TryHackMe Critical Write-Up: Using Volatility For Windows Memory Forensics

Joseph Alan · Follow
Published in System Weakness
5 min read · Jul 18, 2024

This challenge focuses on memory forensics, which involves understanding its concepts, accessing and setting up the environment using tools like Volatility, gathering information from the compromised target, searching for suspicious activity with the obtained data, and extracting and analyzing information from memory dumps using various Volatility plugins.

Task 1 Introduction

Learning Objectives

In this room, we'll cover the following learning objectives.

- Memory Forensics' basic concepts.
- How to access and set up the environment.
- Gathering information from the compromised target.
- Search for suspicious activity using the information obtained.
- Extracting and analyzing data from memory.
- Conclusion & further steps after completing the room.

Task 2 Memory Forensics

- Memory forensics is a subset of computer forensics that analyzes volatile memory, typically on a compromised machine.
- In Windows OS, this corresponds to the Random Access Memory (RAM), whose content is flushed with every reboot or shutdown.
- It's one of the usual initial tasks during an incident response.
- **Difference from Disk Forensics**:
- Provides information about what resides on the target computer.
- Offers details on running processes or applications at a specific time.
- Gives insights into execution flow that may not be present in regular storage units or application logs.
- **Immediate Snapshot**: Memory analysis can provide an immediate snapshot of an application or a timestamp of an attacker's actions.

- **Chronology of Events:** Evidence collected through memory forensics is crucial for creating a timeline of events.
- **Two Main Phases:**

1.Memory Acquisition:

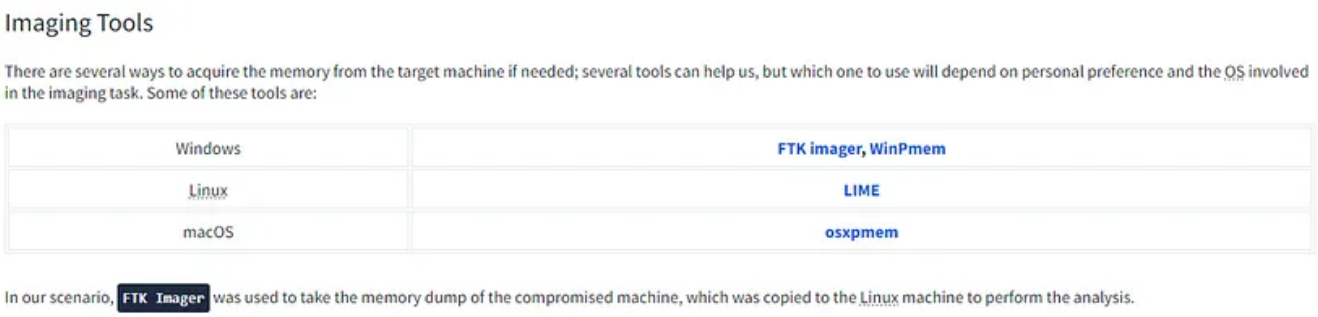
- Copying live memory to a file (dump).
- Essential to perform analysis without risking data loss from an inadvertent reboot.
- Provides proof of analysis if needed.

2. Memory Analysis:

- Detailed examination of the acquired memory dump to extract useful information.

Task 2 Answers

Task 3 Environment & Setup



Accessing the Machine

Before moving forward, start the lab by clicking the Start Machine button. It will take around 2 minutes to load properly. he VM will be accessible on the right side of the split screen. In case the VM is not visible, use the blue Show Split View button at the top of the page. You can also connect directly to the machine using the following information via SSH:

A memory dump named `memdump.mem` will be present at the home address at `/home/analyst`

```
Volatility3
user@machine$ vol -h
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-
                  [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [-
                  [--clear-cache] [--cache-path CACHE_PATH] [--offline] [--sing
                  [--stackers [STACKERS [STACKERS ...]]]
                  [--single-swap-locations [SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_
```

For Windows

Volatility3

```
user@machine$ vol windows --help
usage: volatility [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG]
[-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG] [--clear-cache] [--cache-path CACHE_PATH] [--
offline]
                [--single-location SINGLE_LOCATION] [--stackers [STACKERS [STACKERS ...]]] [--single-swap-locations
[SINGLE_SWAP_LOCATIONS [SINGLE_SWAP_LOCATIONS ...]]]
                plugin ...
volatility: error: argument plugin: plugin windows matches multiple plugins (windows.bigpools.BigPools, windows.cachedump.Cachedump,
windows.callbacks.Callbacks, windows.cmdline.CmdLine, windows.crashinfo.Crashinfo, windows.devicetree.DeviceTree,
windows.dlllist.DllList, windows.driverirp.DriverIrp, windows.drivermodule.DriverModule, windows.driverscan.DriverScan,
windows.dumpfiles.DumpFiles, windows.envars.Envars, windows.filescan.FileScan, windows.getservicesids.GetServiceSIDs,
windows.getsids.GetSIDs, windows.handles.Handles, windows.hashdump.Hashdump, windows.info.Info, windows.joblinks.JobLinks,
windows.ldrmodules.LdrModules, windows.lsadump.Lsadump, windows.malfind.Malfind, windows.mbrscan.MBRScan, windows.memmap.Memmap,
windows.mftscan.ADS, windows.mftscan.MFTScan, windows.modscan.ModScan, windows.modules.Modules, windows.mutantscan.MutantScan,
windows.netscan.NetScan, windows.netstat.NetStat, windows.poolscanner.PoolScanner, windows.privileges.Privs, windows.pslist.PsList,
windows.psscan.PsScan, windows.pstree.PsTree, windows.registry.certificates.Certificates, windows.registry.hivelist.HiveList,
windows.registry.hivescan.HiveScan, windows.registry.printkey.PrintKey, windows.registry.userassist.UserAssist,
windows.sessions.Sessions, windows.skeleton_key_check.Skeleton_Key_Check, windows.ssdt.SSDT, windows.statistics.Statistics,
windows.strings.Strings, windows.svcscan.SvcScan, windows.symlinkscan.SymlinkScan, windows.vadinfo.VadInfo, windows.vadwalk.VadWalk,
windows.vadyarascan.VadYaraScan, windows.verinfo.VerInfo, windows.virtmap.VirtMap)
```

