Start Wearing
PURPLE

ADVERSARY EMULATION WITH LOGGING AND MONITORING

SecureData™ TECHNOLOGIES

WHO AM I

macrosec

AMARJIT LABHURAM [@amarjit_labu]

- ★ Technical Director @ MacroSec Ltd
- ★ Cybersecurity Researcher
- ★ Offensive Security Lover
- ★ Penetration Tester / Red Teamer

HOBBIES:

- ★ Farming
- ★ Fishing
- ★ DJing Electronic Music
- ★ Foodie & Coffee Lover

AGENDA

- What is a Purple Team?
- What is Adversary Emulation?
- Logging & Monitoring
- Demo [Adversary Emulation]
- Running your own Purple Team exercise

ACRONYMS

- **TTP** = Tactics, Techniques & Procedures
- **SOC** = Security Operations Centre
- **DFIR** = Digital Forensics & Incident Response
- **IOC** = Indicators Of Compromise
- **CVE** = Common Vulnerabilities and Exposures
- **CVSS** = Common Vulnerability Scoring System
- **C2** = Command & Control
- **ELK** = Elasticsearch, Logstash & Kibana
- **SIEM** = Security Information Events Management

WHAT IS A PURPLE TEAM?

A team collaboratively working together to test, measure and improve defensive security posture (people, process, and technology).

- Cyber Threat Intelligence - research and provide adversary **Tactic**, **Techniques** & **Procedures** (TTPs)

- Red Team - offensive team in charge of emulating adversaries and TTPs

- Blue Team - the defenders. Security Operations Center (SOC), Threat Hunting Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Providers (MSSP)

Purple Team Exercise Framework

COMMON LANGUAGE

A collaboration means various members need to communicate in a way that every member understands one another.

- CVE & CVSS scores for vulnerabilities in technologies.
- Understanding Attacks:
  1. Cyber Kill Chain
  2. MITRE ATT&CK
- Understanding Adversary behaviour:
  1. Pyramid of Pain
  2. TTP Pyramid

Running Your First Purple Team Exercise: Understand the Cyber Kill Chain, Cyber Threat Intelligence, Emulation, and Response

CYBER KILL CHAIN

https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain

MITRE ATT&CK MATRIX

ATT&CK® Navigator (mitre-attack.github.io)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	BITS Jobs	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (12)	Direct Volume Access	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Execution Guardrails (1)	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Exploitation for Defense Evasion	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	Group Policy Modification	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Group Policy Modification	Hide Artifacts (7)	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Multi-Band Communication		Network Denial of Service (2)
				Hijack Execution Flow (11)	Process Injection (11)	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Resource Hijacking
				Implant Container Image	Scheduled Task/Job (6)	Indicator Removal on Host (6)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Service Stop
				Office Application Startup (6)	Valid Accounts (4)	Indirect Command Execution	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		System Shutdown/Reboot
				Pre-OS Boot (5)		Masquerading (6)	Unsecured Credentials (6)	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		
				Scheduled Task/Job (6)		Modify Authentication Process (4)		Process Discovery		Man-in-the-Middle (2)	Remote Access Software		
						Modify Cloud Compute Infrastructure (4)		Query Registry		Screen Capture	Traffic Signaling (1)		
						Modify Registry		Remote System Discovery			Web Service (3)		
								Software Discovery (1)					

MITRE ATT&CK MATRIX

TACTIC

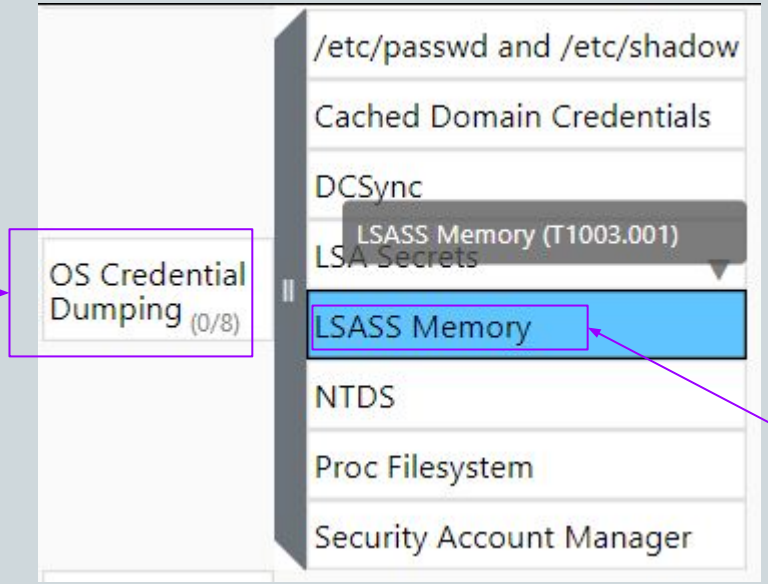
TECHNIQUE

Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)
Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture
Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection
Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data
Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object
Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)
Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)
Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System
OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive
Steal Application Access Token	Network Share Discovery		Data from Removable Media
Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)
Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)
	Peripheral Device Discovery		Input Capture (4)
	Permission Groups Discovery (3)		
	Process Discovery		

