Official incident report

Event ID: 71

Rule Name: SOC134 - Suspicious WMI Activity

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: https://www.linkedin.com/in/ahmed-mansour-5631b5323/

Github link: https://github.com/AhmedMansour93

Table of contents

Event Details

Event ID:
71

Event Date and Time:
Mar, 07, 2021, 04:50 PM

Rule:
SOC134 - Suspicious WMI Activity

Level:
Security Analyst

Hostname:
Desktop-Anderson

File Name:
exec.bat

File Hash:
50459310eded4c520ab5c9e3626a9300

File Size:
52.00 B

Device Action:
Allowed

Network Information Details

Destination IP Address:
204.79.197.203 external

Source IP Address:
172.16.17.54 internal

Destination IP Address: • 204.79.197.203 (External)

- This is a public IP address, indicating traffic from outside your organization's internal network. The destination IP suggests that the internal device is attempting to communicate with an external service or server. Depending on the context, this connection could represent legitimate access or a potential security concern.

Source IP Address: • 172.16.17.54 (Internal)

- This IP address is part of your organization's private IP range (172.16.0.0 to 172.31.255.255), indicating it belongs to a device within your local network. The internal device with this address is initiating the communication, which means the activity is originating from within your environment.

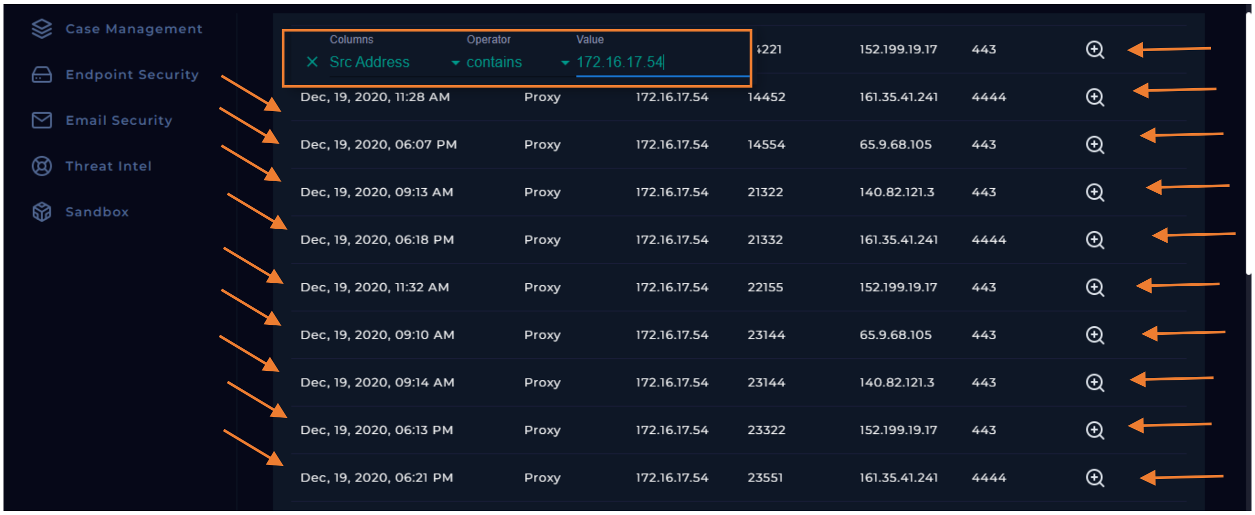
- ## The attack is external

Analysis:

Log Management

We'll proceed by entering the Source IP address and reviewing the results. Based on the time and date of the attack.

Please refer to the attached image for further details regarding the attack.