Plugins are extremely helpful during the analysis when using Volatility3 since they will quickly parse a memory dump for specific data types and sort the data according to the selected plugin. You can find a summary of some of the most relevant plugins below

Windows.cmdline	Lists process command line arguments
windows.drivermodule	Determines if any loaded drivers were hidden by a rootkit
Windows.filescan	Scans for file objects present in a particular Windows memory image
Windows.getsids	Print the SIDs owning each process
Windows.handles	Lists process open handles
Windows.info	Show OS & kernel details of the memory sample being analyzed
Windows.netscan	Scans for network objects present in a particular Windows memory image
Widnows.netstat	Traverses network tracking structures present in a particular Windows memory image.
Windows.mftscan	Scans for Alternate Data Stream
Windows.pslist	Lists the processes present in a particular Windows memory image
Windows.pstree	List processes in a tree based on their parent process ID

Task 3 Answers

Answer the questions below

Which plugin can help us to get information about the OS running on the target machine?

Windows.info — ✓ Correct Answer

Which tool referenced above can help us take a memory dump on a Linux OS?

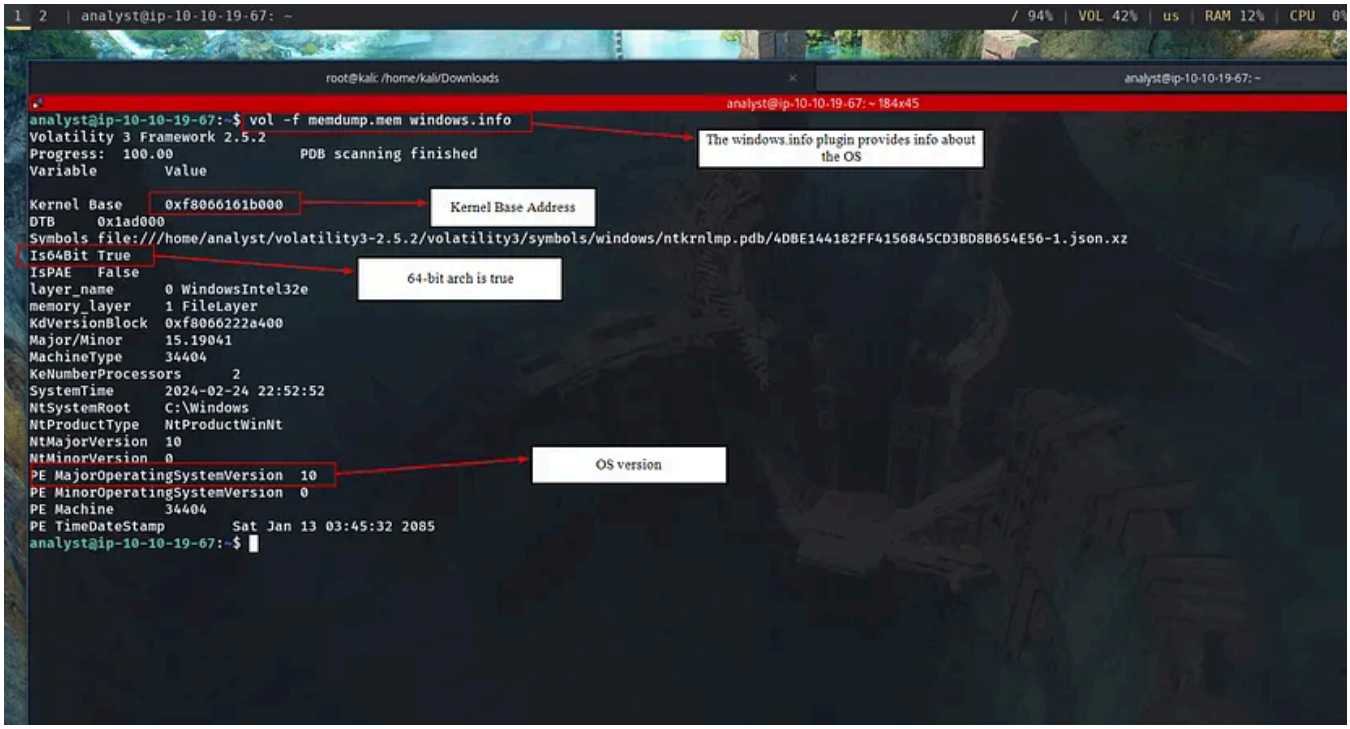
LIME — ✓ Correct Answer

Which command will display the help menu using Volatility on the target machine?

vol -h — ✓ Correct Answer

Task 4 Gathering Target Information

Using `-f` switch to indicate the file to analyze, in this case, `memdump.mem` followed by the plugin `windows.info` used to get the general information, as in the example shown below.



