DFIR: An Introduction

Task 1 Introduction

Learning Objectives

Security breaches and incidents happen despite the security teams trying their best to avoid them worldwide. The prudent approach in such a scenario is to prepare for the time when an incident will happen so that we are not caught off-guard. Thus, Digital Forensics and Incident Response (DFIR) has become an essential subject in Defensive Security. In this room, we will cover some basic concepts of DFIR and introduce rooms that expand on our knowledge of DFIR. The room will cover the following topics:

- Introduction of DFIR
- Some basic concepts used in the DFIR field
- The Incident Response processes used in the industry
- Some of the tools used for DFIR

Task 2 The need for DFIR

What is DFIR?

As already mentioned, 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, use them to determine the extent of compromise in an environment, and restore the environment to the state it was before the incident occurred.

The need for DFIR

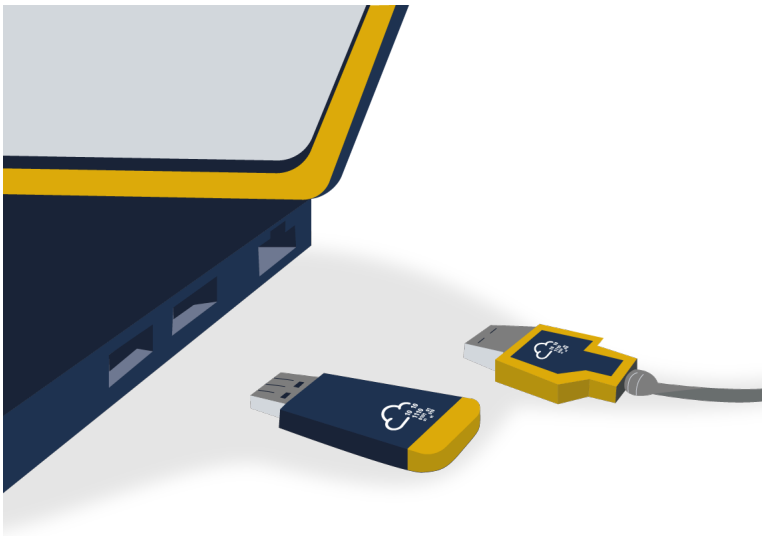
DFIR helps security professionals in various ways, some of which are summarized below:

- Finding evidence of attacker activity in the network and sifting false alarms from actual incidents.
- Robustly removing the attacker, so their foothold from the network no longer remains.
- Identifying the extent and timeframe of a breach. This helps in communicating with relevant stakeholders.
- Finding the loopholes that led to the breach. What needs to be changed to avoid the breach in the future?

- Understanding attacker behavior to pre-emptively block further intrusion attempts by the attacker.
- Sharing information about the attacker with the community.

Who performs DFIR?

As the name suggests, DFIR requires expertise in both Digital Forensics and Incident Response. Dividing these two fields this way, the following skillset is needed to become a DFIR professional:



- **Digital Forensics:** These professionals are experts in identifying forensic artifacts or evidence of human activity in digital devices.
- **Incident Response:** Incident responders are experts in cybersecurity and leverage forensic information to identify the activity of interest from a security perspective.

DFIR professionals know about Digital Forensics and cybersecurity and combine these domains to achieve their goals. Digital Forensics and Incident Response domains are often combined because they are highly interdependent. Incident Response leverages knowledge gained from Digital Forensics. Similarly, Digital Forensics takes its goals and scope from the Incident Response process, and the IR process defines the extent of forensic investigation.

Answer the questions below

What does DFIR stand for? Digital Forensics and Incident Response

DFIR requires expertise in two fields. One of the fields is Digital Forensics. What is the other field? Incident Response

Task 3 Basic concepts of DFIR

Now that we have introduced DFIR and why it is needed, let's learn some basic concepts related to DFIR in this task.

