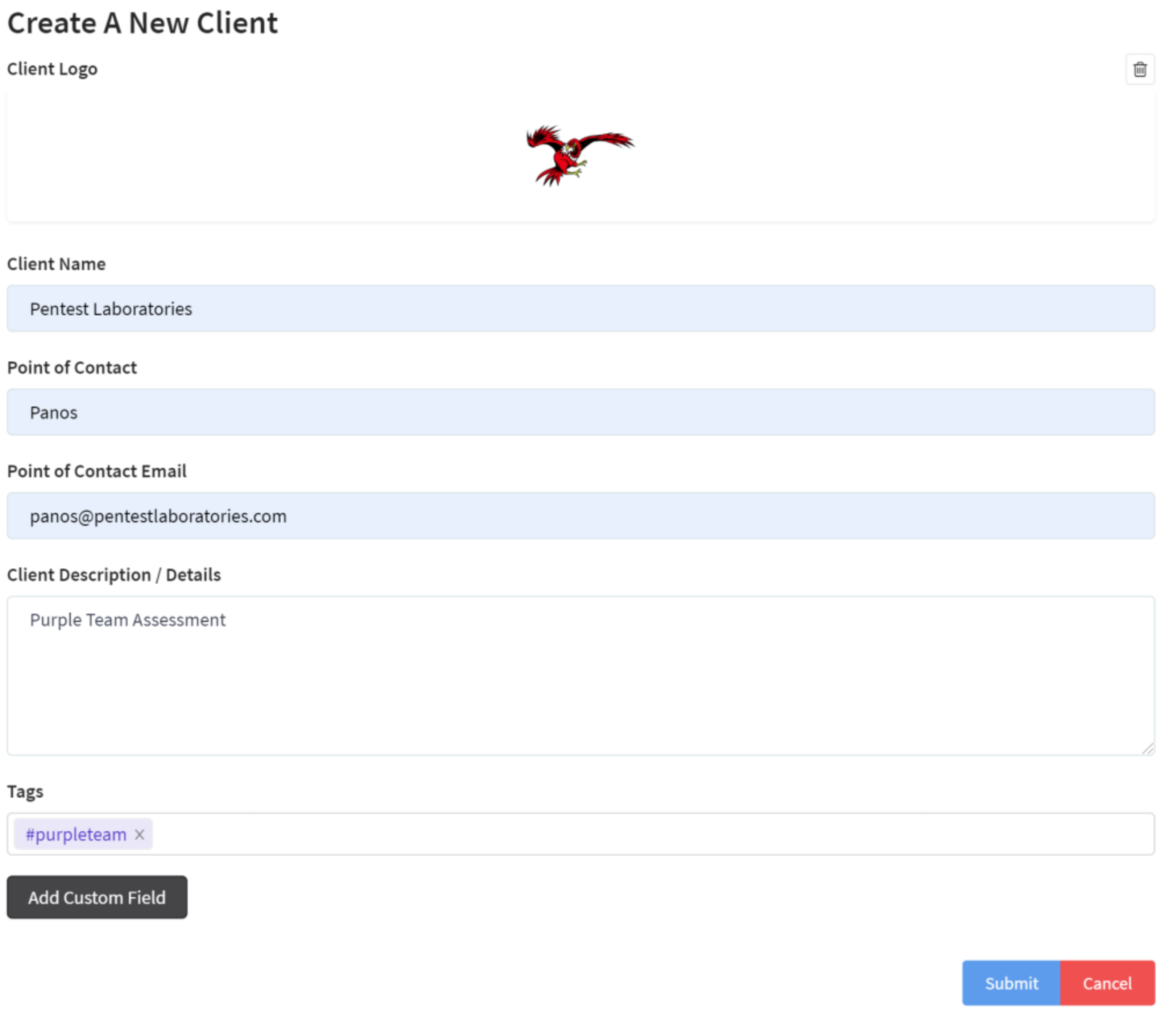
PlexTrac – A Platform for Purple Teaming

March 30, 2021

PlexTrac is a platform which can be used by internal security teams or consultancies to conduct purple team assessments but it can be used also as a pentest reporting tool since it contains a findings database and a unique report template. Pentest Laboratories Ltd have conducted a purple team assessment in order to assess the capabilities of PlexTrac platform.

Prior to the assessment a new client can be created with the associated contact details, client logo and information related to the assessment such as the scope and other details. Pentest Laboratories Ltd details have been used for the purpose of the engagement.



Create A New Client

Client Logo

Client Name: Pentest Laboratories

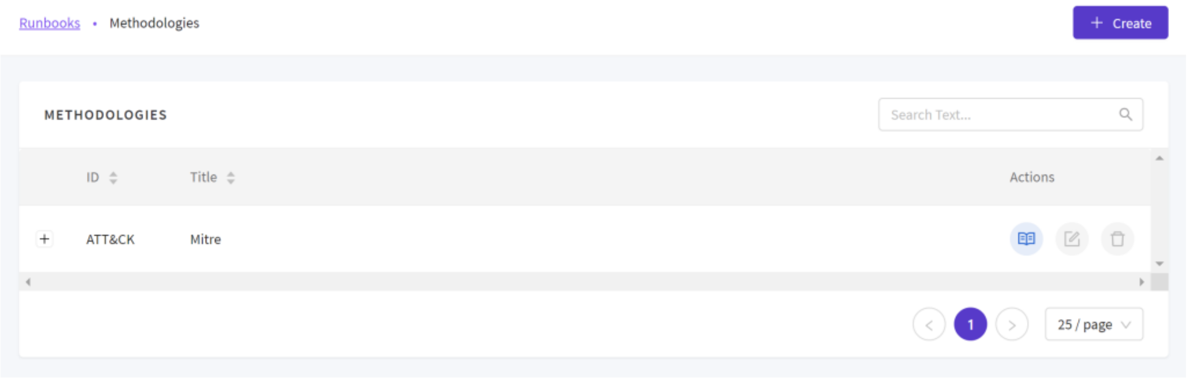
Point of Contact: Panos

Point of Contact Email: panos@pentestlaboratories.com

Client Description / Details: Purple Team Assessment

Tags: #purpleteam ×

By default PlexTrac contains the MITRE ATT&CK methodology which their TTP's (Tactics, Techniques and Procedures) can be incorporated into the assessment.



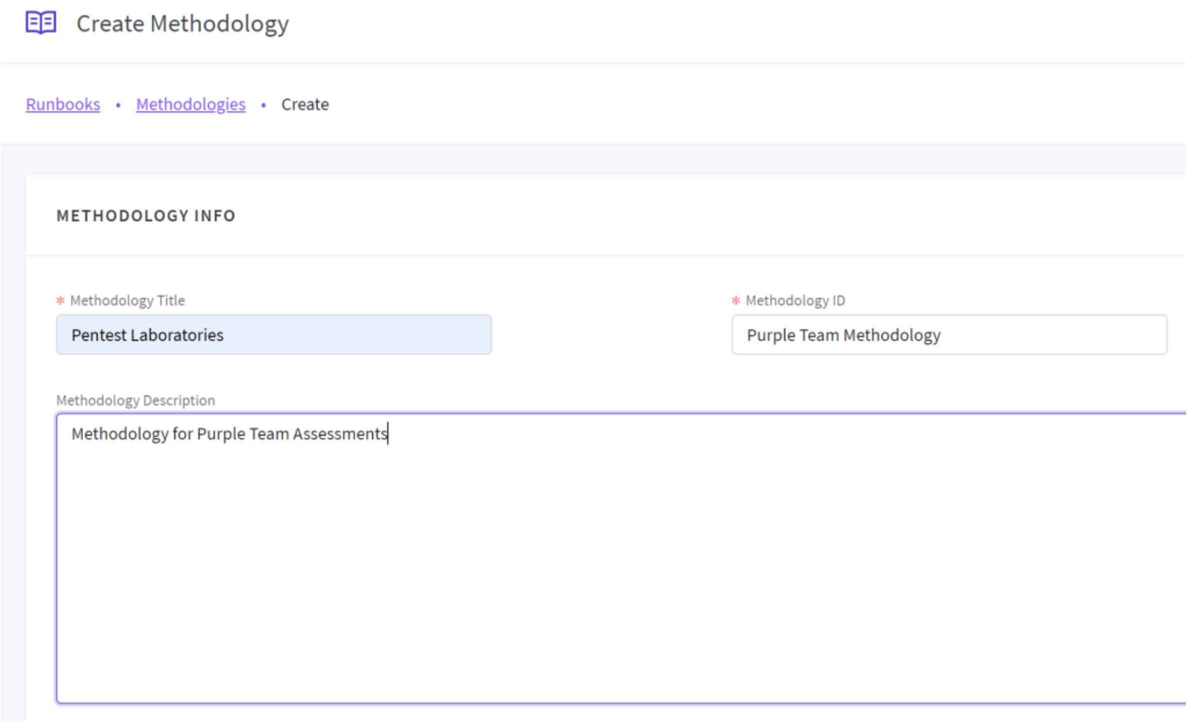
Runbooks • Methodologies

METHODOLOGIES

ID	Title	Actions
ATT&CK	Mitre	

PlexTrac – Mitre Methodology

However for this specific engagement a custom methodology has been created since one of the techniques for that particular scenario is not included in the MITRE framework. Two tactics are going to be implemented (Defense Evasion & Credential Access) and have been selected from the available list.



