PixelBreach

Brute Force Attack and Access Control Simulation

TTPR - Summer 2025

NYC Tech Talent Pipeline | Baruch COLLEGE

Team

Michael Schlichting Barbey - Offensive Security Engineer, Security Researcher

Justin Lui - Scrum Master, Security Analyst, Blue Team Engineer

Rabten Jangchup - Security Analyst, Blue Team Engineer

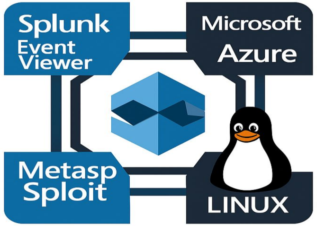
Tahanni Ahmed - System Admin, Documentation

Problem Statement

Goal - Our goal is to emulate a brute force attack & access system control through various vulnerability methods as we highlight the importance of security policies, strong passwords and firewall protection.

Problem Statement - Weak passwords, poor security policies, and inadequate firewall protection leave systems exposed to brute force attacks and unauthorized access. This project demonstrates how easily vulnerabilities can be exploited and emphasizes the need for stronger defenses to protect against outsider threats.

Technologies Used

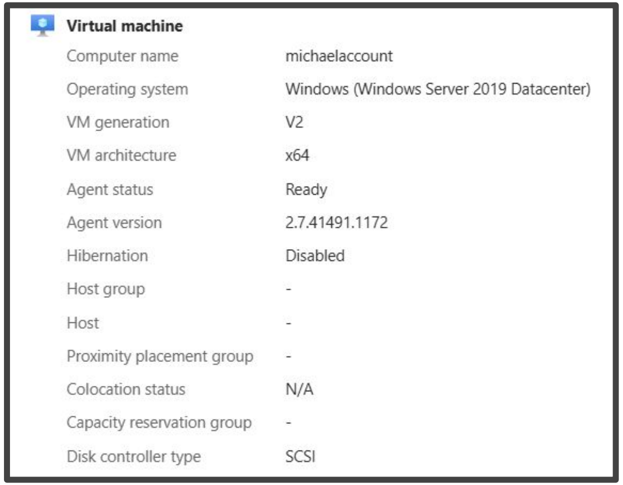


- **Event Viewer** - A Windows application designed to monitor and analyze security logs.
- **Paramiko** - A Python library that establishes a connection via SSH.
- **Metasploit** - Cybersecurity framework with vulnerability exploit tools.
- **Github -** Source control and script access.
- **Microsoft Azure** - Secure platform for deploying virtual machines for both the Blue Team and Red Team.
- **Splunk** - A tool utilized for analysis from Event Viewer logs and creates dashboards for visualization.

Design Process P1 – Deploying & Setup

1. Deploying VMs via Microsoft Azure
2. Enable "Successful" [4624] & "Failure" [4625] Event Logs

- Local Security Policy
  > Security Settings > Local Policies > Audit Policy
- Enable Audit Logon Events
- Enable Audit Account Logon Events



Virtual machine

Computer name	michaelaccount
Operating system	Windows (Windows Server 2019 Datacenter)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1172
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Design Process P2
Brute Force Attack – SSH Protocol

‘`findmy_password.py`’ is a web scraper that collects the 100 worst passwords (2017), and stores them locally to feed ‘`ssh_script.py`’ as a parameter.

‘`ssh_script.py`’ defines the ‘`ssh_brute_force()`’ function to import the modules from the paramiko library –

Design Process P2
Access Control – SMB – RDP Protocol

`metasploit-msfconsole`, a penetration testing framework, composed of an abundant system vulnerability library.

‘`download_image.py`’ is a python script delivered through the SMB exploit. The function is executed from the target’s powershell to scrape the web for the given link and download an image to the target’s Desktop.

Design Process P3
SPL (Search Processing Language) Analysis

Successful Logon

```
source="XmlWinEventLog:Security"

EventCode=4624

Logon_Type=8

host=michaelaccount

|

Table

_time

Source

EventCode

Logon_Type
```

Failed Logons

```
source="XmlWinEventLog:Security"

EventCode=4625

Logon_Type=8

host=michaelaccount

|

Table

_time

Source

EventCode

Logon_Type
```