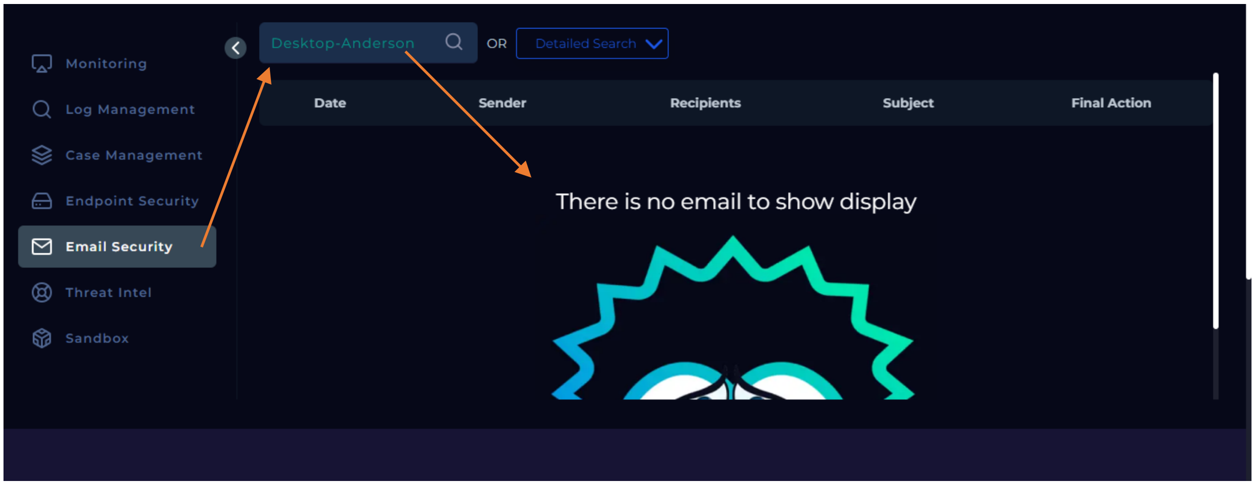
Columns: Src Address
Operator: contains
Value: 172.16.17.54

			221	152.199.19.17	443	⊕
Dec, 19, 2020, 11:28 AM	Proxy	172.16.17.54	14452	161.35.41.241	4444	⊕
Dec, 19, 2020, 06:07 PM	Proxy	172.16.17.54	14554	65.9.68.105	443	⊕
Dec, 19, 2020, 09:13 AM	Proxy	172.16.17.54	21322	140.82.121.3	443	⊕
Dec, 19, 2020, 06:18 PM	Proxy	172.16.17.54	21332	161.35.41.241	4444	⊕
Dec, 19, 2020, 11:32 AM	Proxy	172.16.17.54	22155	152.199.19.17	443	⊕
Dec, 19, 2020, 09:10 AM	Proxy	172.16.17.54	23144	65.9.68.105	443	⊕
Dec, 19, 2020, 09:14 AM	Proxy	172.16.17.54	23144	140.82.121.3	443	⊕
Dec, 19, 2020, 06:13 PM	Proxy	172.16.17.54	23322	152.199.19.17	443	⊕
Dec, 19, 2020, 06:21 PM	Proxy	172.16.17.54	23551	161.35.41.241	4444	⊕

0 Logs records for the Source IP regarding to our alert date and time.

All logs have been completely wiped, indicating that the attacker cleared all traces after executing the attack. This suggests a deliberate attempt to cover their tracks and avoid detection, making post-incident analysis and forensic investigation more challenging. "Check the attached photo".

Email Security:



Desktop-Anderson

Date	Sender	Recipients	Subject	Final Action

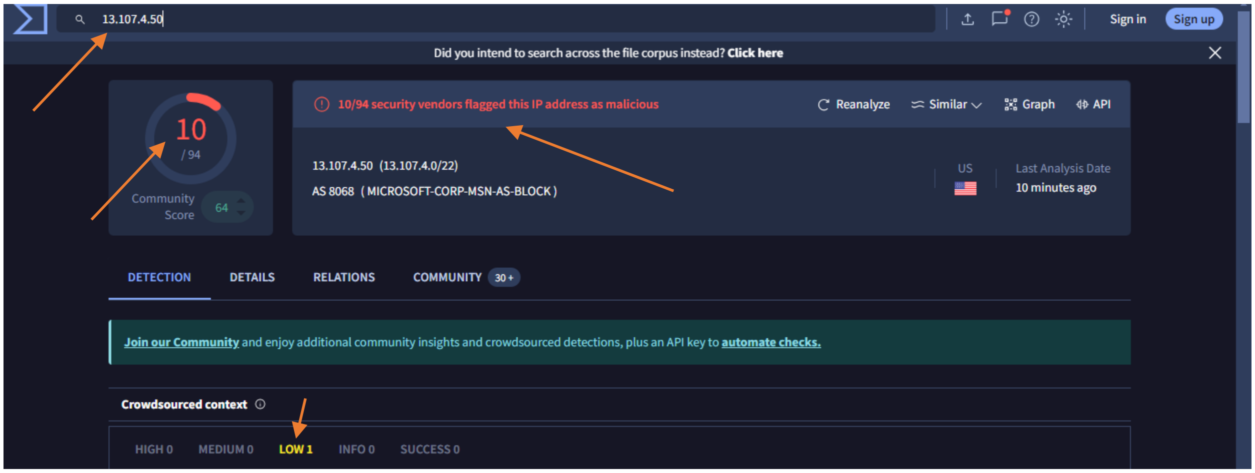
There is no email to show display

I conducted a thorough check by entering the hostname into the email security system to verify whether the attack was premeditated. The results showed no prior associations or activity, and the email in question was empty. Based on this analysis, there is no indication that the attack was planned in advance, suggesting it was likely opportunistic rather than a targeted campaign.

Detection:

Threat Intelligence Results

We will conduct a comprehensive scan of the Destination IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



Did you intend to search across the file corpus instead? **Click here**

10 / 94

Community Score 64

10/94 security vendors flagged this IP address as malicious

13.107.4.50 (13.107.4.0/22)

AS 8068 (MICROSOFT-CORP-MSN-AS-BLOCK)

US

Last Analysis Date 10 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 0 MEDIUM 0 LOW 1 INFO 0 SUCCESS 0

VirusTotal Results for Attacker IP: 204.79.197.203

VirusTotal analysis of the source IP address 204.79.197.203 reveals that 3 out of 94 security vendors have flagged this IP as malicious. The detections include the following:

• CRDF: Malicious

• Criminal IP: Malicious

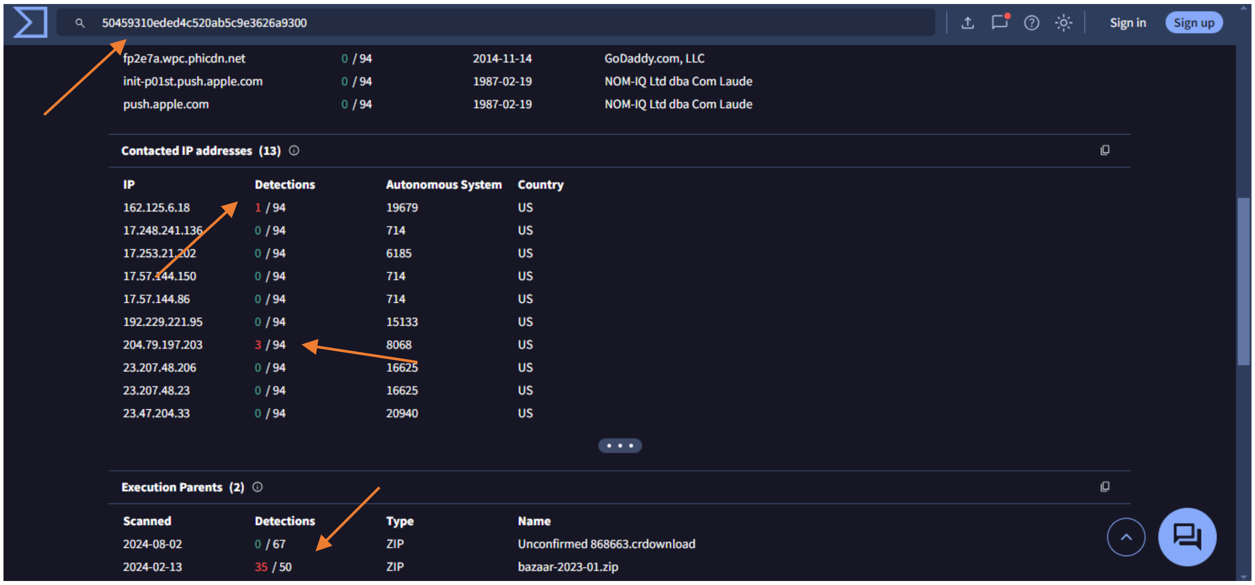
• G-Data: Malware

This indicates a lower level of concern regarding the potential threat posed by this IP address compared to higher detection rates.

