

# Project: LetsDefend, Brute Force Attack

Clay Jones

## Objective:

A SIEM alert was received describing a brute force attack on an endpoint device. Trace back the artifacts from the log management, treat intel, and the endpoint security manager. Contain the endpoint device if affected.

## SIEM Alert:

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 	

## Log Discoveries:

▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=18845 destination_address=172.16.17.148 destination_port=3389 raw_log: {User...
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=51707 destination_address=172.16.17.148 destination_port=3389 raw_log: {User...
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=50807 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=24319 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=10098 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=41175 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=61506 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=27876 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
1 row selected	

▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=33376 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=31454 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=32029 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=52316 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=16578 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=15563 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=47364 destination_address=172.16.17.148 destination_port=3389 raw_log: {}
▼	[Mar, 07, 2024, 11:44 AM] source_address=218.92.0.56 source_port=22667 destination_address=172.16.17.148 destination_port=3389 raw_log: {User...

type	OS
source_address	218.92.0.56
source_port	51548
destination_address	172.16.17.148
destination_port	3389
time	Mar, 07, 2024, 11:44 AM
<b>Raw Log</b>	
Username	Matthew
EventID	4625(An account failed to log on)
Error Code	0xC000006A(user name is correct but the password is wrong)
Source IP	218.92.0.56

🔍	Event
Field	Value
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
<b>Raw Log</b>	
Username	Matthew
EventID	4624(An account was successfully logged on.)
Logon Type	10(RemoteInteractive)

After looking through the log manager, it was shown that multiple attempts were made to brute force into Matthew's account from port 3389. Eventually, the attacker was successfully able to log in after enough attempts.

### Host Contained:

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

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

Containment:

☒

Host Contained

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

Shown from the endpoint security manager, once the attacker gained access, they ran commands such as “whoami”, to confirm they were in, and “net localgroup administrators”, to add, create, or delete a local user group. After seeing such, this host was put in containment and the attacker’s IP was blacklisted and added to the threat intel feed.

### **Lessons Learned:**

To prevent this from happening again, I would strongly suggest:

- Multi Factor Authentication
- Strong password policy
  - Account lockout
- CAPTCHA Challenges
- Implement stronger hashing algorithm
  - IP Blacklist