Task 4 Answers

Answer the questions below

Is the architecture of the machine x64 (64bit) Y/N?

Y ✓ Correct Answer Hint

What is the Verison of the Windows OS

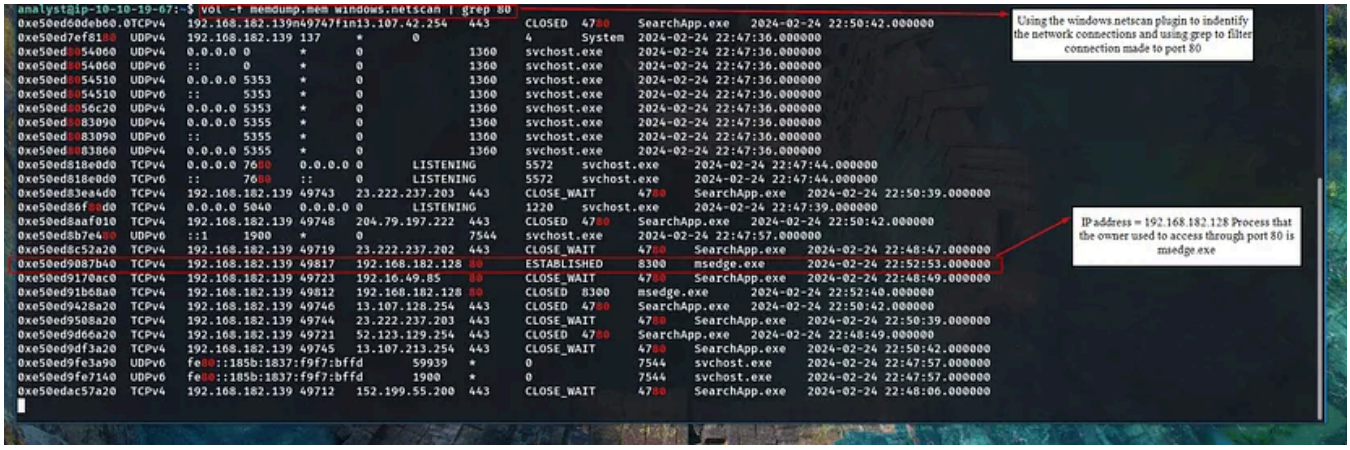
10 ✓ Correct Answer Hint

What is the base address of the kernel?

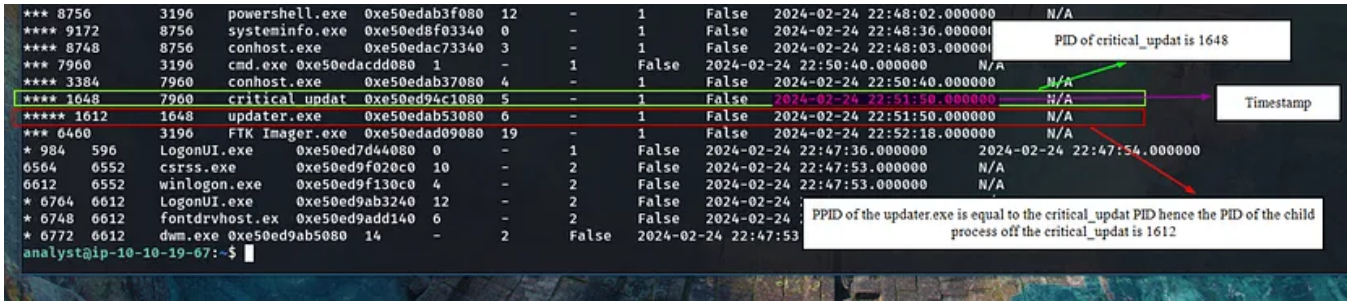
0xf8066161b000 ✓ Correct Answer Hint

Task 5 Searching For Suspicious Activity

Using the windows.netscan plugin



Using the windows.pstree plugin



Task 5 Answers

Answer the questions below

Using the plugin "windows.netscan" can you identify the IP address that establish a connection on port 80?

192.168.182.128 ✓ Correct Answer

Using the plugin "windows.netscan," can you identify the program (owner) used to access through port 80?

msedge.exe ✓ Correct Answer

Analyzing the process present on the dump, what is the PID of the child process of critical_updat?