Artifacts:

Artifacts are pieces of evidence that point to an activity performed on a system. When performing DFIR, artifacts are collected to support a hypothesis or claim about attacker activity. For example, if we are to claim that the attacker used Windows registry keys to maintain persistence on a system, we can use the said registry key to support our claim. In this case, the mentioned registry key will be considered an artifact. Artifact collection is, therefore, an essential part of the DFIR process. Artifacts can be collected from the Endpoint or Server's file system, memory, or network activity.

Most of the time, enterprise environments mainly consist of Windows and Linux Operating Systems. To learn more about the forensic artifacts in these Operating Systems, you can head to the Windows Forensics 1, Windows Forensics 2, or the Linux Forensics room. Windows systems are primarily used for endpoints and server use-cases, like Active Directory Domain Controllers or MS Exchange email servers. Enterprises primarily use Linux systems in the capacity of servers hosting some service, for example, web servers or database servers.

Evidence Preservation:

When performing DFIR, we must maintain the integrity of the evidence we are collecting. For this reason, certain best practices are established in the industry. We must note that any forensic analysis contaminates the evidence. Therefore, the evidence is first collected and write-protected. Then, a copy of the write-protected evidence is used for analysis. This process

ensures that our original evidence is not contaminated and remains safe while analyzing. If our copy under investigation gets corrupted, we can always return and make a new copy from the evidence we had preserved.

Chain of custody:

Another critical aspect of maintaining the integrity of evidence is the chain of custody. When the evidence is collected, it must be made sure that it is kept in secure custody. Any person not related to the investigation must not possess the evidence, or it will contaminate the chain of custody of the evidence. A contaminated chain of custody raises questions about the integrity of the data and weakens the case being built by adding unknown variables that can't be solved. For example, suppose a hard drive image, while being transferred from the person who took the image to the person who will perform the analysis, gets into the hands of a person who is not qualified to handle such evidence. In that case, we can't be sure if he dealt with the evidence correctly and hence didn't contaminate the evidence with his activity.

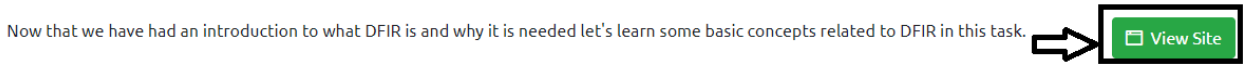
Order of volatility:

Digital evidence is often volatile, i.e., it can be lost forever if not captured in time. For example, data in a computer system's memory (RAM) will be lost when the computer is shut down since the RAM keeps data only as long as it remains powered on. Some sources are more volatile as compared to others. For example, a hard drive is persistent storage and maintains the data even if power is lost. Therefore, a hard drive is less volatile than RAM. While performing DFIR, it is vital to understand the order of volatility of the different evidence sources to capture and preserve accordingly. In the example above, we will need to preserve the RAM before preserving the hard drive since we might lose data in the RAM if we don't prioritize it.

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. A timeline of events needs to be created for efficient and accurate analysis. This timeline of events puts all the activities in chronological order. This activity is called timeline creation. Timeline creation provides perspective to the investigation and helps collate information from various sources to create a story of how things happened.

Now, let's view the attached static site to practice timeline creation and answer the first question. To do that, click on the View Site button in the top-right corner of this task.



Answer the questions below

From amongst the RAM and the hard disk, which storage is more volatile?

RAM

Complete the timeline creation exercise in the attached static site. What is the flag that you get after completion?

THM{DFIR_REPORT_DONE}

Task 4 DFIR Tools

The security industry has built various exciting tools to help with the DFIR process. These tools help save valuable time and enhance the capabilities of security professionals. Let's learn about some of these tools here. You can check out the rooms for these tools on TryHackMe to learn more about them.

Eric Zimmerman's tools:

Eric Zimmerman is a security researcher who has written a few tools to help perform forensic analysis on the Windows platform. These tools help the registry, file system, timeline, and many other analyses. To learn more about these tools, you can check out the Windows Forensics 1 and Windows Forensics 2 rooms, where these tools are discussed concerning the different artifacts found in the Windows Operating System.