Reference result.

- ## The Traffic is Malicious

We will conduct a comprehensive scan File Hash using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



fp2e7a.wpc.phicdn.net	0 / 94	2014-11-14	GoDaddy.com, LLC
init-p01st.push.apple.com	0 / 94	1987-02-19	NOM-IQ Ltd dba Com Laude
push.apple.com	0 / 94	1987-02-19	NOM-IQ Ltd dba Com Laude

Contacted IP addresses (13)

IP	Detections	Autonomous System	Country
162.125.6.18	1 / 94	19679	US
17.248.241.136	0 / 94	714	US
17.253.21.202	0 / 94	6185	US
17.57.144.150	0 / 94	714	US
17.57.144.86	0 / 94	714	US
192.229.221.95	0 / 94	15133	US
204.79.197.203	3 / 94	8068	US
23.207.48.206	0 / 94	16625	US
23.207.48.23	0 / 94	16625	US
23.47.204.33	0 / 94	20940	US

Execution Parents (2)

Scanned	Detections	Type	Name
2024-08-02	0 / 67	ZIP	Unconfirmed 868663.crdownload
2024-02-13	35 / 50	ZIP	bazaar-2023-01.zip

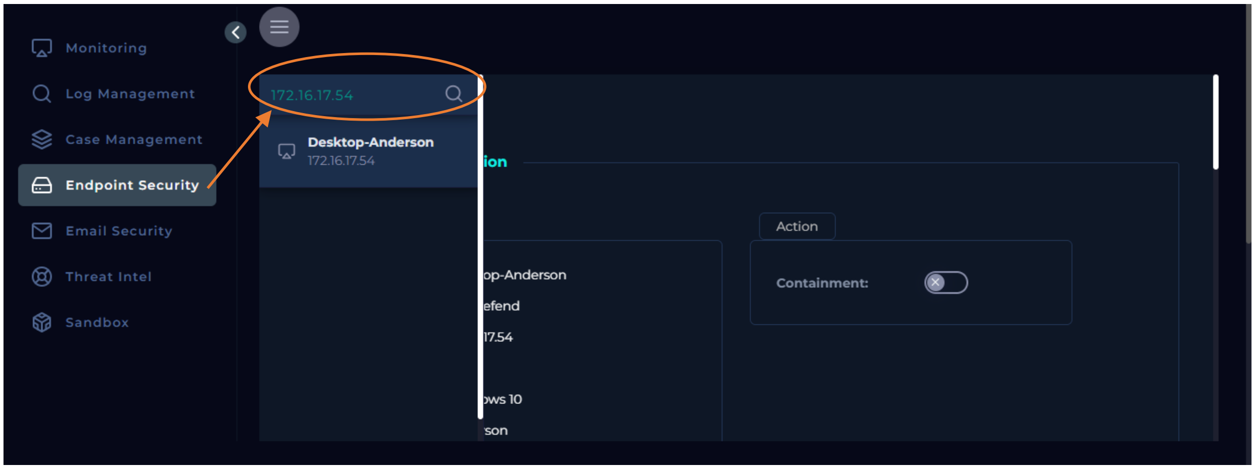
**VirusTotal analysis for the file hash 50459310eded4c520ab5c9e3626a9300

VirusTotal analysis of the file hash 50459310eded4c520ab5c9e3626a9300 is in detection section but there is some malicious IP`s were connected to the hash file.

Reference result.

