Overview:
This project shows a process of setting up a SIEM environment inside VirtualBox using open-source software called Wazuh and an attack simulation platform called Invoke-Atomic, which categorizes attacks via the MITRE ATT&CK framework.

Purpose:
This lab aims to set up an environment to further study different attacks under the MITRE ATT&CK framework and which types of detections are set off by the simulations.

INSTRUCTIONS

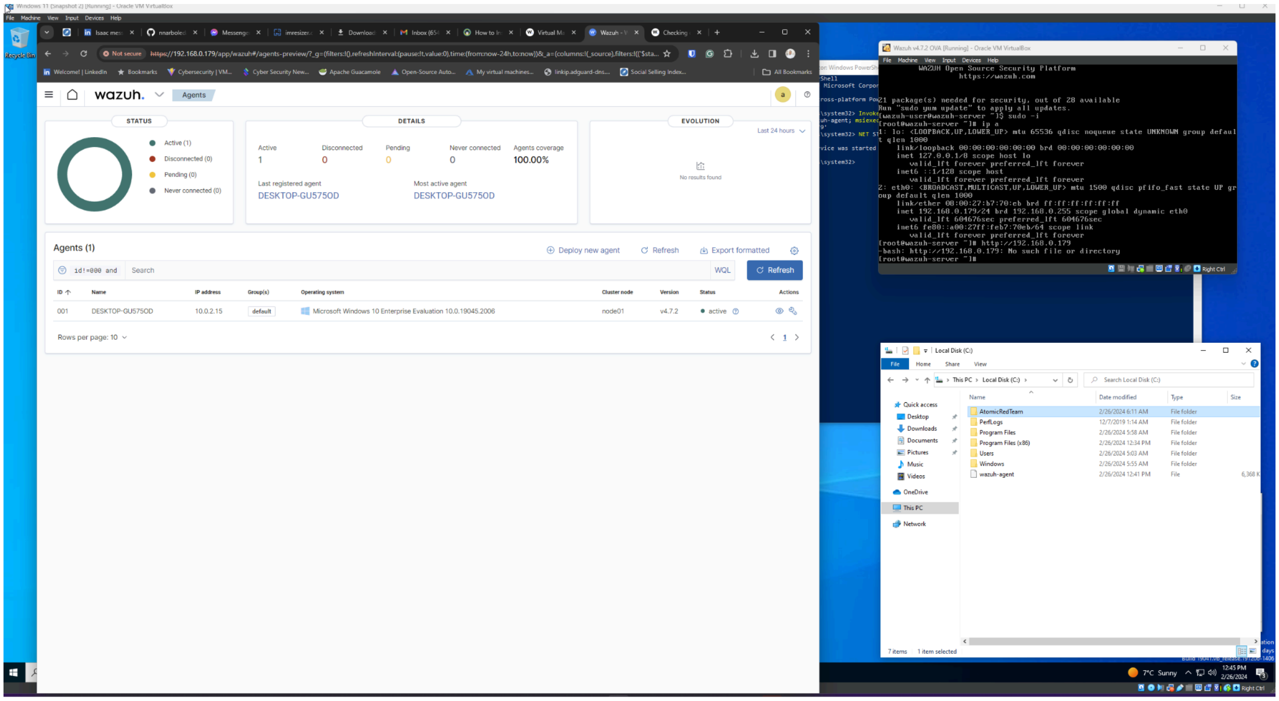
Setting up the SIEM environment:

1) Wazuh was downloaded from their website and set up in VirtualBox, which will serve as the manager server. The version used for this project is the OVA version found at Virtual Machine (OVA) -Installation.
    a) Once Wazuh is installed and running, type the IP address in your host computer's browser and see if it will show the dashboard.
2) A Windows iso was installed in a separate virtual machine, which will be the simulation/victim computer. The Windows iso can be downloaded at Download Windows 11.
3) Once up and running, the Windows virtual machine will be set up as the agent. The instructions can be found at Wazuh agent - Installation guide.
    a) You must run the agent by installing the installer and running the appropriate command in PowerShell.
    b) Note that you must ensure that the IP addresses of the manager server and the agent are different, or the agent will not appear on the Wazuh dashboard.
4) At this point, to check if the environment has been set up correctly, look at the Wazuh dashboard, and it should show 1 agent running.

