SOC LEVEL 1

Contents:

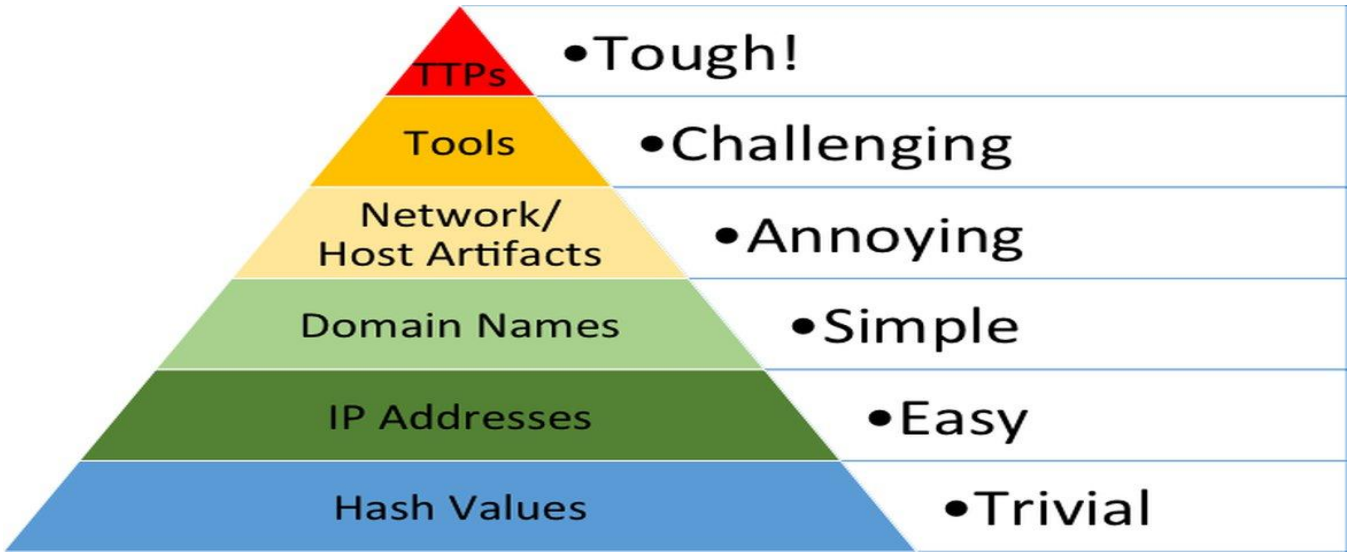
Chapter 1: Cyber Defence Frameworks

1.1 Introduction

The responsibilities for a Junior Security Analyst or Tier 1 SOC Analyst include:

- Monitor and investigate the alerts (most of the time, it's a 24x7 SOC operations environment)
- Configure and manage the security tools
- Develop and implement basic IDS (Intrusion Detection System) signatures
- Participate in SOC working groups, meetings
- Create tickets and escalate the security incidents to the Tier 2 and Team Lead if needed

1.2 Pyramid of pain



[1] Hash Values

- The hash value is a numeric value of a fixed length that uniquely identifies data.
- Types:
  - MD5
  - SHA-1
  - SHA-256
- Security professionals usually use the hash values to gain insight into a specific malware sample
- Attacker can modify a file by even a single bit, which would produce a different hash value.

[2] IP Address

- IP address is used to identify any device connected to a network.

- A common defence tactic is to block, drop, or deny inbound requests from IP addresses on your parameter or external firewall.
- One of the ways an adversary can make it challenging to successfully carry out IP blocking is by using Fast Flux.

DNS Fast Flux:

- It is a DNS technique used by botnets to hide phishing, web proxying, malware delivery, and malware communication activities behind compromised hosts acting as proxies.
- The purpose of using the Fast Flux network is to make the communication between malware and its command and control server (C&C) challenging to be discovered by security professionals.

[3] Domain Name

- Domain Names can be thought as simply mapping an IP address to a string of text.

Domain Names can be a little more of a pain for the attacker to change as they would most likely need to purchase the domain, register it and modify DNS records.

Punny Code:

- Punycode is a way of converting words that cannot be written in ASCII, into a Unicode ASCII encoding
- Example:
  - adıdas.de ➔ http://xn--addas-o4a.de/

Shortened Link:

- Attackers usually hide the malicious domains under URL Shorteners.
- Example:
  - bit.ly
  - tinyurl.com
- You can see the actual web site by appending + or use URL scan

[4] Host Artifacts

- Host artifacts are the traces or observables that attackers leave on the system, such as
  - registry values
  - suspicious process execution
  - IOCs
  - files dropped by malicious applications

[5] Network Artifacts

- Network artifacts can be detected in Wireshark PCAPs by using a network protocol analyser

- Example
  - If you can detect the custom User-Agent strings that the attacker is using, you might be able to block them

[6] Tools

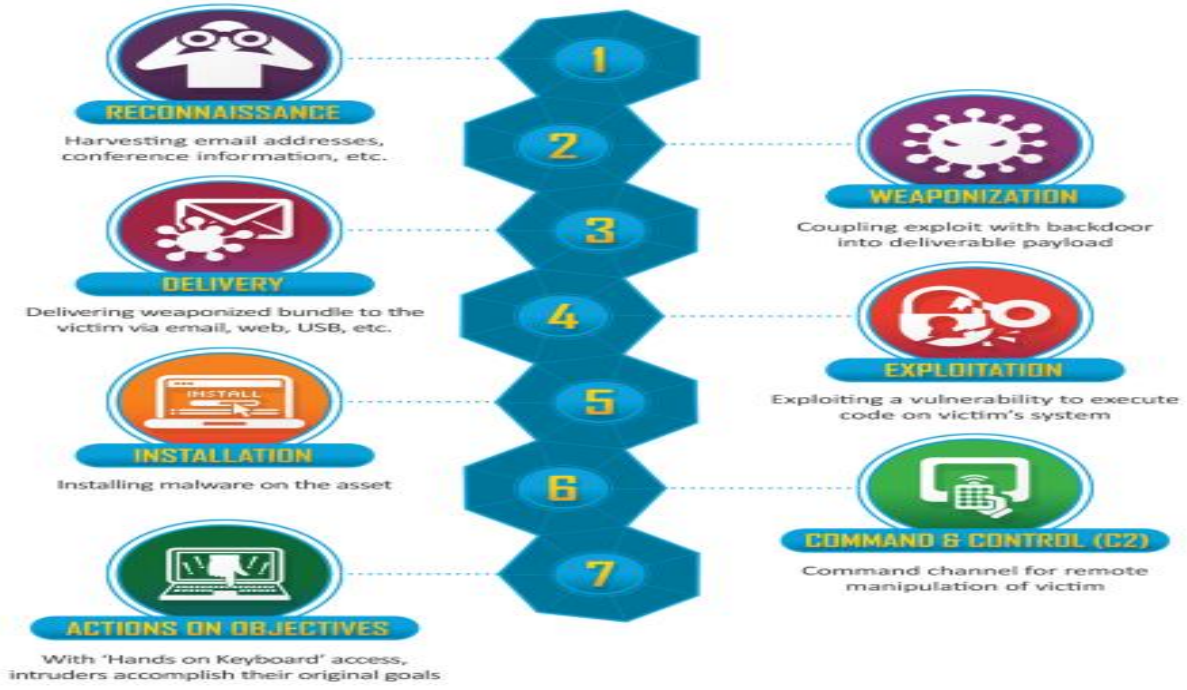
- Attackers would use the utilities to create malicious macro documents (maldocs) for spearphishing attempts, a backdoor that can be used to establish C2 (Command and Control Infrastructure), any custom .EXE, and .DLL files, payloads, or password crackers.
- Antivirus signatures, detection rules, and YARA rules can be great weapons for you to use against attackers at this stage.
- [MalwareBazaar and Malshare] are good resources to provide you with access to the samples, malicious feeds, and YARA results

[7] TTPs

- TTPs stands for Tactics, Techniques & Procedures.
  - The Tactic is the adversary's goal or objective.
  - The Technique is how the adversary achieves the goal or objective.
  - The Procedure is how the technique is executed.
- This includes the whole MITRE ATT&CK Matrix, which means all the steps taken by an adversary to achieve his goal, starting from phishing attempts to persistence and data exfiltration.

1.3 Cyber Kill Chain

The Cyber Kill Chain will help you understand and protect against ransomware attacks, security breaches as well as Advanced Persistent Threats (APTs).



[1] Reconnaissance

- It is discovering and collecting information on the system and the victim.

