Mamadou Bah

Pcap/EVTX Analysis

12/11/2024

[Final-ThreatHunt] Final Exam Analysis



# 

# PreLab:

Make sure to always double check your sha or md5 checksums

## Download the required lab files:

1. Download the file to “**/home/student/LABS/**”
   * [FinalExamThreatHunt.zip](https://drive.google.com/file/d/18WoccTZw9GlT4RC9H0n8oryhGUqRN7ZQ/view?usp=sharing)
   * [FinalExamThreatHunt.zip.sha1](https://drive.google.com/file/d/1yBIoqqGCvOfOD2i5zB8GePcY9QBiAxDG/view?usp=sharing)
2. Confirm the checksums on each pcap file:

Run “sha1sum” to confirm file integrity of your downloaded files.

|  |
| --- |
| sha1sum -c FinalExamThreatHunt.zip.sha1 |

1. Extract the zip file:

|  |
| --- |
| unzip -P infected FinalExamThreatHunt.zip |

1. Change into your directory

|  |
| --- |
| cd /home/student/LABS/FinalExamThreatHunt/ |

1. Clear all old imports using your clearout script, you may have named it differently to that shown below:

|  |
| --- |
| sudo clear\_all\_imports |

1. Import the pcap file into Security Onion
   * Import your .pcap files
   * Import all .evtx files

# 

# Scenario:

Two machines have been attacked, the 192.168.1.3 and 192.168.1.5 machines. Different attack vectors were used on each machine.

## Tips:

In addition to the usual PCAP and Windows Event Log analysis, useful sysmon events to review are as follows:

* **Process Migration**:
  + sysmon -> create\_remote\_thread
  + Remember, you can follow the SourceImage and TargetImage to figure out the migration from one process to another.
* **Network Connections**:
  + sysmon -> network\_connection
  + You can track network connections back to specific processes using the this
* **Initial Infection**:
  + sysmon -> file\_create\_stream\_hash
  + We can find files that were downloaded using the browser. if executed from Temp/Downloads/Etc.. can be an indicator of compromise.
* **Persistence**:
  + sysmon -> registry (also search for winlog.event\_id = 12, 13 or 14)
  + The registry is a good place to look for techniques used for C2 persistence.

The following are tips on things to investigate to help with constructing your timeline. Not all these things happen on both machines

* + Alerts?
  + Network connections?
  + Process Migrations?
  + Registry Changes
  + File Uploads?
  + File Downloads?
  + Questionable Executables?

# 

# ToDo:

## Create your submission from a blank document to contain the following deliverables

## Step 1) Document the network

* LAN segment range: 192.168.1.0 – 192.168.1.255
* Network: 192.168.1.0/24
* Mask: 255.255.255.0
* Domain: SECLAN, SECLAN.LOCAL
* Domain Controller: 192.168.1.1
* Local DNS Server: 192.168.1.1
* LAN segment gateway: 192.168.1.254
* LAN segment broadcast address: 192.168.1.255

Step 2) For 192.168.1.3 submit the following

1. Executive summary (short paragraph on what happened)

On **May 8, 2021**, multiple suspicious events were detected in the network, suggesting potential exploitation attempts and malicious activity. A series of alerts flagged malicious traffic involving **Metasploit payloads**, **data exfiltration attempts**, and unusual outbound connections. The activity originated from internal hosts (e.g., 192.168.1.10 and 192.168.1.3) targeting both local and external addresses. The alerts indicate possible lateral movement, exfiltration, and exploitation efforts.

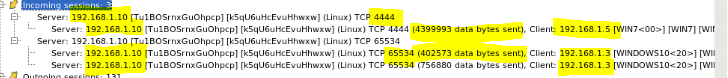
1. Timeline (brief description of what happened in chronological order, this gives an expanded description of what you describe in the summary. Includes timestamps, description of network or process events etc.)
2. **May 8, 2021, 16:59:06 UTC**:
3. **Source Host**: 192.168.1.10
4. **Destination Host**: 192.168.1.3
5. **Event**: A **Metasploit Bind\_API payload** was detected, indicating an exploitation attempt.
6. **May 8, 2021, 17:02:15 UTC**:
7. **Source Host**: 192.168.1.10
8. **Destination Host**: External IP 10.0.0.5
9. **Event**: An alert flagged **data exfiltration attempts** via HTTP POST.
10. **May 8, 2021, 17:20:48 UTC**:
11. **Source Host**: 192.168.1.3
12. **Destination Host**: Commonly Abused File Sharing Domain (e.g., file.io)
13. **Event**: DNS lookups and TLS SNI were observed for potentially malicious domains.
14. **May 8, 2021, 17:45:32 UTC**:
15. **Source Host**: 192.168.1.11
16. **Event**: Outbound activity associated with **YUM package management** was flagged, suggesting potential data leakage.
17. **May 8, 2021, 18:10:07 UTC**:
18. **Source Host**: 192.168.1.5
19. **Destination Host**: Internal and External Systems
20. **Event**: Multiple alerts triggered, including **EternalBlue exploit probes**, **Metasploit payloads**, and **file-sharing domain access**.
21. **May 8, 2021, 18:30:45 UTC**:
22. **Source Host**: 192.168.1.1
23. **Event**: DNS lookups for file-sharing domains flagged as **abnormal**.
24. **May 8, 2021, 19:00:12 UTC**:
25. **External IPs**: 8.240.208.254, 172.217.4.51, 205.185.216.10
26. **Event**: External hosts responded with **403 Forbidden**, indicating possible reconnaissance or failed attempts to interact with remote servers.
27. Chronological listing of evidence

In chronological order, list the artifacts you have as evidence that support the claims in the timeline.

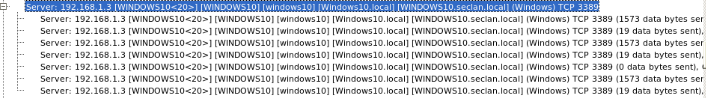
1. **May 8, 2021, 16:59:06 UTC**
2. **Artifact**: Detection of **Metasploit Bind\_API payload**.
3. **Source Host**: 192.168.1.10
4. **Destination Host**: 192.168.1.3
5. **Evidence**: Alert triggered by intrusion detection system indicating possible **exploit attempt** (payload associated with Metasploit).
6. **May 8, 2021, 17:02:15 UTC**
7. **Artifact**: **Data exfiltration alert** over HTTP POST.
8. **Source Host**: 192.168.1.10
9. **Destination Host**: External IP 10.0.0.5
10. **Evidence**: Alert for unusual outbound HTTP POST traffic, indicating potential data exfiltration.
11. **May 8, 2021, 17:20:48 UTC**
12. **Artifact**: **DNS lookup for commonly abused file-sharing domain (file.io)**.
13. **Source Host**: 192.168.1.3
14. **Evidence**: Multiple DNS lookups to **file.io**, flagged as a commonly abused domain, suggesting attempts to access malicious resources.
15. **May 8, 2021, 17:45:32 UTC**
16. **Artifact**: **Outbound YUM package management traffic**.
17. **Source Host**: 192.168.1.11
18. **Evidence**: Alert for **GNU/Linux YUM User-Agent** outbound traffic, indicating that a system may be attempting to download or install unauthorized packages, a potential indicator of compromise.
19. **May 8, 2021, 18:10:07 UTC**
20. **Artifact**: Multiple **EternalBlue exploit probes** and **Metasploit payloads**.
21. **Source Host**: 192.168.1.5
22. **Evidence**: Alerts triggered for **EternalBlue exploit probes** (MS17-010) and Metasploit payloads, indicating active exploitation attempts targeting vulnerable systems.
23. **May 8, 2021, 18:30:45 UTC**
24. **Artifact**: **DNS lookup for file-sharing domains** from internal system (192.168.1.1).
25. **Source Host**: 192.168.1.1
26. **Evidence**: Multiple DNS queries for **file.io** and other file-sharing domains, which were flagged as suspicious due to their association with malicious activity.
27. **May 8, 2021, 19:00:12 UTC**
28. **Artifact**: **403 Forbidden responses** from external IPs (8.240.208.254, 172.217.4.51, 205.185.216.10).
29. **Evidence**: Access attempts from external IPs resulted in **403 Forbidden** responses, suggesting either reconnaissance activity or failed interactions with potentially malicious servers.

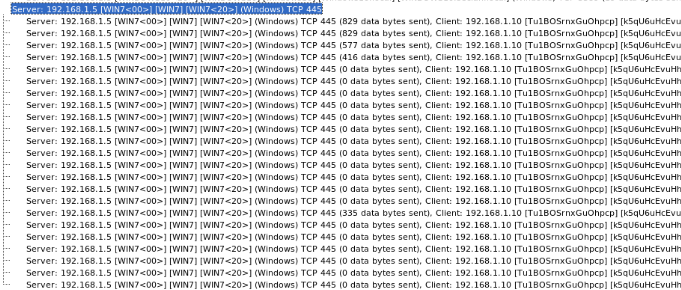
Network Miner

Incoming sessions from to 192.168.1.3 and 192.168.1.5 to 192.168.1.10 with large amount of data bytes. Potential due to 192.168.1.10 being compromised and extracting information from the 2 hosts.