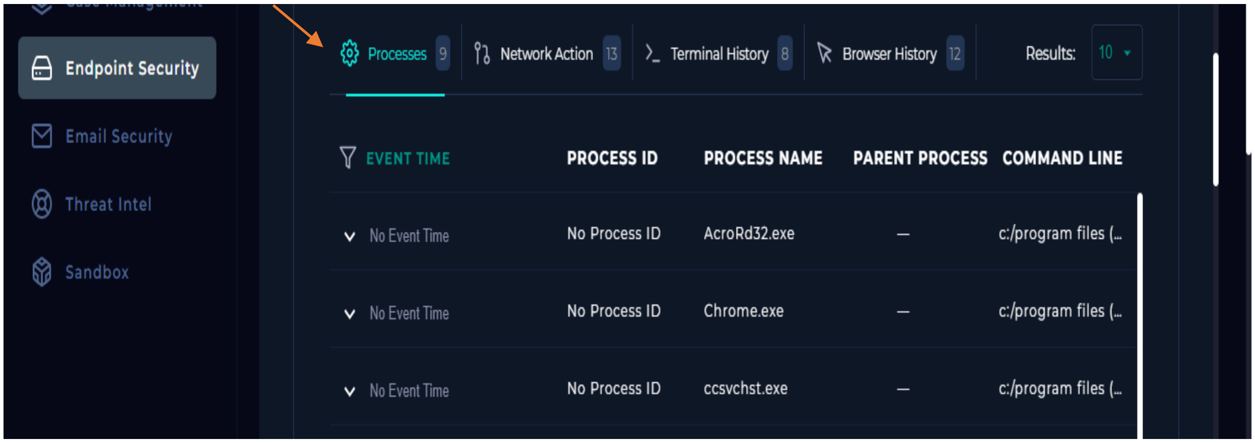
.

Endpoint Security:



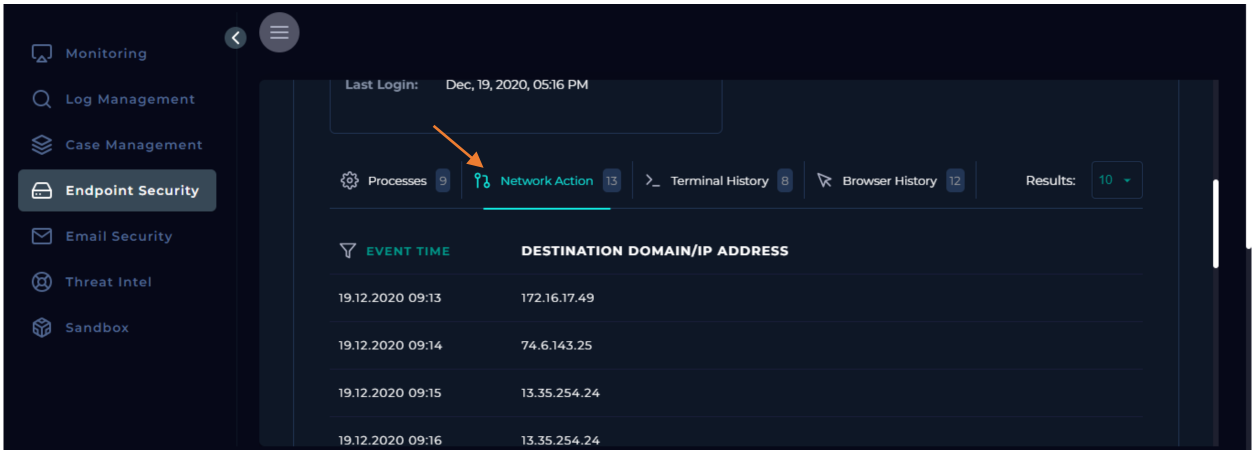
We conducted an analysis of the following sections:

- **Processes section**: everything is normal (see attached photo).



EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
No Event Time	No Process ID	AcroRd32.exe	–	c:/program files (...
No Event Time	No Process ID	Chrome.exe	–	c:/program files (...
No Event Time	No Process ID	ccsvchst.exe	–	c:/program files (...