MITRE ATT&CK MATRIX

TECHNIQUE

T1003

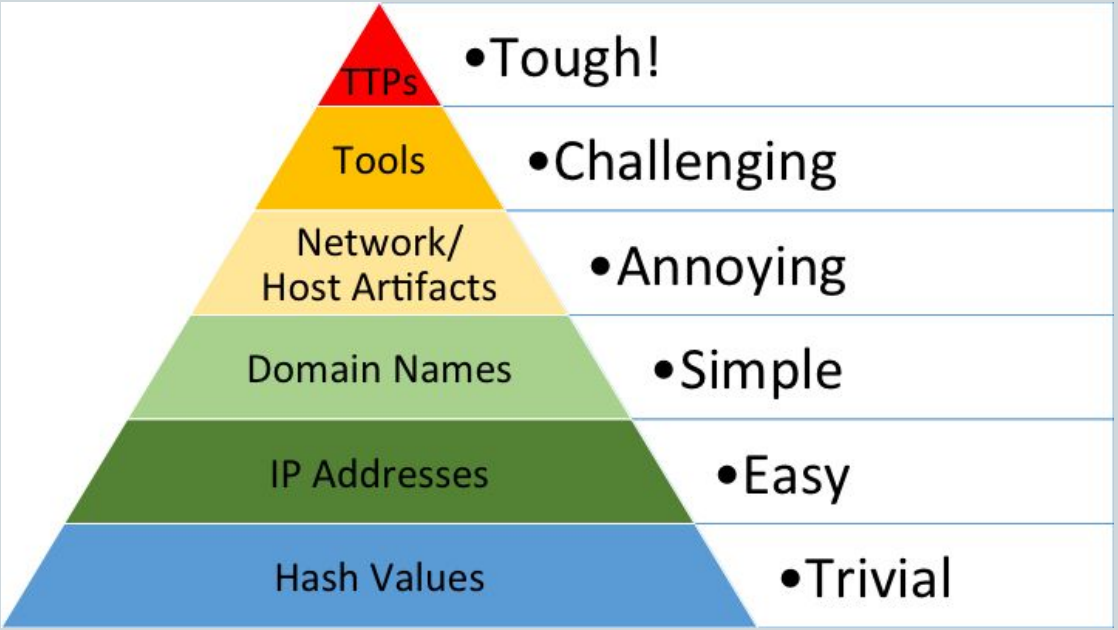


SUB TECHNIQUE

T1003.001

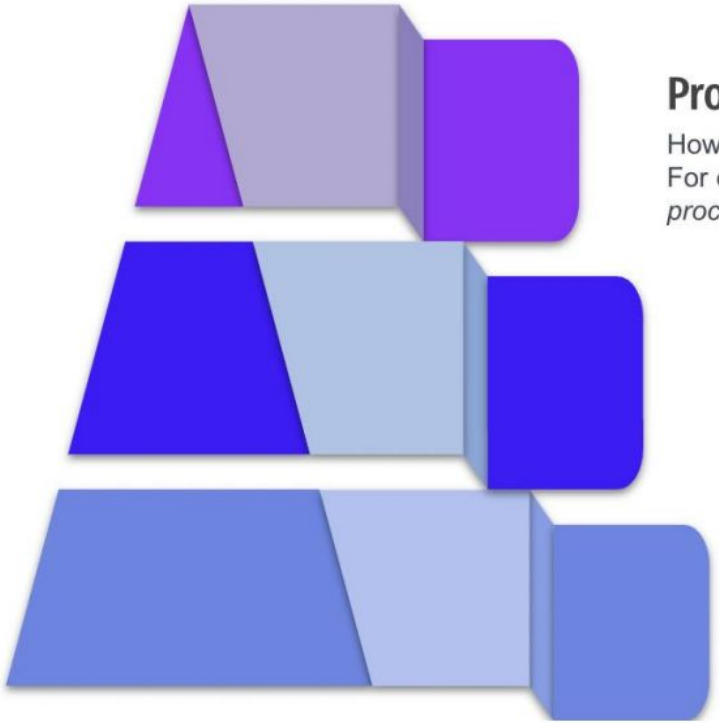
PYRAMID OF PAIN

Purple Team being highly TTP driven would be operating at the top of the pyramid



The Pyramid of Pain | Enterprise Detection & Response (detect-respond.blogspot.com)