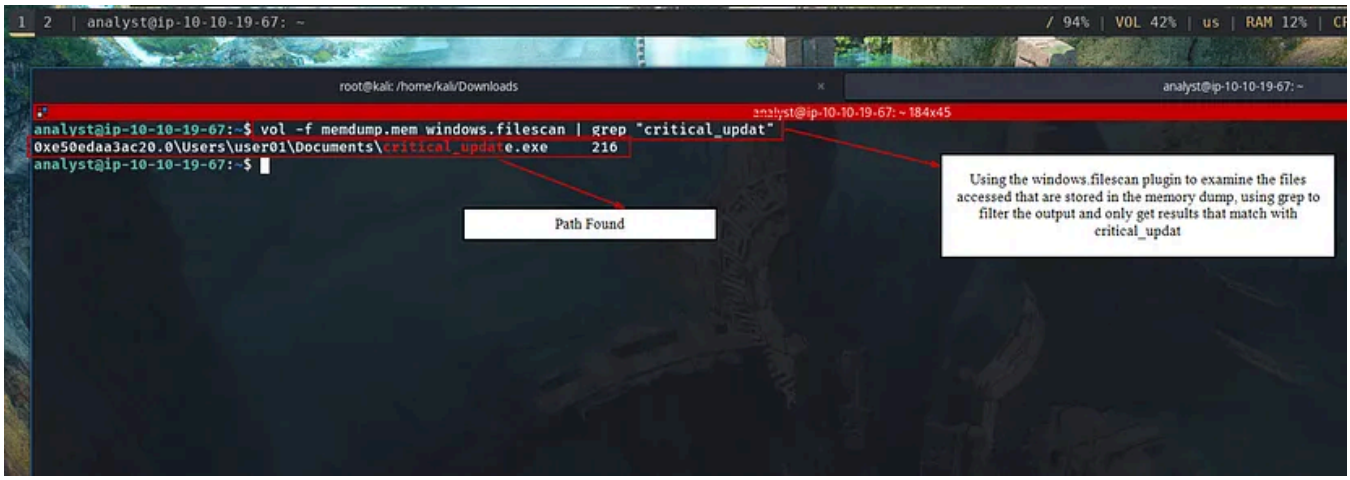
1612 ✓ Correct Answer

What is the time stamp time for the process with the truncated name critical_updat?

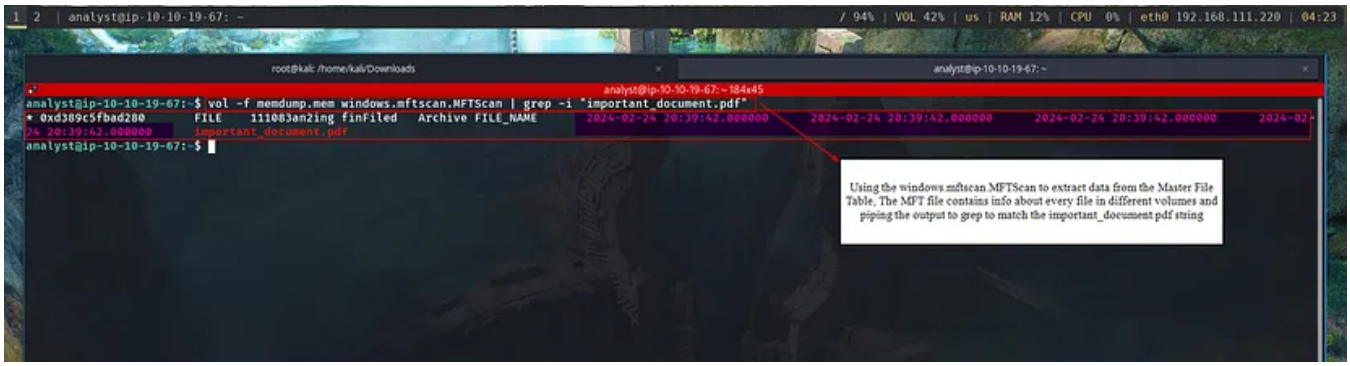
2024-02-24 22:51:50.000000 ✓ Correct Answer