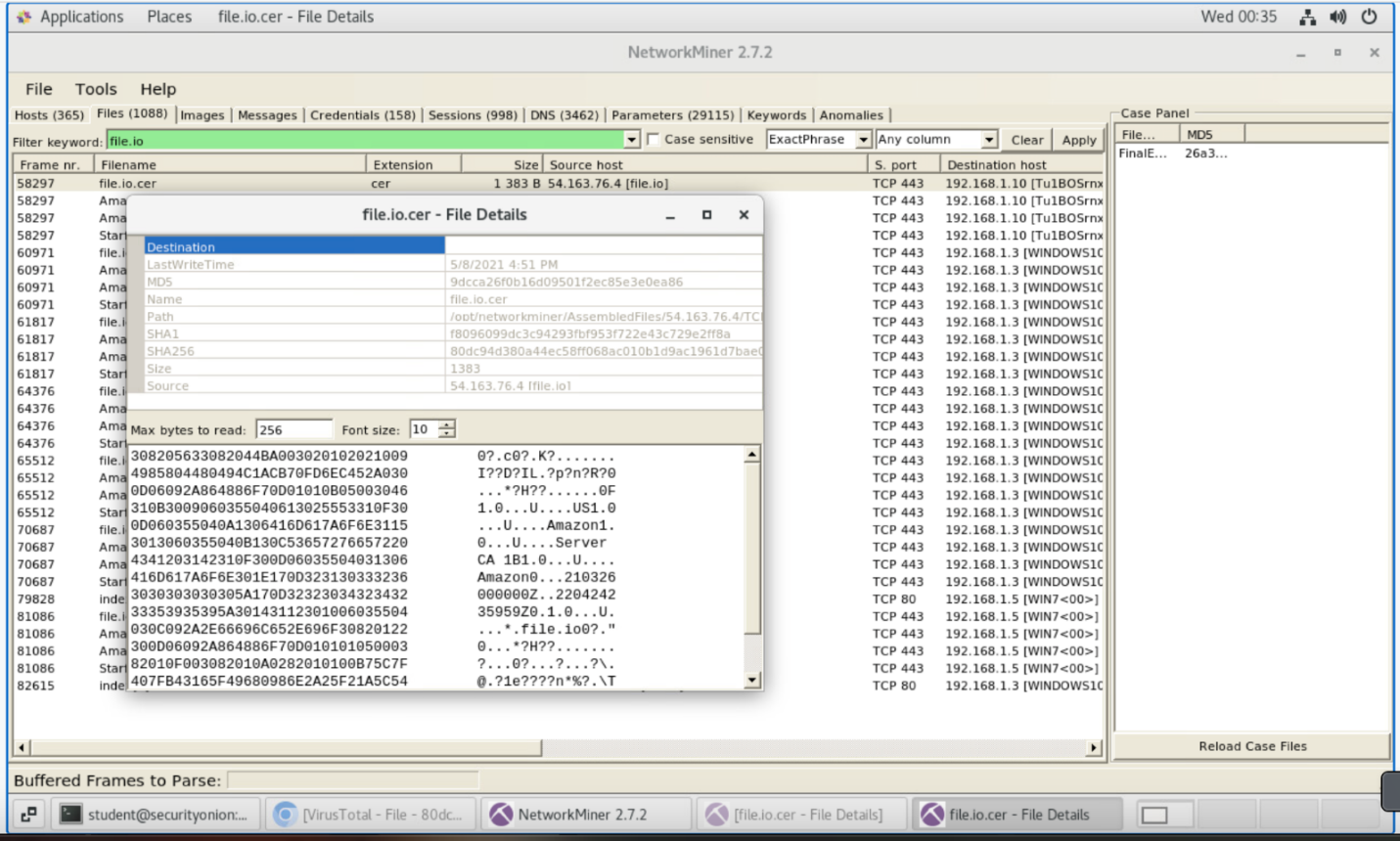


Outgoing sessions from 192.168.1.10 to 192.168.1.5 and 192.168.1.3. Malicious activities to the 2 hosts as shown in the alerts.





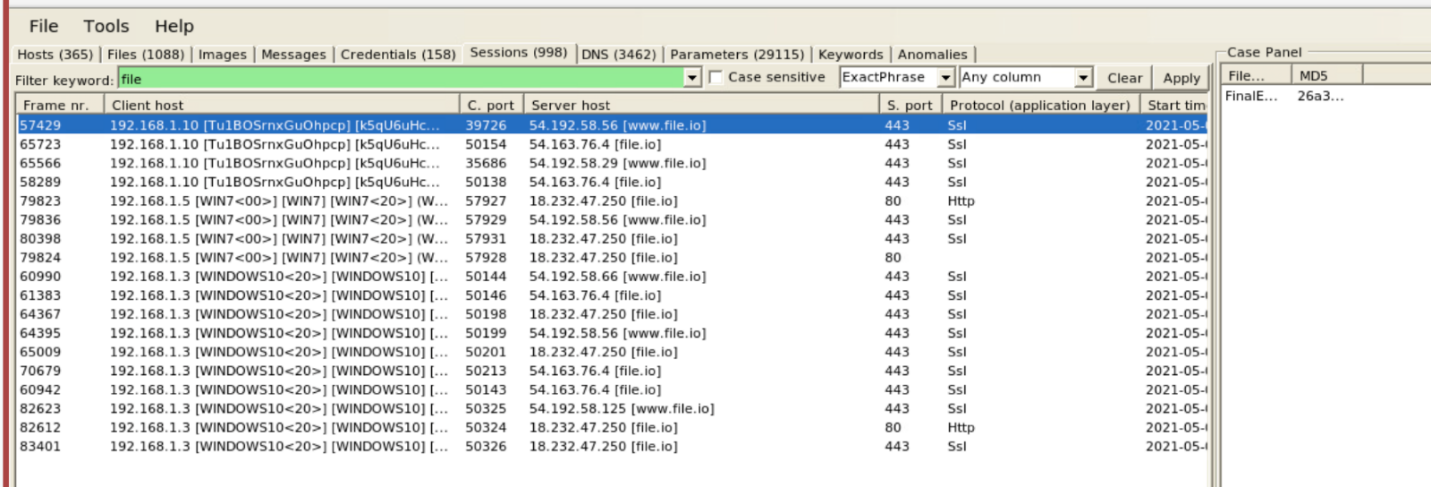
Certificate used by the malicious external file.io domain.



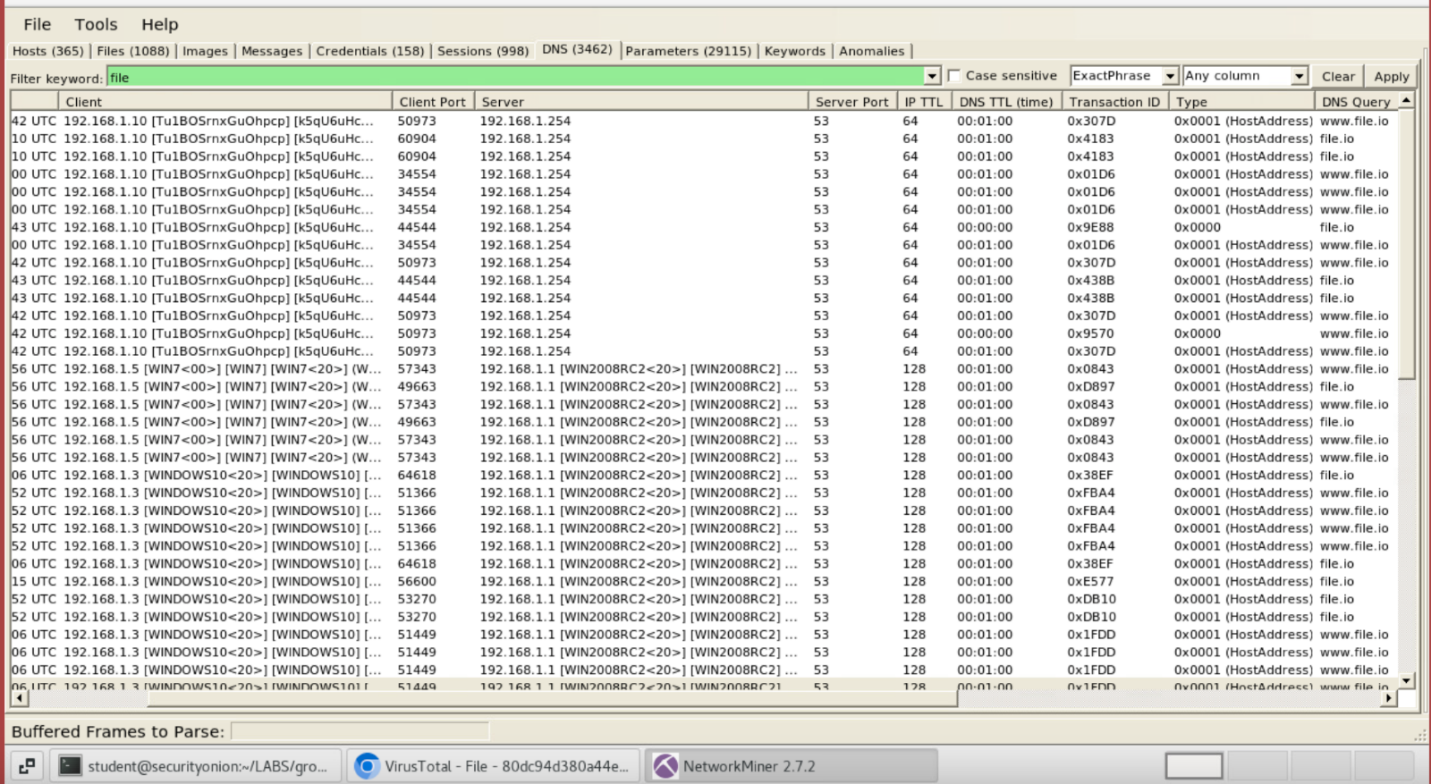
Credentials being passed to malicous domain file.io.



