

EX 10: INTRODUCTION TO ANTIVIRUS

AIM: To learn and understand about antivirus.

Problem:

The screenshot shows a web browser window with the URL `tryhackme.com/room/introtoav`. The page title is "Room completed (100%)". The content is a lesson on Antivirus (AV) software. It starts with a paragraph about functionalities and a link to "The Lay of the Land". The section "AV software in the past and present" describes the history of AV software, mentioning McAfee Associates, Inc. and the first AV software implementation in 1987. It then discusses modern AV software, its GUI, and its support for various operating systems and devices. The lesson concludes with a statement that AV features will be discussed in the next task. Below the text, there are three quiz questions, each with a text input field and a "Correct Answer" button.

functionalities) into one product to provide comprehensive protection against digital threats. For more information about Host-based security solutions, we suggest visiting the THM room: [The Lay of the Land](#).

AV software in the past and present

McAfee Associates, Inc. started the first AV software implementation in 1987. It was called "VirusScan," and its main goal at that time was to remove a virus named "Brain" that infected John McAfee's computer. Later, other companies joined in the battle against viruses. AV software was called scanners, and they were command-line software that searched for malicious patterns in files.

Since then, things have changed. AV software nowadays uses a Graphical User Interface (GUI) to perform scans for malicious files and other tasks. Malware programs have also expanded in scope and now target victims on Windows and other operating systems. Modern AV software supports most devices and platforms, including Windows, Linux, macOS, Android, and iOS. Modern AV software has improved and become more intelligent and sophisticated, as they pack a bundle of versatile features, including Antivirus, Anti-Exploit, Firewall, Encryption tool, etc.

We will be discussing some AV features in the next task.

Answer the questions below

What does AV mean?

Antivirus

✓ Correct Answer

Which PC Antivirus vendor implemented the first AV software on the market?

McAfee

✓ Correct Answer

Antivirus software is a ____-based security solution.

Host

✓ Correct Answer

tryhackme.com/room/introav Room completed (100%)

• Web requests

An emulator stops the execution of a file when enough artifacts are collected to detect malware.

Other common features

The following are some common features found in AV products:

- A self-protection driver to guard against malware attacking the actual AV.
- Firewall and network inspection functionality.
- Command-line and graphical interface tools.
- A daemon or service.
- A management console.

Answer the questions below

Which AV feature analyzes malware in a safe and isolated environment?

Emulator ✓ Correct Answer

An _____ feature is a process of restoring or decrypting the compressed executable files to the original.

unpacker ✓ Correct Answer

Read the above to proceed to the next task, where we discuss the AV detection techniques.

No answer needed ✓ Correct Answer

Task 4 ✓ Deploy the VM

tryhackme.com/room/introav Room completed (100%)

```
Loading: 0s, ETA: 0s [=====] 1/1 sigs
Compiling: 0s, ETA: 0s [=====] 40/40 tasks

C:\Users\thm\Desktop\Samples\AV-Check.exe: YARA.thm_demo_rule.UNOFFICIAL FOUND
C:\Users\thm\Desktop\Samples\backdoor1.exe: OK
C:\Users\thm\Desktop\Samples\backdoor2.exe: OK
C:\Users\thm\Desktop\Samples\elcar.com: OK
C:\Users\thm\Desktop\Samples\notes.txt: OK
```

The output shows we improved our Yara rule to reduce the false-positive results. That was a simple example of how AV software works. Thus, AV software vendors work hard to fight against malware and improve their products and database to enhance the performance and accuracy of results.

The drawback of the signature-based detection is that files will have a different hash value if the binary is modified. Therefore, it is easy for someone to bypass signature-based detection techniques if they know what AV software looks for and how to analyze binaries, as shown in later rooms.

Answer the questions below

What is the `sigtool` tool output to generate an MD5 of the `AV-Check.exe` binary?

f4a974b0cf25dca7fbce8701b7ab3a88:6144:AV-Check.exe ✓ Correct Answer ? Hint

Use the strings tool to list all human-readable strings of the AV-Check binary. What is the flag?

THM[Y0uC4nC-5tr16s] ✓ Correct Answer ? Hint

Task 6 ✓ Other Detection Techniques

Task 7 ✓ AV Testing and Fingerprinting

Result: Hence the experiment was completed successfully.