[2] Weaponization

- Most attackers usually use automated tools to generate the malware or refer to the DarkWeb to purchase the malware
- More sophisticated actors or nation-sponsored APT (Advanced Persistent Threat Groups) would write their custom malware to make the malware sample unique and evade detection on the target.

[3] Delivery

- By choosing the method for transmitting the payload or the malware.
- Examples:
  - Phishing Emails
  - Infected USB
  - Watering hole attack

[4] Exploitation

- To gain access to the system, an attacker needs to exploit the vulnerability.
- After gaining access to the system, the malicious actor could exploit software, system, or server-based vulnerabilities to escalate the privileges or move laterally through the network.

[5] Installation

- Once the attacker gets access to the system, he would want to reaccess the system if he loses the connection to it or if he got detected and got the initial access removed, or if the system is later patched. He will no longer have access to it.
- Persistence can be achieved through
  - Installing a web shell on the webserver.
  - Installing a backdoor on the victim's machine
  - Creating or modifying Windows services.
  - Adding the entry to the "run keys" for the malicious payload in the Registry or the Startup Folder.

[6] Command and Control (C2)

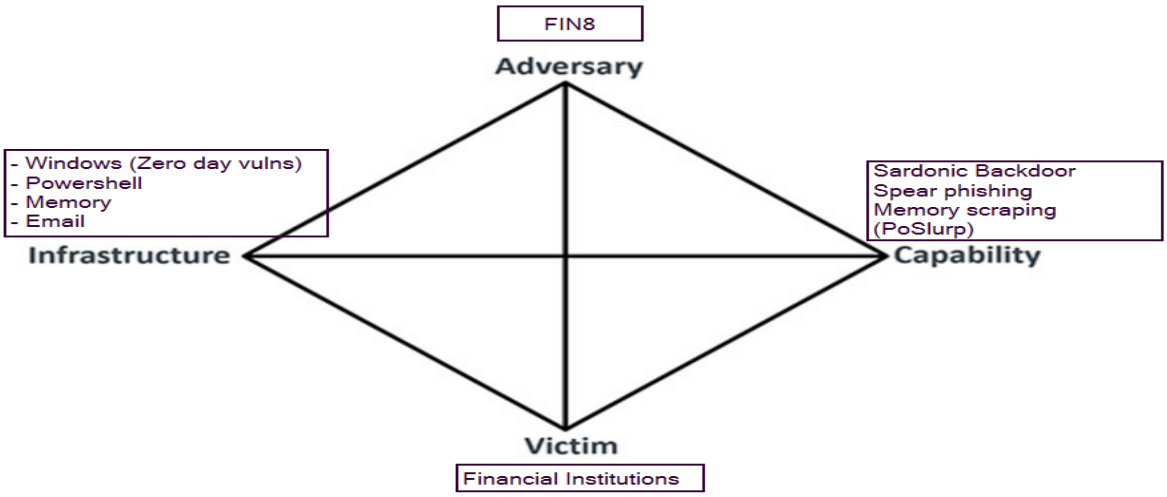
- Attacker opens up the C2 (Command and Control) channel through the malware to remotely control and manipulate the victim.
- The most common C2 channels used by adversaries nowadays:
  - The protocols HTTP on port 80 and HTTPS on port 443
  - DNS (Domain Name Server).

[7] Actions on Objectives (Exfiltration)

- Finally, attacker can achieve his goa by
  - Collect the credentials from users.
  - Internal reconnaissance
  - Collect and exfiltrate sensitive data.

1.4 Diamond Model

The Diamond Model is composed of four core features: adversary, infrastructure, capability, and victim, and establishes the fundamental atomic element of any intrusion activity.



[1] Adversary

- An adversary is also known as an attacker, enemy, cyber threat actor, or hacker.

[2] Victim

- It is a target of the adversary
- Victim Personae are the people and organizations being targeted and whose assets are being attacked and exploited.
- Victim Assets are the attack surface and include the set of systems, networks, email addresses, hosts, IP addresses, social networking accounts, etc., to which the adversary will direct their capabilities.

[3] Capability

- It is also known as the skill, tools, and techniques used by the adversary in the event.
- Capability Capacity is all of the vulnerabilities and exposures that the individual capability can use.
- An Adversary Arsenal is a set of capabilities that belong to an adversary.

[4] Infrastructure

- It is also known as software or hardware.
- Infrastructure is the physical or logical interconnections that the adversary uses to deliver a capability or maintain control of capabilities.
- It has 2 types
  - Type 1 Infrastructure is the infrastructure controlled or owned by the adversary.
  - Type 2 Infrastructure: is the infrastructure controlled by an intermediary.

1.5 MITRE

- MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

- MITRE began to address the need to record and document common TTPs (Tactics, Techniques, and Procedures) that APT (Advanced Persistent Threat) groups used against enterprise Windows networks.

Chapter 2: Cyber Threat Intelligence

2.1 Introduction

- CTI is vital for investigating and reporting against adversary attacks with organisational stakeholders and external communities.
- The primary goal of CTI is to understand the relationship between your operational environment and your adversary and how to defend environment against any attacks.
- You would seek this goal by developing your cyber threat context by trying to answer the following questions:
  - Who's attacking you?
  - What are their motivations?
  - What are their capabilities?
  - What artefacts and indicators of compromise (IOCs) should you look out for?
- CTI Standards & Frameworks
  - MITRE Attack
  - TAXII
  - STIX
  - Cyber Kill Chain
  - Diamond Model

2.2 Tools & Websites

- URL scan
- Abuse.ch
- Phishtool
- VirusTotall
- X-Force
- AbuseIPDB
- MXtoolbox
- Cisco Talos Intelligence

2.3 YARA

- Yara can identify information based on both binary and textual patterns, such as hexadecimal and strings contained within a file.
- Rules are used to label these patterns. For example, Yara rules are frequently written to determine if a file is malicious or not
- Every YARA command requires two arguments to be valid
  - Rule
  - File, directory or process ID to use the rule for

[1] Rule

- Every rule requires both a name and a condition to be valid
- You can use strings to search for specific text or hexadecimal in files or programs.

- you can use desc, short for description, to summarise what your rule checks for.
- Example:

```
rule helloworldmatching{
        strings:
        $hello_world = “Hello World!”
        $hello_world_lowercase = "hello world"
        $hello_world_uppercase = "HELLO WORLD"

        condition:
        any of them
}
```

[2] Modules

- Cuckoo
  - This module allows you to generate Yara rules based upon the behaviours discovered from Cuckoo Sandbox
- Python PE
  - Python's PE module allows you to create Yara rules from the various sections and elements of the Windows Portable Executable (PE) structure

[3] Tools

- You don't have to create many rules from scratch to begin using Yara to search for evil.
- There are plenty of GitHub resources and open-source tools
  - LOKI
  - THOR
  - YAYA

2.4 Open CTI

- OpenCTI is another open-sourced platform designed to provide organisations with the means to manage CTI through the storage, analysis, visualisation and presentation of threat campaigns, malware and IOCs.

2.5 MISP

- Stands for MALWARE INFORMATION SHARING PLATFORM
- It is an open-source threat information platform that facilitates the collection, storage and distribution of threat intelligence
- It is used for:
  - Malware Reverse Engineering
  - Security Investigations
  - Intelligence Analysis

Chapter 3: Network Security and Traffic Analysis

3.1 Introduction

- The essential concern of Network Security focuses on two core concepts
  - Authentication
  - Authorization
- Network security operations contain three base control levels to ensure the maximum available security management
  - Physical
    - Physical security controls prevent unauthorised physical access to networking devices
  - Technical
    - Data security controls prevent unauthorised access to network data
  - Administrative
    - Administrative security controls provide consistency in security operations
- The main approaches and Elements
  - Access Control
    - Firewall
    - NAC (Network Access Control)
    - IAM (Identity and Access Management)
    - VPN
  - Threat Control
    - IDS/IPS
    - DLP
    - EDR
    - SIEM
    - SOAR
- Network Traffic Analysis using the following concepts and tools
  - Sniffing and packet analysis
    - Wireshark
  - Monitoring
    - Zeek
  - IDS/IPS
    - Snort
  - Network forensics
    - Miner
  - Threat Hunting
    - Brim

3.2 Wireshark

- It is commonly used as one of the best packet analysis tools.
- Use cases for using it
  - Detecting and troubleshooting network problems
  - Detecting security anomalies
  - Investigating and learning protocol details
- Sheet Cheat
  - https://cdn.comparitech.com/wp-content/uploads/2019/06/Wireshark-Cheat-Sheet-1.jpg.webp