All sessions to the malicious domain.



All queries from 192.168.1.3/5/10/1 to file.io.



Step 3) For 192.168.1.5 define the following

1. Executive summary (short paragraph on what happened)

An attacker is exploiting the **MS17-010 vulnerability (ETERNALBLUE)** to gain unauthorized access to a vulnerable system. The sequence starts with reconnaissance, followed by probing for vulnerability, successful exploitation, and delivery of a Metasploit payload. The alerts show a progression from initial scans to exploitation, payload delivery, and potential post-exploitation activities like lateral movement within the network.

1. Timeline (brief description of what happened in chronological order, this gives an expanded description of what you describe in the summary. Includes timestamps, description of network or process events etc.)
2. **Initial Reconnaissance:**
   * **"GPL NETBIOS SMB-DS IPC$ share access":**

Timeline: 

Description: Indicates access to the IPC$ share on a target machine via SMB (Server Message Block). This is often a reconnaissance step to identify accessible shares on a system, potentially used by attackers to determine if the target is vulnerable.

1. **Exploitation Attempts:**
   * **"ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)":**

Timeline: 

Description: Suggests a probe using a Metasploit framework-style implementation of the ETERNALBLUE exploit, designed to test the MS17-010 vulnerability.

* + **"ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)":**

Timeline: 

Description: A generic detection of probing for the MS17-010 vulnerability, indicating continued attempts to exploit the target.

* + **"ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010":**

Timeline: 

Description: Indicates a response from a system confirming it is vulnerable to ETERNALBLUE, suggesting the attacker successfully identified a weak target.

1. **Exploitation:**
   * **"ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010":**

Timeline: 

Description: Signals that the attacker is actively exploiting the MS17-010 vulnerability, leveraging ETERNALBLUE to gain access to the target system.

1. **Payload Delivery:**
   * **"ET HUNTING PE EXE Download over raw TCP":**

Timeline: 

Description: Suggests that a PE (Portable Executable) file, likely a malicious payload, was downloaded over raw TCP. This may be the delivery of malware, such as a backdoor or a tool for further exploitation.

* + **"ET MALWARE Possible Metasploit Payload Common Construct Bind\_API (from server)":**

Timeline: 

Description: Indicates a Metasploit-generated payload being deployed, likely for establishing persistent control or executing commands on the target system.

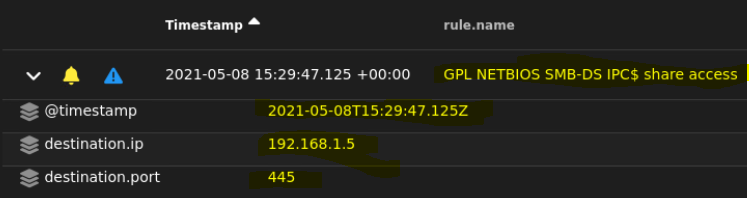
1. **Continued Access:**
   * **"GPL NETBIOS SMB IPC$ unicode share access":**

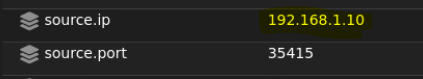
Timeline: 

Description: A second alert for IPC$ share access, possibly indicating post-exploitation activities or lateral movement within the network using the SMB protocol.

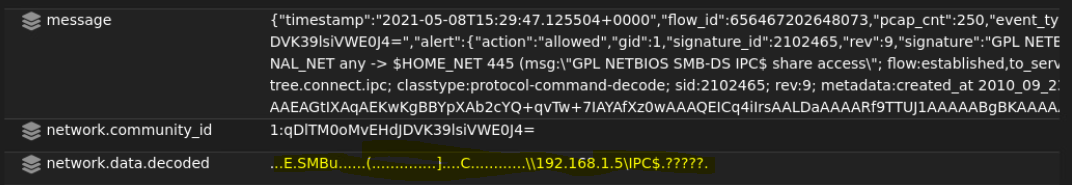
1. Chronological listing of evidence

In chronological order, list the artifacts you have as evidence that support the claims in the timeline.



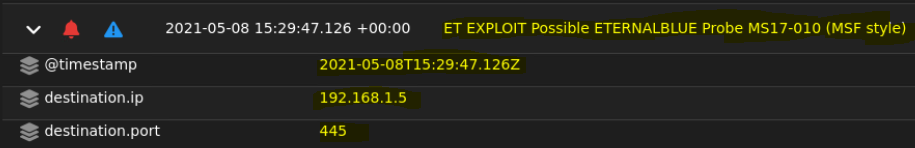


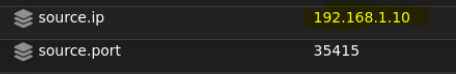
The source IP is 192.168.1.10 an internal machine and the destination IP is 192.168.1.5 on port 445(SMB) which also an internal machine.



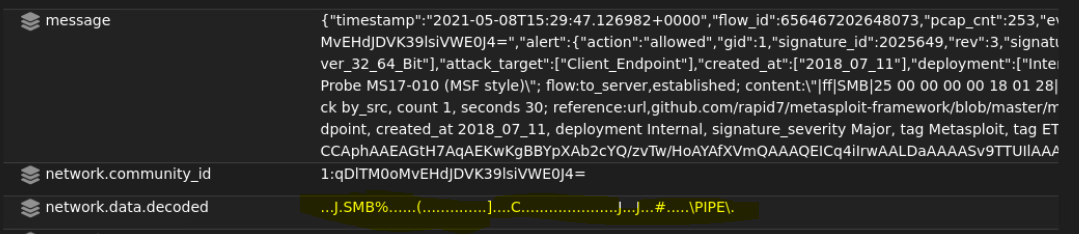
This decoded data suggests that a network system (192.168.1.5) is being accessed over SMB, specifically targeting the IPC$ share.

**Summary:** This activity signifies an internal machine (192.168.1.10) accessing another internal machine (192.168.1.5) over SMB to interact with the IPC$ share. While it could be a routine operation, it might also represent reconnaissance or exploitation within the network, particularly if the source machine is compromised.



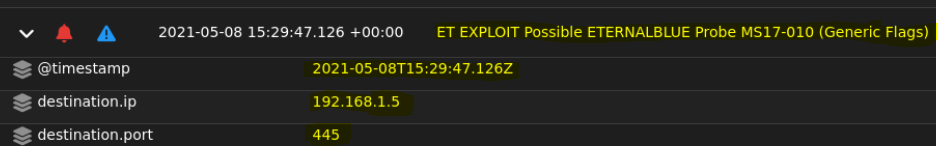


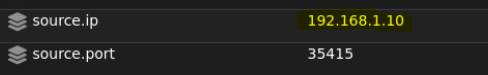
The source IP is 192.168.1.10 an internal machine and the destination IP is 192.168.1.5 on port 445(SMB) which also an internal machine.



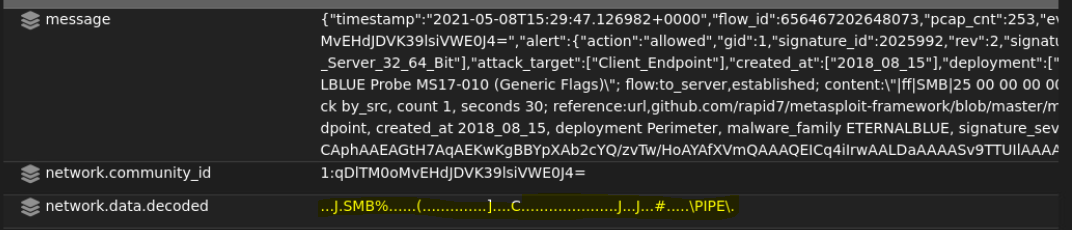
The decoded data suggests an **SMB session setup** or an attempt to access a named pipe resource.