Setting up Invoke-Atomic:

1) The Invoke-Atomic execution framework and the Atomics folder must be installed on the agent machine.
    a) The installation instructions can be found at Installing Invoke AtomicRedTeam.
    b) If you would prefer a video guide, it can be found at Video Guide.

Before moving forward, ensure all elements are set up as shown in the picture below. (resize page for better viewing)



Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last registered agent DESKTOP-GU575OD

Most active agent DESKTOP-GU575OD

Agents (1)

id!=000 and

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	DESKTOP-GU575OD	10.0.2.15	default	Microsoft Windows 10 Enterprise Evaluation 10.0.19045.2006	node01	v4.7.2	active	

```
         WAZUH Open Source Security Platform
                  https://wazuh.com


21 package(s) needed for security, out of 28 available
Run "sudo yum update" to apply all updates.
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:b7:70:eb brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.179/24 brd 192.168.0.255 scope global dynamic eth0
       valid_lft 604676sec preferred_lft 604676sec
    inet6 fe80::a00:27ff:feb7:70eb/64 scope link
       valid_lft forever preferred_lft forever
[root@wazuh-server ~]# http://192.168.0.179
-bash: http://192.168.0.179: No such file or directory
[root@wazuh-server ~]#
```

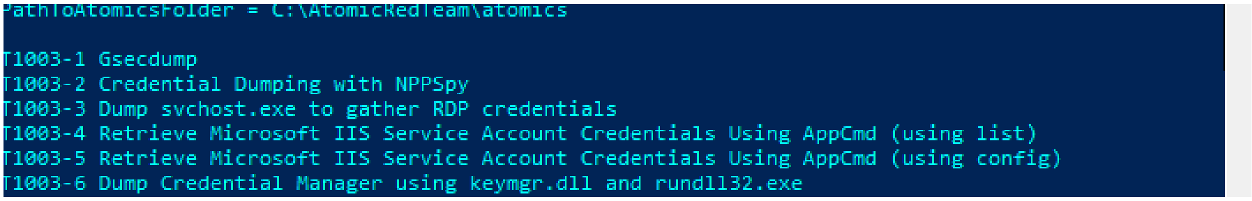
Name	Date modified	Type	Size
AtomicRedTeam	2/26/2024 6:11 AM	File folder	
PerfLogs	12/7/2019 1:14 AM	File folder	
Program Files	2/26/2024 5:58 AM	File folder	
Program Files (x86)	2/26/2024 12:34 PM	File folder	
Users	2/26/2024 5:03 AM	File folder	
Windows	2/26/2024 5:55 AM	File folder	
wazuh-agent	2/26/2024 12:41 PM	File	6,368 K

Running a Simulation:

1) The simulation can be run through Powershell. Instructions can be found at Execution.

