Cybersecurity Lab: Active Directory Brute Force Detection Using Crowbar and Splunk

By: Scott Bartram

Overview

This project simulates a brute-force attack on an Active Directory environment using Crowbar and ART, with Splunk used for detection. The lab includes a Windows Server domain controller, Windows 10 clients, a Splunk server, and an attacker machine running Kali Linux.

Tools Used

- Windows Server
- Windows 10
- Kali Linux / Ubuntu
- Crowbar
- Splunk
- Sysmon
- Atomic Red Team

Lab Setup

- Configured Windows Server as a domain controller.
- Joined two Windows 10 clients to the domain.

- Deployed Splunk and configured it to receive logs on port 9997.
- Created two domain user accounts
    - Tsmith
    - Jsmith
- Enabled Sysmon on endpoints.
- Allowed RDP access on both clients.
- Analyzed alerts from authentication events and PowerShell activity.

Attack Simulation

- Used Crowbar on Kali Linux to perform an RDP brute-force attack.
    - Crowbar -b rdp -u tsmith -C rockyou.txt -s 192.168.10.100/32
- Used the rockyou.txt dictionary file to brute force user passwords.
- Used ART to maliciously create users using PowerShell.
    - Invoke-AtomicTest T1136.001
    - Invoke-AtomicTest T1059.001
- Monitored logs for alerts notifying failed login attempts as well as account creation.

SIEM Integration and Detection

Installed and configured the Splunk Universal Forwarder on Windows 10 endpoints.

Configured Splunk to listen on TCP port 9997.

Logs were ingested into an index named `endpoint`.

Detection was performed using:

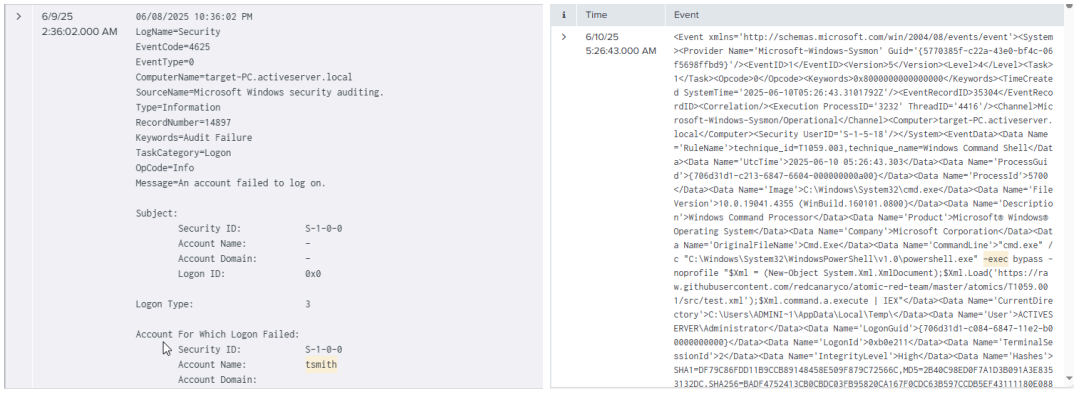
- index=endpoint tsmith
- index=endpoint NewLocalUser

Identified Event Codes:

- **4625**: Failed login attempts
- **4624**: Successful logins

These logs showed the RDP brute-force attempt, including failed access attempts and successful attempts.

Figure 1 & 2:



Analysis and Findings

I was able to get Splunk to successfully capture both login attempts and suspicious Powershell executions. One roadblock that I ran into while completing this lab was crowbar giving me failed RDP attempts. To fix this I went through settings of the users that I created and found they were not under the RDP access list. Throughout the completion of this lab I learned a lot about Splunk and ART.