Create Methodology

Runbooks • Methodologies • Create

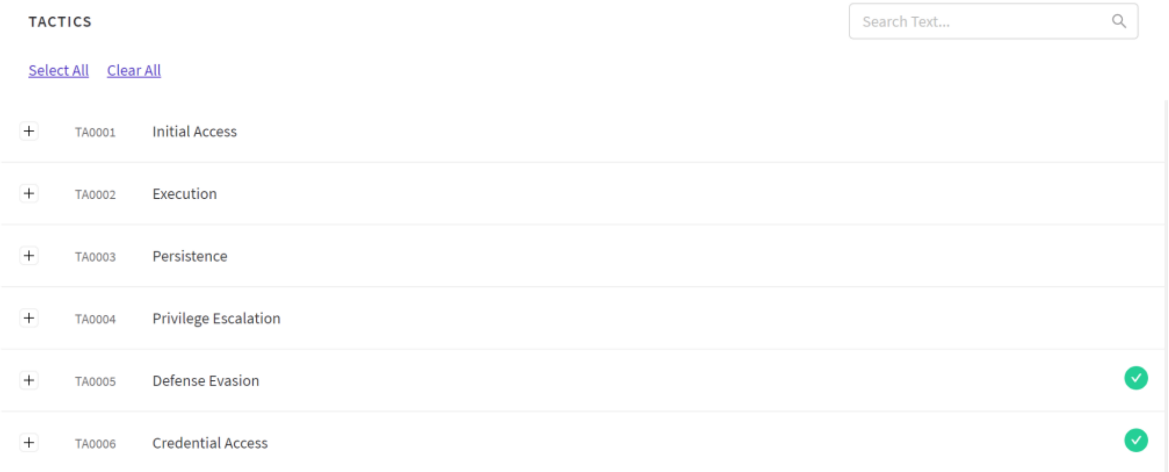
METHODOLOGY INFO

* Methodology Title: Pentest Laboratories

* Methodology ID: Purple Team Methodology

Methodology Description: Methodology for Purple Team Assessments

Custom Purple Team Methodology



TACTICS

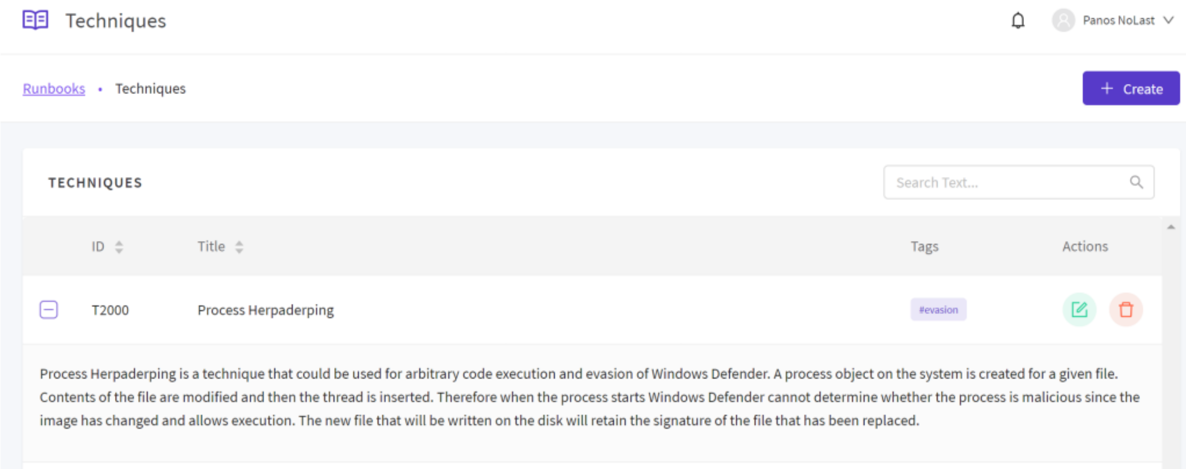
TA0001	Initial Access	
TA0002	Execution	
TA0003	Persistence	
TA0004	Privilege Escalation	
TA0005	Defense Evasion	✓
TA0006	Credential Access	✓

Tactics – Purple Team Methodology

The scope of the engagement was to assess the capability of the blue team to detect two techniques.

1. Process Herpaderping
2. OS Credential Dumping – LSASS Memory

Process Herpadeping is a defense evasion technique which bypasses EDR's via modification of the contents of the file when the process object has been already created on the operating system. This technique is not mapped to MITRE framework therefore it has been added manually on the platform.



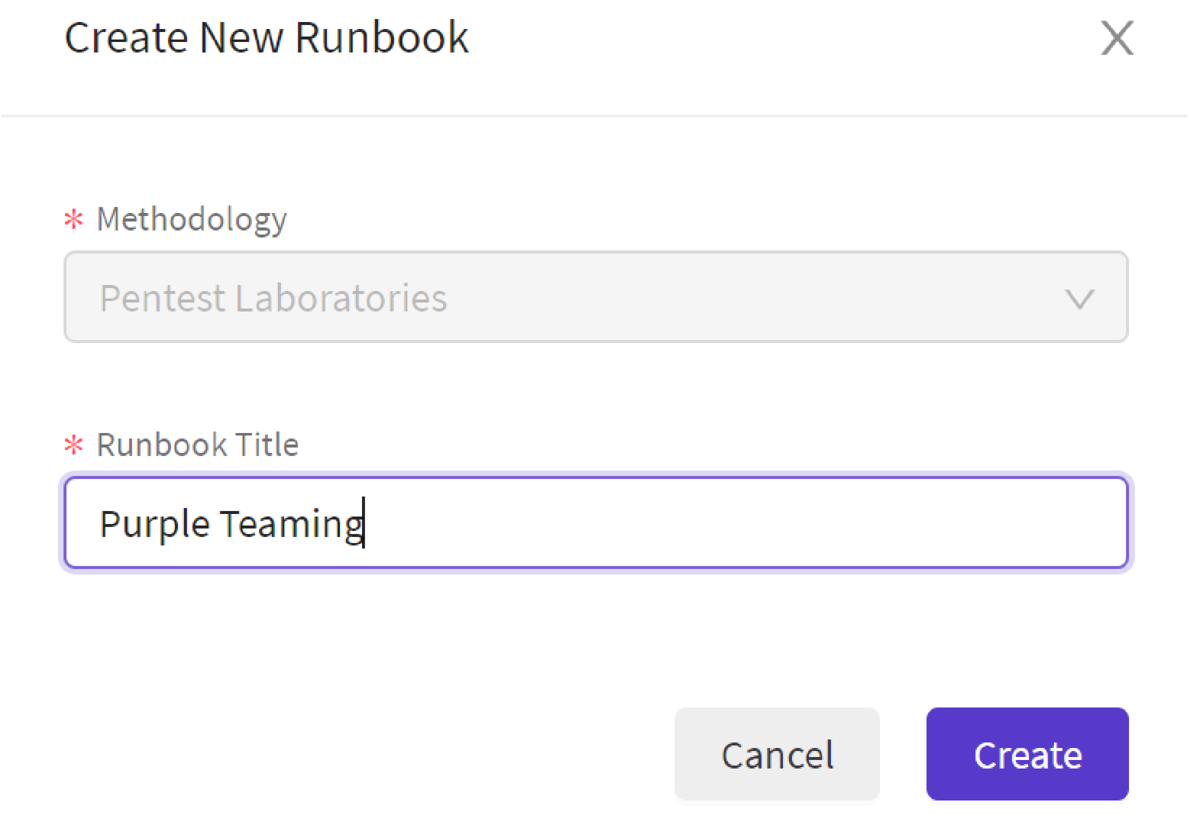
ID	Title	Tags	Actions
T2000	Process Herpaderping	#evasion	

Process Herpaderping is a technique that could be used for arbitrary code execution and evasion of Windows Defender. A process object on the system is created for a given file. Contents of the file are modified and then the thread is inserted. Therefore when the process starts Windows Defender cannot determine whether the process is malicious since the image has changed and allows execution. The new file that will be written on the disk will retain the signature of the file that has been replaced.

Create Technique – Process Herpaderping

Threat actors often attempt to retrieve credentials from the LSASS process. This technique is mapped to MITRE framework as T1003.001 and the associated procedure within scope is: "*Dump LSASS.exe Memory using Windows Task Manager*".

The tactics, techniques and procedures for the purple team exercise have been added into the Runbook – Purple Teaming which follows the custom methodology of Pentest Laboratories.



