

Configuration Manual

**Research Focused on Threat Detection Rule Development utilizing the
Splunk Attack Range to fortify Cybersecurity Analysis.**

MSc Research Project - Cybersecurity

Rajuaravind Sankar
Student ID: X22250042

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Rajuaravind Sankar
Student ID: X22250042
Programme: M.Sc. in Cybersecurity **Year:** 2023-24
Module: M.Sc. Research Project
Supervisor: Mark Monaghan
Submission Due Date: 12 August 2024
Project Title: Research Focused on Threat Detection Rule Development utilizing the Splunk Attack Range to fortify Cybersecurity analysis
Word Count: 1553 **Page Count:** 13

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rajuaravind Sankar
.....

Date: 9 August 2024
.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Rajuaravind Sankar
Student ID: X22250042

1 Introduction

The purpose of this configuration manual is to detail the steps taken to achieve the research objectives. The process involves several phases, including implementing the Splunk Attack Range tool to set up the simulation environment, simulating attack data within that environment, developing and deploying a threat detection rule, and evaluating the effectiveness of the deployed rule. By successfully completing these phases, all the primary objectives of my thesis research have been met.

2 Technologies and Resources Utilized

This section outlines the technologies and resources used in the implementation to achieve my thesis research objectives. The following list provides the information on the resources and technologies used in the research.

- Amazon Web Services
EC2, Elastic IP, VPC, IAM role
- Docker
- Python Programming Language
- Terraform
- Ansible
- Splunk Enterprise
- Splunk Machine learning toolkit App (MLTK)
- Splunk Security Essentials
- MITRE ATT&CK Framework
- Atomic Red Attack Simulation Engine
- Purple Sharp Attack Simulation Engine

3 Implementation Setup

To initiate the research implementation, an EC2 instance was launched, followed by the installation of the necessary Docker software. The Docker service was then configured to start automatically on boot.

```
[root@ip-172-31-91-235 ec2-user]# sudo systemctl status docker.service
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: disabled)
   Active: active (running) since Sat 2024-07-20 13:00:03 UTC; 6min ago
   TriggeredBy: ● docker.socket
   Docs: https://docs.docker.com
   Process: 26734 ExecStartPre=/bin/mkdir -p /run/docker (code=exited, status=0/SUCCESS)
   Process: 26735 ExecStartPre=/usr/libexec/docker/docker-setup-runtimes.sh (code=exited, status=0/SUCCESS)
   Main PID: 26736 (dockerd)
     Tasks: 11
    Memory: 357.2M
       CPU: 1min 29.938s
    CGroup: /system.slice/docker.service
           └─26736 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock --default-ulimit nofile=32768:65536

Jul 20 13:00:02 ip-172-31-91-235.ec2.internal systemd[1]: Starting docker.service - Docker Application Container Engine...
Jul 20 13:00:02 ip-172-31-91-235.ec2.internal dockerd[26736]: time="2024-07-20T13:00:02.505214434Z" level=info msg="Starting up"
Jul 20 13:00:02 ip-172-31-91-235.ec2.internal dockerd[26736]: time="2024-07-20T13:00:02.573418061Z" level=info msg="Loading containers: >
Jul 20 13:00:03 ip-172-31-91-235.ec2.internal dockerd[26736]: time="2024-07-20T13:00:03.208518575Z" level=info msg="Loading containers: >
Jul 20 13:00:03 ip-172-31-91-235.ec2.internal dockerd[26736]: time="2024-07-20T13:00:03.236828059Z" level=info msg="Docker daemon" commi
Jul 20 13:00:03 ip-172-31-91-235.ec2.internal dockerd[26736]: time="2024-07-20T13:00:03.237221974Z" level=info msg="Daemon has completed
Jul 20 13:00:03 ip-172-31-91-235.ec2.internal dockerd[26736]: time="2024-07-20T13:00:03.278128255Z" level=info msg="API listen on /run/dp
Jul 20 13:00:03 ip-172-31-91-235.ec2.internal systemd[1]: Started docker.service - Docker Application Container Engine.
lines 1-22/22 (END)
```