3.3 Zeek

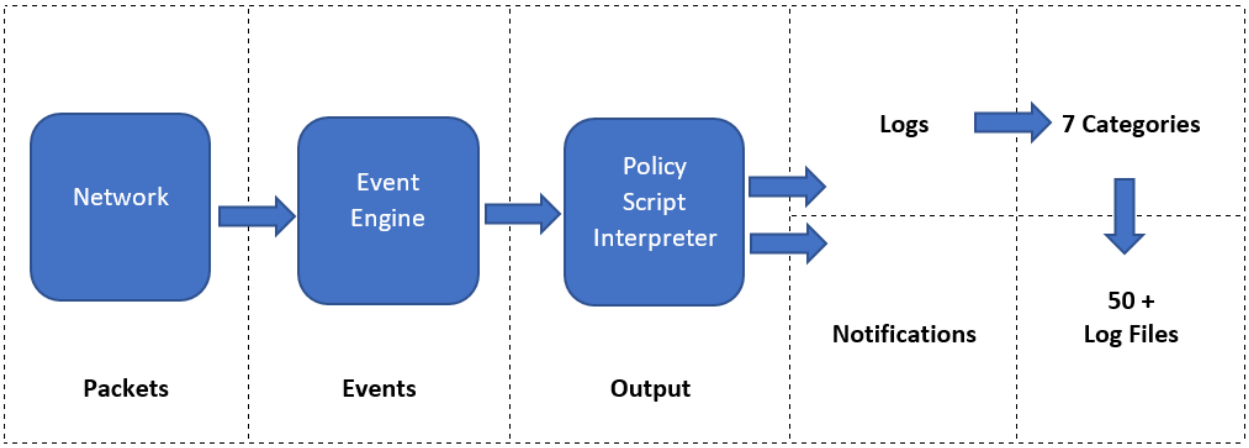
- Zeek (formerly Bro) is an open-source and network monitoring tool (traffic analyser).
- Zeek differs from known monitoring and IDS/IPS tools by providing a wide range of detailed logs ready to investigate both for forensics and data analysis actions.

[1] Network monitoring VS network security monitoring

1. Network monitoring
   - It is highly focused on IT assets like uptime (availability), device health and connection quality (performance) and network traffic balance and management (configuration).

2. Network security monitoring
   - It is focused on network anomalies like rogue hosts, encrypted traffic, suspicious service and port usage, and malicious/suspicious traffic patterns in an intrusion/anomaly detection and response approach.

[2] Zeek Architecture



[3] Zeek Frameworks

- Zeek has several frameworks to provide extended functionality in the scripting layer.

[4] Zeek output

- The default log path is:/opt/zeek/logs/
- Zeek provides 50+ log files under seven different categories and categorising them into seven categories.
    - Network
        - Network protocol logs.
    - Files
        - File analysis result logs.
    - NetControl
        - Network control and flow logs.
    - Detection
        - Detection and possible indicator logs.
    - Network Observations
        - Network flow logs.
    - Miscellaneous
        - Additional logs cover external alerts, inputs and failures.
    - Zeek Diagnostic
        - Zeek diagnostic logs cover system messages, actions and some statistics.

[5] Zeek Signature

- once the match occurs, Zeek will generate an alert and create additional log files (signatures.log and notice.log).
- How to use?
    - Zeek -C -r {PCAP_File} -s {SIG_File}

[6] Zeek Scripts

- Zeek has its own event-driven scripting language, which is as powerful as high-level languages and allows us to investigate and correlate the detected events.
- Zeek scripts use the ".zeek" extension.
- Scripts Location
    - Zeek has base scripts installed by default
        - in "/opt/zeek/share/zeek/base"
    - User-generated or modified scripts
        - in "/opt/zeek/share/zeek/site"
    - Policy scripts

- in "/opt/zeek/share/zeek/policy"
- You can also use a script for a single run, just like the signatures.
  - in "/opt/zeek/share/zeek/site/local.zeek"

3.4 Snort

- SNORT is an open-source, rule-based Network Intrusion Detection and Prevention System (NIDS/NIPS).
- Snort has three main use models
  1. Sniffer mode
  2. Packet Logger mode
  3. NIDS and NIPS modes

[1] How to use Snort?

1. Test

- snort -c /etc/snort/snort.conf -T

Parameter	Description
-c	Identifying the configuration file
-T	Snort's self-test parameter, you can test your setup with this parameter.

2. Sniffer Mode

Parameter	Description
-v	Verbose. Display the TCP/IP output in the console.
-d	Display the packet data (payload).
-e	Display the link-layer (TCP/IP/UDP/ICMP) headers.
-x	Display the full packet details in HEX.
-i	This parameter helps to define a specific network interface to listen/sniff.

3. Packet Logger

Parameter	Description
-l	Identifying the configuration file
-k ASCII	Snort's self-test parameter, you can test your setup with this parameter.
-r	Reading option, read the dumped logs in Snort.
-n	Specify the number of packets that will process/read. Snort will stop after reading the specified number o

4. IDS/IPS Mode

Parameter	Description
-c	Defining the configuration file.
-T	Testing the configuration file.
-N	Disable logging.
-D	Background mode
-A	Alert modes 1. full: Full alert mode, providing all possible information about the alert. 2. fast: Fast mode shows the alert message, timestamp, source and destination IP, along with port numbers. 3. console: Provides fast style alerts on the console screen. 4. cmg: CMG style, basic header details with payload in hex and text format. 5. none: Disabling alerting.

[2] Snort Rule structure

1. Header
2. Option
   - Action Protocol SRC_IP SRC_port Direction DST_IP DST_Port (options)
     - Action:
       - Alert
       - Log
       - Drop
       - Reject
     - Direction
       - Inbound
       - Outbound
     - Options
       - MSG; Message when action happen
       - Content;
       - Sid;
       - Reference;
       - Rev;

3.5 Miner

- NetworkMiner is an open-source traffic sniffer, pcap handler and protocol analyser.
- NetworkMiner is an open source Network Forensic Analysis Tool for Windows

[1] Network Forensics

- It is a specific subdomain of the Forensics domain, and it focuses on network traffic investigation.
- The investigation tries to answer the 5W:
  - Who (Source IP, Port)
  - What (Data/Payload)
  - Where (Destination IP and Port)
  - When (Time and Data)
  - Why (How/What happened)
- Use Cases:
  - Network discovery
  - Packets reassembling
  - Data leakage detection
  - Anomaly and malicious activity detection
  - Policy/Regulation compliance control

3.6 Brim

- Brim is an open-source desktop application that processes pcap files and logs files, with a primary focus on providing search and analytics.
- It also supports Zeek signatures and Suricata Rules for detection.
- Brim reduces the time and effort spent processing pcap files and investigating the log files by providing a simple and powerful GUI application.
- It can handle two types of data as an input:
  1. Packet Capture Files: Pcap files
  2. Log Files: Log files of Zeek

[1] Custom Queries and its use cases

1. Communicated Hosts
   - Query: _path=="conn" | cut id.orig_h, id.resp_h | sort | uniq
2. Frequently Communicated Hosts
   - Query: _path=="conn" | cut id.orig_h, id.resp_h | sort | uniq -c | sort -r
3. Most Active Ports
   - Query: _path=="conn" | cut id.resp_p, service | sort | uniq -c | sort -r count
   - Query: _path=="conn" | cut id.orig_h, id.resp_h, id.resp_p, service | sort id.resp_p | uniq -c | sort -r
4. Long Connections

- Query: _path=="conn" | cut id.orig_h, id.resp_p, id.resp_h, duration | sort -r duration

5. Transferred Data
    - Query: _path=="conn" | put total_bytes := orig_bytes + resp_bytes | sort -r total_bytes | cut uid, id, orig_bytes, resp_bytes, total_bytes
6. DNS and HTTP Queries
    - Query: _path=="dns" | count () by query | sort -r
    - Query: _path=="http" | count () by uri | sort -r
7. Suspicious Hostnames
    - Query: _path=="dhcp" | cut host_name, domain
8. Suspicious IP Addresses
    - Query: _path=="conn" | put classnet := network_of(id.resp_h) | cut classnet | count() by classnet | sort -r
9. Detect Files
    - Query: filename!=null
10. SMB Activity
    - Query: _path=="dce_rpc" OR _path=="smb_mapping" OR _path=="smb_files"
11. Known Patterns
    - Query: event_type=="alert" or _path=="notice" or _path=="signatures"