Task 6 Finding Interesting Data

Using the windows.filescan plugin

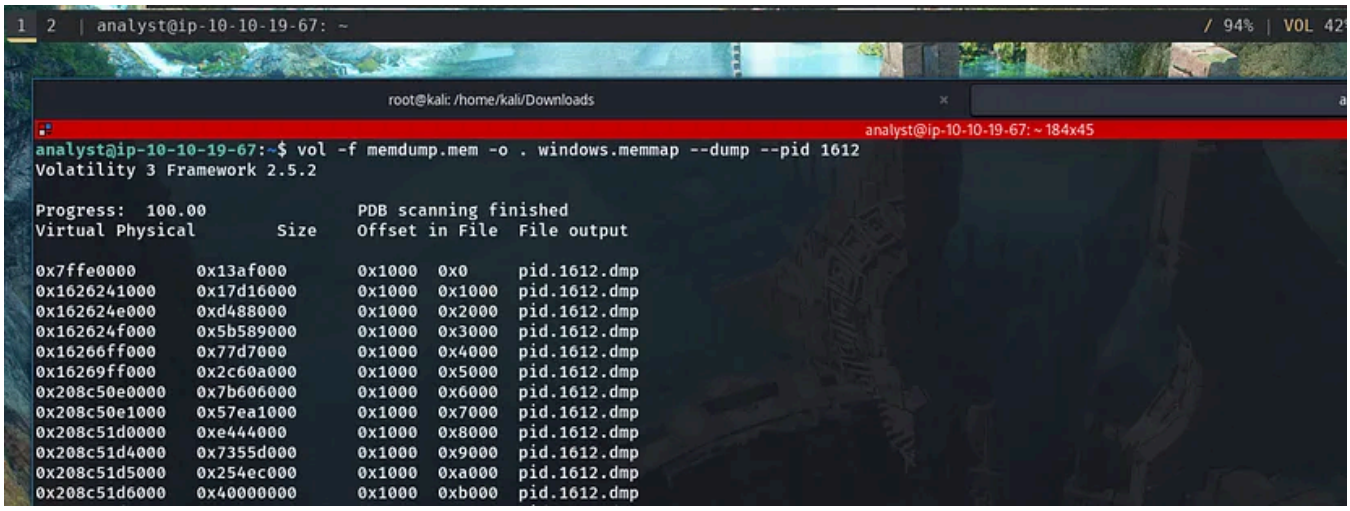


Using the windows.mftscan.MFTScan plugin

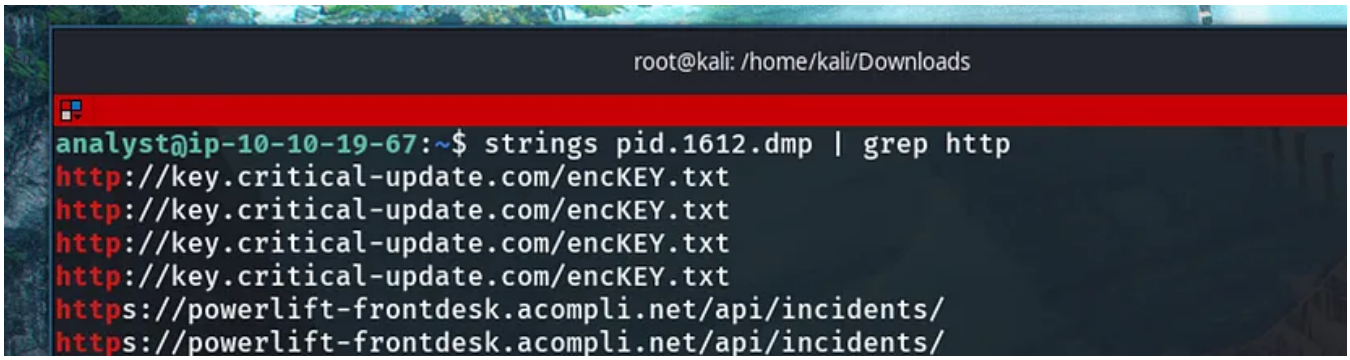


Using the windows.memmap plugin

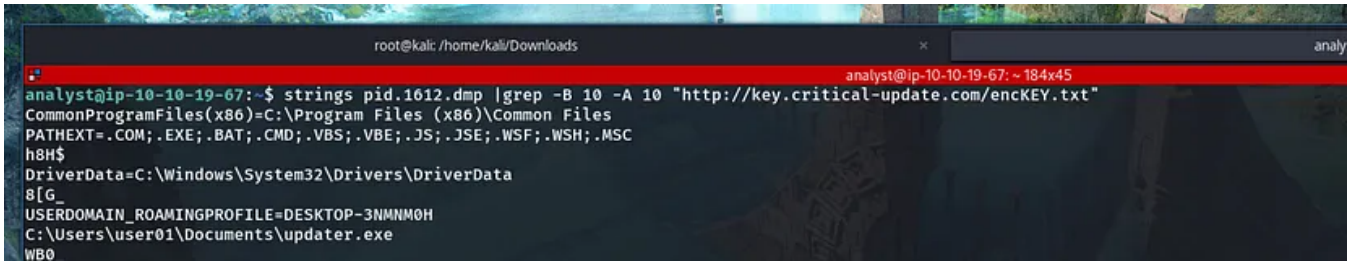
Creating a memory dump of the memory region related to the process ID 1612 as discovered earlier is the process ID of the updater.exe process

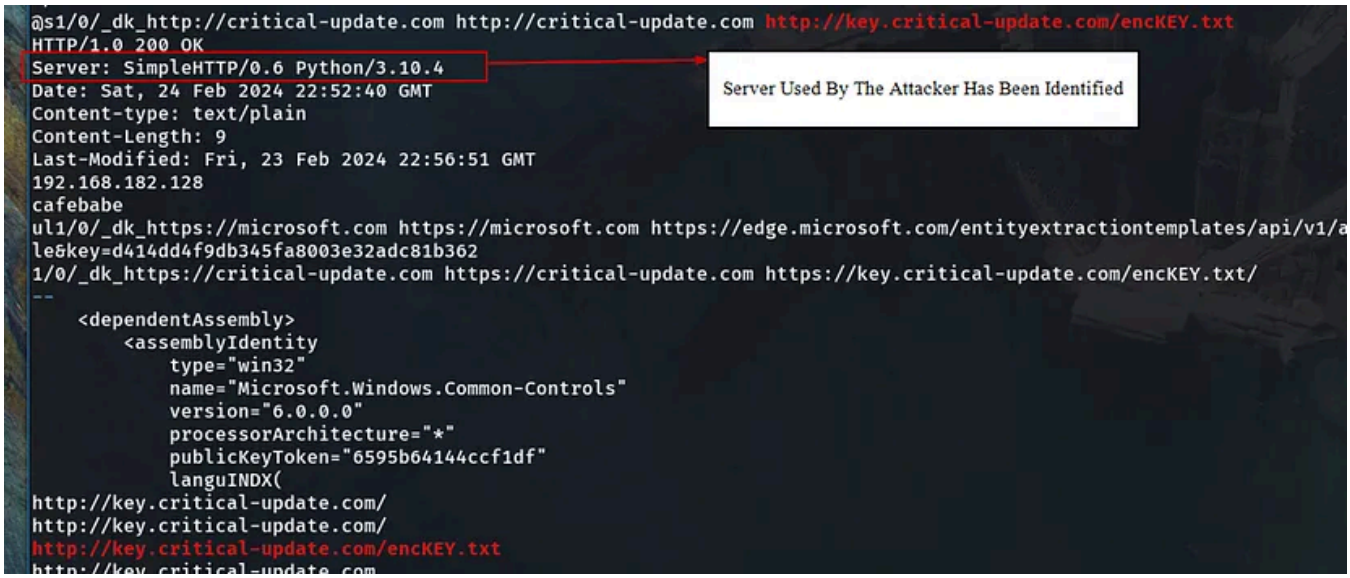


Using the strings command to extract the strings from the memory dump and using grep to match the strings with the string “http”