SIMULATION

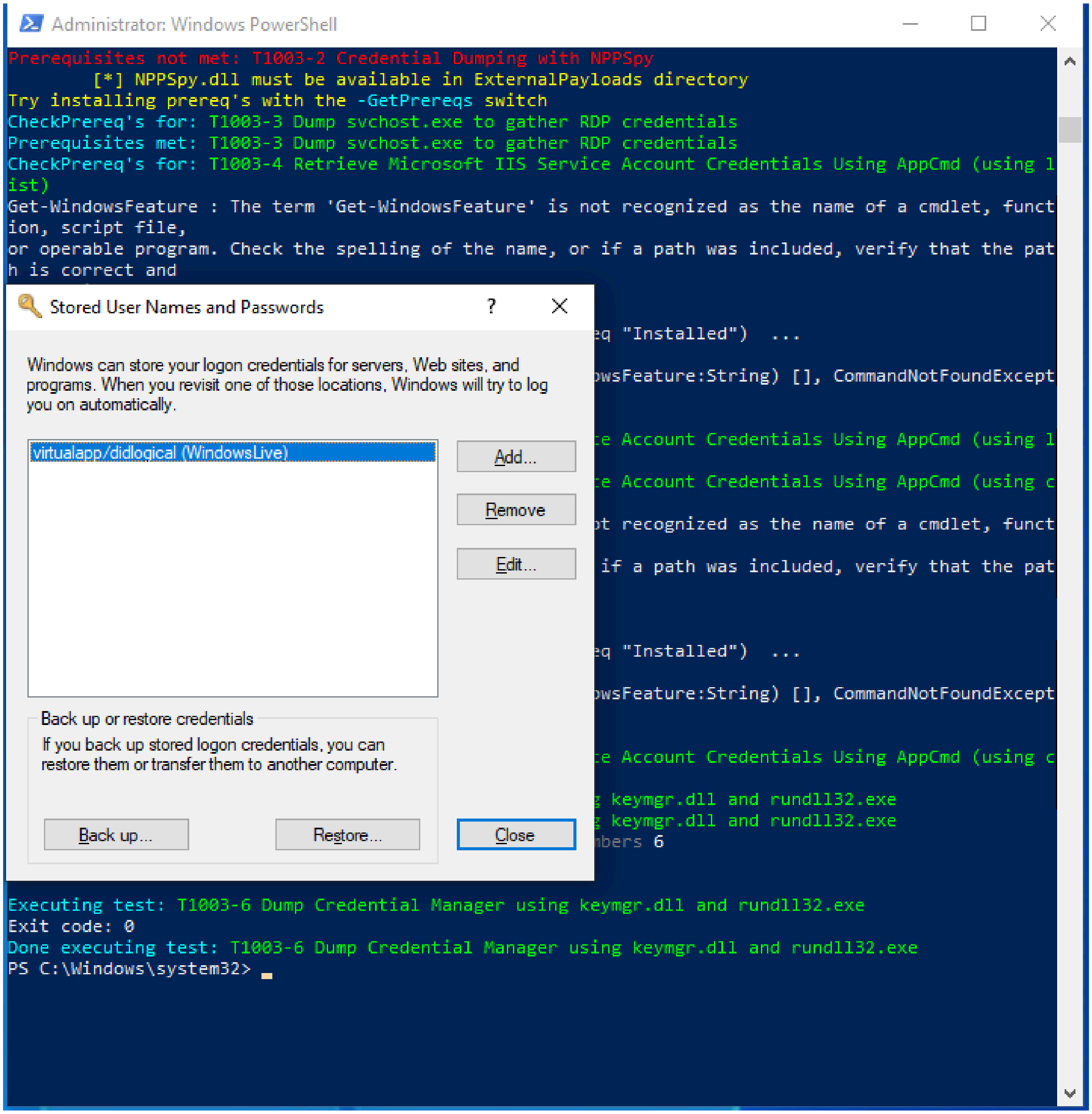
This specific lab used the attack reference T1003 - 6



```
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003-1 Gsecdump
T1003-2 Credential Dumping with NPPSpy
T1003-3 Dump svchost.exe to gather RDP credentials
T1003-4 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using list)
T1003-5 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using config)
T1003-6 Dump Credential Manager using keymgr.dll and rundll32.exe
```