Chapter 4: Endpoint Security Monitoring

4.1 Introduction

- Main concepts will be:

1. Endpoint Security
    - Core windows Processes
    - Task Manager
    - Sysinternals
2. Endpoint Logging and monitoring
    - Windows Event Logs
    - Sysmon
    - OSQuery
    - Wazuh
3. Endpoint Log analysis
    - Event Correlation
    - Baselining

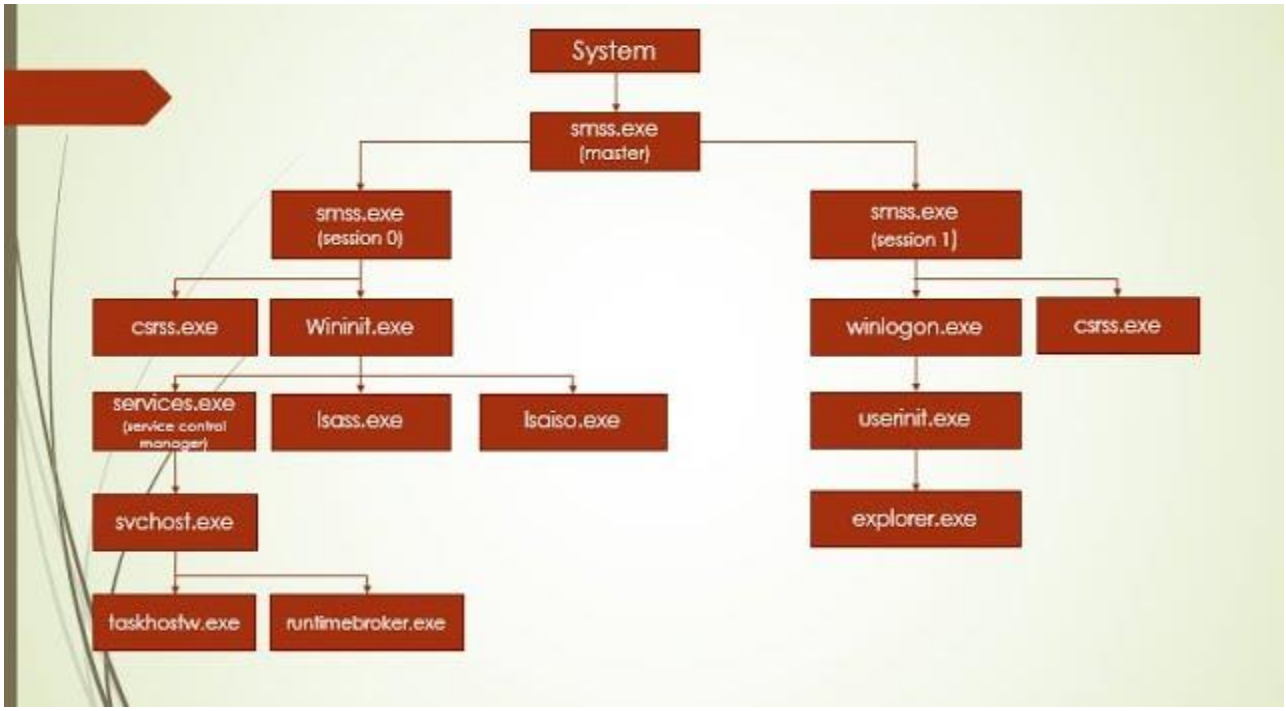
- Task Manager

1. It is a built-in GUI-based Windows utility that allows users to see what is running on the Windows system.
2. It also provides information on resource usage, such as how much each process utilizes CPU and memory.
3. A Task Manager provides some of the Core Windows Processes running in the background.

- More powerful applications that helps in looking at process and the parent-child relationship are

1. Process Hacker
2. Process Explorer
3. CMD
    - Tasklist
    - get-process
    - PowerShell
    - wmic

4.2 Core Windows Processes



[1] System

- The first Windows process on the list.
- The PID for System is always 4
- Parent Process: System Idle Process (0

What is unusual behaviour for this process?

1. A parent process (aside from System Idle Process (0))
2. Multiple instances of System. (Should only be one instance)
3. A different PID. (Remember that the PID will always be PID 4)
4. Not running in Session 0

---

[2] smss.exe

- Stands for Session Manager subsystem (Windows Session Manager)
- It is responsible for creating new sessions.
- It is the first user-mode process started by the kernel.

What is unusual behaviour for this process?

1. A different parent process other than System (4)
2. The image path is different from C:\Windows\System32

3. More than one running process. (children self-terminate and exit after each new session)
4. The running User is not the SYSTEM user
5. Unexpected registry entries for Subsystem

---

[3] csrss.exe

- Stands for Client Server Runtime Process
- This process is always running and is critical to system operation.
- This process is responsible for the Win32 console window and process thread creation and deletion.
- This process is also responsible for making the Windows API available to other processes, mapping drive letters, and handling the Windows shutdown process.
- Parent Process: Created by an instance of smss.exe
- This process is spawned by smss.exe, which self-terminates itself.

What is unusual behaviour for this process?

1. An actual parent process. (smss.exe calls this process and self-terminates)
2. Image file path other than C:\Windows\System32
3. Subtle misspellings to hide rogue processes masquerading as csrss.exe in plainsight
4. The user is not the SYSTEM user.

---

[4] Wininit.exe

- Stands for Windows Initialization Process
- It is responsible for launching in session 0
    1. services.exe (Service Control Manager)
    2. lsass.exe (Local Security Authority)
    3. lsaiso.exe
- It is another critical Windows process that runs in the background, along with its child processes.
- Parent Process: Created by an instance of smss.exe

What is unusual behaviour for this process?

1. An actual parent process. (smss.exe calls this process and self-terminates)
2. Image file path other than C:\Windows\System32
3. Subtle misspellings to hide rogue processes in plain sight
4. Multiple running instances
5. Not running as SYSTEM

[5] services.exe

- Stands for Service Control Manager
- Its primary responsibility is to handle system services: loading services, interacting with services and starting or ending services.
- Information regarding services is stored in the registry, HKLM\System\CurrentControlSet\Services.
- When a user logs into a machine successfully, this process is responsible for setting the value of the Last Known Good control set (Last Known Good Configuration), HKLM\System\Select\LastKnownGood, to that of the CurrentControlSet.
- This process is the parent to several other key processes
    1. svchost.exe,
    2. spoolsv.exe
    3. msmpeng.exe
    4. dllhost.exe

What is unusual behaviour for this process?

1. A parent process other than wininit.exe
2. Image file path other than C:\Windows\System32
3. Subtle misspellings to hide rogue processes in plain sight
4. Multiple running instances
5. Not running as SYSTEM

---

[6] svchost.exe

- Stands for Service Host
- It is responsible for hosting and managing Windows services.
- Since svchost.exe will always have multiple running processes on any Windows system, this process has been a target for malicious use.
- Adversaries create malware to masquerade as this process and try to hide amongst the legitimate svchost.exe processes.
- They can name the malware svchost.exe or misspell it, Another tactic is to install/call a malicious service (DLL).

What is unusual behaviour for this process?

1. A parent process other than services.exe
2. Image file path other than C:\Windows\System32
3. Subtle misspellings to hide rogue processes in plain sight
4. The absence of the -k parameter

[7] lsass.exe

- Stands for Local Security Authority Subsystem Service
- It is responsible for enforcing the security policy on the system.
- It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens.
- It creates security tokens for SAM (Security Account Manager), AD (Active Directory), and NETLOGON.
- It uses authentication packages specified in HKLM\System\CurrentControlSet\Control\Lsa.
- Lsass.exe is another process adversaries target.
- Common tools such as mimikatz are used to dump credentials, or adversaries mimic this process to hide in plain sight.

What is unusual behaviour for this process?

1. A parent process other than wininit.exe
2. Image file path other than C:\Windows\System32
3. Subtle misspellings to hide rogue processes in plain sight
4. Multiple running instances
5. Not running as SYSTEM

---

[8] Winlogon.exe

- Stands for Windows Logon
- It is responsible for handling the Secure Attention Sequence (SAS)
- This process is also responsible for loading the user profile
- It is also responsible for locking the screen and running the user's screensaver

What is unusual behaviour for this process?

1. An actual parent process. (smss.exe calls this process and self-terminates)
2. Image file path other than C:\Windows\System32
3. Subtle misspellings to hide rogue processes in plain sight
4. Not running as SYSTEM
5. Shell value in the registry other than explorer.exe

[9] explorer.exe

- Stands for Windows Explorer
- This process gives the user access to their folders and files.
- It also provides functionality for other features, such as the Start Menu and Taskbar.
- How it works:
    1. The Winlogon process runs userinit.exe, which launches the value in
    2. Userinit.exe exits after spawning explorer.exe.