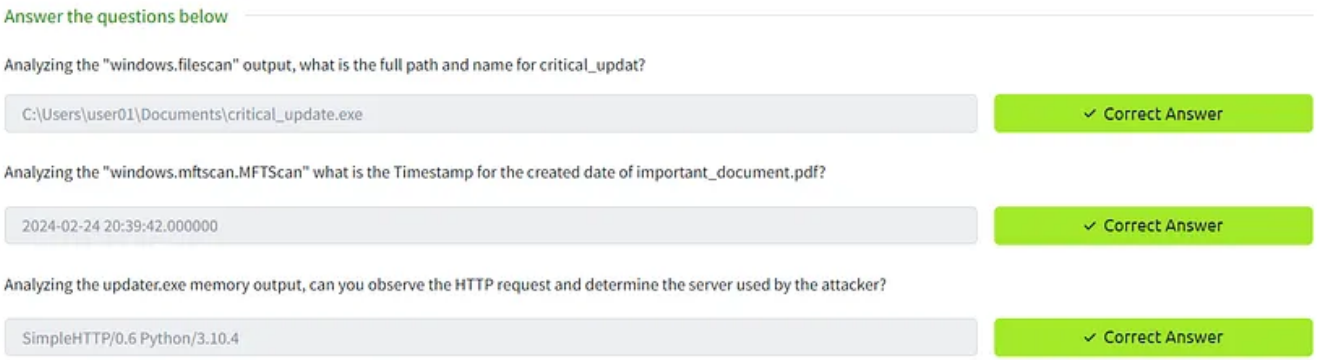


Using the command below to search for the string “http://key.critical-update.com/encKEY.txt" within the file `pid.1612.dmp`, it displays 10 lines before and 10 lines after each match, utilizing the `strings` command to extract readable text from the dump file.





Task 6 Answers



Task 7 Conclusion

Conclusion

In this scenario, we have put into practice the skills necessary to start digging into the world of memory forensics and practice with a tool like volatility, which is widely used among digital forensics professionals.

We learned how to gather information about the machine the dump belongs to, search for connections, enumerate and investigate processes, and examine the content for malicious patterns in a memory dump.

While all the information presented in his room can be used in real-life scenarios, it is possible to delve more deeply into the topic by examining more complex attacks. Some interesting material to get more into it can be the following:

- Windows Forensics 2
- Linux Forensics

- iOS Forensics
- Windows Applications Forensics

Tryhackme Writeup | Tryhackme Walkthrough | Cybersecurity | Forensics | Blue Team

Follow

Published in System Weakness

5.9K Followers · Last published 21 hours ago

System Weakness is a publication that specialises in publishing upcoming writers in cybersecurity and ethical hacking space. Our security experts write to make the cyber universe more secure, one vulnerability at a time.

Follow

Written by Joseph Alan

218 Followers · 225 Following

Cloud Security Engineer | AWS Solutions Architect Professional | CompTIA Cysa+|AWS sysops admin with LAB | TryHackMe top 1%| HackTheBox Rank - Pro Hacker

Responses (1)

What are your thoughts?

Respond

Kanwar Usama
9 days ago

Super work done. Excellent. keep it up.

Reply

More from Joseph Alan and System Weakness

Joseph Alan

Threat Hunting Introduction

Task 1 Introduction

Sep 26, 2023 7 1

In System Weakness by AbhirupKonwar

The best way to find private Bug-Hunting programs

Recon process to find private programs

Dec 25, 2024 234 7

In System Weakness by AbhirupKonwar

Exposed Git Directory P1 Bug

Story of P1 Bug that turned out to be ?