TTP PYRAMID



Procedures

How the technique was carried out.
For example, the attacker used
procdump -ma lsass.exe lsass_dump

Techniques

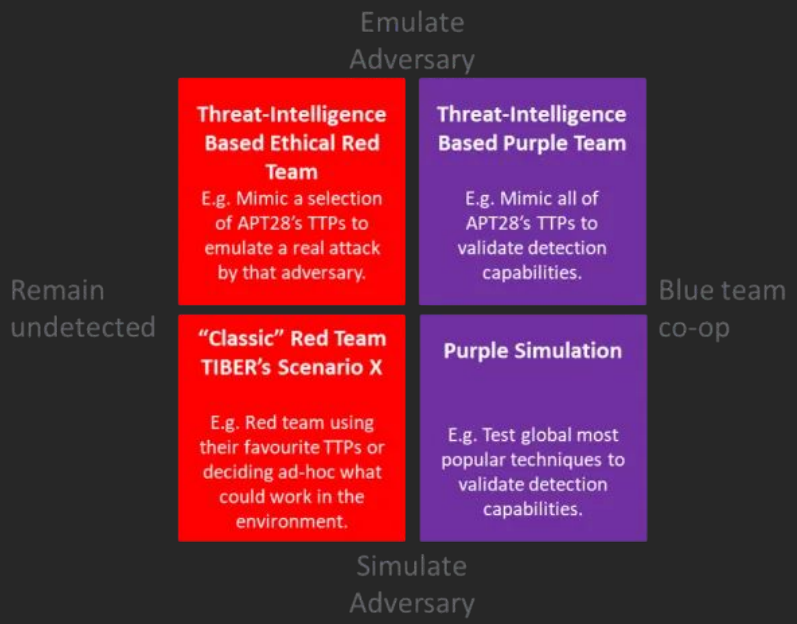
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

SCYTHE Library: Summiting the Pyramid of Pain: The TTP Pyramid

WHAT IS ADVERSARY EMULATION



Adversary emulation is an impersonation, mimicking of someone or something else. Based on threat intelligence, you determine APT28 is most likely to target your organization. To emulate this adversary, you mimic the TTPs they use and test those in your environment. You behave exactly like they would.

Attack Simulation vs Attack Emulation

PENETRATION TESTING VS ADVERSARY EMULATION

PENETRATION TEST	VS.	ADVERSARY EMULATION
Identify and exploit vulnerabilities on a (series of) system(s) to assess security		Assess how resilient an organization is versus a certain adversary / threat actor
Focused on a specific scope (typically an application or network range)		Focused on the execution of a scenario (typically defined by a number of flags)
Primarily tests prevention, typically less focus on detection		Typically tests both prevention and detection (so is less valuable if there is no Blue Team)

Running Your First Purple Team Exercise: Understand the Cyber Kill Chain, Cyber Threat Intelligence, Emulation, and Response

RED TEAMING VS PURPLE TEAMING

RED TEAM	VS.	PURPLE TEAM
A Red Team involves emulation of a realistic threat actor (using TTPs)		A Purple Team involves emulation of a realistic threat actor (using TTPs)
In a typical Red Team, interaction with the Blue Team is **limited** (red vs. blue)		In a typical Purple Team, interaction with the Blue Team is **maximized** (collaboration)
The goal of the Red Team is to **assess** how well the Blue Team prevents and detects		The goal of the Purple Team is to **improve** how well the Blue Team prevents and detects

Running Your First Purple Team Exercise: Understand the Cyber Kill Chain, Cyber Threat Intelligence, Emulation, and Response

LOGGING & MONITORING

Logging is a method of tracking and storing data from security events to allow the opportunity to detect for malicious activity.

Monitoring is a diagnostic tool used for alerting Blue Team to Indicators of Compromise (IOC) by analyzing metrics.

SYSMON

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

LOGGING VIA SYSMON

Sysmon uses a xml configuration file during installation to enable logging of the defined events to be monitored.

```xml
<Sysmon  schemaversion="3.2">
  <!-- Capture all the hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condition="contains">microsoft</Signature>
      <Signature condition="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include"/>
    <!-- Log network connection if the destination port equals 443 -->
    <!-- or 80, and the process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
  </EventFiltering>
</Sysmon>
```

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

LOGGING VIA SYSMON

WHERE DO I BEGIN?