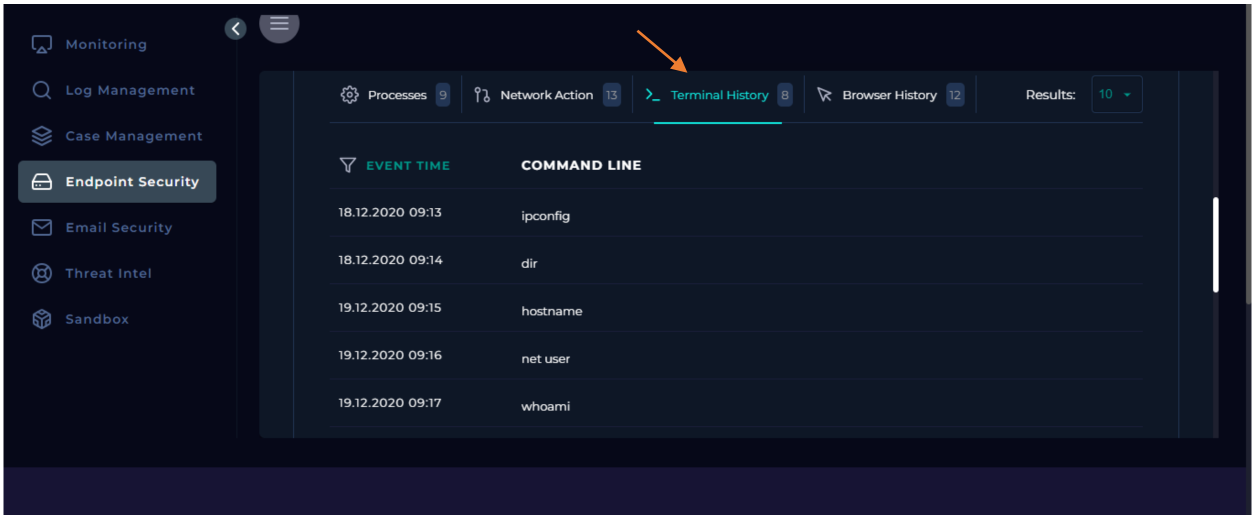
- **Network Action section**: everything is normal (see attached photo).



Last Login: Dec, 19, 2020, 05:16 PM

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
19.12.2020 09:13	172.16.17.49
19.12.2020 09:14	74.6.143.25
19.12.2020 09:15	13.35.254.24
19.12.2020 09:16	13.35.254.24

- **Terminal History section**: In this section, I will provide a step-by-step analysis of the attacker's actions following the successful exploitation of the system. This detailed breakdown will outline each phase of the attack, highlighting the methods used, the assets targeted, and the subsequent impact on the compromised system.



EVENT TIME	COMMAND LINE
18.12.2020 09:13	ipconfig
18.12.2020 09:14	dir
19.12.2020 09:15	hostname
19.12.2020 09:16	net user
19.12.2020 09:17	whoami

Based on the terminal record history, here is a detailed step-by-step breakdown of the attacker's actions:

1. Initial Reconnaissance (ipconfig)

Timestamp: 18.12.2020 09:13

Command: `ipconfig`

- The attacker’s first step was to gather network configuration details of the compromised machine. By running `ipconfig`, they collected valuable information such as IP addresses, subnet masks, and gateway configurations. This helps the attacker understand the network layout and identify potential next targets or routes for lateral movement.

2. Directory Exploration (dir)

Timestamp: 18.12.2020 09:14

Command: `dir`

- The attacker used the `dir` command to list the contents of the current directory, likely to identify important files or directories that could contain sensitive information. This also gives an idea of the system's structure and files available for exploitation.

3. System Identification (hostname)

Timestamp: 19.12.2020 09:15

Command: `hostname`

- On the following day, the attacker executed `hostname` to obtain the name of the compromised system. This helps the attacker uniquely identify the machine in case they are attacking multiple systems within the network.

4. Enumerating Users (net user)

Timestamp: 19.12.2020 09:16

Command: `net user`

- The `net user` command was used to list all user accounts on the system. This step is essential for understanding the available accounts and determining which ones might have administrative privileges for privilege escalation attempts.

5. Confirming Current User Identity (whoami)

Timestamp: 19.12.2020 09:17

Command: `whoami`

- By running `whoami`, the attacker confirmed the current user account they are operating under. This allows them to understand their level of access and privileges on the compromised system.