Create New Runbook

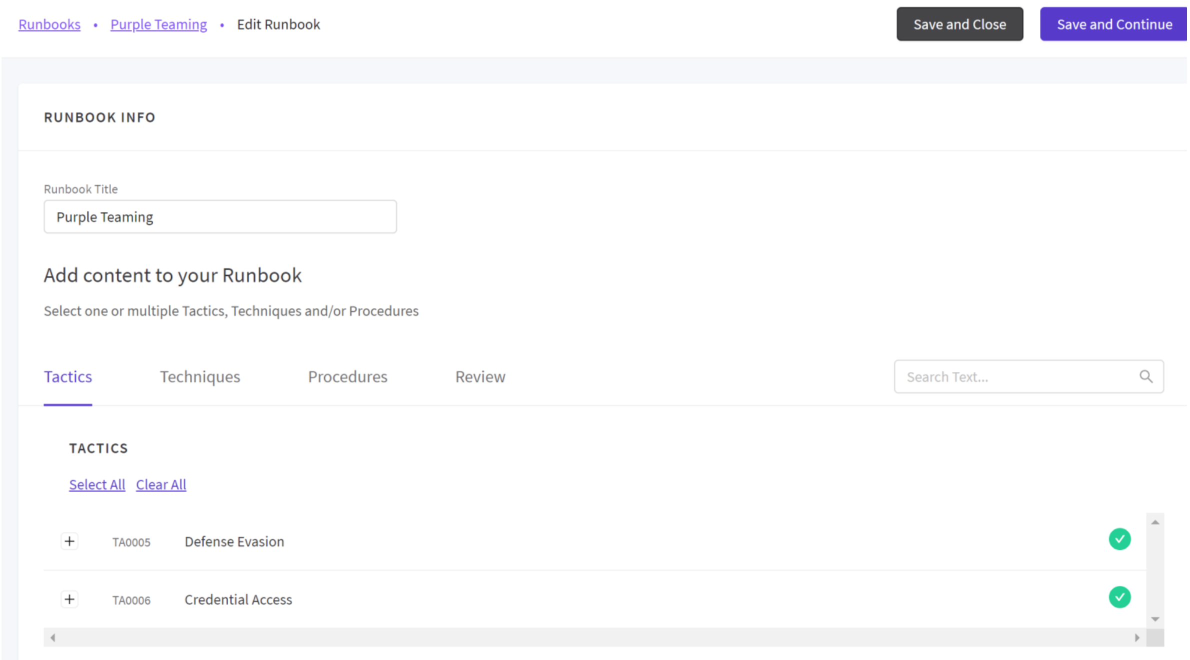
* Methodology

Pentest Laboratories

* Runbook Title

Purple Teaming

PlexTrac – Runbook



RUNBOOK INFO

Runbook Title

Purple Teaming

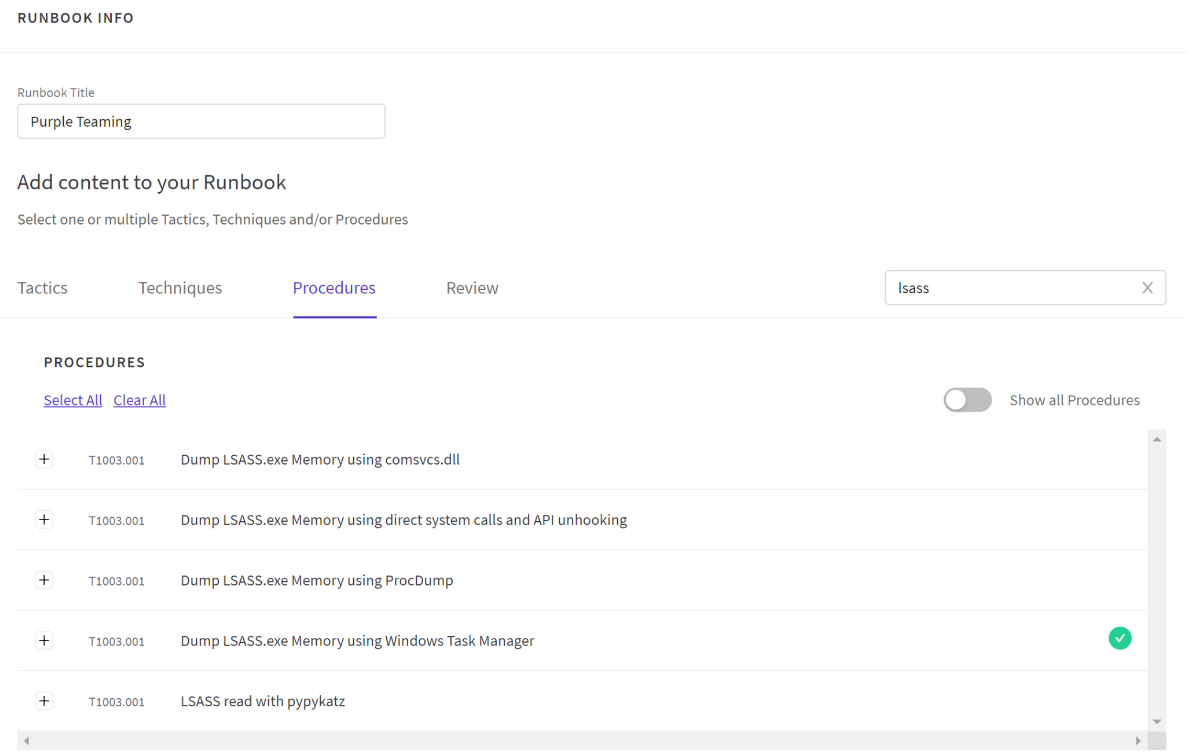
Add content to your Runbook

Select one or multiple Tactics, Techniques and/or Procedures

TACTICS

+	TA0005	Defense Evasion	✓
+	TA0006	Credential Access	✓

Purple Teaming Runbook – Tactics



RUNBOOK INFO

Runbook Title

Purple Teaming

Add content to your Runbook

Select one or multiple Tactics, Techniques and/or Procedures

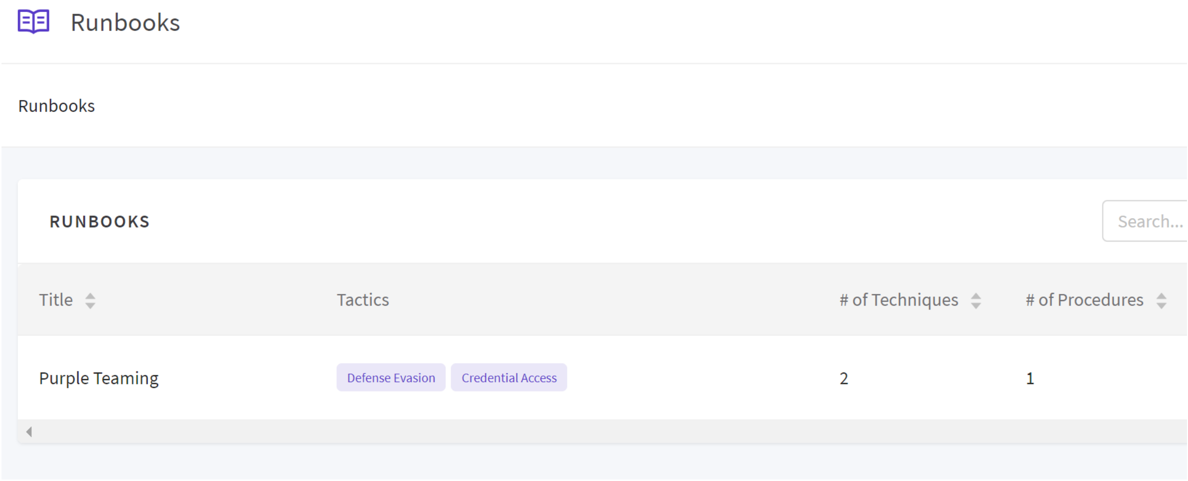
lsass

PROCEDURES

+	T1003.001	Dump LSASS.exe Memory using comsvcs.dll	
+	T1003.001	Dump LSASS.exe Memory using direct system calls and API unhooking	
+	T1003.001	Dump LSASS.exe Memory using ProcDump	
+	T1003.001	Dump LSASS.exe Memory using Windows Task Manager	✓
+	T1003.001	LSASS read with pypykatz	

Purple Teaming Runbook – Procedures

In summary the Purple Teaming RunBook will contain two tactics, two techniques and one procedure.



Runbooks

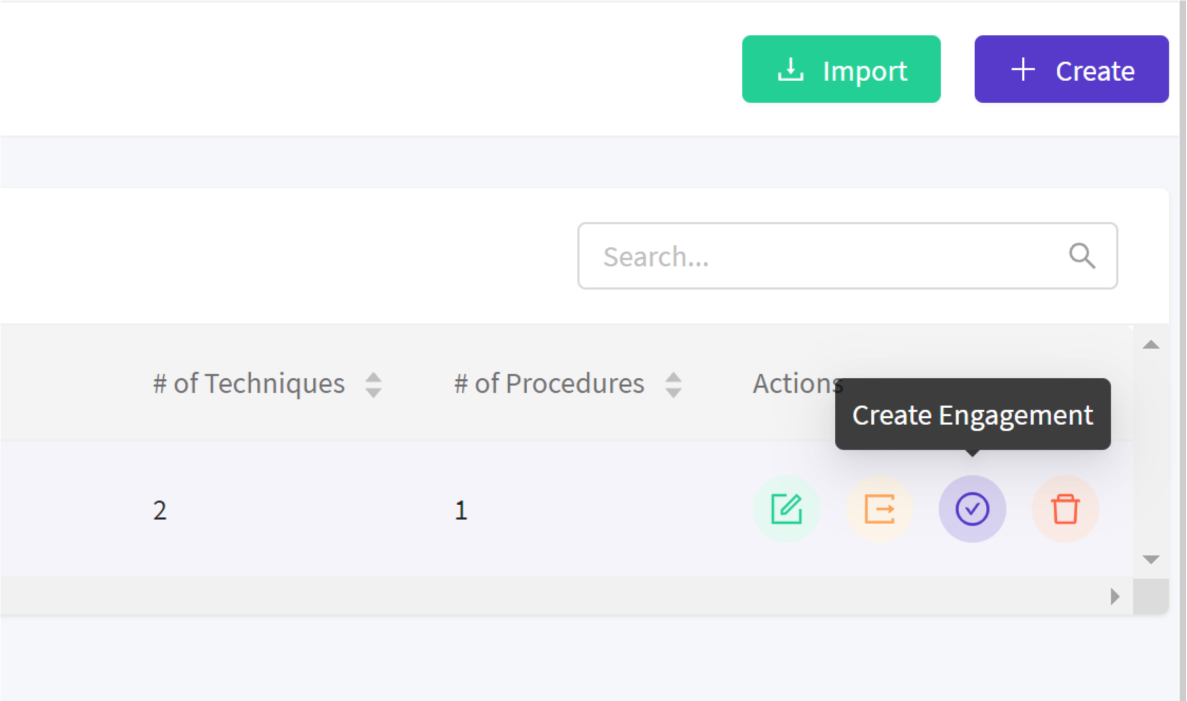
Runbooks

RUNBOOKS

Title	Tactics	# of Techniques	# of Procedures
Purple Teaming	Defense Evasion Credential Access	2	1