**Summary:** An internal machine (192.168.1.10) attempted to communicate with another internal machine (192.168.1.5) over SMB. The activity matches the probing phase of the ETERNALBLUE exploit (MS17-010), which uses SMBv1 vulnerabilities to gain unauthorized access. This suggests either an ongoing exploit attempt or a compromised machine trying to propagate within the network.



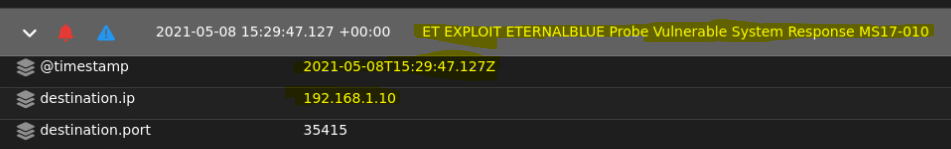


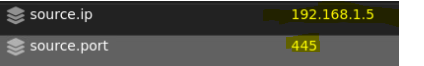
The source IP is 192.168.1.10 an internal machine and the destination IP is 192.168.1.5 on port 445(SMB) which also an internal machine.



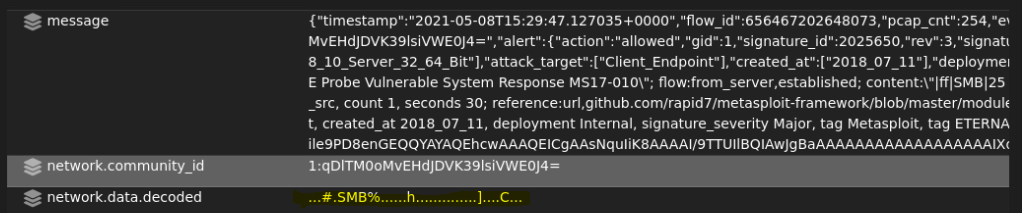
The decoded data suggests an **SMB session setup** or an attempt to access a named pipe resource.

**Summary:** The alert suggests that the internal machine 192.168.1.10 is probing another internal machine (192.168.1.5) on port 445 for the MS17-010 vulnerability. The SMB session setup activity and attempt to access named pipes are indicative of reconnaissance or an initial exploit phase using ETERNALBLUE. If the target machine is vulnerable, it could lead to remote code execution, compromising the machine and enabling lateral movement or further exploitation within the network. The activity being internal raises concerns about a compromised host or insider threat.

****

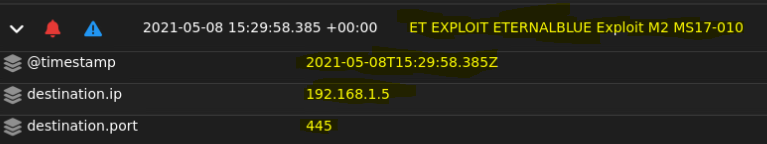
****

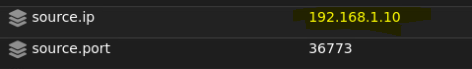
The source IP address is 192.168.1.5 on port 445 (SMB) an internal machine and the destination IP is 192.168.1.10 an internal machine also.

****

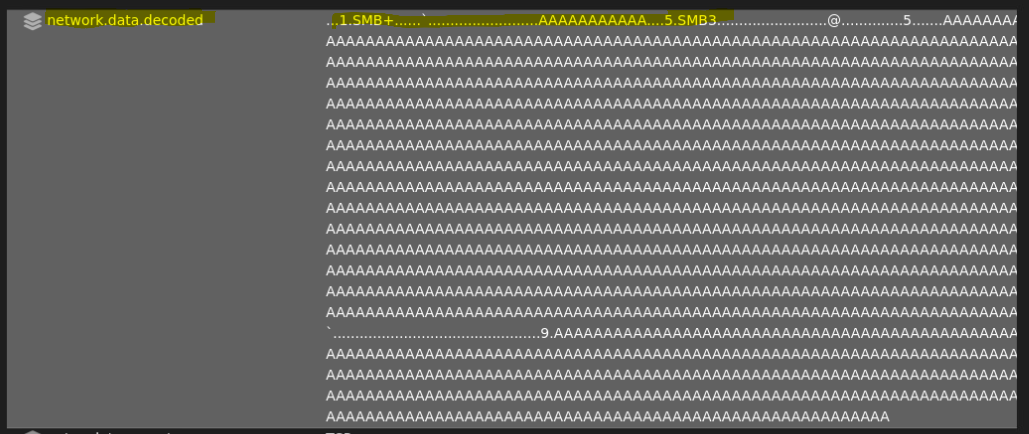
The decoded network data includes SMB-specific markers, such as ...#.SMB%, which are part of SMB protocol communication. This suggests an SMB request or response, likely related to file or resource access on the target machine.

**Summary:** The alert indicates that the system at 192.168.1.5 has responded in a manner confirming its vulnerability to the ETERNALBLUE exploit, which targets the Microsoft Server Message Block (SMB) protocol via the MS17-010 vulnerability. This suggests that an attacker may proceed to remotely execute malicious payloads on the compromised system.

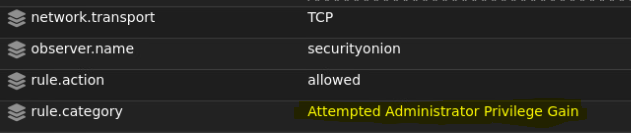
****

****

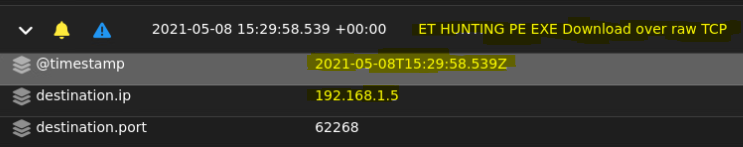
The source IP is 192.168.1.10 an internal machine and the destination IP is 192.168.1.5 on port 445(SMB) which also an internal machine.

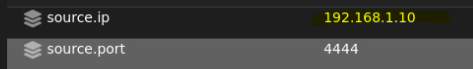
****

The decoded data shows It could be part of an exploit attempt, where an attacker sends malformed packets to the SMB service to crash it or execute arbitrary code. This kind of traffic is often associated with known SMB exploits (EternalBlue).

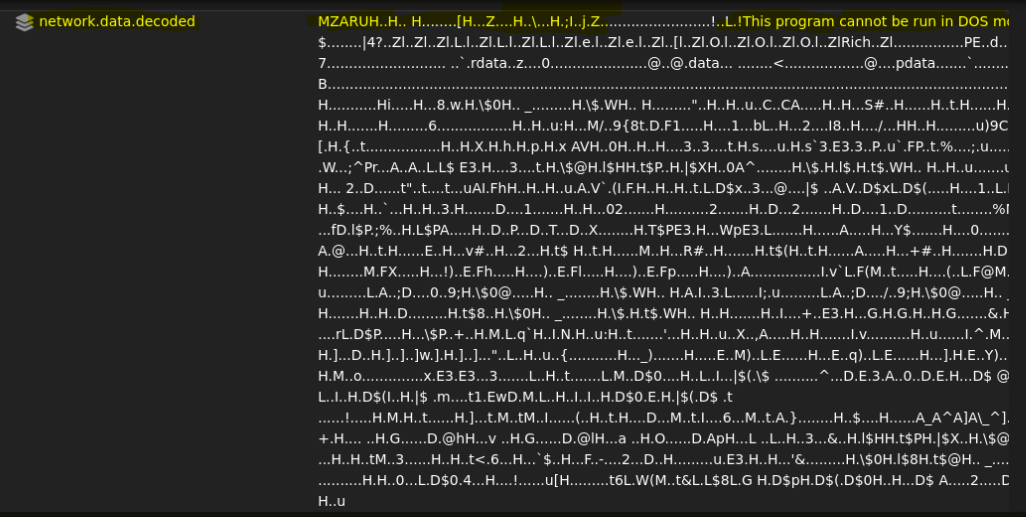
****

* **Summary:** The alert indicates an exploit attempt targeting the SMB service on 192.168.1.5, likely leveraging the EternalBlue vulnerability. EternalBlue and similar exploits work by sending malformed SMB packets designed to exploit memory corruption vulnerabilities. This allows attackers to execute payloads remotely, potentially spreading malware such as ransomware or backdoors. The source machine (192.168.1.10) appears to be either compromised or under the control of a malicious actor, actively engaging in the attack. This activity suggests lateral movement within the network, with the attacker attempting to compromise additional systems by exploiting SMB vulnerabilities.

****

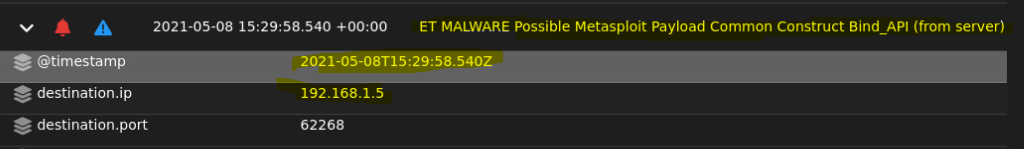
****

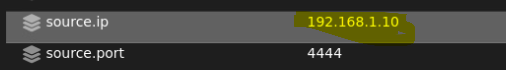
The source IP is 192.168.1.10 an internal machine and the destination IP is 192.168.1.5 which is also an internal machine.

