29% COMPLETE 85/287 Steps

Previous Topic

Next Topic >

500)1X



Management Principles

4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

- PA1) Introduction to Emails and Phishing
 - 7 Topics | 1 Quiz
- PA2) Types of Phishing Emails
 - 10 Topics | 2 Quizzes
- PA3) Tactics and Techniques Used
 - 12 Topics | 2 Quizzes
- PA4) Investigating a Phishing Email
 - 8 Topics | 2 Quizzes
 - Section Introduction, Investigating Emails
 - Artifacts We Need to Collect
 - Manual Collection Techniques Email
 - Manual Collection Techniques Web
 - ✓ Manual Collection Techniques Fil
 Artifacts
 - **⋖** [Video] Collecting Artifacts Manual
 - Automated Collection With PhishTool
 - **Solution** ✓ [Video] Collecting Artifacts Automated
 - Lab) Manual Artifact Extraction
 - Activity) End of Section Review,
- PA5) Analysing URLs, Attachments, and
 Antiferate
 - 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions
 - 12 Topics | 1 Quiz
- O PA7) Report Writing
- 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge
 - 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

- TI1) Introduction to Threat Intelligence
 - 7 Topics
- TI2) Threat Actors & APTs
 - 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence
 - 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence
 - 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence
 - 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns
 - 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

- DF1) Introduction to Digital Forensics
 - 5 Topics
- DF2) Forensics Fundamentals

Manual Collection Techniques - File Artifacts

Blue Team Level 1 Certification (Standard) > PA4) Investigating a Phishing Email > Manual Collecti...

COMPLETE

SBT

BLUE TEAM

LEVEL

1

We need to collect file hashes of malicious attachments to perform reputation checks and implement defensive measures. Hashes are the output of a hashing algorithm, such as MD5 (Message Digest 5) or SHA (Secure Hash Algorithm). These algorithms will produce a unique string that is used to represent the file. If there is a single change to the file, such as editing a text file and changing one character, the hash will be completely different. You can read more about hashes here.

HASHES VIA POWERSHELL

It's most likely that security analysts will be using the Windows OS for day-to-day work. File hashes can be retrieved using PowerShell with the get-filehash command. By default, this will generate a SHA256 hash.



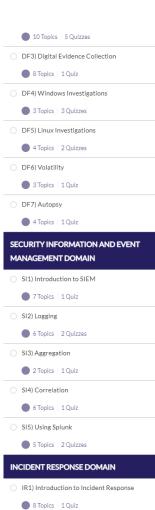
We can also retrieve MD5 and SHA1 hashes using the get-filehash command with the -Algorithm switch.



To make it easier, we can chain PowerShell commands using the; character and retrieve all three hash values at once.



HASHES VIA LINUX CLI



 $\label{prop:command-line} File \ has hes \ can \ be \ easily \ retrieved \ using \ the \ Linux \ command-line. \ The \ three \ commands \ we \ would \ use \ are;$

- sha256sum <file>
- sha1sum <file>
- md5sum <file>

```
reot@SBTLab2:-/Desktop  

root@SBTLab2:-/Desktop  

root@SBTLab2:-/Des
```

CONCLUSION

Whilst typically generating MD5 and SHA1 hashes are enough to perform reputation searches online and taking defensive measures within endpoint detection and response (EDR) platforms, some services such as Talos File Reputation require SHA256 hashes to perform checks against their databases. It's useful to know how to generate all three both in Windows and Linux.



Back to Lesson





rivacy & Cookies Policy