Purple Teaming Runbook

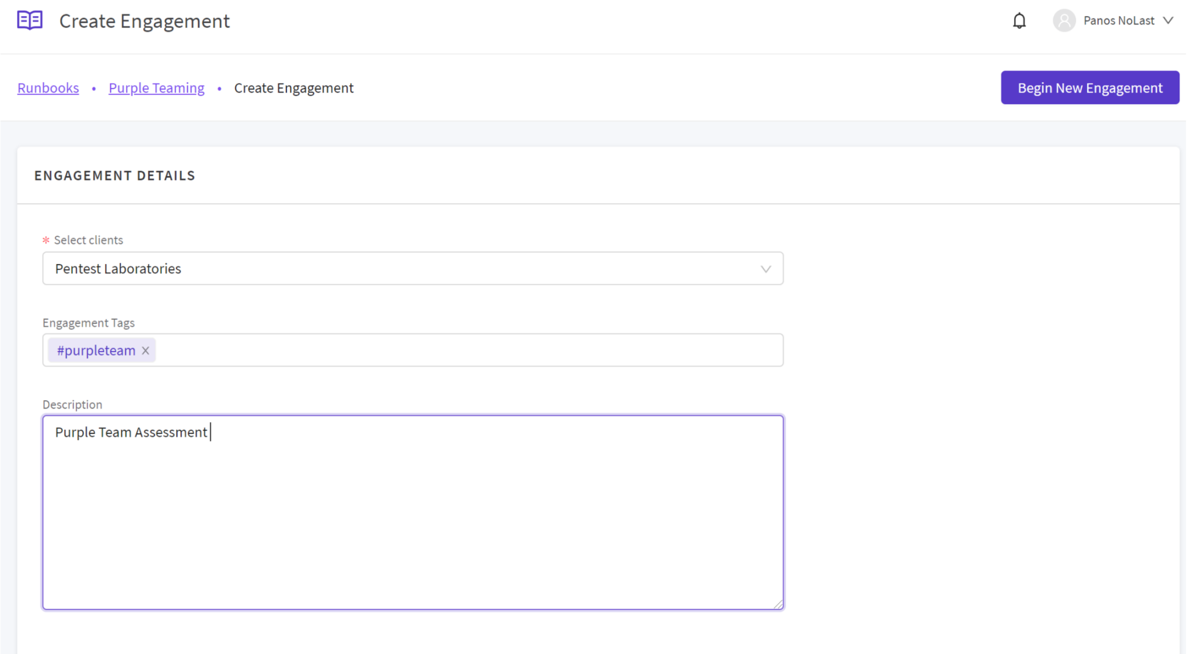
Engagements can be created from the Runbooks section by pressing the check purple button. The Runbook will be associated to the engagement.



# of Techniques	# of Procedures	Actions
2	1	

PlexTrac – Create Engagement

The engagement required some further information such as the Client name in this case Pentest Laboratories, tags which could be custom or associated with MITRE TTP's and description for any other relevant project information.



ENGAGEMENT DETAILS

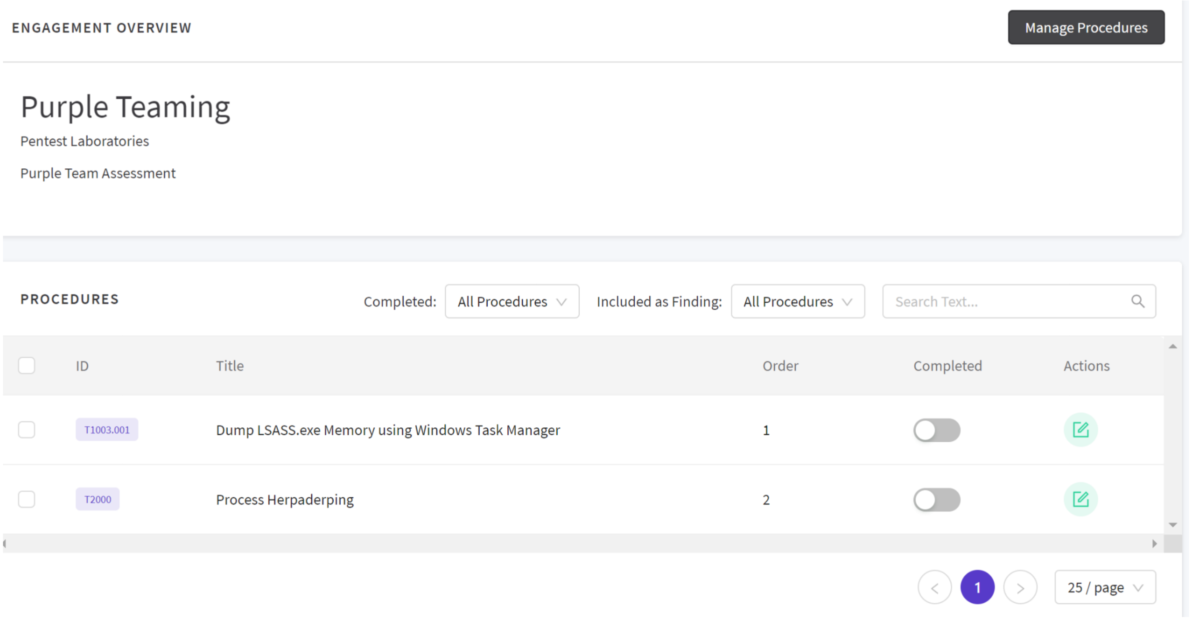
* Select clients: Pentest Laboratories

Engagement Tags: #purpleteam

Description: Purple Team Assessment

PlexTrac – Create Engagement

The engagement has been customized to fit the scope of the purple teaming which was to assess these two procedures as it can be seen from the engagement overview.



ENGAGEMENT OVERVIEW

Purple Teaming

Pentest Laboratories

Purple Team Assessment

PROCEDURES

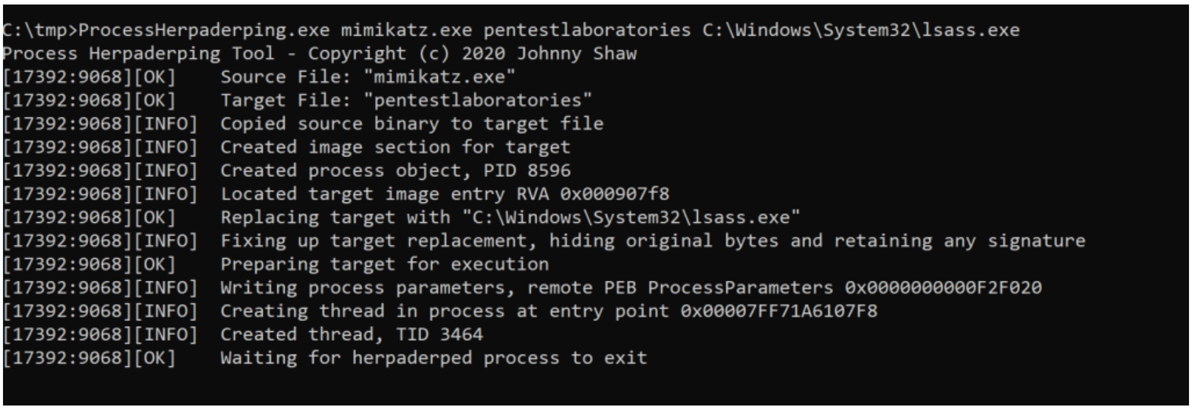
Completed: All Procedures

Included as Finding: All Procedures

□	ID	Title	Order	Completed	Actions
□	T1003.001	Dump LSASS.exe Memory using Windows Task Manager	1	○	✎
□	T2000	Process Herpaderping	2	○	✎

PlexTrac – Engagement Overview

The execution of Process Herpaderping technique was trivial as there is a proof of concept publicly available. This technique has been analysed in detail in the Pentest Laboratories article.

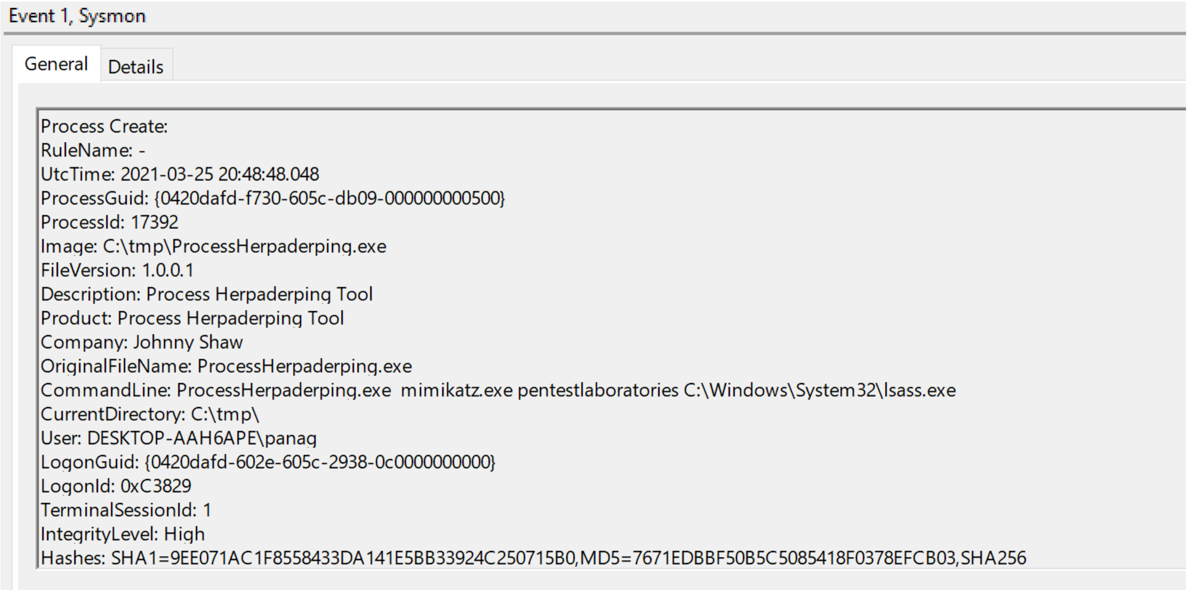


```
C:\tmp>ProcessHerpaderping.exe mimikatz.exe pentestlaboratories C:\Windows\System32\lsass.exe
Process Herpaderping Tool - Copyright (c) 2020 Johnny Shaw
[17392:9068][OK]    Source File: "mimikatz.exe"
[17392:9068][OK]    Target File: "pentestlaboratories"
[17392:9068][INFO]  Copied source binary to target file
[17392:9068][INFO]  Created image section for target
[17392:9068][INFO]  Created process object, PID 8596
[17392:9068][INFO]  Located target image entry RVA 0x000907f8
[17392:9068][OK]    Replacing target with "C:\Windows\System32\lsass.exe"
[17392:9068][INFO]  Fixing up target replacement, hiding original bytes and retaining any signature
[17392:9068][OK]    Preparing target for execution
[17392:9068][INFO]  Writing process parameters, remote PEB ProcessParameters 0x0000000000F2F020
[17392:9068][INFO]  Creating thread in process at entry point 0x00007FF71A6107F8
[17392:9068][INFO]  Created thread, TID 3464
[17392:9068][OK]    Waiting for herpaderped process to exit
```