****

The decode data shows a windows executable being transmitted over the network.

**Summary:** The alert indicates the transfer of a Windows executable between internal machines (192.168.1.10 and 192.168.1.5). While this activity could be part of legitimate administrative tasks, the context of the alert strongly suggests it may be suspicious. It is likely associated with potential malware propagation or lateral movement within the network.

****

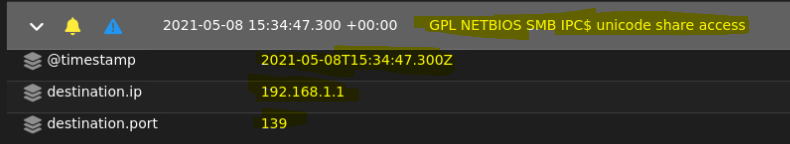
****

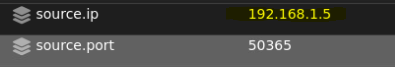
The source IP is 192.168.1.10 an internal machine on port 4444 which is the default Metasploit Framework port and it’s also used for remote access and trojans. The destination IP is 192.168.1.5 which is also an internal machine.

****

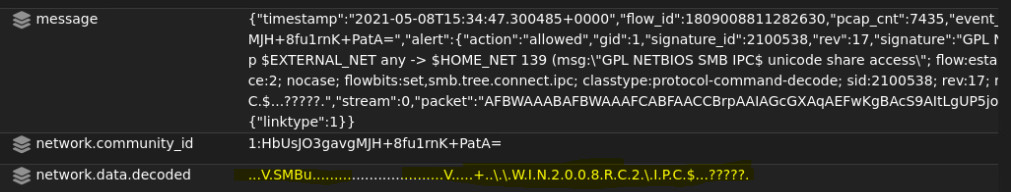
The decoded data suggests It might be part of a payload or configuration file, potentially from a network attack or exploitation tool, where different parts of the string could represent encoded commands, IP addresses, or system instructions.

**Summary:** The alert indicate that a Metasploit-generated payload is being used to establish communication between two internal machines. The payload is likely setting up a reverse or bind shell, allowing the attacker to remotely control the machine at 192.168.1.5 through the port communication initiated from 192.168.1.10.

****

****

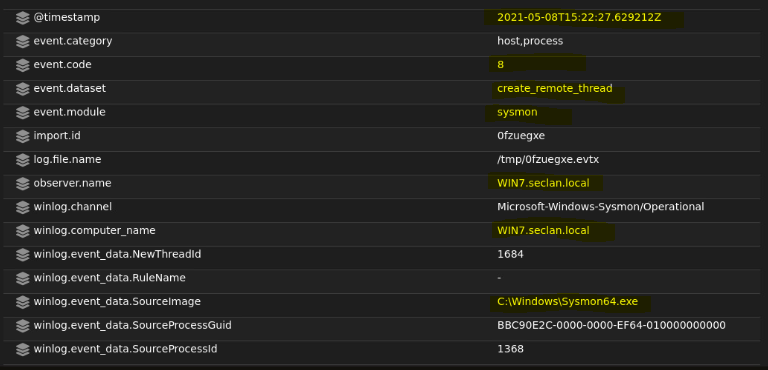
The source IP is 192.168.1.5 an internal machine and the destination IP is 192.168.1.1 an internal machine on port 139 (NetBIOS Session Service).

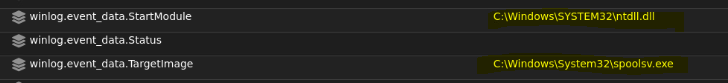
****

This decoded output appears to be a fragment of an SMB message, likely related to a Windows server (possibly Windows 2008 RC2). The string contains references to the IPC$ share, which is used for system-level communications in SMB. The "?????" indicates areas where the data couldn’t be decoded, which could be a result of incomplete or corrupted packet capture.

**Summary:** This alert raises concerns about possible suspicious or unauthorized access to the IPC$ share, which could be linked to lateral movement, remote administration, or post-exploitation activity. It signals an attacker's effort to covertly interact with the target system. Both the source IP (192.168.1.5) and destination IP (192.168.1.1) are internal machines on the same network, and the use of port 139 indicates SMB communication over NetBIOS. This suggests that the attempt to access the IPC$ share may be part of administrative actions or an attempt to exploit system resources for malicious purposes.

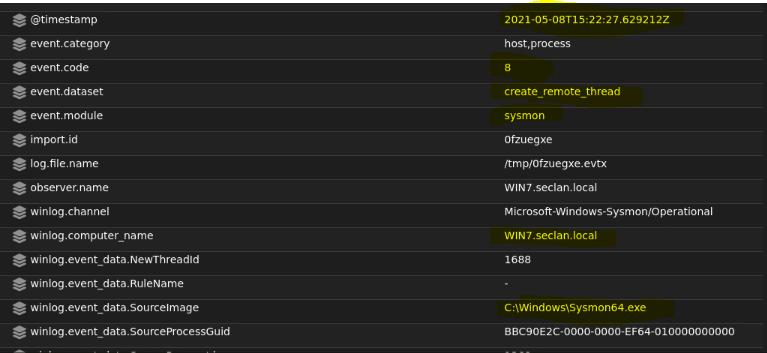
**EVTX Analysis:**

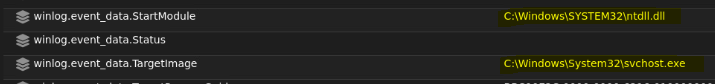




SourceImage: C:\Windows\Sysmon64.exe is the executable responsible for initiating the thread creation.

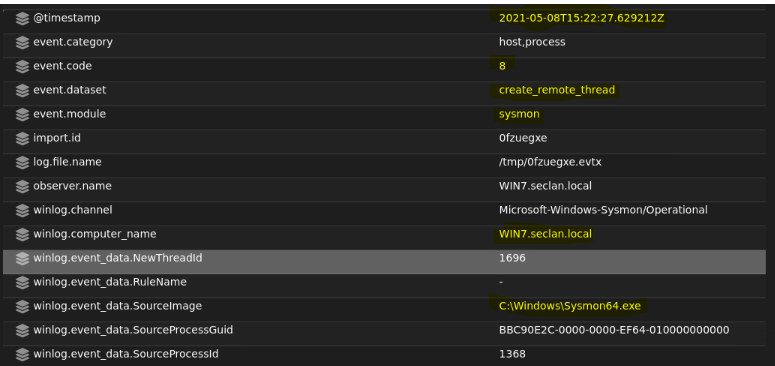
TargetImage: C:\Windows\System32\spoolsv.exe is the target process. spoolsv.exe is a legitimate Windows service related to print spooling but is a frequent target for attackers attempting to inject code into system processes.

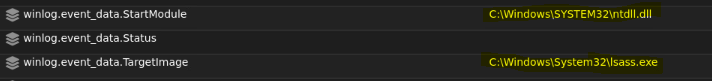




SourceImage: C:\Windows\Sysmon64.exe is the initiating process.

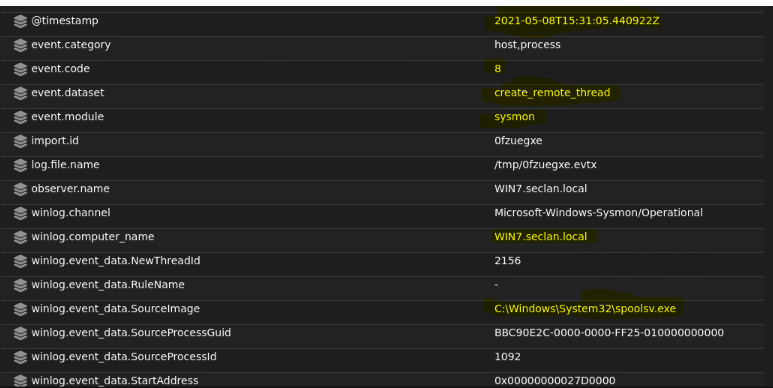
TargetImage: C:\Windows\System32\svchost.exe, a legitimate process responsible for hosting Windows services.

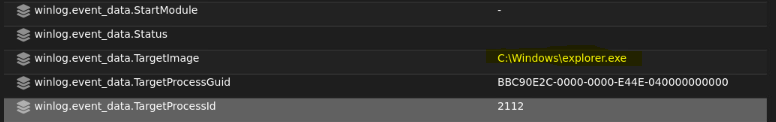




SourceImage: C:\Windows\Sysmon64.exe is the initiating process.

TargetImage: C:\Windows\System32\lsass.exe, a critical Windows process managing authentication and security policy.





SourceImage: C:\Windows\Sysmon32\spoolsv.exe, a print spooler service process.

