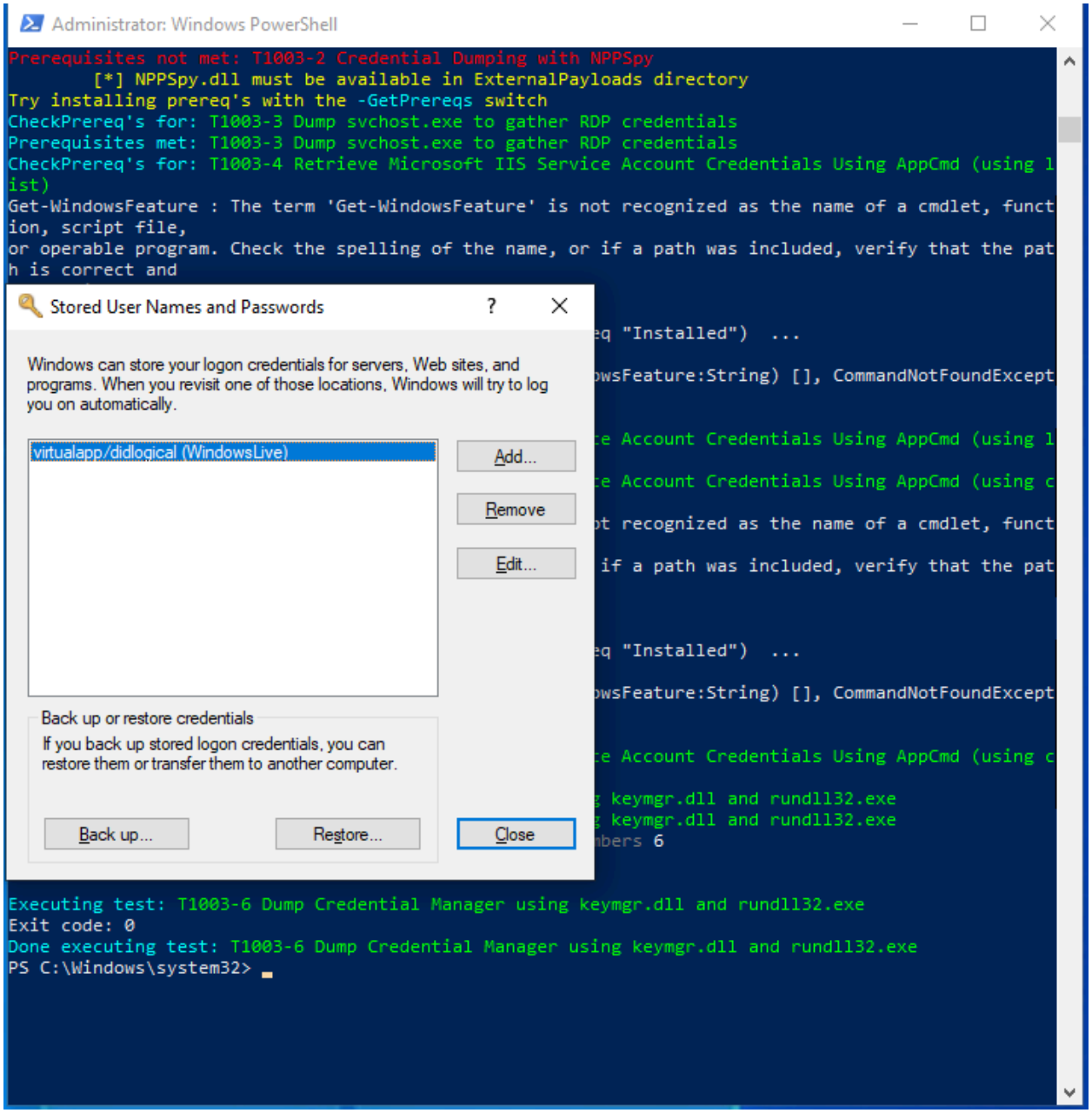


A simulation can be run through PowerShell. Instructions are in the Execution section of the Invoke-Atomic GitHub repository.