Process Herpaderping Implementation

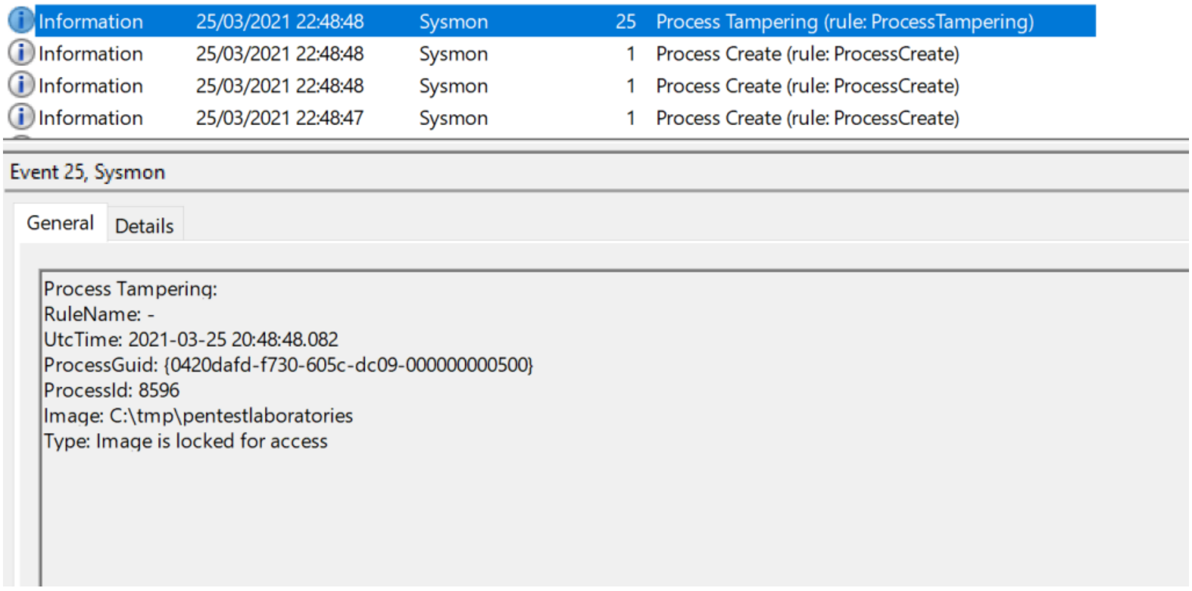
From the perspective of blue teaming the technique has generated two Sysmon events.

1. Event ID 1
2. Event ID 25



```
Process Create:
RuleName: -
UtcTime: 2021-03-25 20:48:48.048
ProcessGuid: {0420dafd-f730-605c-db09-000000000500}
ProcessId: 17392
Image: C:\tmp\ProcessHerpaderping.exe
FileVersion: 1.0.0.1
Description: Process Herpaderping Tool
Product: Process Herpaderping Tool
Company: Johnny Shaw
OriginalFileName: ProcessHerpaderping.exe
CommandLine: ProcessHerpaderping.exe  mimikatz.exe pentestlaboratories C:\Windows\System32\lsass.exe
CurrentDirectory: C:\tmp\
User: DESKTOP-AAH6APE\panag
LogonGuid: {0420dafd-602e-605c-2938-0c0000000000}
LogonId: 0xC3829
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=9EE071AC1F8558433DA141E5BB33924C250715B0,MD5=7671EDBBF50B5C5085418F0378EFCB03,SHA256
```

Sysmon – Process Herpaderping Event ID 1

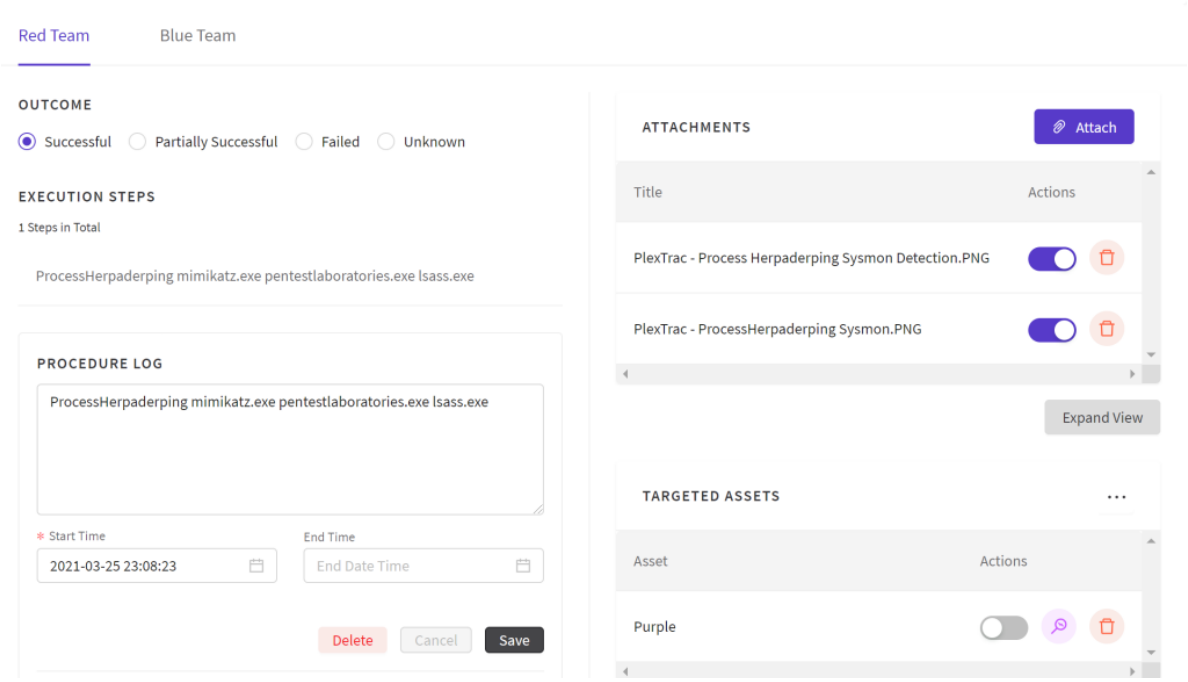


```
Information    25/03/2021 22:48:48    Sysmon    25    Process Tampering (rule: ProcessTampering)
Information    25/03/2021 22:48:48    Sysmon     1    Process Create (rule: ProcessCreate)
Information    25/03/2021 22:48:48    Sysmon     1    Process Create (rule: ProcessCreate)
Information    25/03/2021 22:48:47    Sysmon     1    Process Create (rule: ProcessCreate)
```

```
Process Tampering:
RuleName: -
UtcTime: 2021-03-25 20:48:48.082
ProcessGuid: {0420dafd-f730-605c-dc09-000000000500}
ProcessId: 8596
Image: C:\tmp\pentestlaboratories
Type: Image is locked for access
```

Sysmon – Process Herpaderping Event ID 25

The technique details including the outcome, relevant attachments, asset which the technique was executed and the procedure log details have been captured in PlexTrac in the Red Team tab.



OUTCOME

● Successful ○ Partially Successful ○ Failed ○ Unknown

EXECUTION STEPS

1 Steps in Total

ProcessHerpaderping mimikatz.exe pentestlaboratories.exe lsass.exe

PROCEDURE LOG

ProcessHerpaderping mimikatz.exe pentestlaboratories.exe lsass.exe

* Start Time: 2021-03-25 23:08:23

End Time: End Date Time

ATTACHMENTS

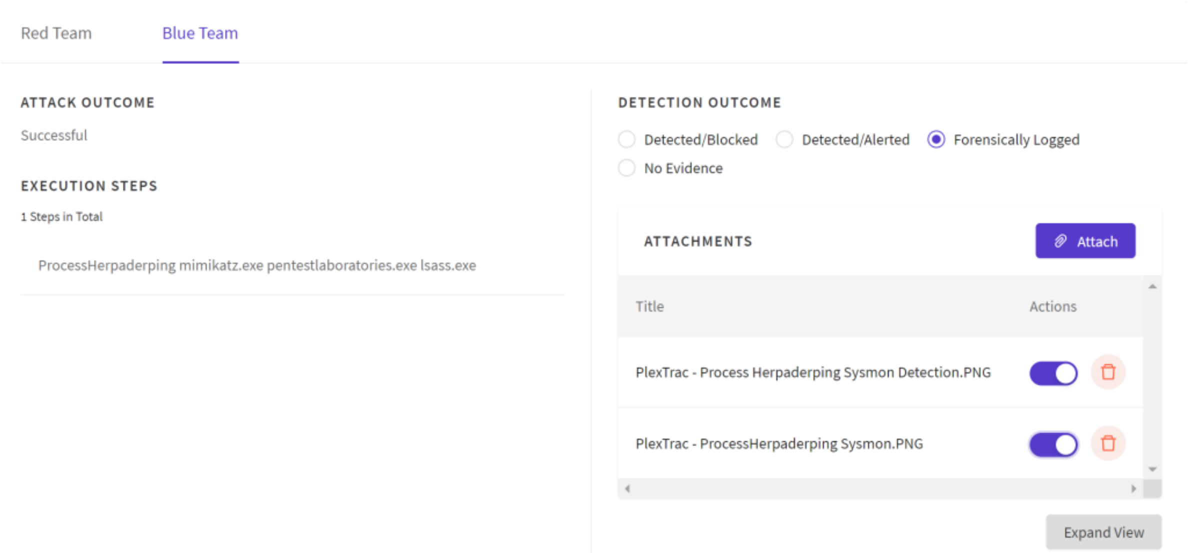
Title	Actions
PlexTrac - Process Herpaderping Sysmon Detection.PNG	
PlexTrac - ProcessHerpaderping Sysmon.PNG	

TARGETED ASSETS

Asset	Actions
Purple	

PlexTrac – Red Team

Even though the technique was successful it has been logged in Sysmon therefore the detection outcome for the blue team was: Forensically Logged. Relevant attachments have been uploaded and the Sysmon logs have been imported into the Procedure Log component with a timestamp about the date and time. However this area it could have been used for activities of the blue team for evaluation of existing procedures and policies once a threat has been discovered.