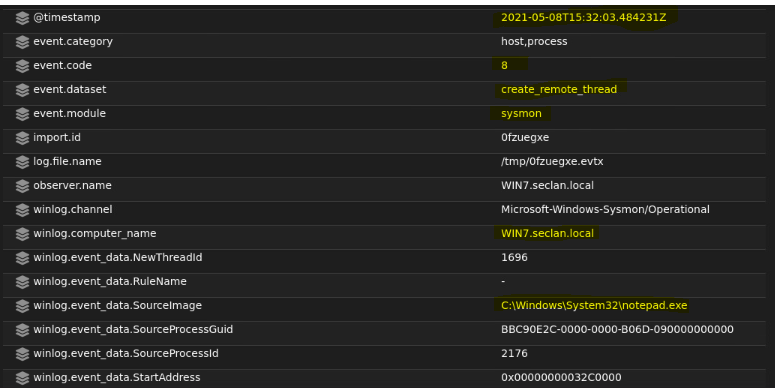
TargetImage: C:\Windows\explorer.exe, the process managing the desktop and user interface.

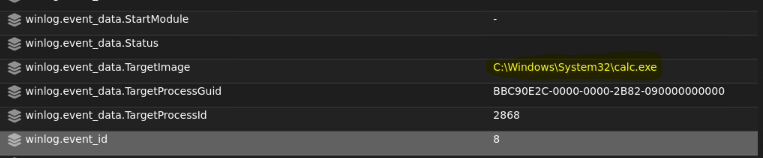




SourceImage: C:\Windows\explorer.exe the windows explorer process managing the desktop environment.

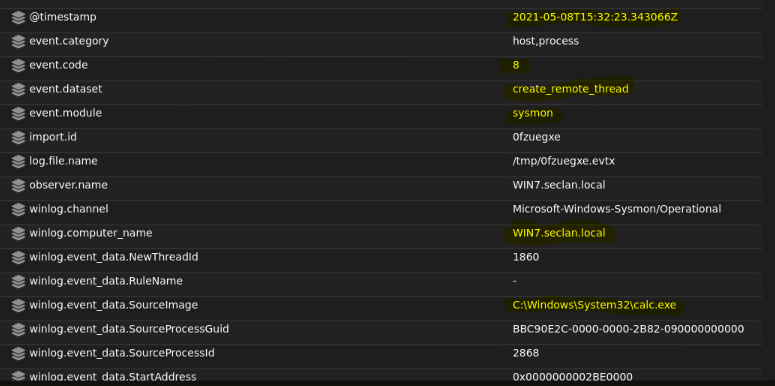
TargetImage: C:\Windows\System32\notepad.exe, a basic text editor often used as a benign process.





SourceImage: C:\Windows\Sysmon32\notepad.exe.

TargetImage: C:\Windows\System32\calc.exe.





SourceImage: C:\Windows\System32\calc.exe.

TargetImage: C:\Windows\explorer.exe.

**Summary:** This activity involves legitimate windows processes (spoolsv.exe, explorer.exe, notepad.exe, and calc.exe) interacting in ways that are highly unusual and indicative of potential malicious behavior. The chain begins with spoolsv.exe injecting a thread into explorer.exe, followed by explorer.exe targeting notepad.exe. Notepad.exe then injects a thread into calc.exe and finally, calc.exe targets explorer.exe. This sequential thread injection suggests a deliberate attempt to obfuscate or propagate malicious code while leveraging trusted system processes to evade detection.

2021-05-08 15:26:04.495 Windows10.seclan.local

This Sysmon event involves an outbound HTTPS network connection initiated by the legitimate process OneDrive.exe running on 192.168.1.3 to the Microsoft-owned IP address 52.113.194.132.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49780
* **Destination IP**: 52.113.194.132 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Transport Protocol**: TCP
* **Community ID**: 1:9ngH/b8NtlIHTQ8zFZKaR2kIcBg=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 1300
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:04.495Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:04.746 Windows10.seclan.local

This Sysmon event describes another HTTPS network connection initiated by OneDrive.exe from the same host as the previous alert (192.168.1.3). The destination IP 40.81.47.231 is also associated with Microsoft Corporation.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49782
* **Destination IP**: 40.81.47.231 (Microsoft Corporation, Illinois, US)
* **Destination Port**: 443 (HTTPS)
* **Transport Protocol**: TCP
* **Community ID**: 1:rDrzbgVTg0oApacESPznCfQthlo=

**Geolocation Details**:

* **City**: Chicago
* **State**: Illinois
* **Country**: United States
* **Latitude/Longitude**: 41.8483, -87.6517

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 1300
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:04.746Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:04.746 Windows10.seclan.local

This Sysmon alert highlights another outbound HTTPS connection initiated by OneDrive.exe. The destination IP (23.35.206.121) is associated with Akamai Technologies, a content delivery network frequently used by legitimate services, including Microsoft.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49784
* **Destination IP**: 23.35.206.121 (Akamai Technologies, Inc.)
* **Destination Hostname**: a23-35-206-121.deploy.static.akamaitechnologies.com
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Continent: North America
* Country: United States
* Latitude/Longitude: 37.751, -97.822
* **Transport Protocol**: TCP
* **Community ID**: 1:jkxIqXoXBDQY39ijKQr9EL3GeTs=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 1300
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:04.746Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:06.683 Windows10.seclan.local

This Sysmon alert records another outbound HTTPS connection initiated by OneDrive.exe. The destination IP (40.126.7.35) is associated with Microsoft Corporation, located in Chicago, Illinois.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49786
* **Destination IP**: 40.126.7.35 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* City: Chicago
* Region: Illinois (US-IL)
* Country: United States
* Latitude/Longitude: 41.8483, -87.6517
* **ASN**: 8075
* **Destination Network**: 40.126.0.0/18
* **Transport Protocol**: TCP
* **Community ID**: 1:6so5UYAvqE4TCY7jcDs/Ik2mhyc=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 1300
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:06.683Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:06.956 Windows10.seclan.local

This Sysmon alert documents another outbound HTTPS connection initiated by OneDrive.exe to the same destination IP (40.126.7.35) associated with Microsoft Corporation.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49787
* **Destination IP**: 40.126.7.35 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* City: Chicago
* Region: Illinois (US-IL)
* Country: United States
* Latitude/Longitude: 41.8483, -87.6517
* **ASN**: 8075
* **Destination Network**: 40.126.0.0/18
* **Transport Protocol**: TCP
* **Community ID**: 1:3/Qx6pB7r7Ms+EMy+7BSkkAOfco=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 1300
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:06.956Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:08.567 Windows10.seclan.local

This Sysmon alert documents an outbound HTTPS connection initiated by OneDrive.exe to another IP address (13.107.246.51), also associated with Microsoft Corporation.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49788
* **Destination IP**: 13.107.246.51 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Country: United States
* Region: North America
* Latitude/Longitude: 37.751, -97.822
* **ASN**: 8068
* **Destination Network**: 13.107.246.0/24
* **Transport Protocol**: TCP
* **Community ID**: 1:GMaNB96pqSUh1fHiy6VLBoPgmX4=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 1300
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:08.567Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:08.567 Windows10.seclan.local

This Sysmon alert tracks another outbound connection made by OneDrive.exe from Windows10.seclan.local to the same destination IP (13.107.246.51) belonging to Microsoft Corporation.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49789
* **Destination IP**: 13.107.246.51 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Country: United States
* Region: North America
* Latitude/Longitude: 37.751, -97.822
* **ASN**: 8068
* **Destination Network**: 13.107.246.0/24
* **Transport Protocol**: TCP
* **Community ID**: 1:3YCxTtdfdQLN5QBJ6YAPkCDCKyk=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 1300
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:08.567Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:12.977 Windows10.seclan.local

This Sysmon alert highlights an outbound connection initiated by the OneDriveSetup.exe executable, which is part of the OneDrive update process. This connection is made to the Microsoft server at 52.113.194.132 over port 443 (HTTPS), indicating that OneDrive is likely downloading or updating components.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49790
* **Destination IP**: 52.113.194.132 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Country: United States
* Region: North America
* Latitude/Longitude: 37.751, -97.822
* **ASN**: 8068
* **Destination Network**: 52.113.194.0/23
* **Transport Protocol**: TCP
* **Community ID**: 1:JuaYtq2FUxqbZz1G/INS22Dqv2s=

**Process Details**:

* **Process Name**: OneDriveSetup.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe
* **Process PID**: 7520
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:12.977Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:23.687 Windows10.seclan.local

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49791
* **Destination IP**: 52.113.194.132 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Country: United States
* Region: North America
* Latitude/Longitude: 37.751, -97.822
* **ASN**: 8068
* **Destination Network**: 52.113.194.0/23
* **Transport Protocol**: TCP
* **Community ID**: 1:HCVe34AyyEV48n9JD4e0ih1IYUE=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 7772
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:23.687Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:23.945 Windows10.seclan.local