Swift On Security sysmon-config

Florian Roth sysmon-config

Sysmon-Modular

LOGGING VIA SYSMON

SYSMON INSTALLATION

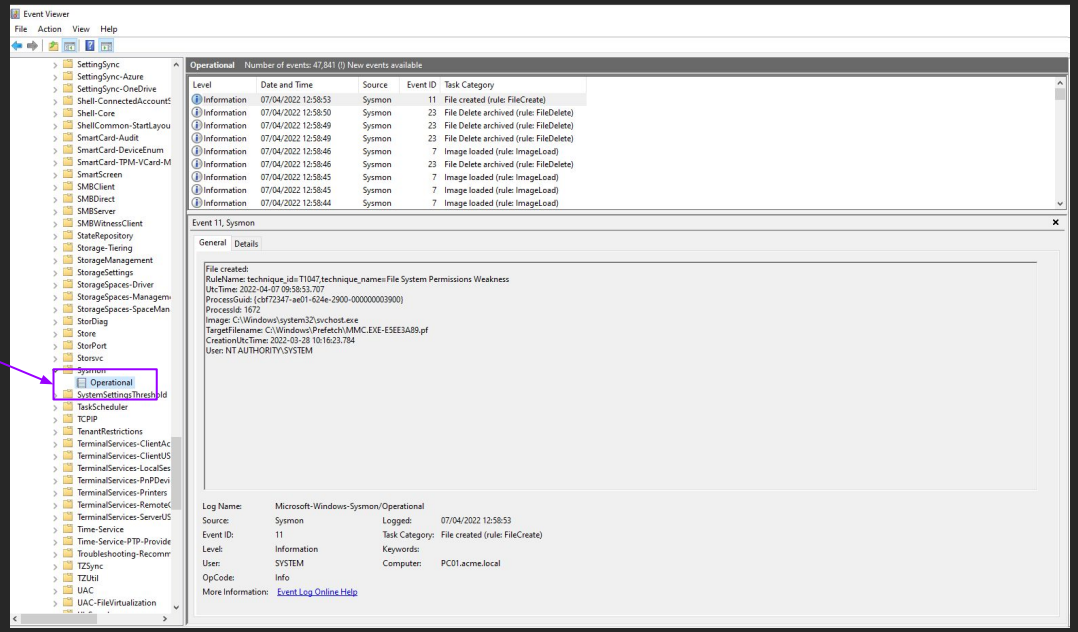
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd Z:\Tools\Sysmon\2022\
PS Z:\Tools\Sysmon\2022> .\Sysmon64.exe -i .\modular.xml -accepteula