In this specific example, I used the attack reference T1003 - 6 as shown below which is a credential dumping attack utilizing kmgr.dll and rund1132.exe.



Upon starting the simulation, the following application (Stored User Names and Passwords) is triggered.



The Wazuh dashboard also registered activity from the attack, stating changes in the registry values and key integrity. The rules 750 and 594 were recorded for further analysis. They can be found on the Security Event tab in the Wazuh dashboard.

›	Feb 27, 2024 @ 15:45:56.694	Registry Key Integrity Checksum Changed	5	594
›	Feb 27, 2024 @ 15:45:56.694	Registry Value Integrity Checksum Changed	5	750
›	Feb 27, 2024 @ 15:45:56.294	Registry Value Integrity Checksum Changed	5	750
›	Feb 27, 2024 @ 15:45:56.232	Registry Key Integrity Checksum Changed	5	594
›	Feb 27, 2024 @ 15:45:56.230	Registry Value Integrity Checksum Changed	5	750
›	Feb 27, 2024 @ 15:45:56.229	Registry Key Integrity Checksum Changed	5	594
›	Feb 27, 2024 @ 15:45:55.115	Windows logon success.	3	60106
›	Feb 27, 2024 @ 15:45:54.021	Registry Value Integrity Checksum Changed	5	750
›	Feb 27, 2024 @ 15:45:53.999	Registry Key Integrity Checksum Changed	5	594
›	Feb 27, 2024 @ 15:45:53.974	Registry Key Integrity Checksum Changed	5	594
›	Feb 27, 2024 @ 15:45:53.946	Registry Key Integrity Checksum Changed	5	594
›	Feb 27, 2024 @ 15:45:53.562	Registry Value Integrity Checksum Changed	5	750
›	Feb 27, 2024 @ 15:45:53.531	Registry Key Integrity Checksum Changed	5	594

T10036

```
<rule id="594" level="5">
<category>ossec</category>
<decoded_as>syscheck_registry_key_modified</decoded_as>
<group>syscheck,syscheck_entry_modified,syscheck_registry,pci_dss_11.5,gpg13_4.13,gdpr_II_5.1.f,hipaa_164.312.c.1,hipaa_164.312.c.2,nist_800_53_SI.7,tsc_PI1.4,tsc_PI1.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
<description>Registry Key Integrity Checksum Changed</description>
<mitre>
<id>T1565.001</id>
<id>T1112</id>
</mitre>
</rule>
```

```
<rule id="750" level="5">
<category>ossec</category>
<decoded_as>syscheck_registry_value_modified</decoded_as>
<group>syscheck,syscheck_entry_modified,syscheck_registry,pci_dss_11.5,gpg13_4.13,gdpr_II_5.1.f,hipaa_164.312.c.1,hipaa_164.312.c.2,nist_800_53_SI.7,tsc_PI1.4,tsc_PI1.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
<description>Registry Value Integrity Checksum Changed</description>
<mitre>
<id>T1565.001</id>
<id>T1112</id>
</mitre>
</rule>
```

It is important to note that not all attack simulations will yield an alert. This is not necessarily a bad thing since it identifies a gap that can be filled in the detection system.

Summary

Building our environment, executing attack simulations, and seeing if any alerts appear on the dashboard can help us begin identifying gaps in our detections and tuning our SIEM to lower the noise and bring the relevant alerts to a higher level in the system. This is where your detection engineering adventure begins.

As a final note, I want to say that the field of cybersecurity is vast, and many disciplines are involved. Don't be discouraged if you are new to the industry and genuinely passionate about defending people from ever-increasing technological threats. We're on this journey together, and I am rooting for you.

Resources

1. https://www.virtualbox.org/
2. https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html
3. https://www.microsoft.com/en-ca/software-download/windows11
4. https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html
5. https://github.com/redcanaryco/invoke-atomicredteam/wiki
6. https://github.com/redcanaryco/invoke-atomicredteam/wiki/Execute-Atomic-Tests-(Local)