What is unusual behaviour for this process?

1. An actual parent process. (userinit.exe calls this process and exits)
2. Image file path other than C:\Windows
3. Running as an unknown user
4. Subtle misspellings to hide rogue processes in plain sight
5. Outbound TCP/IP connections

4.3 Sysinternals

- The Sysinternals tools is a compilation of over 70+ Windows-based tools.
- Each of the tools falls into one of the following categories:
    1. File and Disk Utilities
        - Sigcheck
        - Streams
        - SDelete
    2. Networking Utilities
        - TCPView
    3. Process Utilities
        - Autoruns
        - ProcDump
        - Process Explorer
        - Process Monitor
        - PsEXec
    4. Security Utilities
        - Sysmon
    5. System Information
        - WinObj
    6. Miscellaneous
        - BgInFo
        - RegJump
        - Strings

4.4 Windows Event Logs

- Event logs record events taking place in the execution of a system to provide an audit trail that can be used to understand the activity of the system and to diagnose problems.
- Event logs are crucial for troubleshooting any computer incident and help understand the situation and how to remediate the incident.

- Elements of a Windows Event Log:
  1. System Logs:
     - Records events associated with the Operating System segments.
     - They may include information about hardware changes, device drivers, system changes, and other activities related to the device.
  2. Security Logs:
     - Records events connected to logon and logoff activities on a device.
     - The system's audit policy specifies the events.
  3. Application Logs:
     - Records events related to applications installed on a system. The main pieces of information include application errors, events, and warnings.
  4. Directory Service Events:
     - Active Directory changes and activities are recorded in these logs, mainly on domain controllers.
  5. File Replication Service Events:
  6. DNS Event Logs:
     - DNS servers use these logs to record domain events and to map out
  7. Custom Logs:
     - Events are logged by applications that require custom data storage.
     - This allows applications to control the log size or attach other parameters, such as ACLs, for security purposes.

- There are three main ways of accessing these event logs within a Windows system:
  1. Event Viewer (GUI-based application)
  2. Wevtutil.exe (command-line tool)
  3. Get-WinEvent (PowerShell cmdlet)

  Important Event IDs
  - Service has shut down
    - 1100
  - Audit log was cleared
    - 1102
  - Security log is full
    - 1104
  - Event log automatically backup
    - 1105
  - Indicates when a new PowerShell host process has started.
    - 400
  - Failed attempt at logging
    - 4625
  - Successful attempt at logging
    - 4624

- Registry value modification
  - 4657
- Creation of a new process
  - 4688
- Attempt to access objects in the network.
  - 4663
- Failed Kerberos pre-authentication.
  - 4771

4.5 Sysmon

- Stands for System Monitoring
- It is a tool used to monitor and log events on Windows
- It provides detailed information about process creations, network connections, and changes to file creation time.
- Events within Sysmon are stored in Applications and Services Logs/Microsoft/Windows/Sysmon/Operational

  Important Event IDs
  - Event ID 1: Process Creation
    - This event will look for any processes that have been created.
  - Event ID 3: Network Connection
    - The network connection event will look for events that occur remotely.
  - Event ID 7: Image Loaded
    - This event will look for DLLs loaded by processes, which is useful when hunting for DLL Injection and DLL Hijacking attacks.
  - Event ID 8: CreateRemoteThread
    - will monitor for processes injecting code into other processes.
  - Event ID 11: File Created
    - when files are created or overwritten the endpoint.
  - Event ID 12 / 13 / 14: Registry Event
    - This event looks for changes or modifications to the registry.
  - Event ID 15: FileCreateStreamHash
    - This event will look for any files created in an alternate data stream.
    - This is a common technique used by adversaries to hide malware.
  - Event ID 22: DNS Event
    - This event will log all DNS queries and events for analysis.

How to hunt specific targets?

1. Metasploit
   - We will be hunting the meterpreter shell itself and the functionality it uses.
     - we will look for network connections that originate from suspicious ports such as 4444 and 5555
     - **NOTE:** By default, Metasploit uses port 4444.
2. Mimikatz
   - The first method of hunting for Mimikatz is just looking for files created with the name Mimikatz.
     - We can use the ProcessAccess event ID to hunt for abnormal LSASS (Local Security authority Subsystem service) behavior.
     - If LSASS is accessed by a process other than svchost.exe it should be considered suspicious behavior and should be investigated further
3. Presistence
   - We can hunt persistence with Sysmon by looking for File Creation events as well as Registry Modification events.
     - We will first be looking at the SwiftOnSecurity detections for a file being placed in the \Startup\ or \Start Menu directories.
     - We will again be looking at another SwiftOnSecurity detection this time for a registry modification that adjusts that places a script inside CurrentVersion\Windows\Run and other registry locations.

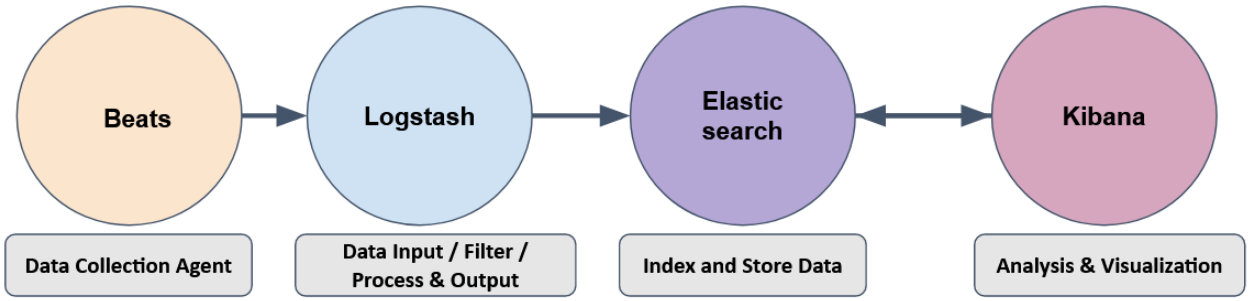
Chapter 5: Security Information and Event Management

5.1 Introduction

- Stands for Security Information and Event Management
- It is a tool that collects data from various endpoints/network devices across the network, stores them at a centralized place and performs correlation on them.
- We can collect logs and events from different multiple sources such as end point, firewall, proxy, etc
- We can divide our network log sources into two logical parts
    1. Host Log sources
    2. Network log sources
- Some common methods used by these SIEM solutions are explained below:
    1. Agent / Forwarder
        - These SIEM solutions provide a lightweight tool called an agent (forwarder by Splunk) that gets installed in the Endpoint.
    2. Syslog
        - Syslog is a widely used protocol to collect data from various systems like web servers, databases, etc., are sent real-time data to the centralized destination.
    3. Manual Upload
        - Some SIEM solutions, like Splunk, ELK, etc., allow users to ingest offline data for quick analysis. Once the data is ingested, it is normalized and made available for analysis.
    4. Port-Forwarding
        - SIEM solutions can also be configured to listen on a certain port, and then the endpoints forward the data to the SIEM instance on the listening port.

5.2 Elastic

- It is the collection of different open source components linked together to help users take the data from any source and in any format and perform a search, analyze and visualize the data in real-time.
- Consists of:
    1. Elastic Search
    2. Logstash
    3. Beats
    4. Kibana



[1] ElasticSearch

- Elasticsearch is a full-text search and analytics engine used to store JSON-formated documents.
- Elasticsearch is an important component used to store, analyze, perform correlation on the data, etc.
- Elasticsearch acts as a database used to search and analyze the data.
- Elasticsearch supports RESTFul API to interact with the data.

[2] Logstach

- It is a data processing engine used to take the data from different sources, apply the filter on it or normalize it, and then send it to the destination which could be Kibana or a listening port.

[3] Beats

- Beats is a host-based agent known as Data-shippers that is used to ship/transfer data from the endpoints to elasticsearch.

[4] Logstach

- Kibana is a web-based data visualization that works with elasticsearch to analyze, investigate and visualize the data stream in real-time.
- It allows the users to create multiple visualizations and dashboards for better visibility

KQL

- Stands for Kibana Query Language
- It is a search query language used to search the ingested logs/documents in the elasticsearch.