System Monitor v13.33 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.60
Sysmon schema version: 4.81
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS Z:\Tools\Sysmon\2022>
```

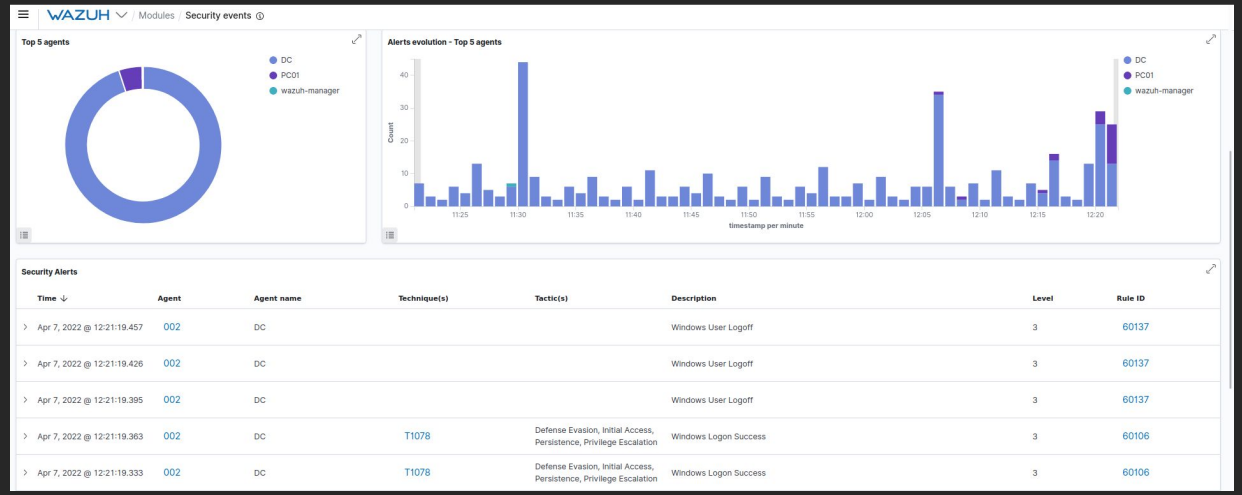
LOGGING VIA SYSMON

SYSMON INSTALLATION

Sysmon logs located here



WAZUH



Wazuh is used **to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats and behavioral anomalies**

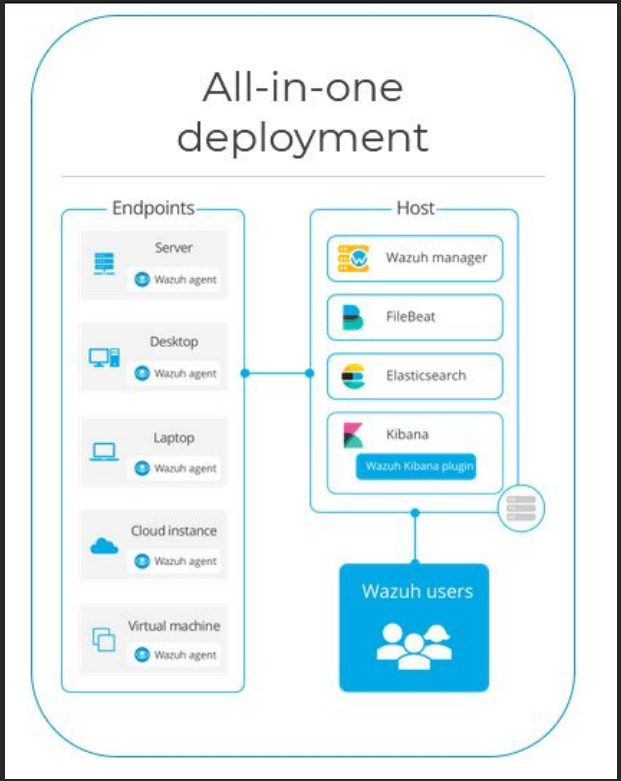
WAZUH

WAZUH

Wazuh is a component that goes on top of the ELK stack (Elasticsearch, Logstash and Kibana) which is a suite of tools that is used to enrich various types of data through analytics including security events thereby functioning like a SIEM.

The Wazuh agent is a single, light-weight monitoring software that runs on most operating systems and provides visibility into the endpoint's security by collecting critical system and application records, inventory data, and detecting potential anomalies.

https://documentation.wazuh.com/current/installation-guide/index.html

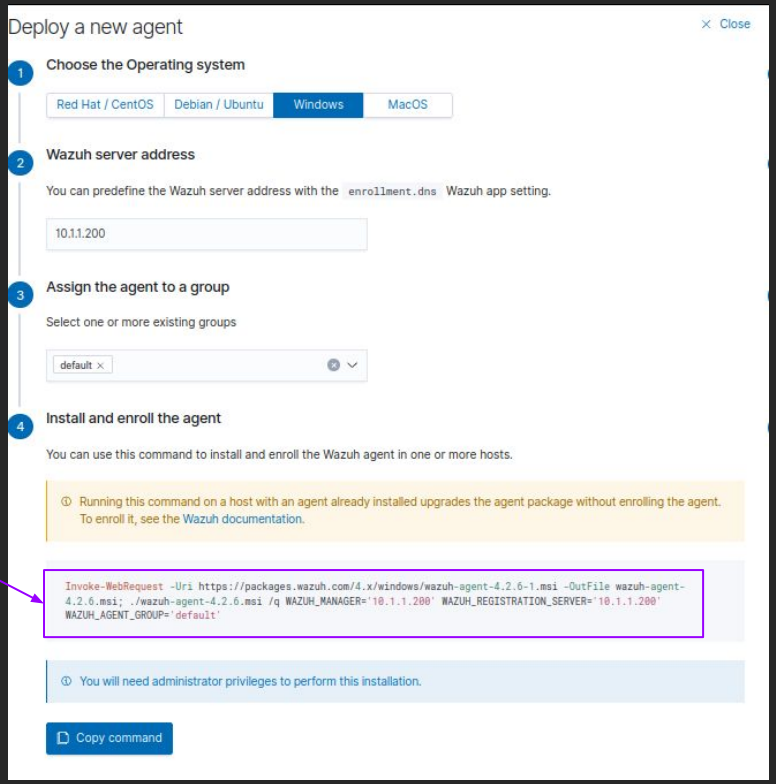


Download Wazuh Virtual Appliance

WAZUH

WAZUH AGENT INSTALLATION

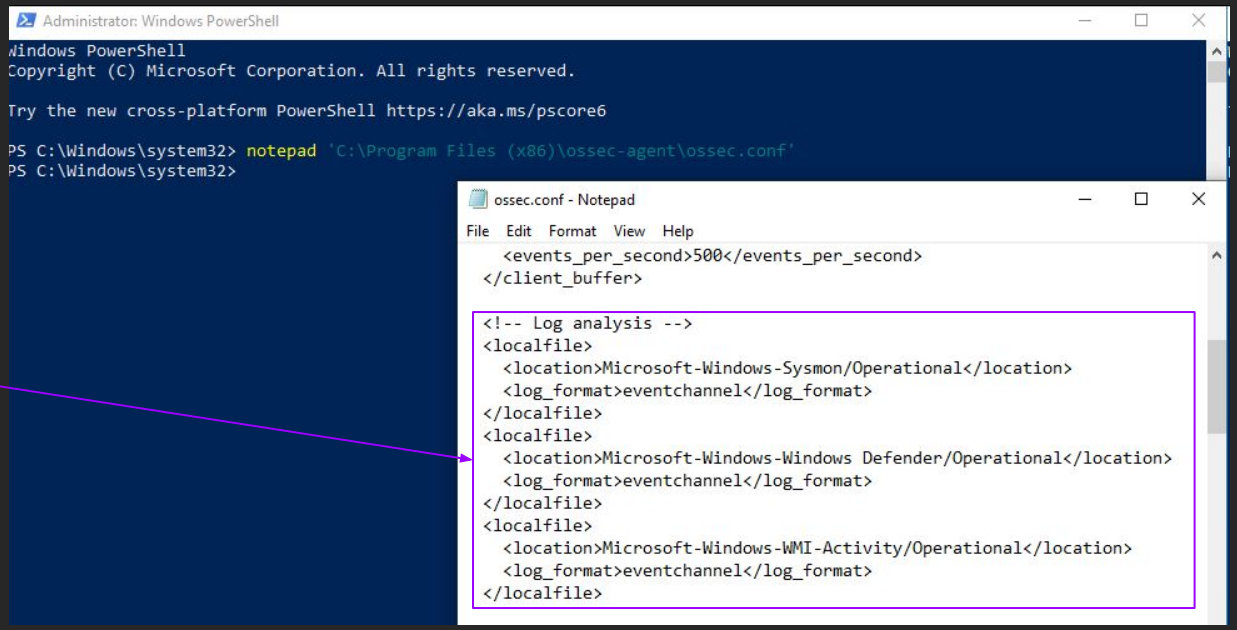
Deploying the Wazuh agent using Powershell script



WAZUH

WAZUH AGENT INSTALLATION

Modifying the **ossec.conf** file to collect logs from Sysmon and Windows Defender



Windows Agent Config

WAZUH

WAZUH RULES CONFIGURATION

Sample rule modified in the **local_rules.xml** file to alert on particular MITRE TTPs

WAZUH / Management / Rules

local_rules.xml