After installing Docker, the Splunk Attack Range Docker image was pulled from Docker Hub using the docker pull command: **docker pull splunk/splunk_range**.

```
[root@ip-172-31-91-235 ec2-user]# docker pull splunk/attack_range
Using default tag: latest
latest: Pulling from splunk/attack_range
bccd10f490ab: Pull complete
094616ab35df: Pull complete
bf5ee18331ab: Pull complete
e513cf278df1: Pull complete
2624215f7886: Pull complete
6c29fa507d71: Pull complete
514570632aea: Pull complete
21f33074e595: Pull complete
4f4fb700ef54: Pull complete
1dff5f0556a9: Pull complete
b5b79f652414: Pull complete
71c25169c304: Pull complete
857b8b8cd451: Pull complete
b0f226bb9882: Pull complete
f8e089e3beca: Pull complete
bd8b9615e31f: Pull complete
651c4f15f465: Pull complete
Digest: sha256:81b9810530518084d732040006628969c6900abddc8da9300eaed90cd0b88273
Status: Downloaded newer image for splunk/attack_range:latest
docker.io/splunk/attack_range:latest
[root@ip-172-31-91-235 ec2-user]#
[root@ip-172-31-91-235 ec2-user]#
```

After pulling the Splunk Attack Range Docker image from Docker Hub, the image was executed as a container to initiate the implementation phase using the command: **'docker run -it splunk/attack_range'**

```
[root@ip-172-31-91-235 ec2-user]#
[root@ip-172-31-91-235 ec2-user]# docker run -it splunk/attack_range
Spawning shell within /root/.cache/pypoetry/virtualenvs/attack-range-536x2-W_-py3.10
root@26b67f032cc9:/attack_range# . /root/.cache/pypoetry/virtualenvs/attack-range-536x2-W_-py3.10/bin/activate
(attack-range-py3.10) root@26b67f032cc9:/attack_range#
(attack-range-py3.10) root@26b67f032cc9:/attack_range#
(attack-range-py3.10) root@26b67f032cc9:/attack_range#
(attack-range-py3.10) root@26b67f032cc9:/attack_range#
```

My AWS account was configured with a dedicated Access Key and Secret ID for the Splunk Attack Range tool, enabling it to automate the creation of the simulation environment on the AWS platform. To follow best practices, a separate IAM role was created, and the newly generated IAM Access Key and Secret ID were used for configuration, as using the root account credentials is not recommended.


```

Apply complete! Resources: 16 added, 0 changed, 0 destroyed.
2024-08-05 15:21:03,674 - INFO - attack_range - attack_range has been built using terraform successfully
2024-08-05 15:21:03,674 - INFO - attack_range - [action] > show

Status Virtual Machines

Name                Status    IP Address    Instance ID
-----
ar-win-root-68570-ar-0    running  52.4.217.125  i-0dceedf357e9b788a
ar-linux-root-68570-ar-0  running  44.215.95.32  i-01f9429f93df352e1
ar-splunk-root-68570-ar   running  52.71.170.186 i-0cfbab996db9feb69


Access Windows via:
RDP > rdp://52.4.217.125:3389
      username: Administrator
      password: LpVHvd15f0ZQ3QYKAi0

Access Linux via:
SSH > ssh -i/attack_range/root-68570.key ubuntu@44.215.95.32
      username: ubuntu
      password: LpVHvd15f0ZQ3QYKAi0

Access Guacamole via:
Web > http://52.71.170.186:8080/guacamole
      username: Admin
      password: LpVHvd15f0ZQ3QYKAi0

Access Splunk via:
Web > http://52.71.170.186:8000
SSH > ssh -i/attack_range/root-68570.key ubuntu@52.71.170.186
      username: admin
      password: LpVHvd15f0ZQ3QYKAi0