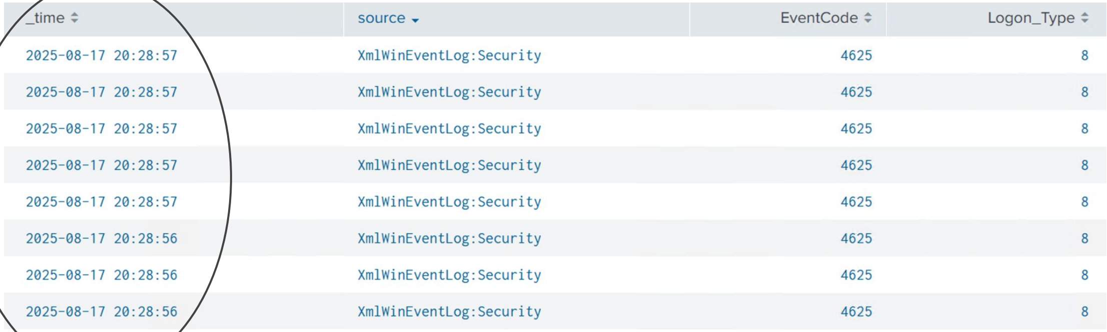
Windows Security Log Event Types
4624 - Successful Logon
4625 - Failed Logon

NetWorkClearText Logon
Credential exchange resembles
a cleartext network logon

Results

Several login attempts milliseconds apart

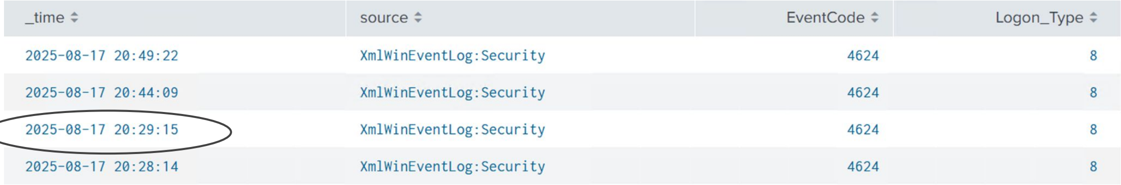
Failed Logins



_time	source	EventCode	Logon_Type
2025-08-17 20:28:57	XmlWinEventLog:Security	4625	8
2025-08-17 20:28:57	XmlWinEventLog:Security	4625	8
2025-08-17 20:28:57	XmlWinEventLog:Security	4625	8
2025-08-17 20:28:57	XmlWinEventLog:Security	4625	8
2025-08-17 20:28:57	XmlWinEventLog:Security	4625	8
2025-08-17 20:28:56	XmlWinEventLog:Security	4625	8
2025-08-17 20:28:56	XmlWinEventLog:Security	4625	8
2025-08-17 20:28:56	XmlWinEventLog:Security	4625	8

Eventual successful login after the spamed login attempts

Successful Logins

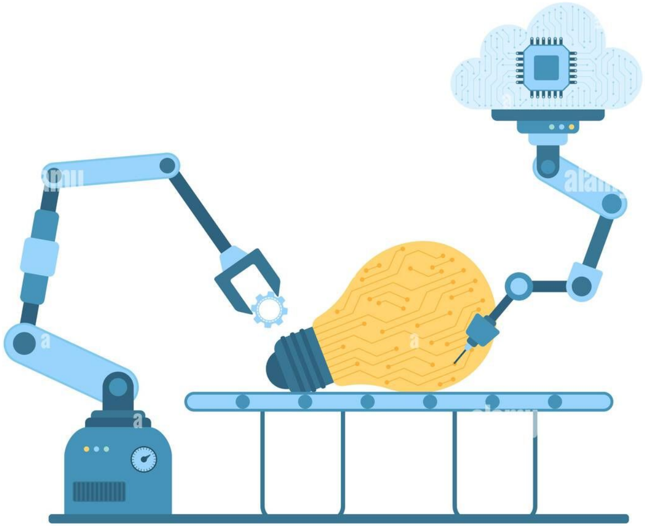


_time	source	EventCode	Logon_Type
2025-08-17 20:49:22	XmlWinEventLog:Security	4624	8
2025-08-17 20:44:09	XmlWinEventLog:Security	4624	8
2025-08-17 20:29:15	XmlWinEventLog:Security	4624	8
2025-08-17 20:28:14	XmlWinEventLog:Security	4624	8

Lessons Learned

How to defend against a brute force attack

- Password complexity
- Password Policies
- Proper Firewall setup



Connect With Us & QnA

Michael Schlichting Barbey

Justin Lui

Rabten Jangchup

Tahanni Ahmed