```xml
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015-2020, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>

<group name="sysmon-modular,">


  <rule id="255500" level="5">
  <if_group>sysmon_event8</if_group>
  <match>technique_name=Process Injection</match>
  <description>MITRE T1055 Process Injection: $(win.eventdata.image)</description>
  <group>MITRE,attack.t1055,</group>
  </rule>

  <rule id="255501" level="5">
  <if_group>sysmon_event1</if_group>
  <match>technique_name=Masquerading</match>
  <description>MITRE T1036 Masquerading: $(win.eventdata.image)</description>
  <group>MITRE,attack.t1036,</group>
```

Download Wazuh local_rules.xml

PROCEDURE LEVEL INTEL

Sample MITRE ATT&CK mapped TTPs from a DFIR report on a recent campaign by the Conti Ransomware group.

https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/

```
T1614.001 - System Location Discovery: System Language Discovery
T1218.010 - Signed Binary Proxy Execution: Regsvr32
T1218.011 - Signed Binary Proxy Execution: Rundll32
T1059.001 - Command and Scripting Interpreter: PowerShell
T1055 - Process Injection
T1003.001 - OS Credential Dumping: LSASS Memory
T1486 - Data Encrypted for Impact
T1482 - Domain Trust Discovery
T1021.002 - Remote Services: SMB/Windows Admin Shares
T1219 - Remote Access Software
T1083 - File and Directory Discovery
T1562.001 - Impair Defenses: Disable or Modify Tools
T1518.001 - Software Discovery: Security Software Discovery
T1047 - Windows Management Instrumentation
T1087.002 - Account Discovery: Domain Account
T1068 - Exploitation for Privilege Escalation
T1082 - System Information Discovery
T1018 - Remote System Discovery
T1053.005 - Scheduled Task/Job: Scheduled Task
T1569.002 - Service Execution
T1071.001 Web Protocols