6. Process Enumeration (tasklist)

Timestamp: 19.12.2020 11:18

Command: `tasklist`

- The attacker ran `tasklist` to view all running processes on the system. This command reveals important details about the active applications and services, which can be leveraged to identify security software or processes that can be killed or exploited further.

7. Targeting a Specific User Account (net user anderson)

Timestamp: 19.12.2020 11:20

Command: `net user anderson`

- The attacker specifically queried details of the user account “anderson” using the `net user anderson` command. This suggests that the attacker might be focusing on this account, possibly due to its elevated privileges or sensitive nature.

8. Network Reachability Check (ping 172.16.20.1)

Timestamp: 19.12.2020 11:21

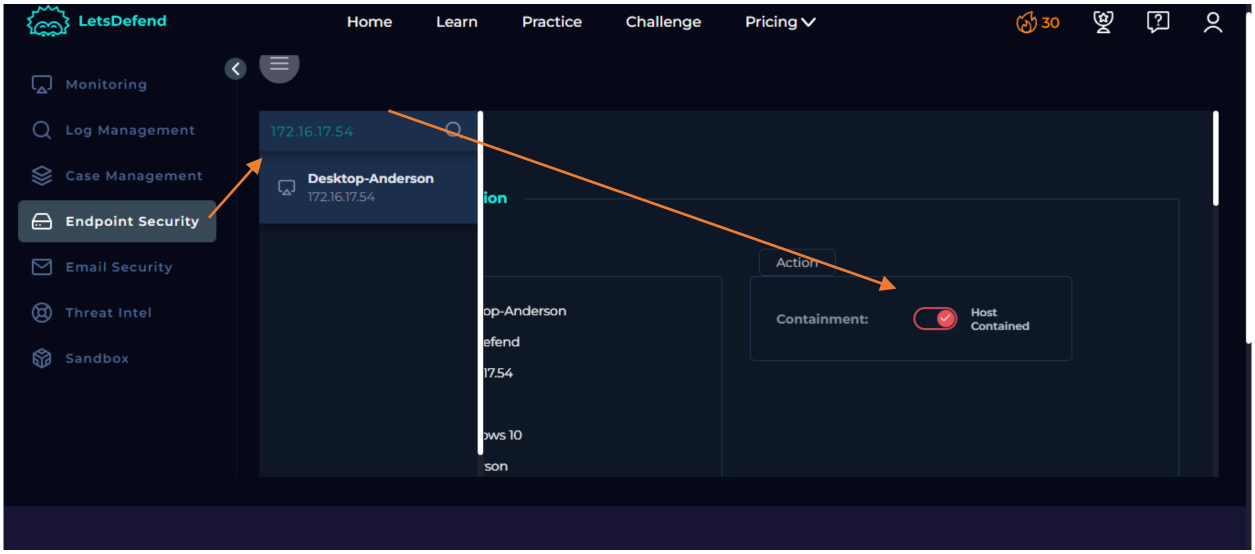
Command: `ping 172.16.20.1`

- Lastly, the attacker used the `ping` command to check the network connectivity and reachability of the IP address `172.16.20.1`. This could indicate an attempt to communicate with another machine within the network or test the connection to a potential target for lateral movement.

Summary

- The attacker initially gathered system and network information to understand the environment. They explored user accounts and processes to assess potential targets and privileges. The specific query for the user “anderson” suggests interest in escalating privileges or accessing sensitive data. Finally, the ping command indicates an attempt to check connectivity, possibly for further exploitation within the network.

The attacker had full control of the compromised device. Immediate containment is required to prevent further impact.



172.16.17.54

Desktop-Anderson
172.16.17.54

op-Anderson
efend
17.54
ows 10
son

Containment: Host Contained

We have successfully initiated the containment.

Conclusion:

The incident in question, identified as **Event ID 71** and categorized under **Rule SOC134 – Suspicious WMI Activity**, represents a significant breach involving external communication and unauthorized access to a corporate asset. Through a series of meticulously executed steps, the attacker gained full control of **Desktop-Anderson**, indicating a high level of intent and sophistication in the attack.