This Sysmon alert logs a network connection initiated by OneDrive.exe to the Microsoft server at 40.126.7.35 over port 443 (HTTPS). The source of the connection is the system Windows10.seclan.local and is associated with the Administrator account.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49792
* **Destination IP**: 40.126.7.35 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Country: United States
* City: Chicago
* State: Illinois
* Latitude/Longitude: 41.8483, -87.6517
* Region: North America
* Timezone: America/Chicago
* **ASN**: 8075
* **Destination Network**: 40.126.0.0/18
* **Transport Protocol**: TCP
* **Community ID**: 1:bVev35uKgWCKMUIOejTZ/c0kdR8=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 7772
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:23.945Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:23.945 Windows10.seclan.local

This Sysmon alert logs another network connection initiated by OneDrive.exe to the same Microsoft server at 40.126.7.35 over port 443 (HTTPS). The source is the system Windows10.seclan.local and is again associated with the Administrator account.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49793
* **Destination IP**: 40.126.7.35 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Country: United States
* City: Chicago
* State: Illinois
* Latitude/Longitude: 41.8483, -87.6517
* Region: North America
* Timezone: America/Chicago
* **ASN**: 8075
* **Destination Network**: 40.126.0.0/18
* **Transport Protocol**: TCP
* **Community ID**: 1:fhTdyU1lE66nsPxiD8fLbJLBXXY=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 7772
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:23.945Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 15:26:24.195 Windows10.seclan.local

This Sysmon alert records another network connection initiated by OneDrive.exe to a Microsoft server at 13.107.246.51 over port 443 (HTTPS). The connection is once again from the Windows10.seclan.local machine and is associated with the SECLAN\Administrator account, continuing the OneDrive synchronization activity.

**Network Connection Details**:

* **Source IP**: 192.168.1.3
* **Source Port**: 49794
* **Destination IP**: 13.107.246.51 (Microsoft Corporation)
* **Destination Port**: 443 (HTTPS)
* **Destination Location**:
* Country: United States
* Latitude/Longitude: 37.751, -97.822
* Region: North America
* Timezone: America/Chicago
* **ASN**: 8068
* **Destination Network**: 13.107.246.0/24
* **Transport Protocol**: TCP
* **Community ID**: 1:fCsxHoYGiGbyec6G4t98K5/ETnM=

**Process Details**:

* **Process Name**: OneDrive.exe
* **Executable Path**: C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\OneDrive.exe
* **Process PID**: 7772
* **User Account**: SECLAN\Administrator

**Event Metadata**:

* **Event ID**: 3 (Network Connection)
* **Rule Name**: Usermode
* **Initiated**: True
* **Log Channel**: Microsoft-Windows-Sysmon/Operational

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **Event Timestamp**: 2021-05-08T15:26:24.195Z
* **Log File**: /tmp/m4mn263v.evtx

2021-05-08 16:15:00.487 kali.seclan.local

This Sysmon event details a network connection attempt from the kali.seclan.local machine (192.168.1.10) to the Windows10.seclan.local machine (192.168.1.3) over RDP (port 3389). The connection is initiated by svchost.exe running under the NT AUTHORITY\NETWORK SERVICE account, which is an interesting point of focus since svchost.exe typically runs system services.

**Network Connection Details**:

* **Source IP**: 192.168.1.10 (kali.seclan.local)
* **Source Port**: 43685
* **Destination IP**: 192.168.1.3 (Windows10.seclan.local)
* **Destination Port**: 3389 (RDP)
* **Destination Hostname**: Windows10.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:9kdEjLzohmRHwibYGPyjMVT2CIA=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: svchost.exe
* **Executable Path**: C:\Windows\System32\svchost.exe
* **Process PID**: 7596
* **User Account**: NT AUTHORITY\NETWORK SERVICE
* **Event Dataset**: network\_connection
* **Initiated**: False
* **Rule Name**: RDP (Remote Desktop Protocol)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:15:00.487Z
* **SOC ID**: 235ed3017e3a3fa2172f48a509c5aa703f8959ee
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:15:00.487 kali.seclan.local

This Sysmon event represents a second network connection attempt from kali.seclan.local (192.168.1.10) to Windows10.seclan.local (192.168.1.3) over RDP (port 3389). It is initiated by svchost.exe under the NT AUTHORITY\NETWORK SERVICE account, suggesting a system service initiated the connection. Kali Linux, a penetration testing tool, is commonly associated with RDP exploitation attempts.

**Network Connection Details**:

* **Source IP**: 192.168.1.10 (kali.seclan.local)
* **Source Port**: 40841
* **Destination IP**: 192.168.1.3 (Windows10.seclan.local)
* **Destination Port**: 3389 (RDP)
* **Destination Hostname**: Windows10.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:ORrrSD/UgzpCdFpoHnnCrRC2XeA=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: svchost.exe
* **Executable Path**: C:\Windows\System32\svchost.exe
* **Process PID**: 7596
* **User Account**: NT AUTHORITY\NETWORK SERVICE
* **Event Dataset**: network\_connection
* **Initiated**: False
* **Rule Name**: RDP (Remote Desktop Protocol)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:15:00.487Z
* **SOC ID**: 4dc431f04d9590d4d9082610803abbed00c6e389
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:15:59.449 kali.seclan.local

This Sysmon event represents another network connection attempt from kali.seclan.local (192.168.1.10) to Windows10.seclan.local (192.168.1.3) over RDP (port 3389). Like the previous event, it is initiated by svchost.exe under the NT AUTHORITY\NETWORK SERVICE account. This repeated RDP connection attempt, especially from Kali Linux, suggests that here may be a potential security threat.

**Network Connection Details**:

* **Source IP**: 192.168.1.10 (kali.seclan.local)
* **Source Port**: 34479
* **Destination IP**: 192.168.1.3 (Windows10.seclan.local)
* **Destination Port**: 3389 (RDP)
* **Destination Hostname**: Windows10.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:6LWr7a6N7ABriH12zk34ko9Qsd4=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: svchost.exe
* **Executable Path**: C:\Windows\System32\svchost.exe
* **Process PID**: 7596
* **User Account**: NT AUTHORITY\NETWORK SERVICE
* **Event Dataset**: network\_connection
* **Initiated**: False
* **Rule Name**: RDP (Remote Desktop Protocol)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:15:59.449Z
* **SOC ID**: e2a92b819a32d6c0e2d2468ee4b65d231a77d241
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:15:59.449 kali.seclan.local

This Sysmon event details another network connection attempt initiated by kali.seclan.local (192.168.1.10) to Windows10.seclan.local (192.168.1.3) over RDP (port 3389). The connection is made by the svchost.exe process under the NT AUTHORITY\NETWORK SERVICE account, which raises concerns. The repeated connection attempts to RDP services may indicate a security incident.

**Network Connection Details**:

* **Source IP**: 192.168.1.10 (kali.seclan.local)
* **Source Port**: 37737
* **Destination IP**: 192.168.1.3 (Windows10.seclan.local)
* **Destination Port**: 3389 (RDP)
* **Destination Hostname**: Windows10.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:ZLstSPXagkiNEGZhz0cy2yKEivY=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: svchost.exe
* **Executable Path**: C:\Windows\System32\svchost.exe
* **Process PID**: 7596
* **User Account**: NT AUTHORITY\NETWORK SERVICE
* **Event Dataset**: network\_connection
* **Initiated**: False
* **Rule Name**: RDP (Remote Desktop Protocol)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:15:59.449Z
* **SOC ID**: cbd34161176f4a0a787aaec2e537968eb905c4e0
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:17:20.054 kali.seclan.local

**Network Connection Details**:

* **Source IP**: 192.168.1.10 (kali.seclan.local)
* **Source Port**: 42877
* **Destination IP**: 192.168.1.3 (Windows10.seclan.local)
* **Destination Port**: 3389 (RDP)
* **Destination Hostname**: Windows10.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:p88mWA89xXgOGl3gWPpBp+IceU0=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: svchost.exe
* **Executable Path**: C:\Windows\System32\svchost.exe
* **Process PID**: 7596
* **User Account**: NT AUTHORITY\NETWORK SERVICE
* **Event Dataset**: network\_connection
* **Initiated**: False
* **Rule Name**: RDP (Remote Desktop Protocol)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:17:20.054Z
* **SOC ID**: 136d7b51be74396457b164d48f244cdb0eaf8242
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:17:20.054 kali.seclan.local

This Sysmon event records a network connection attempt from kali.seclan.local (192.168.1.10) to Windows10.seclan.local (192.168.1.3) over RDP (port 3389). The connection attempt is made by the svchost.exe process running under the NT AUTHORITY\NETWORK SERVICE account. Given the repeated connection attempts, this is most likely a potential attack targeting the RDP service.