```

```
root@089e6726ecf:/attack_range#  
python attack_range.py simulate --ART -t T1003.001 -t ar-win-root-68578-ar-0  
  
By: Splunk Threat Research Team [STRT] - research@splunk.com
```

2024-08-05 17:07:54,511 ~ INFO ~ attack_range ~ [action] > simulate

```
PLAY [all]
```

```
TASK [Gathering Facts]
```

ok: [52.4.217.125]

```
TASK [atomic_red_team : include_tasks]
```

skipping: [52.4.217.125] => (item=T1003.001)

```
TASK [atomic_red_team : include_tasks]
```

included: /attack_range/modules/ansible/roles/atomic_red_team/tasks/run_art_test_windows.yml for 52.4.217.125 => (item=T1003.001)

```
TASK [atomic_red_team : set_fact]
```

ok: [52.4.217.125]

```
TASK [atomic_red_team : debug]
```

ok: [52.4.217.125] => { "technique": "T1003.001"

}

```
TASK [atomic_red_team : Get requirements for Atomic Red Team Technique]
```

changed: [52.4.217.125]

```
TASK [atomic_red_team : Run specified Atomic Red Team Technique]
```

changed: [52.4.217.125]

```
TASK [atomic_red_team : debug]
```

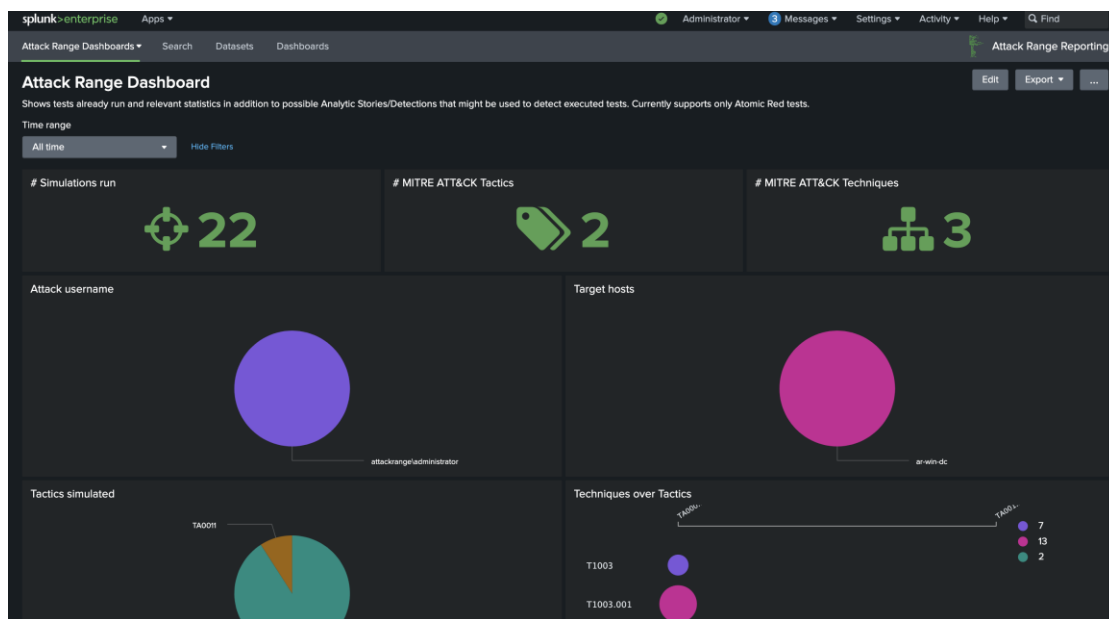
ok: [52.4.217.125] => { "output_ert.stdout_lines": [
 "PathToAtomicsFolder = C:\\AtomicRedTeam\\atomics",

After the simulation environment is set up, an OS Credential Dumping attack targeting LSASS memory is simulated on the Windows instance within the environment. The Atomic Red Team simulation engine is used to carry out this attack simulation on the Windows server. The attack is executed using the following command:

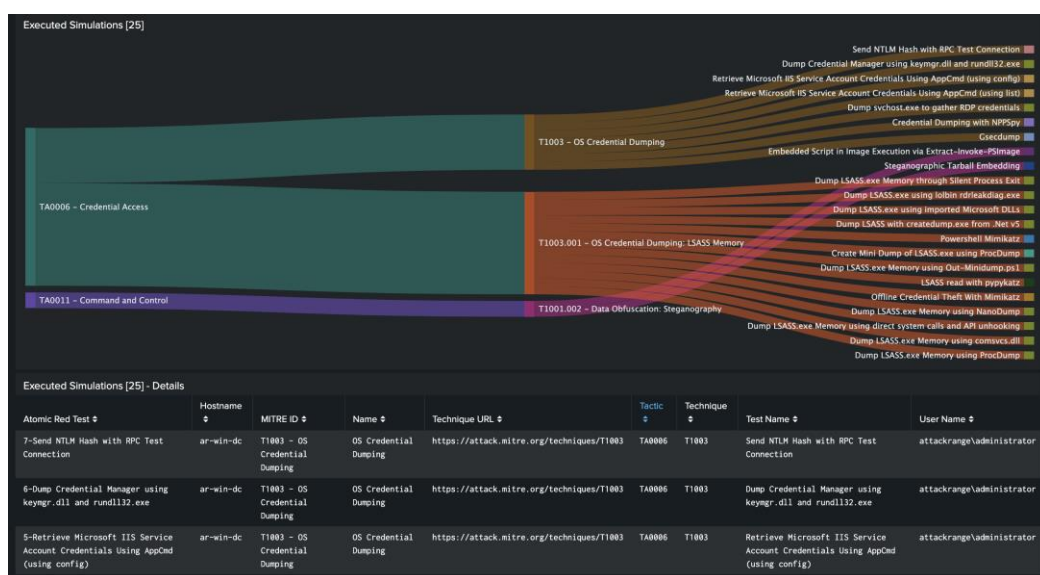
python attack_range.py simulate -e ART -te T1003.001 -t ar-win-root-68570-er-0

In this command:

- **-e** specifies the simulation engine (ART for Atomic Red Team).
- **-te** specifies the attack technique ID (T1003.001 for OS Credential Dumping – LSASS Memory).
- **-t** specifies the instance name where the attack is to be simulated (in this case, ar-win-root-68570-er-0).



The Splunk Attack Range offers a range of Splunk applications within a simulated environment for analyzing attack data. This setup enables users to develop and refine effective threat detection rules



After simulating an attack in the Windows instance within the simulation environment, the Windows machine event logs are analysed to develop threat detection rules. These logs are forwarded from the Windows instance to the Splunk server via the Splunk Universal Forwarder, which was configured as part of the automation process.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk-enterprise' and 'Apps'. Below it, a 'New Search' bar contains the query 'index=win'. The search results show 449,094 events matched. A timeline view is displayed, showing a single event at 16:23:32.000 on 05/08/2024. The event details are shown in a table below the timeline.