The presence of **WMI activity** and the execution of the **exec.bat** file, coupled with suspicious external communication to IP **204.79.197.203**, raised immediate concerns. Upon conducting a comprehensive threat intelligence analysis, VirusTotal flagged the external IP as **malicious** according to three separate security vendors, including **CRDF, Criminal IP, and G-Data**, confirming the malicious nature of the traffic. This external communication underscores the likelihood of data exfiltration or potential further lateral movement across the network.

The attack leveraged **internal IP 172.16.17.54**, signaling an insider origin for the malicious activity. However, the lack of logs during the specified period suggests that the attacker deliberately cleared their tracks, a technique often used by advanced threat actors to hinder forensic investigation and avoid detection. This methodical clearing of logs emphasizes the necessity for improved log retention and tamper-proof logging mechanisms within the organization to prevent future attacks from evading detection.

Forensic Breakdown of the Attack

The attacker's step-by-step process within the compromised device, outlined in the terminal history, reveals a clear methodology aimed at reconnaissance, privilege escalation, and potential lateral movement. After gaining access, the attacker first gathered system and network configuration details using the **ipconfig** and **dir** commands, gaining insight into the network architecture and local file system structure. This stage was essential for understanding the environment and identifying valuable targets or sensitive files.

Following this initial reconnaissance, the attacker ran several commands to enumerate the local users, processes, and system identity, including **net user, hostname, and tasklist**. The focus on the user account **“anderson”** suggests a targeted approach, possibly due to elevated privileges or valuable information associated with the user. The **ping** command executed towards the internal IP **172.16.20.1** could indicate an attempt to map the network further and test connectivity for potential lateral movement to other systems within the environment.

The attacker's ability to execute these commands undetected, and without triggering significant alerts until the external communication, highlights the need for more robust detection mechanisms at the endpoint level. **Behavioral monitoring** and **privilege escalation detection** could have provided earlier warnings, limiting the attacker’s ability to freely explore the compromised system.

Impact and Containment

The malicious nature of the **exec.bat** file, combined with the suspicious communication to an external IP flagged for malicious activity, confirms that this incident posed a significant threat to the organization's security. The fact that the attacker wiped the logs reinforces the notion that the attack was highly coordinated and deliberate, aimed at bypassing detection and leaving minimal forensic evidence.

The timeline of the attacker’s activity—from **reconnaissance** to **network exploration**—indicates a concerted effort to escalate privileges, identify key assets, and possibly move laterally within the network. The querying of the **“anderson”** user account and the subsequent attempt to ping another internal IP suggest the attacker was probing for further weaknesses in the system, likely aiming to expand their foothold within the network.

Immediate containment actions were crucial to limit the scope of the attack and prevent any further compromise. Following the identification of suspicious WMI activity, the compromised device was successfully contained, cutting off any ongoing malicious communication with the external IP. Given the depth of the attack, a full **forensic analysis** of the affected device and network segment is recommended, with special attention to potential lateral movement and data exfiltration attempts.

Recommendations for Future Defense

This incident serves as a critical reminder of the importance of comprehensive **endpoint security measures**, robust **network segmentation**, and continuous **monitoring** of internal traffic. The attacker’s ability to clear logs and avoid detection for a prolonged period highlights the need for **advanced detection mechanisms**, such as **endpoint detection and response (EDR)** solutions capable of identifying abnormal behavior and **file integrity monitoring** systems to detect log tampering.

Further, **privilege management** policies should be revisited, especially concerning critical user accounts like “anderson,” which may hold elevated privileges that could be exploited. Regular audits of user activity, combined with **network traffic analysis**, would have provided earlier insights into the attacker’s attempts to communicate with external entities.

In conclusion, the attack on **Desktop-Anderson** represents a sophisticated attempt at unauthorized access and potential lateral movement. While containment was successful, the depth of the attacker’s activities, including reconnaissance, user enumeration, and external communication, emphasizes the need for **enhanced monitoring**, **advanced detection capabilities**, and **stronger endpoint defenses** to mitigate future risks. The integration of these measures will provide the organization with improved resilience against similar incidents and bolster its overall security posture.