


# EventID@234- SOC176 - RDP Brute Force Detected

## 1. Alert Overview

- **Event ID:** 234
- **Alert Time:** March 07, 2024 — 11:44 AM
- **Alert Rule:** SOC176 – RDP Brute Force Detected
- **Alert Level:** Security Analyst
- **Source IP:** 218[.]92[.]0[.]56
- **Destination IP:** 172[.]16[.]17[.]148
- **Destination Host:** Matthew
- **Protocol:** RDP (Port 3389)
- **Firewall Action:** Allowed
- **Alert Trigger Reason:** Login failure from a single source with different non-existing accounts

EventID :	234
Event Time :	Mar, 07, 2024, 11:44 AM
Rule :	SOC176 - RDP Brute Force Detected
Level :	Security Analyst
Source IP Address :	218.92.0.56
Destination IP Address :	172.16.17.148
Destination Hostname :	Matthew
Protocol :	RDP
Firewall Action :	Allowed
Alert Trigger Reason :	Login failure from a single source with different non existing accounts
Show Hint 	

## 2. Alert Summary

This alert indicates repeated failed RDP login attempts from a single IP address 218[.]92[.]0[.]56 to the internal host Matthew with IP Address 172[.]16[.]17[.]148 .

This behavior suggested that the attacker was attempting to gain unauthorized access through commonly used credentials to gain unauthorized access.

## 3. Investigation Steps

### Source Validation

- The external source IP address 218[.]92[.]0[.]56 indicates a potential security threat on the network.

8

/ 95

Community Score

-1

8/95 security vendors flagged this IP address as malicious

Reanalyze Similar More

218.92.0.56 (218.92.0.0/16)

CN

Last Analysis Date

4 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 32

Crowdsourced context

HIGH 0 MEDIUM 0 LOW 1 INFO 1 SUCCESS 0

SSH bruteforce Attackers [2023-09-20] - according to source ArcSight Threat Intelligence - 2 years ago

Source: alienvault VirusTotal Link: https://www.virustotal.com/gui/ip-address/218.92.0.56/detection Abuse IPDB Link: https://www.abuseipdb.com/check/218.92.0.56

Find more information on CrowdSec CTI - according to source CrowdSec - 1 year ago

Behaviors: SSH Bruteforce

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	ArcSight Threat Intelligence	Malware
BitDefender	Phishing	CyRadar	Malicious
Fortinet	Malware	G-Data	Phishing
Lionic	Malicious	Webroot	Malicious
AlphaSOC	Suspicious	Abusix	Clean

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Mar, 08, 2024, 02:33 PM	IP	218.92.0.56	Malicious	Anonymous

Log Correlation

- 15 login attempts from 218[.]92[.]0[.]56 to 172[.]16[.]17[.]148 with host named Mathew to port 3389.
- There was detected both failed and successful login events:
- This indicates a successful brute force attack.

New Search

Basic Pro

Source Address contains "218.92.0.56"

All Time

Q

30 events (before Mar, 07, 2024, 11:44 AM UTC)

< 1 2 3 >

< Hide Fields

INTERESTING FIELDS

type

source\_address

source\_port

destination\_address

destination\_port

time

raw\_log

Event

type OS

source\_address 218.92.0.56

source\_port 31245

destination\_address 172.16.17.148

destination\_port 3389

time Mar, 07, 2024, 11:44 AM

Raw Log

Username Matthew

EventID 4624(An account was successfully logged on.)

Logon Type 10(RemoteInteractive)

Source IP 218.92.0.56

Endpoint Analysis

- Endpoint logs shows that commands was executed after successful login event.

```
C:\Windows\system32\cmd.exe
whoami
net user letsdefend
```

```
net localgroup administrators
netstat -ano
```

Host Information

Hostname: Matthew

Domain: LetsDefend

IP Address: 172.16.17.148

Bit Level: 64

OS: Windows 10

Primary User: Matthew

Client/Server: Client

Last Login: Mar, 07, 2024, 04:00 AM

Action

Containment:

Host Contained

Processes 268

Network Action 28

>\_ Terminal History 5

Browser History 0

Results: 10

EVENT TIME

COMMAND LINE

Mar 7 2024 11:45:18

"C:\Windows\system32\cmd.exe"

Mar 7 2024 11:45:51

whoami

Mar 7 2024 11:45:58

net user letsdefend

Mar 7 2024 11:46:34

net localgroup administrators

Mar 7 2024 11:46:53

netstat -ano

- This indicates post-compromise reconnaissance activity.

## 4. Investigation Artifacts

- 218[.]92[.]0[.]56 - Source IP Address
- 172[.]16[.]17[.]148 - Destination IP Address
- Matthew - Destination Hostname

## 5. Response & Remediations

### Immediate Action

- **Action:** Isolated affected host ( Matthew ) from the network.
- **Reason:** Prevent lateral movement and data exfiltration.
- **Firewall:** Source IP blocked at the perimeter firewall.

### Recommended Next Step

- Reset and secure the compromise user account(**Matthew**).
- Enforce strong password policies.
- Implement Multi-Factor Authentication (MFA) for RDP access.
- Restrict RDP access to trusted VPN users or internal network only.
- Conduct full endpoints scan for persistence mechanisms and malicious binaries.
- Review other hosts for failed RDP login attempts from the same source.

## 8. MITRE ATT&CK Mapping

Tactic	Technique ID	Technique	Evidence
Initial Access	T1110	Brute Force	Multiple 4625 failures
Execution	T1059	Command-Line Interface	cmd.exe execution
Discovery	T1082	System Information Discovery	whoami , net user
Lateral Movement	T1021	Remote Services (RDP)	RDP login success

---

## 7. Lessons Learned

- Exposed RDP ports remain a major entry vector for brute-force attacks.
  - Lack of MFA and weak credential hygiene were key enabling factors.
  - IP reputation checks can rapidly validate external threats.
  - Regular auditing and log monitoring are crucial to detect brute-force behavior early.
-