S0552 - AdFind
S0154 - Cobalt Strike
S0097 - Ping
```

PURPLE TEAM EXERCISE TOOLS

Atomic Red Team

Infection Monkey

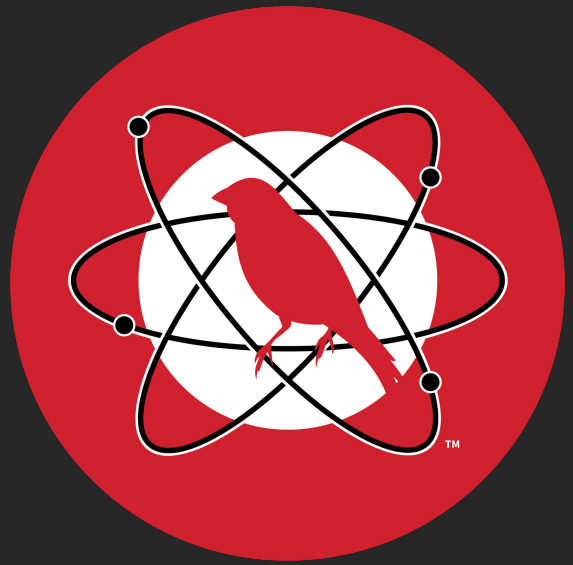
CALDERA

Scythe

APT Simulator

AttackIQ

ATOMIC RED TEAM



Atomic Red Team is library of tests mapped to the MITRE ATT&CK framework. Security teams can use Atomic Red Team to quickly, portably, and reproducibly test their environments.

https://github.com/redcanaryco/atomic-red-team

ATOMIC RED TEAM

ATOMIC RED TEAM FRAMEWORK INSTALLATION

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> powershell -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atom
icredteam.ps1' -UseBasicParsing);
PS C:\Windows\system32>
PS C:\Windows\system32> Install-AtomicRedTeam -getAtomics -Force
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
PS C:\Windows\system32>
```

ATOMIC RED TEAM

USING ATOMIC RED TEAM FRAMEWORK

```
PS C:\Windows\system32>
PS C:\Windows\system32> Install-AtomicRedTeam -getAtomics -Force
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest function
See Wiki at https://github.com/redcanaryco/invoke-atomicredteam/wiki for complete details
PS C:\Windows\system32>
PS C:\Windows\system32> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
PS C:\Windows\system32>
PS C:\Windows\system32>
```

ATOMIC RED TEAM

USING ATOMIC RED TEAM FRAMEWORK

The **-ShowDetailsBrief** tag shows brief information on the selected Tactic and the various Procedures that will be tested.

```
PS C:\Windows\system32> Invoke-AtomicTest T1003.001 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003.001-1 Dump LSASS.exe Memory using ProcDump
T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
T1003.001-4 Dump LSASS.exe Memory using NanoDump
T1003.001-6 Offline Credential Theft With Mimikatz
T1003.001-7 LSASS read with pypykatz
T1003.001-8 Dump LSASS.exe Memory using Out-Minidump.ps1
T1003.001-9 Create Mini Dump of LSASS.exe using ProcDump
T1003.001-10 Powershell Mimikatz
T1003.001-11 Dump LSASS with .Net 5 createdump.exe
T1003.001-12 Dump LSASS.exe using imported Microsoft DLLs
PS C:\Windows\system32>
```

ATOMIC RED TEAM

USING ATOMIC RED TEAM FRAMEWORK

```
PS C:\Windows\system32> Invoke-AtomicTest T1003.001-1 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Prerequisites not met: T1003.001-1 Dump LSASS.exe Memory using ProcDump
        [*] ProcDump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001
\bin\procdump.exe)

Try installing prereq's with the -GetPrereqs switch
PS C:\Windows\system32>
```

The **-CheckPrereqs** tag checks if all the prerequisites are in place on the system to run that particular Atomic Test. If they are not satisfied it will give the command to install them.

ATOMIC RED TEAM

USING ATOMIC RED TEAM FRAMEWORK

```
PS C:\Windows\system32> Invoke-AtomicTest T1003.001-1 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Attempting to satisfy prereq: ProcDump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam
\atomics\T1003.001\bin\procdump.exe)
Prereq successfully met: ProcDump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atom
ics\T1003.001\bin\procdump.exe)
PS C:\Windows\system32>
```

The **-GetPrereqs** tag will install any missing components for the particular Atomic Test to be ran.