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



```
Prerequisites not met: T1003-2 Credential Dumping with NPPSpy
        [*] NPPSpy.dll must be available in ExternalPayloads directory
Try installing prereq's with the -GetPrereqs switch
CheckPrereq's for: T1003-3 Dump svchost.exe to gather RDP credentials
Prerequisites met: T1003-3 Dump svchost.exe to gather RDP credentials
CheckPrereq's for: T1003-4 Retrieve Microsoft IIS Service Account Credentials Using AppCmd (using l
ist)
Get-WindowsFeature : The term 'Get-WindowsFeature' is not recognized as the name of a cmdlet, funct
ion, script file,
or operable program. Check the spelling of the name, or if a path was included, verify that the pat
h is correct and

                                                         eq "Installed")  ...

                                                        owsFeature:String) [], CommandNotFoundExcept

                                                         e Account Credentials Using AppCmd (using l

                                                         e Account Credentials Using AppCmd (using c

                                                         ot recognized as the name of a cmdlet, funct

                                                          if a path was included, verify that the pat


                                                         eq "Installed")  ...

                                                        owsFeature:String) [], CommandNotFoundExcept

                                                         e Account Credentials Using AppCmd (using c

                                                        g keymgr.dll and rundll32.exe
                                                        g keymgr.dll and rundll32.exe
                                                        mbers 6

Executing test: T1003-6 Dump Credential Manager using keymgr.dll and rundll32.exe
Exit code: 0
Done executing test: T1003-6 Dump Credential Manager using keymgr.dll and rundll32.exe
PS C:\Windows\system32> _
```

Stored User Names and Passwords

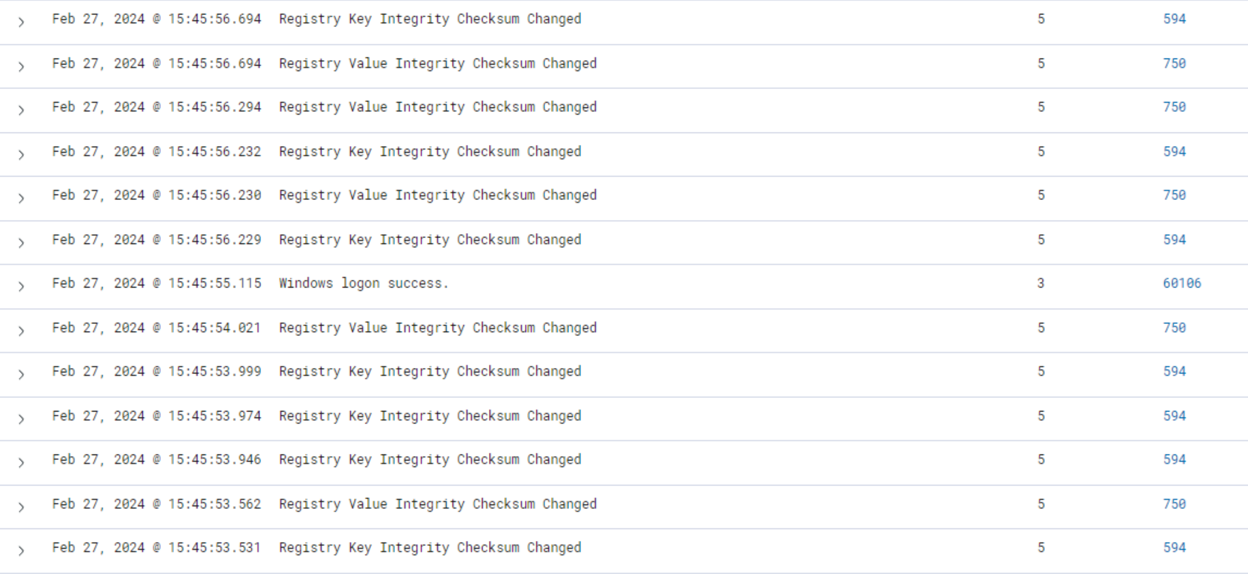
Windows can store your logon credentials for servers, Web sites, and programs. When you revisit one of those locations, Windows will try to log you on automatically.

virtualapp/didlogical (WindowsLive)