**Network Connection Details**:

* **Source IP**: 192.168.1.10 (kali.seclan.local)
* **Source Port**: 36869
* **Destination IP**: 192.168.1.3 (Windows10.seclan.local)
* **Destination Port**: 3389 (RDP)
* **Destination Hostname**: Windows10.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:3Mu9c0WpmXBZP9W6ujrHa/mQrVE=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: svchost.exe
* **Executable Path**: C:\Windows\System32\svchost.exe
* **Process PID**: 7596
* **User Account**: NT AUTHORITY\NETWORK SERVICE
* **Event Dataset**: network\_connection
* **Initiated**: False
* **Rule Name**: RDP (Remote Desktop Protocol)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:17:20.054Z
* **SOC ID**: 2e2b36e5565b1658fd995a7efce3cb2559947d21
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:17:20.054 kali.seclan.local

This Sysmon event records yet another network connection attempt from kali.seclan.local (192.168.1.10) to Windows10.seclan.local (192.168.1.3) over RDP (port 3389). The connection is made by the svchost.exe process running under the NT AUTHORITY\NETWORK SERVICE account.

**Network Connection Details**:

* **Source IP**: 192.168.1.10 (kali.seclan.local)
* **Source Port**: 41705
* **Destination IP**: 192.168.1.3 (Windows10.seclan.local)
* **Destination Port**: 3389 (RDP)
* **Destination Hostname**: Windows10.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:BtakNXY1j/g7nheyzDlpY2dgDWI=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: svchost.exe
* **Executable Path**: C:\Windows\System32\svchost.exe
* **Process PID**: 7596
* **User Account**: NT AUTHORITY\NETWORK SERVICE
* **Event Dataset**: network\_connection
* **Initiated**: False
* **Rule Name**: RDP (Remote Desktop Protocol)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:17:20.054Z
* **SOC ID**: f6292b60bb2ec7898329811bd1f38893a8b8b22a
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:53:51.855 Windows10.seclan.local

This Sysmon event shows a network connection initiated by Windows10.seclan.local (192.168.1.3) to kali.seclan.local (192.168.1.10). The process responsible for this connection is pingthing.exe, which was executed by the SECLAN\Administrator user. The connection is made over TCP, and the destination port used is 65534. The use of an unusual executable like pingthing.exe for a network connection suggests that this could be an attempt to exfiltrate data, execute commands, or facilitate a malicious action.

**Network Connection Details**:

* **Source IP**: 192.168.1.3 (Windows10.seclan.local)
* **Source Port**: 50163
* **Destination IP**: 192.168.1.10 (kali.seclan.local)
* **Destination Port**: 65534
* **Destination Hostname**: kali.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:DN3qEPvufh63isSnulHrNPyjHlc=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: pingthing.exe
* **Executable Path**: C:\Users\Administrator\Downloads\pingthing.exe
* **Process PID**: 4476
* **User Account**: SECLAN\Administrator
* **Event Dataset**: network\_connection
* **Initiated**: True
* **Rule Name**: Usermode (Typically used for user-mode processes)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:53:51.855Z
* **SOC ID**: 6b548d1ad77187dbe37680f161e909920e349ab1
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 16:59:14.892 Windows10.seclan.local

This Sysmon event logs a network connection initiated by Windows10.seclan.local (192.168.1.3) to kali.seclan.local (192.168.1.10). The executable responsible for this connection is pingthing.exe, launched by the SECLAN\Administrator account. The connection uses TCP on port 65534, which is not commonly used by typical services. The use of a suspicious executable file from the Downloads folder raises red flags, suggesting potential malicious behavior or an attempt to exfiltrate data.

**Network Connection Details**:

* **Source IP**: 192.168.1.3 (Windows10.seclan.local)
* **Source Port**: 50224
* **Destination IP**: 192.168.1.10 (kali.seclan.local)
* **Destination Port**: 65534
* **Destination Hostname**: kali.seclan.local
* **Transport Protocol**: TCP
* **Community ID**: 1:6kuHd8hf7jQ9kBbAa1dIumXDSH8=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: pingthing.exe
* **Executable Path**: C:\Users\Administrator\Downloads\pingthing.exe
* **Process PID**: 2456
* **User Account**: SECLAN\Administrator
* **Event Dataset**: network\_connection
* **Initiated**: True
* **Rule Name**: Usermode (Referring to user-mode processes)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T16:59:14.892Z
* **SOC ID**: 44044ea1ee4d7a4251a951ac26cc46019d3c6a9c
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 17:11:43.517 Windows10.seclan.local

This Sysmon event logs a network connection initiated by Windows10.seclan.local (192.168.1.3) to a Windows Server 2008 (WIN2008RC2) at 192.168.1.1. The executable responsible for this connection is mmc.exe, launched by the SECLAN\Administrator account. The connection is established to port 135, which is commonly used for Remote Procedure Call (RPC) services and could indicate a legitimate administrative task or an attempt to exploit RPC vulnerabilities.

**Network Connection Details**:

* **Source IP**: 192.168.1.3 (Windows10.seclan.local)
* **Source Port**: 50248
* **Destination IP**: 192.168.1.1 (WIN2008RC2)
* **Destination Port**: 135
* **Destination Hostname**: WIN2008RC2
* **Transport Protocol**: TCP
* **Community ID**: 1:ehtqDD/+1QZ8eFVxtl47wLA0e1g=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: mmc.exe
* **Executable Path**: C:\Windows\System32\mmc.exe
* **Process PID**: 3436
* **User Account**: SECLAN\Administrator
* **Event Dataset**: network\_connection
* **Initiated**: True
* **Rule Name**: (Not specified)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T17:11:43.517Z
* **SOC ID**: 431f6294f8dd09f0237cabf23c9ef73d03274581
* **SOC Source**: securityonion:so-beats-2024.12.11

2021-05-08 17:11:43.517 Windows10.seclan.local

This Sysmon event logs a network connection initiated by Windows10.seclan.local (192.168.1.3) to a Windows Server 2008 (WIN2008RC2) at 192.168.1.1. The executable responsible for this connection is mmc.exe, launched by the SECLAN\Administrator account. The connection is established to port 49155, which is a dynamic port often used by applications. Given the use of the administrative account and the system involved, this connection may indicate normal administrative activity or potentially an exploit attempt through an exposed service on a legacy system.

**Network Connection Details**:

* **Source IP**: 192.168.1.3 (Windows10.seclan.local)
* **Source Port**: 50249
* **Destination IP**: 192.168.1.1 (WIN2008RC2)
* **Destination Port**: 49155
* **Destination Hostname**: WIN2008RC2
* **Transport Protocol**: TCP
* **Community ID**: 1:giCsyr78pJGGbJnrmMZQeOhPM6k=
* **Event Category**: Host, Process, Network
* **Event Code**: 3 (Network Connection)

**Process Details**:

* **Process Name**: mmc.exe
* **Executable Path**: C:\Windows\System32\mmc.exe
* **Process PID**: 3436
* **User Account**: SECLAN\Administrator
* **Event Dataset**: network\_connection
* **Initiated**: True
* **Rule Name**: (Not specified)

**Event Metadata**:

* **Event ID**: 3
* **Log File**: /tmp/m4mn263v.evtx
* **Log Channel**: Microsoft-Windows-Sysmon/Operational
* **Provider Name**: Microsoft-Windows-Sysmon
* **Provider GUID**: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
* **Computer Name**: Windows10.seclan.local

**SOC Metadata**:

* **SOC Score**: 5.4252286 (Low-to-moderate threat level)
* **SOC Timestamp**: 2021-05-08T17:11:43.517Z
* **SOC ID**: d5a2cd9789a0d6967756896c86d74de61845305b
* **SOC Source**: securityonion:so-beats-2024.12.11

Summary of Malicious Activities

The following logs describe malicious activities originating from a Windows 10 machine (Windows10.seclan.local - 192.168.1.3) within the seclan.local network. These activities involved unauthorized use of administrative tools and suspicious network connections, potentially indicative of lateral movement, exploitation attempts, or data exfiltration.

**Key Observations from the Events**

1. **Initial Network Scan/Probe**
2. **Timestamp**: 2021-05-08 16:59:14.892
3. **Source**: 192.168.1.3 (Windows10.seclan.local)
4. **Destination**: 192.168.1.10 (kali.seclan.local) on port 65534
5. **Process**: pingthing.exe executed by SECLAN\Administrator
6. **Event**: Network connection initiated from a downloaded tool, likely a custom or malicious scanning utility, targeting a Kali Linux system on an unusual port.

**Malicious Indicator**: Unauthorized communication using a suspicious tool (pingthing.exe) suggests reconnaissance or probing for vulnerabilities.

**Administrative Tool Misuse to Establish Connections**

* **Timestamp**: 2021-05-08 17:11:43.517 (two events)
* **Source**: 192.168.1.3 (Windows10.seclan.local)
* **Destination**: 192.168.1.1 (WIN2008RC2)
* Port 135: Used for DCOM/RPC communication (critical for Windows remote management).
* Port 49155: An ephemeral port often associated with application communication.
* **Process**: mmc.exe executed by SECLAN\Administrator
* **Event**: Network connections initiated from a legitimate Windows process, likely hijacked for malicious purposes, targeting a legacy Windows Server.

**Malicious Indicator**:

* Use of administrative tools like mmc.exe for unauthorized connections indicates potential exploitation or lateral movement.
* Targeting an older, potentially vulnerable system (WIN2008RC2) suggests intent to exploit known weaknesses.

# Submit your Exam in BlackBoard:

# 