Dec 11, 2024 312 3

Joseph Alan

Expose TryHackMe Write-Up

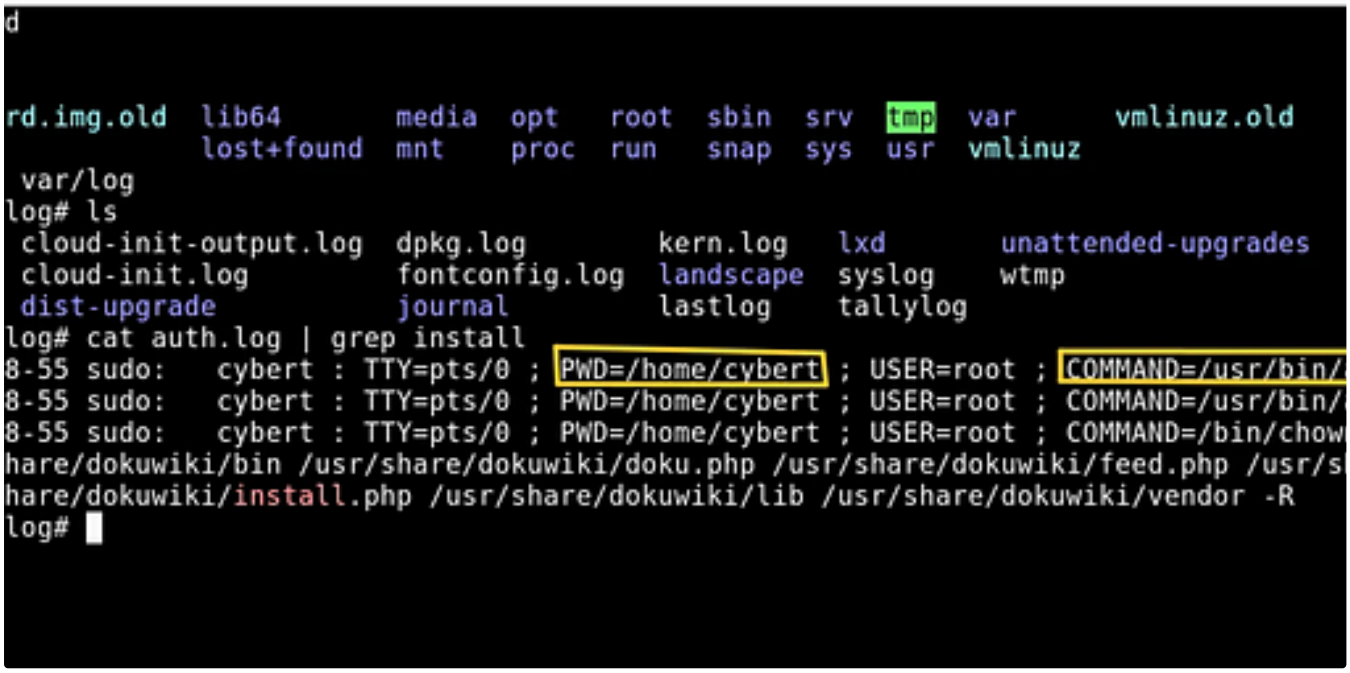
Expose

Sep 24, 2023 5

See all from Joseph Alan

See all from System Weakness

Recommended from Medium

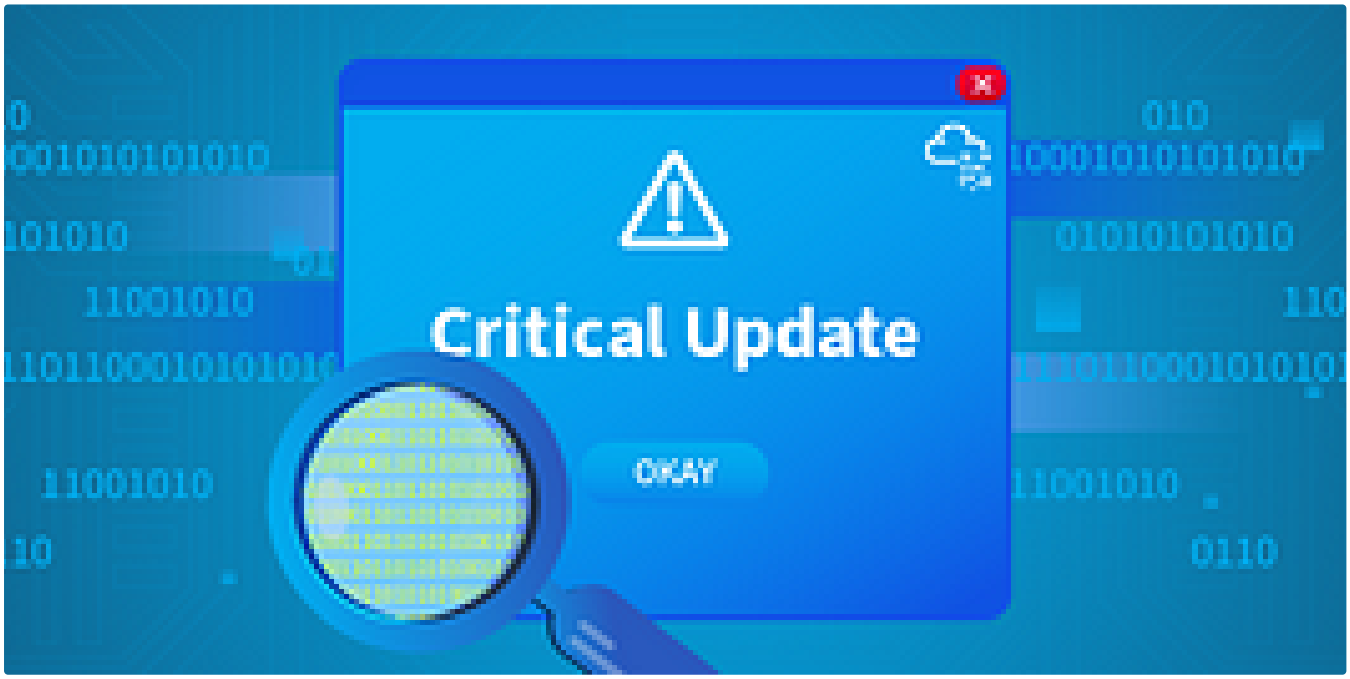


Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here: https://tryhackme.com/room/disgruntled

