RR

# Bruteforce

Can you analyze logs from an attempted RDP bruteforce attack?

Grep Text Editor Excel

| Points | Difficulty | Solves | OS |
|---|---|---|---|
| 20 | Medium | 8635 | Windows/Linux |

| | | |
|---|---|---|
| Bruteforce.zip<br>110 KB | Password<br>BTLO | Download File |

| First-Blood | | Created By | |
|---|---|---|---|
| LonerVamp | 1357 days ago | BTLO | 1357 days ago |

## Recent Solves

| | | |
|---|---|---|
| RR | Rifko Satrio Rahmadani | Today |
| KK | Karta Kusuma | Today |
| | Tatang Bukhori | Today |
| WP | Welly Prasena | Today |
| RW | Rais Akbar Wibowo | Today |

## Scenario

Scenario

**Can you analyze logs from an attempted RDP bruteforce attack?**

One of our system administrators identified a large number of Audit Failure events in the Windows Security Event log.

There are a number of different ways to approach the analysis of these logs! Consider the suggested tools, but there are many others out there!

⚠ **Found an issue with this challenge? Click here to report it!**

## Challenge Submission

Question 1) How many Audit Failure events are there? (Format: Count of Events) *(3 points)*

Solved!

Question 2) What is the username of the local account that is being targeted? (Format: Username) *(2 points)*

Solved!

Question 3) What is the failure reason related to the Audit Failure logs? (Format: String) *(3 points)*

Solved!

Question 4) What is the Windows Event ID associated with these logon failures? (Format: ID) *(3 points)*

Solved!

Question 5) What is the source IP conducting this attack? (Format: X.X.X.X) *(3 points)*

Solved!

Question 6) What country is this IP address associated with? (Format: Country) *(3 points)*

Solved!

Question 7) What is the range of source ports that were used by the attacker to make these login requests? (LowestPort-HighestPort - Ex: 100-541) *(3 points)*

Solved!