5.3 Splunk

- Splunk is one of the leading SIEM solutions in the market that provides the ability to collect, analyze and correlate the network machine logs in real-time.
- Consists of:
  1. Splunk Forwarded
  2. Indexer
  3. Search Head

Splunk Components:

[1] Splunk Forwarder

- Splunk Forwarder is a lightweight agent installed on the endpoint intended to be monitored
- Its main task is to collect the data and send it to the Splunk instance.
- It does not affect the endpoint's performance as it takes very few resources to process.

[2] Indexer

- Splunk Indexer plays the main role in processing the data it receives from forwarders.
- It takes the data, normalizes it into field-value pairs, determines the datatype of the data, and stores them as events.

[3] Search Head

- It is the place within the Search & Reporting App where users can search the indexed logs

How To add data?

- It has a total of 5 steps to successfully upload the data.
  1. Select Source -> Where we select the Log source.
  2. Select Source Type -> Select what type of logs are being ingested.
  3. Input Settings ->Select the index where these logs will be dumped and hostname to be associated with the logs.
  4. Review -> Review all the gif
  5. Done -> Final step, where the data is uploaded successfully and ready to be analyzed.

Chapter 6: Digital Forensics and Incident Response

6.1 Introduction

What is DFIR?

- Stands for Digital Forensics and Incident Response
- This field covers the collection of forensic artifacts from digital devices such as computers, media devices, and smartphones to investigate an incident.
- This field helps Security Professionals identify footprints left by an attacker when a security incident occurs

Basic Concepts of DFIR:

1. Artifacts

- Artifacts are pieces of evidence that point to an activity performed on a system.

2. Evidence Preservation

- When performing DFIR, we must maintain the integrity of the evidence we are collecting.
- the evidence is first collected and write-protected. Then, a copy of the write-protected evidence is used for analysis.

3. Chain of custody

- When the evidence is collected, it must be made sure that it is kept in secure custody.

4. Order of Volatility

- While performing DFIR, it is vital to understand the order of volatility of the different evidence sources
- Data in a computer system's memory (RAM) will be lost when the computer is shut down

5. Timeline Creation

- Once we have collected the artifacts and maintained their integrity, we need to present them understandably to fully use the information contained in them.
- Timeline creation provides perspective to the investigation and helps collate information from various sources to create a story of how things happened.

The Incident Response process:

1. NIST

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

2. NIST

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

6.2 Windows Forensics

6.2.1 Windows Registry

- The Windows Registry is a collection of databases that contains the system's configuration data.
- This configuration data can be about the hardware, the software, or the user's information
- You can view the registry using regedit.exe, a built-in Windows utility to view and edit the registry.
- The Windows registry consists of Keys and Values.
- A Registry Hive is a group of Keys, subkeys, and values stored in a single file on the disk.

Structure of the Registry:

- The registry on any Windows system contains the following five root keys:
  1. HKEY_CURRENT_USER (HKCU)
  2. HKEY_USERS (HKU)
  3. HKEY_LOCAL_MACHINE (HKLM)
  4. HKEY_CLASSES_ROOT (HKCR)
  5. HKEY_CURRENT_CONFIG (HKCC)

Root Keys:

1. HKEY_CURRENT_USER (HKCU)
   6. Contains the root of the configuration information for the user who is currently logged on.
   7. The user's folders, screen colours, and Control Panel settings are stored here.
2. HKEY_USERS (HKU)
   8. Contains all the actively loaded user profiles on the computer.
3. HKEY_LOCAL_MACHINE (HKLM)
   9. Contains configuration information particular to the computer (for any user)

4. HKEY_CLASSES_ROOT (HKCR)
    10. Is a subkey of HKEY_LOCAL_MACHINE\Software
    11. makes sure that the correct program opens when you open a file by using Windows Explorer.
5. HKEY_CURRENT_CONFIG: (HKCC)
    12. Contains information about the hardware profile that is used by the local computer at system startup.

Registry Hives:

- If you only have access to a disk image, you must know where the registry hives are located on the disk.
- The majority of these hives are located in the C:\Windows\System32\Config
    1. DEFAULT (mounted on HKEY_USERS\DEFAULT)
    2. SAM (mounted on HKEY_LOCAL_MACHINE\SAM)
    3. SECURITY (mounted on HKEY_LOCAL_MACHINE\Security)
    4. SOFTWARE (mounted on HKEY_LOCAL_MACHINE\Software)
    5. SYSTEM (mounted on HKEY_LOCAL_MACHINE\System)
- Two other hives containing user information can be found in the User profile directory.
    1. NTUSER.DAT (mounted on HKEY_CURRENT_USER when a user logs in)
        - The NTUSER.DAT hive is located in the directory C:\Users\<username>\
    2. USRCLASS.DAT (mounted on HKEY_CURRENT_USER\Software\CLASSES)
        - The USRCLASS.DAT hive is located in the directory C:\Users\<username>\AppData\Local\Microsoft\Windows.
- The Amcache Hive
    1. This hive is located in C:\Windows\AppCompat\Programs\Amcache.hve
    2. Windows creates this hive to save information on programs that were recently run on the system.
- Transaction Logs and Backups:
    1. The transaction logs can be considered as the journal of the changelog of the registry hive.
    2. Registry backups are the opposite of Transaction logs.

Data Acquisition:

- It is recommended practice to image the system or make a copy of the required data and perform forensics on it.
- When we go to copy the registry hives from %WINDIR%\System32\Config, we cannot because it is a restricted file. **(Solution???)**

- we can use one of the following tools:

1. KAPE
2. Autopsy
3. FTK Imager

- Once we have extracted the registry hives, we need a tool to view these files as we would in the registry editor, we can use the following tools:

1. Registry Viewer
2. Zimmerman's Registry Explorer
3. RegRipper

How to Perform Forensics?

System Information and system account:

1. **OS Version**
   - To find the OS version, we can use the following registry key:
     1. SOFTWARE\Microsoft\Windows NT\CurrentVersion
2. **Current Control Set**
   - The hives containing the machine's configuration data used for controlling system startup
     1. SYSTEM\ControlSet001
     2. SYSTEM\ControlSet002
3. **Autoruns**
   - The following registry keys include information about programs or commands that run when a user logs on
     1. NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
     2. NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce
     3. SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
     4. SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
     5. SOFTWARE\Microsoft\Windows\CurrentVersion\Run
4. **SAM**
   - The SAM hive contains user account information, login information, and group information
     1. SAM\Domains\Account\Users

Usage or knowledge of files/folder:

1. **Recent Files**
   - Windows maintains a list of recently opened files for each user
   - This information is stored in the NTUSER hive
2. **ShellBags**
   - This information about the Windows 'shell' is stored and can identify the Most Recently Used files and folders
     1. USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags

2. USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
3. NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
4. NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

- Evidence of Execution

1. UserAssist

- These keys contain information about
  1. The programs launched
  2. The time of their launch
  3. The number of times they were executed.
- The User Assist key is present in the NTUSER hive, mapped to each user's GUID
- However, programs that were run using the command line can't be found in the User Assist keys.

2. BAM/DAM

- BAM stands for Background Activity Monito
- DAM stands for Desktop Activity Moderator
- This location contains information about last run programs, their full paths, and last execution time.
  1. SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
  2. SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID

- External Devices/USB device forensics

1. Device identification

- The following locations keep track of USB keys plugged into a system.
  1. SYSTEM\CurrentControlSet\Enum\USBSTOR
  2. SYSTEM\CurrentControlSet\Enum\USB

6.2.2 Windows File systems

File Systems:

1. FAT

- Stands for File Allocation Table
- The FAT creates a table that indexes the location of bits that are allocated to different files.
- Structure:
  1. Cluster
     - A cluster is a basic storage unit of the FAT file system
     - Each file stored on a storage device can be considered a group of clusters containing bits of information
  2. Directory

        - A directory contains information about file identification, like file name, starting cluster, and filename length.
    3. File Allocation Table
        - The File Allocation Table is a linked list of all the clusters.

    In summary, the bits that make up a file are stored in clusters. All the filenames on a file system, their starting clusters, and their lengths are stored in directories. And the location of each cluster on the disk is stored in the File Allocation Table.

- Types:
    1. FAT 12
    2. FAT 16
    3. FAT 32
    4. exFAT

2. NTFS

- Stands for New Technology File System
- It offers more in terms of security, reliability, recovery capabilities, and volume size.
- we can say that the NTFS file system data is organized in the Master File Table.
- It is a structured database that tracks the objects stored in a volume.

How to Perform Forensics?