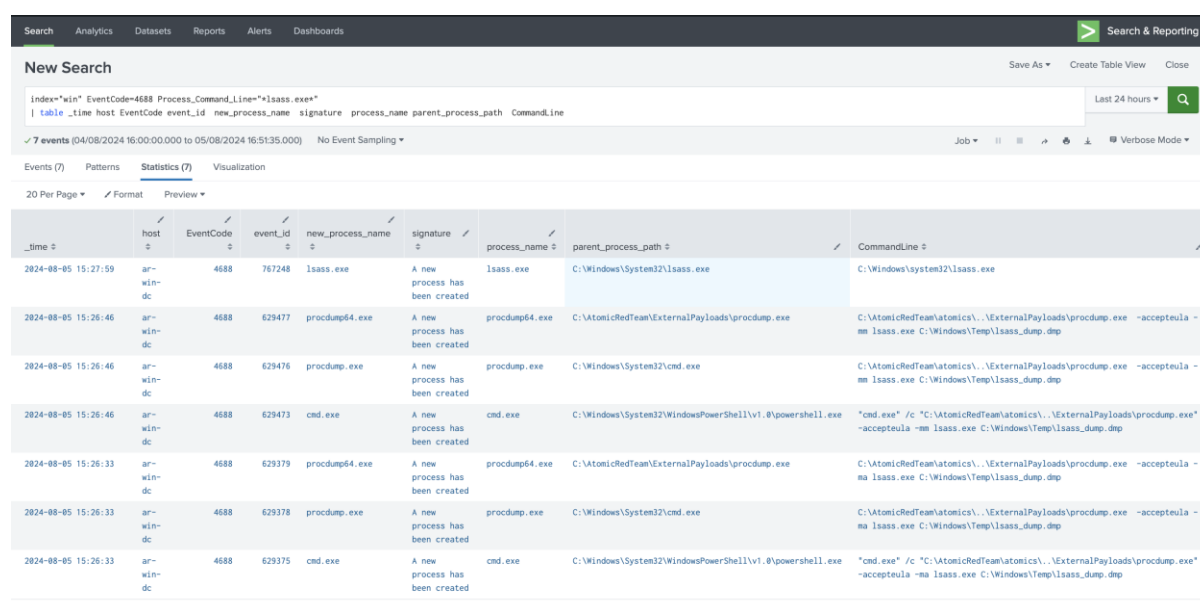
Time	Event
05/08/2024 16:23:32.000	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5778385F-C22A-43E8-BF4C-06F5698FFB09}" /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>9</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2024-08-08T16:23:32.25988400Z" /><EventRecordID>6818</EventRecordID><Correlation><Execution ProcessID="2668" ThreadID="2288" /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>ar-win-dc.attackrange.local</Computer><Security UserID="S-1-5-18" /></System><EventData><Data Name="RuleName"></Data><Data Name="UtcTime">2024-08-08 16:23:32.259</Data><Data Name="ProcessGuid">{13FA861A-F88B-66B0-AA00-000000009703}</Data><Data Name="ProcessID">2868</Data><Data Name="Image">C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name="FileVersion">9.8.2</Data><Data Name="Description">Registry monitor</Data><Data Name="Product">splunk Application</Data><Data Name="Company">Splunk Inc.</Data><Data Name="OriginalFileName">splunk-regmon.exe</Data><Data Name="CommandLine">C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name="CurrentDirectory">C:\Windows\System32</Data><Data Name="User">NT AUTHORITY\SYSTEM</Data><Data Name="LogonGuid">{13FA861A-F88B-66B0-E783-000000000000}</Data><Data Name="LogonID">0x3e7</Data><Data Name="TerminalSessionID">0</Data><Data Name="IntegrityLevel">System</Data><Data Name="Hashes">MD5=B6A4D27EE93FB7EE14DED01CBE8DA71_SHA256=C40DF32D3564EA53CEE7828B5F55A0C8E9AC308AE49051B041829AA96CA544_IMPHASH=9374AAB4494C2195A38F44F0036C8858</Data><Data Name="ParentProcessGuid">{13FA861A-F89B-66B0-2A00-000000009703}</Data><Data Name="ParentProcessID">2636</Data><Data Name="ParentImage">C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name="ParentCommandLine">C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe service</Data><Data Name="ParentUser">NT AUTHORITY\SYSTEM</Data></EventData></Event>

The presence of various useful Splunk apps on the Splunk server streamlines and enhances the process of developing threat detection rules. Among these, the Splunk Security Essentials app is particularly instrumental in formulating detection rules for OS credential dumping attacks.

The screenshot shows the Splunk Security Essentials interface. At the top, there's a navigation bar with 'splunk-enterprise' and 'Apps'. Below it, a 'Security Content' section is displayed. The search bar contains the query 'dumping'. The results are filtered by 'Security Use Case' (All), 'Category' (All), and 'Data Sources' (All). The 'Featured' section shows several security use cases, each with a description and a 'Searches Included' section.