Oct 22, 2024



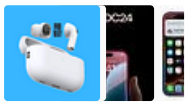
In T3CH by Axoloth

TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

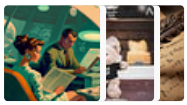
Jul 21, 2024 104

Lists



Tech & Tools

22 stories · 380 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves

Staff picks

796 stories · 1561 saves

Natural Language Processing

1884 stories · 1529 saves

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

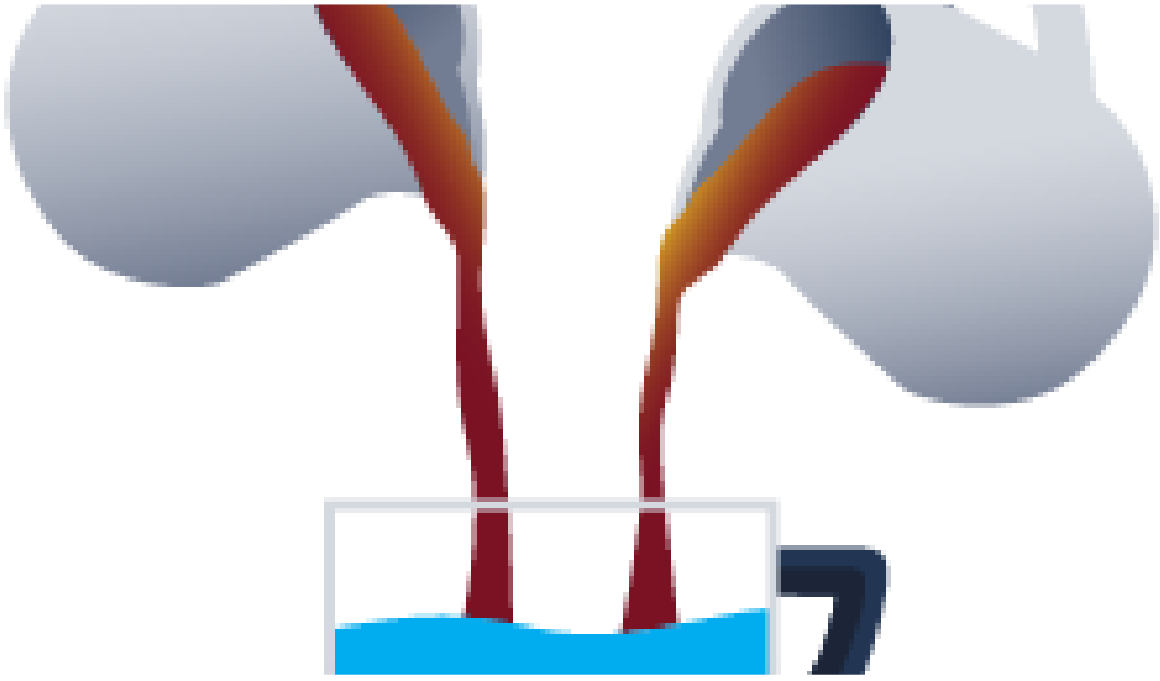
Nov 28, 2024 50

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

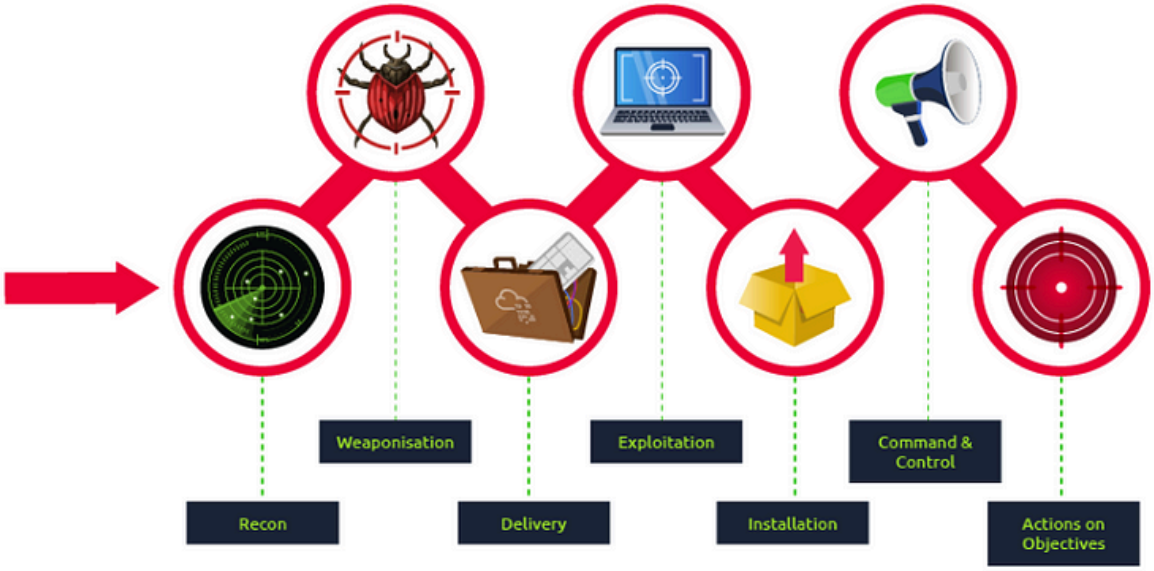


MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2



RosanaFSS

TryHackMe: Threat Hunting With YARA, detailed Write-up

This room focuses on using YARA for threat hunting.

Nov 26, 2024