- ### Recovering Deleted Files
    1. When we delete a file from the file system, the file system deletes the entries that store the file's location on the disk.
    2. Similarly, there is data on the disk in different unallocated clusters, which can possibly be recovered.
    3. Using tool called “Autopsy”

- ### Evidence of Execution

    let's learn where to find artifacts present in the file system to perform forensic analysis.

    1. **Windows Prefetch Files**
        - When a program is run in Windows, it stores its information for future use
        - This stored information is used to load the program quickly in case of frequent use.
        - This information is stored in prefetch files which are located in the C:\Windows\Prefetch directory.
        - We can use Prefetch Parser (PECmd.exe) from Eric Zimmerman's tools for parsing Prefetch files and extracting data

- To run Prefetch Parser on a file and save the results in a CSV, we can use the following command:
  - PECmd.exe -f <path-to-Prefetch-files> --csv <path-to-save-csv>
- Similarly, for parsing a whole directory, we can use the following command:
  - PECmd.exe -d <path-to-Prefetch-directory> --csv <path-to-save-csv>

2. **Windows 10 Timeline**
   - It contains the application that was executed and the focus time of the application.
   - The Windows 10 timeline can be found at the following location:
     - C:\Users\<username>\AppData\Local\ConnectedDevicesPlatform\{randomfolder}\ActivitiesCache.db
   - We can use Eric Zimmerman's WxTCmd.exe for parsing Windows 10 Timeline.
     - WxTCmd.exe -f <path-to-timeline-file> --csv <path-to-save-csv>

3. **Windows Jump Lists**
   - Windows introduced jump lists to help users go directly to their recently used files from the taskbar.
   - This data is stored in the following directory:
     - C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestination
   - We can use Eric Zimmerman's JLECmd.exe to parse Jump Lists.
     - JLECmd.exe -f <path-to-Jumplist-file> --csv <path-to-save-csv>

File/Folder Knowledge

1. **Shortcut files**
   - Windows creates a shortcut file for each file opened either locally or remotely
   - The shortcut files contain information about the first and last opened times of the file and the path of the opened file
   - Shortcut files can be found in the following locations:
     - C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent
     - C:\Users\<username>\AppData\Roaming\Microsoft\Office\Recent
   - We can use Eric Zimmerman's LECmd.exe (Lnk Explorer) to parse Shortcut files
     - LECmd.exe -f <path-to-shortcut-files> --csv <path-to-save-csv>

- External Devices/USB device forensics

1. **Setupapi**
    - When any new device is attached to a system, information related to the setup of that device is stored in the setupapi.dev.log
        - C:\Windows\inf\setupapi.dev.log

6.3 Linux Forensics

How to Perform Forensics?

- OS and account information
    1. OS Release information
        - in /etc/os-release
    2. User Accounts
        - In /etc/passwd | column -t -s :
    3. Group Information
        - in /etc/group
    4. Sudoers List
        - in /etc/sudoers
    5. Login Information
        - in /var/log/wtmp
        - in /var/log/btmp
    6. Authentication Logs
        - in /var/log/auth.log

- System Configuration
    1. Hostname
        - /etc/hostname
    2. Time zone
        - /etc/timezone
    3. Network Configuration
        - /etc/network/interfaces
    4. Active network connections
        - netstat
    5. Running processes
        - ps
    6. DNS information
        - /etc/hosts
        - /etc/resolv.conf

- Persistence mechanisms
    1. Cron jobs
        - /etc/crontab
    2. Service startup
        - /etc/init.d
    3. .Bashrc
        - .bashrc

- Evidence of Execution
    1. Sudo execution history
        - cat /var/log/auth.log* |grep -i COMMAND|tail
    2. Bash history
        - cat ~/.bash_history
    3. Files accessed using vim
        - cat ~/.viminfo

- Log files
    1. Syslog
        - /var/log/syslog
    2. Auth logs
        - cat /var/log/auth.log* |head
    3. Third-party logs
        - /var/log/

6.4 Tools

6.4.1 Autopsy

- It is an open source and powerful digital forensics platform
- It has a capability of analysing all types of mobile devices and digital media (Disk Image)
- Autopsy case files have a ".aut" file extension.

Data Sources:

- Supported Disk Image:
    1. Raw Single (For example: *.img, *.dd, *.raw, *.bi
    2. Raw Split (For example: *.001, *.002, *.aa, *.ab, etc)
    3. EnCase (For example: *.e01, *.e02, etc)
    4. Virtual Machines (For example: *.vmdk, *.vhd)

Ingest Modules:

- Each Ingest Module is designed to analyse and retrieve specific data from the drive.
- You can do that by using 2 ways:
    1. Configuring ingest modules while adding data sources
    2. Using ingest modules after adding data sources

Practical Hands-on:

- https://www.youtube.com/watch?v=Dlrn3ZRzn2I

6.4.2 Redline

- It is a FireEye tool
- You can analyze a potentially compromised endpoint through the memory dump, including various file structures.
- Here is what you can do using Redline:
    1. Collect registry data (Windows hosts only)
    2. Collect running processes
    3. Collect memory images (before Windows 10)
    4. Collect Browser History
    5. Look for suspicious strings

Data Collection:

- There are three ways or options to collect data using Redline:
    1. Standard Collector
        - This method configures the script to gather a minimum amount of data for the analysis.
    2. Comprehensive Collector
        - This method configures the script to gather the most data from your host for further analysis.
    3. IOC Search Collector (Windows only)
        - This method collects data that matches with the Indicators of Compromise (IOCs) that you created with the help of IOC Editor.

1. **Standard Collector**
    - There will be five tabs, which include Memory, Disk, System, Network, and Other.
    - Then you have to choose the folder where the results will be set
    - Go to that folder and run "RunRedlineAudit" script as administrator
    - Note: This process may take between 15-20 minutes to complete.
    - After the script is finished, you will notice a new file created - AnalysisSession1 (in the Sessions folder) with the .mans extension.

2. **IOC Search Collector**
    - They are artifacts of the potential compromise and host intrusion on the system or network
    - IOCs can be MD5, SHA1, SHA256 hashes, IP address, C2 domain, file size, filename, file path, a registry key, etc.
    - One of the great tools you can use is IOC Editor, created by FireEye

Practical Hands-on:

- https://www.youtube.com/watch?v=HXv45dsL8xI

6.4.3 Kape

- Stands for Kroll Artifact Parser and Extractor
- It parses and extracts Windows forensics artifacts.
- It provides forensic artifacts from a live system or a storage device much earlier than the imaging process completes.

How does it Work?

1. **Collecting**
    - The collection of files (targets), KAPE adds the files to a queue and copies them in two passes.
        i. It copies the files that it can. (This works for files that the OS has not locked.)
        ii. The rest of the files are passed to a secondary queue.
    - The copied files are saved with original timestamps and metadata and stored in a similar directory structure.

2. **Processing**
    - Once the data is collected, KAPE can process it using modules.
    - The modules can be independent binaries that run on the collected data and process them to extract information.

Target:

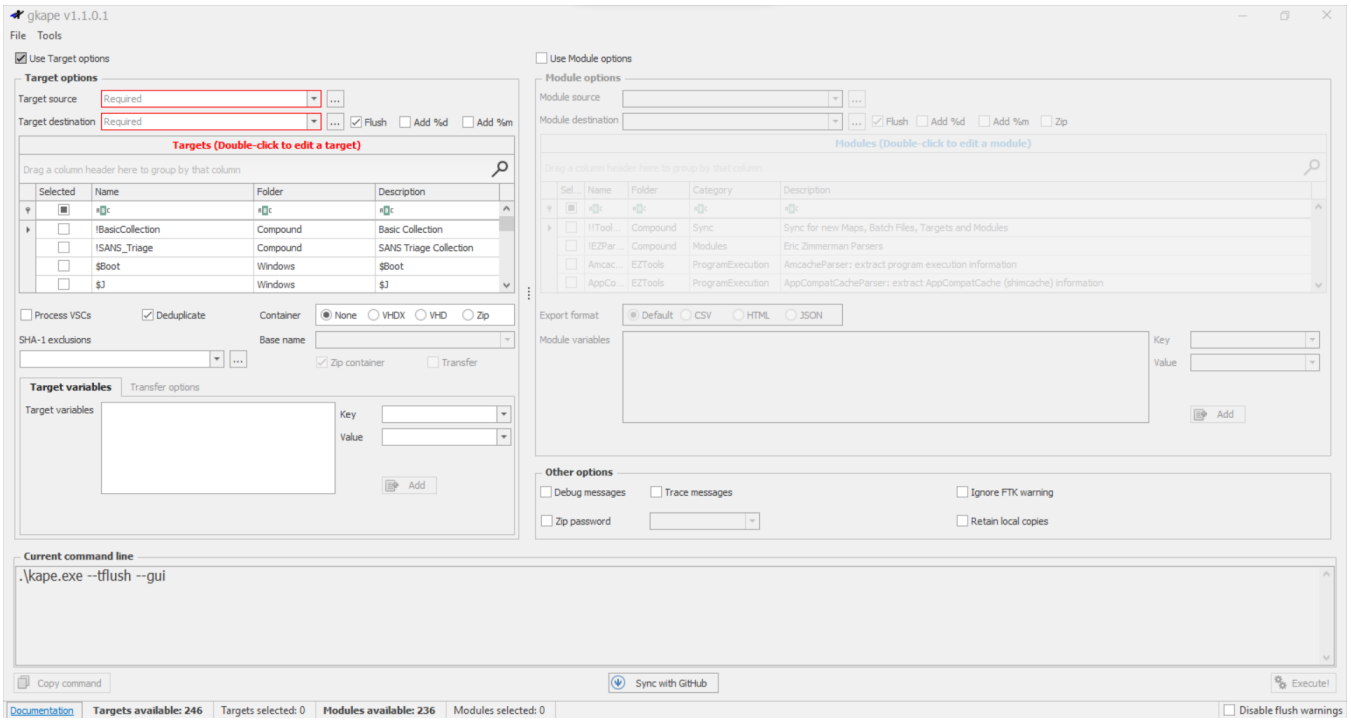
- Targets are the artifacts that need to be collected from a system or image and copied to our provided destination.
- Target's extension is .tkape
- Compound Targets help us collect multiple targets by giving a single command.