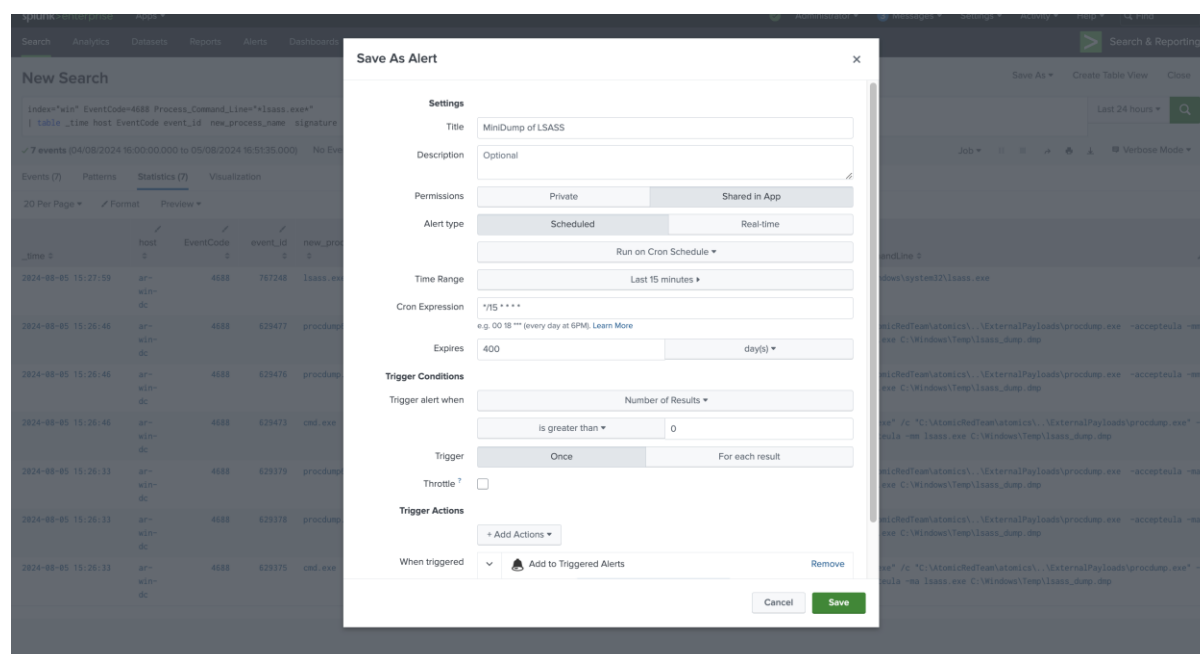
Security Use Case	Category	Data Sources	Featured
Access LSASS Memory For Dump Creation	All	All	All
Create Remote Thread Into LSASS	All	All	All
Creation Of Shadow Copy With Wmic And Powershell	All	All	All
Detect Credential Dumping Through LSASS Access	All	All	All
Detect Mimikatz Using Loaded Images	All	All	All
Unsigned Image Loaded By LSASS	All	All	All

Through effective analysis of Windows event logs and understanding the correlation between event codes and process IDs, events with event code 4688—associated with the LSASS memory process in OS credential dumping attacks—are identified and filtered. This analysis facilitates the development of a robust and efficient threat detection rule.