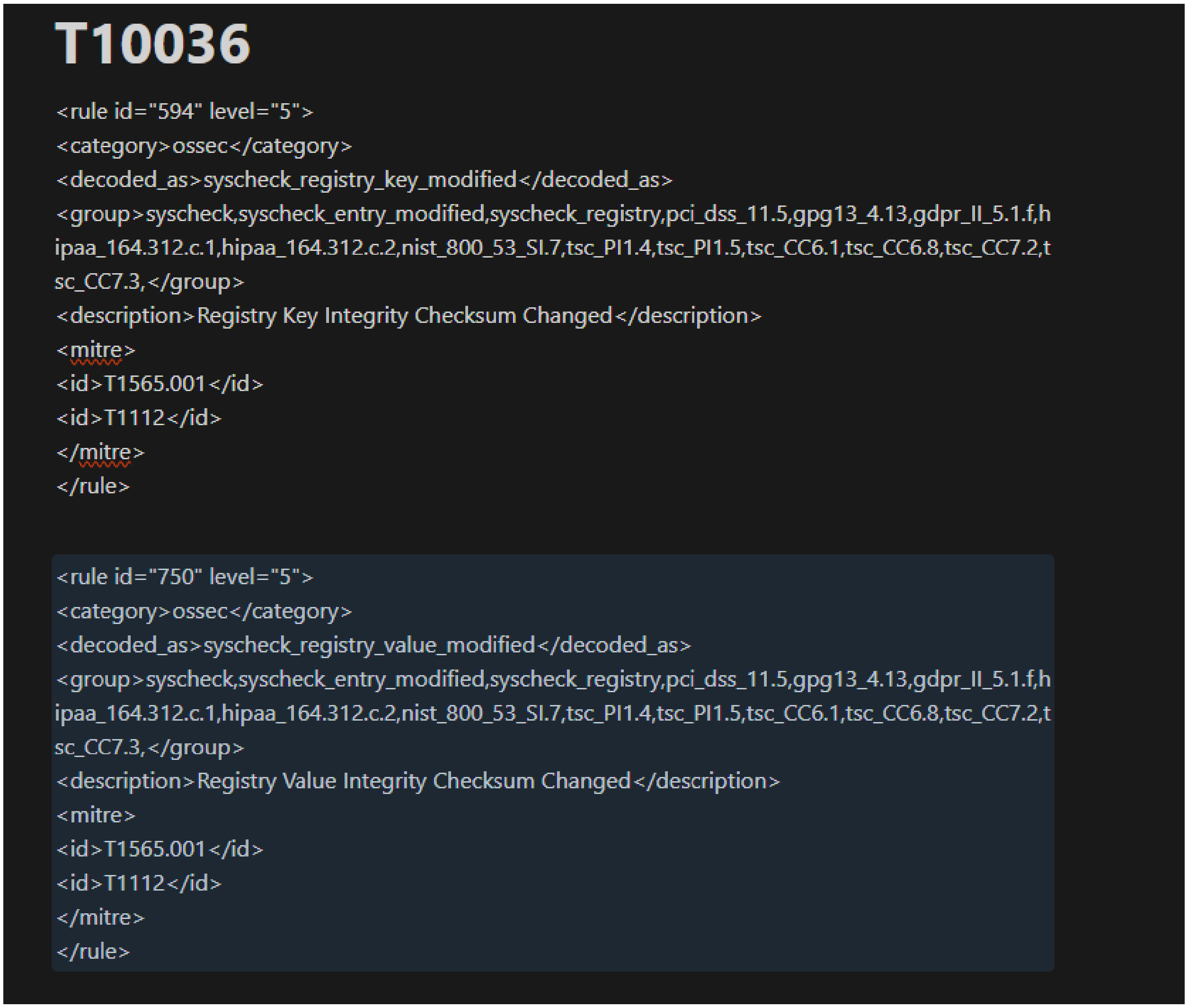
Back up or restore credentials

If you back up stored logon credentials, you can restore them or transfer them to another computer.

The Wazuh dashboard also registered activity from the attack, stating changes in the registry values and key integrity. The rules 750 and 694 were recorded for further analysis.



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>
```