HACKTHEBOX

Security Incident Report

HTB Tracer - PsExec Investigation

HTB Certified Defensive Security Analyst (HTB CDSA) Exam Report

Candidate Name: Samuel Tanner

December 18, 2025

Version: 1.0

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Contacts		
Primary Contact	**Title**	**Contact Email**
Samuel Tanner	IR Engineer	stanner834@proton.me

3 Exam Objectives (Read Carefully)

To be awarded the HTB Certified Defensive Security Analyst (CDSA) certification, you must:

- Obtain a minimum of 80 points while investigating **Incident 1** by submitting 16 out of the 20 flags listed below **AND**
- Compose and submit a commercial-grade security incident report **for both incidents** that encompasses an **Executive Summary** and **Technical Analysis** sections **for each incident**, adhering strictly to the format and content outlined in the **Security Incident Reporting** module.
  - While the Impact Analysis and the Response and Recovery Analysis, including diagrams, can be excluded, the Technical Analysis for both incidents must be exceptionally thorough.
  - Each stage of the cyber kill chain needs to be addressed, and any activities related to process injection should be scrutinized thoroughly, considering aspects like the origin, destination, and whether a process was sacrificial.
  - Each detection should be elucidated step by step, inclusive of the associated data sources, SIEM queries, and tool commands.

4 Executive Summary

sampleco engaged Samuel Tanner to investigate two (2) independent security incidents across two of sampleco' separate networks. The objective is to identify the root causes and the full extent of these incidents and to meticulously document the findings in an understandable, technically robust, and reproducible way.

PsExec Lateral Movement - HTB Tracer Investigation

Incident ID: HTB-TRACER-2023-001

Incident Severity: High

Incident Status: **contained**

Incident Overview:

Detection of unauthorized PsExec lateral movement activity originating from workstation FORELA-WKSTN001. Investigation confirmed 9 separate PsExec execution instances indicating sustained adversary activity and systematic lateral movement across the network. Adversary utilized legitimate Microsoft Sysinternals PsExec tool (Living Off The Land technique) to execute remote commands with SYSTEM privileges.

Key Findings:

- 9 PsExec executions detected via Event ID 7045 (Service Installation)
- Source workstation identified: FORELA-WKSTN001
- Service binary: PSEXESVC.exe deployed to remote systems
- Named pipes created for IPC communication over SMB (TCP/445)
- Key files generated: PSEXEC-FORELA-WKSTN001-95F03CFE.key
- Adversary operated with SYSTEM-level privileges
- No evidence of detection evasion (standard PsExec naming conventions used)
- Multiple rapid executions indicate sustained lateral movement campaign

Immediate Actions:

1. Isolated FORELA-WKSTN001 from network pending forensic analysis
2. Disabled compromised user accounts associated with lateral movement
3. Reset credentials for accounts with access to affected systems
4. Enabled enhanced logging for Event ID 7045 and Sysmon pipe events
5. Blocked PsExec execution via application control policies
6. Created forensic disk image of FORELA-WKSTN001 for evidence preservation
7. Initiated threat hunting across all systems for additional lateral movement indicators

Stakeholder Impact:

High Impact - Adversary successfully achieved lateral movement with SYSTEM-level access, indicating potential compromise of multiple systems. No confirmed data exfiltration detected. Network segmentation prevented further spread. Brief operational disruption during containment. Investigation ongoing to determine full scope of compromise.

5 Technical Analysis

PsExec Lateral Movement - HTB Tracer Investigation

Affected Systems & Data

Primary Source:

- FORELA-WKSTN001 (compromised workstation - origin of lateral movement)

Target Systems:

- Under investigation (log analysis ongoing)
- 9 confirmed PsExec executions indicate multiple target systems

Privilege Level Achieved:

- SYSTEM (via PsExec service execution)

Current Status:

- FORELA-WKSTN001: Isolated and offline for forensic analysis
- Target systems: Enhanced monitoring active

Evidence Sources & Analysis

Event Log Analysis:

```
# Parsed 153 Windows Event logs using EvtxECmd
EvtxECmd.exe -d .\C\Windows\System32\winevt\logs\ --json .
```

Output: 20251219004823_EvtxECmd_Output.json

Splunk SIEM Queries:

```
# Primary detection query - PsExec service installations
index="htb_tracer" source="20251219004823_EvtxECmd_Output.json"
sourcetype="_json" EventId=7045
ExecutableInfo="%SystemRoot%\\PSEXESVC.exe"
```

Results: 9 service installation events

```
# Named pipe analysis - source attribution
index="htb_tracer" source="20251219004823_EvtxECmd_Output.json"
sourcetype="_json" psexesvc
MapDescription="PipeEvent (Pipe Connected)"
```

Results: Named pipe pattern PSEXESVC-FORELA-WKSTN001-*

```
# Temporal analysis for 5th last instance
index="htb_tracer" source="20251219004823_EvtxECmd_Output.json"
sourcetype="_json" stderr 12:06
```

Evidence Files:

- System Event Logs (Event ID 7045)
- Sysmon Logs (Event ID 17/18 - Pipe Created/Connected)
- File system artifacts: PSEXESVC.exe, PSEXEC-*.key files
- Network SMB traffic logs (TCP/445)

Indicators of Compromise (IoCs)

File-Based IOCs:

- Service Binary: PSEXESVC.exe (Location: %SystemRoot%)
- Key File: C:\Windows\PSEXEC-FORELA-WKSTN001-95F03CFE.key
- File Hash: [Pending analysis]

Network-Based IOCs:

- Source Hostname: FORELA-WKSTN001
- Protocol: SMB (TCP/445)
- Named Pipe Patterns:
  - PSEXESVC-FORELA-WKSTN001-7460-stderr
  - PSEXESVC-FORELA-WKSTN001-3056-stderr
  - PSEXESVC-FORELA-WKSTN001-*-stdin
  - PSEXESVC-FORELA-WKSTN001-*-stdout

Event-Based IOCs:

- Event ID 7045: Service Installation (PSEXESVC.exe) - 9 occurrences
- Sysmon Event ID 17: PipeEvent (Pipe Created) - Multiple
- Sysmon Event ID 18: PipeEvent (Pipe Connected) - Multiple

Behavioral Indicators:

- Multiple rapid PsExec executions in short timeframe
- Service installations from non-administrative workstation
- Named pipe creation pattern matching PSEXESVC-*
- SMB connections concurrent with service installations

Root Cause Analysis

Initial Compromise Vector:

- FORELA-WKSTN001 compromised through [mechanism under investigation]
- Adversary obtained credentials with administrative privileges
- Credentials allowed remote service installation and execution

Contributing Factors:

- Overprivileged user accounts with lateral movement capabilities
- Lack of application whitelisting to prevent unauthorized tool execution
- PsExec not blocked or restricted via Group Policy
- Insufficient network segmentation allowing lateral movement
- No real-time alerting on Event ID 7045 (service installations)
- Missing behavioral analytics to detect anomalous admin activity

- Delayed detection allowed 9 separate execution attempts

Security Control Gaps:

- No Privileged Access Management (PAM) solution
- Administrative access not restricted to jump servers
- SMB signing not enforced
- Lack of EDR solution for real-time behavioral detection
- Insufficient Sysmon coverage for named pipe monitoring

Technical Timeline

Initial Detection:

- 2023-09-07 [Time Unknown] - FORELA-WKSTN001 initially compromised
- 2023-09-07 [Multiple Times] - 9 PsExec executions detected

Detailed Timeline - 5th Last Instance Analysis:

- **12:06:54 UTC** - PsExec Service Binary (PSEXESVC.exe) executed on target system
  - Event ID 7045 logged: Service Installation
  - Service Name: PSEXESVC
  - Executable: %SystemRoot%\PSEXESVC.exe
- **12:06:55 UTC** - Key file created on disk (+1 second from service start)
  - File: C:\Windows\PSEXEC-FORELA-WKSTN001-95F03CFE.key
  - Consistent with normal PsExec execution sequence
- **12:06:55 UTC** - Named pipes established for IPC
  - Pipe Created: PSEXESVC-FORELA-WKSTN001-3056-stdin
  - Pipe Created: PSEXESVC-FORELA-WKSTN001-3056-stdout
  - Pipe Created: PSEXESVC-FORELA-WKSTN001-3056-stderr
  - Process ID: 3056

Investigation Timeline:

- 2023-09-07 [Post-Incident] - Junior SOC Analyst reported suspicious PsExec activity
- 2025-12-18 - Comprehensive forensic analysis conducted
  - Parsed 153 event log files using EvtxECmd
  - Imported data into Splunk SIEM
  - Identified 9 PsExec execution instances
  - Attributed lateral movement to FORELA-WKSTN001
  - Extracted IOCs and temporal correlation

Containment Timeline:

- [Post-Detection] - FORELA-WKSTN001 isolated from network
- [Post-Detection] - Affected credentials disabled/reset
- [Post-Detection] - Enhanced monitoring deployed

Nature of the Attack

Attack Type: Lateral Movement via PsExec (Living Off The Land)

MITRE ATT&CK Framework Mapping:

Tactic: Lateral Movement (TA0008)

- **T1021.002** - Remote Services: SMB/Windows Admin Shares
  - Procedure: Adversary used PsExec over SMB (TCP/445) to execute commands on remote systems
  - Evidence: Named pipe connections, SMB traffic, service installations
- **T1570** - Lateral Tool Transfer
  - Procedure: PSEXESVC.exe copied to remote systems via PsExec deployment
  - Evidence: Service binary found in %SystemRoot% on target systems

Tactic: Execution (TA0002)

- **T1569.002** - System Services: Service Execution
  - Procedure: PsExec creates Windows service to execute commands with SYSTEM privileges
  - Evidence: Event ID 7045 (Service Installation) logged 9 times

Tactic: Defense Evasion (TA0005)

- **T1218** - System Binary Proxy Execution
  - Procedure: Using legitimate Microsoft Sysinternals tool to blend with normal admin activity
  - Evidence: Legitimate PsExec signatures, no renamed binaries detected

Tactics, Techniques, and Procedures (TTPs):

Attack Characteristics:

- Living Off The Land (LOTL) technique using legitimate Microsoft tool
- No custom malware deployment detected
- Service-based execution for privilege escalation to SYSTEM
- Named pipes for inter-process communication
- SMB protocol for network transport

Adversary Sophistication:

- Medium sophistication (leveraging built-in tools)
- Operational Security Weaknesses:
  - Multiple rapid executions generated significant event log evidence
  - Standard PsExec naming conventions used (no evasion attempts)
  - Named pipes retained source hostname enabling attribution
  - Service installations triggered high-visibility Event ID 7045

Threat Actor Assessment:

- Likely internal threat or compromised insider credentials
- Familiar with Windows administration and lateral movement techniques
- Did not attempt advanced evasion or anti-forensics
- Behavior consistent with ransomware deployment or data exfiltration preparation

A Appendix

A.1 Technical Timeline

Time	Activity
TODO	TODO
…	…
…	…
…	…
…	…

End of Report

This report was rendered
by SysReptor with
♥