_time	host	EventCode	event_id	new_process_name	signature	process_name	parent_process_path	CommandLine
2024-08-05 15:27:59	ar-win-dc	4688	767248	lsass.exe	A new process has been created	lsass.exe	C:\Windows\System32\lsass.exe	C:\Windows\system32\lsass.exe
2024-08-05 15:26:46	ar-win-dc	4688	629477	procdump64.exe	A new process has been created	procdump64.exe	C:\AtomicRedTeam\ExternalPayloads\procdump.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -acceptteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:46	ar-win-dc	4688	629476	procdump.exe	A new process has been created	procdump.exe	C:\Windows\System32\cmd.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -acceptteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:46	ar-win-dc	4688	629473	cmd.exe	A new process has been created	cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"cmd.exe" /c "C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe" -acceptteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:33	ar-win-dc	4688	629379	procdump64.exe	A new process has been created	procdump64.exe	C:\AtomicRedTeam\ExternalPayloads\procdump.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -acceptteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:33	ar-win-dc	4688	629378	procdump.exe	A new process has been created	procdump.exe	C:\Windows\System32\cmd.exe	C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe -acceptteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp
2024-08-05 15:26:33	ar-win-dc	4688	629375	cmd.exe	A new process has been created	cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"cmd.exe" /c "C:\AtomicRedTeam\atomic\...\ExternalPayloads\procdump.exe" -acceptteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp

The detection rule for OS credential dumping attacks targeting LSASS memory is developed using an SPL query and saved as an alert in Splunk Enterprise. This alert is configured to run every 15 minutes with a time range window of the previous 15 minutes, enhancing the efficiency of threat detection. Additionally, a trigger action notification is set up, so whenever the alert is activated, a notification will appear in the Splunk Enterprise server notification bar.



Search

Analytics

Datasets

Reports

Alerts

Dashboards

New Search

Index="win" EventCode=4688 Process.Command.Line="*lsass.exe"

| table _time host EventCode event_id new_process_name signature

7 events (04/08/2024 16:00:00.000 to 05/08/2024 16:51:35.000)

No Event Sampling

Events (7)

Patterns

Statistics (7)

Visualization

20 Per Page

Format

Preview

_time	host	EventCode	event_id	new_pro
2024-08-05 15:27:59	ar-win-dc	4688	767248	lsass.exe
2024-08-05 15:26:46	ar-win-dc	4688	629477	procdump64.exe
2024-08-05 15:26:46	ar-win-dc	4688	629476	procdump.exe
2024-08-05 15:26:46	ar-win-dc	4688	629473	cmd.exe
2024-08-05 15:26:33	ar-win-dc	4688	629379	procdump64.exe
2024-08-05 15:26:33	ar-win-dc	4688	629378	procdump.exe
2024-08-05 15:26:33	ar-win-dc	4688	629375	cmd.exe

Save As Alert

Settings

Title

MinDump of LSASS

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run on Cron Schedule

Run on Cron Schedule

Time Range

Last 15 minutes

Cron Expression

* * * * *

e.g. 00 18 * * * (every day at 6PM). Learn More

Expires

400

day(s)

Trigger Conditions

Trigger alert when

Number of Results

is greater than

0

Trigger

Once

For each result

Throttle

Trigger Actions

+ Add Actions

When triggered

Add to Triggered Alerts

Remove

Cancel

Save

7

The screenshot below displays the configured threat detection alert for Minidump of LSASS in the Splunk Enterprise server.

<h2>MiniDump of LSASS</h2>	
Enabled: Yes. Disable	Trigger Condition: .. Number of Results is > 0. Edit
App: search	Actions: ▼ 1 Action Edit
Permissions: Shared Globally. Owned by admin. Edit	🔔 Add to Triggered Alerts
Modified: 5 Aug 2024 16:54:45	
Alert Type: Scheduled. Cron Schedule. Edit	