ATTACK OUTCOME

Successful

EXECUTION STEPS

1 Steps in Total

ProcessHerpaderping mimikatz.exe pentestlaboratories.exe lsass.exe

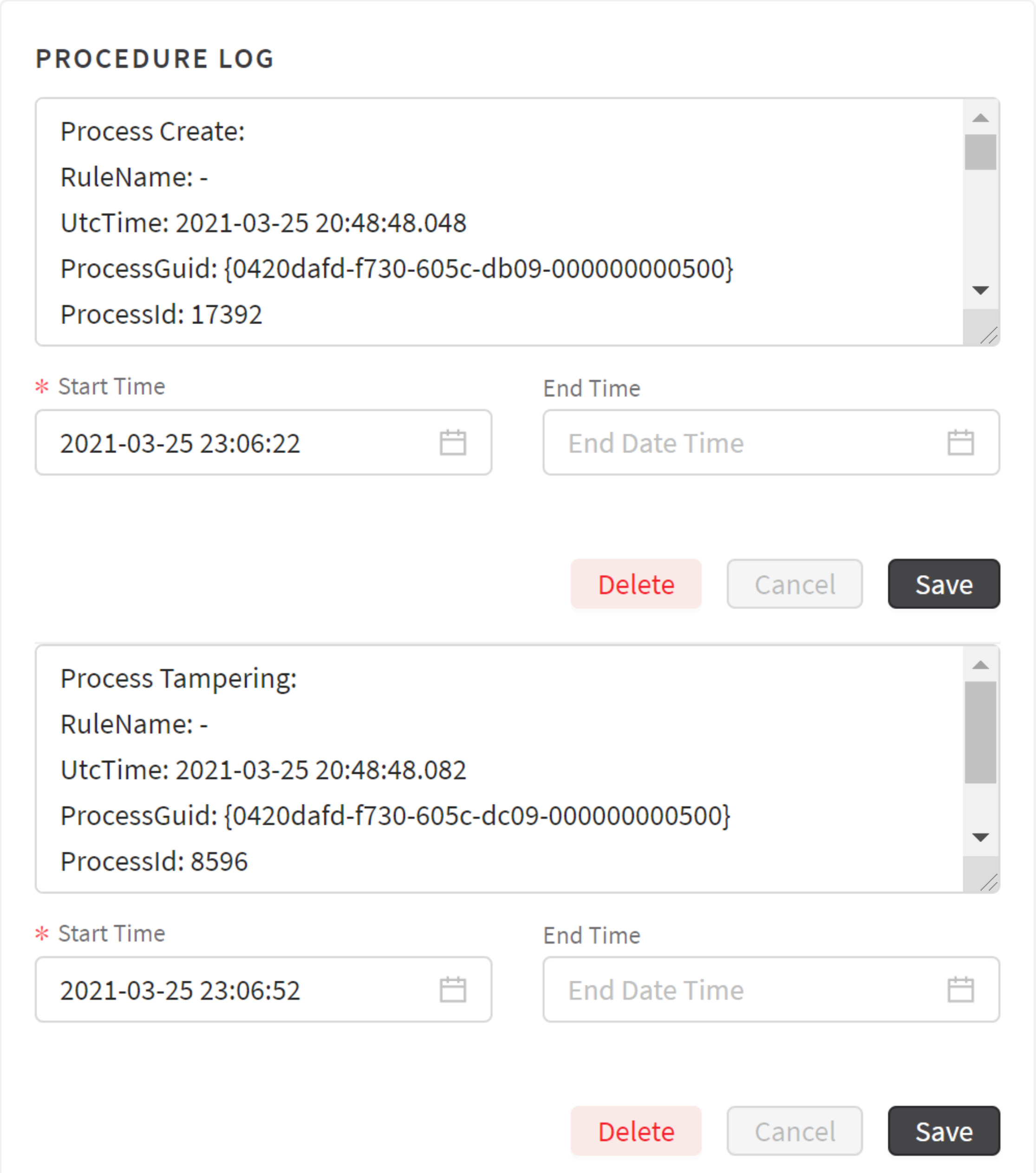
DETECTION OUTCOME

○ Detected/Blocked ○ Detected/Alerted ● Forensically Logged ○ No Evidence

ATTACHMENTS

Title	Actions
PlexTrac - Process Herpaderping Sysmon Detection.PNG	
PlexTrac - ProcessHerpaderping Sysmon.PNG	

PlexTrac – Blue Team



PROCEDURE LOG

```
Process Create:
RuleName: -
UtcTime: 2021-03-25 20:48:48.048
ProcessGuid: {0420dafd-f730-605c-db09-000000000500}
ProcessId: 17392
```

* Start Time: 2021-03-25 23:06:22

End Time: End Date Time

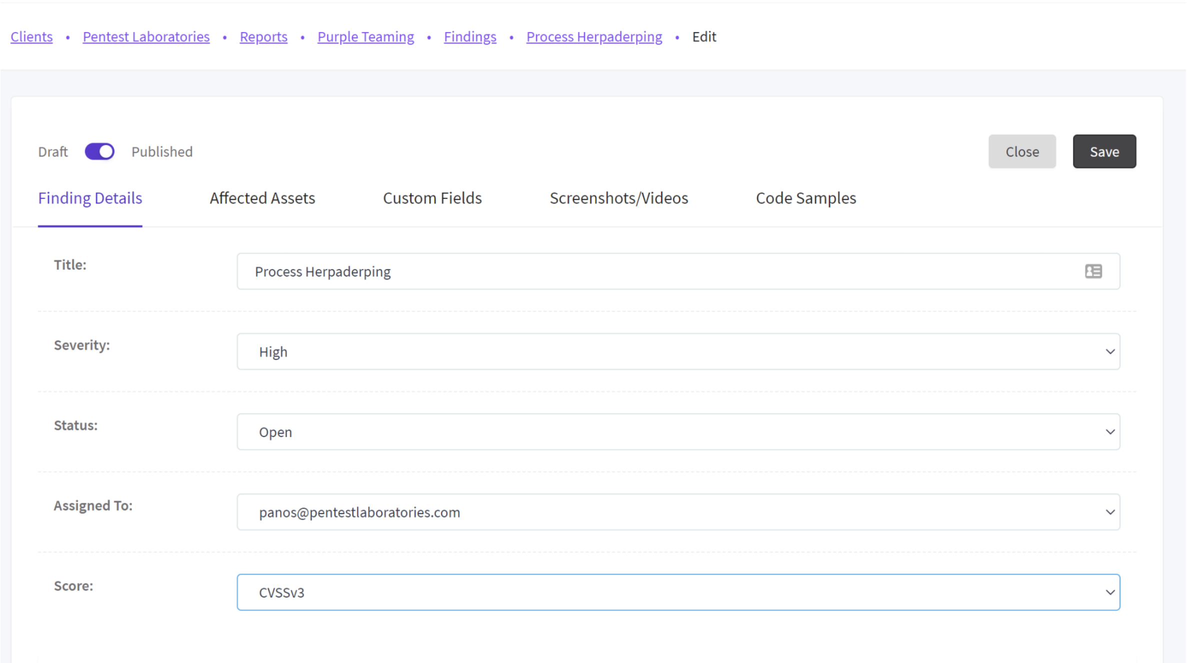
```
Process Tampering:
RuleName: -
UtcTime: 2021-03-25 20:48:48.082
ProcessGuid: {0420dafd-f730-605c-dc09-000000000500}
ProcessId: 8596
```

* Start Time: 2021-03-25 23:06:52

End Time: End Date Time

PlexTrac – Procedure Log

The same procedure has been followed in PlexTrac and for the other technique of dumping the lsass via the task manager. The results of the engagement have been added into the online report as PlexTrac contains various fields similarly to other pentest reporting tools. Code samples, screenshots and videos of the assessment could be added as well.



Clients • Pentest Laboratories • Reports • Purple Teaming • Findings • Process Herpaderping • Edit
Draft
Published
Close
Save
Finding Details
Affected Assets
Custom Fields
Screenshots/Videos
Code Samples