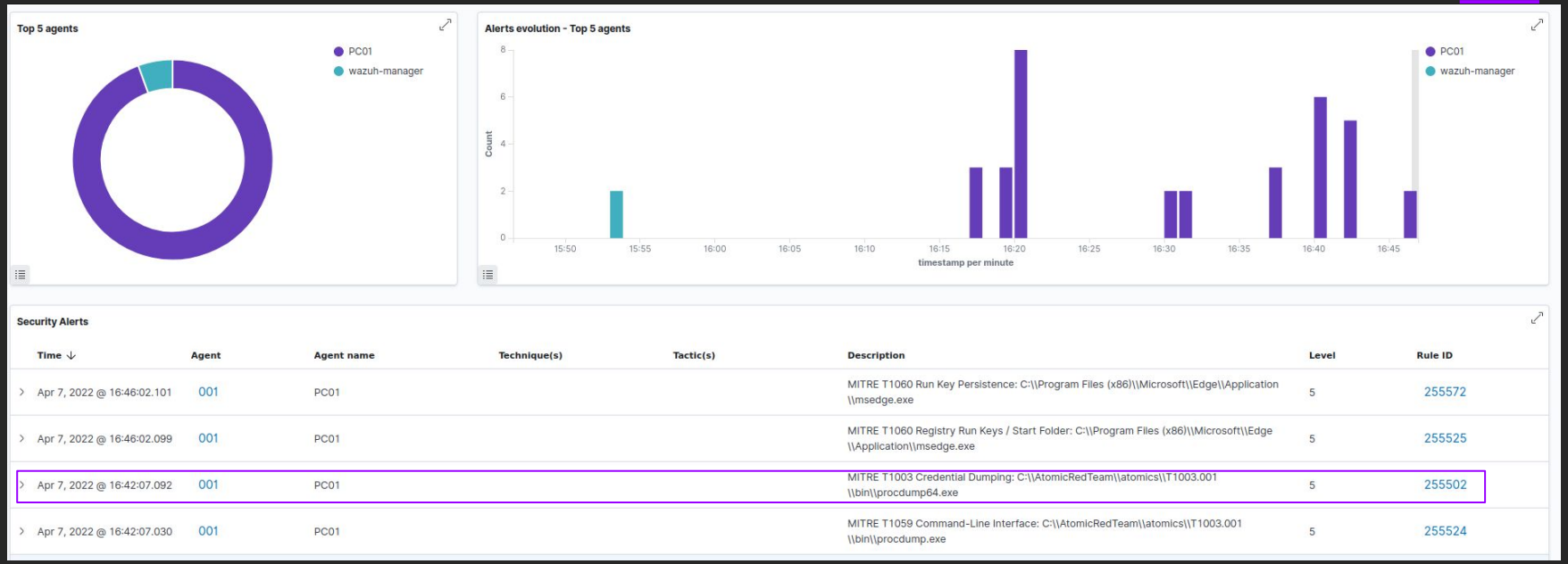
ATOMIC RED TEAM

USING ATOMIC RED TEAM FRAMEWORK

Running the Atomic Test and output showing successful running of the Procedure.

```
PS C:\Windows\system32> Invoke-AtomicTest T1003.001-1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1003.001-1 Dump LSASS.exe Memory using ProcDump
ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com
[16:42:07] Dump 1 initiated: C:\Windows\Temp\lsass_dump.dmp
[16:42:07] Dump 1 writing: Estimated dump file size is 54 MB.
[16:42:08] Dump 1 complete: 54 MB written in 0.7 seconds
[16:42:08] Dump count reached.
Done executing test: T1003.001-1 Dump LSASS.exe Memory using ProcDump
```

ATOMIC RED TEAM



Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 7, 2022 @ 16:46:02.101	001	PC01			MITRE T1060 Run Key Persistence: C:\\Program Files (x86)\\Microsoft\\Edge\\Application \\msedge.exe	5	255572
Apr 7, 2022 @ 16:46:02.099	001	PC01			MITRE T1060 Registry Run Keys / Start Folder: C:\\Program Files (x86)\\Microsoft\\Edge \\Application\\msedge.exe	5	255525
Apr 7, 2022 @ 16:42:07.092	001	PC01			MITRE T1003 Credential Dumping: C:\\AtomicRedTeam\\atomics\\T1003.001 \\bin\\procdump64.exe	5	255502
Apr 7, 2022 @ 16:42:07.030	001	PC01			MITRE T1059 Command-Line Interface: C:\\AtomicRedTeam\\atomics\\T1003.001 \\bin\\procdump.exe	5	255524

The test creates an alert on the Wazuh dashboard.

ATOMIC RED TEAM

USING ATOMIC RED TEAM FRAMEWORK

```
PS C:\Windows\system32> Invoke-AtomicTest T1003.001-1 -Cleanup
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing cleanup for test: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Done executing cleanup for test: T1003.001-1 Dump LSASS.exe Memory using ProcDump
```

The **-Cleanup** tag allows us to revert any changes done on the system when the Atomic Test was ran.

macrosec

SecureData TECHNOLOGIES

DEMO

REFERENCES & RESOURCES

- https://documentation.wazuh.com/current/index.html
- https://documentation.wazuh.com/current/virtual-machine/virtual-machine.html
- https://wazuh.com/blog/emulation-of-attck-techniques-and-detection-with-wazuh/
- https://documentation.wazuh.com/current/user-manual/manager/manual-email-report/smtp-authentication.html
- https://wazuh.com/blog/how-to-send-email-notifications-with-wazuh/
- https://raw.githubusercontent.com/Hestat/ossec-sysmon/master/local_rules.xml
- https://raw.githubusercontent.com/Hestat/ossec-sysmon/master/windows-agent.conf
- https://github.com/redcanaryco/atomic-red-team
- https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain
- http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- https://www.scythe.io/library/summiting-the-pyramid-of-pain-the-ttp-pyramid
- https://blog.nviso.eu/2020/01/23/thoughts-on-red-team-nomenclature/