To evaluate and verify the configured OS credential dumping threat detection rule, the same attack is simulated once more on the Windows instance within the simulation environment.

```
+ ... {$exePath = resolve-path \"$env:ProgramFiles\dotnet\shared\Microsoft.N ...",
"   + CategoryInfo          : ObjectNotFound: (C:\Program File...oft.NETCore.App:String) [Resolve-Path], ItemNotFoundE ",
"     xception",
"   + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.ResolvePathCommand",
" },
"The expression after '&' in a pipeline element produced an object that was not valid. It must result in a command ",
"name, a script block, or a CommandInfo object.",
"At line:2 char:3",
"+ & \"$exePath\" -u -f $env:Temp\ldotnet-lsass.dmp (Get-Process lsass).id)",
"+ ~~~~~~",
"   + CategoryInfo          : InvalidOperation: (:String) [], RuntimeException",
"   + FullyQualifiedErrorId : BadExpression",
"Exit code: 0",
"Done executing test: T1003.001-11 Dump LSASS with createdump.exe from .Net v5",
"Executing test: T1003.001-12 Dump LSASS.exe using imported Microsoft DLLs",
"Exit code: 0",
"Done executing test: T1003.001-12 Dump LSASS.exe using imported Microsoft DLLs",
"Executing test: T1003.001-13 Dump LSASS.exe using lolbin rdpleakdiag.exe",
"Directory: C:\\Users\\ADMINI-1\\AppData\\Local\\Temp",
Mode                LastWriteTime         Length Name
----                -
d-----             7/23/2024    6:56 PM                  t1003_001-13-rdrleakdiag
"C:\\Windows\\System32\\rdrleakdiag.exe /p 596 /o C:\\Users\\ADMINI-1\\AppData\\Local\\Temp\\t1003_001-13-rdrleakdiag /fullmemdump /wait 1",
"Minidump file, minidump_596.dmp can be found inside C:\\Users\\ADMINI-1\\AppData\\Local\\Temp\\t1003_001-13-rdrleakdiag directory.",
"Exit code: 0",
"Done executing test: T1003.001-13 Dump LSASS.exe using lolbin rdpleakdiag.exe",
"Executing test: T1003.001-14 Dump LSASS.exe Memory through Silent Process Exit",
"This version of C:\\AtomicRedTeam\\ExternalPayloads\\nanodump.x64.exe is not compatible with the version of Windows you're running. Check your compu
ter's system information and then contact the software publisher.",
"Exit code: 1",
"Done executing test: T1003.001-14 Dump LSASS.exe Memory through Silent Process Exit"
}
}

TASK [atomic_red_team : Cleanup after execution] *****
changed: [100.27.123.96]

PLAY RECAP *****
100.27.123.96      : ok=8    changed=3    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
[attacker@kali ~]$ sudo docker exec -it container1 sh
root@container1:/# cat /dev/random | dd of=/tmp/attack_payload.bin bs=1M count=1
```

The configured threat detection rule was successfully triggered and demonstrated efficient performance in identifying the OS credential dumping LSASS memory attack. Consequently, the primary objective of developing an effective threat detection rule using the Splunk Attack Range tool has been successfully achieved.

splunk enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

MiniDump of LSASS

Enabled: _____ Yes, Disable
 App: _____ search
 Permissions: Shared Globally, Owned by admin, Edit
 Modified: _____ 5 Aug 2024 16:58:16
 Alert Type: _____ Scheduled, Cron Schedule, Edit

Trigger Condition: .. Number of Results is > 0. Edit
 Actions: _____ <1 Action Edit
 Add to Triggered Alerts

Trigger History

20 per page ▾

	TriggerTime ↕	Actions
1	2024-08-05 17:11:02 UTC	View Results

References

1. *Attack Range AWS — Attack Range 3.0.0 documentation.* (n.d.). https://attack-range.readthedocs.io/en/latest/Attack_Range_AWS.html
2. *OS credential Dumping: LSASS Memory, Sub-Technique T1003.001 - Enterprise | MITRE ATT&CK®.* (n.d.). <https://attack.mitre.org/techniques/T1003/001>
3. *OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®.* (n.d.). <https://attack.mitre.org/techniques/T1003/>
4. *Splunk.* (n.d.). *GitHub - splunk/attack_range: A tool that allows you to create vulnerable instrumented local or cloud environments to simulate attacks against and collect the data into Splunk.* GitHub. https://github.com/splunk/attack_range
5. *“docker container commit.”* (2024, February 9). *Docker Documentation.* <https://docs.docker.com/reference/cli/docker/container/commit/>
6. *IAM roles - AWS Identity and Access Management.* (n.d.). https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html