Title: Process Herpaderping

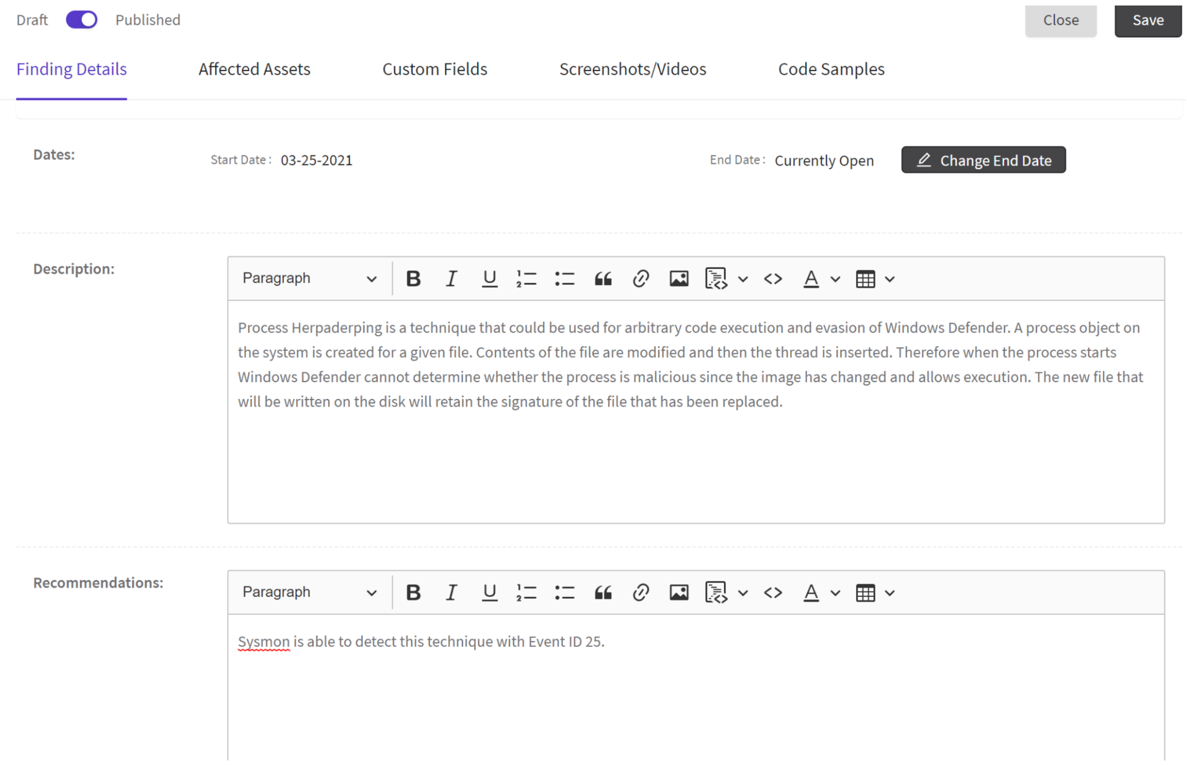
Severity: High

Status: Open

Assigned To: panos@pentestlaboratories.com

Score: CVSSv3

PlexTrac Findings – Process Herpaderping



Dates: Start Date : 03-25-2021 End Date : Currently Open

Description:

Process Herpaderping is a technique that could be used for arbitrary code execution and evasion of Windows Defender. A process object on the system is created for a given file. Contents of the file are modified and then the thread is inserted. Therefore when the process starts Windows Defender cannot determine whether the process is malicious since the image has changed and allows execution. The new file that will be written on the disk will retain the signature of the file that has been replaced.

Recommendations:

Sysmon is able to detect this technique with Event ID 25.

PlexTrac – Finding Details

The executed techniques can be viewed directly in the PlexTrac platform, including all the details that have been logged during the engagement, severity and date which provide the ability of managers and members to view the results of the assessment with all the technical details, screenshots and logs.

Process Herpaderping

Report

Purple Teaming

Description

Process Herpaderping is a technique that could be used for arbitrary code execution and evasion of Windows Defender. A process object on the system is created for a given file. Contents of the file are modified and then the thread is inserted. Therefore when the process starts Windows Defender cannot determine whether the process is malicious since the image has changed and allows execution. The new file that will be written on the disk will retain the signature of the file that has been replaced.

STATUS

Open

SEVERITY

High

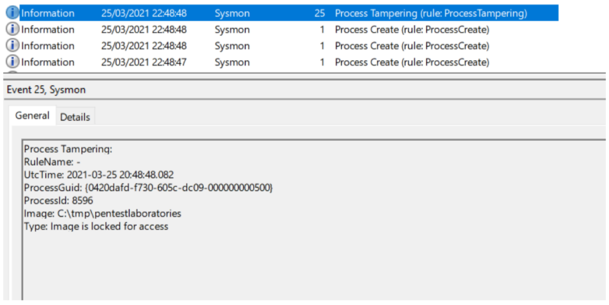
ASSIGNEE

panos@pentestlaboratories.com

DATE REPORTED

3/25/2021

Exhibit 1. PlexTrac - Process Herpaderping Sysmon Detection.PNG



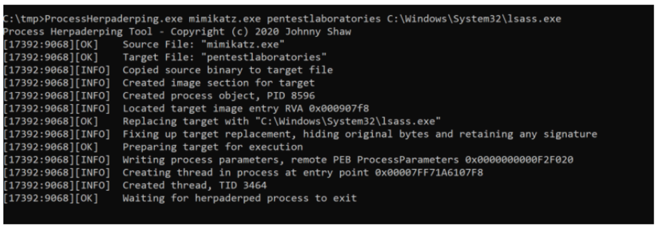
```
Information   25/03/2021 22:48:48   Sysmon   25   Process Tampering (rule: ProcessTampering)
Information   25/03/2021 22:48:48   Sysmon    1   Process Create (rule: ProcessCreate)
Information   25/03/2021 22:48:48   Sysmon    1   Process Create (rule: ProcessCreate)
Information   25/03/2021 22:48:47   Sysmon    1   Process Create (rule: ProcessCreate)
```

Event 25, Sysmon

```
Process Tampering:
RuleName: -
UtcTime: 2021-03-25 20:48:48.082
ProcessGuid: {0420dafd-f730-605c-dc09-000000000500}
ProcessId: 8596
Image: C:\tmp\pentestlaboratories
Type: Image is locked for access
```

Exhibit 2. PlexTrac - ProcessHerpaderping Sysmon.PNG

Exhibit 3.



```
C:\tmp>ProcessHerpaderping.exe mimikatz.exe pentestlaboratories C:\Windows\System32\lsass.exe
Process Herpaderping Tool - Copyright (c) 2020 Johnny Shaw
[17392:9068][OK]    Source File: "mimikatz.exe"
[17392:9068][OK]    Target File: "pentestlaboratories"
[17392:9068][INFO]  Copied source binary to target file
[17392:9068][INFO]  Created image section for target
[17392:9068][INFO]  Created process object, PID 8596
[17392:9068][INFO]  Located target image entry RVA 0x000907f8
[17392:9068][OK]    Replacing target with "C:\Windows\System32\lsass.exe"
[17392:9068][INFO]  Fixing up target replacement, hiding original bytes and retaining any signature
[17392:9068][OK]    Preparing target for execution
[17392:9068][INFO]  Writing process parameters, remote PEB ProcessParameters 0x0000000000F2F020
[17392:9068][INFO]  Creating thread in process at entry point 0x00007FF71A6107F8
[17392:9068][INFO]  Created thread, TID 3464
[17392:9068][OK]    Waiting for herpaderped process to exit
```

Code Sample 1.

```
ProcessHerpaderping.exe mimikatz.exe pentestlaboratories lsass.exe
```