Module:

- It runs specific tools against the provided set of files.
- The output is in the form of CSV or TXT files.

- Module's extension is .mkape

KAPE GUI



Hands-on Challenge

- https://www.youtube.com/watch?v=AcYNcZurEOA

6.4.4 Volatility

- Volatility is a free memory forensics
- Commonly used by malware and SOC analysts within a blue team or as part of their detection and monitoring solutions.
- Volatility is written in Python
- It is extracting digital artifacts from volatile memory (RAM) samples.

Memory Extraction:

- Extracting a memory dump can be performed in numerous ways
- Tools that can be used to extract a memory from a bare-metal machine.
    1. FTK Imager
    2. Redline
    3. FastDump
- For virtual machines
    1. VMWare - .vmem
    2. Hyper-V - .bin

3. VirtualBox - .sav file *this is only a partial memory file

Plugins Overview:

- Volatility will automatically identify the host and build of the memory file.
- There are several plugins available with Volatility as well as third-party plugins
- Plugins:
    1. **Identifying Image Info and Profiles**
        - `windows.info`
            - `Syntax: python3 vol.py -f <file> windows.info`
    2. **Listing Processes and Connections**
        - `Pslist`
            - `Syntax: python3 vol.py -f <file> windows.pslist`
        - `Psscan`
            - `Syntax: python3 vol.py -f <file> windows.psscan`
        - `Pstree`
            - `Syntax: python3 vol.py -f <file> windows.pstree`
        - `Netstat`
            - `Syntax: python3 vol.py -f <file> windows.netstat`
        - `Dlllist`
            - `Syntax: python3 vol.py -f <file> windows.dlllist`
    3. **Advanced Memory Forensics**
        - `Ssdt`
            - `Syntax: python3 vol.py -f <file> windows.ssdt`
        - `Modules`
            - `Syntax: python3 vol.py -f <file> windows.modules`
        - `Driverscan`
            - `Syntax: python3 vol.py -f <file> windows.driverscan`

Hands-on challenge

- https://www.youtube.com/watch?v=2DZqg2rcYTk

Chapter 7: Phishing

7.1 Introduction

- Email address consists of 3 parameters:
    1. User Mailbox (Username)
    2. @
    3. Domain
- Email Protocols
    1. SMTP
        - Stands for Simple Mail Transfer Protocol
        - Works on port 25
        - It is utilized to handle the sending of emails.
    2. POP3
        - Stands for Post Office Protocol
        - Works on port 110
        - It is responsible transferring email between a client and a mail server.
        - Emails are downloaded and stored on a single device.
    3. IMAP
        - Stands for Internet Message Access Protocol
        - Works on port 143
        - It is responsible transferring email between a client and a mail server.
        - Sent messages are stored on the server.
- Process
    1. MUA (Mail User Agent)
    2. MSA (Mail Submission Agent)
    3. MTA (Mail Transfer Agent)
    4. MDA (Mail Delivery Agent)
- Email basic headers
    1. From
        - The sender's email address
    2. Subject
        - The email's subject line
    3. Date
        - The date when the email was sent
    4. To
        - The recipient's email address
    5. CC
        - Carbon copy
    6. X-Originating-IP
        - The IP address of the email was sent from (this is known as an X-header)
    7. Smtp.mailfrom/header.from
        - The domain the email was sent from (these headers are within Authentication-Results)

8. Reply-To
    - This is the email address a reply email will be sent to instead of the From email address

- Body consist of:
    1. Text
    2. Attachment
        - URL
        - File

7.2 Phishing and how to prevent?

Phishing Types:

- There are different types of malicious emails can be classified as one of the following:
    1. Spam
        - Unsolicited junk emails sent out in bulk to a large number of recipients.
    2. Phishing
        - Emails sent to a target(s) purporting to be from a trusted entity to lure individuals into providing sensitive information.
    3. Spear phishing
        - Takes phishing a step further by targeting a specific individual(s) or organization seeking sensitive information.
    4. Whaling
        - It is similar to spear phishing, but it's targeted specifically to C-Level high-position individuals (CEO, CFO, etc.), and the objective is the same.
    5. Smishing
        - Takes phishing to mobile devices by targeting mobile users with specially crafted text messages.
    6. Vishing
        - It is similar to smishing, but instead of using text messages for the social engineering attack, the attacks are based on voice calls.

Email Header Security:

1. SPF

- Stands for Sender Policy Framework
- It is used to authenticate the sender of an email.
- An SPF record is a DNS TXT record containing a list of the IP addresses that are allowed to send email on behalf of your domain."
- Example:

v=spf1 ip4:127.0.0.1 include:_spf.google.com -all

- v=spf1 -> This is the start of the SPF record
- ip4:127.0.0.1 -> This specifies which IP (in this case version IP4 & not IP6) can send mail
- include:_spf.google.com -> This specifies which domain can send mail
- -all -> (Fail) non-authorized emails will be rejected {OR} ■ ~all -> (Soft Fail)

2. DKIM

- Stands for DomainKeys Identified Mail
- It is used for the authentication of an email that's being sent.

  v=DKIM1; k=rsa; p=.....

  - v=DKIM1-> This is the version of the DKIM record. This is optional.
  - k=rsa -> This is the key type. The default value is RSA.
  - p= -> This is the public key that will be matched to the private key, which was created during the DKIM setup

3. DMARC

- Stands for Domain-Based Message Authentication, Reporting, and Conformance
- It uses a concept called alignment to tie the result of two other open source standards, SPF and DKIM , to the content of an email.

  v=DMARC1; p=quarantine; rua=mailto:postmaster@website.com

  - v=DMARC1 -> Must be in all caps, and it's not optional
  - p=quarantine -> If a check fails, then an email will be sent to the spam folder (DMARC Policy)
  - rua=mailto:postmaster@website.com -> Aggregate reports will be sent to this email address

7.3 Phishing Analysis Tools

- **Below is a checklist of the pertinent information an analyst (you) is to collect from the email header:**
  1. Sender email address
  2. Sender IP address
  3. Reverse lookup of the sender IP address
  4. Email subject line
  5. Recipient email address (this information might be in the CC/BCC field)
  6. Reply-to email address (if any)
  7. Date/time

- **Afterward, we draw our attention to the email body and attachment(s) (if any).**

1. Any URL links (if an URL shortener service was used, then we'll need to obtain the real URL link)
2. The name of the attachment
3. The hash value of the attachment (hash type MD5 or SHA256, preferably the latter)

Header Analysis:

- **Tools**
    1. https://ipinfo.io/
        - Analyze sender IP address
    2. URLScan
        - Scan URLs
    3. Messageheader from the Google Admin Toolbox."Tool"

Body Analysis

- **Extract URL**
    1. cyberchef (Extract URLs)
- **Attachment (Get hash of the file)**
    1. Talos File Reputation
    2. Virus Total

Sandbox Analysis:

1. Hybrid Analysis
2. Anyrun