KAPE:

Kroll Artifact Parser and Extractor (KAPE) is another beneficial tool by Eric Zimmerman. This tool automates the collection and parsing of forensic artifacts and can help create a timeline of events. You can check out the KAPE room to learn more about KAPE.

Autopsy: 

Autopsy is an open-source forensics platform that helps analyze data from digital media like mobile devices, hard drives, and removable drives. Various plugins for autopsy speed up the forensic process and extract and present valuable information from the raw data sources. TryHackMe's Autopsy room can help if you want to learn more about it.

Volatility: 

Volatility is a tool that helps perform memory analysis for memory captures from both Windows and Linux Operating Systems. It is a powerful tool that can help extract valuable information from the memory of a machine under investigation. You can learn more about Volatility in the Volatility room.

Redline: 

Redline is an incident response tool developed and freely distributed by FireEye. This tool can gather forensic data from a system and help with collected forensic information. You can learn more about Redline in the Redline room.

Velociraptor: 

Velociraptor is an advanced endpoint-monitoring, forensics, and response platform. It is open-source but very powerful. TryHackMe has created a Velociraptor room for you to learn more about it.

While all these tools are helpful while performing DFIR, it is essential to understand the process followed to achieve our goals. The next task will focus on the Incident Response process and how we can leverage Digital Forensics in that process.

Task 5 The Incident Response process

In Security Operations, the prominent use of Digital Forensics is to perform Incident Response. We will learn the Incident Response process and observe how Digital Forensics helps in the IR process in this task.

Different organizations have published standardized methods to perform Incident Response. NIST has defined a process in their SP-800-61 Incident Handling guide, which has the following steps:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-incident Activity

Similarly, SANS has published an Incident Handler's handbook. The handbook defines the steps as follows:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

The steps defined by SANS are often summarized as the acronym PICERL, making them easy to remember. We can see that the steps specified by SANS and NIST are identical. While NIST combines Containment, Eradication, and Recovery, SANS separates them into different steps. **Post-incident activity** and **Lessons learned** can be comparable, while **Identification** and **Detection and Analysis** have the same implications.

Now that we understand that the two processes are similar let's learn briefly what the different steps mean. We explain the PICERL steps as they are easier to remember by the acronym, but as described above, they are identical to the steps defined by NIST.

1. **Preparation**: Before an incident happens, preparation needs to be done so that everyone is ready in case of an incident. Preparation includes having the required people, processes, and technology to prevent and respond to incidents.

2. **Identification**: An incident is identified through some indicators in the identification phase. These indicators are then analyzed for False Positives, documented, and communicated to the relevant stakeholders.
3. **Containment**: In this phase, the incident is contained, and efforts are made to limit its effects. There can be short-term and long-term fixes for containing the threat based on forensic analysis of the incident that will be a part of this phase.
4. **Eradication**: Next, the threat is eradicated from the network. It has to be ensured that a proper forensic analysis is performed and the threat is effectively contained before eradication. For example, if the entry point of the threat actor into the network is not plugged, the threat will not be effectively eradicated, and the actor can gain a foothold again.
5. **Recovery**: Once the threat is removed from the network, the services that had been disrupted are brought back as they were before the incident happened.
6. **Lessons Learned**: Finally, a review of the incident is performed, the incident is documented, and steps are taken based on the findings from the incident to make sure that the team is better prepared for the next time an incident occurs.

Answer the questions below

At what stage of the IR process are disrupted services brought back online as they were before the incident?

Recovery

At what stage of the IR process is the threat evicted from the network after performing the forensic analysis?

Eradication

What is the NIST-equivalent of the step called "Lessons learned" in the SANS process?

Post-incident Activity

Task 6 Conclusion

That was all for this room. Let's reiterate what we learned here.

- We learned what DFIR is and where it is used.
- We learned why we need to perform DFIR.
- We learned the basic concepts like the chain of custody, evidence preservation, and order of volatility.
- We learned about some of the tools used in the industry like EZ tools, KAPE, Autopsy, etc.
- The PICERL process for incident response