Execution Steps

- ProcessHerpaderping mimikatz.exe pentestlaboratories.exe lsass.exe

Offensive Outcome

Successful

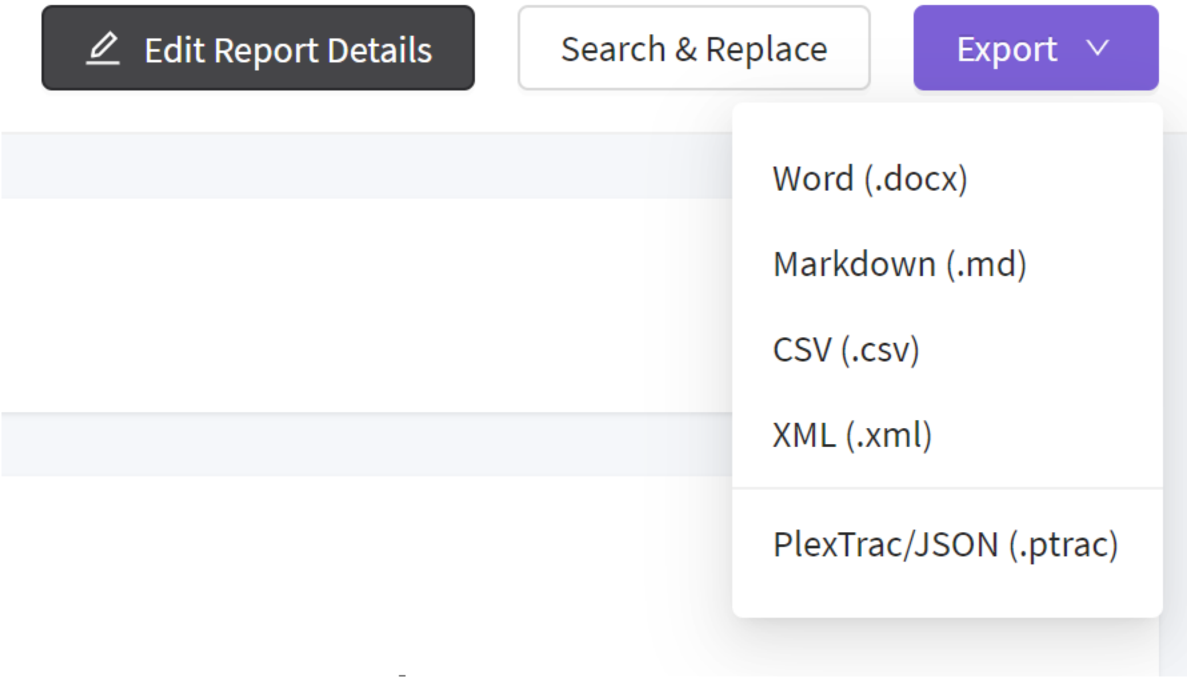
Detection Outcome

Forensically Logged

Procedure Log

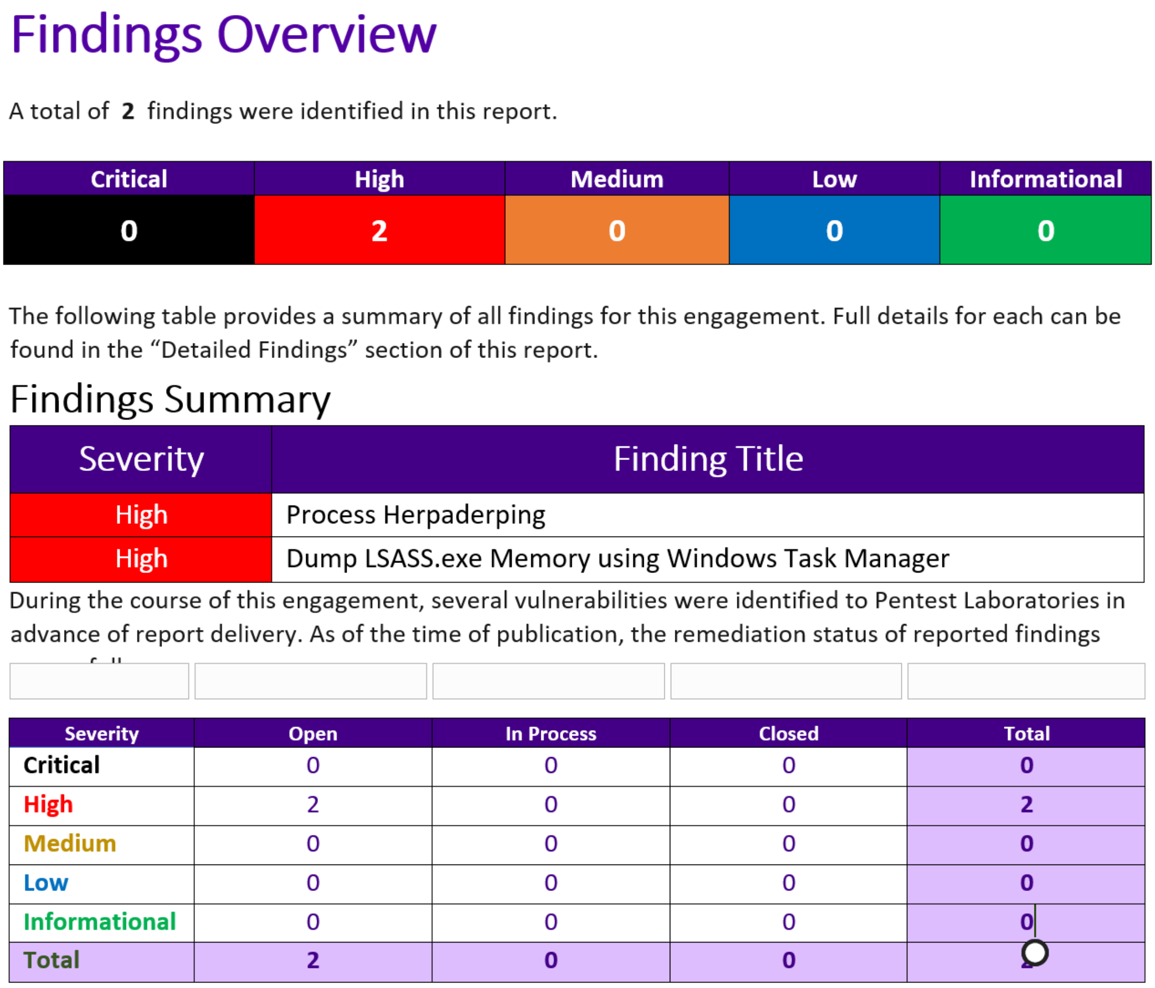
Blue Procedure: Process Create:
RuleName: -
UtcTime: 2021-03-25 20:48:48.048
ProcessGuid: {0420dafd-f730-605c-db09-000000000500}
ProcessId: 17392
Image: C:\tmp\ProcessHerpaderping.exe
FileVersion: 1.0.0.1
Description: Process Herpaderping Tool
Product: Process Herpaderping Tool

The results of the report could be exported into various formats as it can be seen below.



PlexTrac – Report Export Options

For this assessment the results have been exported into a word document. The template was very clean with a similar structure of pentest report templates with an Executive Summary, Findings Overview and Detailed Findings where the information was exported from the platform directly into the word document without breaking the template formatting.



Findings Overview

A total of **2** findings were identified in this report.

Critical	High	Medium	Low	Informational
0	**2**	**0**	**0**	**0**

The following table provides a summary of all findings for this engagement. Full details for each can be found in the "Detailed Findings" section of this report.

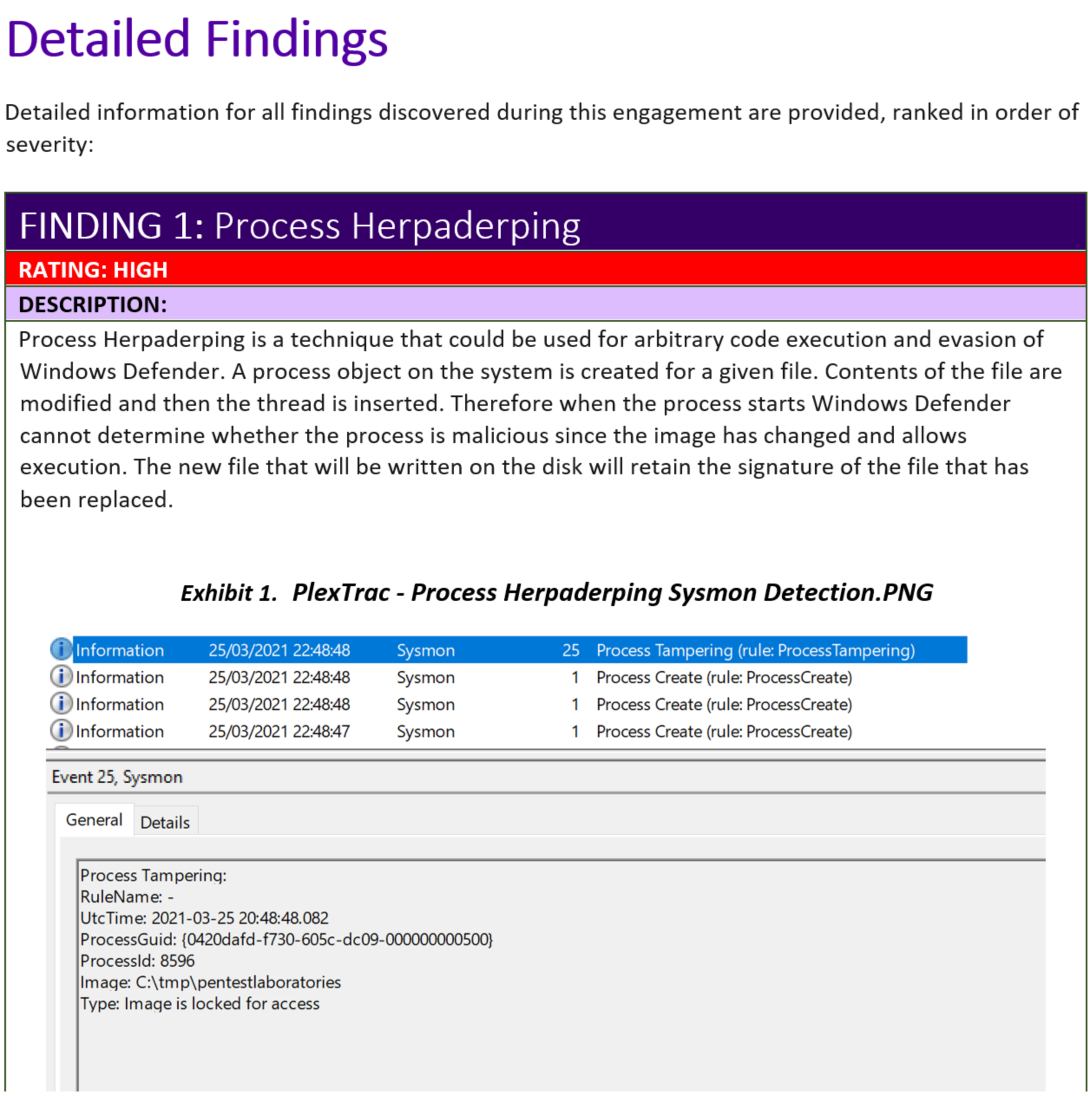
Findings Summary

Severity	Finding Title
High	Process Herpaderping
High	Dump LSASS.exe Memory using Windows Task Manager

During the course of this engagement, several vulnerabilities were identified to Pentest Laboratories in advance of report delivery. As of the time of publication, the remediation status of reported findings

Severity	Open	In Process	Closed	Total
Critical	0	0	0	**0**
High	2	0	0	**2**
Medium	0	0	0	**0**
Low	0	0	0	**0**
Informational	0	0	0	**0**
Total	**2**	**0**	**0**	**2**

PlexTrac – Report Findings Summary



Detailed Findings

Detailed information for all findings discovered during this engagement are provided, ranked in order of severity:

FINDING 1: Process Herpaderping

RATING: HIGH

DESCRIPTION:

Process Herpaderping is a technique that could be used for arbitrary code execution and evasion of Windows Defender. A process object on the system is created for a given file. Contents of the file are modified and then the thread is inserted. Therefore when the process starts Windows Defender cannot determine whether the process is malicious since the image has changed and allows execution. The new file that will be written on the disk will retain the signature of the file that has been replaced.

Exhibit 1. PlexTrac - Process Herpaderping Sysmon Detection.PNG

```
Information   25/03/2021 22:48:48   Sysmon   25   Process Tampering (rule: ProcessTampering)
Information   25/03/2021 22:48:48   Sysmon    1   Process Create (rule: ProcessCreate)
Information   25/03/2021 22:48:48   Sysmon    1   Process Create (rule: ProcessCreate)
Information   25/03/2021 22:48:47   Sysmon    1   Process Create (rule: ProcessCreate)
```

Event 25, Sysmon

```
Process Tampering:
RuleName: -
UtcTime: 2021-03-25 20:48:48.082
ProcessGuid: {0420dafd-f730-605c-dc09-000000000500}
ProcessId: 8596
Image: C:\tmp\pentestlaboratories
Type: Image is locked for access
```

PlexTrac – Detailed Findings

Conclusion

Purple Team assessments require a collaboration platform which will have the necessary components and provide flexibility in terms of reporting and customization. PlexTrac have been developed with the mindset of organizing, storing and exporting the results of the engagement in a clean format. Managers can get visibility of the reports and the status of findings, consultancies can get a reporting tool for their engagements as the writeups database contains a high volume of issues and finally red and blue teams can get a platform which they could store results from purple team assessments. Conducting engagements with PlexTrac was definitely a unique experience and a product to be considered for red and blue teams.

For more information about PlexTrac capabilities visit their website and follow them on their social media: